Security University

1821 Michael Faraday Drive, Suite 100
Reston, VA 20190

Super Qualified

Sondra Schneider,
President, Security University
1821 Michael Faraday Dr, Suite 100
Reston, VA 20190
203-249-8364
s0ndra@securityuniversity.net
Jan 2025

never
never
never
give
up

(winston churchill)

The SU Program & Course Catalog is edited & published by SU a Vocational Non-College Degree School. It serves as a general source of information for SU students. The information in the Catalog should not be regarded as a contract between the students and SU. All information is subject to change without warning. SU is located at 1821 Michael Faraday Dr. Suite 100, Reston VA 20190, 203-249-8364
SU does not provide financial aid, loans, tuition assistance, or scholarships. A student can independently request a loan from a bank.
SU is Army, Army Reserve, MYCAA Spouse and USAF Credential Assistance Program approved. SU is MSA-CESS accredited until 2032.

Certified to Operate by State Council of Higher Education for Virginia (SCHEV).

"This institution is approved to provide classes approved by the ARMY COOL & ARMY Ignited Program and approved to offer GI Bill® apprenticeship educational benefits by the Virginia State Approving Agency. "*GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA). More information about education benefits offered by VA is available at the official U.S. government website at http://www.benefis.va.gov/gibill.*"

Welcome

Dear Future Cyber Professional,

Let me be the first to welcome you to SU and to the hot cyber security profession and welcome to SU's Center for Qualified Cyber Security Excellence & Mastery.

We train leaders in cyber security. Whether you're starting your cyber IT career, mastering your hands-on skills, or developing your team, we're with you. We believe education is life-long learning and career growth. This catalog is designed to provide you all you need to know about your SCHEV approved, MSA-CESS accredited non-degree Qualified Cyber Security Certificate Program(s) of Mastery.

Perception of higher education is shifting and skills based training is more important than ever. Don't let the lack of a degree define you. You can earn a SU Qualified Cyber Security Certificate and gain critical experience in the field. There is an increase in cyber job postings that don't require a degree, and studies suggest the future is hands-on, performance based skills talent. As a skilled cyber security professional you are a highly valuable asset.

Cyber security is by far the hottest job in tech. SU's Center for Cyber Security Excellence and Mastery Programs include 10 performance based courses with industry certifications with practicums to make you eligible for cyber employment. When it comes to professional growth, the right program can make all the difference. We pride ourselves on providing courses led by industry experts with years of hands-on experience. They don't just teach; they share actionable insights and practical applications to help you thrive in your job from day one.

We have made every effort to make this catalog relevant and understandable in order to answer any questions you might have about your school experience here at SU. If there are [any] further questions, call me, your school president, or any member of our team who is happy to assist you. I urge you to take full advantage of SU's programs. I think you will find that our escalating cyber curriculum's are critical to build your skills and competencies beyond your expectations at all levels.

Our qualified cyber security programs inspire confidence to achieve a better lifestyle for you and your family. While it is important to learn great technical cyber skills, it is also essential for you to learn how to communicate with your cyber peers, C-level management and the community of cyber professionals. When you master those skills, you will find that "anything is possible".

Lastly, SU's mission is to upskill the IT cyber workforce. Cyber security is a critical mission to keep our nation cyber safe. Engage, participate and enjoy this journey.

I wish you the best of luck and success in the coming months and for the rest of your cyber security career. I look forward to meeting you in the near future to personally welcome you to Security University and the hottest jobs in tech.

With warmest regards,

Sondra Schneider

President, Security University

SU Mission

The mission of SU is striving to provide our students with the highest quality information security education available through our Cyber Security, Information Security, and Information Assurance Certification training for IT Security Professionals Worldwide.

To provide quality cyber security career- oriented higher education to a diverse student population. In addition, we incorporate both professional and personal development into our programs to help our students achieve a lifetime of success.

In coordination with our mission, SU has established the following goals:

- To offer students real-life based programs developed by instructors, faculty and staff through regular assessment and consultation with workforce offices, other educators, industry leaders, and potential employers (desires) of our students and life long learning.

- To offer accelerated learning scheduling options to accommodate the distinctive needs of the adult non-traditional students.

- To assist students in realizing their potential by establishing basic IT/cyber skills assessment, with an escalating step by step learning methodology with hands-on performance based competencies based on assessment and practicum evaluation.

- To provide student services that contribute to students' success and achievement

- To provide career development strategies and employment assistance to facilitate students' successful transition from military careers or the advancement of their cyber careers

- To provide highly motivated and qualified graduates to meet the current and projected needs of the defense contractors and employers we serve

The goals of SU are simple and unassuming. We want to teach students the best possible cyber security education, skills and techniques to become successful in the cyber security profession.

SU History

Since 1999 SU and the Center for Cyber Security Excellence and Mastery has led the cyber security professional education industry in hands-on performance based cyber security computer training & education. Success is doing it once. Mastery is the ability to do it repeatedly at the same level of excellence. Many people will experience success, but few will experience cyber mastery.

In 1985 Sondra Schneider moved from Miami Fla to NYC for Equitrac systems. Realizing the need for connecting systems, *sneakernet* was a solvable communications issue. She focused on fiber connectivity and what could be run on fiber. Before founding Security University, Sondra worked at Fujitsu Networks UK. Fujitsu funded the first e-community pilot. Next Sondra worked for Datapoint Systems who created the 8080 data chip-set [Intel inside] and created the first p2p video on the desktop player for 30 frames full-motion video over copper. Early 1990 Sondra worked at Metropolitan Fiber Systems MFS Datanet selling fiber connectivity [the Internet] to AOL, PSINet, Mindspring, Earthlink, and Prodigy creating and installing fiber installations on the eastern seaboard [what became} the Internet fiber backbone. After MFS Datanet, she became the first ATT Internet person when everything was analog, tasked with increasing 800 revenue she created the first 1800 flowers webpage and posted it to what had become "the internet "- 24 months before the netscape browsers existed, or 36 months before wallet side technology existed, increasing the 800 dial client revenue. By late 1994 she met the firewall developers from BBN (Bolt Beranek, Newan) and contracted BBN to install the first ATT client firewall at the White House. In 1996 Sondra left ATT for start-up; The WheelGroup. A USAF Information Warefare group. Managing the Northeast for the Netranger scanning tool, the first live scanning intrusion detection tool that could see and kill bad guys on your network. In 1996 Wheelgroup was acquired by CISCO and Sondra used the stock proceeds to start the first information security practice in the USA called IFSec. Sondra created "tiger teams' to mitigate new digital threats against networks, welcome banners, and high use systems. In 1999 Sondra sold IFSec to PriceWaterhouse and started Security University (SU) "Center for Qualified Cyber Security Excellence & Mastery".

The IT/ Cyber talent shortage started in 1996. Everyone lacked qualified IT/cyber talent and growing. SU was first to deliver hands-on performance based programs, classes and certifications creating SU's Q/SA "Qualified / Security Analysis/ Penetration Testing Skills and Methodologies" class delivered at the 2008 Blackhat Conference, designed to validate student's cyber security skills. In 2001 SU was first to deliver hands-on Software Security Coder Training and Certification, and in 2004 SU was the first to provide the Qualified/ Forensic Professionals Validated Skills Program and License for Microsoft. For 25 years, SU courses and Security University Testing exams have provided critical cyber security skills to qualify and validate the cyber security workforce.

SU's Center for Cyber Security Excellence and Mastery delivers SU's Qualified Cyber Security Certificate Programs of Mastery that can be completed in 2-7 years. Each Qualified program provides essential credentials to validate student's hands-on mastery of their cyber skills.

The SU's Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery designation purpose is to recognize "qualified individuals" who have distinguished themselves as knowledgeable, competent and proficient cyber security practitioners who have validated their hands-on mastery of their tactical security skills. Experience isn't enough. Employers need something quantifiable and verifiable to show them their staff is competent to do the task/ job with hands on expertise from rigorous skills. This provides corporations and governmental agencies worldwide the opportunity to hire highly *qualified, certified* and *validated* cyber security practitioners who have mastered hands-on cyber security skills. Former students C. Mercer and J. Hutson say once they earned (a number of) performance based SU cyber security certifications they had a higher earning potential with expanded career opportunities. Being *qualified*, *certified with validated* with hands on cyber security skills makes a statement about who you are and recognized as a serious, knowledgeable and dedicated cyber security professional – part of a globally recognized family of qualified and validated cyber security professionals.

SU is SCHEV Certificated to Operate in VA, and MSA-CESS Accredited until 2032.

SU Overview

Since 1999, SU has addressed the need for qualified and validated cyber security professionals at SU's Center for Cyber Security Excellence and Mastery in Reston Virginia. SU's Qualified/ Information Security Professional Certificate Program of Mastery [Q/ISP] validates cyber security skills for IS & IA professionals in the DMV and our nation's cyber security workforce.

The Q/ISP Qualified Cyber Security Certificate Programs of Mastery include intense practicums that validate a student's mastery of their cyber skills. Employers and students choose SU for professional development and continuing education, qualified cyber security certificate programs, to refresh their cyber/IT career, expand their hands-on cyber skills and earn credentials that make them more attractive to employers and win contracts. The 10 year trend among non-credit seeking adult learners is the stackability of certifications and credentials to increase my salary and quality of life.

Most of our students are kinesthetic learners, student who comprehend best by doing. SU's goal is to have the students go back to work with useful knowledge and a practical skillset. Cyber is a psychomotor skill that requires experimentation, practice, and application. The labs are taught by practitioner instructors. The instructor measures student skills to apply a lab/lecture balance accordingly. The student classroom is designed so that students acquire practical hands-on mastery experience with a complete menu of cyber skills to help students gain high wage, in-demand cyber employment.

SU's Qualified Cyber Security Certificate Programs of Mastery methodology comes from 25 years of cyber education and performance based education using an accelerated stacked and latticed "Schneider Method" of successively more challenging courses delivered step by step. **Students have up to seven years to complete a Qualified Certificate Programs of Mastery** that develops key cyber skills, cyber habits and cyber mastery.

SU's Qualified Cyber Security Certificate Programs of Mastery (Q/ISP, Q/IAP, Q/WP, Q/SSE, Q/CND) *rigorously* qualify and validate cyber security professionals with hands-on, performance based tactical security skills necessary to deliver the capability to establish, operate, defend, exploit, and attack in, through, and from the cyberdomain with a consistent process and methodology.

SU library of continuing education aids, which include a UTube channel, textbooks, periodicals, DVD's, and other reference materials that support the cyber education process. Students receive e-books and SU's online quiz engine to use throughout their Certificate program.

SU's goal is strategic so cyber security professionals achieve mastery at the highest level. A specific and measurable vocational result is described in each class to help you reach and achieve your hands-on cyber security goals.

Sondra Schneider, President
s0ndra@securityuniversity.net
1-203-249-8364

SU Center for Qualified Cyber Security Excellence & Mastery
5 SU Qualified/ Cyber Security Professional® Certificate Programs of Mastery

Welcome to SU's Q/ISP, Q/IAP, Q/WP, Q/SSE, Q/CND Certificate Programs of Mastery Framework. Here students have up to 7 yrs to complete a SU Qualified/ Cyber Security Certificate Program. SU Programs are SCHEV Approved and MSA-CESS Accredited Vocational Non-Degree Certificate Programs. Programs are face-to-face or hybrid modalities that may lead to cyber certs, credentials & employment.

Q/ISP
QUALIFIED/ INFORMATION SECURITY PROFESSIONAL
Q/EH
QUALIFIED/ ETHICAL HACKER
Q/SA
QUALIFIED/ SECURITY ANALYST
Q/PTL
QUALIFIED/ PENETRATION TESTER LICENSE
Q/FE
QUALIFIED/ FORENSICS EXPERT
Q/ND
QUALIFIED/ NETWORK DEFENDER
Security University

Supra Qualified

SU Qualified Cyber Security Certificate Program List 2025-2026 www.securityuniversity.net

	Qualified Matters. **Success is doing it once.** Mastery is the ability to do it repeatedly at the same level of excellence. Many people will experience success, but few will experience mastery.		
	Course Title Class fee excludes exam fee* - exams are required to graduate	Course Hours	Retail Costs
	SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery * This is the cost of the program when you pay tuition up front or opt to pay by class w/exam below.	936 hrs	Program $26,500*
	The *SU Q/ISP®* Certificates Program of Mastery and related micro badges identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their cyber knowledge and proficiency with validated security skills and hands-on practical security experience *defending network mission assurance*.		
R	Q/SA® Qualified/ Security Analyst Certification Class w/exam	72	$3,990
R	Q/PTL® Qualified/ Penetration Tester License workshop	72	$3,900
R	Q/EH® Qualified/ Ethical Hacker Certification Class w/exam	72	$3,990
R	Q/ND® Qualified/ Network Defender Certification Class w/exam	72	$3,990
R	Q/FE® Qualified/ Forensic Expert Certification Class w/exam	72	$3,990
R	SU CISSP® Certified Information Security Systems Professional Class*	72	$3,990
R	SU Security+® CompTIA Certification Class w/exam	72	$3,490
R	SU SecurityX® - [formerly CASP] Certification Class w/exam	72	$3,990
R	Linux/UNIX® Security Certification Class w/exam	72	$3,990
R	Cloud Computing Security Knowledge Certification Class w/exam	72	$3,990
R	Q/PTL® Qualified/ Penetration Tester License Practicum	72	$3,990
R	Q/ND® Qualified/ Network Defender Certification Practicum	72	$3,990
R	Q/FE® Qualified/ Forensic Expert Certification Class Practicum	72	$3,990
E	SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam	72	$3,990
E	Advanced Cloud Security and Applied SecDevOps Certification Class w/exam	72	$3,990
E	TCP/IP and Key Features of Wireshark Class w/exam	72	$3,990
E	How to Conduct Network Vulnerability Analysis Class w/exam	72	$3,990
E	Python Forensics Certification Class w/exam	72	$3,990
E	PowerShell Forensics Certification Class w/exam	72	$3,990
E	Python/Powershell Incident Response Certification Class w/exam	72	$3,990
	SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery * This is the cost of the program when you pay tuition up front or opt to pay by class w/exam below.	936 hrs	Program $26,500*

SU Q/IAP® Certificate Program of Mastery and related micro badges {Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission *assurance*.			
R	Q/AAP® Qualified/ Access, Authentication & PKI Professional Certification Class w/exam	72	$3,990
R	Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam	72	$3,990
R	Q/CA CMMC Cyber Security Maturity Model Certification Class w/exam	72	$3,990
R	SU Security+® CompTIA Certification Class w/exam	72	$3,490
R	SU CISSP® ISC2® Certified Information Security Systems Professional Class*	72	$3,990
R	SU SecurityX® - [formerly CASP] Certification Class w/exam	72	$3,990
R	SU CISA® Certified Information Security Auditor Certification Class w/exam	72	$3,990
R	SU CISM® Certified Information Security Manager Certification Class*	72	$3,990
R	Certified ISO 27001 SU ISMS® Lead Auditor Certification Class w/exam	72	$3,990
R	Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam	72	$3,990
R	SU CMMC Cyber Security Maturity Model Practicum	72	$3,990
R	PMP Project Manager Professional Certification Class*	72	$3,990
R	Q/ISO Qualified/ Chief Information Security Officer Certification Class w/exam	72	$3,990
E	Scrum Master Certification Class w/exam	72	$3,990
E	ITIL V4 Certification Class w/exam	72	$3,990
E	SU CIPP® Certified Information Privacy Professional Certification Class w/exam	72	$3,990
E	Q/CSO Qualified/Cyber Security Officer Certification Class w/exam	72	$3,990
E	ISSEP® ISC2® Information Security Systems Engineer Certification Class w/exam	72	$3,990
E	ISC2 SSCP Systems Security Certified Practitioner Certification Class w/exam	72	$3,990
E	Qualified/ Internet Threat Security Awareness Training and Compliance for Mgt /exam	72	$3,990
E	Qualified/ Security Hacking Certificate Class for Managers w/exam	72	$3,990
SU Q/WP® Qualified Wireless Professional Certificate Program of Mastery CPoM * This is the cost of the program when you pay tuition up front or opt to pay by class w/exam below.		936	Program $26,500*
SU's Q/WP Certificate Program of Mastery mission is to educate security professionals in the technology of wireless infrastructures, [WLAN] products, enabling students to design, deploy, secure and manage complex wireless connections securely.			
R	Q/WAD® Qualified/ Wireless Analyst & Defender Certification Class w/exam	72	$3,990
R	Q/WP® Qualified/ Wireless Professional Certification Class w/exam	72	$3,990
R	Q/WSP® Qualified/ Wireless Security Professional Certification Class w/exam	72	$3,990
R	Q/WAD® Qualified/ Wireless Analyst & Defender Practicum	72	$3,990
R	Q/WP®/ Q/WSP® Qualified Wireless & Qualified Wireless Security Professional Certification Class w/exam	144	$6,990
R	SU Security+® CompTIA Certification Class w/exam	72	$3,490
R	SU SecurityX®- [formerly CASP] Certification Class w/exam	72	$3,990
R	PMP Project Manager Professional Certification Class*	72	$3,990
R	Q/WLANPD Qualified/ Wireless Local Area Network Planning and Design Class w/exam	72	$3,990
R	Q/WLANPD Qualified/ Wireless Local Area Network Planning and Design Practicum	72	$3,990
R	Q/WNST Qualified/ Wireless Network and IoT Security Testing Class w/exam	72	$3,990
R	Q/WDNO Qualified/ Wireless Deceptive Network Optimization Class w/exam	72	$3,990
E	ITIL V4 Certification Class w/exam	72	$3,990
E	Scrum Master Certification Class w/exam	72	$3,990
SU Q/SSE® Qualified/ Software Security Expert Certificate Program of Mastery * This is the cost of the program when you pay tuition up front or opt to pay by class w/exam below.		936 hrs	Program $26,500*
The *SU Q/SSE®* Certificate Program of Mastery and related secure coding micro badges identify and certify "qualified persons" who subscribe to a rigorous requirement to maintain their knowledge and proficiency securing code. The mission is to know secure coding techniques that minimize the adverse effects of SQL or other malicious hacker attacks on code.			
R	Q/SSE® Qualified/ Software Security Expert 5 Day Certification Class w/exam	72	$3,990
R	Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class w/exam	72	$3,990
R	Q/STP® Qualified Software Testing Certification Class w/exam	72	$3,990
R	How to Break & FIX Web Security Certification Class w/exam	72	$3,990
R	How to Break & FIX Software Security Certification Class w/exam	72	$3,990
R	Fundamentals of Secure Software Programming Certification Class w/exam	72	$3,990
R	Q/SH/D® Qualified/ Software Hacker / Defender Certification Class w/exam	72	$3,990
R	Q/STBP® Qualified/ Software Tester Best Practices Certification Class w/exam	72	$3,990
R	Introduction to Reverse Engineering Certification Class w/exam	72	$3,990
R	SU Security+® CompTIA Certification Class w/exam	72	$3,490
R	Q/SSE® Qualified/ Software Security Expert Practicum	72	$3,990

R	Introduction to Reverse Engineering Practicum	72	$3,990
R	Q/SH/D® Qualified/ Software Hacker / Defender Practicum	72	$3,990
Q/CND® Qualified/ Cyber Network Defense Professional Certificate Program of Mastery * This is the cost of the program when you pay tuition up front or pay by class w/exam below.		936 hrs	Program $26,500*
SU's Q/CND Qualified/ Cyber Network Defense and Offensive missions are threaded into the Network Cyber Defense Training classes. The mission is to master defensive scenarios to protect your networks from the hacker. This training is for those who seek qualified cyber network defense, cy ops and threat attack careers. The Q/CND Certificate Program of Mastery Program is an accredited program with related cyber micro credentials.			
R	IDS I Catching the Hackers Intro to Intrusion Detection Certification Class w/exam	72	$3,990
R	IDS II Catching the Hackers II: Systems to Defend Networks Certification Class w/exam	72	$3,990
R	IDS III: On-site Log Analysis, Event Correlation and Response Certification Class w/exam	72	$3,990
R	Q/MC® Qualified/ Mission Critical Certification Class w/exam	72	$3,990
R	Q/CDA Qualified/ Cyber Defense Analyst Certification Class w/exam	72	$3,990
R	SU Security+® CompTIA Certification Class w/exam	72	$3,490
R	SU SecurityX®- [formerly CASP] Certification Class w/exam	72	$3,990
R	SU CISSP® Certified Information Security Systems Professional Class*	72	$3,990
R	Linux/UNIX® Security Certification Class w/exam	72	$3,990
R	CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam	72	$3,990
R	Cloud Computing Security Knowledge Certification Class w/exam	72	$3,990
R	IDS II: On-site Log Analysis, Event Correlation and Response Practicum	72	$3,990
R	IDS III: On-site Log Analysis, Event Correlation and Response Practicum	72	$3,990
E	TCP/IP and Key Features of Wireshark Class w/exam	72	$3,990
E	How to Conduct Network Vulnerability Analysis Class w/exam	72	$3,990
E	Python Forensics Certification Class w/exam	72	$3,990
E	PowerShell Forensics Certification Class w/exam	72	$3,990
E	Python/Powershell Incident Response Certification Class w/exam	72	$3,990
CISSP® is a registered trademark of {ISC)2® -SU CISSP Training classes are not endorsed or sponsored by {ISC)2® /CEH® CHFI® are EC Council registered trademarks SU CWNA / CWSP classes are not endorsed or sponsored by CWNP®. SU CIPP® Training classes are not endorsed or sponsored by IAPP®. R is a required E is an elective. Practicals are required "validation" to support mastery evidence claim of knowing something. *CISSP, CISA and PMP exams excluded in class fee. SU Accelerated Qualified/ Registered Cyber Apprenticeship Programs are eligible for veteran education benefits. Earn 8 Cyber Certs/ 24 mo/ attend 8 hands-on classes. Employer agreement and Apprenticeship agreement required for apprenticeship program. Advance your cyber career skills at SU. SU Testing (SUT) owns Q/ISP® ,, Q/IAP®, Q/WP®, Q/SSE® , Q/CND® Exams. Certificate Program of Mastery Exams are high stakes, on site, on-line, on-demand testing at TESTRAC.com/SecurityUniversity			

All Students are required to register online at the SU website REGISTER ME Tab {https://www.securityuniversity.net/reg.php).

NONSTANDARD TERM DEFENITION AND PRIOR CREDIT WAIVER

A term that is shorter or longer than a standard quarter or semester. The number of instructor-student contact hours is increased proportionately each week to compensate for the difference in length. All courses are 72 contact hours of face to face, 40 hours instruction with pre study or post class practicums of 32 hours **[veterans using the VA ED benefits can only attend face to-face modality]** Prior credit (PC) waiver subsume pre-class hours.

ADMISSIONS REQUIREMENTS - SU does not discriminate on the basis of race, color, age, sex, gender, religion, sexual orientation, ethnic origin / national origin, disability, perceived gender, or gender identity in admissions, career services, or any other activities. Applicants will not be denied admission on the basis of any of the foregoing factors, but applicants must meet all requirements specified for admission. A Student must meet the state minimum age requirement to enter school (if applicable) and must submit the following:

- A copy of a valid state or federal issued photo identification
- Has sufficient knowledge of the Transmission Control Protocol/Internet Protocol (TCP/IP)
- Or verified 2 months of work experience or employer enrollment.
- A yes or no answer with school president is sufficient to confirm one's knowledge of TCP/IP.
- A resume can verify 2 months of work experience using TCP/IP.
- A school transcript or credential validation is requested for prior credit and PC waiver.

STUDENT ADMISSION AND ORIENTATION INFORMATION:

All incoming Students must attend an in-person orientation the morning of the first day of class or program. During orientation student learn about responsibilities and standards, prior credit, attendance, testing & graduation.

All classes are in taught in English. All face-to-face courses begin @7:45am first day and 8am there after unless otherwise specified, with an hour for lunch and 2 morning and afternoon 15 min breaks. SU building is open from 7am – 6pm. Schedule hours are equal to the class contact hours in the course syllabus and catalog. Students may come into the building before 7pm or after 6pm by calling for access. Each class syllabus includes the specific class time. SU facility has 1 classroom [seats 50 students], 1 conference room seats 15 students. 95% attendance is expected of all students. A instructor may remove a student who misses 3+ hours of class. The course syllabus includes attendance policies that affect student outcomes, including tardiness and early departures from class.

STUDENT RESPONCIBILITIES

Students share the responsibility of developing and maintaining an academic and professionally conducive environment with the management and staff of this institution. It is expected that each student will respect and uphold the rights of all who are involved in the educational and administrative processes of this institution by adhering to the practices and principles described herein. Students are expected to progress towards an educational, professional or vocational objective. A vocational objective is one that leads to an occupation, and the awarding of a diploma or certificate which reflects educational attainment. Student responsibilities include consistent attendance, conscientious effort within the classroom to promote an open exchange of information, and compliance with standard academic practices. Students are advised of their right to pursue their education in a setting free of harassment or discrimination, and are expected to apply the same values to the staff and their peers. Program of education. (i) Is any program course which is pursued by a service member, veteran, dislocated worker, non-traditional student which is a combination of cyber security courses pursued at SU. The combination of cyber security classes is accepted as necessary to meet requirements for a predetermined educational, professional or vocational objective to obtain a Qualified Cyber Security Certificate Program of Mastery. Programs consist of 13 courses which fulfill requirements for one cyber Security certificate objective related to a cyber security career field. Including a full-time program of apprenticeship or on-job training.

STUDENT’S RIGHT TO CANCEL - CANCELLATION AND TUITION REFUNDS POLICY & FINANCIAL AID

SU does not provide Financial Aid, Loans or scholarships at this time. Student may secure private loans to pay tuition and fees. Please check with the President to discuss financial options at 203-249-8364. veterans, prospective or current student may cancel their *program or class enrollment* through the last day of class and receive a 100% refund of tuition paid, excluding third party completed exam fee. Any student registration paid by credit card is responsible for the 6% credit processing fee. If a student pre-paid tuition $26,500/ 13 courses CPoM program, and student cancels the program, SU refunds the unused tuition to payee or VBA if certified before class ended. A refund is equal to the tuition paid less the full or discounted cost of class completed. Exam fees are not repaid. Applicants must request a refund via email or phone call. SU refunds within 45 days after receipt of a written request or call from the last date attended. SU reserves the right to cancel a class at any time. SU will refund the class cost and fees less 6% credit processing fee. SU’s liability is limited to the class cost not exam fee. SU cannot be held liable for other related expenses, i.e., airfare, airline penalties, lodging, etc. Should a student re-schedule due to extenuating or unforeseen circumstances, students can re-register for the next class date at no penalty or additional charge. Veteran refunds are based on class certified ppost

SCHOOL POLICY

School attendance is required to complete a 72hr class that results in a SU participant completion certificate. The ability to apply what students learn in hands-on classes and labs is critical to a student's course of study and may require face to face attendance. Veterans are approved for face to face modality instruction. Once a student completes the course hours they have completed the course objectives. A practicum when required, is a hands-on post-class 72hr assessment that ensures students are able to express in writing how to list, describe, report, compare, demonstrate, and analyze what they learned in SU exams. Once they complete class they have reached their learning objectives. Students attending class for CPE’s (contining professional education) required by a certifying body are exempt from exams unless they choose to advance their career from taking and passing the exam. SU reserves the right to deny admission to any applicant who SU, on the basis of background, record, statements, and conduct during the admissions process, determines to not be qualified to succeed in or benefit from an academic program offered by SU. School may accept valid credential. in place of course hours. An official transcript can be used to determine the entry point into the program to provide a better educational experience.

A student from enrolling or Impose any penalty, including the assessment of late fees, the denial of access to classes, libraries, or other institutional facilities Require that a covered individual borrow additional funds, because of the student's inability to meet his or her financial obligations to the school.

Student using CH 31 or 33 must provide a certificate of eligibility [COE] until the VA provides payment to the school or 90 days after the school certifies tuition and fees. Exam fees approved by the SAA are included in class fees on each invoice and receipt. SU does not assess late fee penalties, or denies access to classes, school facilities, or require student to borrow additional funds due to delayed payments to SU under chapter 31 or 33 unless the student is less than 100% covered. Reinstatement: a student whose service in the uniform has required an interruption or sudden withdrawal or pro-longed absence from a class or their CPoM program are eligible to re-enroll for the class at no penalty after consulting with the School President. Students have up to 7 years to complete their Qualified Cyber Security Certificate Program of Mastery.

PRIOR CREDIT POLICY:
Per, 38CFR 21.4254 (c)(4), VA eligible Students are requested to provide a copy of all post-secondary transcripts (not just those for cyber programs). The school maintains written and digital records [if provided] of a current resume for previous education and training. Appropriate credit is granted for previous education and training, with the training period shortened proportionately for credentials earned prior to attending SU, and the Student and VA so notified. **PRIOR CREDIT (PC) WAIVER** can subsume required pre-class study.

INDEPENDENT STUDY NOT APPROVED FOR VETERANS, ATTENDANCE, PROBATION & SUSPENSION:
Attendance is recorded during the 40 hr class pre class study & exam. Independent study is not SAA approved. Students attend [3 wks] online FTF 10.75 hr and 1 wk 40 hr FTF onsite instructor led class. If attendance falls below 95% upon evaluation, SU will require the student to correct attendance or be placed on 90 day probation. If, at the end of the probation period, the student's cumulative attendance does not meet 95%, the Student's VA benefits will be terminated. Students whose absences result from mitigating circumstances will not be terminated and alternate plans for continuing attendance without termination from the school may be made to make up hours, at the discretion of the President. Veterans may not be certified for benefits during this period of make-up and VA will be notified within 30 days of the change in student status. Students who have been terminated from the school for unsatisfactory attendance may be re-admitted at the discretion of the President or CSO. SU will notify the SAA of student's attendance actions, if any that will be taken if a student fails to meet the minimum course requirement. Grounds for suspension: providing fraudulent documentation of requirements for admission. Failure to attend classes regularly resulting in unsatisfactory conduct. Refusal to complete assigned classes work. Breach of school rules and regulations. Falsification of school records. Cheating, Hazing, Theft Conduct or conditions that pose a direct, adverse threat (including bullying) to Students, guests or employees of SU. Failure to make required cash payments. Intentional destruction of school property, destruction of other Students' or staff members' property. Physical violence and threats of violence can mean immediate dismissal / suspension without previous warning.

VETERAN SCHEDULE & START DATE CHANGES
Schedule changes may be approved. An approval is dependent upon the course rotation. Student who meets the admissions requirements for a start date may request a change to their start date at no penalty.

VETERAN CONDUCT POLICY
Students must conduct themselves in a respectable manner at all times. Disruptive or inappropriate behavior deemed unsatisfactory conduct by school officials will result in immediate termination of veteran's educational benefits, loss of and possible dismissal from SU. Re-admittance after conduct dismissal requires reapplication to the school.

VETERAN ACADEMIC PROGRESS POLICY
Academic progress will be evaluated during each class If academic progress falls below 95% upon formal evaluation, the student will be placed on probation. If, at the end of the probation period, the Student's cumulative academic progress does not meet 95%, the Student's VA benefits will be terminated. Certification to VA for payment will not be resumed until the Student has returned to a satisfactory academic status.

SU PROVIDES TO VETERANS AND STUDENTS
A personalized Education Training Invoice (ETI) that includes costs and receipts, student debt estimates; designated points of contact for academic and advising. Accreditation of all new programs prior to enrolling students and Institutional refund policies aligned with SCHEV. This institution will not tolerate the unauthorized reproduction of software or otherwise copyrighted material by employees or students. This policy defines software as any electronic copyrighted material, including but not limited to software applications, video, audio, or other date files. Student Expectations:

- To exhibit good conduct in the classroom and community
- To complete the course of study in a timely and acceptable manner
- To demonstrate good attendance
- To follow the rules and regulations of the institution
- To respect the facilities and equipment
- To remain respectful in the expression of opinions and ideas
- Maintain the safety of employees and other students at all times

RELIEF, REFUND, AND REINSTATEMENT OF TUITION POLICY
Provides for tuition relief, refunds, and reinstatement of students whose service in the uniform services has required their sudden withdrawal or prolonged absence from their enrollment at the institution and provides for the required re-enrollment of such students. Students who withdrew as a result of military deployment, mobilizations or duty changes are entitled to return anytime to continue their Qualified Certificate Program of Mastery. If the CPoM program was paid in full the appropriate refund will be refunded.
PII - By policy SU does not provide (unencrypted) PII to anyone.

NON-ACCREDITED COURSES Security University does deliver non-accredited courses

VETERANS ATTEND ONLY APPROVED CLASSES AND CROSS REFERENCE TO ENSURE STUDENTS ONLY CERTIFIED AND ENROLL FOR COURSES THAT HAVE BEEN APPROVED BY THE SAA WITHIN THE PROGRAM:
Students with a valid COE Certificate of Eligibility letter or Entitlement will be reviewed against SAA approved classes to ensure that students are only certified for courses that have been approved by the SAA Chapter 33 or 31, on or before the first day of class and noted in the student record including reviewing their VA Educational Benefits and Estimated Financial Plan. Veterans can only attend classes approved by the SAA in that program to ensure students are only certified for courses that have been approved by the SAA within the program. Veterans attending SU approved courses attend face to face instructor led class. Veterans using their education benefits can only attend in the face-to-face modality. Veterans are not approved for independent study, distance education, or hybrid modalities. SU records student attendance weekly.

INTERRUPTION OF ENROLLMENT

When a student withdraws prior to graduation, the student may re-enter SU within seven years and retain full academic credit, provided the courses are still applicable to the program. Returning students who have completed practicals need not redo. Students will maintain the original CPoM cost with an absence of less than six months during their program. Students with an absence of more than six months are subject to tuition rates in effect at the time of readmission. They may be required to undergo skill proficiency examination, particularly if significant curriculum changes are involved. In addition, these students will also be required to return into the program/ curriculum taught at the time of readmission. While returning students are not required to reapply for admission, they must schedule an appointment to discuss their return to SU's CPoM and go through the formal readmission process. The student’s records are reviewed by the following departments:

- Student Records will review satisfactory academic progress;
- Student Accounts will review for outstanding balances;
- Financial Aid if any will review unresolved financial issues; and
- Academic Affairs will review attendance and academic preparedness to resume the program at SU.

Students must have approval by all departments in order to complete the readmission process.

SATISFACTORY ACADEMIC PROGRESS (SAP)

SU calculates Satisfactory Academic Progress using both qualitative (class completion) and quantitative measurements (incremental completion rate/ max time frame) at specified evaluation periods. SAP periods are based on enrollment in a Program, class schedule, and subsequent class registrations towards completing a program. Students completing daily activity are making progress in their class and Program.
Students agreements include the following:

- SU conducts course eligibility against SCHEV approved class list with *new* student prior to enrollment
- Students must discloses transfers credit or hours asap after registering in a class and certificate program
- Students review policies regarding the award of [academic or credential] prior credit learning experiences
- SU discloses programs and costs, including tuition, fees, and other charges on class invoice and receipt
- SU provide access to the President 7X24 or financial aid advisor
- Students are not charged if they "drop/add," withdrawal, or request re-admission based on military duties
- Students have designated POC for academic and financial aid counseling and student support services
- SU does not pressure students to attend classes using veteran education benefits.
- SU awards learning acquired for specialized military training of occupational experience when applicable.

- **SU STANDARDS OF PROGRESS**

  A student's progress (SOP) is tracked daily based on how well they complete the class assignments and labs for the Exemplary (100-85%), Proficient (84-70%) or Failing (69% and below) grades by participation in assignments and the successful completion of course labs, quizzes and required exam. Students earn a participation certificate documenting their class completion and a transcript of their continued pursuit of their Qualified Cyber Security Certificate Program of Mastery.

1. Each class registration and syllabus is emailed to students with a student agreement and refund policy. The email contains information on how a students will receive a certificate upon completion of class or program.
2. Student attendance and progress is reviewed by the faculty and the president daily. Students are expected to attend 95% of the 40 hour class with pre or post 32 hours in order to meet the attendance requirement, unless a student is approved for extenuating circumstance or makes up class time. Students are expected to sign in and out of class daily and participate in quizzes, labs and practicums (if any). At the end of every class, the president and faculty review attendance and academic data to determine who have completed class and award participation certificates and update transcript. Waivers for 32 hour prior credit is reviewed upon request.

INCREMENTAL COMPLETION RATE (ICR)

Students enrolled in advanced level programs must complete a minimum of 95% of the cumulative hours attempted at the end of each course for satisfactory academic progress.

MAXIMUM TIME FRAME

The number of hours attempted in your time as a student is measured. Students enrolled in a 936 hour program should complete a class or 72 hrs a year, or complete a few classes per year.

GRADING PROCEDURE AND CERTIFICATE PROGRAM SATISFACTORY ACADEMIC PROGRESS

To be in good academic standing with SU and to be eligible to receive Title IV financial aid (if available) students must maintain satisfactory academic progress. Grading Policy - students must attain a Proficient or Exemplary grades during the week to pass. SU measures and accurately reflects student proficiency using a grading system of Exemplary (100-85%), Proficient (84-70%) or failing (69% and below). Students pass or fail the class based on attendance and standard of progress, quizzes, and learning outcomes. *Exams are not included to determine a final pass/fail grade, but are required to complete a class program unless the student is attending only for continuing professional education credit (CPE).* Practicum assess measure student skills and competency. Ample practice and feedback is generously provided during hands-on cyber range labs. Students are evaluated based upon performance and attendance. In case of a failure, the student can retake the practicum assessment. The first passing grade will be recorded as class completion. Practicums validate students experiential cyber skills and evaluated on a pass- no passed basis post class.

COURSE DESCRIPTION

Each Qualified Cyber Security Certificate Program of Mastery consists of 10 required instructor led courses and practicals to validate students are competent in their cyberskills to be an effective cyber security professional. Instructor led courses involve performing advanced procedures and services on live systems for defensive and offensive security. Each program provides students with an understanding of the fundamentals and procedures of cyber security, system administration, networks and network security, defensive and offensive security skills necessary to complete a successful cyber security job task. SU training is developed by a global team of cyber security experts and CNSS approved since 2008. Training covers the full spectrum of cyber security experience levels, from beginner to advanced, for a variety of roles including security operations (SOC), DevSecOps, WebAppSec, PenTesting, and more that align with the specific needs of core cyber security roles to defend today's threat landscape with the right skills.

EDUCATIONAL OBJECTIVES / GOALS:

Qualified Cyber Security Certificate Program of Mastery within 7 years. Upon completion of required classes and practicums in a Qualified Cyber Security Certificate Program of Mastery a student graduates.

Students will have the following:

Basic and advanced practical cyber security skills that lead to high wage in-demand jobs.

Mastery of in-demand cyber security skills, with a portfolio of projects using real-world data sets.

Proficiency to advance your cyber security career.

Earn a Qualified Cyber Security Certificate Program of Mastery Completion Certificate.

Earn cyber security [industry] certification credentials employers seek to advance your cyber career.

SU's NICE publication provides a fundamental reference in support of building a workforce capable of meeting a student's vocation objective and cyber security needs by using a common, consistent lexicon to describe cyber security work by category, specialty area, and work role using a superset of cyber security knowledge, skills, and abilities (KSAs) and tasks necessary for each cyber work role. SU courses include the NICE Framework for cyber security education, training, workforce development, planning, and education.

COURSE FORMAT

Course content is identified and prioritized through NICE, National Initiative for Cyber Education and Cyber Industry standards with employer's desires. SU classes are approved for face to face or hybrid classes [hybrid classes are exclude veterans using education benefits]. The accelerated program class includes approx 32hrs pre-class +40hrs of instructor led class contact, quizzes, labs, reading assignments and final exam - passing the final exam is a requirement for CPoM graduation.

INSTRUCTIONAL METHODS

SU classes are instructors led to achieve competency in all the various cyberskill sets, through problem solving, self-paced study [self study is not GI BIll approved], interactive theory, hands-on practice and exam assessment. Enrichment activities and practical's are provided so student can individualize their cyber education roadmap, gaining experience to extend their learning to improve or enhance skills, knowledge, and well-being. Practical's provides opportunities for students to pursue learning in their own areas of cyber interest and strengths. Enrichment keeps advanced students engaged and supports their accelerated academic needs.

REFERENCES

Each classroom will have the following: Textbooks, Tools / Equipment and cyber tools. In addition, the school is provided with an internet connection allowing accessibility to current Websites, Videos, and Tutorials. Electronic and/or hard copies of any Textbooks, Periodicals or other Reference Materials may also be available. The school has a library of additional educational materials (i.e. books, magazines, CDs, DVDs, etc.) which the students utilize to supplement their learning.

GRADUATION REQUIREMENTS

In orderto graduate students must complete curriculum requirements, exams and fulfill all financial obligations.

Upon completion of all course requirements, successful completion of the instructor led classes, and earning requisite credential after passing requisite exam, and passing the practicums is required to obtain a Qualified Cyber Security Professional [participation] Certificate, that leads to high wage, in-demand cyber employment. A security+ credential makes students eligible for IAT Level II cyber jobs.

TUITION

Each Qualified Cyber Security Certificate Program of Mastery fee is $26,500 and consists of 13 required instructor led face to face / hybrid courses , pass exams, and complete practicums. Prior credit is applied on a case by case basis. A cyber certification with the class participation cert may reduce certificate fee. Students may pay up front $26,500 or pay as you go [a single class and exam]. Class fees are listed in the catalog and online. Students are provided SU's 2page course program list first day of class. Graduation requirements are listed in catalog and online. Students using veteran benefits enrolling in program can enroll in a single class or entire $26,500 tuition fee for all class costs and exam fees. SU will invoice the veteran only from the SAA approved Certificate Program list.

STUDENT SERVICES

During career planning interviews and student orientation, students receive information about the Qualified Cyber Security Certificate Programs of Mastery goals, graduation requirements of each program, course, policies affecting students, and services available to students.

Our goal is to provide you with a clear picture about:

- Program requirements
- Student performance expectations
- Successful enrollment and financial planning

CAREER PLACEMENT ASSISTANCE

SU strives to assist every student in obtaining a cyber security career-related position. Employer opportunities are available from employer recruiters. Career guidance is available. Regulations prohibit any school, college or institution of higher learning from guaranteeing placement as an inducement to enter school. SU provides career advise but does not provide placement services or employment opportunities. Student training plan consultation (upon request) helps student’s determine a certificate certification path. SU post current cyber job openings and career fair links on SU website (http://www.securityuniversity.net/classifieds.php). SU sends emails to students with local and national career fair events and job announcements. Upon registering for class, SU’s President reviews each student’s current resume to determine eligibility create an independent training plan and cyber credentials program to increase interview opportunities that may lead to high wage in-demand employment. SU students can request a review of their own qualifications for CPE credits (Continuing Professional Education) or validate their cyber credentials, modify personal records, accesses information pertaining to their certification(s) by contacting SU President 7X24 via email to make an appointment.

CAREER OPPORTUNITIES

Here are some of the careers available to our graduates:

Sample Job Titles
CISO, ISSO, ISSO II, PKI engineer, Network Security Engineer, Assurance Officer, Compliance Manager
Blue Team Technician, Certified TEMPEST Professional, Certified TEMPEST Technical Authority,
Computer Network Defense (CND) Auditor, Ethical Hacker, Forensic Engineer, Reverse Engineering Engineer
Governance Manager/ Information Security Engineer/ Internal Enterprise Auditor, CMMC auditor, ISO compliance.
Network Security Engineer/ Penetration Tester, Red Team Technician/ Reverse Engineer Risk/Vulnerability Analyst
Technical Surveillance Countermeasures Technician/ Vulnerability Manager and much more

SCHOOL

PROGRAM CANCELLATION POLICY

If the start of a program needs to be delayed or cancelled, the School will work with the Student to arrange a new start date. Should a refund be required, it will be done in accordance with the refund policy contained within this catalog.

WEATHER OR EMERGENCY SCHOOL CLOSINGS

The President makes the decision to open late or close. Check your text messages, Facebook, local TV and/or radio stations for school information.

LEAVE OF ABSENCE

SU does not offer leaves of absence.

ATTENDANCE POLICY

All students are expected to attend all classes according to the schedule on their course registration page (course/ certificate enrollment (agreement).

RECORD RETENTION POLICY

The school maintains educational records and attendance records for a period of seven years. A transcript shall be retained permanently. These records include:

- Evidence of compliance with admissions requirements
- Courses for previous experience or training
- Dates of admission, start, completion, or withrawl dates
- Reasons for withdrawals, when known
- Daily attendance
- Tuition records, when applicable

WITHDRAWAL POLICY

A Student will be considered as withdrawn when one of the following occurs:

1. The Student officially notifies the President, of his/her intent to withdraw.
2. The School officially notifies the Student of dismissal from the program.

STUDENT CODE OF CONDUCT

Misconduct is considered to be in conflict with the educational objectives of the school and thus subject to immediate dismissal. Misconduct is cheating, forgery, plagiarism, furnishing false information, alteration of school documents, disruption or obstruction of teaching or administration, physical abuse of any person on school premises, theft or damage to school premises and property of other students, and use of alcoholic beverages and/or illegal drugs on school property. Any sexual misconduct in class will not be tolerated. A student may appeal an immediate dismissal.

PROFESSIONAL DRESS CODE

Students at SU are held to the professional dress code. Dress is business casual. We require all students to present themselves in a professional manner with regard to attire, personal hygiene and appearance. Students should dress in a manner that is appropriate for a business setting. Clothing must be clean and neat and must fit appropriately.

POLICY AGAINST HARASSMENT

SU has developed a “Policy against Harassment” that is given at the time of enrollment. The Policy provides information on how an individual can bring any violations of the Policy to SU s attention. It also includes guidelines for the investigation of complaints and enforcement of the Policy. Please address any questions regarding the Policy to the president.

ZERO TOLERANCE- STUDENT CONDUCT AND CONDITIONS FOR DISMISSAL

SU has zero tolerance for any forms of violence or threats, offensive language or aggressive behavior, bullying, use of or possession of illegal substances or alcohol, possession of firearms, ammunition, explosives, fireworks, or any other dangerous weapon (any instrument that may be used to inflict bodily harm), theft and fraud.

GRIEVANCE PROCEDURE GUIDELINES

SU has an open door policy. Issues or concerns should immediately be shared with the president. If the issue or concern is not resolved or the student, staff, or interested third party feels uncomfortable addressing the issue in person a formal written complaint may be submitted to the President. If a resolution is not found and you want to file a formal complaint you must follow the steps below:

1. Request a grievance form from the President or any other staff member.
2. Email completed grievance form to s0ndra@securityuniversity.net

a. Complete all fields, b. Give clear detailed information, c. Complete contact information

After submission to the President Email address, you will receive notification, within 3 business days, notifying you your grievance has been received.

3. If after careful evaluation, the problem cannot be solved through discussion, the complaint will be referred to the SU Advisory Board.
4. The President will respond within ten (10) calendar days of receipt of the complaint and review the allegations.

a. If additional information from the complainant is needed a representative from SU will contact you.
b. After the grievance is investigated, you will be informed of the steps taken to correct the problem, or information to show the allegations are not warranted or based on fact.
5. Records of complaints are retained according to the School's record keeping policy.
Non-Retaliation - Policy Statement - If a complainant wishes to pursue a matter, a complaint form is available through the Schools' accrediting agency. SU's accrediting agency requires the complainant attempt to resolve any issues through the School's complaint process prior to filing a complaint with the school's accrediting agency. This procedure does not in any way limit a student's right to exercise his or her legally protected rights. A complaint may also be filed with the school's accrediting or regulatory agency. Middle States Commission on Secondary Schools 3624 Market Street, 2 West, Philadelphia, PA 19104 Main Telephone Number: 267-284-5000 Fax: 610-617-1106 Fax: 215-662-0957 Email: info@msa-cess.org
6. If the Student complaint cannot be resolved after exhausting the School's grievance procedure, the Student may file a complaint with the State Council of Higher Education for Virginia. The Student should submit an online complaint at: http://www.schev.edu/ State Council of Higher Education for Virginia Private and Out-of-State PostSecondary Education 101 N. 14th Street, 9th Floor James Monroe Building, Richmond, VA 23219 Tel: (804) 225-2600 | Fax: (804) 225-2604
7. "The Virginia State Approving Agency (SAA) is the approving authority of education and training programs for Virginia. Our office investigates complaints of veterans and ARMY Ignited beneficiaries. While most complaints should initially follow the school grievance policy, if the situation cannot be resolved at the school, the beneficiary should contact our office via email at saa@dvs.virginia.gov."

FAMILY EDUCATION RIGHT TO PRIVACY ACT POLICY (FERPA)

In accordance with the Family Education Rights and Privacy Act, it is the policy of SU (the "School") to maintain confidentiality of information entrusted to it by eligible Students. Therefore, prior to each release of information an "Authorization for Release of Information" form must be filled out by the eligible Student for every request of Student information to a third party. A Student may review the Student's record by contacting the President to make an appointment. A Student shall be permitted to review his/her record on file anytime by email request to the president. An eligible Student may seek to amend education records that the Student believes to be inaccurate, misleading, or otherwise in violation of the Student's privacy rights.

TITLE IX OF THE EDUCATION AMENDMENTS OF 1972

SU is committed to providing a safe educational environment which is free of violence, harassment and discrimination. Therefore, in accordance with Title IX of the Education Amendments of 1972 and the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act), along with its amendments made pursuant to the Violence Against Women Reauthorization Act of 2013 (VAWA), SU has adopted strict policies regarding these matters. Additionally, in accordance with our school's obligations under Title IX, SU will excuse Student absences due to pregnancy or related conditions, as long as the Student's doctor deems the absences to be medically necessary. The doctor will also need to identify the dates which should be excused based on his/her medical determination.

NON DISCRIMINATION POLICY

SU does not discriminate on the basis of race, color, age, sex, gender, religion, sexual orientation, ethnic origin / national origin, disability, perceived gender, or gender identity in its programs or activities. Questions regarding non-discrimination policies can be referred to you by the school's president.

SOCIAL MEDIA GUIDELINES

Students are responsible for what they post on social networking sites (including but not limited to Facebook, Instagram, Pinterest, Twitter, YouTube, blogs, wikis, file-sharing and user-generated video and audio). SU does not permit ethnic slurs, personal insults, obscenity, and intimidation, cyber bullying or engaging in conduct that would not be acceptable in SU on any of SU's social media sites. SU reserves the right to remove any posts at its discretion. It is the duty of SU to protect itself from undue harm related to information that is shared on social networking sites.

COPYRIGHT INFRINGEMENT POLICY

Unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject a Student to civil and criminal liabilities. A summary of the penalties may be found at: www.copyright.gov/title17/92appf.pdf. Students who engage in illegal downloading or unauthorized distribution of copyrighted materials using the school's information system will be terminated.

CALENDAR - FEDERAL HOLIDAY SCHEDULE OBSERVED

Dec 29- Christmas thru Jan 9 New Years & Winter Break- University Closed

2 Career Testimonials:

As an Army Information Systems Management (FA53) officer focusing on Cyber Defense, I've had the opportunity to train and certify in several IA/CND specific programs as well as work a myriad of Army Cyber Defense workforce training and development issues.

Having just recently completed the SU (SU) Qualified Security Analyst (Q|SA) and Qualified Penetration Tester License (Q|PTL) courses I can confidently say that Sondra and her team have built an exceptional program of instruction; capturing the essential elements of security analysis and penetration testing methodologies and delivering them in a clear and concise format in a blended learning environment of lecture and hands-on practical skill development with scenario-based final examinations. SU training techniques are a perfect match for our military cyber defense workforce goals since they not only train the relevant concepts of cyber defense and its CND specialties but also in the case of Q|SA and Q|PTL courses challenge the students to apply those concepts in a "tactical" setting that an actual security analyst or penetration tester might see.

SU's Q/ISP Q|SA / Q|PTL program of instruction is impressive and superior to some other training programs in several ways; one of them being the daily hands-on assessment of critical skills being taught. Another was the realistic practical final exam which included a penetration test with a final report that required some in-depth analysis of the resulting sets of data. I spent 30 post-course hours alone on analyzing the data and developing a 32 page report. That's definitely an experience you're not going to get through other training programs that teach a 5 day curriculum that's predominately lecture based. The Q|SA and Q|PTL courses also expose the students to a wide range of open and closed source automated tools for use in security analysis and penetration testing as well as the built-in assessment and exploitation capabilities of both Linux and Windows based operating systems. I honestly can't understand how we expect to conduct defense in depth across the GiG without our technical workforce understanding basic exploitation, which is exactly what's missing from many other approved certifications. SU equally balances this with methodology and analysis techniques rather than relying on specific toolsets since tools frequently change and are always subject to interpretation of their results.

Many leaders and managers in a resource constrained environment try to meet RMF compliance by targeting those one-shot, many-kills certifications that are on the DoD 8570.01M chart with little regard for how relevant the training might be for certain 8570 categories. No better example can be given than the inclusion of CISSP as an IAT validating certification. Being a CISSP I can attest that it's a great certification for a security manager as it is wide and deep in several essential bodies of knowledge. But it will not enable a security technician, especially at the enclave level, to secure enterprise environments from a hands-on technical approach nor understand the threat and environment essential to effective defense in depth. Therefore it adds little value for an organization to have an IAT-III CISSP from a technical standpoint, but practically, that person can also fill other roles since CISSP covers everything from IAT-I through IAM-III. Hence, managers focus on CISSP and miss excellent training like SU's Q/ISP & Q/IAP programs.
SU training should be a major part of any organization's information security training programs. Major, Shane LipTAk

Testimonal II
As an Army Cyber Warfare Officer (17A) and professional cyber educator, I have participated in thousands of hours of cyber training through various training providers. I have extensive experience in cyber education from the perspective of a student, instructor, and content developer. I was immersed as a student in months of cyber training as a member of a Cyber Protection Team (CPT). I also participated in, and later instructed, cyber training courses for various government agencies. I also have years of experience in higher education as an adjunct professor of cyber security. Therefore, I have a uniquely experienced opinion on cyber security training and education.

It is my opinion that the quality of training provided by SU is of the highest standards desired by employers and government agencies. SU takes a unique graduated approach towards training and apprenticeship. Most training providers offer many individual classes, without considering the bigger picture of trainee development. SU's custom incremental approach to training forces trainees to retain and apply skills and theory gained in foundational classes into more advanced training scenarios. For examples, SU's Q/ISP curriculum provides trainees with extended exposure to tools, tactics, and techniques in a unique systemic manner that I believe is ideal for cyber professional skills development. It provides the desired balance between traditional university style education and stand-alone immersion classes.

SU also provides advanced training paths in topics such as network defense, penetration testing, exploitation, digital forensics, and software security that is tailored to the trainee's long-term skills acquisition goals. The instruction is provided by proven leaders in the field and guarantees graduates have the immediately applicable skills to be relevant in the cyber fight. In my experience, few practitioners can apply the skills gained in a traditional immersion course into the workforce. I have led, trained, and worked alongside with cyber professionals who have earned numerous industry certifications. However, it has been shown time and again that these certifications provide mere exposure without the critical analysis and creative thinking required to solve tough problems in our evolving cyberspace. SU addresses this shortcoming with their training model and apprenticeship.

SU comes with my highest recommendation for government, military, and civilian employers seeking a training approach to prepare our cyber workforce. Adam Duby Captain, USA - Department of Computer Science, University of Colorado at Colorado Springs

Super Qualified

QUALIFIED
IS OUR
BUSINESS
Security University

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Q/SA® QUALFIED/ SECURITY ANALSYT CERTIFICATION W/EXAM
W/ PENTERATION TESTING LICENSE WORKSHOP

How to look at your network through a hacker's eyes… and close the doors on unauthorized penetration.

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery CPoM / non degree-
Q/SA® Qualified/ Security Analyst Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Workshop Required
Q/EH® Qualified/ Ethical Hacker Certification Class w/exam
Q/ND® Qualified/ Network Defender Certification Class w/exam
Q/FE® Qualified/ Forensic Expert Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
SU Security+® CompTIA Certification Class w/exam
SU SecurityX®- [formerly CASP] Certification Class w/exam
Linux/UNIX® Security Certification Class w/exam
Cloud Computing Security Knowledge Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Practicum
Q/ND® Qualified/ Network Defender Certification Practicum
Q/FE® Qualified/ Forensic Expert Certification Class Practicum

The Q/ISP Certificate Program of Mastery Q/SA- Q/PTL Qualified/ Security Analyst Penetration Tester certification class & Q/PTL Qualified/ Penetration Tester License validation lab prepares you to learn "how to do Vulnerability Analysis" & "how to report" how compromised the network can be. You learn SU's Vulnerability Analysis & Penetration Testing process and methodology while doing "no harm". SU courses and certificate programs of mastery are designed to provide you with an immersive learning experience -- from hands-on workshops, certifications, with deep dives on a particular cyber security topic or technology. Every class is structured to give you expertise in critical areas that you can immediately put to use.

The majority of the class consists of probing target networks, gaining user-level access and demonstrating just how compromised the network can be. SU teaches you the red team skills like leaving an innocuous file on a secure part of a network as a calling card, as if to say, "This is your friendly red team. We danced past the comical precautionary measures you call security hours ago. This file isn't doing anything, but if we were anywhere near as evil as the hackers we're simulating, it might just be deleting the very secrets you were supposed to be protecting. Have a nice day!"

The Q/SA® - Q/PTL® is the only security skills assessment certification that validates your Qualified/ Security Analyst Penetration Tester skills. There is only one way to get a **Q/PTL Qualified/ Penetration License** - you EARN one, not buy one.

To achieve your Q/PTL you must perform a real penetration test the last day of class and report back a "Practicum", fully detailed management report. Your report is due to SU 60 days from the start of class. This practicum shows your penetration testing skills and valids them beyond question. Nightly exercise are no walk in the park, each Q/PTL session increases in complexity and scope. The more skilled the security team becomes, the more complex the target range.

Class Fee:	$3,990 w exam
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr + 32 hr pre class study 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practicum for CPoM
Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Titles
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager
Information Security Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist
Security Administrator
Security Analyst
Security Control Assessor
Security Engineer

KU Outcomes:
* Students will be able to describe potential system attacks and the actors that might perform them.
* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.
Systems Security Analysis - Conducts and documents the systems integration, testing, operations, maintenance, and security of an information environment. Coordinates threat and mitigation strategies across the enterprise

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 18M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation
Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Live *CYBER RANGE offers advanced, high-fidelity attack vectors on LIVE infrastructures for Persistent Cyber Training Environments, with COTS and Bespoke Missions, deployed as SaaS, On-Prem, Transportable*

Who Should Attend System and Network Administrators, Security Personnel, Auditors, and Consultants concerned with network security.
Learning Objectives

• Develop tailored focused, well defined rules of engagement for penetration testing projects- conducted in a safe manner
• Conduct reconnaissance using metadata, search engines, & public information to understand the target environment
•Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS finger- printing, and version scanning to develop a map of target environments
• Learn how to properly execute Nmap, and sripts to extract information from target systems
• Configure and launch a vulnerability scanners, like Nessus, Metaspolit , to discovery vulnerabilities in un/authenticated and scans safely, and customize the output from such tools to represent the business risk to the organization
•Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
•Utilize the Windows and Linux command likes to plunder target systems for vital information that can further the overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
•Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
•Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional pass- word cracking, rainbow table password cracking, and pass-the-hash attacks
•Utilize wireless attack tools for Wifi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a projects scope
•Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and risk faced by an organization.

Lesson Plan Lesson I **class quiz study Penetration concepts you will master during this hands on class**

- Attacking network infrastructure devices
- Hacking by brute forcing remotely
- Security testing methodologies
- Security exploit testing with IMPACT from Core Security
- Stealthy network recon
- Remote root vulnerability exploitation
- Multi-OS banner grabbing
- Privilege escalation hacking
- Unauthorized data extraction
- Breaking IP-based ACLs via spoofing
- Evidence removal and anti-forensics
- Hacking Web Applications
- Breaking into databases with SQL Injection
- Cross Site Scripting hacking
- Remote access trojan hacking
- Offensive sniffing
- Justifying a penetration test to management and customers
- Defensive techniques

Expectations Your are expected to complete the hands-on lab exercises -

- Capture the Flag hacking exercises
- Abusing DNS for host identification
- Leaking system information from Unix and Windows
- Stealthy Recon
- Unix, Windows and Cisco password cracking
- Data mining authentication information from clear-text protocols
- Remote sniffing
- Malicious event log editing
- Harvesting web application data
- Data retrieval with SQL Injection Hacking

25 years ago SU started training security professionals with the very best penetration step by step process and methodology class, SU is still the leader in security Analysis & Penetration Testing Certifications in the industry. Now you can take the same Penetration Testing process and methodology class that trains the US Air Force, Army, Navy and Marines trained to defend military networks. Your class is taught by SSME (Security Subject Matter Experts) who know the "Art of Penetration Testing & Hacking". You'll gain serious tactical security skills that will set you apart from your peers. *"This is an class, the instructor was excellent & very knowledgeable. I feel that I am leaving this course a much better Security Specialist. Wilson DHS"*

Appendix I,II,III - Packet Filtering, IDS Log Analysis, Vulnerability, Log Analysis, IPS & IDS correlation, IDS & IPD countermeasures, Wireless Security, Software Security, Network Security, Event Correlation, Threat Mgt, Security Polices, Virus Malware, Code Review, Reverse Engineering, COOP, Incident Response, CMMC compliance requirements aside, penetration testing is an absolutely critical aspect of any security class. Actors test every company's defenses every day.

Lesson Plan Lesson

1. Gather the Data

A first look at a network site, from the eyes of a potential hacker. The simple, and often overlooked, things that tell hackers if a site is worth a penetration attempt.

Lesson Plan Lesson 2

2. Penetrate the Network

How hackers get past the security and into the data.

- Non-intrusive target search
- Intrusive target search
- Data analysis

Lesson Plan Lesson 2 & 3

3. Network Discovery Tools and Techniques: Hands-On Exercises

- Discovery/profiling objectives
- Locating Internet connections
- Host-locating techniques: manual and automated
- Operating system footprinting
- Evaluating Windows and Unix-based network discovery software tools
- Evaluating Windows and Unix-based application scanning software tools
- Review Step-by-step process of each scanning and profiling tool
- Directory services: DNS, DHCP, BOOTP, NIS
- Look-up services: finger, whois, search engines
- Remote sessions: telnet, "r" commands, X-Windows
- File sharing and messaging: FTP, TFTP, World Wide Web
- Windows Server Message Block (SMB), Network File
- Systems (NFS), and E-mail
- Sample exploits using common TCP/IP and NetBIOS utility software

***Lesson Plan 4 1*4 hr Lecture & labs**

4. Analyze the Results

Tips and techniques for effective, actionable penetration test analysis.

- Identifying network services
- Pinpointing vulnerabilities
- Demonstrating risks
- Reviewing reports and screens from prominent discovery/profiling tools
- Analyzing current configuration

5. Real World Scenarios

- Abusive E-mail
- Embezzlement
- Pornography
- Denial-of-service
- Web defacement
- Trojan Horse

Lesson Plan 4 Lesson

6. Write the Report

- How to combine methodology results
- How to prioritized results that generate management attention and buy-in
- How to provides clear, workable action items.

In-Class Exercises

- Building and maintaining a target list
- Running PGP (Pretty Good Privacy)
- Conducting multiple non-intrusive and intrusive target searches
- Tools and techniques for testing for Web site vulnerabilities
- Probing and attacking network firewalls
- Performing multiple remote target assessment
- Performing multiple host assessment
- Writing up the final report

- ***50 Question Online Exam 1PM - 3 Hr Q/PTL Penetration Test 2-5pn 1 hr gather data 6pm***

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932 | Edition: 4

For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013)

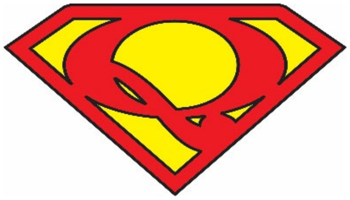
The book below is recommended for those interested in understanding how their own computers work for personal edification

How Computers Work, Ninth Edition Ron White Que Publishing, 2007 ISBN 0-7897-3613-6

This last book below is recommended for aspiring hackers, those interested in programming techniques and low-level optimization of code for applications beyond the scope of this course. Hacker's Delight, Second Edition Henry S. Warren Jr. Addison-Wesley, 2012 ISBN 0-321-84268-5

Weapon of a CyberSecurity Warrior
Weapon of a CyberSecurity Warrior

Super Qualified



Security University® Q/ISP® Certificate Inspires Utmost Competence

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Q/PTL QUALIFIED/ PENETRATION TESTER LICENSE WORKSHOP PRACTICUM

The Most Respected Qualification and Validation for Penetration Testing Professionals

This Mandatory QPTL course validates your excellence in security penetration training and education. Your Q/PTL license holds you in high respect among your peers. The Qualified/ Penetration Tester License standardizes methodology and best practices for penetration testing professionals. The learning objective of a Q/TPL Qualified/ Penetration Tester License is to ensure that each professional licensed by SU follows a mandatory code of ethics, best practices and compliance in the sphere of penetration testing and ensures each professional can validate their Q/PTL skills from an authorized source. The Qualified Penetration Tester License class trains security professionals to analyze the network and software vulnerabilities of a network exhaustively to improve security. SU's license vouches for their professionalism and expertise. SU courses and certificate programs of mastery are designed to provide you with an immersive learning experience -- from hands-on workshops, certifications, with deep dives on a particular cyber security topic or technology. Every class is structured to give you expertise in critical areas that you can immediately put to use.

Detailed Resume with professional experience, transcript or certifications with references. Agree to SU Code of Ethics. Attend Q/PTL Workshop. A practicum provides adequate evidence to support the claim of knowing something.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr + 32 hr pre-class study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD Live Penetration Test 3 hrs.
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practicum for CPoM

Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final a requirement for graduation.

Sample Job Titles
Blue Team Technician
Certified TEMPEST Professional
Certified TEMPEST Technical Authority
Close Access Technician
Computer Network Defense (CND) Auditor
Compliance Manager
Ethical Hacker
Governance Manager
Information Security Engineer
Internal Enterprise Auditor
Network Security Engineer
Penetration Tester
Red Team Technician
Reverse Engineer
Risk/Vulnerability Analyst
Technical Surveillance Countermeasures Technician
Vulnerability Manager

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus,saint PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl'

KU Outcomes:

* Students will be able to describe potential system attacks and the actors that might perform them.

* Students will be able to describe cyber defense tools, methods and components.

* Students will be able to apply cyber defense methods to prepare a system to repel attacks.

* Students will be able to describe appropriate measures to be taken should a system compromise occur.

LPT Training *Learning Objectives*

PTL is a professional qualification that is used to measure penetration testing skills.
Perform fuzz testing to enhance your company's SDL process
Exploit network devices and assess network application protocols
Escape from restricted environments on Linux and Windows
Test cryptographic implementations
Model the techniques used by attackers to perform 0-day vulnerability discovery and exploit development
Develop more accurate quantitative and qualitative risk assessments through validation
Demonstrate the needs and effects of leveraging modern exploit mitigation controls
Reverse engineer vulnerable code to write custom exploits

Lesson Plan I Lecture & Labs Introduction to Ethical Hacking, Ethics and Legality

1.1. Ethical Hacking terminology
1.2. Importance of Information Security in Today's World
1.3. Identifying different types of hacking technologies
1.4. Elements of Security, confidentiality, authenticity, integrity, availability
1.5. Evolution of Technology
1.6. Essential terminologies
1.7. Five Stages of Assessment & Hacking
1.7.1. Passive and active reconnaissance
1.7.2. Scanning
1.7.3. Gaining assess
1.7.4. Maintaining access
1.7.5. Covering tracks
1.8. Types of Hacker Classes
1.8.1. Ethical Hacker and Crackers
1.8.2. What do Ethical hackers do?
1.8.3. Goals hackers try to achieve
1.8.4. Security, functionality, and ease of use triangle
1.8.5. Operating System Level Attacks
1.8.6. Application Level Attacks
1.9. Skills required to become an ethical hacker
1.10. Vulnerability Research
1.11. Ways to conduct ethical hacking
1.11.1. Creating a Security Evaluation Plan
1.11.2. Types of ethical hacks
1.11.3. Testing types
1.11.4. Ethical Hacking Report
1.12. Legal implications of hacking
1.13. Computer Crimes and Implications
1.14. Understanding 18.U.S.C.-1029 and 1030 U.S. Federal Law
1.15. International Cyber Laws

2. Lecture
Footprinting and Social Engineering
2.1. Footprinting
2.1.1. Define footprinting
2.1.2. Describe the information gathering methodology
2.1.3. Describe competitive intelligence
2.1.4. Foot printing tools
2.1.5. Understand Whois and A RIN Lookups
2.1.6. Identify different types on DNS records
2.1.7. Understand how traceroute is used in footprinting
2.1.8. Understand how E-mail tracking works
2.1.9. Understand how web spiders work
2.2. Social Engineering
2.2.1. What is Social Engineering?
2.2.2. Common types of attacks
2.2.3. Understand Insider attacks
2.2.4. Understand Identity theft
2.2.5. Describe Phishing attacks
2.2.6. Understand online scams
2.2.7. Understand URL obfuscation
2.2.8. Social engineering countermeasures

Lesson Plan 2 Lecture & Labs

3. .5 Hr Lecture
Scanning and Enumeration
3.1. Scanning
3.1.1. Define port scanning, network scanning, and vulnerability scanning
3.1.2. Understand the CEH methodology
3.1.3. Understand Ping Sweep techniques
3.1.4. Understand Nmap command switches
3.1.5. Understand SYN, Stealth, XMAS, NULL, IDLE, and FIN scans
3.1.6. List TCP communication flag types
3.1.7. Understand war dialing techniques
3.1.8. Understand banner grabbing and OS fingerprinting techniques
3.1.9. Understand how proxy servers are used in launching an attack
3.1.10. How do Anonymizers work
3.1.11. Understand HTTP tunneling techniques
3.1.12. Understand IP spoofing techniques
3.2. Enumeration
3.2.1. What is enumeration
3.2.2. What is meant by null sessions
3.2.3. Null Session Countermeasures
3.2.4. What is SNMP enumeration
3.2.5. SNTP enumeration countermeasures
3.2.6. Windows 2000 DNS Zone transfer
3.2.7. UNIX enumeration
3.2.8. What are the steps involved in performing enumeration

Lesson Plan 3 Lecture & Labs

4. Lecture
System Hacking
4.1. Understand password cracking techniques
4.2. Password cracking countermeasures
4.3. Understand different types of passwords
4.3.1. Passive online attacks
4.3.2. Active online attacks
4.3.3. Offline attacks
4.3.4. Non-electronic attacks
4.4. Understanding Keyloggers and other spyware technologies
4.5. Understand escalating privileges
4.5.1. Executing applications
4.5.2. Buffer overflows
4.6. Understanding rootkits
4.6.1. Planting rootkits on Windows 2000 and XP machines
4.6.2. Rootkit embedded TCP/IP stack
4.6.3. Rootkit countermeasures
4.7. Understanding how to hide files
4.7.1. NTFS File Streaming
4.7.2. NTFS Stream countermeasures
4.8. Understanding steganography Technologies
4.9. Understanding How to cover your tracks and erase evidence – Covert hacking
4.9.1. Disabling Auditing
4.9.2. Clearing the event log

5. Lecture
Trojans, Backdoors, Viruses, and Worms
5.1. Trojans and Backdoors
5.1.1. What is a trojan
5.1.2. What is meant by overt and covert channels
5.1.3. List the different types of Trojans
5.1.4. How do reverse-connecting Trojans work
5.1.5. Understand how the netcat Trojan works

5.1.6. What are the indications of a trojan attack
5.1.7. What is meant by “Wrapping”?
5.1.8. Trojan construction kit and trojan makers
5.1.9. What are countermeasure techniques in preventing Trojans
5.1.10. Understand trojan-evading techniques
5.1.11. System file verification sub-objective to trojan countermeasures

5.2. Viruses and worms
5.2.1. Understand the difference between a virus and a worm
5.2.2. Understand the types of viruses
5.2.3. Understand antivirus evasion techniques
5.2.4. Understand virus detection methods

6. Lecture
Sniffers
6.1. Understand the protocols susceptible to sniffing
6.2. Understand active and passive sniffing
6.3. Understand ARP poisoning
6.4. Understand ethereal capture and display filters
6.5. Understand MAC flooding
6.6. Understand DNS spoofing techniques
6.7. Describe sniffing countermeasures

7. Lecture
Denial of Service and Session Hijacking
7.1. Denial of Service
7.1.1. Understand the types of DoS attacks
7.1.2. Understand how DDoS attacks work
7.1.3. Understand how BOTs/BOTNETs work
7.1.4. What is a “Smurf” attack
7.1.5. What is “SYN” flooding
7.1.6. Describe the DoS/DDos countermeasures

7.2. Session Hijacking
7.2.1. Understand spoofing vs. hijacking
7.2.2. List types of session hijacking
7.2.3. Understand sequence prediction
7.2.4. What are the steps in performing session hijacking

7.2.5. Describe how to prevent session hijacking

Lesson Plan 4 Lecture & Labs

8. Lecture
Hacking Web Servers, Web Application Vulnerabilities, and Web-based Password Cracking Techniques-
8.1. Hacking Web Servers
8.1.1. List the types of web server vulnerabilities
8.1.2. Understand the attacks against web servers
8.1.3. Understand IIS Unicode exploits
8.1.4. Understand patch management techniques
8.1.5. Describe web server hardening methods

8.2. Web application vulnerabilities
8.2.1. Understanding how web applications work
8.2.2. Objectives of web application hacking
8.2.3. anatomy of an attack
8.2.4. Web application threats
8.2.5. Understand Google hacking
8.2.6. Understand web application countermeasures

8.3. Web-Based password cracking techniques
8.3.1. List the authentication types
8.3.2. What is a Password Cracker?
8.3.3. How does a Password Cracker work?
8.3.4. Understand password attacks: classification
8.3.5. Understand password-cracking countermeasures

9. Lecture
SQL Injection and Buffer Overflows
9.1. SQL Injection
9.1.1. What is SQL injection
9.1.2. Understand the steps to conduct SQL injection
9.1.3. Understand SQL server vulnerabilities
9.1.4. Describe SQL Injection countermeasures

9.2. Buffer Overflows
9.2.1. Identify different types of buffer overflows and methods of detection
9.2.2. Overview of stack-based buffer overflows
9.2.3. Overview of buffer overflow mutation techniques

10. Lecture
Wireless Hacking
10.1. Overview of WEP, WPA Authentication mechanisms and cracking techniques
10.2. Overview of wireless sniffers and locating SSIDs, MAC spoofing
10.3. Understand rogue access points
10.4. Understand wireless hacking techniques
10.5. Describe the methods used to secure wireless networks

11. Lecture
Physical Security
11.1. Technical Security
11.2. Operational Security & Infosec
11.3. Physical security breach incidents
11.4. Understanding physical security
11.5. What is the need for physical security
11.6. Security Roles and Responsibilities
11.6.1. Administrative and Personnel Security
11.6.2. Security Planning & Implementation
11.7. Securing transmission media
11.7.1. Tempest Security
11.8. Securing Storage media
11.9. Securing Equipment
11.10. Securing Facilities
11.11. Factors affecting physical security

Lesson Plan 5 Lecture & Labs

12. Lecture
Linux Hacking
12.1. Linux basics
12.2. Understand how to compile a Linux kernel
12.3. Understand GCC compilation commands
12.4. Understand how to install Linux kernel modules 12.5. Understand Linux hardening methods

13. Lecture
Evading IDS’s, Honeypots, and Firewalls
13.1. Types of intrusion detection systems and evasion techniques
13.2. Firewall types and Honeypot evasion techniques

14. Lecture
15. Cryptography
15.1. Overview of cryptography and encryption techniques
15.2. Describe how public and private keys are generated

15.3. Overview of the MD5, SHA, RC4, RC5, and Blowfish algorithms

16. Lecture
Penetration Testing Methodologies
16.1. Defining security assessments
16.2. Overview of penetration testing methodologies
16.3. List the penetration testing steps
16.4. Overview of the Pen-Test legal framework 16.5. Overview of the Pen-Test deliverables
17. 22 Hr Labs

Risk & Vulnerability Surveys and Assessments

Information Gathering
Vulnerability Analysis
External Penetration Testing
Internal Network Penetration Testing
Router Penetration Testing
Firewall Penetration Testing
IDS Penetration Testing
Wireless Network Penetration Testing
Denial of Service Penetration Testing
Password Cracking Penetration Testing
Social Engineering Penetration Testing
Application Penetration Testing
Physical Security Penetration Testing
Database Penetration testing
VPN Penetration Testing
Penetration Testing Report Analysis, Penetration Testing Report and Documentation Writing, Penetration Testing Deliverables and Conclusion -

50 Question Online SUT Exam 1PM 3 Hr Penetration Test 2-5pn 1 hr gather data 6pm

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.
Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step **Books** - No books are required for this course. However, you may want to supplement your preparation by using tube videos.

Q/ISP Qualified/ Information Security Professional Certificate of Mastery

Q/EH® QUALIFIED/ ETHICAL HACKER CERTIFICATION/ WITH EXAM [CEH]

Hands-on Tactical Security skills training is what you want to achieve secure networks and secure information - learning how to hack and secure networks in today's world is about staying ahead of the hackers. No organization can fight back against cyber-attacks if their security and system administration staff does not know how the most current attacks are launched and the technical details that allow the attacks to be blocked."
This Intense 32+ 40 hour 1 week Q/EH® Qualified/ Ethical Hacker class provides you with basic understanding of the hacking skills and tools required to determine potential security weakness in your organization. This class is your next class after Security+ and before CISSP®. Be ready for SERIOUS tactical hands-on labs with advanced Ethical Hacker skills learning how to defend networks from cyber-attack. Step up to Qualified with the Q/EH® Certification. SU courses and certificate programs of mastery are designed to provide you with an immersive learning experience -- from hands-on workshops, certifications, with deep dives on a particular cyber security topic or technology. Every class is structured to give you expertise in critical areas that you can immediately put to use.

- DoD Navy 'P Sparks IAM' - "I sat through SU's Q/EH® class which was fairly impressive and asked a large number of questions concerning their other SUT Exams. Looking at the challenges that the DOD is attempting to address, the Q/ISP strikes me as more appropriate than most of the current SUT Exams. This course/exam group is multi-functional, each section dealing with a very IA oriented goal/need. The Q/PTL® which is part of the Q/ISP® Q/SA® requires a written test, a three hour examination of a specialized test scenario (also graded) and two months of lab time to complete a full assessment report. One of the student reports was 20 pages in length. Definitely a high level of competence to receive a certification."

"Yes. Please quote me, the instructor was great, he was very knowledgeable. I had CEH™ and CHFI™ training from another vendor and I did receive certification but I wish I had attended your classes instead, I would have learned much more."

No death by power point - the Q/EH® study guide engages you in real world scenarios, no old hacking tools, like other Ethical Hacking classes. More than 35 hands-on tactical security labs to ensure you're qualified and validated to defend networks from cyber threats.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40hr 1 wk + 32 hr pre-class study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 4 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practica Fail > 95% Attendance

Sample Job Titles
Blue Team Technician
Certified TEMPEST Professional
Certified TEMPEST Technical Authority
Close Access Technician
Computer Network Defense (CND) Auditor
Compliance Manager /Ethical Hacker
Governance Manager/ Information Security
Engineer/ Internal Enterprise Auditor
Network Security Engineer/ Penetration Tester
Red Team Technician/ Reverse Engineer
Risk/Vulnerability Analyst
Technical Surveillance Countermeasures
Technician/ Vulnerability Manager

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. *Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.Machines a Dual Core 18M Ram, T Gig drives, running MS OS, linux, and VMWare Workstation*
Tools for class - Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl'e able to describe potential system attacks and the actors that might perform them.
* Students KU Outcomes:

* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

- Instruction and review with an experienced master of ethical hacking
- QEH Certification Exam on site last day of class

- Access to SU's IT Professional Reference Library of targeted studies
- snacks

Learning Objectives:

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of attack techniques, evaluate actors and thwart further actor activity
- Utilize tools to discover malware, including rootkits, back- doors, and trojan horses, choosing appropriate defenses/ response tactics for each
- Use built-in command-line tools, as well as Linux netstat, ps, and lsof to detect an actors presence on a machine
- Analyze routers,ARP tables, switch CAM tables to track an actor activity to dentify a suspect
- Use memory dumps and the Volatility tool to determine an actors activities on a machine, the malware installed, and other machines the actor used as pivot points across the network
- Gain access of a target machine using Metasploit, and then detecting the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how actors use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an actors tactics
- Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choosing appropriate response actions based on each actor's flood technique

Analyze shell history files to find compromised machines, actor-controlled accounts, sniffers, and backdoors QED certification, tests on the following 22 domains.

1. QED Ethics and Legal Issues
2. QED c
3. QED Scanning
4. QED Enumeration
5. QED System Hacking
6. QED Trojans and Backdoors
7. QED Sniffers
8. QED Denial of Service
9. QED Social Engineering
10. QED Session Hijacking
11. QED Hacking Web Servers
12. QED Web Application Vulnerabilities
13. QED Web Based Password Cracking Techniques
14. QED SQL Injection
15. QED Hacking Wireless Networks
16. QED Virus and Worms
17. QED Hacking Novell
18. QED Hacking Linux
19. QED IDS, Firewalls and Honeypots
20. QED Buffer Overflows
21. QED Cryptography
22. QED Penetration Testing Methodologies

Lesson Plan 1

Qualified Ethical Hacker /Defender (QEH/D) Module 1: Ethics and Legality **Lecture/Labs**

- Understand Ethical Hacking terminology
- Define the Job role of an ethical hacker
- Understand the different phases involved in ethical hacking
- Identify different types of hacking technologies
- List the 5 stages of ethical hacking?
- What is hacktivism?
- List different types of hacker classes
- Define the skills required to become an ethical hacker
- What is vulnerability research?
- Describe the ways in conducting ethical hacking
- Understand the Legal implications of hacking
- Understand 18 U.S.C. § 1030 US Federal Law

Qualified Ethical Hacker /Defender (QEH/D)) Module 2: Footprinting **Lecture/Labs**

- Define the term Footprinting
- Describe information gathering methodology
- Describe competitive intelligence
- Understand DNS enumeration
- Understand Whois, ARIN lookup
- Identify different types of DNS records
- Understand how traceroute is used in Footprinting
- Understand how E-mail tracking works
- Understand how web spiders work

Qualified Ethical Hacker /Defender (QEH/D) Module 3: Scanning **Lecture Labs**

- Define the term port scanning, network scanning and vulnerability scanning
- Understand the CEH scanning methodology
- Understand Ping Sweep techniques
- Understand nmap command switches
- Understand SYN, Stealth, XMAS, NULL, IDLE and FIN scans
- List TCP communication flag types
- Understand War dialing techniques
- Understand banner grabbing and OF fingerprinting techniques

Lesson Plan 2

Qualified Ethical Hacker /Defender (QEH/D) Module 5: System Hacking **lecture/ Labs**

- Understanding password cracking techniques
- Understanding different types of passwords
- Identifying various password cracking tools
- Understand Escalating privileges

- Understand how proxy servers are used in launching an attack
- How does anonymizers work
- Understand HTTP tunneling techniques
- Understand IP Spoffing Techniques

Qualified Ethical Hacker /Defender (QEH/D) Module 4: Enumeration **Lecture/ Labs**

- What is Enumeration?
- What is meant by null sessions
- What is SNMP enumeration?
- What are the steps involved in performing enumeration?
- Understanding keyloggers and other spyware technologies
- Understand how to Hide files
- Understanding rootkits
- Understand Steganography technologies
- Understand how to covering your tracks and erase evidences

Qualified Ethical Hacker /Defender (QEH/D)) Module 6: Trojans and Backdoors **Lecture/ Labs**

- What is a Trojan?
- What is meant by overt and covert channels?
- List the different types of Trojans
- What are the indications of a Trojan attack?
- Understand how “Netcat” Trojan works
- What is meant by “wrapping”
- How does reverse connecting Trojans work?
- What are the countermeasure techniques in preventing Trojans?
- Understand Trojan evading techniques

Qualified Ethical Hacker /Defender (QEH/D) Module 7: Sniffers **Lecture Labs**

- Understand the protocol susceptible to sniffing
- Understand active and passive sniffing
- Understand ARP poisoning
- Understand ethereal capture and display filters
- Understand MAC flooding
- Understand DNS spoofing techniques
- Describe sniffing countermeasures

Lesson Plan 3

Qualified Ethical Hacker /Defender (QEH/D) Module 8: Denial of Service **Lecture Labs**

- Understand the types of DoS Attacks
- Understand how DDoS attack works
- Understand how BOTs/BOTNETS work
- What is “smurf” attack
- What is “SYN” flooding
- Describe the DoS/DDoS countermeasures

Qualified Ethical Hacker /Defender (QEH/D)) Module 9: Social Engineering **Lecture Labs**

- What is Social Engineering?
- What are the Common Types of Attacks
- Understand Dumpster Diving
- Understand Reverse Social Engineering
- Understand Insider attacks
- Understand Identity Theft
- Describe Phishing Attacks
- Understand Online Scams
- Understand URL obfuscation
- Social Engineering countermeasures

Qualified Ethical Hacker /Defender (QEH/D) Module 10: Session Hijacking **Lecture Labs**

- Understand Spoofing vs. Hijacking
- List the types of Session Hijacking
- Understand Sequence Prediction
- What are the steps in performing session hijacking
- Describe how you would prevent session hijacking

Qualified Ethical Hacker /Defender (QEH/D) Module 11: Hacking Web Servers **Lecture Labs**

- List the types of web server vulnerabilities
- Understand the attacks Against Web Servers

- Understand IIS Unicode exploits
- Understand patch management techniques
- Understand Web Application Scanner
- What is Metasploit Framework?
- Describe Web Server hardening methods

Lesson Plan 4

Qualified Ethical Hacker /Defender (QEH/D) Module 12: Web Application Vulnerabilities **Lecture Labs**

- Understanding how web application works
- Objectives of web application hacking
- QSAAnatomy of an attack
- Web application threats
- Understand Google hacking
- Understand Web Application Countermeasures

Qualified Ethical Hacker /Defender (QEH/D) Module 13: Web Based Password Cracking Techniques **Lecture Labs**

- List the Authentication types
- What is a Password Cracker?
- How does a Password Cracker work?
- Understand Password Attacks - Classification
- Understand Password Cracking Countermeasures

Qualified Ethical Hacker /Defender (QEH/D) Module 14: SQL Injection **Lecture Labs**

- What is SQL injection?
- Understand the Steps to conduct SQL injection
- Understand SQL Server vulnerabilities
- Describe SQL Injection countermeasures

Qualified Ethical Hacker /Defender (QEH/D) Module 15: Hacking Networks **Lecture Labs**

- Overview of WEP, WPA authentication systems and cracking techniques
- Overview of Sniffers and SSID, MAC Spoofing
- Understand Rogue Access Points
- Understand hacking techniques
- Describe the methods in securing networks

Qualified Ethical Hacker /Defender (QEH/D) Module 16: Virus and Worms **Lecture Labs**

- Understand the difference between an virus and a Worm
- Understand the types of Viruses
- How a virus spreads and infects the system
- Understand antivirus evasion techniques
- Understand Virus detection methods

125 online EXAM starts at 1pm (3 hr exam)

Lesson Plan 5

Qualified Ethical Hacker /Defender (QEH/D) Module 17: Physical Hacking **Lecture Labs**

- Physical security breach incidents
- Understanding physical security
- What is the need for physical security?
- Who is accountable for physical security?
- Factors affecting physical security

Qualified Ethical Hacker /Defender (QEH/D) Module 18: Linux Hacking **Lecture Labs**

- Understand how to compile a Linux Kernel
- Understand GCC compilation commands
- Understand how to install LKM modules
- Understand Linux hardening methods

Qualified Ethical Hacker /Defender (QEH/D) Module 19: IDS, Firewalls and Honeypots **Lecture Labs**

- List the types of Intrusion Detection Systems and evasion techniques
- List firewall and honeypot evasion techniques

Qualified Ethical Hacker /Defender (QEH/D) Module 20: Buffer Overflows **Lecture Labs**

- Overview of stack based buffer overflows
- Identify the different types of buffer overflows and methods of detection
- Overview of buffer overflow mutation techniques

Qualified Ethical Hacker /Defender (QEH/D) Module 21: Cryptography **Lecture Labs**

- Overview of cryptography and encryption techniques
- Describe how public and private keys are generated
- Overview of MD5, SHA, RC4, RC5, Blowfish algorithms

Qualified Ethical Hacker /Defender (QEH/D) Module 22: Penetration Testing Methodologies **Lecture Labs**

- Overview of penetration testing methodologies
- List the penetration testing steps
- Overview of the Pen-Test legal framework
- Overview of the Pen-Test deliverables
- List the automated penetration testing tools

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential with SU or another school unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.
Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013) The book below is recommended for those interested in understanding how their own computers work for personal edification

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery CPoM / non degree-
Q/SA® Qualified/ Security Analyst Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Workshop Required
Q/EH® Qualified/ Ethical Hacker Certification Class w/exam
Q/ND® Qualified/ Network Defender Certification Class w/exam
Q/FE® Qualified/ Forensic Expert Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Certification Class *
SU Security+® CompTIA Certification Class w/exam
SU SecurityX®- [formerly CASP] Certification Class w/exam
Linux/UNIX® Security Certification Class w/exam
Cloud Computing Security Knowledge Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Practicum
Q/ND® Qualified/ Network Defender Certification Practicum
Q/FE® Qualified/ Forensic Expert Certification Class Practicum

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery SU

CompTIA CySA+ CYBERSECURITY ANALYST+ CERTIFICATION CLASS W/EXAM

As attackers have learned to evade traditional signature-based solutions, an analytics-based approach has become extremely important. CompTIA CySA+ certification applies behavioral analytics to the IT security market to improve the overall state of IT security. Analytics have been successfully integrated into the business intelligence, retail and financial services industries for decades. Now they are also applied to IT security. Security analytics greatly improves threat visibility across a broad attack surface by focusing on network behavior, including an organization's interior network. Threats are better detected using analytics.

Class Fee:	*$3,990*
Time:	*72 hrs*
Learning Level:	*Intermediate*
Contact Hours:	*40 hr 1 wk + 32 hr pre-study & 2hr exam*
Prerequisites:	*TCP/IP knowledge.*
Credits:	*72 CPE / 3 CEU*
Method of Delivery:	*face-to-face*
Instructor:	*TBD*
Method of Evaluation:	*95 % attendance 100 % completion of Lab*

Grading: Pass = Attendance + labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. Text Materials: SU Cardwell Q/SA -CySA handbook, labs, online quizzes SU resource CD's and 500 exam questions. *No tools for this class, students bring on their own laptop machines with www.freepractice test.com and exam force pre installed. CySA+ addresses the increased diversity of knowledge, skills and abilities (KSAs) required of today's security analysts and validates what is currently necessary to perform effectively on the job. CySA+ certification reflects the KSAs needed to analyze the state of security within modern IT environments, including:*

Lesson	Description	Matching CySA+ Objectives (Samples)
1. Cyber Defense Analyst **PR-DA-001**	Uses data collected from a variety of cyber- defense tools (e.g., intrusion detection system (IDS) alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	1.1 — Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes 1.2 — Given a scenario, analyze the results of a network reconnaissance 1.3 — Given a network-based threat, implement or recommend the appropriate response and countermeasure

2. Cyber Defense Infrastructure Support Specialist PR-INF-001	Tests, implements, deploys, maintains and administers the infrastructure hardware and software.	1.4 — Explain the purpose of practices used to secure a corporate environment 2.3 — Compare and contrast common vulnerabilities found in the following targets within an organization 4.3 — Given a scenario, review security architecture and make recommendations to implement compensating controls
3. Cyber Defense Incident Responder PR-IR-001	Investigates, analyzes and responds to cyber-incidents within the network environment or enclave.	3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 3.3 — Explain the importance of communication during the incident response process 3.4 — Given a scenario, analyze common symptoms to select the best course of action to support incident response 3.5 — Summarize the incident recovery and post-incident response process
4. Vulnerability Assessment Analyst PR-VA-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy or local policy. Measures effectiveness of defense-in- depth architecture against known vulnerabilities.	2.1 — Given a scenario, implement an information security vulnerability management process 2.2 — Given a scenario, analyze the output resulting from a vulnerability scan 2.3 — Compare and contrast common vulnerabilities found in the following targets within an organization
5. Warning Analyst AN-TA-001	Develops unique cyber-indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes and disseminates cyber-warning assessments.	1.1 — Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes 1.2 — Given a scenario, analyze the results of a network reconnaissance 3.3 — Explain the importance of communication during the incident response process
6. Cyber Crime Investigator ***IN-CI-001***	Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.	3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 3.5 — Summarize the incident recovery and post-incident response process 4.1 — Explain the relationship between frameworks, common policies, controls and procedures 4.5 — Compare and contrast the

		general purpose and reasons for using various cybersecurity tools and technologies
7. Forensics Analyst IN-FO-001	Conducts deep-dive investigations on computer- based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber-intrusion incidents.	1.1 — Given a scenario, apply ironmental reconnaissance techniques using appropriate tools and processes 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 4.5 — Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies
8. Cyber Defense Forensics Analyst IN-FO-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	2.2 — Given a scenario, analyze the output resulting from a vulnerability scan 3.1 — Given a scenario, distinguish threat data or behavior to determine the impact of an incident 3.2 — Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation 3.4 — Given a scenario, analyze common symptoms to select the best course of action to support incident response

Q/ISP Qualified/ Information Security Professional Certificate of M ,

Q/ND QUALIFIED/ NETWORK DEFENDER CERTIFICATION CLASS W/EXAM AND PRACTICUM

Q/ND® Qualified/ Network Defender Certification Class w/exam
This is the last class of the Q/ISP Qualified/ Information Security Professional Certification. It's the class that shows you defensive scenario's to protect your networks from the hacker attacks and internal misconfiguations, data breaches and compromises. If network defense certification and security skills assessment is your goal, this class teaches you network firewall & router monitoring and defense, deep packet analysis/ including IDS & IPS, DNA malware detection and re-engineering. You learn offense from a defensive position with a "5 step" best practice process to measure your network defense goals.

75% hands-on labs for improving risk at DMZs, internet facing connections, external partner connections, intranet traffic, and managing security breaches. This certification is all about "real life" network defense scenarios.

Class Fee:	$3,990
Time:	72 hours
Learning Level:	Entry Level
Contact Hours:	40hr 1 wk + 32 hr pre-class study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab Grading: Pass = Attendance + Completion of Labs and Practicum Fail > 95% Attendance This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator
Network Analyst
Network Security Engineer
Network Security Specialist
Security Analyst
Security Engineer
Security Specialist
Systems Security Engineer

Who Should Attend

Information Security administrators, Information Systems Managers, Auditors, Network Administrators, Consultants, Systems and Data Security Analysts, and others seeking to enhance their FW, IPV security knowledge.

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class - Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , SAINT , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl', Hekix, Digtal DNA, Triumphant, soft wall fw, CISCO FW, Cisco routers

KU Outcomes:
* Students will be able to describe potential system attacks and the actors that might perform them.
* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives

Identify the threats against network infrastructures and mitigate risk/impact of attacks
Learn how to harden the network firewalls, and the SIEMs that analyze a network threat to detect the adversary
Decode and analyze packets using various tools to identify anomalies and improve network defenses
Understand how the write snort signatures and apply at points of compromise
Understand the 6 steps in the incident handling process and how to run an incident handling capability
Learn how to use tools to identify /remediate malware
Create a data classification program, deploy data loss prevention solutions at layer 2/3
In-depth Packet Analysis labs

- Hands on Snort & IPS labs
- Hands-on reverse engineering viruses & trojan labs
- Mitigate site spoofing & phishing
- Mitigating botnets
- False alarms vs. real threats analysis
- IPS Filtering techniques
- NAC's - effective containment technique
- Best practices, step by step process for perimeter protection
- Define a recovery strategy
- 5 steps that establish measurable goals for network defenses.

Lesson Plan 1

1. Review of Internet

Attacks

hacker trends and motives
denial-of-service attacks: SYN floods, smurf, Trinoo and others
network probes and scans
IP spoofing
Trojan horses
application-level attacks

2. Characteristics of the Firewall Environment

objectives of firewalls
creating security domains
perimeter and internal firewalls
firewall rule sets
defining the firewall stance: default deny vs. default allow
firewall platforms
common commercial firewalls
host-based firewalls
firewall appliances
firewall configurations
dual-homed configurations
demilitarized zones (DMZs)
screened sub-networks
multi-homed configurations
high availability firewalls
positioning Network Services in the firewall environment
servers on the firewall
single server vs. multiple server
access to internal applications
firewall architectures: packet filters, proxy-based firewalls, hybrid firewalls
issues not addressed by firewalls: poor passwords, data-driven attacks, modems, internal attacks

3. Firewall Security Policies

risk assessment approach
identifying essential services
identifying key threats
vulnerability assessment
developing firewall rule sets
supporting essential network services
"dangerous" network services
creating policies for inbound access and outbound access
Network Address Translation (NAT) and PortAddress Translation (PAT)
additional elements of the firewall security policy
denial-of-service filters
account management and authentication
remote management

4. Standard (Stateless) Packet Filters

packet filter design
identifying where packet filtering is performed
rules processing
ingress and egress filtering
packet filter control points
connection parameters
TCP flags
ICMP message types
permitting established connections
configuring packet filters to control access to common protocols: HTTP, SMTP, DNS
advanced packet filter usage
addressing denial-of-service attacks: LAND, ping floods, SYN floods
dynamic access controls
authentication, authorization and accounting (AAA)
limitations of packet filters
handling difficult protocols: FTP, multimedia

5. Lesson Plan 2
Stateful Inspection Firewalls

stateful inspection firewall design
overcoming the limitations of standard (stateless) packet filters
control points for stateful inspection firewalls
strengths and weaknesses of stateful inspection technology
configuring the TCP/IP protocol stack

IP forwarding issues
maintaining stateful information
connection tables and performance
pseudo connections for UDP
network address translation techniques
application protocol handling
handling FTP and streaming protocols
application data
Web content: ActiveX controls, Java applets

6. Proxy-Based Firewalls

proxy firewall design
characteristics of proxy-based connections
important differences between proxy firewalls and caching proxy servers
address hiding
circuit-level proxies
application-layer proxies
strengths and weaknesses of proxy firewalls
configuring the TCP/IP protocol stack for proxy firewalls
hardening the protocol stack
IP forwarding issues
application proxy rules processing
application protocol and data handling
configuring application proxies to support SMTP, FTP, HTTP
configuring generic proxy servers
onE-to-one
any-to-one

- The need for IPVs
- How to configure
- How to integrate with firewalls & VPN's
- What VPN's to use with which firewalls
- Gartner's report on IPV & IPV matrix

10. Content Filtering and Other Network Perimeter Safeguards

the need for content filters
deploying content filters
SMTP filters
anti-virus
blocking Trojans and Worms at the SMTP server
spam filtering
anti-relaying
Web site filtering blockers
database management
recommended policies and actions
filtering mobile code: ActiveX, Java, JavaScript
intrusion detection tools
Integrating firewalls

Lesson Plan 4

1. Preparation - Laying the groundwork for effective malware

7. Proxy Servers for Internal to External Access

types of proxy servers
Winsock proxy servers
SOCKS proxy servers
Web proxy servers
configuring clients for proxy servers, client applications, client operating systems, port redirectors on proxy server gateways

8. Personal Firewalls

the need for personal firewalls
the mobile user
home office users
Trojan horse problems
managing the personal firewall
standard templates vs advanced configuration
user managed vs. centralized management
common personal firewalls

Lesson Plan 3

9. VPN's

- The need for VPN's
- How to configure
- How to integrate with firewalls
- What VPN's to use with which firewalls

Securing network connections using VPN
Prevention Tools

firewall penetration-testing tools
securing network connections using VPNs

11. Firewall, VPN & Prevention Management

assessing the firewall, VPN & IPV vendors
independent certification of firewall & VPN products
installation, training and after sales support
assigning resources for firewall, VPN & IPV management
firewall & VPN administrator responsibilities
88 creating a secure platform for prevention
creating a bastion host
NT hardening
Unix hardening
creating system baselines
monitoring the firewall
firewall, VPN, & IPV alerts
incident handling: best practices
log file management: content and processing tools
keeping up to date: key E-mail lists and Web sites

incident management with a look at the current state of malware threats and their evolution.

- Malware defined
- Environments where viruses & malware thrive
- Malware risks
- Review the new threat - blended attacks

- Trojan review & analysis
- Patch Management using PatchLink Update
- Strengths and weaknesses of current anti-virus products
- Install Confidence on-line, NORTON, SOPHOS, MCAFEE and other virus software in Hands-On labs

2. Detection - In a recent study, less than a third of the participants realized they'd experienced a malware attack. How to detect and analyze a malware incident quickly and accurately.

- Advanced virus & trojan diagnosis and identification
- Identifying missing Patches
- False positives alarms vs. actual incidents
- NIMDA, CODE RED and others - learn what they do
- Dissecting audit records
- Determining source and scope of infection

3. Containment and secure application review - A look at the two essential containment techniques — stopping the malware spread, bad coding and halting the side affects.

- Filtering inbound and outbound network traffic
- The importance of public relations
- Identifying patch impact
- Limiting exposure by secure application coding

4. Eradication - If a virus or other malware does attack, how to remove it completely in the most effective and permanent manner.

- Reviewing system configuration and initialization items
- Removing modifications to courses and data files
- Benefits and challenges of current removal techniques

5. Recovery and patching your network - Returning the network and any other affected systems to full operation, with minimal impact. Special emphasis on systems and data backup recovery techniques.

- Returning the network systems to full operation
- Patch deployment
- What was the impact.
- systems and data backup recovery techniques
- A review of Core Security Impact vulnerability exploit tool to ensure patch updates.

6 . Response and follow-Up - How and why did the attack happen, how was it removed, and what lessons can be applied to possible future attacks? The final and most crucial step in a successful incident management program

- Establishing a incident response team based on the type of incident
- Documenting lessons learned
- Metric collection and trend analysis
- Establishing measurable goals for compliance

- Anti-virus and anti-trojan product strengths and weaknesses
- Determining a detection treatment for trojans & viruses
- Selecting effective containment and patching techniques
- Removing infections and residual affects
- Defining patch management goals and compliance metrics
-

Q/ND Practicum Q/ND QUALIFIED/ NETWORK DEFENDER PRACTICUM

– Configuration Exercise - Practicum: Create Configuration Guides for Servers(running on VMs) and a Lab Manual
1. Based on the virtual machines used in the Q/ND class labs (aSIEM (open source or proprietary), a Firewall, a web server, a bastion host and a Web Application Firewall - WAF) you will create secure server and (virtual) network configurations to protect a scenario you create (a public facing Web server for a Cloud service provided to the Internet).Your scenario should list the CVEs you are mitigating the threat of by your setup.
2. You get to decide how are you going to configure each virtual server as well as what base VM and/or OS is used for each server (firewall, SIEM, Bastion, WAF, Web Server / IDS) BASED ON THE TREAT VECTOR
3. As you build the Firewall virtual machine from scratch. You are free to implement a Firewall by the method / software of your choosing (including creating “firewall rules” in the simulation Cisco router, using Linux IPtables, or by installing the SmoothWall firewall).
a. You must configure at least 15 firewall rules in the Firewall you build. These rules should provide a strong security architecture specifically to mitigate the threats in your scenario by CVE number.
4. You need to run a Web Server with an Network IDS running on it to show what traffic is making it to the Web Server from outside. This virtual machine can be based on either Windows (e.g. IIS plus Windows Snort) or Linux (Apache plus Snort). We recommend the Linux virtual machine.
a. The Snort IDS should be configured with SNORT rules to verify that a strong security architecture and policy has been implemented by your firewall. It should be appropriate to prove that each of the 15 firewall rules configured is performing properly (by checking for the threats in the scenario’s CVEs).
5. You’ll describe how you configured each server in your test initially (pre-test) as well as (Post-test) the final and secure configuration. a. Pre-Design Test – initial base configuration. Then evaluate the insecurities. b.Post-Design Test – final configuration after you designed the security defenses.
6. In addition you are going to produce a Lab Manual –a step by step guide(a “how to” -- bring up this VM, bring up that VM, etc.). You need to detail exactly how you installed, configured and tested each component.
7. There are required four (4) network protocols/services you need to support passing from the Internet through your ‘Firewall’s filters into the network: a.SSH - to the (1) Bastion Host, (2) external firewall, (3) Web Application Firewall and (4) Web server.
b. WWW - from outside to the web server (but it must be forced to go the the web server via the Web Application Firewall).
c. EMAIL -- external inbound email. You are free to keep the email outside the network on an outsourced cloud service.
d. DNS -- Just used on the external segment (through router is good enough) e.g. to thepublic WWW server.
8. There are five virtual machine servers that you need to configure and describe – along with step by step instructions on how to set up and secure in the Lab manual: Firewall (You must list the filtering rules providing the Firewall function).

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Q/FE QUALIFIED/ FORENSICS EXPERT CERTIFICATION CLASS W/EXAM

How to detect the crime, track the criminal, and assemble the evidence.

Finally, a tactical Forensics class that provides everything you need to know to be a Qualified/ Forensic Expert with an online exam at the end of the course with a 90 day practicum to validate & prove your forensic skills. Learn everything relating to computer forensics & digital forensics rights. From how to establish a proper chain of custody that is admissible in a court of law to recovering files from intentionally damaged media.

Cyber crime is out performing traditional crime. Qualified/ Forensics Experts are needed by today's companies to determine the root cause of a hacker attack, collect evidence legally admissible in court, and protect corporate assets and reputation.

High-profile cases of corporate malfeasance have elevated electronic evidence discovery as indispensable to your company. A recent law review claims: A lawyer or legal team without a Forensic Expert on their case is sure to lose in today's courtroom!

Learn more about SU's Federation of Q/FE's Qualified/ Forensic Experts & Examiners

Learning Objectives:

Discover the root of how computer crimes are committed.
Learn how to find traces of illegal or illicit activities left on disk with forensics tools and manual techniques.
Learn how to recover data intentionally destroyed or hidden.
How to recover encrypted data.
Steps to collect evidence from hard drives and live systems.
How to recover data from digital cameras and cell phones.
You will create an effective computer crime policy, and gain the hands on skills to implement it.

Sample Job Titles
Computer Crime Investigator
Incident Handler
Incident Responder
Incident Response Analyst
Incident Response Coordinator
Intrusion Analyst
Computer Forensic Analyst
Computer Network Defense Forensic Analyst
Digital Forensic Examiner
Digital Media Collector
Forensic Analyst
Forensic Analyst (Cryptologic)
Forensic Technician
Network Forensic Examiner

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-class study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance; 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practicum for CPoM Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: labs, QFE Investigation Materials, resource CD's and threat vector and investigation attack handouts. Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl', Access Data,

Who Should Attend: Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators, Consultants, Systems and Data Security Analysts, and others concerned with enhanced information security.
Students will be able to describe potential system attacks and the actors that might perform them.

* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives:

- The basics of computer forensics
- Proven investigative strategies
- Tracking an offender on the Internet and intranets
- Tips and techniques for incident response
- Proper handling of evidence
- Working with law enforcement

Lesson Plan 1

Intro to Computer Crimes

If you don't know exactly what computer crime is, you can't effectively protect your organization. Knowledge and understanding begins here.

Lecture labs Detecting Computer Crime

- Factors affecting detection
- Intrusion indicators
- Detection Methods
- Digital Forensics defined
- Data Hiding
- Text Searching

Lecture labs

Setting Up a Forensics Group

A crucial part of any computer crime prevention strategy is deciding who's going to be responsible… and how they're going to achieve their goals.

- Staffing recommendations
- Establishing policies
- Providing the right training
- Time-proven best practices
- Sample policies and reports

Lesson Plan 2

Lecture labs

High-Tech Investigations

When a criminal strikes, the right incident response strategy and investigative tactics can spell the difference between a business writE-off and a civil judgment or criminal conviction.

- Investigating Computer Crimes and Incidents
- Objectives/basics of investigations
- Scoping the investigation
- Classifying the investigation
- Determining how the crime was committed
- Discerning which questions you are trying to answer
- Data capture, discovery, and recovery
- Analyzing evidence
- Following accepted forensics protocols
- Organizing the investigation
- Investigative challenges
- Performing the investigation
- Civil litigation and restitution
- Criminal prosecution: dealing with suspects
- Planning for an incident before it occurs
- Recommended response team members
- Determining the ROI of an investigation
- Developing a computer incident flow chart

Lesson Plan 3

Lecture lab

Advanced Computer Forensics

An advanced look at computer crime evidence and the best methods for retrieving it.

- Types of forensics — field vs. lab
- Forensics basics — Acquire, Authenticate, Analyze
- Acquiring legally sufficient evidence
- Authenticating the evidence
- Analyzing the evidence
- Windows and UNIX/Linux forensics
- Hardware and software recommendations

Tracking an Offender

If you can't locate the offender — and, even more important, the offending computer — you're back to square one. Tips, tools, and techniques for locating the offending computer on the network, on an intranet, and the Internet.

- Determining civil, criminal, and internal "proof"
- Processing a scene that includes digital evidence
- Proper seizure techniques

Lesson Plan 4

Lecture labs

Digital Forensics Tools (Hands-On Labs)

- Misc. Software tools
- Traveling computer forensics kit
- Secure forensics laboratory
- EnCase demo
- Access data demo
- Fastbloc
- Diskscrub from NTI,
- SMART image program
- Nature of the media
- Quick preview of content
- Image acquisition

Lesson Plan 5

Lecture labs

Proper Evidence Handling

Once you've decided to devote time and manpower to investigating an incident, you'll want to ensure the evidence you collect is viable for civil, criminal, or internal prosecution.

- Processing the evidence
- Maintaining chain of custody
- The role of image backups

Lecture labs

Evidence

- Rules of evidence
- Legal recovery
- Types/classification of evidence
- Direct
- Real
- Documentary
- Demonstrative
- Public
- Private
- Legal
- Proprietary
- Intrusive
- Analyzing computer evidence
- Chain of custody and evidence life cycle
- Search and seizure
- Pulling the plug
- Removing the hardware
- Hardware check
- On-site backup
- On-site searches
- Executing search and seizure

Lecture lab

Working with Law Enforcement

A good working relationship with law enforcement is an important part of every corporate computer crime strategy.

How to work with law enforcement — before and after the crime — to achieve optimal results.

- Omnibus Act
- Privacy Protection Act and Electronic Communications Privacy Act
- Fourth Amendment
- Privacy and other laws
- Search warrants
- What law enforcement can do to help
- When, how, and why to contact law enforcement
- Pertinent laws and rules of evidence
- Statement of damages — actual and projected
- Jurisdictional issues

Hands-On Class Exercises

- Analysis of operating systems, hard drives, and PDAs
- Locating, handling, and processing digital evidence
- Important case studies
- Tools and sources for updated learning

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Q/FE QUALIFIED/FORENSIC EXPERT PRACTICUM

How to detect the crime, track the criminal, and assemble the evidence practicum.

Finally, a tactical Forensics practicum that provides everything you need to know to be a Qualified/ Forensic Expert with an with a ***90 day practicum to validate & prove your forensic skills***. Learn everything relating to computer forensics & digital forensics rights. From how to establish a proper chain of custody that is admissible in a court of law to recovering files from intentionally damaged media.

Cyber crime is out performing traditional crime. Qualified/ Forensics Experts are needed by today's companies to determine the root cause of a hacker attack, collect evidence legally admissible in court, and protect corporate assets and reputation. High-profile cases of corporate malfeasance have elevated electronic evidence discovery as indispensable to your company. A recent law review claims: A lawyer or legal team without a Forensic Expert on their case is sure to lose in today's courtroom!

Learn more about SU's Federation of Q/FE's Qualified/ Forensic Experts & Examiners

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance and Practicum   Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. Text Materials: SU Course materials Forensic handbook, labs, online quizzes SU resource CD's and 500 exam questions. No tools for this class, students bring on their own laptop machines with www.freepractice test.com and exam force pre installed. CySA+ addresses the increased diversity of knowledge, skills and abilities (KSAs) required of today's security analysts and validates what is currently necessary to perform effectively on the job. CySA+ certification reflects the KSAs needed to analyze the state of security within modern IT environments, including

Forensic Expert Practicum

120 day practicum to analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Digital Forensics Practicum requirement tasks

- T0027: Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
- T0036: Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
- T0048: Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not

limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.

- T0049: Decrypt seized data using technical means.
- T0075: Provide technical summary of findings in accordance with established reporting procedures.
- T0087: Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.
- T0103: Examine recovered data for information of relevance to the issue at hand.
- T0113: Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
- T0165: Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.
- T0167: Perform file signature analysis.
- T0168: Perform hash comparison against established database.
- T0172: Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).
- T0173: Perform timeline analysis.
- T0175: Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
- T0179: Perform static media analysis.
- T0182: Perform tier 1, 2, and 3 malware analysis.
- T0190: Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).
- T0212: Provide technical assistance on digital evidence matters to appropriate personnel.
- T0216: Recognize and accurately report forensic artifacts indicative of a particular operating system.
- T0238: Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
- T0240: Capture and analyze network traffic associated with malicious activities using network monitoring tools.
- T0241: Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
- T0253: Conduct cursory binary analysis.
- T0279: Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
- T0285: Perform virus scanning on digital media.
- T0286: Perform file system forensic analysis.
- T0287: Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).
- T0288: Perform static malware analysis.
- T0289: Utilize deployable forensics toolkit to support operations as necessary.
- T0312: Coordinate with intelligence analysts to correlate threat assessment data.
- T0396: Process image with appropriate tools depending on analyst's goals.
- T0397: Perform Windows registry analysis.
- T0398: Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.
- T0399: Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.
- T0400: Correlate incident data and perform cyber defense reporting.
- T0401: Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
- T0432: Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
- T0532: Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.
- T0546: Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.

Skills

- S0032: Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
- S0047: Skill in preserving evidence integrity according to standard operating procedures or national standards.
- S0062: Skill in analyzing memory dumps to extract information.
- S0065: Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
- S0067: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
- S0068: Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

- S0069: Skill in setting up a forensic workstation.
- S0071: Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).
- S0073: Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
- S0074: Skill in physically disassembling PCs.
- S0075: Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).
- S0087: Skill in deep analysis of captured malicious code (e.g., malware forensics).
- S0088: Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).
- S0089: Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
- S0090: Skill in analyzing anomalous code as malicious or benign.
- S0091: Skill in analyzing volatile data.
- S0092: Skill in identifying obfuscation techniques.
- S0093: Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.
- S0131: Skill in analyzing malware.
- S0132: Skill in conducting bit-level analysis.
- S0133: Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.
- S0156: Skill in performing packet-level analysis.

Knowledge

- K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cyber security and privacy.
- K0004: Knowledge of cyber security and privacy principles.
- K0005: Knowledge of cyber threats and vulnerabilities.
- K0006: Knowledge of specific operational impacts of cyber security lapses.
- K0018: Knowledge of encryption algorithms
- K0021: Knowledge of data backup and recovery.
- K0042: Knowledge of incident response and handling methodologies.
- K0060: Knowledge of operating systems.
- K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- K0077: Knowledge of server and client operating systems.
- K0078: Knowledge of server diagnostic tools and fault identification techniques.
- K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
- K0117: Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
- K0118: Knowledge of processes for seizing and preserving digital evidence.
- K0119: Knowledge of hacking methodologies.
- K0122: Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
- K0123: Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
- K0125: Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
- K0128: Knowledge of types and collection of persistent data.
- K0131: Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
- K0132: Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
- K0133: Knowledge of types of digital forensics data and how to recognize them.
- K0134: Knowledge of deployable forensics.
- K0145: Knowledge of security event correlation tools.
- K0155: Knowledge of electronic evidence law.
- K0156: Knowledge of legal rules of evidence and court procedure.
- K0167: Knowledge of system administration, network, and operating system hardening techniques.
- K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

- K0182: Knowledge of data carving tools and techniques (e.g., Foremost).
- K0183: Knowledge of reverse engineering concepts.
- K0184: Knowledge of anti-forensics tactics, techniques, and procedures.
- K0185: Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
- K0186: Knowledge of debugging procedures and tools.
- K0187: Knowledge of file type abuse by adversaries for anomalous behavior.
- K0188: Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).
- K0189: Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer’s display device).
- K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
- K0254: Knowledge of binary analysis.
- K0255: Knowledge of network architecture concepts including topology, protocols, and components.
- K0301: Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- K0304: Knowledge of concepts and practices of processing digital forensic data.
- K0347: Knowledge and understanding of operational design.
- K0624 : Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

Abilities

- A0005: Ability to decrypt digital data collections.
- A0043: Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

SECURITY+ CompTIA CERTIFICATION W/EXAM

How to plan for network security that matches your technology infrastructure from top to bottom.

Security+ Certification is the primary course you will need to take if your job responsibilities include securing network services, network devices, and network traffic. It is also the main course you will take to prepare for the CompTIA Security+ examination. In this course, you will build on your knowledge and professional experience with computer hardware, operating systems, and networks as you acquire the specific skills required to implement basic security services on any type of computer network.
When you're through, you'll have a comprehensive, roadmap understanding of the network security architecture techniques and tactics that will take your organization into the future… safely.

Class Fee:	$3,490
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab grading:
Pass = Attendance + Labs and Quizzes Fail > 95% Attendance
This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in face to face classes. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

Who Should Attend

IT professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as NetWare, Macintosh, UNIX/Linux, and OS/2, who wants to: further a career in Information Technology by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ examination;
Network Security Administrators, Security Personnel, Auditors, and Consultants concerned with network security, and Consultants, as well as others seeking to tie together their organization's discreet tactical advanced security solutions into a strategic information security framework.
KU Outcomes

* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements
Text Materials: quiz labs, SU free Practice tests and resources. Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Learning Objectives -

Tips for taking the exam & SU Pre-class Study Techniques
1.0 Security Governance, Risk, and Compliance (Risk Management) 21%
2.0 jjj Threats, Attacks and Vulnerabilities 18%
3.0 Architecture and Design 21%
4.0 Identity and Access Management 16%
5.0 Cryptography and Public Key Infrastructure (PKI) 13%
6.0 Cyber Security Technologies and Tools 11%
Note: Further information about the exam (e.g., # of questions, time, scoring) is included at the end of this document.
CompTIA Security+ Certification SY0-601 provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security.

In our Instructor Led Security+ Course, you will learn to:
Proactively implement sound security protocols to mitigate security risks

Quickly respond to security issues
Proactively and retroactively identify where security breaches may have occurred

Architect and design a enterprise network, on-site or in the cloud, with security in mind

Lesson Plan

1.0 Security Governance, Risk, and Compliance (Risk Management)

1.1 Cyber Security Concepts

- Confidentiality, integrity, availability
- Business drivers for cyber security: risk, compliance
- Roles in Cyber Security management
- Regulatory compliance overview

1.2 Cyber Security Risk Management Concepts and Processes

- Threat and risk assessment
- Quantitative risk analysis
- Qualitative risk analysis
- Information classification
- Risk response choices
- Change management

1.3 Comparing and Contrasting Cyber Security Controls

- Types of security controls - administrative, technical, physical
- Cyber Security control intent

1.4 Policies, Standards, Procedures, and Administrative Controls for Cyber Security

- General security policies
- Business agreement types
- Continuing education
- Acceptable use policy/rules of behavior

1.5 Data Media Storage Protection, Handling, and Disposal

- Data destruction and media sanitization
- Data sensitivity labeling and handling
- Data retention and disposal policies
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Roles in data management

1.6 Cyber Security Incident Response Procedures

- Incident response planning and management
- Incident response process
- After action report (AAR)

1.7 Fundamentals of Cyber Security Forensics

- Evidence chain of custody
- Evidence acquisition, preservation, and protection
- Order of volatility
- Legal hold

1.8 Measuring Risk through Business Impact Analysis (BIA)

- Threats to business continuity
- Identification of critical systems
- Measurements of downtime/outage impact
- Privacy impact assessment (PIA)
- Privacy threshold assessment (PTA)

1.9 Business Continuity and Disaster Recovery Concepts

- Types of backup – full, incremental, differential
- Methods of backup: removable media, electronic
- Geographic considerations for backups
- Alternate/recovery sites
- Recovery testing

2.0 Cyber Security Threats, Attacks and Vulnerabilities 2.1 Identifying and Characterizing Threat Actors Types of actors

- Attributes of actors

2.2 Types of Cyber Security Attacks

- Malware attacks
- Social engineering
- Application/service attacks
- Hijacking and related attacks
- attacks
- Cryptographic attacks
- Online vs. offline

2.3 Impact Associated with Types of Vulnerabilities

- End-of-life systems
- Embedded systems
- Lack of vendor support
- Race conditions
- Memory leaks
- System sprawl/undocumented assets
- Architecture/design weaknesses
- New threats/zero day
- Improper certificate and key management

2.4 Explaining Vulnerability Scanning and Penetration Testing Concepts

- Vulnerability and penetration testing objectives
- Active and passive reconnaissance
- Intrusive vs. non-intrusive
- Black box/White box/Gray box
- Credentialed vs. non-credentialed
- Target organization reconnaissance
- Network discovery and enumeration
- Port scanning and banner grabbing
- Vulnerability scanning
- Exploit scripts and exploit consoles
- False positives and false negatives
- Reporting results to management

3.0 Architecture and Design

4 hrs Lecture 2 hr Labs

3.1 Using Cyber Security Frameworks and Configuration Baselines

- Benchmarks/secure configuration guides
- Defense-in-depth/layered security

3.2 Implementing Network Cyber Security Architectures

- Zones/topologies
- Network address translation (NAT)/Port address translation (PAT)
- Segregation/segmentation/isolation
- Security device/technology placement
- Software Defined Networking (SDN)

3.3 Implementing Secure Systems Design

- Hardware/firmware security
- Operating systems
- Patch management
- System hardening
- Peripherals

3.4 Deploying Secure Staging Practices and Procedures

- Sandboxing
- Staging environments
- Secure baseline
- Integrity measurement

3.5 Addressing the Security Implications of Embedded Systems

- Supervisory control and data acquisition (SCADA)/Industrial Control System (ICS)
- Smart devices/Internet of Things (IoT)

3.6 Defining Secure Application Design, Development, and Deployment

- System development life-cycle (SDLC) models – waterfalls vs agile
- DevOps (Software Development/Software Operations)
- Secure DevOps (DevSecOps)
- Version control and change management
- Provisioning and deprovisioning
- Secure coding techniques
- Code quality and testing
- Programming model verification - Compiled vs. runtime code

3.7 Virtualization and Cloud Computing Security

- Hypervisors
- Application cells/containers
- Virtual desktop infrastructure (VDI)/Virtual desktop ethernet (VDE)
- Cloud deployment models
- Cloud service models
- Cloud access security broker (CASB)

3.8 Using Resiliency and Automation Strategies to Reduce Risk

- Automation/scripting
- Snapshots
- Savepoints
- Live boot media
- Redundant Array of Independent Disks (RAID)

3.9 Physical and Environmental Security Controls

- Fencing/gates/cages
- Barricades/bollards
- Security guards
- Lighting
- Cameras
- Motion detection
- Signs
- Alarms
- Safe and secure enclosures
- Mantrap
- Airgap
- Faraday cage
- Protected distribution/protected cabling
- Physical access control: Proximity cards, biometric factors, smart cards
- Cable locks
- Logs
- Environmental controls: HVAC, hot and cold aisles, fire suppression

4.0 Identity and Access Management

4.1 Identity and Access Control Management Concepts

- Access control concepts and architecture
- User authentication credentials
- Something you are
- Something you have
- Something you know
- Somewhere you are
- Multifactor authentication / Two-factor authentication (2FA)
- Two-way authentication

4.2 Installing and Configuring Authentication Protocols

- Single Sign-On (SSO): Kerberos, transitive trust,
- Federation: personal, business
- Password authentication protocol (PAP)
- Challenge handshake authentication protocol (CHAP)
- Extensible authentication protocol (EAP)
- Authentication, authorization, and accounting (AAA): RADIUS, TACACS+, Diameter
- IEEE 802.1x
- Lightweight directory access protocol (LDAP)

4.3 Implementing Access Control Management

- Discretionary access control (DAC)
- Attribute-based access control (ABAS)
- Role-based access control
- Rule-based access control
- Mandatory access control (MAC)/Trusted computing system
- File system security
- Database security

4.4 User Account and Identity Management Policies and Administration

- Account types
- Separation of duties
- Least privilege
- Privileged user account controls
- Onboarding/Offboarding
- Permission auditing and review
- Usage auditing and review
- Time-of-day restrictions
- Re-certification
- Account maintenance

- Group-based access control
- Location-based policies

5.0 Cryptography and Public Key Infrastructure (PKI)

4 hrs Lecture 2 hr Labs

5.1 Basic Concepts of Cryptography

- Cryptography concepts and terminology
- Encryption strength/work factor
- Deployment: data-in-transit/data-at-rest/data-in-use
- Session keys
- Secure key exchange
- Ephemeral key
- Perfect forward secrecy
- Digital signatures

5.2 Explaining Cryptography Algorithms and Their Basic Characteristics

- Symmetric algorithms
- Cipher modes
- Asymmetric algorithms
- Hashing algorithms
- Key stretching and salting
- Message authentication codes

5.3 Install and Configure Security Settings

- cryptographic protocols
- Network authentication protocols for applications

5.4 Implement Public Key Infrastructure (PKI)

- Digital certificate components
- Types of certificates
- Certificate assignees
- Certificate formats (file types)
- Chain of trust/Trust anchors
- PKI architecture
- Root authority
- Certificate authorities (CA)
- Registration authorities (RA)
- Validation authorities (VA)
- Certificate revocation lists (CRL)
- Online certificate status protocol (OCSP)

5.5 Steganography

6.0 Cyber Security Technologies and Tools

6.1 Install and Configure Cyber Security Network Components

- Firewalls
- VPN technologies
- Routers
- Switches
- Proxy servers
- Load balancers
- Web security gateways
- Web application firewalls (WAF)
- Data loss prevention (DLP)
- E-mail guards and gateways
- access points (WAP)
- Network Intrusion Detection System (NIDS)/Network Intrusion Prevention System (NIPS)
- Security Information and Event Management (SIEM)
- Encryption devices

6.2 Cyber Security Assessment Tools

- Protocol analyzer
- Network scanners
- Command line tools

6.3 Troubleshooting Cyber Security Scenarios

- Unencrypted credentials/clear text
- Logs and events anomalies
- Permission issues
- Access violations
- Certificate issues
- Data exfiltration
- Misconfigured devices
- Firewalls
- access points
- Weak security configurations
- Personnel issues

6.4 Analyzing and Interpreting Output from Cyber Security Technologies

- HIDS/HIPS
- Antivirus
- File integrity check
- Host-based firewall
- Application whitelisting/blacklisting
- Removable media control
- Advanced malware tools
- Patch management tools
- Unified Threat Management (UTM)
- Data Loss Prevention (DLP)
- Data execution prevention (DEP)
- Web application firewall

6.5 Implementing Secure Communications Protocols

- Secure protocols
- Secure Shell (SSH)
- Secure Socket Layer (SSL)/Transport Layer Security (TLS)
- Voice and video
- Time synchronization
- Email and web
- File transfer
- Directory services
- Remote access
- Domain name resolution/Domain name system (DNS)
- Routing and switching

6.6 Deploying Mobile Device Security

- Connection methods
- Mobile device management concepts
- Enforcement and monitoring
- Deployment models

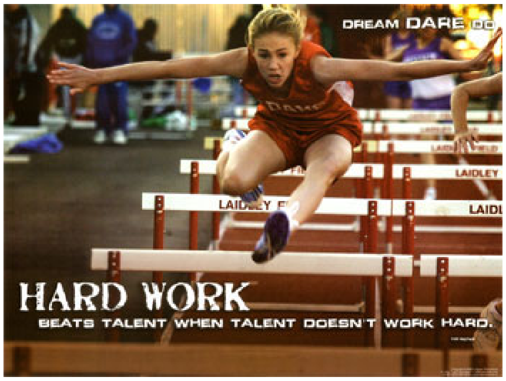
Exam Version: CompTIA Security+ SY0-601
Exam Fee: $495 per exam attempt
Exam Location: You can take the exam on site last day of class - we are a mobile testing site

Time Allocated: 90 minutes per exam Exam Score Range: Scores range from 100-900 , Minimum Pass Score: 750
Number Of Questions: Not more than 90 questions per exam (usually 60-75 in recent months)
Exam format: Linear format; computer-based test (CBT) - multiple choice, multiple answer, performance-based
Prerequisites: You should have a basic understanding of operating systems and TCP/IP networking similar to that obtained from CompTIA Strata IT Fundamentals and Network+ or equivalent work experience. Network+ and A+ certifications are recommended by CompTIA, but not required Validation Period: Certification expires after 3 years, unless Continuing Professional Education (CPE) requirements and maintenance fees are met - contact www.comptia.org for more details Score Report : Delivered immediate on test completion

Lesson Plan
Access Control - Policies, standards and procedures that define who users are, what they can do, which resources they can access, and what operations they can perform on a system.
Administration - Identification of information assets and documentation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability.
Audit and Monitoring - Determining system implementation and access in accordance with defined IT criteria. Collecting information for identification of and response to security breaches or events.
Risk, Response and Recovery - The review, analysis and implementation processes essential to the identification, measurement and control of loss associated with uncertain events.
Lesson Plan Day5 7hr lecture 1 hr labs/quizzes
Cryptography - The protection of information using techniques that ensure its integrity, confidentiality, authenticity and non-repudiation, and the recovery of encrypted information in its original form.
Data Communications - The network structure, transmission methods and techniques, transport formats and security measures used to operate both private and public communication networks.
Malicious Code - Countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses and other related forms of intentionally created deviant code.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.



Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

SU CompTIA SECURITYX® (formerly CASP) - CERTIFICATION CLASS W/EXAM

How to plan for network security that matches your technology infrastructure from top to bottom.

SecurityX® (formerly CASP) is CompTIA's first advance-level certification for enterprise technical security leads. SecurityX certification is an international, vendor-neutral certification that designates IT professionals with advanced-level security skills and knowledge. Achieving CASP certification proves your competency in enterprise security, risk management, research and analysis, and integrating computing, communications, and business disciplines. Becoming SecurityX certified confirms that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. SecurityX certifies that you can apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

Secure X is designed for seasoned security specialists whose work deals with the day-to-day operations of an IT environment's security aspects. It takes what you learn in a CompTIA Security+ course and strengthen while reinforcing your expertise in this widely accepted standard for network security professionals. Besides enterprise level security, you will also further develop skills in areas such as research, analysis, and the integration of computing and communications in a business environment. This course is the perfect opportunity for seasoned IT security professionals to hone existing skills and build new ones in a wide range of security-related disciplines that will allow companies to carry on operations in safe and secure environments. As businesses throughout the area and across the world become more connected and more reliant on IT, the need for experts to act as administrators is only going to rise with time.

8570.1 Approved SecurityX certification is included in the approved list of certifications that meet the DoD Directive 8570.1 and 8140 requirements. It is approved as a baseline certification for the IAT Level III, IAM Level II, and IASAE Level I and II.

Class Fee:	$3,990
Time:	Advanced
Learning Level:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Contact Hours:	Understanding of TCP/IP Protocols
Prerequisites:	72 CPE / 3 CEU
Credits:	
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs and quizzes Fail > 95% Attendance

Sample Job Title
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/ Network Analyst
Network Security Engineer /Network Security Specialist
Security Analyst/ Security Engineer
Security Specialist/ Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend

Individuals seeking the CompTIA SecurityX® (formerly CASP) certification (Exam CAS-002) IT professionals with a minimum of 10 years of experience in IT administration and at least five years of hands-on security in an enterprise environment. Enterprise Network Defense (END) Infrastructure Support - Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources. Monitors the network to actively remediate unauthorized activities.

Text Materials: quiz labs, SU free Practice tests and resources.
Machines a Dual Core 1G RamM, 1 Gig drives, running MS OS, linux, and VMWare Workstation

KU Outcomes
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

What You'll Learn

- Manage risk in the enterprise
- Integrate computing, communications, and business disciplines in the enterprise
- Use research and analysis to secure the enterprise
- Integrate advanced authentication and authorization techniques

- Implement cryptographic techniques
- Implement security controls for hosts
- Implement security controls for storage
- Analyze network security concepts, components, and architectures, and implement controls
- Implement security controls for applications
- Integrate hosts, storage, networks, and applications in a secure enterprise architecture
- Conduct vulnerability assessments
- Conduct incident and emergency responses

CompTIA SecurityX® (formerly CASP) Course Outline
Domain 1 Risk Management and Incident Response
Lesson 1A: Information Security Concepts and Terminology
Lesson 1B:Risks Associated with Business and Industry Influences;
Lesson 1C:Risk Mitigation Planning, Strategies, and Controls;
Lesson 1D:Security and Privacy Policies, Standards, and Procedures;
Lesson 1E:Incident Response and Recovery Procedures

Domain 2 Enterprise Security
Lesson 2A: Cryptographic TConcepts Techniques
Lesson 2B: Host and Storage Security controls;
Lesson 2C: Application Security;
Lesson 2D: Network Security Components

Domain 3 Technical Integration of Enterprise Components
Lesson 3A: Enterprise Storage Security Integration of Hosts, Storage, Networks, and Applications
Lesson 3B: Integration of Advanced Authentication and Authorization Technologies

Domain 4 Integration of Computing, Communications, and Business Disciplines
Lesson 4A: Facilitation of Collaboration Across Business Units to Achieve Security Goals
Lesson 4B: Selection of Controls to Secure Communications and Collaboration
Lesson 4C: Designing and Implementing Security Activities Across the Technology Life Cycle

Domain 5 Research, Analysis, & Assessment
Lesson 5A: Research Methods to Determine Industry Trends and Impact to the Enterprise
Lesson 5B: Analyze Scenarios to Secure the Enterprise
Lesson 5c: Methods and Tools to Conduct Security Assessments

Why get Secure X Certified?

Getting your Secure X certification will ensure that your services will always be in demand, no matter where you go

1. Managing Risk
Identify the Importance of Risk Management
Assess Risk
Mitigate Risk
Integrate Documentation into Risk Management

2. Integrating Computing, Communications, and Business Disciplines
Facilitate Collaboration across Business Units
Secure Communications and Collaboration Solutions
Implement Security Activities throughout the Technology Life Cycle

3. Using Research and Analysis to Secure the Enterprise
Determine Industry Trends and Effects on the Enterprise
Analyze Scenarios to Secure the Enterprise

4. Integrating Advanced Authentication and Authorization Techniques
Implement Authentication and Authorization Technologies
Implement Advanced Identity Management

5. Implementing Cryptographic Techniques
Describe Cryptographic Concepts
Choose Cryptographic Techniques
Choose Cryptographic Implementations

6. Implementing Security Controls for Hosts
  Select Host Hardware and Software
  Harden Hosts
  Virtualize Servers and Desktops
  Implement Cloud Augmented Security Services
  Protect Boot Loaders

7. Implementing Security Controls for Enterprise Storage
  Identify Storage Types and Protocols
  Implement Secure Storage Controls

8. Analyzing and Implementing Network Security
  Analyze Network Security Components and Devices
  Analyze Network-Enabled Devices
  Analyze Advanced Network Design
  Configure Controls for Network Security

9. Implementing Security Controls for Applications
  Identify General Application Vulnerabilities
  Identify Web Application Vulnerabilities
  Implement Application Security Controls

10. Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture
  Implement Security Standards in the Enterprise
  Select Technical Deployment Models
  Secure the Design of the Enterprise Infrastructure
  Secure Enterprise Application Integration Enablers

11. Conducting Vulnerability Assessments
  Select Vulnerability Assessment Methods
  Select Vulnerability Assessment Tools

12. Responding to and Recovering from Incidents
  Design Systems to Facilitate Incident Response
  Conduct Incident and Emergency Responses

Classroom Labs
  Lab 1: Integrate Documentation into Risk Management 1hr
  Lab 2: Secure Communications and Collaboration Solutions 1hr
  Lab 3: Analyze Scenarios to Secure the Enterprise .5hr
  Lab 4: Implement Authentication and Authorization Technologies .5hr
  Lab 5; Choose Cryptographic Techniques .5hr
  Lab 6: Harden Hosts .5hr
  Lab 7: Virtualize Servers and Desktops .5hr
  Lab 8: Protect Boot Loaders .5hr
  Lab 9: Implement Secure Storage Controls .5hr
  Lab 10: Configure Controls for Network Security .5hr
  Lab 11: Implement Application Security Controls 1hr
  Lab 12: Select Vulnerability Assessment Tools 1hr
  Lab 13 Design Systems to Facilitate Incident Response 1hr
  Lab 14: Conduct Incident and Emergency Response 1hr

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. **Books** – Ebooks are provided for this course. No external books are required.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Q/AAP QUALIFIED/ ACCESS, AUTHENTICATION & PKI PROFESSIONAL W/EXAM

Access, Authentication, Identity and PKI methods and processes to raise the level of information security to make your network infrastructure more secure. Web and other forms of E-Commerce introduce a whole new group of information security challenges. Traditional password authentication, access controls and network perimeter security safeguards fall short. Data traveling over untrusted networks must be protected by encryption methods that are highly dependent on flexible and robust key management schemes. This 40 hr 1 wk + 32 hr hands-on class, teaches you how to plan, evaluate, develop, and implement a successful enterprise network security framework using Public Key Infrastructure (PKI), authentication, identity, and access authorization systems. You will install multiple certification authorities, various smart cards, tokens and biometrics that will raise the level of information security in your organization. Upon completion of the course, you'll have all the experience, confidence, and tools you need to plan Certificate Policy & Certificate Practice Statements and execute a fully integrated PKI. Note: **This class is intended to be a practical product design/integration course & does not cover encryption mathematics.**

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance +Labs& Quizzes Fail > 95% Attendance
Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts
Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation

Sample Job Titles
Computer Network Defense (CND) Analyst (Cryptologic)
Cybersecurity Intelligence Analyst
Enterprise Network Defense (END) Analyst
Focused Operations Analyst
Incident Analyst/Network Defense
Technician/ Network Security Engineer
Security Analyst/ Security Operator
Sensor Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Risk Management - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to ensure new and existing information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and monitoring assurance from internal and external perspectives.
Learning Objectives
Install 7 different encryption keys - individual and enterprise. Share keys, secure repudiation.
Stand up with policy multiple certificate authorities. HSPD-12 tools– In an effort to better secure federal resources and reduce the potential for terrorist attacks, Homeland Security Presidential Directive 12 (HSPD-12)
The goal of HSPD-12 is to require federal agencies to adopt a standard, secure, and reliable identification card (the "PIV card") for employees and contractors – and to ensure that it's only issued only to intended individuals. student is able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline.

* Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security.
* Students will be able to examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.

Learning Objectives

- Defending your electronic assets from hackers
- Encryption & Identity Mgt tools
- Security design and control methods
- Return on investment strategies and methods
- How to plan & Implement a PKI
* Threats and Adversaries
* Vulnerabilities and Risks
* Basic Risk Assessment
* Security Life-Cycle
* Intrusion Detection and Prevention Systems
* Cryptography
* Data Security (in transmission, at rest, in processing)
* Security Models
* Access Control Models (MAC, DAC, RBAC)
* Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation,
Privacy* Security Mechanisms & I &A Audit

Who Should Attend:

Information Technology and Information Security Architects, Information Security Officers and Managers, Network and System Engineers, Consultants, Information Security Analysts, Information Technology Auditors, E-Commerce Application Developers and Integrators, and enterprise network security solutions.

Lesson Plan:

1. **Cryptography Refresher: concepts, algorithms, key management Lecture labs**
2. **Public Key Infrastructure (PKI) Lecture labs**
3. **Network Security Refresher**
   - Network Defense and Countermeasure
   - Penetration Testing
   - Transmission Security
   - Security Roles and Responsibilities

4. **Digital Certificates and Digital Signatures Lecture labs**
   - Defining the role of digital certificates
   - Analysis of digital certificate structures
   - Defining the difference between digital signatures vs. digital certificates
   - Digital signatures: definitions and applications
   - Security services provided through the use of digital certificates and digital signatures: authentication, access control, integrity, non-repudiation
   - Hands-on exercises: encryption and digital signing

5. **Certification Authorities and Directory Services Lecture labs**
   - Roles and responsibilities of Certificate Authorities (CAs)
   - Registration and certification process
   - Certificate management: singular and multiple CA environments
   - Certificate value and verification criteria
   - Cross certification
   - Key recovery
   - Defining enterprise directory services
   - Integrating PKI with directory services and security systems
   - Hands-on exercises: installing a certificate server and using digital certificates for sample security applications

6. **PKI Product Comparisons and Demonstrations Lecture labs**
   - Developing and prioritizing a PKI criteria shopping list
   - Comparison matrix
   - Middleware products
   - Multiple product demos
   - Outsourcing CA hosting
   - Hands-on exercises: installing and implementing a PKI system (multiple products including: NETSCAPE, SYPRUS, Entrust, Baltimore, RSA XCERT)

7. **Sorting out Different User Authentication Mechanisms Lecture labs**
   - Pitfalls of remembered password systems
   - Encryption: Digital certificates and digital signatures
   - Smart cards
   - Tokens
   - Biometrics
   - Combing authentication mechanisms for multi-factor authentication
   - Hands-on exercises: using smart cards and biometric authentication tools

8. **Overcoming Pitfalls in Encryption and Certificate Management Lecture labs**
   - Avoiding common pitfalls in the use of encryption and PKI

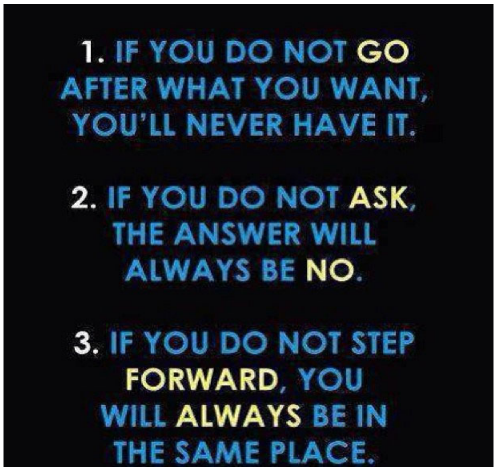
- How to avoid underestimating the complexity of a PKI rollout
- Challenges associated with encryption
- Key management
- Case Studies: An examination of how PKI and CAs have been used in real organizations

8. Deploying a PKI Lecture labs

- Defining the deployment model:
- Deployment success factors
- Identifying and overcoming both technology and non-technology challenges
- Determining the deployment approach
- Building a PKI deployment team
- Selecting deployment tools
- Case Study/Team Exercises: Creating a PKI Framework

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to the outcome on Friday of class. The course is graded as a pass or fail solely on your attendance and participation in quizzes, labs other assessed activities. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CoM / non degree
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification w/exam
Q/CA CMMC Cyber Security Maturity Model Certification class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU Secure X®-[formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum
PMP Project Manager Professional Certification Class*
Q/ISO Qualified/ Chief Information Security Officer Certification Class w/exam



1. IF YOU DO NOT GO AFTER WHAT YOU WANT, YOU'LL NEVER HAVE IT.

2. IF YOU DO NOT ASK, THE ANSWER WILL ALWAYS BE NO.

3. IF YOU DO NOT STEP FORWARD, YOU WILL ALWAYS BE IN THE SAME PLACE.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Q/NSP QUALIFIED/ NETWORK SECURIT POLICY ADMINISTRATOR & SOA SECURITY SERVICES ORIENTED ARCHITECT W/ EXAM

How to develop and implement security technologies, policies & strategies your organization needs to raise your level of information security and assurance.

This 72 hour class provides a step by step way to take separate, diverse parts of your security technologies e.g., vulnerability penetration testing, anti-virus and incident response, certificates and network identity, firewalls, IDS (intrusion detection systems) and Forensics' investigations together into a cohesive and effective security policy and awareness program. Learn how to build a program to reduce the Human Security gap in your company. Today's security policies need to build awareness of the potential problems while minimizing the cost of security incidents. Only if policies are well developed and accepted can you raise the level of information security awareness in your enterprise.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs Fail > 95% Attendance

Sample Job Titles
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Command Information Officer
Information Security Policy Analyst
Information Security Policy Manager
Policy Writer and Strategist

Who Should Attend

Strategic Planning and Policy Development - Applies technical and organizational knowledge to define an entity's strategic direction, determine resource allocations, establish priorities, and identify programs or infrastructure required to achieve desired goals. Develops policy or advocates for policy change that will support new initiatives or required changes and enhancements.

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: labs, resource CD's and attack handouts. Machines a Dual Core 24M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation. KU outcomes:

* Students shall be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. * Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities.* Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.

Learning Objectives: After completing the polices it's time to bring the whole network together and deliver a secure infrastructure. You'll merge today's security technologies into your network with the assurance that your layering defense tactics and providing early warning systems. Bring together the separate, tactical, diverse parts of your network with the services, mechanisms, and objects that reflect security policies, business functions, and technologies into a process involving risk assessment, policy, awareness, technology and security management, and audit functions. Building a security architecture involves close examination of current business processes, technical capability, information security documentation, and existing risk. Students will leave this class with a document template outlining a best practice for an information security architecture framework. When you're through, you'll have a comprehensive, roadmap understanding of the network security architecture.

Lecture labs

1. Establishing the Basics

- Defining policies, standards, and procedures
- Managing an information security program
- Determining organizational needs
- Government and commercial publications available
- Organizing the process
- Creating workable information security policies
- ROI and policies
- Baseline assessments

2. Beyond the Basics: Real Life

- Policies, procedures, and standards in a changing environment
- Systems audit and event monitoring
- Data availability, integrity, and confidentiality
- Incident escalation and response
- Operations, administration, and maintenance security
- Application development and integration security
- Continuity and recovery planning
- Coordinate with/advise management

3. Building the Plan

- Information collection and amalgamation
- Baseline assessments
- Conducting reviews of existing infrastructure and processes
- Performing gap analysis and risk assessments
- Understanding synergistic relationships — policy, procedures, standards, and guidelines
- Creating the architecture framework designs — logical, physical, process flow
- Creating an integration roadmap — budgets, scheduling
    - Creating the Security Policies and Procedures Manual (SPPM)
    - Creating the Security Administrator Manual (SAM) requirements outline
    - Applying the principles: creating policy teams, writing and testing the policies, standards, and procedures
    - Management approval process

3. Advanced Awareness Programs

- Awareness, training, and the difference between them
- Getting the word out
- Changing behavior
- Finding allies
- Monitoring and maintaining the program

In-Class Exercises

- Defining the enterprise environment
- Determining organizational policy needs
- Creating organizational policies
- Security policies, standards, and procedures in a changing environment
- Developing an Advanced Awareness Program

Lecture Labs

1. Security Architecture Component Review

- Defining an information security architecture
- Critical information security domains
- Determining your organizational needs
- People, policy, process, and technology
- Component dependencies
- Information security program layers
- Technical architecture models
- Database Security

2. Advanced Security Architecture Discussion

- Awareness and training
- Governance, compliance, and audit
- Perimeter protection and countermeasures
- Authentication, authorization, and accounting

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. A practicum provides adequate evidence to support the claim of knowing something. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CoM
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA CMMC Cyber Security Maturity Model Certification class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX®- [formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Q/CA® CMMC CYBER SECURITY MATURITY MODEL CERTIFICATION CLASS W/ EXAM
Formerly RMF - Qualified/ Certification and Accreditation Administration Certification Class w/exam

This class is designed for key personnel responsible for the management and implementation of the NIST SP800-37 CMMC formerly the Certification and Accreditation process. This course will provide a historical reference to all relevant legislation and guidance. In addition, interactive workshops during the course will engage students to directly participation, thus ensuring a higher degree of retention and focus. Hands On *Note*: This class can be easily tailored to meet the certification and accreditation needs of any organization.

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/Network Analyst
Network Security Engineer/ Network Security Specialist/ Security Analyst
Security Engineer/ Security Specialist
Systems Security Engineer

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry to Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU 4012, 4015, 4016A
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practium Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend *Enterprise Network Defense (END) Infrastructure Support - Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources. Monitors the network to actively remediate unauthorized activities.* DoD Information Security and IT managers; Information Assurance Officers and Managers; Information Security Analysts, Consultants and Contractors; Security and Certification Officials responsible for developing C&A packages
Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
KU outcomes:
Students will be able to describe the DoD system certification and accreditation processes.
Students will be able to define certification and accreditation.

Mananagement, Program Implementation and Documenting Mission Needs.

•Analyzing, Assessing, Measuring, Managing and Mitigating IS Threats, Vulnerabilities and Associated Risks.
•Legal Issues, Intrusion Forensics and Incident Response, Intrusion Prevention, Detection, Response, Recovery & Reporting.
•Physical, System, Data Access Control.
•Life-Cycle Security & Life-Cycle Management in Defending the Information Environment (Information Operations).
•Configuration Management, Consequence Management, Contingency and Disaster Recovery Planning (BCP)).
•Certification, Evaluation and Network Security Certification and Accreditation (C&A).
•System Certification Requirements including Policies, Processes, Procedures and Protocols.
•Fundamentals of Threat/ Vulnerability Analysis and Risk Management
•Countermeasure IS and Assessment
•Certification and Accreditation of systems
•Testing And Evaluation

The following outlines the scope and objectives for *SU's Certification and Accreditation Workshop.*

Business Needs / Course Goals for C&A 1 hrs Lecture 0 hr Labs

Understanding Roles & Responsibilities
Phases 1-4 of C&A
Phases 1-9 of RA
Classification of System
Understanding Legislation
FISMA, SOX 404, HIPAA
Understanding C&A in Lifecycle

Development phase to RA and C&A
Identifying Risk Assessment in C&A
Boundary Accreditation in a system environment
Identifying a system boundary
Accreditation Decision Model
Communicate what transpires in delivering a decision; IATO, Full Accreditation, Do Not Accredit
FISMA Scorecard
Positive and negative impacts
17 Baseline Management, Operational, & Technical Policies
Understanding policy source, relationships, procedures, controls, and testing

Levels of Certification and Starting the Review

At the beginning of a C&A project, the C&A team determines the impact of a loss of confidentiality, Integrity, or availability of the system, based on this impact level and guidance in the following documents, the C&A package is built.
•FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
•Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf Volume I
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf Volume II

The outcome of the C&A process is to put together a collection of documents that describe the security posture of the systems, an evaluation of the risks, and recommendations for correcting deficiencies. It is what's known as a Certification Package. A typical Certification Package usually consists of a minimum of half a dozen documents, though more documentation may be required if the systems contain classified information or highly sensitive data. Each agency is responsible for defining their own C&A process and it must be well-documented in the form of a Handbook. The C&A Handbook is based on one of the three well-known methodologies (NIST, DITSCAP, or NIACAP) with various customizations that are unique for each particular agency. Preparing the C&A package is sometimes referred to as a C&A Review.

Once a Certification Package has been prepared, Mission Assurance auditors review the package and then make decisions on whether or not the systems should be accredited according to the proposed recommendation. All federal agencies must obtain an Authority to Operation (ATO) before their systems can be legitimately and legally used for production purposes.

If the Certification Package does not appear to contain the right information, or if the information reported in the package is considered unacceptable (for example, if there are unacceptable risks cited with inappropriate safeguards to mitigate the risks) the agency may be given an Interim Authority to Operation (IATO), which allows them to operate their systems for usually three months while they correct their deficiencies.

What You Will Learn
The Q/CA RMF examination tests the breadth and depth of a candidate's knowledge by focusing on the seven domains which comprise the Q/CA RMF exam and be prepared for the CAP CBK®, taxonomy of information security topics:
Understanding the Security Authorization of Information Systems
Categorize Information Systems
Establish the Security Control Baseline
Apply Security Controls
Assess Security Controls
Authorize Information System
Monitor Security Controls

The ideal candidate should have experience, skills or knowledge in any of the following areas:
IT Security
Information Assurance
Information Risk Management
Certification
Systems Administration
One - two years of general technical experience
Two years of general systems experience
One - two years of database/systems development/network experience
Information Security Policy

Technical or auditing experience within government, DoD the financial or health care industries, and/or auditing firms
Strong familiarity with NIST documentation

Upon the completion of our Q/CA Course, students will know how to: The goal of the course is to prepare professionals for the challenges of authorization and accreditation concepts and functions. Our program will provide you with a quick and proven method for mastering this huge range of knowledge. Depending on the requirements of the particular agency, other documents or variations of these particular documents may also be required. NIST publishes an excellent collection of documents that provide guidance for the C&A review that will explain what sort of information should be reported in each of the required documents.

Lesson Plan
Domain 1: Describe the Risk Management Framework (RMF)

Module 1: Domain Introduction
Module 2: Domain Terminology and References
Module 3: Historical and Current Perspective of Authorization
Module 4: Introducing the Examples Systems
Module 5: Introduction to the Risk Management Framework (RMF)
Module 6: The RMF Roles and Responsibilities
Module 7: The RMF Relationship to Other Processes
Module 8: Example System Considerations
Module 9: End of Domain Review and Questions

Domain 2: RMF Step 1: Categorize Information Systems

Module 1: Domain Introduction
Module 2: Domain Terminology and References
Module 3: RMF Step 1 - Roles and Responsibilities
Module 4: Preparing to Categorize an Information System
Module 5: Categorize the Information System
Module 6: Categorizing the Examples System
Module 7: Describe the Information System and Authorization Boundary
Module 8: Register the Information System
Module 9: RMF Step 1 Milestones, Key Activities and Dependencies
Module 10: End of Domain Review and Questions

Domain 3: RMF Step 2: Select Security Controls

Module 1: Domain Introduction
Module 2: Domain Terminology and References
Module 3: RMF Step 2 - Roles and Responsibilities
Module 4: Understanding FIPS 200
Module 5: Introducing SP 800-53
Module 6: The Fundamentals
Module 7: The Process
Module 8: Appendix D - Security Control Baselines
Module 9: Appendix E - Assurance and Trustworthiness
Module 10: Appendix F - Security Control Catalog
Module 11: Appendix G - Information Security Programs
Module 12: Appendix H - International Information Security Standards
Module 13: Appendix I - Overlay Template
Module 14: Appendix J - Privacy Control Catalog
Module 15: Identify and Document Common (Inherited) Controls
Module 16: System Specific Security Controls
Module 17: Continuous Monitoring Strategy
Module 18: Review and Approve Security Plan
Module 19: RMF Step 2 Milestone Checkpoint
Module 20: Example Information Systems
Module 21: End of Domain Review and Questions

Domain 4 - RMF Step 3: Implement Security

Module 1: Domain Introduction
Module 2: Domain Terminology and References
Module 3: RMF Step 3 - Roles and Responsibilities
Module 4: Implement Selected Security Controls
Module 5: Contingency Planning
Module 6: Configuration, Patch and Vulnerability Management
Module 7: Firewalls and Firewall Policy Controls
Module 8: Interconnecting Information Technology Systems
Module 9: Computer Security Incident Handling
Module 10: Security Awareness and Training
Module 11: Security Considerations in the SDLC
Module 12: Malware Incident Prevention and Handling
Module 13: Computer Security Log Management
Module 14: Protecting Confidentiality of Personal Identifiable Information
Module 15: Continuous Monitoring
Module 16: Security Control Implementation
Module 17: Document Security Control Implementation
Module 18: RMF Step 3 Milestone Checkpoint
Module 19: End of Domain Review and Questions

Domain 5 - RMF Step 4: Assess Security Control

Module 1: Domain Introduction
Module 2: Domain Terminology and References
Module 3: RMF Step 4 - Roles and Responsibilities
Module 4: Understanding SP 800-115
Module 5: Understanding SP 800-53A
Module 6: Prepare for Security Control Assessment
Module 7: Develop Security Control Assessment Plan
Module 8: Assess Security Control Effectiveness
Module 9: Develop Initial Security Assessment Report (SAR)
Module 10: Review Interim SAR and Perform Initial Remediation Actions
Module 11: Develop Final SAR and Optional Addendums
Module 12: RMF Step 4 Milestone Checkpoint
Module 13: End of Domain Review and Questions

Domain 6 - RMF Step 5: Authorize Information System

Module 1: Domain Introduction

Module 2: Domain Terminology and References
Module 3: RMF Step 5 - Roles and Responsibilities
Module 4: Develop Plan of Action and Milestones (POAM)
Module 5: Assemble Security Authorization Package
Module 6: Determine Risk
Module 7: Determine the Acceptability of Risk
Module 8: Obtain Security Authorization Decision
Module 9: RMF Step 5 Milestone Checkpoint
Module 10: End of Domain Review and Questions

Domain 7 - RMF Step 6: Monitor Security Controls

Module 1: Introduction
Module 2: Domain Terminology and References
Module 3: RMF Step 6 - Roles and Responsibilities
Module 4: Understanding SP 800-137
Module 5: Determine Security Impact of Changes to System and Environment
Module 6: Perform Ongoing Security Control Assessment
Module 7: Conduct Ongoing Remediation Actions
Module 8: Update Key Documentation
Module 9: Perform Periodic Security Status Reporting
Module 10: Perform Ongoing Determination and Acceptance
Module 11: Decommission and Remove System
Module 12: RMF Step 6 Milestone Checkpoint
Module 13: End of Domain Review and Questions

The Q/CA practicum measures of the knowledge, skills and abilities required for C&A personnel. In particular, this measures knowledge to setup the formal processes used to assess risk and establish security requirements based on regulatory standards. It's a very important job which ensures that information systems have appropriate security controls to mitigate potential risk, as well as protecting against damage to assets or individuals. Civilians, state and local governments, as well as

To qualify for the Q/CA® credential, a candidate must: The Q/CA candidate must have a minimum of two years of direct full-time security professional work experience in CMMC, Certification and Accreditation of systems. Valid professional experience includes the direct application of appropriate certification and accreditation, knowledge in certification and accreditation related work performed as a practitioner, auditor, consultant, vendor, investigator or instructor.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step. **Books** - No books are required for this course. However, you may want to supplement your preparation for class.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
ISC^2 CISSP® CERTIFICATION CLASS (The Official SU CISSP Training)

SU ISC2 CISSP Certified Information System Security Professional Certification Class w/exam

SU provides comprehensive CISSP class materials for your students, not only helping students achieve certification, but teaching them the complex concepts embodied in the CBK and hands-on labs. Students will learn the contents & concepts of the diverse 10 domains essential elements necessary for thorough security today and how they should work together to provide true in-depth

Class Fee:	$3,990* (+ $799 exam fee excluded)
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	register at Pearson Vue Testing Center
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practicum for CPoM

Fail > 95% Attendance

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider/ Cybersecurity Officer
Enterprise Security Officer /Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect/ Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face-to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: SU CISSP Class handbook, labs, online quizzes SU resource CD's and 500 exam questions.
No tools for this class, students bring on their own laptop machines with www.freepractice test.com and exam force pre installed.
Security Program Management - Oversees and manages information security program implementation within the organization or other area of responsibility. Manages strategy, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and/ or other resources.

KU outcomes:
Students will be able to describe the DoD system certification and accreditation processes.
Students will be able to define certification and accreditation.

Your learning Objectives are: Lesson Plan 1-5

Objectives

Domain 1 Security& Risk

Governance and Organizational Roles
Laws, Regulations, and Compliance
Professional Ethics
Risk Management and Analysis – Threats, Risks, and Countermeasures
Business Continuity Planning – Business Impact Analysis
Information Security Policies, Standards, Procedures, Baselines, and Guidelines
Security Awareness, Training, and Education

Domain 2 - **Asset Security**

- Information Classification and Ownership
  Information Security Controls
  Information Security and Audit Frameworks
  Protection of Privacy
  Data Marking, Handling, Retention, and Disposal

Domain 3 – Identity and Access Management

- Access Control Concepts
  User Identification, Authentication, and Session Protection
  Single/Reduced Sign-on and Federation
  Information Access Control Authorization Systems
  Directory Management of Identity and Access Control Information
  Attacks on Access Controls
  Access Control Management

Domain 4 – Security Engineering

- **Security Engineering – Architecture:**

  Security Design and Capabilities
  Information Security Models
  Security Evaluation Models (Criteria)

- **Security Engineering – Distributed Computing:**

- Client/Server
  Web Application Security
  Database Security
  Virtualization Security
  Cloud Computing Security
  Mobile Device Security

- **Security Engineering – Cryptography:**

  - Cryptography Methods and Algorithms
    Public Key Infrastructure
    Security Engineering - Physical Security:
    Facilities Protection and Access Control
    Environmental Safeguards

Domain 5 – Communication and Network Security

- Fundamental Network Concepts and Architectures
  Network Device Management and Security
  Network User Authentication
  Network Perimeter Security
  Securing Communications Channels
  Network Security
  Voice Communications Security
  Network Attack Identification and Mitigation

Domain 6 – Software Development Security

- Software Lifecycle Development Methodologies
  Security in Software Design and Testing
  Software Change Control and Configuration Management
  Security Considerations for Commercial Off-The-Shelf Software
  Artificial Intelligence

Domain 7 – Security Operations

- **Security Operations – General:**

  - Operations and Administrative Controls
    Change and Configuration Management
    Operating and Maintaining Preventive Measures
    Patch and Vulnerability Management

- **Security Operations – Incident Management:**

  - Incident Response
    Understanding and Supporting Investigations
    Event Logging and Monitoring Activities

- **Security Operations – Business Continuity:**

  - Backup and Fault Tolerance
    Business Continuity and Disaster Recovery

Domain 8 – Security Assessment and Testing

- Security Assessment and Testing Strategies
  Conducting Security Control Testing
  Collecting and Analyzing Security Process Data
  Conducting or Facilitating Independent Security Audits

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SSCP® SYSTEMS SECURITY CERTIFIED PRACTITIONER

This class, Systems Security Certified Practitioner (SSCP®) credential offers information security tacticians, with implementation orientations, the opportunity to demonstrate their level of competence with the seven domains of the compendium of best practices for information security, the (ISC)^2 SSCP CBK®.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	Testing located at Pearson Vue Testing Center
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading: Pass Attendance, Completion of Labs & quizzes Fail > 95% Attendance	

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider
Cybersecurity Officer/Enterprise Security Officer
Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect /Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer.

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

The SSCP credential is ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators.

KU outcomes:
Students will be able to describe the DoD system certification and accreditation processes.
Students will be able to define certification and accreditation.

Learning Objectives.
The curriculum for the SSCP seminar is under continuous review, ensuring current information relevant to the seven CBK domains below. For additional details on the CBK, download a copy of the free SSCP Study Guide. Security Program Management - Oversees and manages information security program implementation within the organization or other area of responsibility. Manages strategy, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and/or other resources.

40 hrs lecture and labs

Lesson Plan 1 Access Control - Policies, standards and procedures that define who users are, what they can do, which resources they can access, and what operations they can perform on a system.
Lesson Plan 2 Administration - Identification of information assets and documentation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability.
Lesson Plan 3 Audit and Monitoring - Determining system implementation and access in accordance with defined IT criteria. Collecting information for identification of and response to security breaches or events.
Lesson Plan 4 Risk, Response and Recovery - The review, analysis and implementation processes essential to the identification, measurement and control of loss associated with uncertain events.
Lesson Plan 5 Cryptography - The protection of information using techniques that ensure its integrity, confidentiality, authenticity and non-repudiation, and the recovery of encrypted information in its original form.
Lesson Plan 6 Data Communications - The network structure, transmission methods and techniques, transport formats and security measures used to operate both private and public communication networks.
Lesson Plan 7 Malicious Code - Countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses and other related forms of intentionally created deviant code. 3 hour exam

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.
Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

ISSEP Certification Training Class

ISSEP® INFORMATION SYSTEMS SECURITY ENGINEERING PROFESSIONAL

Getting ISSEP certified with SU shows your Qualified.

During our 72 hour Official Information Systems Security Engineering Professional (ISSEP) training, students will live, learn, and take the exams at one of our state-of-the-art education centers. This blended-learning course employs outcome-based (Lecture | Lab) delivery that focuses on preparing you with the real-world skills required to pass the certification exams (and to hit the ground running in your career). The ISSEP Certification Class focuses on the technical knowledge required of government information systems security engineers such as ISSE processes and government regulations

We send you the Official ISC2 Guide to the CISSP-ISSEP Prep Book as soon as you register for our class.
All Student's will receive the following:
Four full days of the top ISSEP® training in the industry
Instruction by a high level security expert
ISSEP® Courseware developed & updated on a continual basis to map to the current
ISSEP® exam objectives / ISSEP CBK - sent out upon registration / Practice Questions & Quizzes /Full practice test
Opportunity to come back to attend another ISSEP® class up to one year

*All ISSEP training sessions are taught by a certified ISSEP.

Class Fee:	$3,990
Time:	40hrs
Learning Level:	Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance, Labs and quizzes Fail > 95% Attendance

Sample Job Title
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/ Network Analyst
Network Security Engineer/ Network Security Specialist / Security Analyst
Security Engineer/ Security Specialist
Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Steps to ISSEP® Certification - Enterprise Network Defense (END) Infrastructure Support - Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources. Monitors the network to actively remediate unauthorized activities

- ○ Register for a Test Pass Academy ISSEP 72 hour class
- ○ Read over the ISSEP Prep Book before class
- ○ Register / Pay for the ISSEP exam
- ○ Attend all 72 hours of training
- ○ Take the ISSEP exam shortly after the end of training
- ○ Pass the ISSEP exam!!

ISSEP Exam Prep Daily lesson

Student has previously completed 32 hours of Hybrid lessons

- **Lesson 1 -** Domain 4: U.S. Government Information Assurance Regulations
- **Lesson 2** - Domain 1: Systems Security Engineering
- **Lesson 3 -** Domain 2: Certification & Accreditation
- **Lesson 4 -** Domain 3: Technical Management
- **Lesson 5** Module A Systems Security Engineering Module B Technical Management Module C Certification and Accreditation Module D United States Government Information Assurance (IA) Regulations

Topics	Upon completion of this module, the ISSEP student will be able to employ Information Assurance Technical Framework (IATF) processes to discover users' information protection needs and design systems that will effectively and efficiently address those needs. In addition, the ISSEP student will understand the concepts of defense in depth, risk assessment, and the systems lifecycle.
Topics	Upon completion of this module, the ISSEP student will be able to describe system development models and relate security tasks to these models.
Topics	Upon completion of this module, the ISSEP student will be able to identify, understand, and implement the Certification and Accreditation (C+A) processes.
Topics	Upon completion of this module, the ISSEP student will be able to identify, understand and apply the practices as defined by the United States Government Information Assurance regulations.
Exam	Exam ISSEP certification

Prerequisites for the ISSEP from (ISC)2®

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

SU CISA® CERTIFIED INFORMATION AUDITOR CERTIFICATION CLASS W/EXAM

Class Fee: $3,990 (+ $899 exam fee excluded)
Time: 72 hrs
Learning Level: Basic
Contact Hours: 40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites: Understanding of TCP/IP
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance +labs & quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

System components and determine how they will interact in a composed system.
** Students will be able to analyze a system design and determine if the design will meet the system security requirements*
Learning Objectives:

- ISACA IS Auditing Standards, Guidelines and Procedures and Code of Professional Ethics
- Control objectives and controls related to IS
- CoBit controls
- Procedures used to store, retrieve, transport, and dispose of confidential information assets
- Control Self-Assessment (CSA)
- IS auditing practices and techniques
- IT governance frameworks
- Quality management strategies and policies
- Risk management methodologies and tools
- Use of control frameworks (e.g., CobiT, COSO, ISO 17799)
- Practices for monitoring and reporting of IT performance
- Benefits management practices for CISA Certification
- Processes for managing emergency changes to the production systems
- Use of maturity and process improvement models (e.g., CMM, CobiT)
- Contracting strategies, processes and contract management practices
- Control objectives and techniques that ensure the completeness, accuracy, validity, and authorization of transactions and data within IT systems applications
- Enterprise architecture design related to data, applications, and technology
- Acquisition and contract management processes
- System development methodologies and tools and an understanding of their strengths and weaknesses
- Data conversion tools, techniques, and procedures
- Business Impact Analysis (BIA)
- CISA question and answer review
- CISA Training
- Capacity planning & monitoring techniques for CISA Certification Training

Some of the content in our CISA training class includes: A Training Course
02/13 Ch. 1: The IS Audit Process

- IT Governance
- Systems and Infrastructure Life Cycle Management – Part I
- Systems and Infrastructure Life Cycle Management – Part II
- IT Service Delivery and Support

- Protection of Information Assets – Part I
- Protection of Information Assets – Part II
- Business Continuity
- Information Security Governance (Domain 1)
- Information Risk Management and Compliance (Domain 2)
- Information Security Program Development and Management – Managing and Directing (Domain 3-A)
- Information Security Program Development and Management – Services and Operations (Domain 3-B)
- Information Security Program Development and Management – Information Technology (Domain 3-C)
- Information Security Incident Management (Domain 4)

Module 1—The IS Audit Process-
Information Security Governance (Domain 1)
This module provides a review of the knowledge required of an information systems (IS) audit/assurance professional to ensure that an organization's information technology and business systems are protected and controlled. Also included is a review of IS audit standards, guidelines and best practices.

ISACA IS Auditing Standards and Guidelines
IS Auditing Practices and Techniques
Gathering Information and Preserving Evidence
Control Objectives and IS-Related Controls
Risk Assessment in an Audit Context
Audit Planning and Management Techniques
Reporting and Communication Techniques
Control Self-Assessment

Module 2—CISA's Role in IT Governance

Information Risk Management and Compliance (Domain 2)
This module provides a review of the development of sound control practices and mechanisms for management oversight and review required of an information systems (IS) audit/assurance professional who is responsible for providing assurance that an organization has the structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of IT governance.

IT Governance Basics
IT Governance Frameworks
Information Security Policies
The IT Organization's Roles and Responsibilities
Enterprise Architecture
Risk Management
Process Improvement Models
IT Contracting Strategies
Monitoring and Reporting IT Performance
IT Human Resource Management
IT Resource Investment and Allocations Practices

Module 3—CISA's Role in Systems and Infrastructure Life Cycle Management

Information Security Program Development and Management – Managing and Directing (Domain 3-A)
This module provides a review of the methodologies and processes organizations employ when they develop and change application systems and infrastructure components. Also included is the role of an information systems (IS) audit/assurance professional in providing assurance that management practices meet the organization's objectives for the development/acquisition, testing, implementation, maintenance and disposal of systems and infrastructure.

Benefits Management Practices
Project Governance Mechanisms
Project Management Practices, Tools and Control Frameworks
Risk Management Practices
Project Success Criteria and Risks
Configuration, Change and Release Management
Application Controls

Enterprise Architecture
Requirements Analysis
Acquisition and Contract Management
System Development Methodologies and Tools
Quality Assurance Methods
Managing Testing Processes
Data Conversion Tools, Techniques and Procedures
System Disposal
Certification and Accreditation
Post implementation Reviews
System Migration and Deployment

Module 4—CISA's Role in IT Service Delivery and Support
Information Security Program Development and Management – Services and Operations (Domain 3-B)
This module provides a review of service level management practices, including incident and problem management, capacity planning and systems performance monitoring. In addition, the module outlines the role of the IS audit/assurance professional in auditing and reviewing the various aspects of service level management.

Service Level Management Practices
Operations Management Best Practices
Systems Performance Monitoring Processes, Tools and Techniques
Functionality of Hardware and Network Components
Database Administration Practices
System Software Functionality
Capacity Planning and Monitoring Techniques
Managing Scheduled and Emergency Changes
Incident and Problem Management Practices
Software Licensing and Inventory Practices
System Resiliency Tools and Techniques

Module 5—CISA's Role in Protection of Information Assets
Information Security Program Development and Management – Information Technology (Domain 3-C)This module provides a review of the key components an IS audit/assurance professional must be aware of to evaluate and ensure an organization's confidentiality, integrity, and availability of information assets including logical and physical access controls, network infrastructure security, environmental controls and other processes and procedures used to maintain security of confidential information assets.

Information Security Management
Logical Access Controls
Network Infrastructure Security
Attack Methods and Techniques
Responding to Security Incidents
Security Systems and Devices
Encryption and PKI Components
Virus Detection Tools and Techniques
Penetration Testing
Environmental Protection Practices and Devices
Physical Security Systems
Data Classification Schemes
Voice-Over IP
Transport and Disposal of Information Assets
Security of Portable and Devices

Module 6—CISA's Role in Business Continuity and Disaster Recovery
Information Security Incident Management (Domain 4)
This module provides a review of the practices and knowledge required of an information systems (IS) audit/assurance professional who is responsible for providing assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of information technology (IT) services, while minimizing the business impact.

Backup Basics
Legal Elements

Business Impact Analysis
Business Continuity and Disaster Recovery Plans Development and Maintenance
Business Continuity and Disaster Recovery Plan Testing
uman Resources Management
Invoking the Business Continuity Plan
Alternate Processing and Recovery Strategies
What's Included:
Access to 50+ online modules totaling 54 hours of training.
Over 1000 CISA Exam practice questions
Lecture and Text books.
Required Prerequisites:
Workstation running any Operating System with a web browser
High Speed Internet Connection

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

SU CISM® CERTIFIED INFORMATION SECURITY MANAGER CERTIFICATION CLASS

CISM® Certified Information Security Manager

The CISM® (Certified Information Security Manager) certification is the primary certification for information security professionals who oversee, manage, design and/or assess an enterprise's information security.

The management-focused CISM is a unique certification for individuals who design, build and manage enterprise information security programs. The CISM certification promotes international practices and individuals earning the CISM become part of an elite peer network, attaining a one-of-a-kind credential. In comparison to other certifications, CISM covers a wide body of knowledge and is recommended by the sponsoring organization, ISACA, that those sitting for the CISM certification attend a CISM training session.
For those subject to DoD 8570.01-M "Information Assurance Workforce Improvement Program," ISACA's Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certifications are among those approved for DoD information assurance (IA) professionals.

SU's offers an intensive 72 hour CISM review for those wishing to prepare for the CISM exam. Our classis specifically designed to cover the new material that is on the 2010 exams. Each student progresses through a number of skill checks to ensure knowledge is retained. The CISM instructors are certified with the CISM designation, and serve on local ISACA boards. Worldwide Recognition although certification may not be mandatory for you at this time, a growing number of organizations are recommending that employees become certified. To help ensure success in the global marketplace, it is vital to select a certification class based on universally accepted technical practices.

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider
Cybersecurity Officer/ Enterprise Security Officer
Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect/ Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer.

Class Fee:	$3,990 (+ $800 exam fee excluded
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
KU Outcomes -* Students will be able to analyze system components and determine how they will interact in a composed system.* Students will be able to analyze a system design and determine if the design will meet the system security requirements

This 72 hour course is structured to follow the CISM review manual and examination flow. A full day is provided for each of the core competencies and associated task and knowledge statements, thereby ensuring a detailed and thorough coverage of all areas that will be tested. The fundamental thrust of examination is on understanding the concepts and critical thinking, not on memorizing facts. As a result, the course will be presented in an interactive manner to ensure the underlying concepts are understood and examination questions can be analyzed properly to achieve the best answer.

Lesson Plan:

1 Information Security Governance & Strategy
Information Security Governance Overview
Effective Information Security Governance
Information Security Concepts
Information Security Manager
Scope and Charter of IS Governance
Information Security Governance Metrics
Information Security Strategy Overview
Developing an Information Security Strategy
Information Security Strategy Objectives
Determining Current State of Security
Information Security Strategy
Strategy Resources
Strategy Constraints
Action Plan for Strategy
Implementing Security Governance
Action Plan Intermediate Goals

2 Risk Management
Risk Management Overview
Risk Management Strategy
Effective IS Risk Management
IS Risk Management Concepts
Implementing Risk Management

Risk Assessment and Analysis Methodologies
Risk Assessment
Controls and Countermeasures
Information Resource Valuation
Recovery Time Objectives
Integration With Life Cycle Processes
Security Control Baselines
Risk Monitoring and Communication
Training and Awareness
Documentation

3 Information Security Program Development
IS Program Development Overview
Effective IS Program Development
IS Program Development Concepts
Information Security Manager
Scope and Charter of IS Program Development
IS Program Development Objectives
Defining an IS Program Development Road Map
IS Program Resources
Implementing an IS Program
Information Infrastructure and Architecture
Physical and Environmental Controls
IS Program Integration
IS Program Development Metric

4 Information Security Program Management
IS Management Overview
Organizational Roles and Responsibilities
The IS Management Framework
Measuring IS Management Performance
Common IS Management Challenges
Determining the State of IS Management
IS Management Resources
Other IS Management Considerations
Implementing IS Management

5 Incident Management and Response
Incident Management and Response Overview
Incident Management
Concepts Scope and Charter of Incident Management
Information Security Manager
Incident Management Objectives
Incident Management Metrics and Indicators
Defining Incident Management Procedures
Incident Management Resources
Current State of Incident Response Capability
Developing an Incident Response Plan
Developing Response and Recovery Plans
Testing Response and Recovery Plans
Executing Response and Recovery Plans

Post event Reviews

Grades -All students must ordinarily take all quizzes, lab, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable.
Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

CMMC CYBER SECURITY MATURITY MODEL CERTIFICATION W/ EXAM

To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. With its streamlined requirements, CMMC 2.0: Cuts red tape for small and medium sized businesses Sets priorities for protecting DoD information Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

Overview of the CMMC Program - The Cyber Security Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cyber security requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements. The framework has three key features: Tiered Model: CMMC requires that companies entrusted with national security information implement cyber security standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.

Assessment Requirement: CMMC assessments allow the Department to verify the implementation of clear cyber security standards.

Implementation through Contracts: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

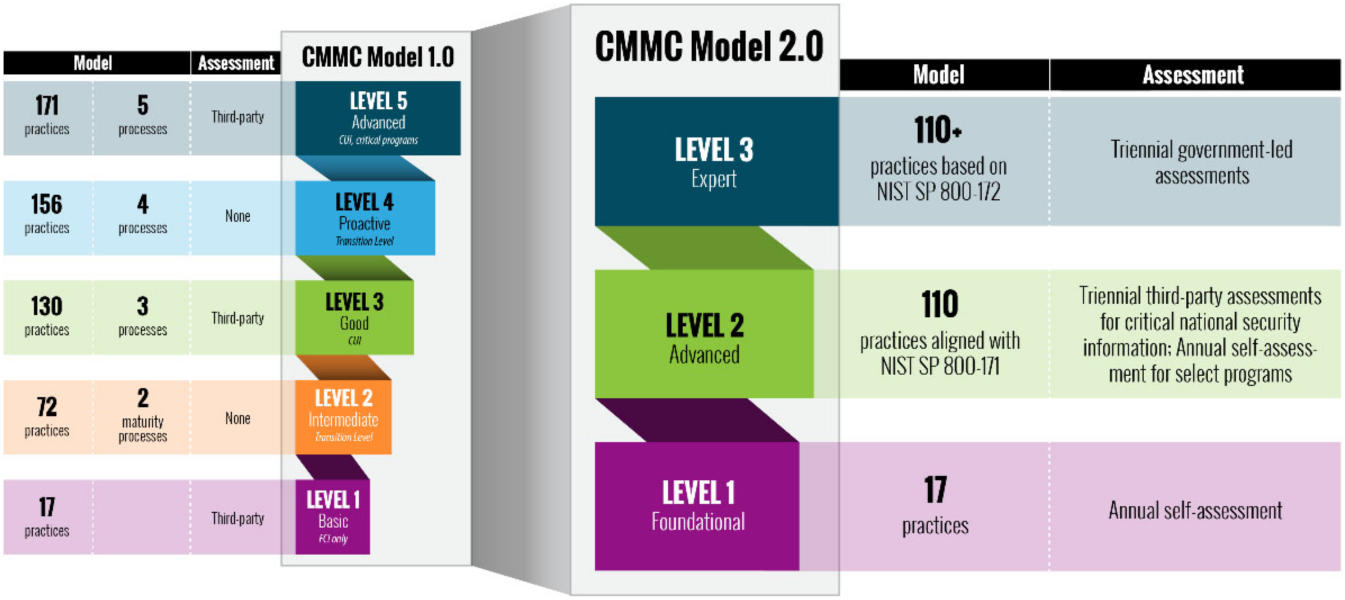
Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD - EXAM
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

In 2019 the Department of Defense (DoD) announced the creation of the Cyber Security Maturity Model Certification (CMMC) to govern the Defense Industrial Base (DIB). Cyber Security Maturity Model Certification (CMMC) relies on self-assessments and third party assessors. The CMMC builds from NIST 800-171 but also includes controls from other cyber security frameworks. Where CMMC differs is in both the maturity model and the role of third-party assessors.



Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

With the implementation of CMMC 2.0, the Department is introducing several key changes that build on and refine the original program requirements. These are: Introduction to the CMMC, Understanding the Supply Chain, Protecting Sensitive Data, Understanding the CMMC Methodology, Building Business Better Through Cyber security, Network Diagrams and Scope

Learning Objectives: 72 hrs Lecture
Students will gain a general understanding of how to audit for CMMC Compliance.

On the surface, project management seems straightforward. However, at best, only 80% of projects end up being economically. Spirit of collaboration: Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification. Added flexibility and speed: Allows waivers to CMMC requirements under certain limited circumstances. On November 4, 2021 the Department of Defense unveiled an update to the Cyber Security Maturity Model Certification framework – CMMC 2.0 – to streamline compliance, increase flexibility, and lower cost for manufacturers and IT providers. About CMMC 2.0

You will learn the 5 Step Guide to Understand:
- How to leverage your NIST 800-171 compliance efforts in preparation for CMMC 2.0
- The relationship between NIST 800-171 and CMMC 2.0
- What should your System Security Plan (SSP) include?
- What is a Plan of Action & Milestone (POAM) and how are they best used?
- How can I implement the requirements in a way that enables CMMC 2.0 validation?

Modules 72 hrs lecture
Lesson 1: 10 hrs Level I Introduction to Cyber Security Maturity Model Certification / History and Players of CMMC
Lesson 2: 10 hrs Securing Sensitive Data
Lesson 3: 10 hrs CMMC Implementation Level 1-3
Lesson 4: 10 hrs Identity and Access Management
Lesson 5: 10 hrs CMMC Methodology
Lesson 6: 10 hrs CMMC Implementation Level 4
Lesson 8: 12 hrs CMMC Implementation Level 5 network diagrams and scope

DFARS Clause 252.204-7012 and NIST 800-171 cyber security requirements for primes and subcontractors are no longer voluntary and DoD audits, coupled with the Cyber Security Maturity Model Certification (CMMC) version 2.0 will require all companies conducting business with the DoD to be certified by a third party. Audit ready, third party verified compliance with DFARS/NIST 800-171 involves much more than documentation and accomplishing it cost-effectively for your business requires an approach informed by the experience gained from hundreds of implementations. CyberSheath created this easy to follow 5 Step Guide informed by real world implementation experience to enable you to quickly and efficiently comply and pass any audit.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books -

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, SecurityX , ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practicum)
SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission *assurance*.
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA Qualified/ CMMC Cyber Security Maturity Model Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX®- [formerly CASP] Certification Class w/exam
PMP® Project Manager Professional Certification Class*
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Certification Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementation Certification Class w/exam
Advanced Cloud Security and Applied SecDevOps Class w/exam
SU CMMC Cyber Security Maturity Model Practicum Required

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery
PROJECT MANAGER PROFESSIONAL CERTIFICATION PMP

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, SecurityX, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practicum)
SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission *assurance*.
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA CMMC Cyber Security Maturity Model Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX®- [formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class *
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum
PMP Project Manager Professional Certification Class*

Get results using time-tested strategies and practical, hands-on tools to execute and succeed in project management. You'll learn how to scope projects effectively, improve time budgeting and resource allocation, and get the project done on time and within budget.

Class Fee:	$3,900 (+ $899 exam fee - excluded)
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study &2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: System administrators, security administrators, Security auditors. Unix box owners. Anyone who has a vested interest in managing their projects. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions.

KU Outcomes:
* Students will be able to describe potential system attacks and the actors that might perform them.
* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives: 72hrs Lecture
Students will gain a general understanding of how to manage projects.
Lesson 1 Organizing the Project and Its Components On the surface, project management seems straightforward. However, at best, only 80% of projects end up being economically successful. The remaining 20% of projects usually cost more than estimated, run late, or fail to satisfy goals or meet objectives. In this course, Instructors shares clear, understandable, and practical methods for achieving better results. You will practice breaking down a project into pieces that can be scheduled, tracked, and controlled. While this is not a

prep course for a project management certification, it will be quite valuable for anyone who is interested in pursuing one. This program will equip you with the concepts, tools, and language of project management that can be applied to any size and type of project. The course is not specific to any formal project management software (e.g. Microsoft Project), but will require that learners have Microsoft Excel with its free Solver add-on installed.

Lesson 2 Planning and Managing Resources . Students will identify strategies to integrate resource availability constraints into project planning, scheduling, and control. This course is designed for project managers who seek better practical results for aligning available resources with tasks and bringing activities to completion on time. Students will examine compression strategies for bringing a project that's running late back on track and will explore how to handle common types of project creep, such as handling customer requests that require extra time, and working with team members who decide independently to invest extra effort in a task. This course combines a focus on formal project management mechanisms with an emphasis on the human element: what can project managers do to resolve issues brought about in the normal course of working with customers, team members, and stakeholders?

Lesson 3 Assessing, Managing, and Mitigating Project Risk Risk management is a key function in project management. Project managers should be able to apply a variety of risk-management tools in their work, including performing risk identification, quantification, response, monitoring, and control. In this course you will examine the nature and types of project risk and learn to apply specific mitigation strategies. You'll have an opportunity to analyze a past project you've worked on and assess what the risks might have been and why. Then you'll analyze the outcomes: Did the known risks come to fruition? What were the leading indicators? What could they have done for contingency planning at the beginning? By asking these questions, you'll then be able to perform several calculations to compute the probability that a project will finish on time.

Lesson 4 Using Earned Value Management for Project Managers -Project managers need to keep things on track by keeping a close eye on the scope of and resources invested in a project. Forecasting, adjusting, and applying corrective measures during the project lifecycle are also key functions of a project manager. This set of processes and protocols that help ensure project success is called earned value management (EVM). Every project manager should have at least a working knowledge of EVM and its theoretical underpinnings.This course is designed for project managers who seek an introduction to EVM to achieve better practical results for implementing project controls, including financial controls and schedule controls. The calculations presented here are meant for any experienced project manager, including those who are not engineers, to apply to any size project. Students in this course will be most successful if they have a foundational understanding of standard project management tools and processes including project networks, project budgets and schedules, and work breakdown structures.

Lesson 5 Agile Project Management Approaches In traditional project management, we tend to make assumptions: the customer knows precisely what they want, or the team's workflow and tasks will go according to plan and in sequence. Practically speaking, this is rarely the case. Sometimes the customer doesn't know what they need until they see an early iteration of your team's work and can provide feedback. Because of this, work is usually done incrementally. We must build flexibility, even agility, into the model in order to succeed.This course is designed for project managers who want to get better practical results with adaptive approaches to projects. Students in this course will be most successful if they have a foundational understanding of traditional project management tools and processes including project networks, budgets and schedules.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

ITIL V4 CERTIFICATION W/EXAM

ITIL stands for Information Technology Infrastructure Library.ITIL is a set of best practice processes for delivering IT services to your organization’s customers. ITIL has its foundations in the IT world, but its principles can easily be used outside of it, within Facilities or HR departments, for instance.You can maximize value to the business by aligning your organization’s processes and services with your business needs. Applying ITIL offers multiple advantages by: Giving input for process improvements and helping to solve service delivery issues. Stimulating process-based thinking and working, while making the effects of doing this visible. Introducing a general terminology used by service providers and customers, so that everyone is always on the same page

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, SecurityX, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practicum)
SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission *assurance*.
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA CMMC Cyber Security Maturity Model Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX®-[formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum
PMP Project Manager Professional Certification Class*
Q/ISO Qualified/ Chief Information Security Officer Certification Class w/exam

Get results using best practices for delivering IT services to your clients. You’ll learn how to scope projects effectively, improve time budgeting and resource allocation, and improve IT services within budget.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: System administrators, security administrators, Security auditors. Unix box owners. Anyone who has a vested interest in managing their projects. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions.

KU Outcomes:
* Students will be able to describe best practice processes for delivering IT services to your organization’s customer.
* Students will be able to apply a framework in your organization.

Learning Objectives:
Students will gain a general understanding of how to manage lifecycle Technical frameworks.

Lesson 1
ITIL V4 – the five lifecycle stages
ITIL V4 was introduced in 2011. In this latest iteration, the framework consists of five lifecycle stages. These stages are split up into multiple processes relying on service principles, processes, roles and performance measures.
The five lifecycle stages are:
Service Strategy: focuses on defining your organization’s strategy to serve customers, and how to maintain and implement that strategy. The goal of this lifecycle stage is to make your organization think and act in a strategic manner.
Service Design: focuses on converting the Service Strategy into reality, by designing and developing new service offerings, or improving your organization’s existing offerings.
Service Transition: focuses on bringing together all assets within a service and ensuring these are integrated and tested. Also focuses on the quality of a new or changed service before it becomes operational.
Service Operation: focuses on ensuring that there are robust best practices that support responsive services. For instance, Incident Management and your organization’s service desk are part of this stage.
Continual Service Improvement: focuses on improving the effectiveness and efficiency of your organization’s IT processes and services. Basically, this lifecycle stage continuously improves the other four stages
Problem Management: can ITIL fix the problem?

Lesson II Six guidelines for successfully implementing ITIL
TOP desk believes that you should apply the parts of ITIL that help your organization offer better services.
Keep the following six guidelines in mind when applying the framework in your organization:
Realize ITIL is a theory, not a goal in itself. It is a theoretical framework, not a best practice. It’s a means to an end.
Start from your daily practice. Use a concrete problem when applying the stages and processes. Don’t start from the theories themselves.
Give your employees the knowledge they need. Because ITIL V4 is much more comprehensive than V2, it’s no longer worth sending your organization’s employees to a complete Foundation training.
Dare to choose. Which processes do you need and, more importantly, in which order do you want to use them?
Don’t overestimate your organization’s maturity. In some organizations, basic call or change management workflows can still be improved. It’s better to focus on that, instead of implementing ITIL as soon as possible.
Low priorities don’t mean a process isn’t important. Some processes, such as setting up a Service Catalogue, aren’t prioritized highly in the Service Design lifecycle phase. This doesn’t mean a Service Catalogue isn’t important.

Lesson III
What is ITSM?
What is ITIL?
What is Shift Left?
What is Incident Management?
What is IT Asset Management?
What is IT Change Management?
What is Workforce Enablement?
What is Agile Service Management?
What is Knowledge Management?
Best practices for your IT Service Management department
Agile Project Management Approaches In traditional project management, we tend to make assumptions: the customer knows precisely what they want, or the team's workflow and tasks will go according to plan and in sequence. Practically speaking, this is rarely the case. Sometimes the customer doesn't know what they need until they see an early iteration of your team's work and can provide feedback. Because of this, work is usually done incrementally. We must build flexibility, even agility, into the model in order to succeed.This course is designed for project managers who want to get better practical results with adaptive approaches to projects. Students in this course will be most successful if they have a foundational understanding of traditional project management tools and processes including project networks, budgets and schedules.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery
SCRUM MASTER CERTIFICATION CLASS W/EXAM

Our Certified ScrumMaster (CSM) workshop is a dynamic and engaging 72 hours of immersion into Scrum. We will learn Scrum by doing Scrum through experiential hands-on exercises, peer discussion, and self-learning. Your trainer will share practical experiences and proven techniques for successfully implementing Scrum in your workplace. You will become eligible to take the test upon completion of the course, and you will be fully prepared to pass with flying colors. Students to attend our workshops have a very high pass rate!

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM (Q/AAP, Q/NSP, Q/CA*, Security+, CISSP, CISM, SecurityX, ISMS Lead Auditor/ Lead Implementer, CMMC III, Q/CSO, Q/CA Practicum)
SU Q/IAP® Certificate Program of Mastery and related micro badges (Q/IAP, Q/AAP, Q/NSP, Q/SOA, Q/CA) identify and certify "qualified persons" who subscribe to a rigorous requirement for maintaining their knowledge and proficiency with validated security skills and hands-on practical security experience for information mission *assurance*.
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA Qualified/ CMMC Cyber Security Maturity Model Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX® - [formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Certification Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementation Certification Class w/exam
PMP Project Manager Professional Certification Class*
Q/ISO Qualified/ Chief Information Security Officer Certification Class

The Scrum Master Certification program will prepare you to master the most popular Agile project management methodology in industry. With this online SSGI Scrum Master certification, you will position yourself as an Agile expert who has the ability to develop and deliver quality products to customers.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential - face-to-face or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance
This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: The Scrum Master Certification course is intended for: project managers, team leads, management, Scrum team members, Six Sigma professionals and other business professionals interested in pursuing in-demand Scrum Master Certification.

Our Certified ScrumMaster (CSM) workshop is a dynamic and engaging 72 hours of immersion into Scrum. We will learn Scrum by doing Scrum through experiential hands-on exercises, peer discussion, and self-learning. Your trainer will share practical experiences and proven techniques for successfully implementing Scrum in your workplace. You will become eligible to take the test upon completion of the course, and you will be fully prepared to pass with flying colors. The program has been designed for professionals who are seeking a management role or currently maintain a leadership position.

Learning Objectives:
Students will gain a general understanding of how to create agile scrum.
Lesson 1: 12 hr Introduction and
Lesson 2: 12 hrs Frameworks & Methodologies
Lesson 3: 12 hrs Extreme Programming
Lesson 4: 12 hrs Lean
Lesson 5: 12 hrs Kanban
Lesson 6: 12 hrs Scrum Framework

Lessons 1-6 include:
2. Project Management Frameworks
3. Agile Methodology
4. Waterfall Methodology
5. Scrum Framework
6. How Scrum Works
7. Product Owner
8. Scrum Master
9. Development Team
10. User Stories
11. Product Backlog
12. Release Planning
13. Sprint Planning and Backlog
14. Estimation and Velocity
15. Technical Debt
16. Sprints
17. Daily Scrum
18. Sprint Review
19. Sprint Retrospective
20. Summary

As a Scrum Master, you will enable your Scrum Team to realize its full potential. Once you complete this program, you will acquire necessary skills to run your Scrum Team using the Agile/Scrum Framework. You will also learn about team roles, events, artifacts, rules, and how to apply them in your daily job. Through experiential hands-on exercises, peer discussions and self-learning techniques**.** Ther is a course workbook packed with bonus content and learning resources. Gain practical experiences and proven techniques for successfully Scrum out team.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

CIPP CERTIFIED INFORMATION PRIVACY PROFESSIONAL CERTIFICATION CLASS W/EXAM

If you're pursuing your Certified Information Privacy Professional/United States (CIPP/US) certification, you'll need to study hard.That's The IAPP is the largest, global information privacy community for professionals who want to develop and advance their careers managing data privacy. The ANSI/ISO accredited certification programs for privacy professionals, including the CIPP/US.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face)
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality. This class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage an Contingency Planning program.

Practicing Privacy – Understanding Laws and Concepts -Show the world you know data privacy laws and regulations and how to apply them. Demonstrate your mastery of jurisdictional laws, regulations and enforcement models, plus legal requirements for handling and transferring data. * Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives:

Phase I

The CIPP/US curriculum provides an in-depth view of U.S. federal and state privacy statutes; detailed analysis of sectoral laws, civil and criminal enforcement; and an overview of the EU's General Data Protection Regulation and the California Consumer Privacy Act. The U.S. Privacy Environment
Data Use by Sector
Government and Court Access to Data
Workplace Privacy
State Privacy and Breach Notification Laws Course Lesson Plans

Phase II — Establishing Baseline

Our privacy training programs can help:

Reduce risk of a data breach by making privacy a shared business objective
Improve decision-making among employees who handle data
Facilitate collaboration and communication across departments
Demonstrate your commitment to data privacy and protection to customers, partners, regulators and staff

Phase II — Using the Tools and Creating an Effective Plan

This is the hands-on phase where students will apply contingency planning principles they have learned while using use the tools we have surveyed to begin a contingency plan for their organization.

Self-assess—Each IAPP exam comes with two tools for determining how ready you are:

The body of knowledge is an outline of the information covered in the exam and represents the breadth of knowledge qualified candidates should possess on the topic. Use it to identify subjects you know well and those you should study more deeply.

The exam blueprint tells you how many questions to expect on each topic. Use it to map out a study strategy—allowing more time for topics with many questions, for example.

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Q/CISO QUALIFIED/ CHIEF INFORMATION SECURITY OFFICER CERTIFICATION CLASS W/ EXAM

If you're pursuing your Q/CISO Qualified/ Chief Information Security Officer Certification class, you'll need to study hard. This class is a comprehensive review of executive levels of information security & industry best practices merged with a comprehensive exam preparation for the Q/CISO exam. Bringing together all the components required for a C-Level positions, the CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of
Grading: Pass = Attendance + Lab	Labs and Practicum Fail > 95% Attendance

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage an Contingency Planning program.

How much does a Chief Information Security Officer make in the United States? The average Chief Information Security Officer salary in the United States is **$230,204** as of April 26, 2022, but the range typically falls between **$201,017** and **$265,867**. Salary ranges can vary widely depending on many important factors, including education, certifications, additional skills, the number of years you have spent in your profession. With more online, real-time compensation data than any other website, Salary.com helps you determine your exact pay target.

Chief information security officers may have been best known for being thrown under the bus in the aftermath of a data breach. Now they're making a reputation for themselves as tech's most wanted, and highest paid. And rightfully so. Cybercrime Magazine recently caught up with Jeremy King, president and founder at Benchmark Executive Search, for a discussion about CISOs at the world's largest companies. It used to be that a cyberattack was a CISO's worst nightmare, and a sure-fire sign that a pink slip would follow. In 2020, it's a fact that every company has been hacked (or will be). Major corporations globally, with the help of law enforcement and private sector cyber defenders, have come to the realization that it's not the CISO's fault, and ousting one will only open up another can of worms — namely recruiting a replacement in a highly competitive market that is suffering through a severe workforce shortage. Instead, CISOs are being heralded for their ability to plan for the worst, and to react calmly, legally, methodically, and swiftly, in response to cyber intrusions.

Learning Objectives:
Domain 1: Governance (Policy, Legal, and Compliance) Information Security Management Program Defining an Information Security Governance Program Regulatory and Legal Compliance
Risk Management

Domain 2: IS Management Controls and Auditing Management
Designing, deploying, and managing security controls
Understanding security controls types and objectives
Implementing control assurance frameworks
Understanding the audit management process

Domain 3: Security Program Management & Operations The role of the CISO

Information Security Projects
Integration of security requirements into other operational processes

Domain 4: Information Security Core Concepts
Access Controls
Physical Security
Disaster Recovery and Business Continuity Planning
Network Security
Threat and Vulnerability Management
Application Security
System Security
Encryption
Vulnerability Assessments and Penetration Testing

Domain 5: Strategic Planning, Finance, & Vendor Management
Security Strategic Planning
Alignment with business goals and risk tolerance
Security emerging trends
Key Performance Indicators (KPI)
Financial Planning
Development of business cases for security
Analyzing, forecasting, and developing a capital expense budget
Analyzing, forecasting, and developing an operating expense budget
Return on Investment (ROI) and cost-benefit analysis
Vendor management
Integrating security requirements into the contractual agreement and procurement process

Note: If required student information is not brought to class a "practice set" of information will be available. **Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. B**ooks** - No books are required for this course. However, you may want to supplement your preparation.

SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery CPoM / non degree
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA CMMC Cyber Security Maturity Model Certification class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX®-[formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum
PMP Project Manager Professional Certification Class*
Q/ISO Qualified/ Chief Information Security Officer Certification Class w/exam

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

Q/CSO QUALIFIED/CYBER SECURITY OFFICER CERTIFICATION CLASS W/EXAMS

Hands On

If you're pursuing your Q/CSO Qualified/ Cyber Security Officer Certification class, you'll need to study hard. This class is a comprehensive review of executive levels of information security & industry best practices merged with a comprehensive exam preparation for the Q/CISO exam. Bringing together all the components required for a C-Level positions, the CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage a cyber risk program.

It used to be that a cyberattack was a CISO's worst nightmare, and a sure-fire sign that a pink slip would follow. In 2020, it's a fact that every company has been hacked (or will be). Major corporations globally, with the help of law enforcement and private sector cyber defenders, have come to the realization that it's not the CISO's fault, and ousting one will only open up another can of worms — namely recruiting a replacement in a highly competitive market that is suffering through a severe workforce shortage. Instead, CISOs are being heralded for their ability to plan for the worst, and to react calmly, legally, methodically, and swiftly, in response to cyber intrusions.
Discussions: CISO Compensation Strategies for recruiting and retaining security leaders
Discussions Compensation -"Money, of course, is something that every CISO wants to hear about," says King, a serial connector in the cyber security space, and a board member for several non-profit organizations related to our field.

Some Fortune 500 and Global 2000 corporations are giving their information security head honchos — oftentimes those with military backgrounds — seven-figure pay packages. One company paid a $3.89 million annual salary to fill its CISO position. The Los Angeles Times reports that big companies are paying big bucks to its top cyber fighters. Another company paid a $650,000 salary to fill its CISO role in 2012, and last year they bumped the pay up to $2.5 million for a new recruit in the same position. In 2016, annual CISO compensation in the largest U.S. cities was topping out at between $380,000 and $420,000. Cybersecurity Ventures has observed a gradual uptick of those figures, and we expect to see an increase in the number of organizations that will move the needle to the $500,000 to $1 million range over the next five years.
Discussion ROI: -If a $1 billion company suffers a breach resulting in a $700 million post-hack market valuation, then how much less is their CISO worth? What about a CISO who prevents such cyber catastrophes from happening in the first place — how much more is she or he worth?
These are the types of questions that C-suite executives and HR chiefs are well-advised to be answering for themselves.
Over the next several years we'll be seeing more large organizations dishing out 7-figure pay packages to "A-players" who get A-results. Now even boardroom executives and shareholders are concerned with the possibility of a cyber intrusion that can lead to a plummeting stock price.
Discussion -where are you in the Org Chart -Cybersecurity Ventures forecasts that 100 percent of large corporations (Fortune 500, Global 2000) globally will have a CISO or equivalent position by the end of 2021 (up from 70 percent in 2018), although many of them will be unfilled due to a lack of experienced candidates. "We may see the CISO position mandated," If that comes to pass, then the big concern is placing unqualified candidates into the positions. Every big company wants the best

CISO, but there's not enough of even the mediocre players to go around. There's also the issue of who should be taking attendance of the CISOs. There is no clear-cut place for security leaders on the org chart. Who they report to varies by company and it can be the chief compliance officer, the chief information officer (CIO), or the chief legal officer. While the idea of elevating the CISO role to new heights and rebranding them as chief risk officers or chief resilience officers (CROs) who report directly to the CEO is a nice one, the market doesn't seem ready for it.

Discussion Military Experience -"A lot of large enterprise CISOs come from the (U.S.) military. They have a longer track record of protecting data, or the new oil," says King, referring to a statement from IBM's former chairman and CEO Ginni Rometty: "We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true — even inevitable — then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."

A recent study by Cybersecurity Ventures calculated 13 percent of Fortune 500 CISOs served in the U.S. military. Altogether, 66 alumni of the United States Armed Forces currently serve as CISOs for the largest companies in the U.S.

If data becomes so important that it's the lifeblood of an organization, then companies will spare no expense in hiring the best person for the CISO job. Cybersecurity Ventures expects this will lead to an uptick in the number of security professionals with military backgrounds being placed as Fortune 500 and Global 2000 CISOs.

King notes that military personnel with substantial cyber security experience will see a 2X to as much as 5X bump in pay when they switch over to the private sector. But, it's not about the money for these women and men. "It's about the mission of protecting companies related to national security — there's a passion that never leaves them — it's in their blood," he says.

Discussion Turnover is rampant when it comes to chief information security officers at the largest companies in the U.S.

The average tenure for CISOs has been estimated at 18 to 26 months by various sources. By comparison, The average tenure for a CIO at the top 1,000 U.S. companies is 54 months, according to Korn Ferry. What explains the CISO merry-go-round at large enterprises? "The demand is so high and the job is so darn tough,". "The stress level is off the roof because a CISO can be right 99 out of 100 times, and a cybercriminal only has to be right once." And when the cybercriminal is right, it can be front-page news. Being in the news is not good for a CISO's career, or resume. At least not if they're captaining the ship when their organization suffers a high profile cyberattack or data breach. If you're a security leader who gets the budget, invests it, and still has the same persistent threats, then it's going to be a very stressful job. "When they (CISOs) quit for no apparent reason, it's usually personal,"

Recruiting -It's predicted that there will be 3.5 million unfilled cybersecurity jobs by 2027 —And the talent supply is so thin that deputy CISOs are being lured away by headhunters in order to fill the number one positions. CISOs also have their own teams to recruit and retain, which is perhaps their most difficult challenge of all. Whether you think CISOs are underappreciated or overpaid, the times are a-changin', and it's a good time to be one.

Learning Objectives:

Domain 1: Governance (Policy, Legal, and Compliance), Information Security Management Program, Defining an Information Security Governance Program, Regulatory and Legal Compliance, Risk Management

Domain 2: Security Program Management & Operations, The role of the CISO, Information Security Projects, Integration of security requirements into other operational processes

Domain 3: Information Security Core Concepts, Access Controls, Physical Security, Disaster Recovery and Business Continuity Planning, Network Security, Threat and Vulnerability Management, Application Security, System Security, Encryption Vulnerability Assessments and Penetration Testing

Domain 4: IS Management Controls and Auditing Management, Designing, deploying, and managing security controls, Understanding security controls types and objectives, Implementing control assurance frameworks, Understanding the audit management process

Domain 5: Strategic Planning, Finance, & Vendor Management, Security Strategic Planning, Alignment with business goals and risk tolerance.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

QUALIFIED/ COMPUTER SECURITY AWARNESS TRAINING W/ EXAM

Turning your weakest security link into your greatest security asset!

The ultimate goal of the SU Security Awareness class is to reduce the risks that every organization faces from lapses in security from staff. When bad things happen, it’s usually because our users simply didn't know better. Who can blame them? The moving target of computer security is hard to hit, even for seasoned security practitioners. Without good training that is continuously reinforced and updated, it is easy to get behind the threat curve and make mistakes.

However, security savvy employees have an advantage because **what they know influences their behavior.** They know about the threat of viruses, so they don't download questionable software or open attachments that they didn't request. This is just one example of awareness reducing organizational risk. The training requires only a browser and internet connection.

Computer Network Defense (CND) Analyst (Cryptologic)
Cybersecurity Intelligence Analyst
Enterprise Network Defense (END) Analyst
Focused Operations Analyst
Incident Analyst/ Network Defense Technician
Network Security Engineer/ Security Analyst
Security Operator/ Sensor Analyst

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Our Security Awareness Class Includes: *Text Materials: labs, SU Pen Testing Materials, resource CD’s and attack handouts. Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation*
KU Outcomes

* Students will be able to describe how risk relates to a system security policy.
* Students will be able to describe various risk analysis methodologies.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
* Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.
The SU Security Awareness Class is a **complete** package that offers a **combination of training methods.** It is designed to introduce users to computer threats and demonstrate the steps that can be taken to avoid them. Organizationally, this has many benefits.

Lesson Plans:
Educates your users about computer and Internet security risks.
Conveys security best practices to help prevent damage due to avoidable mishaps.
Most cost effective way to increase security across your organization.
Empowers the individual to perform IT security best practices.
Supports your organizations security efforts and investments from the ground up.
Aligns the security effort and supports the bottom line.

This security awareness class ensures that our content satisfies the awareness training requirements of a broad range of industries. If your organization needs more than just the default curriculum you will be able to purchase the option of customizing the Security Awareness Class in the first half of 2023 to include other awareness areas and even your policies.

Basic Awareness Curriculum
Passwords

Q/ISP Qualified/ Information Security Professional Certificate of Mastery

QUALIFIED/ INTERENT SECURITY AWARNESS TRAINING AND COMPLIANCE for MGT W/EXAM

Turning your weakest security link into your greatest security asset!

The ultimate goal of the SU Security Awareness and Compliance program for Management is to educate management about what to look for to reduce risks that every organization faces from lapses in security. When bad things happen, its usually because our users simply didn't know better. Who can blame them? The moving target of computer security is hard to hit, even for seasoned security practitioners. Without good training that is continuously reinforced and updated, it is easy to get behind the threat curve and make mistakes.

Knowing how to get the most from your management team to create security savvy employees is the driving force behind this session. Not only will we share with you what makes security savvy employees, you will also learn **how to influences their behavior.** Your management team will understand the “who, what, and where” with regard to the threat of viruses, and other security risks. The clearly will “lead the way” for strong security management, and become the security stakeholders and champions for the enterprise. Downloading questionable software or opening attachments that they didn't request is no longer a threat when everyone is looking out for bad things that happen on your network. These are just a few examples of awareness reducing organizational risk for managers.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance   Fail > 95% Attendance

Computer Support Specialist
Customer Support
Help Desk Representative
Service Desk Operator
Systems Administrator
Technical Support Specialist
User Support Specialist

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

KU Outcomes
* Students will be able to describe how risk relates to a system security policy.
* Students will be able to describe various risk analysis methodologies.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
* Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Our Internet Threat Security Awareness Training and Compliance Program Includes:
Text Materials: labs, Hacking Testing Materials, resource CD’s and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

The SU Security Awareness and Compliance Program is a **complete** package that offers a **combination of training methods.** It is designed to introduce users to computer threats and demonstrate the steps that can be taken to avoid them. Organizationally, this has many benefits. Educates your managers about users and computer and Internet security risks.
Conveys security best practices for management to help prevent damage due to avoidable mishaps. Most cost effective way to increase security awareness across your organization. Empowers the manager to perform IT security best practices from the top down..
Supports your organizations security efforts and investments from the ground up. Aligns the security effort and supports the bottom line.

Our security awareness class ensure that our content satisfies the awareness training requirements of a broad range of industries. If your organization needs more than just the default curriculum you will be able to purchase the option of customizing the Security Awareness Class to include other awareness areas and even your policies.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery

QUALIFIED/ SECURITY HACKING CERTIFICATE FOR MANAGERS W/EXAM

This 72 hour Qualified Security Hacking Certificate class and exam teaches IT Managers & Computer Security Professionals how to be an security hacker to defend your network from malicious software like Trojans, viruses and phishing attempts. In this class you will see 15+ network & computer security tools, you'll learn Network Penetration Testing & Security Hacking, Firewall VPN best practices, understand how Viruses and Trojans get on your network and how to, with effective Patch Management, mitigate risk. Including, how to stop buffer overflows by writing secure code. Lastly, this class shows you how to do computer investigations *without* compromising your data.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid Instructor: TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager Information Assurance (IA) Program Manager Information Assurance (IA) Security Officer Information Security Program Manager Information Systems Security Manager (ISSM) Information Systems Security Officer (ISSO) Information Systems Security Operator

Who should attend:

CIO's, Network Managers, Operations Managers, IT Security Auditor's, IT Auditors, Bank Examiners. Information Systems Security Operations - Oversees and ensures that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program. Advises the Authorizing Official (AO), an information system owner, or the Chief Information Security Officer (CISO) on the security of an information system or program.

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.

Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Tools for class- Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl' **Ethical Hacking - Gather the Data -** You'll uncover the hackers' favorite penetration techniques and how to protect against them.

KU Outcomes
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

Learning Objectives:

Lesson Plan
Ethical Hacker - Ethics and Legality
What is an Exploit?
The security functionality triangle
The actor's process
Passive & active reconnaissance
Types of attacks
Categories of exploits
Goals attackers try to achieve

- Skills required for ethical hacking
- Categories of Ethical Hackers
- What do Ethical Hackers do?
- Security evaluation plan
- Types of Ethical Hacks
- Testing Types
- Ethical Hacking Report
- Cyber Security Enhancement Act of 2002
- Computer Crimes

Ethical hackers and crackers -Who are they
Self proclaimed ethical hacking

- Hacking Punishment

- **Ethical Hacker: Footprinting**
  What is Footprinting
- Steps for gathering information
- Whois
- http://tucows.com
- Hacking Tool: Sam Spade
- Analyzing Whois output
- NSLookup
- Finding the address range of the network
- ARIN
- Traceroute
- Hacking Tool: NeoTrace
- Visual Route
- Visual Lookout
- Hacking Tool: Smart Whois
- Hacking Tool: eMailTracking Pro
- Hacking Tool: MailTracking.com

- **Lesson Plan   Ethical Hacker: Scanning**
  Determining if the system is alive?
- Active stack fingerprinting
- Passive stack fingerprinting
- Hacking Tool: Pinger
- Hacking Tool: Friendly Pinger
- Hacking Tools
- Detecting Ping sweeps
- ICMP Queries
- Hacking Tool: netcraft.com
- Port Scanning
- TCPs 3-way handshake
- TCP Scan types
- Hacking Tool: IPEye
- Hacking Tool: IPSECSCAN
- Hacking Tool: nmap
- Port Scan countermeasures
- Hacking Tool: HTTrack Web Copier
- Network Management Tools
- SolarWinds Toolset
- NeoWatch
- War Dialing
- Proxy Servers
- Hacking Tool: SocksChain
- Surf the web anonymously
- TCP/IP through HTTP Tunneling
- Hacking Tool: HTTPort
- Hacking Tool: Tunneld
- Hacking Tool: BackStealth

- Find & fix web server vulnerabilities
  Data mining authentication information
  Hacking by brute forcing remotely

- **Defend your networks** against unauthorized access and denial-of-service attacks at the permiter
  You will examine the weaknesses of firewall architectures
  Securing mail with VPN
  Examine E-shoplifting
  Hack SSL-enabled sites
  The impact of Zero-day viruses to are nothing compared to Trojans.
- What is a Trojan Horse?
- Overt and Covert /BoSniffer
- Hacking Tool: NetBus
- ComputerSpy Key Logger
- Hacking Tool: Beast Trojan
- Wrappers /Hacking Tool: Whack a Mole Trojan
  Construction Kit /Writing Trojans in Java
- Covert Channels /ICMP Tunneling
- Backdoor Countermeasures
- BO Startup and Registry Entries
- NetBus Startup and Registry Keys
- Port Monitoring Tools
- fPort
- TCPView
- Process Viewer
- Inzider - Tracks Processes and Ports
- Trojan Maker
- Man-in-thE-Middle Attack
- Hacking Tool: dsniff
- System File Verification
- TripWire

- Reverse WWW Shell

- **How to detect the crime, track the criminal, and assemble the evidence.**
  Computer Forensics and Investigations as a Profession Understanding Computer Forensics
- Comparing Definitions of Computer Forensics
- Exploring a Brief History of Computer Forensics
- Developing Computer Forensics Resources
- Preparing for Computing Investigations
- Understanding Enforcement Agency Investigations
- Understanding Corporate Investigations
- Maintaining Professional Conduct

- **Understanding Computer Investigations**
  Preparing a Computer Investigation
- Examining a Computer Crime
- Examining a Company-Policy Violation
- Taking a Systematic Approach
- Assessing the Case
- Planning Your Investigation
- Securing Your Evidence
- Setting Up Your Workstation for Computer Forensics
- Executing an Investigation
- Gathering the Evidence
- Copying the Evidence Disk
- Analyzing Your Digital Evidence
- Completing the Case
- Critiquing the Case

Penetration concepts you will see during this class
Attacking network infrastructure devices
Hacking by brute forcing remotely
Security testing methodologies
Security exploit testing with IMPACT from Core Security
Stealthy network recon
Remote root vulnerability exploitation
Multi-OS banner grabbing
Privilege escalation hacking
Unauthorized data extraction
Breaking IP-based ACLs via spoofing
Evidence removal and anti-forensics
Hacking Web Applications
Breaking into databases w/SQL Injection Cross Site Scripting hacking & Remote access trojan hacking & Offensive sniffing
Justifying a penetration test to management and customers
Defensive techniques

Instructor-led demo exercises
Abusing DNS for host identification
Leaking system information from Unix and Windows
Stealthy Recon
Unix, Windows and Cisco password cracking Remote buffer overflow exploit lab I Stack mashing
Remote heap overflow exploit lab - Beyond the Stack
Remote keylogging
Data mining authentication - from clear-text protocols
Remote sniffing
Malicious event log editing
Transferring files through firewalls
Hacking into Cisco routers
Harvesting web application data
Data retrieval with SQL Injection Hacking

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step
Books – Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.
Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932 | Edition: 4
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013)The book below is recommended for those interested in understanding how their own computers work for personal edification

Q/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

ISMS LEAD AUDITOR CLASS W/ EXAM

The ISO 27001 lead audit training course teaches participants the foundations of the audit of Information Security Management System (ISMS). Taking place over 72 hour, including the official certification exam, the course gives students basic training in how to conduct audits in accordance with the registration process for the ISO 27001:2005 standard. The lectures and audit exercises are based on the guidelines for the ISO 19011:2002 audit as well as the various standards in the ISO 27000 family.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs and Practicum Fail > 95% Attendance

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator
Network Analyst/ Network Security Engineer
Network Security Specialist/Security Analyst
Security Engineer/Security Specialist
Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality[excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Learning Level: Basic Auditor to Advanced
KU outcomes:
Knowledge of new and emerging IT
Knowledge of IT compliance and assurance
Knowledge of the capabilities and functionality of compliance

Target Audience IT Security Managers , IT Managers , Auditors interested in ISO 27001 :2005 or ISO 17799 :2005 / ISO 27002: 2007 Standards , Information Security Consultants
Pre-class study Initial knowledge of ISO/IEC 17799:2005 and ISO 27001:2005 standards, and base knowledge of information security is required.

Learning Objectives
Review of the ISO 27001:2005 prerequisites
Understanding of the relations between ISO 27001:2005 and ISO/IEC 17799:2005
Security related threat and vulnerabilities apprenticeship evaluation
Understanding of the security controls and counter-measures
Comprehension of the auditor's roles and responsibilities
Apprenticeship of the relative phases of an information security management system audit

Curriculum Lesson 1
Introduction to information security management system management with ISO 27001 8 hrs
Objectives and course structure
Information Security Standard
Certification Process
Fundamental Principles of Information Security
Information Security Management System
Lesson 2: Audit initiation 6 hrs Lecture 2hr labs
Fundamental Audit Concepts and Principles
Evidence based approach
Audit Preparation
Documentary Audit
Preparing for the On-site Audit Activities Conducting On-site Activities

Lesson 3: Conduct the audit
Communication during the audit
Audit Procedures
Drafting of conclusions and non-conformity reports
Lesson 4: Conclude the audit
Audit Documentation Review of the Audit Notes
Audit Conclusions
Managing an audit program
The competence and evaluation of auditors
Training Closure
Lesson 5: Examination
3-hour review and hands-on labs of an ISO 27001 Lead Auditor and 3-hour exam leading to certification as an ISO 27001 Lead Auditor.

Prerequisites: The ISMS Foundation course or basicknowledge of the ISO 27001 and ISO 27002 standards is recommended.
A copy of the ISO 19011, ISO 27001 and ISO 27002 standards will be provided to participants.
A certificate of attainment will be given to participants who successfully pass the examination

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books – 3 Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SU Q/IAP® Qualified/ Information Assurance Professional Certificate of Mastery CoM / non degree (Q/AAP, Q/NSP, Q/CA*, CISSP CISM, SecurityX & Security+ , ISMS ISO 27001) Practicals * below
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class w/exam
Q/NSP® Qualified/ Network Security Policy Administrator Certification Class w/exam
Q/CA CMMC Cyber Security Maturity Model Certification class w/exam
SU Security+® CompTIA Certification Class w/exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class*
SU SecurityX ®-[formerly CASP] Certification Class w/exam
SU CISA® Certified Information Security Auditor Certification Class w/exam
SU CISM® Certified Information Security Manager Certification Class*
Certified ISO 27001 SU ISMS® Lead Auditor Class w/exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class w/exam
SU CMMC Cyber Security Maturity Model Practicum
PMP Project Manager Professional Certification Class*
Q/ISO Qualified/ Chief Information Security Officer Certification Class w/exam

Q/ISP Qualified/ Information Assurance Professional Certificate Program of Mastery
CERTIFIED ISO 27001 LEAD IMPLEMENTATION CLASS W/EXAM

ISO 27001 – Information Security Management Systems (ISMS) Implementation course teaches students the necessary steps of information security management system implementation as specified in ISO 27001. This intensive seventy-two hour course provides students with useful knowledge to ISMS implementation according to the ISO 27001 standard.

The course is based on the ISO 27003 standard " *Security Techniques - Information Technology* (in development)". The course is conceived specifically for those who wish to understand the ISMS implementation steps according to the criteria of the ISO 27001: 2005 standard. The students equally acquire the essential knowledge to provide necessary help to other individuals and organizations that desire to conform to the standard. The training is also aligned with best practices in regards to project management according to the Project Management Institute (PMI) and the International Project Management Association (IPMA) as well as the ISO 10006 standard, " *Guidelines for quality management in project"* .

Class:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95%
Attendance

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/Network Analyst
Network Security Engineer
Network Security Specialist
Security Analyst/Security Engineer
Security Specialist/Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Learning Level: Basic Auditor to Advanced
KU outcomes
Knowledge of new and emerging IT compliance
Knowledge of compliance and assurance
Knowledge of the capabilities and functionality of compliance

ISO 27001-ISMS Lead Implementer (72 hours)
The ISO 27001 - ISMS Lead Implementer course informs participants about the steps required for the implementation of a management system as specified in ISO 27001:2005. This intensive 72 hour course provides students with a knowledge of the steps required for the implementation of an ISMS in accordance with the requirements of the ISO 27001 standard. The course is in line with the best practices in project management as defined by the Project Management Institute (PMI) as well as the ISO 10006 standard, "Guidelines to quality in project management".
Curriculum

Lesson 1 : ISMS
Introduction to management systems
Presentation of ISO 27001 and ISO 27002 standards
Fundamental Principles of Information Security
Preliminary analysis
Project management

Lesson 2 : Plan
Governance
Risk analysis
Statement of applicability

Lesson 3 : Do
Document management program
Controls and processes design
Controls implementation Formation, awareness and communication
Incidents management

Operation Management

Lesson 4 : Check, Act and certification audit

Monitoring

Metrics and dashboards

Internal audit

Management review

Continual improvement

Certification audit

Lesson 5 : Practicum and Examination

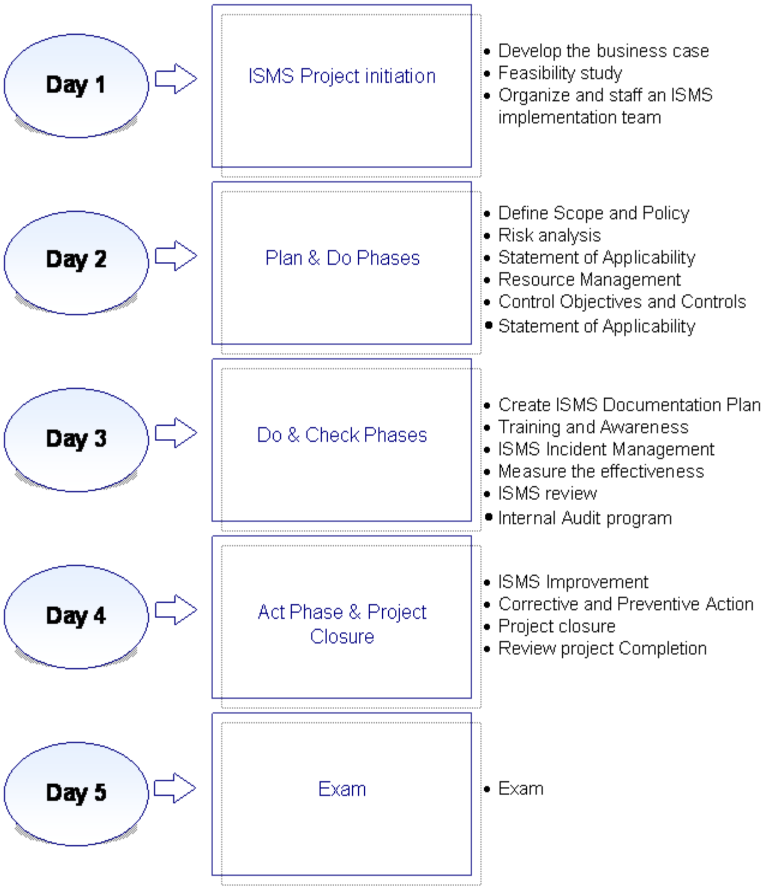
Risk analysis practicum

Statement of applicability practicum

3-hour examination leading to certification as an ISO 27001 - ISMS Lead Implementer.

The training and examination are in the process of being certified by RABQSA, a US certification body.

Prerequisites : The ISMS Foundation course or basic knowledge of the ISO 27001 and ISO 27002 standards is recommended General information : Maximum number of students: 20 A copy of the ISO 27001 and ISO 27002 standards will be provided to participants. ***Grade****s -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step*


Day 1
ISMS Project initiation
• Develop the business case
• Feasibility study
• Organize and staff an ISMS implementation team
Day 2
Plan & Do Phases
• Define Scope and Policy
• Risk analysis
• Statement of Applicability
• Resource Management
• Control Objectives and Controls
• Statement of Applicability
Day 3
Do & Check Phases
• Create ISMS Documentation Plan
• Training and Awareness
• ISMS Incident Management
• Measure the effectiveness
• ISMS review
• Internal Audit program
Day 4
Act Phase & Project Closure
• ISMS Improvement
• Corrective and Preventive Action
• Project closure
• Review project Completion
Day 5
Exam
• Exam

Q/WP Qualified/ Wireless Professional Certificate Program of M

Q/WP QUALIFIED/ WIRELESS PROFESSIONAL CERTIFICATION CLASS W/EXAM

Learn to successfully survey, install, administer and secure enterprise class Wi-Fi networks.
The Q/WP certification is the enterprise Wi-Fi certification for the Q/WP Class.Since 1999, Taught by SU's advanced Q/WP & Q/WSP training materials are Qualification Training in the US. Improving education to the expert level you expect from SU.

Achieving Q/WP sets your career on a firm foundation, ensuring you have the skills to successfully survey, install, and administer enterprise Wi-Fi networks. In this hands-on course, you will gain a full understanding of how radio frequency affects networking so you can perform site surveys, design a high-performance network, and protect both users and sensitive data from potential intruders. Plus, you will explore advanced topics such as VoWLAN deployments, seamless mobile connectivity, and detailed frame analysis. You will use enterprise-class hardware and software tools during live lab exercises, simulating a state-of-the-art production environment.

Included in class fee is Ebook , SU Practice exams for QWP This SU hands-on, defense in-depth class has 18+ labs to give you the chance to use products from vendors like AirMagnet, Aruba, Meru, AirDefense, CISCO, AirTight Networks, Wi-Spi, Cognio Spectrum Analysers, PROXIM, YDI and much more than the standard

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator
Network Analyst / Network Security Engineer
Network Security Specialist
Security Analyst/ Security Engineer
Security Specialist /Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Learning Objectives: Enterprise Network Defense Analysis - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the enterprise network in order to protect information, information systems, and networks from threats*.*

- Ownership concepts of 801, blue tooth and man's
- security policy creation and alignment
- design and control methods
- Return on investment strategies and methods
- Automated tools and management strategies *Q/WP Class textbook, Q/WSP Study guide, labs. CWNA/ CWSP ebooks*

KU Outcomes
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

Who Should Attend Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators and Engineers , Consultants, Systems and Data Security Analysts, Compliance Officers, Chief Security Officers, and others concerned with securityAll attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 security solutions using hardware and software from the following vendors:

Lesson Plan 18 hrs lecture/ 27hrs labs:

1. **Lesson Plan 1**
   Introduction to 802.11 LANS

   1.1. Standards organizations responsible for shaping the 802.11 Lan Protocol
   1.2. How Standards compliance is enforced for 802.11 WLAN vendors
   1.3. Examine the 802.11 standard and various amendments
   1.4. Discuss additional networking standards that are commonly used to enhacnce 802.11 WLAN

2.

Radio Frequency Fundamentals

- 2.1. Physical Aspects of RF propagation
- 2.2. Types of losses and attenuation that affect RF communications
- 2.3. Types of modulation used for communications
- 2.4. How channels and bandwidth are related to each other in networks
- 2.5. Three types of Spread Spectrum used in networking
- 2.6. RF Math Calculations
- 2.6.1. RF Units of measure
- 2.6.2. Basic RF Mathematics
- 2.6.3. RF signal measurements
- 2.6.4. Understand link budgets
- 2.6.5. Define and calculate system operating margin (SOM)

3. 802.11 Service Sets

- 3.1. Explain three types of service sets defined for use within 802.11 WLANs
- 3.2. Roaming within a WLAN
- 3.3. Load Balancing as a method to improve congestion in WLANs

Lesson Plan 2

4.

RF Power Output Regulations

- 4.1. Understand international, regional, and local RF spectrum management organizations
- 4.2. Understand RF channels in the unlicensed 2.4 GHz and 5 GHz frequency ranges

5. Power over Ethernet

- 5.1. Recognize the two types of devices used in Power over Ethernet (PoE)
- 5.2. Recognize the differences between the tow types of Power Sourcing Equipment (PSE)
- 5.3. Understand the two ways in which power can be delivered using PoE
- 5.4. Understand the importance of planning to maximize the efficiency of PoE

Spectrum Technologies

- 5.5. Uses of Spread Spectrum
- 5.6. Frequency Hopping
- 5.7. Direct Sequencing
- 5.8. Comparing DSSS to FHSS
- 5.9. Co-location and Throughput Analysis

6. LAN Operation

- 6.1. Ad Hoc networks
- 6.2. Infrastructure networks
- 6.3. Bridged Networks
- 6.4. Repeater Networks
- 6.5. Mesh Networks
- 6.6. WLAN Switched networks
- 6.7. Enterprise Gateway networks
- 6.8. Enterprise Encryption Gateway networks
- 6.9. Virtual AP networks
- 6.10. Evolution of WLAN architectures
- 6.11. WLAN management

Lesson Plan 3

7. LAN Security

- 7.1. Security Policy and Procedures
- 7.2. Legacy 802.11 Security Components
- 7.3. 802.11i Security Components
- 7.4. WPA – personal
- 7.5. WPA – Enterprise
- 7.6. WPA 2 – personal
- 7.7. WPA2 - Enterprise
- 7.8. Types of Network Attacks
- 7.9. Baseline Security Practices (SOHO, SMB, Enterprise)

8. 802.11 Analysis and Troubleshooting

- 8.1. Introduction to 802.11 Protocol Analysis
- 8.2. 802.11 Data Frames
- 8.3. 802.11 Control Frames
- 8.4. 802.11 Management Frames
- 8.5. Frame Fragmentation
- 8.6. Power Saving Operations
- 8.7. Transmission Rates

9. Coordinating 802.11 Frame Transmission

- 9.1. Differences between CSMA/CD and CSMA/CA
- 9.2. Distributed Coordination Function (DCF)
- 9.3. Quality of Service in 802.11 WLANS

Lesson Plan 4

10. Antennas

- 10.1. Antenna characteristics and behaviors
- 10.2. Types of antennas commonly used with WLANS
- 10.3. Advances Antenna Systems
- 10.4. Antenna Placement and mounting
- 10.5. Antenna Safety
- 10.6. Types of antenna cables, connectors and accessories

Lesson Plan

11. Site Surveying

- 11.1. Understanding the need for a site survey
- 11.2. Defining Business Requirements and justification
- 11.3. Facility Analysis
- 11.4. Interviewing Network Management and users
- 11.5. Identifying Bandwidth Requirements
- 11.6. Determining contours of RF coverage
- 11.7. Documenting installation problems
- 11.8. Locating Interference
- 11.9. Reporting Methodology and procedures
- 11.10. Understanding specifics of each vertical market
- 11.11. Understanding the customers network topology

11.12. Creating appropriate documentation during and after the site survey
11.13. Understanding Safety Hazards
11.14. Using appropriate hardware and software to perform the survey
11.15. Understand the need for spectrum analysis
11.16. Manual RF site surveys
11.17. Predictive site Surveys
11.18. Dense AP deployment

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books – 3 Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Those Less Comfortable – Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick ngebretson (Jun 24, 2013)
The book below is recommended for those interested in understanding how their own computers work for personal edification
How Computers Work, Ninth Edition Ron White Que Publishing, 2007 ISBN 0-7897-3613-6
This last book below is recommended for aspiring hackers, those interested in programming techniques and low-level optimization of code for applications beyond the scope of this course. Hacker's Delight, Second Edition Henry S. Warren Jr. Addison-Wesley, 2012 ISBN 0-321-84268-5

SU Q/WP® Qualified Professional Certificate Program of Mastery CPoM non degree (4 Q/WP®, Security+®, SecurityX)
Q/WAD® Qualified/ Analyst & Defender Certification Class w/exam
Q/ WP® Qualified/ Professional Certification Class w/exam
Q/WSP® Qualified/ Security Professional Certification Class w/exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Qualified Wireless professional / Qualified Security Professional Certification Class w/exam
SU Security+® CompTIA Certification Class & Exam
SU SecurityX ® Certified Professional Certification Class & Exam
PMP Project Manager Professional Certification Class*
Q/WLANPD Qualified/ Local Area Network Planning & Design Class w/exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing Class w/exam
Q/WDNO Qualified/ Deceptive Network Optimization Class w/exam

Q/WP Qualified/ Professional Certificate Program of Mastery

QWSP® QUALIFIED/ WIRELESS SECURITY PROFESSIONAL CLASS W/EXAM

SU's Q/WSP® training materials are the MOST RESPECTED Security Certification Training in the world!
Since 1999 SU has delivered the most effective and complete certification training that gets your secure!
This Q/WSP® course targets experienced professionals who are looking for critical hands-on skills in security, including how hackers attack w-networks and the learn how to preventing them from doing so. CWNA or Q/WP required Q/WSP Certification class.

The Q/WSP® Hacking Security course consists of hands on learning using the latest enterprise security tools and security auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion, DDoS tools and techniques, functionality of the standard, the inner-workings of each EAP type used with LANs today, and every class and type of WLAN security solution available on the market - from intrusion prevention systems to network management systems you learn skills for implementing and managing security in the enterprise with layer2 and layer3 hardware and software solutions. Practicum is required for class completion.

Class Duration: This class consists of 72 hours of hands on learning using the latest enterprise LAN security and auditing equipment. This class addresses in detail LAN Intrusion, Security Policy, and Security Solutions.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/ Network Analyst
Network Security Engineer
Network Security Specialist
Security Analyst /Security Engineer
Security Specialist/ Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for gradution.

- What you will learn:
- security policy creation and alignment
- Security design and control methods
- Return on investment strategies and methods
- Automated tools and management strategies

Who Should Attend:

Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators and Engineers, Consultants, Systems and Data Security Analysts, Compliance Officers, Chief Security Officers, and others concerned with security
KU Outcomes
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

Lesson Plan 21 hrs lecture/ 24 hrs labs:

All attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 security solutions using hardware and software from the following vendors:
Prerequisites: *Knowledge of the Q/WP is required prior to taking the Q/WSP exam. It is recommended that all students have at least 12 months experience in a network security related field prior to enrolling in the course.*
Hands-on Lab Exercises: These are the actual labs taught in the LAN Security Course:

- Packet Analysis & Spoofing
- Rogue Hardware & Default Settings
- RF Jamming & Data Flooding
- Information Theft
- Hijacking and DoS Attacks
- Access Point VPNs
- Scalable VPN Solutions
- EAP - Cisco (LEAP)
- Layered Security
- Bridging Security
- 802.1x and EAP-TTLS
- SSH2 Tunneling & Local Port Redirection

The LAN Security course consists of hands on learning using the latest enterprise LAN security and auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with LANs today, and every class and type of WLAN security solution available on the market - from intrusion prevention systems to network management systems.

All attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 security solutions using hardware and software from the following vendors:

1. **Lesson Plan 1**
WLAN Intrusion
1.1. Intrusion Tools
1.2. Intrusion Techniques
1.3. LAB – WLAN Intrusion Tools and Techniques

2. Physical Security
2.1. Controlled Physical access to premises and infrastructure
2.2. Social Engineering
2.3. Policy Adherence
2.4. Proper use of Security Solutions

3. MAC Layer Security
3.1. Use of VLANs for layer-2 segmentation in WLANs
3.2. PrE-shared key security solutions
3.3. 802.1X/EAP framework and security solutions
3.4. Extensible Authentication Protocol (EAP) framework and comparisons
3.5. Detailed discussion of each EAP type used in today's WLANs including in-dedpth frame exchange graphics 3.6. Wi-Fi Protected Areas
3.7. 802.11i terms, framework, and in-depth operational explanations
3.8. 802.11i/RSN functional graphics and frame capture explanations
3.9. Explanations of how 02.1X/EAP solutions changed to 802.11i/RSN solutions
3.10. 802.11i frame format explanations and graphics

Lesson Plan 2
4. The 802.11i amendment
IP Security – Network Layer Security
5.1. PPTP VPN
5.2. IP Framewoark and implementation discussion and graphical detail

Lesson Plan 3
6. LAB – 802.1X/EAP & VLAN based Security Solutions

7. Hardware and Software Solutions
7.1. "Fat" access points
7.2. WLAN switches/controllers
7.3. WLAN bridges
7.4. SOHO/SMB solutions
7.5. Enterprise Encryption Gateways (EEGs)
7.6. Enterprise Gateways (EWGs)
7.7. WLAN routers
7.8. WLAN Network Management Systems (WNMS)
7.9. WLAN mesh routers
7.10. WLAN Intrusion Detection/Prevention Systems (WIDS/WIPS)

Lesson Plan Day 3
8. Lab Exercises
8.1. Secure WLAN Bridging
8.2. WLAN Switching
8.3. Enterprise Encryption Gateways (EEGS)
8.4. Enterprise W ireless Gateways (EWGs)
8.5. SOHO?SMB solutions
8.6. WLAN Routers

9. Application Security
9.1. Secure Shell (SSH1/SSH2) as a terminal application and VPN solution
9.2. SSLv3/TLSv1 for E-mail, FTP, and web browsing
9.3. SNMPv3 for authenticated and encrypted network management

Lesson Plan 4
10.

Authentication, Authorization, and Accounting (AAA) Systems

10.1. Local Authentication in APs, EWGs, WLAN switches, and WLAN routers
10.2. RADIUS authentication and proxy serices
10.3. KERBOS authentication
10.4. LDAP authentication
10.5. Per-user and per-Group authorization options
10.6. Role Based access control (RBAC)
10.7. Bandwidth management

11.

WIDS Solutions- Protocol Analyzers

11.1. Hardware and software types available
11.2. Performance and security analysis
11.3. Connectivity Troubleshooting
11.4. Channel/spectral monitoring
11.5. Distributed analysis with WIDS
11.6. Three Types of WIDS – explanation of each
11.7.

12. **Lesson Plan 5**

LAB Exercises

12.1. WLAN Network Management Systems
12.2. WLAN Intrusion Detection Systems

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books – 3 Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

SU Q/WP® Qualified Professional Certificate Program of Mastery CPoM non degree (3 Q/WP® - Q/WP, Q/WSP, (or Q/WP- Q/WSP classes) Q/WAD + Security+®, SecurityX)
Q/WAD® Qualified/ Analyst & Defender Certification Class w/exam
Q/ WP® Qualified/ Professional Certification Class w/exam
Q/WSP® Qualified/ Security Professional Certification Class w/exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Qualified Wireless Professional / Qualified Security Professional Certification Class & Exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX® Certified Certification Class w/exam
PMP Project Manager Professional Certification Class*
Q/WLANPD Qualified/ Local Area Network Planning & Design Class w/exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing Class w/exam
Q/WDNO Qualified/ Deceptive Network Optimization Class w/exam

Q/WP Qualified/ Professional Certificate Program of Mastery

QWAD QUALIFIED/ WIRELESS ANALYST AND DEFENDER CERTIFICATION CLASS W/EXAM QWAD QUALIFIED/ WIRELESS ANALYST AND DEFENDER PRACTICUM

The Q/WAD (Qualified/ Analysis Professional) certification is an advanced LAN certification, focusing entirely on the analysis and troubleshooting of LAN systems. In this 72 hour class the Q/WAD + Hacking Networks, learning objectives begin with the frame structures and exchange processes for each of the 802.11 series of standards, and then apply that base of knowledge to how and when to use the tools that are available for analyzing and troubleshooting today's LANs. The Q/WAD certified individual will be able to confidently analyze and troubleshoot any LAN system using any of the market leading software and hardware analysis

Class Duration: The class consists of 72 hours of hands on learning using the latest enterprise LAN security and auditing equipment, addressing in detail LAN Intrusion, Security Policy and Solutions.

Who Should Attend:

Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators and Engineers, Consultants, Systems and Data Security Analysts, Compliance Officers, Chief Security Officers, and others concerned with security

Class Fee:	$3,990
Time:	72 hrs
Contact Hours:	40 hr Lecture 32 hr pre class study & 2hr exam
Learning Level:	Basic Understanding of TCP/IP Protocols
Prerequisites:	72 CPE / 3 CEU
Credits:	TBD
Instructor:	
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/ Network Analyst
Network Security Engineer/ Network Security Specialist/ Security Analyst /Security Engineer/ Security Specialist/ Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: Q/WAP Class textbook, labs.

Learning Objectives: General Knowledge Areas: Reflect basic types of knowledge for cybersecurity professionals and reside within multiple Specialty Areas.

Knowledge of computer networking concepts and protocols, and network security methodologies.
*Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

1. A proven advanced skill set.
    - Intimate knowledge of the inter-workings of IEEE 802.11 standards
    - Understanding of the use of common tools found in LAN protocol analyzers
    - Detailed knowledge of appropriate application of a protocol analyzer
    - A thorough understanding of LAN troubleshooting from performance and security perspectives
2. A unique and uniquely recognized certification.
    - The CWAP is the only vendor neutral LAN analysis certification.
    - The CWAP certification is without equal or competition, and is recognized and endorsed by nearly all of the leading LAN analysis vendors in the market today.
3. Proven ability to perform advanced troubleshooting and analysis.
    - Performance and security analysis to the maximum potential of the available protocol analyzer.
    - Troubleshooting from various perspectives in a variety of LAN implementations.
    - Verification of Layer 2, 3 & 7 security solutions during security audits.
    - Application analysis testing from a performance perspective in single mode and 802.11b/g mixed mode environments.

- Detailed site surveys using the latest surveying features of LAN protocol analyzers.
- Detailed analysis of decode information taken from LAN protocol analyzers for the purpose of troubleshooting.

Who Should Attend:

Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators and Engineers, Consultants, Systems and Data Security Analysts, Compliance Officers, Chief Security Officers, and others concerned with security

Learning Objectives - effective use of the following tools in class:

Class Lesson Plan:

The following list contains the materials covered in the lecture portion of the course: Lesson Plan Day 1

Physical Layer

- PLCP and PMD Sub-layers
- PLCP header fields and subfields

DCF Mode

- Interframe Spacing
- Backoff Algorithms
- Frame exchange processes

PCF Mode

- Media access rules
- Frame exchange processes

MAC frame fields and subfields

MAC layer addressing

- BSS
- ESS
- WDS

802.11e topical coverage

Wired connectivity standards for access points and bridges

- 802.1h
- RFC1042

Using LAN protocol analyzers

- Performance analysis
- Security analysis
- Distributed analysis
- Protocol decode analysis
- Site Surveying
- Application Analysis

Lesson Plan Day 2

Use of 802.11 series of standards, hardware & terminology

- MPDU
- MMPDU
- MSDU
- PPDU
- PSDU

Hacking Networks Class Topics

- Vulnerabilities of open networks
- Packet analysis & locating rogue access points- AirMagnet demo
- Available counter measures and solutions to stop the leaks
- How to defend your LAN from hackers
- Demos incl: jamming & data flooding, spoofing and more.

Bottom line: You'll leave knowing how to defend your network from hacking and how to locate unauthorized access points before the hacker takes over your network . Hacking networks is 4 days of hacking and workshops

- Packet Analysis & Spoofing
- Rogue Hardware & Default Settings
- RF Jamming & Data Flooding
- Information Theft
- Hijacking and DoS Attacks
- Access Point VPNs
- Scalable VPN Solutions
- EAP - Cisco (LEAP)
- Layered Security
- Bridging Security
- 802.1x and EAP-TTLS
- SSH2 Tunneling & Local Port Redirection

Class Outline

Lesson Plan 3
Risk Assessment

- Assets to protect
- Threats to protect against
- Legal protection
- Costs
- Basic security measures
- Threat analysis
- Impact analysis

Threat Analysis & Hacking Methodology

- Target profiling
- Physical security
- Social engineering
- bridges
- Packet analysis
- Information theft
- Malicious data insertion
- Denial of Service (DoS)
- Peer-to-peer hacking
- Unauthorized control

Rudimentary Security Measures

- SSID
- MAC filters
- Static WEP
- Default configurations
- Firmware upgrades
- Physical security
- Periodic inventory

1hrs Lecture 0hr Labs
Intermediate Security Measures

- Rogue equipment
- Cell sizing
- Protocol filters
- SNMP
- Discovery protocols
- segment configuration
- Remove vulnerabilities
- Client security
- IP Services

Lesson Plan 4
Advanced Security Measures

- security policy
- Authentication & encryption
- DMZ and VLANs
- Audits
- Traffic pattern analysis
- Authenticated DHCP

LAN Auditing Tools

- Discovery tools
- Password crackers
- Share enumerators
- Network management and control
- protocol analyzers
- Manufacturer defaults
- Password sniffers
- Antennas and WLAN equipment
- OS fingerprinting and port scanning
- Application sniffers
- Networking utilities
- Network discovery and management
- Hijacking users
- RF Jamming and Dataflooding tools
- WEP crackers
- Auditing tools
- Information gathering
- Unauthorized access
- Denial of service

Lab exercises

Packet analysis & spoofing
Rouge hardware & default settings
RF Jamming & data flooding

Lesson Plan5
Hardware & Software Solutions

- RADIUS with AAA Support
- RADIUS Details
- Kerberos
- Static and Dynamic WEP and TKIP
- 802.1x
- Extensible Authentication Protocol (EAP)
- VPNs
- Encryption Schemes
- Routers
- Switch-Routers
- Firewalls
- MobileIP VPN Solutions
- Enterprise Gateways
- Switches, VLANs, & Hubs
- SSH2 Tunneling & Port Redirection
- Thin Client Solutions

Prevention & Countermeasures

- 802.1x
- 802.11i
- TKIP
- AES
- Intrusion detection
- US Federal and state laws

Implementation and Management

- Design and implementation
- Equipment configuration and placement
- Interoperability and layering
- Security management

Exam Online w/ penetration test

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books – Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking.

SU Q/WP® Qualified Professional Certificate Program of Mastery CPoM non degree (3 Q/WP® - Q/WP, Q/WSP, (or Q/WP- Q/WSP classes) Q/WAD + Security+®, SecurityX®)
Q/WAD® Qualified/ Analyst & Defender Certification Class w/exam
Q/ WP® Qualified/ Professional Certification Class w/exam
Q/WSP® Qualified/ Security Professional Certification Class w/exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Wireless Professional / Qualified Security Professional Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX® Certification Class w/exam
PMP Project Manager Professional Certification Class*
Q/WLANPD Qualified/ Local Area Network Planning & Design Class w/exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing Class w/exam
Q/WDNO Qualified/ Deceptive Network Optimization Class w/exam

QWAD QUALIFIED/ WIRELESS ANALYST AND DEFENDER PRACTICUM

In this 72 hr practicum, students validate their advanced Wireless analyst skills with a framework provided by the instructor. Students prepare an entire multi-user network with branch locations and offices in 12 cities. Student will secure wireless architecture of the 802.11 standards, and then apply that base of knowledge to how and when to use the tools that are available for analyzing and troubleshooting today's WLANs. The Q/WAD certified individual will be able to confidently analyze and troubleshoot any LAN system using any of the market leading software and hardware analysis and write the report.

Practicum Duration: 72 hours of hands on validating their wireless skills using the latest enterprise LAN security and auditing equipment, addressing in detail LAN Intrusion, Security Policy and Solutions.

Q/WP Qualified/ Professional Certificate Program of Mastery

Q/WP®/ Q/WSP® BOOTCAMP CLASS [QUALIFIED WIRELESS / QUALIFIED WIRELESS SECURITY PROFESSIONAL CERTIFICATION CLASSES] W/EXAM

Hands On

Q/WAD QUALIFIED/ WIRELESS ANALYST & DEFENDER Security University

(144 hours class)

This SU course targets experienced networking professionals who wish to gain critical skills in networking security, including how hackers attack networks and the means for preventing them from doing so. This multi- course prepares you for the Q/WP & Q/WSP exams and CWNA™ & CWSP™ Exams.

SU's Qualified Wireless Professional & Wireless Security Professional class consists of hands on learning using the latest enterprise LAN security and auditing equipment. This 144 hour class drills into LAN Administration and Security course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with LANs today, and every class and type of WLAN security solution available on the market - from intrusion prevention systems to network management systems.

IT professionals must become knowledgeable about wireless security. This class teaches students the necessary skills for implementing and managing wireless security in the enterprise by creating layer2 and layer3 hardware and software solutions with tools from industry leading manufacturers.

This hands-on, defense in-depth class has 15+ labs to give you the chance to use wireless products to secure networks. Our expert instructors take you through everything you need to know to do a proper site survey, design and implement a WLAN and will advance into the crucial aspects of hacking and testing vulnerabilities on your networks showing you security threats and weaknesses of LANs. Top analysis tool labs. Q/WP™ is the top ranking Hands-on Professional Certification today. A vendor-neutral certification that requires mastery of fundamentals. By earning both the Q/WP™ & Q/WSP™ credentials, network engineers and administrators demonstrate that they have the skills necessary to administer, install, configure and troubleshoot network systems.

Class Fee:	$6,990 for both classes
Time:	144 hrs
Learning Level:	Entry
Contact Hours:	2 wks 40 hrs 64 hr pre-study & 2 hr exams
Prerequisites:	Understanding of TCP/IP
Credits:	Protocols 144 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality. [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Titles
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/Network Analyst
Network Security Engineer/Network Security Specialist
Security Analyst/ Security Engineer
Security Specialist/ Systems Security Engineer

Learning objectives

- Ownership concepts
- security policy creation and alignment
- design and control methods
- Return on investment strategies and methods
- Automated tools and management strategies

KU Outcomes * Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

Lesson Plan 40hr:

12.
Introduction to 802.11 LANS

- 12.1. Standards organizations responsible for shaping the 802.11 Lan Protocol
- 12.2. How Standards compliance is enforced for 802.11 WLAN vendors
- 12.3. Examine the 802.11 standard and various amendments
- 12.4. Discuss additional networking standards that are commonly used to enhacnce 802.11 WLAN

13.
Radio Frequency Fundamentals

- 13.1. Physical Aspects of RF propagation
- 13.2. Types of losses and attenuation that affect RF communications
- 13.3. Types of modulation used for communications
- 13.4. How channels and bandwidth are related to each other in networks
- 13.5. Three types of Spread Spectrum used in networking
- 13.6. RF Math Calculations
- 13.6.1. RF Units of measure
- 13.6.2. Basic RF Mathematics
- 13.6.3. RF signal measurements
- 13.6.4. Understand link budgets
- 13.6.5. Define and calculate system operating margin (SOM)

14. 802.11 Service Sets

- 14.1. Explain three types of service sets defined for use within 802.11 WLANs
- 14.2. Roaming within a WLAN
- 14.3. Load Balancing as a method to improve congestion in WLANs

15. RF Power Output Regulations

- 16.1. Understand international, regional, and local RF spectrum management organizations
- 16.2. Understand RF channels in the unlicensed 2.4 GHz and 5 GHz frequency ranges

17.
Power over Ethernet

- 17.1. Recognize the two types of devices used in Power over Ethernet (PoE)
- 17.2. Recognize the differences between the tow types of Power Sourcing Equipment (PSE)
- 17.3. Understand the two ways in which power can be delivered using PoE
- 17.4. Understand the importance of planning to maximize the efficiency of PoE

18.
Spectrum Technologies

- 18.1. Uses of Spread Spectrum
- 18.2. Frequency Hopping
- 18.3. Direct Sequencing
- 18.4. Comparing DSSS to FHSS
- 18.5. Co-location and Throughput Analysis

19.
LAN Operation

- 19.1. Ad Hoc networks
- 19.2. Infrastructure networks
- 19.3. Bridged Networks
- 19.4. Repeater Networks
- 19.5. Mesh Networks
- 19.6. WLAN Switched networks
- 19.7. Enterprise Gateway networks
- 19.8. Enterprise Encryption Gateway networks
- 19.9. Virtual AP networks
- 19.10. Evolution of WLAN architectures
- 19.11. WLAN management

20.
LAN Security

- 20.1. Security Policy and Procedures
- 20.2. Legacy 802.11 Security Components
- 20.3. 802.11i Security Components
- 20.4. WPA – personal
- 20.5. WPA – Enterprise
- 20.6. WPA 2 – personal
- 20.7. WPA2 - Enterprise
- 20.8. Types of Network Attacks
- 20.9. Baseline Security Practices (SOHO, SMB, Enterprise)

21.
802.11 Analysis and Troubleshooting

- 21.1. Introduction to 802.11 Protocol Analysis
- 21.2. 802.11 Data Frames
- 21.3. 802.11 Control Frames
- 21.4. 802.11 Management Frames
- 21.5. Frame Fragmentation
- 21.6. Power Saving Operations
- 21.7. Transmission Rates

22.
Coordinating 802.11 Frame Transmission

- 22.1. Differences between CSMA/CD and CSMA/CA
- 22.2. Distributed Coordination Function (DCF)
- 22.3. Quality of Service in 802.11 WLANS

23.
Antennas

- 23.1. Antenna characteristics and behaviors

Q/WP Qualified/ Professional Certificate Program of Mastery

Q/WLANPD QUALIFIED / WIRELESS LOCAL AREA NETWORK PLANNING AND DESIGN PRACTITIONER

This class aims to provide students with fundamental knowledge into core concepts of the latest and next generation mobile and wireless networks. Throughout the course, students will be exposed to theoretical and practical aspects regarding the architecture and applications of Cellular, LTE, and 4G/5G systems. In addition, basic concepts of Wireless LAN (WLAN), Mobile Peer-to-Peer (MP2P), wireless sensor networks (WSN) and emerging opportunistically connected mobile/ vehicular networks (MANET and VANET), will be explored.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-stud & 2hr exam
Prerequisites:	TCP/IPknowedge
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass Attendance, Completion of Labs & quizzes Fail > 95% Attendance

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider
Cybersecurity Officer/Enterprise Security Officer
Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect /Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer.

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final Exam - passing the final exam is a requirement for graduation.

Introduction

The Q/WLANDP Wireless LAN Design course consists of instructor-led training applicable to the design of wireless LANs using the latest technologies including 802.11n and 802.11ac. The course goes in-depth into the design process and provides attendees with the knowledge needed to plan, deploy and test modern 802.11-based networks. It also prepares students for the Q/WLANDP examination. Students who complete the course will acquire the necessary skills for preparing, planning performing and documenting site surveys and wireless LAN design procedures.

Course Outline- The following list contains the materials covered in the lecture portion of the course.

WLAN Design Overview

LESSON 1.

- Importance of good design
- Impact of bad design
- Design process
- Design skills
- Design toolkit
- Pre-planning
- Customer interaction
- Requirements gathering

Lesson 2

- Discovering existing systems
- Documenting the environment
- Defining constraints
- Creating documentation
- Client device types
- Application types
- Application-specific design
- High density design issues
- Standard corporate networks

Lesson 3 2 hr labs 1 lecture

Industry-specific designs

- Government
- Healthcare
- Hospitality
- Education
- Retail
- Public hotspots
- Transportation
- Mobile offices

Lesson 4

Outdoor and mesh

- Remote networks and branch offices
- Last-mile/ISP and bridging
- Defining vendor issues
- Operational planes
- Design models
- Understanding architecture differences
- RF spectrum
- RF behaviors
- Modulation and coding schemes
- RF accessories
- Throughput factors
- Antennas

23.2. Types of antennas commonly used with WLANS
23.3. Advances Antenna Systems
23.4. Antenna Placement and mounting
23.5. Antenna Safety
23.6. Types of antenna cables, connectors and accessories

24.

Site Surveying

24.1. Understanding the need for a site survey
24.2. Defining Business Requirements and justification
24.3. Facility Analysis
24.4. Interviewing Network Management and users
24.5. Identifying Bandwidth Requirements
24.6. Determining contours of RF coverage
24.7. Documenting installation problems
24.19.
24.8. Locating Interference
24.9. Reporting Methodology and procedures
24.10. Understanding specifics of each vertical market
24.11. Understanding the customers network topology
24.12. Creating appropriate documentation during and after the site survey
24.13. Understanding Safety Hazards
24.14. Using appropriate hardware and software to perform the survey
24.15. Understand the need for spectrum analysis
24.16. Manual RF site surveys
24.17. Predictive site Surveys
24.18. Dense AP deployment

Qualified/ Security Professional

Certification Q/WP002 QUALIFIED/ SECURITY PROFESSIONAL

Hands On

This course targets experienced networking professionals who wish to gain critical skills in networking security, including how hackers attack networks and the means for preventing them from doing so.

Class Duration**: The class consists of 72 hours of hands on learning using the latest enterprise LAN security and auditing equipment. This class addresses in detail LAN Intrusion, Security Policy, and Security Solutions.**

Learning Objectives:

- Security concepts
- security policy creation and alignment
- Security design and control methods
- Return on investment strategies and methods
- Automated tools and management strategies

Who Should Attend:

Information Security Officers, Information Systems Managers, Telecommunications and Network Administrators and Engineers, Consultants, Systems and Data Security Analysts, Compliance Officers, Chief Security Officers, and others concerned with security

Lesson Plan:

All attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 security solutions using hardware and software from the following vendors:

KU Outcomes
* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
* Students will be able to plan, organize and perform penetration testing on a simple network.
* Students will be able to analyze system components and determine how they will interact in a composed system.
* Students will be able to analyze a system design and determine if the design will meet the system security requirements

The LAN Security course is 72 hours of instructor-led study, incorporating both lecture and hands-on labs. The lab exercises consume more than 80% of the class time, providing thorough hands-on training and escalating technical workshops for all attendees.

Certification: This course may be used - and is the ideal track - for preparing students for the QUALIFIED Security Professional™ exam (exam # PW0-200), which is delivered at all Prometric Testing Centers worldwide. The Q/WSP certification is the first vendor neutral security certification that focuses solely on testing the IT professional's knowledge of securing enterprise LAN solutions.

Prerequisites: Understanding of TCP/IP Protocols is required prior to taking the Q/WSP exam. It is *recommended* students have experience in a network security related field prior to enrolling in the course.

Hands-on Lab Exercises: These are the actual labs taught in the LAN Security Course:

- Packet Analysis & Spoofing
- Scalable VPN Solutions
- EAP - Cisco (LEAP)

- Rogue Hardware & Default Settings
- RF Jamming & Data Flooding
- Information Theft
- Hijacking and DoS Attacks
- Access Point VPNs
- Layered Security
- Bridging Security
- 802.1x and EAP-TTLS
- SSH2 Tunneling & Local Port Redirection

The LAN Security course consists of hands on learning using the latest enterprise LAN security and auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, functionality of standard, the inner-workings of LANs to WLAN security solutions, to intrusion prevention systems and network mgt systems.

Lesson 1
WLAN Intrusion
Intrusion Tools
Intrusion Techniques
LAB – WLAN Intrusion Tools and Techniques
Physical Security
Controlled Physical access to premises and infrastructure
Social Engineering
Policy Adherence
Proper use of Security Solutions
MAC Layer Security
Use of VLANs for layer-2 segmentation in WLANs
PrE-shared key security solutions
802.1X/EAP framework and security solutions
Extensible Authentication Protocol (EAP) framework and comparisons
Detailed discussion of each EAP type used in today's WLANs including in-dedpth frame exchange graphics
Wi-Fi Protected Areas
802.11i terms, framework, and in-depth operational explanations
802.11i/RSN functional graphics and frame capture explanations
Explanations of how 02.1X/EAP solutions changed to 802.11i/RSN solutions
802.11i frame format explanations and graphics
The 802.11i amendment
IP Security – Network Layer Security PPTP VPN
IP Frameswoark and implementation discussion in detail
LAB – 802.1X/EAP & VLAN based Security Solutions

Lesson 2
Hardware and Software Solutions
"Fat" access points
WLAN switches/controllers
WLAN bridges
SOHO/SMB solutions
Enterprise Encryption Gateways (EEGs)
Enterprise Gateways (EWGs)
WLAN routers
WLAN Network Management Systems (WNMS)
WLAN mesh routers
WLAN Intrusion Detection/Prevention Systems (WIDS/WIPS)
Lab Exercises
  Secure WLAN Bridging
  WLAN Switching
  Enterprise Encryption Gateways (EEGS)
  Enterprise W ireless Gateways (EWGs)
  SOHO?SMB solutions
  WLAN Routers
Lesson 3
Application Security
Secure Shell (SSH1/SSH2) as a terminal application and VPN solution
SSLv3/TLSv1 for E-mail, FTP, and web browsing
SNMPv3 for authenticated and encrypted network management
Authentication, Authorization, and Accounting (AAA) Systems
Local Authentication in APs, EWGs, WLAN switches, and WLAN routers
RADIUS & Kerberos authentication and proxy services
LDAP authentication
Per-user and per-Group authorization options
Role Based access control (RBAC)
Bandwidth management

Lesson 4
IDS Solutions- Protocol Analyzers
Hardware and software types available
Performance and security analysis
Connectivity Troubleshooting
Channel/spectral monitoring
Distributed analysis with WIDS
Three Types of WIDS – explanation of each
LAB Exercises
WLAN Network Management Systems
WLAN Intrusion Detection Systems

802.11n and antennas
Choosing APs
Powering APs

Lesson 5
Site survey tools
Site survey preparation
Predictive site surveys
Manual site surveys
Site survey principles and processes
Quality of Service (QoS) overview
QoS application points
Roaming support

Lesson 6
Bad security
Authentication solutions
Encryption solutions
Security best practices
Intrusion prevention
Network health status
Troubleshooting and validation process
Troubleshooting and validation tools
Common problems

Lesson 7
Requirements Analysis
Designing for Clients and Applications
Designing for Industry
Vendor Selection Processes

Lesson 8
Radio Frequency Planning
WLAN Hardware Selection

Lesson 9
Site Surveys
Designing for QoS
Designing for Security
Installation Testing, Validation and Troubleshooting
Design Troubleshooting

Lesson 10
Case Studies are for groups to explore concepts learned in the lecture materials. Potential case studies include:

Designing for future capacity
Designing in a moderate interference environment
Designing multiple SSID networks

Lesson 11 Dynamic Hands-on Lab Exercises
Trainers may include hands-on lab time using any or all of the following tools:

Spectrum analyzer
Protocol analyzer
Site survey software
Diagramming software
Various wireless adapters and antennas
Various wireless AP

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.
Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/WP Qualified/ Wireless Professional Certificate Program of Mastery

Q/WDNO QUALIFIED/ WIRELESS DECEPTIVE NETWORK OPTIMIZATION CLASS W/EXAM

Getting wireless certified with Security University shows your Qualified.

The IDC estimates that there would be 152,200 IoT devices connected every minute by 2025, indicating that there would be about 80 billion IoT devices connected annually. While IoT devices have numerous benefits and are immensely helpful for different purposes, they also pose as attractive vulnerabilities for cybercriminals. Be it insecure passwords, networks, ecosystem interfaces or any other vulnerability and weakness, once an IoT device is compromised, it can lead to major losses for any organization, and not just financially.

Questions & Quizzes /Full practice test

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	TCP/IP Knowledge
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance, Labs and quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title

Network security engineers
Cybersecurity analysts
Network and security analysts
Full stack engineers
Information system security architects
Network security administrators
Product security analysts
IT security analysts
Security test engineers
Application security testers/analysts
Security delivery analysts, etc.

This class is about security testing and attack surface management to teach wireless Penetration Testing using a penetration testing and vulnerability management methodology. Its experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces, historically testing over 1 million assets to find 4 million unique vulnerabilities. This IoT security class also incorporates hands-on practical exercises for a thorough experiential and practical learning experience to the participants.

The course aims to cover the following:

Introduction to Wireless IoT security
Introduction to basic IoT
Terminology and initiatives
Device security and gateway security
Communication protocols
IoT cloud platforms and their security
IoT ecosystem and penetration testing approaches
Attack and fault trees
Threat modelling IoT systems, applications and hardware
IoT testing and security automation
IoT hacking

This course is highly recommended for current and aspiring:
IoT Exam Prep Daily Schedule

- **Lesson 1 -** Domain 4: IoT testing and security automation
- **Lesson 2** - Domain 1: Introduction to Wireless IoT security
- **Lesson 3 -** Domain 2: Attack and fault tree
- **Lesson 4 -** Domain 3: IoT ecosystem and penetration testing approaches
- **Lesson 5** Domain 5: IoT hacking
- **Lesson 6** Domain 6: Privacy and Security

- **Lesson 7** Domain 7: IoT Pen Testing

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Q/WP Qualified/ Wireless Professional Certificate Program of Mastery

Q/WNST QUALIFIED/ WIRELESS NETWORK AND IOT SECURITY TESTING CLASS W/EXAM

Getting wireless certified with Security University shows your Qualified.

The IDC estimates that there would be 152,200 IoT devices connected every minute by 2025, indicating that there would be about 80 billion IoT devices connected annually. While IoT devices have numerous benefits and are immensely helpful for different purposes, they also pose as attractive vulnerabilities for cybercriminals. Be it insecure passwords, networks, ecosystem interfaces or any other vulnerability and weakness, once an IoT device is compromised, it can lead to major losses for any organization, and not just financially.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	TCP/IP Knowledge
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance, Labs and quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Title

Network security engineers
Cybersecurity analysts
Network and security analysts
Full stack engineers
Information system security architects
Network security administrators
Product security analysts
IT security analysts
Security test engineers
Application security testers/analysts
Security delivery analysts, etc.

To the leader in enterprise penetration testing and attack surface management, today announced the launch of its IoT penetration testing services, which will be added to its existing suite of penetration, adversary simulation, and attack surface management capabilities. With the stark growth of IoT adoption over the past few years, pentesting is now a critical asset for companies to understand and assess the overall strength and accountability of their internet-connected systems against sophisticated and targeted cyber attacks.

This class teaches the following capabilities:

ATM Penetration Testing. Identify the security issues and common vulnerabilities on relevant ATM systems and provide actionable recommendations for improving the overall security posture. Learn more about ATM pentesting.
Automotive Penetration Testing. Identify security issues on relevant vehicles and provide recommendations to improve the current systems – at any stage of automotive development. Learn more about automotive pentesting.
Medical Device Penetration Testing. Through a combination of threat modeling and penetration testing, determine possible medical device security risks and identify whether devices meet or exceed the current standards and recommendations by the FDA Premarket Cybersecurity Guidelines. Learn more about medical device pentesting.
Operational Technology (OT) Architecture and Security Review. Identify industrial control system (ICS) vulnerabilities with a focus on the OT processes in a Defense in Depth strategy. Students will investigate the configuration and architecture of the systems and help address issues with asset inventory, network configuration, and segmentation. Learn more about OT architecture and security review. Embedded Penetration Testing. Identify embedded system vulnerabilities in a multitiered penetration test across multiple disciplines. Look for security gaps at all stages of embedded development that may affect each layer of the device. Learn more about embedded pentesting.

“IoT has become part of our daily lives, but these devices and systems are often overlooked from a security perspective. Tapping into our innovation-driven culture and our best-in-class technologies. This pentesting testing class is uniquely qualified to find and help fix the most critical security gaps in these systems,” to future-proofing IoT security worldwide.” To keep up with the growth of IoT and assist with the complexity in this space. There is currently a gap in the market to effectively monitor and assess the risks of these devices. This IoT security class also incorporates hands-on practicum exercises for a thorough experiential and practicum learning experience to the participants.

The course aims to cover the following:
Red Team Operations & Attack Surface Management
Simulated attacks through a red team engagement enhance your information security program. Red team operations put your organization's security controls, security policies, incident response, and cyber security training to the test. Attack Surface Management detects known, unknown, and potentially vulnerable public-facing assets, as well as changes to your attack surface that may introduce risk. How? Through a combination of powerful Attack Surface Management (ASM) technology platform, penetration testing experts, and 20+ years of pentesting expertise.

This course is highly recommended for system admins and pen testers:

- **Lesson 1 -** Red Team simulations & Operation Models
- **Lesson 2**- Assumed breach | Black box testing
- **Lesson 3 –** Identify and respond to threats RED TEAM OPS
- **Lesson 4** Attack Surface Management
- **Lesson 5** Identify and protect the unknown
- **Lesson 6** Continuous Penetration Testing
- **Lesson 7** Manual Exposure Triaging
- **Lesson 8** Asset Discovery with Attack Surface Monitoring
- **Lesson 9** Asset Intelligence
- **Lesson 10** High Risk Port Discovery

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Security Awareness Curriculum

- Policy
- Passwords
- Computer Viruses
- Malicious Code
- Phishing
- Incident Response
- Personal Use and Gain
- Intrusion Detection
- Data Backup and Storage
- Inventory Control
- Physical Security
- Social Engineering

We guarantee your staff will flood you with real corporate security concerns when the session is over!
Act now to manage your weakest security link into your greatest security asset. Reduce your corporate risk by training your managers and users by changing their behavior and create an organizational culture of security by empowering your users with security awareness knowledge. Customize your computer security training to meet computer security awareness and compliance or increase the overall "security awareness" in your company, for a small fee attached to your training class.

Our instructors are passionate about security! Give us your staff and managers for a computer security awareness "eyeful" that will have them reacting to unsecured client sensitive documentation, stopping unknown visitors in the hallways, and be more enthusiastic about protecting your corporate assets. Customized "takeaways" for your employees to practice safe internet security at home for secure remote access to protect your corporate assets. *Internet Security and Awareness Training quotes from recent sessions:*
" the first 4 hours had me sqirming in my seat about how much I did not know" Heath Care IS Director

" Valuable information! Too much information in one day. I walked away with 3 pages of questions to ask my teams". CISO Financial

This Internet Security and Awareness threat workshop motivated me to provide an onsite for my team. There are so many changes we need to make, especially about the threat of trojans and rougues" Alaska Health Care Director

Grades -All students must ordinarily take all quizzes, labs, final exam, and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Computer Viruses
Data Backup and Storage
Incident Response
Personal Use and Gain
Environmental
Inventory Control
Physical Security
Social Engineering

We guarantee your staff will flood you with real corporate security concerns when the session is over!

Act now to turn your weakest security link into your greatest security asset. Reduce your corporate risk by training your users and changing their behavior and create an organizational culture of security by empowering your users with knowledge.
Internet Security and Awareness Training. Customize your computer security training to meet computer security awareness and compliance or increase the overall "security awareness" in your company.
Our instructors are passionate about security! Give us your staff and managers for a computer security awareness "eyeful" that will have them reacting to unsecured client sensitive documentation, stopping unknown visitors in the hallways, and be more enthusiastic about protecting your corporate assets.
Security awareness training specially crafted for Executives, IT managers, security professionals, system administrators and risk managers that educates you about "what" questions to ask to direct and support successful enterprise computer security programs.

Grades -All students must ordinarily take all quizzes, labs, final exam, and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Q/WP Qualified/ Professional Certificate Program of Mastery

Q/WLANPD QUALIFIED/ LOCAL AREA NETWORK NETWORK PLANNING CLASS AND DESIGN W/EXAM

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Title
Information Systems Security Engineer
Intrusion Detection System (IDS) Administrator
Intrusion Detection System (IDS) Engineer
Intrusion Detection System (IDS) Technician
Network Administrator/ Network Analyst
Network Security Engineer
Network Security Specialist
Security Analyst/ Security Engineer
Security Specialist/ Systems Security Engineer

This accelerated class is taught using face to face modality or hybrid modality. [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Introduction - The Enterprise Wi-Fi Fundamentals v1.0 course provides the networking professional a foundation of knowledge for entering into or advancing within the networking industry. From basic RF theory and regulatory requirements to implementation of WLAN devices, this course focuses on bringing Wi-Fi sales and support professionals up-to-speed on the latest in 802.11 technologies in a practicum way. 50 hours of labs.

KU Outcomes
** Students will be able to plan, organize and perform penetration testing on a simple network.*
** Students will be able to analyze system components and determine how they will interact in a composed system.*
** Students will be able to analyze a system design and determine if the design will meet the system security requirements*

Audience: Wi-Fi sales professionals, project managers, networkers new to Wi-Fi **Prerequisites**: None

Introduction to Networking
Understanding Network Models
Understanding Protocols
SDUPDU
OSI – The de facto reference model
The seven layer model
Equipment per layer
Mapping other protocols into the OSI model
TCP/IP – four layer model

Wi-Fi Organizations and Standards

- Regulatory Bodies
- IEEE
- Wi-Fi Alliance
- WLAN Connectivity
- WLAN Security
- WLAN QoS & Power-Save
- IEEE 802.11 Standards,
- Amendments, and Drafts
- 802.11-2007
- 802.11a/b/g
- 802.11e/h/i
- 802.11n Draft

Wi-Fi Hardware & Software

- Access Points
- Lightweight
- Autonomous
- WLAN Routers
- WLAN Bridges
- WLAN Repeaters
- WLAN Controllers/Switches
- Direct-connect APs
- Distributed-connect APs
- PoE Infrastructure
- Midspan
- Endpoint
- Client hardware and software
- Antenna types and uses

Wi-Fi Security & Compliance

- 802.11 Legacy Security Methods
- Encryption – TKIP/CCMP
- Authentication Passphrases & 802.1X/EAP
- WPA/WPA2-Personal
- WPA/WPA2-Enterprise
- WPS Pushbutton/ PIN

- RolE-Based Access Control (RBAC)
- VPN Security
- Intrusion
- Protection Systems (WIPS)
- PCI Compliance
- HIPAA Compliance
- Enforcing Compliance

Wi-Fi Site Surveying

- Information gathering and reporting
- Multiple Channel Architecture (MCA) cell planning basics
- Single Channel Architecture (SCA) cell planning basics
- Predictive Site Survey
- Manual Site Survey
- Passive Survey
- Active Survey
- Mesh Access Layers
- Use of Analyzers
- Protocol
- Survey
- Spectrum
- Identifying and locating RF interference sources
- Wi-Fi vs. Non-Wi-Fi
- Hardware placement limitations
- Best practices for antenna use

Wi-Fi Operational Concepts

- Range, coverage, and capacity
- Frequencies/channels used
- Channel reuse and co-location
- Active and passive scanning
- Power saving operation
- Data rates and throughput
- Dynamic rate selection
- Authentication and association
- The distribution system and roaming
- Infrastructure and ad hoc modes
- BSSID and ESSID
- Protection mechanisms

Applications, Support, & Troubleshooting

- Installation/configuration of common network types
- Small Office / Home Office (SOHO)
- Extension of existing networks into remote locations
- Building-to-building connectivity
- Public hotspots
- Mobile office, classroom, industrial, and healthcare
- Municipal and law-enforcement connectivity
- Corporate data access and end-user mobility
- Last-mile data delivery (WISP)
- Transportation networks
- Recognize and troubleshoot network problems
- Decreased throughput
- Intermittent or no connectivity
- Weak signal strength
- Device upgrades
- Wi-Fi Network Optimization Procedures
- Infrastructure hardware selection and placement
- Identifying, locating, and removing sources of interference
- Client load-balancing
- Analyzing infrastructure capacity and utilization
- Multipath and hidden nodes

Radio Frequency (RF) Fundamentals

- Units of RF measurements
- Factors affecting network range and speed
- Environment
- LinE-of-sight
- Interference
- Defining differences between physical layers
- OFDM
- HR/DSSS
- MIMO

Spread Spectrum Concepts

- OFDM & HR/DSSS channels
- Co-location of HR/DSSS and OFDM systems
- Adjacent-channel and co-channel interference
- WLAN / WPAN co-existence
- CSMA/CA operation half duplex

RF Antenna Concepts

- Passive gain
- Beam widths
- Simple diversity
- Polarization
- Antenna Mounting
- Pole/mast mount
- Ceiling mount
- Wall mount
- WLAN Accessories
- RF cables
- RF connectors
- Lightning arrestors and grounding rods

Classroom Demonstrations

AP/Client Connectivity with WPA2-Personal Security and PoE Power, Spectrum Analysis of RF Environment ,Protocol Analysis of RF Environment, Configuration Parameter Modification in an EnterprisE-Class Autonomous AP.

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/SSE® QUALIFIED SW/SECURITY EXPERT CLASS W/ EXAM

Hands On

SU Q/SSE® Qualified/ Software Security Expert Certification Certificate Program of Mastery CoM nondegree (9 Q/SSE classes + Security+, SecurityX)
Q/SSE® Qualified/ Software Security Expert Certification Class w/exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class w/exam
Q/STP® Qualified Software Testing Certification Class w/exam
How to Break & FIX Web Security Certification Class w/exam
How to Break & FIX Software Security Certification Class w/exam
Fundamentals of Secure Software Programming Certification Class w/exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class w/exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class w/exam
Introduction to Reverse Engineering Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
Q/SSE® Qualified/ Software Security Expert Practicum
Introduction to Reverse Engineering Practicum
Q/SH/D® Qualified/ Software Hacker / Defender Practicum

Everyone whether they write protocols or internal processes is responsible for using secure programming techniques to minimize the adverse effects of attacks, test the code for software security and know how to fix the software for security.

This 5 part, 40 hr 1 wk + 32 hr pre-study class delivers the best of all the Software Security classes and more. It includes items that are classed as defensive in nature (e.g. checking error return codes before using handles and other data structures that should have been created, or protecting against using a pointer after it has been released). It also includes items how to prevent attacks and lastly a step by step process to FIX software and lastly provides Solutions and Counter Measures to protect your code.

Class Fee:	$3,990
Learning Level:	Entry
Time:	72 hrs
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality.

Sample Job Titles
Analyst Programmer/Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/ Security Engineer
Software Developer/ Software Engineer
Architect Systems Analyst/ Web App Developer

[excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 40 hr 1 wk + 32 hr pre-study contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Class Materials *Class handbook, lab, SU resource and attack handouts*

Who Should Attend

Software testers, software developers, development and test managers, security auditors and anyone involved in software production for resale or internal use will find it valuable. Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants Q& A Specialists. Secure Software Engineering – Develops, modifies, enhances, and sustains new or existing computer applications, software, or utility programs following software assurance best practices throughout the software lifecycle.

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.

Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Tools for class- Whois, Google Hacking, Nslookup, Sam Spade, Traceroute, NMap, HTTrack, Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat, John the ripper, Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe), LCP, Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact, Snort , Infostego, Etherape, Firefox with plugins (Hackbar, XSSme) , webgoat, Ounce, Foritfy, X Wget, Cyrpto tool, 'Curl'.

KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Lesson Plan **Lesson 1 Part A**
Know your Code
Introduction to Software Security
Common Coding and Design Errors
System-Level
Data Issues
Information Disclosure
On the Wire
Tools

Web Vulnerabilities **.** Web sites
Defensive Coding Principles
Security Testing and Quality Assurance
Each section includes depth hands on lab

Lesson 2 /3 Part B Know your Enemy

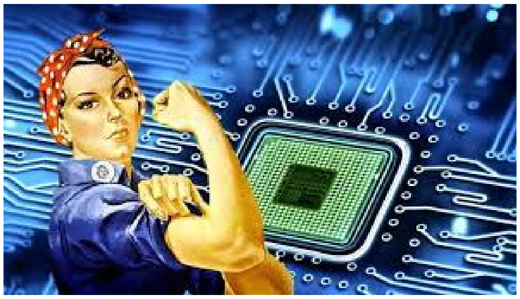
I A step by step methodology and models for effective software testing
II How to develop an insight to find those hard-to-find bugs
III How to test Inputs and Outputs from the User Interface
IV How to test Data and Computation from the User Interface
V How to test the File System Interface
VI How to test the Software/OS Interface
VII How to use tools to inject faults for File System and OS testing

Gathering information on the target
Attacking the client / Attacking State **/**Attacking Data /Attacking the server /Web Services /Privacy Tool
support Hands-on lab attacking a site full of vulnerabilities
Lessons 4 & Part C
Know your Security Solutions

Lesson 5 C
Web Attacks and Counter Measures Methodology
Security Vulnerabilities and Counter Measures
Best Practices

1. System-Level
2. Data Parsing
3. Information Disclosure
4. On the Wire
5. Web sites

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step.



Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/ST® QUALIFIED/SOFTWARE TESTING CLASS W/EXAM

This class is unique in the security industry. As a follow on to the class How to Break and FIX Software Security/
This 40hr 1 wk class is less lecture and more hands on labs. In this class students work on the actual application looking for security vulnerabilities that they are testing day in and day out. The security testing class takes top quality assurance testers into leading security testers with passion, knowledge and experience security testing their application.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practicum	Fail > 95% Attendance
Class Materials:	SU textbook and testing software

Sample Job Titles
Analyst Programmer
Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/Security Engineer SW
Developer Software Engineer /Architect
Systems Analyst/ Web App Developer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who should attend:
Porgramming Managers and your teams. Software testers, software developers, development and test managers, security auditors and anyone involved in software production for resale or internal use will find it valuable. Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists.
KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class - Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, Ounce, Fortiyf, IDA pro Helix, X Wget, Cyrpto tool, 'Curl'

Learning Objectives

- **SSL vulnerabilities and testing**
- **Proper encryption use in web application**
- **Session vulnerabilities and testing**
- **Cross Site Request Forgery**
- **Business logic flaws**
- **Concurrency**
- **Input related flaws and related defense**
- **SQL Injection vulnerabilities, testing and defense**

Lesson Plan
Self Study and Nightly Assignments. Students will need to complete reading and analyze how specific security issues correspond to their area of testing focus of the application.
Lesson 1
Security Briefings. Each morning will start with a briefing on the security issues specific to the application. Application-specific security

testing issues are discussed every morning and then immediately implemented against the application and throughout the day-long deep security testing sessions.

Lesson 2- 5

Application-specific Security Testing . Several days of intense hands-on security testing of the application is performed by the students. The class is broken into two-person teams who compete to find the most security defects by performing specific attacks on the sections of the product they typically perform QA testing.

Corporate Requirements. To achieve the required results, your company needs to provide access to a developer knowledgeable of the entire application, the complete threat model as well as details on past defects discovered in the application. This will enable a strategic attack plan to be created prior to the course that will be discussed and explained during the class.

Additionally, your company needs to make sure the students do all pre-class reading and all nightly assignments. This will be an intense several days of security education and testing that will push each student as they evolve from top quality assurance testers into lead security testers. Prizes should be provided to the students for each security defect discovered with special prizes to the top three teams based on the number and severity of the security bugs they find.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practium in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

SU Q/SSE® Qualified/ Software Security Expert Certification Certificate Program of Mastery CPoM nondegree (9 Q/SSE classes + Security+, SecurityX)
Q/SSE® Qualified/ Software Security Expert Certification Class w/exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class w/exam
Q/STP® Qualified Software Testing Certification Class w/exam
How to Break & FIX Web Security Certification Class w/exam
How to Break & FIX Software Security Certification Class w/exam
Fundamentals of Secure Software Programming Certification Class w/exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class w/exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class w/exam
Introduction to Reverse Engineering Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
Q/SSE® Qualified/ Software Security Expert Practicum
Introduction to Reverse Engineering Practicum
Q/SH/D® Qualified/ Software Hacker / Defender Practicum

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/SSPT® LICENSE QUALIFIED/SW SECURITY PENETRATION TESTER LICENSE W/ EXAM

Hands On

New Rules to Attack Software

This 40 hour 1 wk hands-on class introduces you to "How to penetrate your software," a step by step methodology to effectively and efficiently attack software. You will learn a very applied and non-rigid approach to test software for common bugs. It's a departure from conventional network penetration in which porgrammers prepare a written attack plan and then use it as a script when attacking the software. The class teaches you how to plan attacks "on the fly" by providing you with insight, experience, and a nose for where bugs are hiding. This workshop is presented in an "interwoven" format where each topic has a hands-on component so that you can explore the attacking techniques and software tools using real software.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid TBD
Instructor:	
Class Materials:	SU textbook and testing software
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Titles
Analyst Programmer/Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/Security Engineer
Software Developer/ Software Engineer
Architect/ Systems Analyst/ Web AppDeveloper

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend -Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists, Secure Software Engineering – Develops, modifies, enhances, and sustains new or existing computer applications, software, or utility programs following software assurance best practices throughout the software lifecycle.

KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Learning Objectives:

- A step by step methodology and models for effective software testing
- A plan for on-the-fly testing
- How to develop an insight to find those hard-to-find bugs
- How to attack Inputs and Outputs from the User Interface
- How to attack Data and Computation from the User Interface
- How to attack the File System Interface
- How to attack the Software/OS Interface
- How to use Holodeck Lite to inject faults for File System and OS testing

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class - Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl', Ounce, Fortify.

Lesson Plan 40 hrs

Lesson 1 & 2

I. Introduction Are you a Hacker or a Tester? Learn the difference

- Learn about the three characteristics of good testing
- Where are the bugs? Learn methods to seek the "hidden" ones
- Overview of Fault models

II. Understanding the Environment
Learn the difference between the four interfaces to your application
Why does each environmental interface need to be attacked?
Gain the knowledge regarding the environment so you can find more bugs

III. Software Capabilities
Understand the four capabilities and how they affect you as a tester
Learn how to seek the bugs that destroy the software's capabilities

IV. Software Testing Learn the two most important factors to ensure great testing

V. An Overview of the Methodology of How To Attack Software

What are the four basic capabilities of software?

Learn how to determine which attacks apply to your application.

Understand the secret to structuring your attacks into related scenarios.

Learn how to conduct an attack and recognize success

a.) The User Interface (UI)
What are the four areas within the UI that need to be tested?
Learn how these areas interact and why they can be difficult to test

UI Areas 1 & 2 - The Input and Output Domains Understand the two domains and why they are so important to attack Learn the six input domain attacks and how to apply them

Learn how to test inputs tested individually and in combination

Learn the four output domain attacks and how to apply them

Learn the secret to concentrating on what incorrect results could occur and then find the inputs to force them

UI Area 3 -Stored Data Explore how stored data can become corrupted

Learn how to successfully apply four stored data attacks

UI Area 4- Computation

Understand what computation is happening inside the program

Learn four testing techniques that "get in the way" of the desired computation

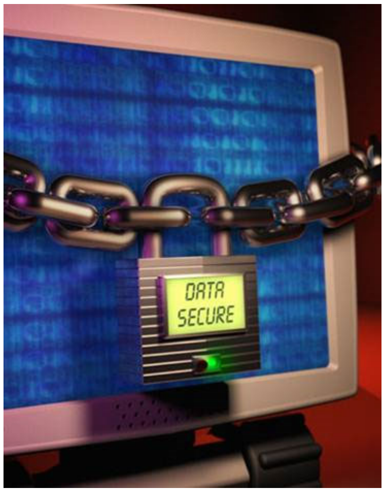
b.) The Kernel Interface
Learn how memory can cause applications to fail
Learn how to effectively test the kernel through "controlled" testing

c.) The File System Interface
Understand how the file system can cause applications to fail
Learn and use two important attacks to evaluate the vulnerabilities in the file system interface

d.) The Software Interface
Understand how reused software can cause applications to fail
Learn and use two important methods to test the software interface

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on FriLesson of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step
Books – 3 Ebooks are provided for this course. No external books are required. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.
Those Less Comfortable – Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick ngebretson (Jun 24, 2013) The book below is recommended for those interested in understanding how their own computers work for personal systems. This last book below is recommended for aspiring hackers, those interested in programming techniques and low-level optimization of code for applications beyond the scope of this course. Hacker's Delight, Second Edition Henry S. Warren Jr. Addison-Wesley, 2012 ISBN 0-321-84268-5

SU Q/SSE® Qualified/ Software Security Expert Certification Certificate Program of Mastery CPoM nondegree (9 Q/SSE classes + Security+, SecurityX)
Q/SSE® Qualified/ Software Security Expert 5 Day Certification Class w/exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class w/exam
Q/STP® Qualified Software Testing Certification Class w/exam
How to Break & FIX Web Security Certification Class w/exam
How to Break & FIX Software Security Certification Class w/exam
Fundamentals of Secure Software Programming Certification Class w/exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class w/exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class w/exam
Introduction to Reverse Engineering Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
Q/SSE® Qualified/ Software Security Expert Practicum
Introduction to Reverse Engineering Practicum
Q/SH/D® Qualified/ Software Hacker / Defender Practicum



Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

HOW TO BREAK AND FIX WEB APPPLICATION SECURITY CLASS W/EXAM

In this 40 hour 1wk class is all about the web as the internet's killer app. Web servers ARE the target of choice for hackers, making them "King of the Internet". 97% of all web applications are vulnerable and better network security isn't the only answer. We will explore a model for web application testing as well as web application concerns including accountability, availability, confidentiality and integrity. We will go well beyond the OWASP 10, looking at 19 specific web application attacks including attacking the client, state, data and the server.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance
Text Materials: Class handbook, lab, SU resource CD's and attack handouts This accelerated class is taught using face to face modality or hybrid modality.
[excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Sample Job Titles
Analyst Programmer/Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/Security Engineer
Software Developer/Software Engineer/Architect
Systems Analyst/Web Application Developer

Who Should Attend -Software testers, software developers, development and test managers, Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists.

Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class - Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, ounce, Fortify, ISS real secure, X Wget, Cyrpto tool, 'Curl'
KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Learning Objectives
Access Control- The student will demonstrate understanding of access control attacks and mitigation strategies, as well as applying the best practice in avoiding access control issues.
AJAX Technologies and Security Strategies - The student will demonstrate an understanding of JavaScript and XML (AJAX) architecture, common attacks against AJAX technologies and best practices for securing applications using AJAX.
Authentication - The student will demonstrate understanding of web authentication, single sign on methods, third party session sharing and common weaknesses, as well as how to develop test strategies, and apply best practices.
Business Logic and Concurrency - The student will demonstrate a general understanding of business logic flaws and concurrency issues in web applications, and how to test for and mitigate against these weaknesses.
Cross Origin Policy Attacks and Mitigation - The student will demonstrate an understanding of methods attackers use to circumvent single origin policy enforcement and best practices for preventing, detecting or mitigating these attacks in web applications.
Cross Site Scripting- The student will demonstrate an understanding of what cross site scripting is and how to use best practices and browser controls to prevent it.
CSRF- The student will demonstrate understanding of the conditions that make a CSRF attack possible, the steps an attacker takes and how to mitigate CSRF attacks.Encryption and Protecting Sensitive Data- The student will demonstrate understanding of how cryptographic components work together to protect web application data in transit and in storage and also when and where to use encryption or tokenization to protect sensitive information.

Incident Detection and Handling - The student will demonstrate an understanding of the controls and processes used to log errors and events, how to mitigate automated bot and spam scripts, and how to detect and respond to incidents in the web application environment. Input Validation and Encoding- The student will demonstrate understanding of the threats related to user inputs of web applications and the strategies and general practice to handle user input properly to mitigate input related attacks. Rich Interface Addon Security - The student will demonstrate an understanding of common Rich InterfaceApplication (RIA) platforms (such as Flash, Silverlight, HTML5), common attacks against these technologies and best practices for securing applications using RIA. Session Management- The student will demonstrate understanding of what sessions are, how to test and mitigate common weaknesses, and how to properly implement session tokens and cookies in a web application. SQL Injection - The student will demonstrate an understanding of what SQL Injection is and how to use best practices to prevent it. Vulnerability Management and Penetration Testing - The student will demonstrate understanding of at a high level the processes for managing vulnerabilities and penetration testing a web application.Web Environment Configuration Hardening - The student will demonstrate an understanding of environmental controls and operational procedures needed to secure servers and services that host web applications. Web Mechanism and Architecture Security- The student will demonstrate understanding of the building blocks of web applications and how components work together to provide HTTP content as well as high level attack trends. Web Services Security- The student will demonstrate an understanding of Service Oriented Architecture (SOA), common attacks against web services components (SOAP, XML, WSDL, etc) and best practices for securing web services.

Lesson Plan

Lesson 1
Gathering information on the target

- How web apps are built
- Attack 1: Looking for information in HTML comments
- Attack 2: Guessing filenames and directories
- Attack 3: Vulnerabilities in example applications

Lesson 2
Attacking the client

- The need for a rich UI
- Attack 4: Selections outside of ranges
- Attack 5: Client side validation

Lesson 3
Attacking State

- Why state is important
- Attack 6: Hidden fields
- Attack 7: cgi parameters
- Attack 8: cookies
- Attack 8: Forceful browsing
- Attack 9: session hijacking

Lesson 4
Attacking Data

- Attack 10: Cross-site scripting
- Attack 11: SQL Injection
- Attack 12: Directory traversal
- Attack 13: Buffer overflows
- Attack 14: Canonicalization
- Attack 15: Null-string attacks

½ Lesson | Attacking
the server

- Attack 17: SQL injection II stored procedures
- Attack 18: Command injection
- Attack 19: fingerprinting the server
- Attack 20: Death by 1,000 cuts (DOS)
- Attack 19: Fake cryptography
- Attack 20: Breaking basic authentication
- Attack 21: Cross Site Tracing

Web Services

- Moving to web services
- Common Attacks
- Constraints on input and output
- Attack 22: web services specific attacks

Privacy

- Who you are, where have you been
- Methods for gathering data

Tool support

- A review of web security/vulnerability scanning tools
- Introduction to HolodeckWeb
  Hands-on lab attacking a site full of vulnerabilities

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

HOW TO BREAK AND FIX SOFTWARE SECURITY W/EXAM

Hands On

This 40 hr 1 wk hands-on class introduces you to "How To Break and FIX Software Security," a step by step methodology to effectively and efficiently test software. You will learn a very applied and non-rigid approach to bang software for common bugs. It's a departure from conventional testing in which testers prepare a written test plan and then use it as a script when testing the software. The class teaches you how to plan tests "on the fly" by providing you with insight, experience, and a nose for where bugs are hiding. This workshop is presented in an "interwoven" format where each topic has a hands-on component so that you can explore the testing techniques using real tools.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance
Text Materials: Class handbook, lab, SU resource & attack handouts

Sample Job Titles
Analyst Programmer/Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/Security Engineer
Software Developer/Software Engineer
Architect/ Systems Analyst/Web App Developer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Who Should Attend -Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists
KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Lesson Plan
Learning Objectives:

- A step by step methodology and models for effective software testing
- A plan for on-the-fly testing
- How to develop an insight to find those hard-to-find bugs
- How to test Inputs and Outputs from the User Interface
- How to test Data and Computation from the User Interface
- How to test the File System Interface
- How to test the Software/OS Interface
- How to use Holodeck Lite to inject faults for File System and OS testing

Take-Home Bonus:
Participants will also receive a copy of How to Break Code, Exploiting Code or a Practical Guide to Testing, a reference book of published testing articles, course notes, checklists, drive containing fault injection software testing tool

Class Lesson Plan
Lesson 1 & Lesson 2 I. Introduction
Are you a Hacker or a Tester? Learn the difference
Learn about the three characteristics of good testing

Where are the bugs? Learn methods to seek the "hidden" ones
Overview of Fault models

II. Understanding the Environment
Learn the difference between the four interfaces to your application
Why does each environmental interface need to be tested?
Gain the knowledge regarding the environment so you can find more bugs
III. Software Capabilities
Understand the four capabilities and how they affect you as a tester
Learn how to seek the bugs that destroy the software's capabilities

Lesson 3 Software Testing Learn the two most important factors to ensure great testing
V. An Overview of the Methodology of How To Break Software
What are the four basic capabilities of software?
Learn how to determine which attacks apply to your application.
Understand the secret to structuring your attacks into related scenarios.
Learn how to conduct an attack and recognize success

Lesson 4
a.) The User Interface (UI) What are the four areas within the UI that need to be tested?
Learn how these areas interact and why they can be difficult to test
UI Areas 1 & 2 - The Input and Output Domains
Understand the two domains and why they are so important to test
Learn the six input domain attacks and how to apply them
Learn how to test inputs tested individually and in combination
Learn the four output domain attacks and how to apply them
Learn the secret to concentrating on what incorrect results could occur and then find the inputs to force them
UI Area 3 -Stored Data Explore how stored data can become corrupted
Learn how to successfully apply four stored data attacks
UI Area 4- Computation
Understand what computation is happening inside the program
Learn four testing techniques that "get in the way" of the desired computation

Lesson 5
b.) The Kernel Interface Learn how memory can cause applications to fail
Learn how to effectively test the kernel through "controlled" testing
1 hrs Lecture
c.) The File System Interface Understand how the file system can cause applications to fail
Learn and use two important attacks to evaluate the vulnerabilities in the file system interface
1 hrs Lecture
d.) The Software Interface Understand how reused software can cause applications to fail
Learn and use two important methods to test the software interface exam using breaking and testing SW.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step
Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. Those Less Comfortable - Hacking for Dummies,
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013)

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

FUNDEMENTAS OF SECURE SOFWARE PROGRAMMING CLASS W/EXAM

Everyone, whether they write protocols or internal processes is responsible for using secure programming techniques to minimize the adverse effects of attacks, whether those attacks are intentional or accidental. If a process deep in the lines of a product crashes because it receives bad data or because a resource that should have been there was not, it is still a crash and reduces the availability. It includes items that are classed as defensive in nature (e.g. checking error return codes before using handles and other data structures that should have been created, or protecting against using a pointer after it has been released). It also includes items that may be more normally associated with cryptographic procedures (e,g. random number generation, encryption algorithms, etc.)

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance + Labs and Practicum Fail > 95% Attendance
Text Materials:	Class handbook, lab, SU resource & attack handouts

Sample Job Titles
Analyst Programmer/ Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
Information Assurance (IA) Engineer
Information Assurance (IA) Software Developer
Information Assurance (IA) Software Engineer
Research & Development Engineer
Secure Software Engineer/Security Engineer
Software Developer/Software Engineer/Architect
Systems Analyst/ Web Application Developer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality] [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Who Should Attend: Software testers, software developers, development and test managers, security auditors and anyone involved in software production for resale or internal use will find it valuable. Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists.
Text Materials: labs, SU Pen Testing & Software testing Materials, resource CD's and attack handouts.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/ Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, IDA pro, Fortify, Web Inspect, X Wget, Cyrpto tool, 'Curl' KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming
Learning Objectives

- Discover the infrastructure within the application
- Identify the machines and operating systems
- SSL configurations and weaknesses
- Explore virtual hosting and its impact on testing
- Learn methods to identify load balancers
- Software configuration discovery
- Explore external information sources
- Google hacking
- Learn tools to spider a Web site
- Scripting to automate Web requests and spidering
- Application flow charting
- Relationship analysis within an application
- JavaScript for the attacker

Lesson Plan

Lesson I Introduction to Software Security

Common Coding and Design Errors
Students will learn about the range of software development errors that create application security, reliability, availability and confidentiality failures. Specifically in this section we will deal with those vulnerabilities that are common across language implementations (C, C++ and Java). For each vulnerability type, the course will cover real-world examples illustrated in code - of failures along with methods to find, fix and prevent each type of flaw.

Lesson 2
System-Level Accepting Arbitrary Files as Parameters; Default or Weak Passwords; Permitting Relative and Default Paths
Offering Administrative, Software and Service Back Doors; Dynamic Linking and Loading; Shells, Scripts and Macros
Data Issues
Parsing Problems
Integer Overflows
Information Disclosure
Storing Passwords in Plain Text
The Swap File and Incomplete Deletes
Creating Temporary Files
Leaving Things in Memory
Weakly-Seeded Keys and Random Number Generation
On the Wire
Trusting the Identity of a Remote Host (Spoofing)
Volunteering Too Much Information
Proprietary Protocols
Loops, Self References and Race Conditions

Tools Lesson 3
II. Web Vulnerabilities . The web is different. We will address common web vulnerabilities, how to find them, how to prevent them.
Web sites Cross Site Scripting; Forceful Browsing; Parameter Tampering; Cookie Poisoning; Trusting SSL; Hidden Field Manipulation; SQL injection; Security on the Client; Trusting the Domain Security Model

Lesson **4**
III. Defensive Coding Principles
This section is designed to educate developers and testers on the general principles of secure coding. This includes a historical perspective on software failure, when good design goes bad, and 18 defensive coding principles to live by.

Lesson 5 –
IV. Security Testing and Quality Assurance
This includes the difference between functional and security testing, understanding and application's entry points, and spotting three classes of security bugs: dangerous inputs, rigged environment and logic vulnerabilities. **Each section will have an in depth hands on lab**

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.
Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932 | Edition: 4 **For Those More Comfortable** The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013)

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/SH/D QUALIFIED SOFTWARE HACKER/DEFENDER CLASS W/EXAM

The true threat: insiders and outsiders. This 72 hour class begins with examples of security breaches, then move to current day exploits and vulnerabilities of real application code. The case studies will illustrate the broad range of threats that organizations face from both external actors as well as insiders. For each attack scenario, we will go through the underlying flaws, exploits, vulnerabilities and consequences.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP protocol
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading:	Pass = Attendance + Labs and Practicum Fail > 95% Attendance
Text Materials:	SU Class handbook, lab, SU resource CD's and attack handouts.

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/Security Engineer
Security Solutions Architect/Systems Engineer/ Systems Security Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend Information Security and IT managers; Information Assurance Programmers; Information Security Analysts and Consultants; Internal Auditors and Audit Consultants; QA Specialists, Systems Security Architecture - Designs and develops system concepts and works on the capabilities phases of the systems development lifecycle. Translates technology and environmental conditions (e.g., laws, regulations, best practices) into system and security designs and processes.
Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation

Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, Web Inspect, Ida Pro, Helix, Wget, Cyrpto tool, 'Curl' software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Learning Objectives

- Explore methods to zombify browsers
- Discuss using zombies to port scan or attack internal networks
- Explore attack frameworks
- AttackAPI
- BeEF
- XSS-Proxy
- Walk through an entire attack scenario
- Exploit the various vulnerabilities discovered
- Leverage the attacks to gain access to the system
- Learn how to pivot our attacks through a Web application
- Understand methods of interacting with a server through SQL injection
- Exploit applications to steal cookies
- Execute commands through Web application vulnerabilities
- Threat Modeling

Lesson 1 and ½ Lesson 2
Examine some trends in software vulnerabilities. Over the years, the industry has seen some distinct trends emerge in vulnerabilities. One of the most interesting is the fact that actors have moved their assaults to the application layer instead of the network layer. This section examines those trends in detail.

Lesson 2 & ½ Lesson 3
Live vulnerability and exploit tour! This is the core of the class. In this section, attendees will go through a wide range of software vulnerabilities and the instructor will show sample exploits for these vulnerabilities live. This tour will span today's most pervasive vulnerabilities including cross-site scripting, SQL injection, buffer overflows, format string vulnerabilities, and many others. Attendees will gain awareness and key insights into these vulnerability types as well as the ease with which the actor community can exploit them.

Lesson 4
Tools and Threats. The threat is growing and so is the number of tools that lower the bar for actors. This section takes the audience inside the underground world of the actor and illustrates the range of tools available to adversaries.

Lesson 5
Thinking Like the Actor: Threat Modeling. A critical step in securing an application or system is to methodically think through threats. In this section we present several techniques for threat modeling and also walk the audience through the process of modeling threats against several systems.

Lesson 6
Incorporating Threats Into Software/System Design, Development, Testing and Deployment. By thinking about threats at each stage of the development lifecycle, we can make software and systems that are more resilient to attack. Attendees will walk away with an introduction to tools and techniques to build security in.
75 question Online exam last day of class

Grades -All students must ordinarily take all quizzes, labs, final exam, and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.
Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932 | Edition: 4 For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Ngebretson (Jun 24, 2013)
The book below is recommended for those interested in understanding how their own computers work for personal edification

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/SSTBT QUALIFIED/ SOFWARE SECURITY TESTER BEST PRACTICES CLASS W/EXAM

How do you find security flaws beyond simple ones like buffer overflows? Most of the current software security testing falls into one of two categories: random corruption of files or network protocols and rE-executing existing, known vulnerabilities against new versions of software. In 72 hours you will learn how hackers find subtle and innovative flaws and exploit them, you need a more methodical, creative process to find them before you do. Learn what it takes to do an application security threat assessment of your software before they go live. You'll develop a comprehensive security test strategy and build a team with the right mix of skills and experience to execute it. Discover approaches for using fault injection to find application security vulnerabilities before your software is exposed to hackers.

Sample Job Titles
Analyst Programmer/ Computer Programmer
Configuration Manager
Database Developer/Engineer/Architect
IA Engineer/ IA Software Developer
IA Software Engineer/ Research & Development Engineer
Secure Software Engineer/Security Engineer
Software Developer/Software Engineer/Architect
Systems Analyst/Web App Developer

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. *Text Materials: SU Class handbook, lab, SU resource CD's and attack handouts.* Students be able to produce software components that satisfy their functional requirements without introducing vulnerabilities

* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming.

Learning Objectives.
Learn how to plan a security testing effort and integrate security testing into your QA process
Learn about risk assessments, test prioritizations and threat modeling
Acquire the skills to recognize and expose the most insidious security vulnerabilities in your applications
Discover tools, techniques and processes to make security an integral part of your release process and to create a security aware culture In your test team.
Learn the many categories of security bugs that may exist in your software and the secrets of application security testing

Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Saint Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,,webgoat, IDA Pro, X Wget, Cyrpto tool, 'Curl' Fority, Ounce.

Who Should Attend? This is a must-have class for functional testers who need to make the transition to finding security bugs. It is also essential for test managers because it teaches the soup to nuts process of security testing and how this type of testing fits in to the overall QA process. Additionally, developers and test managers, security auditors and anyone involved in software production. Attendees gain the skills and techniques to build a security testing team and expose the most insidious application security vulnerabilities.

Lesson Plan

Lesson 1 & ½ Lesson 2
I. Introduction

- Where does security testing fit into the product lifecycle?
- Definition of a security bug.
- The role of a security tester in the organization.
- Overview of security testing elements

Lesson 2
II. Methodology

- Security testing roles
- Threat modeling
- Risk assessments
- Security test planning
- Test team organization and management.
- Reporting

Lesson 3 & 4
III. In-Depth Look at Security Vulnerabilities

each vulnerability will be analyzed for cause, symptoms, prevention and tools to test in software.

1. System
Accepting Arbitrary Files as Parameters
Permitting Relative and Default Paths
Offering Administrative, Software and Service Back Doors
Default or Weak Passwords
Shells, Scripts and Macros
Dynamic Linking and Loading

2. Data Parsing
Buffer Overflows
Advanced Buffer Overflows
Format String Attacks
Integer Overflows

3. Information Disclosure
Storing Passwords in Plain Text
Creating Temporary Files
Leaving Things in Memory
The Swap File and Incomplete Deletes
Weekly-Seeded Keys and Random Number Generation
Trusting the Operating System APIs

4. On the Wire
Trusting the Identity of a Remote Host (Spoofing)
Proprietary Protocols
Volunteering Too Much Information
Loops, Self References and Race Conditions

5. Web sites
Cross Site Scripting
Forceful Browsing
Parameter Tampering
Cookie Poisoning
Hidden Field Manipulation
SQL Injection
Security on the Client
Trusting the Domain Security Model
Trusting SSL

Lesson 4
IV. Conclusion
Applying the techniques Learning
from past mistakes Case studies
50 question Online exam

Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

INTRODUCTION TO REVERSE ENGINEERING CERTIFICATIION CLASS W/EXAM

Hands On

Rapidly identify areas of vulnerability in software then target those areas with surgical precision? How can you exercise specific code paths with assurance while monitoring precisely your applications behavior? How can you log bug after bug while your teammates watch with envy? The answer lies in one of the most powerful techniques you can apply to software. Technology so lethal to executing software, it's almost not fair.

Sample Job Title
Application Security Tester
Information Systems Security Engineer
Quality Assurance (QA) Tester
Research & Development Engineer
Research & Development Research Engineer
Security Systems Engineer
Software Quality Assurance (QA) Engineer
Software Quality Engineer/ Systems Engineer
Testing and Evaluation Specialist/ Web App Developer

Class Fee:	$3,990
Time:	472 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + labs and Practicum Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

KU Outcomes
* Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
* Students will be able to describe the characteristics of secure programming

Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation
Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, IDA Pro, Saint, X Wget, Cyrpto tool, 'Curl' Fortify, Ounce.

Learning Objectives
complimentary skill set that will immediately set you apart from your peers. Reverse engineering training they will never look at software quite the same again. learn the foundation for acquiring data, identify vulnerable hot spots' in your application.
hex editors, disassemblers, resource editors.

Shatter the myth that binary code represents unintelligible and unchangeable hexadecimal values. You learn the basics of assembly language on the Intel architecture. The knowledge gained in this first segment on assembly will be one of the key building blocks to understanding the output of common reverse engineering tools and learning to write exploit code for buffer overruns. The class will then proceed to teach you how to use IDA Pro, the most powerful and widely used disassembler on the market. During this course you will be exposed to several such tools including SoftIce and Holodeck (our powerful fault injection tool).

Next, we give you insight into the most common security flaw that plagues modern software the buffer overflow. We will dissect this type of vulnerability in depth and walk you through the anatomy of a buffer overflow. After this introduction, we then proceed through hands-on exercises to help you uncover potential buffer overflows in applications using tools such as IDA Pro and Olly Debugger. Next, we proceed to teach you how to determine if a buffer overflow is exploitable and the theory behind exploits.

Who Should Attend?
This is an essential course for software testers, software developers, development and test managers, and anyone involved in software production.

Lesson Plan **Lesson 1**

I. Introduction to Reverse Engineering

History
Groups
State of the art

II. Assembly for Reverse Engineers

Instruction set review

Stack mechanics
High-level language mapping

Lesson 2
III. The Reverse Engineers Toolset
Debuggers
Disassemblers
Editors
Utilities
Virtual Machines

Lesson 3
IV. Vulnerability analysis and exploitation using reverse engineering techniques
Intro to IDAPro
Using IDA
DA scripts

Lesson 4
V. Finding Vulnerabilities through Binary Scanning

75 question Online exam

Grades -All students must ordinarily take all quizzes, labs, final exam, and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.

Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

- Problem scope
- Vulnerable functions
- High level language
- Binary signatures
- Hands on: Scripting IDA to recognize vulnerabilities in binary code

Lesson 5
VI. Bug Advocacy: Exploiting Vulnerabilities
Locating code flaws with hostile testing
Engineering op code exploits
Hands on: Intro Shell code lab
Hands on: Advanced shell code lab

VII. Wrap up
Advanced technologies
Course summary and closing

Those Less Comfortable - Hacking for Dummies, Kevin Beaver - Publication Date: January 29, 2013 | ISBN-10: 1118380932 | Edition: 4
For Those More Comfortable The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick ngebretson (Jun 24, 2013)
The book below is recommended for those interested in understanding how their own computers work for personal edification
How Computers Work, Ninth Edition Ron White Que Publishing, 2007 ISBN 0-7897-3613-6
This last book below is recommended for aspiring hackers, those interested in programming techniques and low-level optimization oode for applications beyond the scope of this course. Hacker's Delight, Second Edition Henry S. Warren Jr. Addison-Wesley,

Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

IDS I CATCHING THE HACKERS I - INTRODUCTION TO INTRUSION DEDECTION W/EXAM

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

Q/CND® Qualified/ Cyber Network Defense Certificate of Mastery
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class w/exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert w/exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class w/exam
Q/MC® Qualified/ Mission Critical Certification Class w/exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX®-[formerly CASP] Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
Linux/UNIX® Security Certification Class w/exam
CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam
Cloud Computing Security Knowledge Certification Class w/exam
IDS II: On-site Log Analysis, Event Correlation and Response Practicum
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This 40 hr 1 wk + 32 hr pre-study seminar investigates the strengths and weaknesses of network- and host-based intrusion detection systems (IDS). You will explore the leading IDS products on the market today. You will compare insourcing and outsourcing options and gain the knowledge you need to make informed decisions about which is best suited to your organization. You will explore the pros and cons of perimeter defenses. A demo of hacker attack methods will illustrate port scans, buffer overruns, and other network assaults in action. When you leave this cutting-edge seminar, you will know where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures. Bonus: You will receive a Network Intrusion Defense Kit drive.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP networking
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 2. 100 % completion of Lab
Grading: Pass = Attendance+ labs & quizzes Fail > 95% Attendance

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/ Security Engineer
Security Solutions Architect
Systems Engineer/ Systems Security Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and post class exam - passing the exam is a requirement for graduation.
Class Materials – SU class textbook, Labs and resources CD K
U Outcomes

* Students will be able to write a system security policy.
* Students will be able to describe and write various risk analysis methodologies.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
* Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend:

CIO's; Information Security Officers; Information Technology Managers, administrators, and Auditors; Telecommunications and Network Administrators; Consultants; Systems and Data Security Analysts; Project Managers; and Technology Planners

1. Introduction to IDS

- defining the role of intrusion detection in your overall network security program
- firewalls Vs IDS’s
- strengths and weaknesses of host-based and network-based IDS

2. Comparing IDS Solutions

- Cisco's Secure solutions
- NFR Flight Recorder
- Intrusion.com
- ISS RealSecure SAFEsuite
- Shadow
- Tripwire Enterprise
- NAI
- AXENT Intruder Alert
- Dragon/Entarasys
- CyberSafe Centrax
- Symantec
- freeware/shareware tools for intrusion detection solutions

3. Managed /Insourcing vs. Outsourcing Options

4. Implementing IDS

choosing an intrusion detection system

- host-based and network-based IDS
- key attributes of IDS
- placement determination
- who administers the IDS
- integrating IDS and firewalls

5. IDS and threat management: staff roles --clearly define responsibilities

- law enforcement contact
- overall coordinator
- documentation
- logging

7. the role of IDS in threat management --forensic gathering tool

- early-warning system
- escalation procedures
- document security policy and procedures
- defining the scope of incidents to be managed
- IDS alarm severity level definitions
- incident response sources
- integrating IDS and firewalls
- IDS case studies: insourcing vs. outsourcing
- developing an effective incident response capability

8. Reacting to Threats

- monitoring traffic
- sending an alert: console, audible, pager, E-mail
- taking action based on policy
- forcing the session to disconnect
- blocking all network access from the attacking source
- blocking all network access
- incident response resources

9. Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

10. Essential Tools and Resources

11. What You Can Expect in the Future

Cyber threat evasion and threat mitigation
Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Cyber Threat Vector on live cyber range
Validating the Threats: Hacker Attack Methods

- cyber range threats
- reconnaissance
- mapping networks
- access points
- relationships between systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while your mitigating the threat step by step.**Books** - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. Those Less Comfortable **- Hacking for Dummies**

Weapon of a CyberSecurity Warrior
Weapon of a CyberSecurity Warrior
Weapon of a CyberSecurity Warrior

Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

CATCHING THE HACKERS II: SYSTEMS TO DEFEND NETWORKS CERTIFICATION CLASS W/ EXAM

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

An essential component in any comprehensive enterprise security program is the ability to detect when your networks or systems are being probed or attacked, or have been compromised in some manner. Intrusion detection systems give you this critical monitoring capability.

In this up-close, 40 hr 1 wk class look at intrusion detection systems (IDS), you'll get a firm grip on everything from the leading IDS systems and attack signatures to creating a Threat Management Procedure. You will learn about the different types of intrusion detection systems, how they operate, how they should be managed, how and where they should be deployed, who the players are, and whether IDS is something that should be outsourced or kept in-house. After installing multiple IDS solutions, you will benefit from a demonstration of hacker attack methodologies and see for yourself how IDS can help to detect them. You will explore new directions in the IDS arena that promise to make intrusion detection systems easier to manage and a more effective part of your information security strategy. Through a wide array of exciting hands-on exercises you will not only install and configure IDS systems but you will observe first-hand many hacker "attacks" and exploits and how they appear to IDS systems. Implementation exercises will include of a representative sample of the latest IDS tools will include a combination of both freeware and commercial IDS tools. You will have the opportunity to create real attack scenarios to see how and learn from the best how to detect, read, react, and defend your network against from serious attacks.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid Instructor: TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Title
IA Operational Engineer
IA Security Officer
IS Analyst/Administrator
IS Manager/ IS Specialist
IS Security Engineer
IS Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

KU Outcomes:
* Students will be able to write a system security policy, Students will be able to describe and write various risk analysis methods.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses. * Students will be able to compare the advantages and disadvantages of various risk assessment methodologies.* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend: CIOs with responsibility for Computer Security, Network Administrators, Information Security Architects, Auditors, Consultants, and all others concerned with network perimeter security.

Learning Objectives different types of intrusion detection systems, how they operate, how they should be managed, how and where they should be deployed, who the players are, and whether IDS is something that should be outsourced or kept in-house. After installing multiple IDS solutions, you will benefit from a demonstration of hacker attack methodologies and see for yourself how IDS can help to detect them. *Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts.Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation*Tools for class, Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan

Class Lesson Plan

Lesson 1
Role and Operating Characteristics of IDS

- Identifying major IDS functions
- Defining the role of IDS related to firewalls and other network perimeter security safeguards

1. **Choosing an Intrusion Detection System**
   - Host-based vs. network-based IDS
   - Key attributes for positioning IDS in the network
   - Determining who administers the IDS

2. **Lesson 2**
   IDS Architecture
   - Integrating IDS and firewalls
   - Sensors
   - Collectors
   - Management consoles
   - IDS in the weeds

3. **Lesson 3**
   IDS Operation
   Sensors
   - Definition of anomalous traffic
   - Minimizing false positives
   - Correlation with other SMTP sources
   - Multiple security management consoles
   - Hands-on exercises: installing and configuring a sample of prominent IDS products (SNORT, Cisco Secure Intrusion Detection, ISS Real Secure, and Enterasys Dragon IDS)

4. **Threat Management: Reacting to the Attack**
   - Best practices for defining responsibility
   - Establishing a law enforcement contact
   - The role of an overall IDS coordinator

5. **Lesson 4**
   The Role of IDS in Threat Management
   - Using IDS as forensic gathering tool
   - Early warning systems
   - Escalation procedures
   - Creating a framework for IDS alert criteria and response center

6. **Document Security Policy and Procedures**
   IDS alarm severity levels
   - Incident response sources
   - Integrating IDS and firewalls
   - IDS case studies
   - Developing an effective incident response capability
   - Hands-on exercises: Creating a template for managing the people and the processes for IDS Defense Procedures.

7. **Lesson 5**
   Real-Time Reaction to Threats
   Sending an alert — console, audible, pager, E-mail
   - Taking action based on policy
   - Forcing the session to disconnect
   - Blocking access from the attacking source
   - Blocking all network access
   - Incident response resources

8. **Validating the Threats: Looking at Hacker Attack Methods**
   - Hacker attacks
   - Bug exploitation
   - Buffer overruns
   - Attack Scenarios
   - Common types of attacks that an IDS can help detect
   - Network scans
   - Port scans
   - Denials-of-service: Smurf, Land, Trin00, Stacheldraht
   - "DE-synching" an IDS
   - Fragmentation
   - What an IDS might not detect
   - CGI exploits
   - Malformed URL's
   - Other application-layer attacks
   - Race condition
   - Trust exploitation
   - Social engineering
   - Physical access
   - Hands-on exercises:
     Real-time TCP/IP monitoring
     - Live signature review and analysis

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.

SU Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

IDS III ON-SITE LOG ANAYLSIS, EVENT CORRELATION AND RESPONSE CERTIFICATION w/ EXAM

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

Q/CND® Qualified/ Cyber Network Defense Certificate program of Mastery CPoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, SecurityX or CISSP) Practicals as evidence to support the claim of knowing something
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class w/exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert w/exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class w/exam
Q/MC® Qualified/ Mission Critical Certification Class w/exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX ® [formerly CASP] Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
Linux/UNIX® Security Certification Class w/exam
SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam
Cloud Computing Security Knowledge Certification (CCSK) Class w/exam
IDS II: On-site Log Analysis, Event Correlation and Response Practicum
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This 72 hour class investigates how to strengthen network- and host-based intrusion detection systems (IDS). You will explore the leading IDS products on the market today, including Cisco, ISS real secure, SNORT, Tripwire Enterprise (and shareware) and more. You will compare managed services to make informed decisions about which is best suited to your organization. You will explore the pros and cons of perimeter defenses and deep internal defenses. Hacker attack labs will enrich your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you leave this cutting-edge seminar, you will know where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures. Bonus: You will receive a Network Intrusion Defense Kit drive.

Class Fee:	$3,990
Time:	72hrs
Learning Level:	Advanced
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Basic competency with TCP/IP & Linux.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 2. 100 % completion of Lab

Grading: Pass = Attendance+ labs & quizzes Fail > 95% Attendance

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/ Security Engineer
Security Solutions Architect
Systems Engineer/ Systems Security Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
KU Outcomes

* Students will be able to write a system incidence response policy.
* Students will be able to describe and write various risk analysis methodologies.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
* Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend:

CIO's; Information Security Officers; Information Technology Managers, administrators, and Auditors; Telecommunications and Network Administrators; Consultants; Systems and Data Security Analysts; Project Managers; and Technology Planners

Class Lesson Plan

1. Introduction to IDS

- defining the role of intrusion detection in your overall network security program
- firewalls Vs IDS's
- strengths and weaknesses of host-based and network-based IDS

2. Comparing IDS Solutions

- Cisco's Secure solutions
- NFR Flight Recorder
- Intrusion.com
- ISS RealSecure SAFEsuite
- Shadow
- Tripwire Enterprise
- NAI
- AXENT Intruder Alert
- Dragon/Entarasys
- CyberSafe Centrax
- Symantec
- freeware/shareware tools for intrusion detection solutions

3. Managed /Insourcing vs. Outsourcing Options

4. Implementing IDS

choosing an intrusion detection system

- host-based and network-based IDS
- key attributes of IDS
- placement determination
- who administers the IDS
- integrating IDS and firewalls

5. IDS and threat management: staff roles --clearly define responsibilities

- law enforcement contact
- overall coordinator
- documentation
- logging

7. the role of IDS in threat management --forensic gathering tool

- early-warning system
- escalation procedures
- document security policy and procedures
- defining the scope of incidents to be managed
- IDS alarm severity level definitions
- incident response sources
- integrating IDS and firewalls
- IDS case studies: insourcing vs. outsourcing
- developing an effective incident response capability

8. Reacting to Threats

- monitoring traffic
- sending an alert: console, audible, pager, E-mail
- taking action based on policy
- forcing the session to disconnect
- blocking all network access from the attacking source
- blocking all network access
- incident response resources

9. Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

10. Essential Tools and Resources

11. What You Can Expect in the Future

Cyber threat evasion and threat mitigation
Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Cyber Threat Vector on live cyber range
Validating the Threats: Hacker Attack Methods

- cyber range threats
- reconnaissance
- mapping networks
- access points
- relationships between systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

IDS III On-site Log Analysis, Event Correlation and Response Certification Class Practicum
Insider threat is one of the most dangerous security threat, and a much more complex issue. These insiders can be a former or a disgruntled employee or any business associate that has or had an authorized access to information for any particular organization. They have control and security measures. Hence continuous monitoring is essential to track each and every activity within the network. Log management is a strong technique which includes both Log analysis with event correlation which provides the root cause of any attack and network can be protected from security violations. Though intrusion detection is complex process, while checking the ability to detect intrusive behavior within the internal environment, it has to take care of suppressing the false alarm rate. Some strong approach is required on the basis of which decisions can be taken fast.

This 72 hour practicum class investigates how to strengthen network- and host-based intrusion detection systems (IDS). You will use and report on tools that log data risk and review and compare threats to make informed decisions about which is best suited to the task at hand. You will decide what best works for perimeter defenses and deep internal defenses. You will build unique Hacker attack scenarios to demonstrate your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you leave this cutting-edge class, you will provide a schematic of where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. **Books** - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below

Q/CDA Qualified/ Cyber Defense Analyst Certificate Program of Mastery

MISSION CRITICAL PLANNING CERTIFICATION CLASS W/EXAM Hands On

How to select the right tools and develop effective Contingency Planning for information systems.
More than ever your corporate data is at risk. During this 72 hour class, you'll learn the principles of contingency planning and develop an A to Z disaster recovery plan for information assurance in your organization. This interactive workshop / lab will jump start your contingency planning processes for large or small organizations. You will walk away with a portfolio of near and long term answers and initiatives for critical asset management risk, contingency plans and disaster recovery

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP networking
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid Instructor: TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Title
Contracting Officer (CO)
Contracting Officer Technical Representative (COTR)
Information Assurance (IA) Manager
Information Assurance (IA) Program Manager
Information Assurance (IA) Security Officer
Information Security Program Manager
Information Systems Security Manager (ISSM)
Information Systems Security Officer (ISSO)
Information Systems Security Operator

This accelerated class is taught using face to face modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Who should attend: CIOs with responsibility for Contingency Planning, Network Administrators, Information Security Architects, Auditors, Consultants, and all others seeking to plan, implement, and/or manage a Contingency Planning program.

KU Outcomes:
* Students will be able to describe potential system attacks and the actors that might perform them.
* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives:
Basics of contingency planning
Business Impact Analysis (BIA) tools "test drive" leading contingency planning software.
Determine your organizations most critical applications,
Explore Maximum Allowable Delay (MAD),
Configure time techniques,
Establish disaster recovery teams
Designate a control center methodology
Develop a process for real-time disaster recovery for your organization.
Contingency planning product(s)
Import existing personnel
Equipment records
Establish the recovery teams you will need,
Recovery strategies (hot site, cold site, reciprocal agreements, etc.),
Test your contingency plan

Course Lesson Plans
Phase I — Establishing Baseline
Before the tools of contingency planning can be effectively used, the concepts behind the tools must be understood. Anyone can buy a tool; knowing how to apply the tool makes the tool effective. In this first phase of our training you will learn the concepts and definition used by certified business continuity planners to effectively communicate project priorities and establish contingency planning project boundaries.

Defining Terms
Cost, Benefits and ROI with Contingency Plans
Disaster Prevention
Levels of Effort (LAN, WANS, Mainframe)
Establishing the Scope
Project Management
BCP Planner/Coordinator
Team Leaders

Team Members
management Support
Anatomy of a Disaster
Recovery Phases
Emergency Response
Situation Assessment
Recovery Strategy
Interim Ops
Restoration
Recovery Strategies
Hot sites
Warm site
Cold sites
Mobile recovery
Reciprocal Agreements
Mix and Match
Testing the plan
Paper tests
Team testing
Unannounced tests
Complete tests
Testing cautions
Creating a usable test plan

Phase II — Finding the Right Tools
After mastering the basics concepts, what comes next?
A survey of the tools that can help more efficiently develop and maintain a contingency plan.

Contingency Planning Tools
Business Impact Analysis
Manual tools
Automated Tools
Disaster Recovery Plans
Manual Tools
Automated Tools
Business Resumption Plans
Manual Tools
Automated Tools

Phase III — Using the Tools and Creating an Effective Plan
This is the hands-on phase where students will apply contingency planning principles they have learned while using use the tools we have surveyed to begin a contingency plan for their organization.

Selecting the tool that fits
Business Impact Analysis
Manual tools
Automated Tools
Disaster Recovery Plans
Manual Tools
Automated Tools
Creating a disaster recovery plan
Determining critical application recover times
Selecting team members
Selecting recovery strategy(ies)
Building the data center plan
Suggested Information for Students to bring to class**:
Organizational chart
List of all Host (server or mainframe) based applications and a description of what they do
List of all IT hardware in data center
List of communications equipment in data center
List of all data center personnel with associated skill sets

**Note: If required student information is not brought to class a "practice set" of information will be available.
Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. However, what ultimately matters in this course is not so much where you end up relative to your classmates but where you end up relative to yourself in on Friday of class. The course is graded as a pass or fail solely on your attendance and participation. B**ooks** - No books are required for this course. However, you may want to supplement your preparation.

QUALIFIED IS OUR BUSINESS
Security University

Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery
QCND QUALIFIED/CYBER DEFENSE ANALYST W/EXAM

SU's Q/CND Qualified/ Cyber Network Defense and Offensive missions are threaded into the Network Cyber Defense Analyst Training classes. The mission is to master defensive scenarios to protect your networks from the hacker. This training is for those who seek qualified cyber network defense, cy ops and threat attack careers. The Q/CND Certificate Program of Mastery Program is an accredited program with related cyber micro credentials.

SU training techniques are a perfect match for our military cyber defense workforce goals and cyber operations since they not only train the relevant concepts of cyber defense analyst nd its CND specialties but also in the case of Q|SA and Q|PTL courses challenge the students to apply those concepts in a tactical mastery level setting that an actual security analyst or penetration tester might see. SU also provides advanced training paths in topics such as network defense, penetration testing, exploitation, digital forensics, and software security that is tailored to the trainee's long-term skills acquisition goals. The instruction is provided by proven leaders in the field and guarantees graduates have the immediately applicable skills to be relevant in the cyber fight. In my experience, few practitioners can apply the skills gained in a traditional immersion course into the workforce. Instructors have led, trained, and worked alongside with cyber professionals who have earned numerous industry certifications. However, it has been shown time and again that these certifications provide mere exposure without the critical analysis and creative thinking required to solve tough problems in our evolving cyberspace. SU addresses this shortcoming with their mastery level training model and apprenticeship.

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

An essential component in any comprehensive enterprise security program is the ability to detect when your networks or systems are being probed or attacked, or have been compromised in some manner. Intrusion detection systems give you this critical monitoring capability.

In this up-close, 40 hr 1 wk + 32 hr pre-study class look at intrusion detection systems (IDS), you'll get a firm grip on everything from the leading IDS systems and attack signatures to creating a Threat Management Procedure. You will learn about the different types of intrusion detection systems, how they operate, how they should be managed, how and where they should be deployed, who the players are, and whether IDS is something that should be outsourced or kept in-house. After installing multiple IDS solutions, you will benefit from a demonstration of hacker attack methodologies and see for yourself how IDS can help to detect them. You will explore new directions in the IDS arena that promise to make intrusion detection systems easier to manage and a more effective part of your information security strategy. Through a wide array of exciting hands-on exercises you will not only install and configure IDS systems but you will observe first-hand many hacker "attacks" and exploits and how they appear to IDS systems. Implementation exercises will include of a representative sample of the latest IDS tools will include a combination of both freeware and commercial IDS tools. You will have the opportunity to create real attack scenarios to see how and learn from the best how to detect, read, react, and defend your network against from serious attacks.

Class Fee: $3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites: Understanding of TCP/IP Protocols
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid Instructor: TBD
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practicum Fail > 95% Attendance

Sample Job Title
IA Operational Engineer
IA Security Officer
IS Analyst/Administrator
IS Manager/ IS Specialist
IS Security Engineer
IS Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
KU Outcomes:

* Students will be able to write a system security policy, Students will be able to describe and write various risk analysis methods.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses. * Students will be able to compare the advantages and disadvantages of various risk assessment methodologies.* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Who Should Attend: CIOs with responsibility for Computer Security, Network Administrators, Information Security Architects, Auditors, Consultants, and all others concerned with network perimeter security.

Learning Objectives different types of intrusion detection systems, how they operate, how they should be managed. L*abs, SU Pen Testing*

Materials, resource CD's and attack handouts.Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare

Class Lesson Plan

Lesson 1
Role and Operating Characteristics of IDS

- Identifying major IDS functions
- Defining the role of IDS related to firewalls and other network perimeter security safeguards

1. **Choosing an Intrusion Detection System**
   - Host-based vs. network-based IDS
   - Key attributes for positioning IDS in the network
   - Determining who administers the IDS

2. **Lesson 2**
   IDS Architecture
   - Integrating IDS and firewalls
   - Sensors
   - Collectors
   - Management consoles
   - IDS in the weeds

3. **Lesson 3**
   IDS Operation
   - Sensors
   - Definition of anomalous traffic
   - Minimizing false positives
   - Correlation with other SMTP sources
   - Multiple security management consoles
   - Hands-on exercises: installing and configuring a sample of prominent IDS products (SNORT, Cisco Secure Intrusion Detection, ISS Real Secure, and Enterasys Dragon IDS)

4. **Threat Management: Reacting to the Attack**
   - Best practices for defining responsibility
   - Establishing a law enforcement contact
   - The role of an overall IDS coordinator

5. **Lesson 4**
   The Role of IDS in Threat Management
   2 hr Lecture 2 hr labs
   - Using IDS as forensic gathering tool
   - Early warning systems
   - Escalation procedures
   - Creating a framework for IDS alert criteria and response center

6. **Document Security Policy and Procedures**
   - IDS alarm severity levels
   - Incident response sources
   - Integrating IDS and firewalls
   - IDS case studies
   - Developing an effective incident response capability
   - Hands-on exercises: Creating a template for managing the people and the processes for IDS Defense Procedures.

7. **Lesson 5**
   Real-Time Reaction to Threats

   - Sending an alert — console, audible, pager, E-mail
   - Taking action based on policy
   - Forcing the session to disconnect
   - Blocking access from the attacking source
   - Blocking all network access
   - Incident response resources

8. **Validating the Threats: Looking at Hacker Attack Methods**
   - Hacker attacks
   - Bug exploitation
   - Buffer overruns
   - Attack Scenarios
   - Common types of attacks that an IDS can help detect
   - Network scans
   - Port scans
   - Denials-of-service: Smurf, Land, Trin00, Stacheldraht
   - "DE-synching" an IDS
   - Fragmentation
   - What an IDS might not detect
   - CGI exploits
   - Malformed URL's
   - Other application-layer attacks
   - Race condition
   - Trust exploitation
   - Social engineering
   - Physical access
   - Hands-on exercises:
     Real-time TCP/IP monitoring
     - Live signature review and analysis

fs -All students must ordinarily take all quizzes, labs, exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.

Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

LINUX /UNIX SECURITY W/EXAM

Hands On

Q/CND® Qualified/ Cyber Network Defense Certificate of Mastery CPoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, SecurityX or CISSP)
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class w/exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert Class w/exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class w/exam
Q/MC® Qualified/ Mission Critical Certification Class w/exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX® [formerly CASP] Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
Linux/UNIX® Security Certification Class w/exam
CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam
Cloud Computing Security Knowledge Certification Class w/exam
IDS II: On-site Log Analysis, Event Correlation and Response Practicum
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This fast-paced, hands-on class will teach you how to secure UNIX and lock down Linux to protect a system from compromise. You'll learn how the attacks work and how to use hard-core hardening to defeat the bulk of them. You'll learn how to take your machines to a state of minimum necessary risk. This hands-on class teaches you how to tighten all major aspects of the operating system for security, balancing this with the purpose of the system and the needs of your organization. You'll learn how to tune kernel and operating system parameters, deactivate components, and tighten the components that remain. You'll examine major server applications tightening, including Apache, Sendmail, WU-FTPd, vsftpd, and BIND. Along the way, you'll understand how external and internal actors use privilege escalation and how you can lessen their odds of gaining root. You'll also learn to apply key security concepts, from defense-in-depth to least privilege to risk evaluation, to determine what actions you should take and in what order of priority.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understand TCP/IP Protocols.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance

Sample Job Title
Information Assurance (IA) Operational Engineer
Information Assurance (IA) Security Officer
Information Security Analyst/Administrator
Information Security Manager or Specialist
Information Systems Security Engineer
Information Systems Security Manager
Platform Specialist/ Security Administrator
Security Analyst/ Security Control Assessor
Security Engineer

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend: System administrators, security administrators, Security auditors. Unix box owners. Anyone who has a vested interest in keeping their systems from being compromised. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions. While others are welcome, complete lack of familiarity is too great a burden to overcome in 72 hr class.

Text Materials: labs, SU Pen Testing &nLinux Testing Materials, resource CD's and attack handouts.Machines a Dual Core 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation Tools for class -Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat, X Wget, Cyrpto tool, 'Curl'

KU Outcomes:

* Students will be able to describe potential system attacks and the actors that might perform them.
* Students will be able to describe cyber defense tools, methods and components.
* Students will be able to apply cyber defense methods to prepare a system to repel attacks.
* Students will be able to describe appropriate measures to be taken should a system compromise occur.

Learning Objectives:
Students will gain a general understanding of how to harden systems to prevent or contain a system compromise.

- Configure Solaris and Linux for much greater resilience to attack.
- Understand each Solaris and Linux network service and be capable of judging which can or cannot be safely restricted or deactivated.
- Understand each Solaris and Linux boot script and be capable of judging which scripts can or cannot be safely deactivated.
- Audit the Solaris and Linux file permissions and Set-UID/GID programs to combat compromise and escape privilege escalation.
- Configure Apache Web servers for greater resistance to attack.
- Configure vsftpd FTP servers for greater resistance to attack.
- Configure a Linux-based firewall
- Passwords Attacks and Alternative Authentication Techniques
- Memory Attacks, Buffer Overflows
- Configure BIND DNS servers to greater resistance to attack.
- Trojan Horse Programs and Rootkits
- Network-Based Attacks
- Configure Sendmail Mail servers for greater resistance to attack.
- Configure POP and IMAP servers for greater resistance to attack.
- Vulnerability Scanning Tools
- Monitoring and Alerting Tools
- Audit systems with free tools to find better security settings, including Bastille, Titan and the Center for Internet Security's tools
- Network Security Tools
- Configure WU-FTPd FTP servers for greater resistance to attack.
- SSH for Secure Administration
- Forensic Investigation
- Understand and set kernel and operating system variables for best security
- Unix Logging and Kernel-Level Auditing
- Network Time Protocol
- Solaris and Linux Security
- Secure Configuration of BIND, Sendmail, Apache
- Common Issues with Users and Management

Each student will practice the techniques learned on their own Linux system. A shared Solaris machine will also be available for Solaris practice. Students are welcome to harden their own laptop systems as well, in preparation for the hostile networks that can often be found at security conferences.

Day 1
Core Operating System Hardening
The first day of the course will focus on core operating system hardening, teaching students how to thoroughly audit and lock down a Linux system. This process is tailored very closely to a system's purpose, such that it optimizes a system for the greatest security that is operationally possible. Single-purpose bastion hosts obviously see the most benefit, though general purpose sysadmin workstations still gain a good deal of resistance to break-in. This first day will cover the following major areas/tasks:
Boot Security and Physical Security
An actor with physical access to a Linux machine can usually gain root with trivial attacks. Students will learn both the attacks and how to defend against them.
The Vulnerability Cycle and Patching Recommendations
Many vulnerabilities can be trivially countered by applying patches. On the other hand, applying patches is not easy in an enterprise environment. Students will learn the background required to make intelligent patching decisions and will be introduced to tools which automate this process.
Lesson 2:
Network Daemon Audit
Programs that listen to the network provide most outside actors with their first access to a victim system. Students will learn how to audit

the system for network-accessible daemons. By learning the purpose of each daemon, students will learn how to greatly decrease a hosts' network presence.

General Daemon Audit

Once an actor has some kind of access to a system, privileged system daemons present a primary avenue for further attack and privilege escalation. Students will learn to audit these daemons. By learning the purpose of each one, students will learn which daemons they can safely deactivate.

Host-based Firewall Construction Once the system's set of listening network daemons has been reduced, it's accessibility to actors via the network can be further shored up by adding a host-based firewall. Students will be introduced to simple stateful firewalling that can be applied to individual hosts.

Set-UID Audit

Outside of already-running system daemons, Set-UID programs represent the most commonly-used method of privilege escalation. These programs give a user a temporary privilege increase to perform a specific task -- unfortunately, that privilege increase becomes general and non-temporary when these programs are successfully attacked. Students will learn how to audit these programs and maintainably reduce an actor's ability to use them to attack the system.

Permissions Audit

Poor file permissions can allow an ordinary user to gain system user privileges or to access/compromise data. Students will be introduced to a basic permissions audit.

Lesson 3: Server Application Hardening

The second day of the course will focus on server application hardening. Students will learn how to apply access control mechanisms to particular server functionalities, how to prune out server functionality that's not in use, and how to confine server processes so that a compromised server application does not necessarily compromise the entire system. Students will also be introduced to real network/server architecture changes that can greatly increase security at a site. Learning to harden these servers is extremely important to the security of an organization, both because of their important functions and because they are widely accessible resources. Finally, students will learn to build a chroot prison for each network service, to prevent a compromised service on a system from turning into a fully-compromised system.

Tightening DNS Servers An actor who can compromise an organization's internal DNS server can re-route much of the important traffic on a network. An actor who can compromise an organization's external DNS server can re-route traffic away from the organization. In either case, he can usually gain a foothold to attack the internal network. Students will learn how to configure Unix BIND DNS servers for much greater resiliency to attack. As a part of this, they will learn how to configure Split-Horizon DNS and BIND 9 "views," to greatly reduce the external accessibility of internal DNS servers. They will also learn how to confine DNS server programs so that, if successfully attacked, they will not grant an actor either the ability to easily modify data or to compromise the host operating system.

Say 5 Tightening FTP Servers FTP servers represent one of the more often-vulnerable Unix network daemons in the past five years. Students will learn how to configure an FTP server to be more resistant to attacks by learning how past attacks have worked and how best practices can defeat these attacks. This focuses on both vsftpd and wu-ftpd.

Tightening Apache Web Servers Web servers represent the single most multipurpose publically-accessible server application in use today. Apache, in particular, has a lead in market share specifically because of the extremely wide array of functions that it can serve and the ease in which an increasing community of developers can add functionality. This wide scope of functionality, of course, comes with a cost -- it increases the probability that the server will contain vulnerable code. Students will learn how to configure Apache security modules and how to configure an Apache webserver to offer only what functionality is used by their site. They will also learn some of the weaknesses of the CGI model and how they can address them with programs like suexec and cgiwrap. Finally, they will learn how to greatly reduce their chances of having vulnerable code deployed by removing Apache modules that are not in use at their site.

Lesson 5 Tightening Mail Servers

Webmail on Unix operating system. While vulnerabilities are very uncommon, they tend to bring extreme consequences, both because Webmail l runs with root privilege and because so much sensitive data moves through E-mail.

Students will learn how to tighten Webmail configuration against attack, looking at jailing the Webmail process, dropping its privilege level, and configuring it for better resistance to attack and spam. They'll also learn how to deploy a split horizon (internal/external) model to their mail servers, to protect the internal mail server and its valuable data from external attack.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Books - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below.

Q/CDA Qualified/ Cyber Defense Analyst Certificate Program of Mastery

CompTIA CySA+ CYBERSECURITY ANALYST CERTIFICATION TRAINING

This fast-paced, 95% hands-on LABS class will teach you how to secure networks and protect a system from compromise. You'll learn how the attacks work and how to use hard-core hardening to defeat the bulk of them. You'll learn how to take your machines to a state of minimum necessary risk.

This hands-on class teaches you how to tighten all major aspects of the operating system for security, balancing this with the purpose of the system and the needs of your organization. You'll learn how to DEFEND DNS, PKI and kernel and operating system parameters, deactivate components, and tighten the components that remain. You'll understand how external and internal attackers use privilege escalation and how you can lessen their odds of gaining root. You'll also learn to apply key security concepts, from defense-in-depth, continuous monitoring, least privilege to risk evaluation, to determine what actions you should take and in what order of priority.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2 hr exam
Prerequisites:	Understand TCP/IP networking
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Lab & quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Who Should Attend:
System administrators, security administrators, security auditors. unix admins. Anyone who has a vested interest in keeping their systems from being compromised. This course targets system or network administrators and security admins/auditors with an understanding of Unix commands and basic operating system functions. While others are welcome, complete lack of familiarity is too great a burden to overcome in a three day class.

Text Materials: labs, SU Pen Testing & Linux Testing Materials, resource CD's and attack handouts.
Machines a Dual Core 36M Ram, 350 Tdrives, running MS OS, linux, and VMWare Workstation

Tools for class
Whois, Google Hacking, Nslookup , Sam Spade, Traceroute , NMap , HTTrack , Superscan , Nessus, PSTool, Nbtstat, Solarwinds ,Netcat , John the ripper , Nikto/Wikto ,Web Scarab , HTTP Tunnel (hts.exe) , LCP ,Cain and Abel, Ettercap system hacking ,John the Ripper Wireshark sniffers, TCP dump, D sniff , tcpdump, Metasploit, ISS exploit, web app,Core Impact , Snort , Infostego, Etherape ,Firefox with plugins (Hackbar, XSSme...) ,, ebgoat,
X Wget, Cyrpto tool, 'Curl'

What You Will Learn:
The mission of the CND class is to train the network defender on basic to advanced security concepts and techniques used to detect, recognize, identify, and mitigate network threats and vulnerabilities and how to report them.

- Privilege Escalation
- Reconnaissance
- Scanning
- Enumeration

- Sniffing
- Password Cracking Techniques
- System Hacking
- Buffer Overflows
- Social Engineering
- SQL Injection
- Hacking Linux
- Virus Worms Trojans Rootkits
- IDS, Firewalls and Honeypots
- Denial of Service
- Cryptography
- Session Hijacking
- Web Application Vulnerabilities
- Hacking Web Servers
- Penetration Testing Methods
- DLL/Code injection
- ARP Poisoning
- Log Tampering
- Data Hiding and Evasion
- Alternate Data Streams
- Locked directories
- Special Shell Folder Locations
- Steganography
- Find/Grep Utilities
- Basic SQL
- File comparison
- Push/Pull logging
- Network mirroring /Port Mirroring/SPAN
- UNIX Epoch Time
- Network Traffic Analysis

2) Linux and Unix fundamentals

- Network Traffic Analysis
- Examine how to mitigate or eliminate general problems that apply to all
- Unix-like operating systems,
- vulnerabilities in the password
- authentication system,
- file system,
- virtual memory system,
- applications that commonly run on Linux and Unix.
- configuration guidance and practical, real-world examples,
- tips, and tricks.

Data Analysis tools and Fundamentals
IS.2. Learn how to create, edit, and manage changes to network access control lists on firewalls and IPS.
IS.3. Learn Anti-Virus or Audit/Remediation administration including installation, configuration, maintenance, and backup/restore.

- Data Correlation (Data Fusion)
- Logging Architectures and Data Sources
- IP Anomalies and Bogon Routing

- TCP Anomalies
- UDP Anomalie
- Data Correlation (Data Fusion)
- Logging Architectures and Data Sources
- IP , TCP, UDP, ICMP, HTTP Anomalies
- Reverse Shells
- Directory Traversals
- Unicode Exploits
- Command Injection
- IIS Web Service Logging Locations
- HTTP.sys Error Logging
- FTP Bouncing
- Active FTP
- Passive FTP
- SMTP & Unsolicited Mail
- SNMP ver1, 2 or 3?
- RDP Hijacking
- SSL/TLS and SSH Hijacking, with a twist of DNS and ARP Poisoning
- Back up and restore

Lesson 3
Intrusion Analysis
IS.5. Learn how to manage and administer the updating of rules and signatures for specialized CND applications. (IDS/IPS, anti-virus, and content blacklists)
IS.6. Learn how to Identify potential CND implementation conflicts (e.g., tool/signature testing and optimization).
IS.7. Learn how to build and administer CND test bed to evaluate new CND applications, rules/signatures, access controls, and configurations of CND-SP managed platforms.
A.2.How to analyze network alerts skills
A.3. How to validate network alerts
A.4. How to analyze log files from a variety of sources (host logs, network traffic logs, firewall logs, and ISD logs) or SIM
A.5. Learn how to identify anomalous activity and analyze network traffic and how they threaten network resources.
A.7. Learn to write signatures for CND network tools in response to new or observed threats.
A.8. Learn how to do event correlation from a variety of sources to gain situational awareness and determine the effectiveness of an observed attack.
A.9. Notify CND managers, CND incident responders, and other CND-SP team members of suspected CND incidents and articulate the event's history, status, and potential impact for further action.

- RDP Hijacking
- Analyze network alerts
- Validate network alerts
- Analyze log files from host logs, network traffic logs, IDS logs
- Identify anomalous activity and analyze network traffic & how they threaten resources
- Write signatures for network tools in response to new or observed threats
- Event correlation from a variety of sources to determine the effectiveness of the attack.

Lesson 4
Basic Forensic tools and Fundamentals

IR.2. You will understand how to collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) to mitigate potential CND incidents.
IR.3. You will learn how perform initial, forensically sound collection of images to discern mitigation/ remediation.
IR.4.Learn how to coordinate with and provide expert technical support to resolve CND incidents.

IR.5.You will learn how to track and document CND incidents from initial detection through final resolution.
IR.6. You will learn the step by step process of CND incident triage to determine scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation.
IR.7. You will learn how to correlate incident data and perform CND trend analysis and reporting.
IR.8. You will coordinate with intelligence analysts to correlate threat assessment data.
IR.9. You will learn how to serve as technical experts to law enforcement for incident details & expert testimony
IR.10. You will perform real-time CND Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRT).
IR.11. You will learn how to maintain deployable CND toolkit (e.g., specialized CND software/hardware) to support IRT missions.
IR.12. You will learn who to write and publish CND guidance and reports on incident findings to appropriate constituencies.

- Data Breach Cases &, Intrusion Analysis
- U.S. Laws Investigators you should know
- Evidence Acquisition/Analysis/Preservation Laws and Guidelines
- Forensic Collection of Images
- Forensic Reports and Testimony
- Step by Step Forensics Methodology
- File System Essentials
- Evidence Integrity and Chain of Custody
- Advanced Forensic Evidence Acquisition and Imaging
- File System Timeline Analysis
- Key Forensic Acquisition/Analysis & Correlation Concepts
- Volatile Evidence Gathering and Analysis
- Forensic Analysis Key Methods
- Key Windows File System Analysis Concepts
- File System and Data Layer Examination
- Metadata and File Name Layer Examination
- Windows FAT File System Examination
- Windows NTFS File System Examination
- Linux/Unix File System Examination
- Image File Conversion (E01, Raw, AFF)
- Windows System Restore and Shadow Volume Copy Exploitation
- File Sorting and Hash Comparisons
- Live Response and Volatile Evidence Collection
- Windows Registry Analysis
- Windows Internal File Metadata
- Application Footprinting and Software Forensics
- Automated GUI Based Forensic Toolkits

Lesson 5
Incident handling
AC.2. You will learn applicable CND policies, regulations, and compliance documents specifically related to CND auditing.
AC.3. You will learn how to do step by step CND vulnerability assessments.
AC.4. You will learn how to do step by step CND risk assessments.
AC.5. You will learn how to conduct authorized penetration testing of network assets.
AC.6. You will learn how to analyze site CND policies and configurations and evaluate compliance with regulations and enclave directives.
AC.7. You will learn how to prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.

- The step-by-step penetration tester assessment process and methodology workshops
- The latest cyber attack vectors defenses to stop them
- Proactive and reactive defenses of a computer attack with 12 live scenarios
- Scanning for, exploiting, and defending systems
- Strategies and tools for detecting each type of attack
- Attacks and defenses for Windows, Unix, switches, routers and other systems
- Application-level vulnerabilities, attacks, and defenses
- Developing an incident handling process and preparing a team for battle
- Legal issues in incident handling
- Recovering from computer attacks and restoring systems for business

Lesson 6
Current Trends & developments / Qualified/ Network Defense Exercise QNDX

Scenario #1—Attacks with no perimeter to soft systems
Scenario #2—Defense with no perimeter and soft systems
Scenario #3—Attacks with no perimeter to hard systems
Scenario #4—Defense with no perimeter and hard systems
Scenario #5—Attacks through perimeter to hard systems
Scenario #6—Defense with perimeter and hard systems
Scenario #7—DOS attacks on hardened network
Scenario #8—DOS defenses with hardened network
Scenario #9—Concurrent attack/defense with no perimeter
Scenario #10—Concurrent attack/defense with perimeter
Scenario #11—Concurrent DOS attack/defense
Scenario #12—Ad Hoc: This scenario can be tailor-made to fit any specific learning objectives.

Each class builds networks with a secure channel (i.e., VPN) setup, start/stop times and dates, roles (attacker or defender), ROE, and learning objectives that will be drafted and published with the described pre-defined Q/ISP Project scenarios and SOW (Scope of Work) establish parameters of scenarios. These twelve scenarios and SOW will serve as the necessary administrative coordination between QNDX participants. Though the exact content of these scenario descriptions and SOW will not be finalized until approved, the generalized contents and descriptions follow.

The SOW will contain four main elements.
1) A statement regarding the intent of QNDX participation.
2) Elaboration regarding the mandatory implementation of a secure VPN tunnel between the participating networks.
3) Delineation of Qualified -exercise ethical conduct and ROE.
4) A statement indicating that each Major has notified their local IT authorities regarding the exercise, and that each side has taken measures to ensure that their SOW network activities will not adversely hinder routine network operations.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
CLOUD COMPUTING SECURITY KNOWLEDGE CERTIFICATION W/EXAM

As organizations migrate to the cloud, they need information security professionals who are cloud-savvy. The Cloud Computing certificate is widely recognized as the standard of expertise for cloud security and gives you a cohesive and vendor-neutral understanding of how to secure data in the cloud. The Cloud credential is the foundation to prepare you to earn additional cloud credentials specific to certain vendors or job functions.
This class provides the foundational knowledge needed to utilize cloud services and enables you to gain critical insights into topics such as data security, key management, and identity and access management and speak with confidence about cloud security concerns.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE 3 Credit
Method of Delivery:	Residential (face-to-face) or Hybrid TBD
Instructor:	
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs& Quizzes Fail > 95% Attendance
Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Who Is This Program For?
Cloud Computing Analyst, Cloud Administrator, Cloud Architect, Cloud Engineer, Enterprise Architect, Security Administrators, Security Architect and Systems Engineer are cloud security job roles.

What you will learn:
Introduction to Information Security within Cloud Computing
Selecting secure cloud services begins with understanding business requirements. This course will teach you to identify and select secure cloud services based upon business requirements.

The Certificate of Cloud Computing Security Knowledge, enables you to gain critical insights into topics such as data security, key management, and identity and access management. You'll have the skills and knowledge of Managing Cloud Security and Risk needed to reduce risks to an acceptable degree to the business. With an expanding array of cloud services being offered daily it is easy for the inexperienced to lack awareness of security functions in cloud offerings. In this course, Introduction to Information Security within Cloud Computing, you'll learn to identify and select secure cloud services based upon business requirements. First, you'll explore the detailed definition of cloud computing. Next, you'll discover the deployment and service models of cloud computing. Finally, you'll learn how to use a matrix to review the controls enacted by a cloud provider. When you're finished with this course, you'll have the skills and knowledge of, Introduction to Information Security within Cloud Computing needed to select secure cloud services that meet business requirements.

Introduction:

Lesson 1:
Defining Cloud Computing and Essential Characteristics
Chapter 13: Security as a Service
Chapter 14: Related Technologies
Chapter 15: ENISA Cloud Computing: Benefits, Risks and Recommendations for Security
Chapter 3: Legal Issues, Contracts, and Electronic Discovery
Defining Cloud Computing and Essential Characteristics
Standard Definition of the Cloud

NIST Definition of Cloud Computing
ISO IEC 17788: Definition of Cloud Computing
Summary

Lesson 2:
Understanding Cloud Deployment and Service Models
Chapter 6: Management Plan E and Business Continuity
Chapter 7: Infrastructure Security
Cloud Deployment Models
Cloud Service Models
CSA’S Logical Model
M3 C4 Summary

Lesson 3:
Establishing a Secure Cloud Architecture
Chapter 8: Virtualization and Containers
Chapter 9: Incident Response
Chapter 10: Application Security
Chapter 11: Data Security and Encryption
Chapter 12: Identity, Entitlement, and Access Management
CSA Enterprise Architecture
CSA-BOSS Pillar
CSA–ITOS Pillar
CSA–Services Pillar
CSA–Risk Management Pillar
NIST Cloud Computing Reference Architecture
Using the Cloud Control Matrix
Selecting a CSP
Summary and labs

Lesson 4:
Understanding Governance and Enterprise Risk Management in the Cloud
Chapter 1: Cloud Computing Concepts and Architectures
Chapter 2: Governance and Enterprise Risk Management
Understanding Governance and Enterprise Risk Management In the Cloud
Review of Governance Frameworks Cloud Governance Tools
Enterprise Risk Management Frameworks
Risks Related to Service and Deployment Models
Summary and labs

Lesson 5:
Maintaining Compliance and Audit Management in the Cloud
Appendix A: Cloud Security Lexicon
Appendix B: Cloud Security Standards and Certifications
Appendix C: Sample Cloud Policy
Compliance Objectives
Industry Specific Compliance
Cloud Audit Management
Attestation of Cloud Controls
Certification of Cloud Controls

Summary
Lesson 6:
Compiling Legal Issues, Contract, and Electronic Discovery
Chapter 4: Compliance and Audit Management
Chapter 5: Information Governance
Common Concerns for Cloud Data Privacy
Country and Regional Data Privacy Laws
European Union and European Economic Area
The Americas
Electronic Discovery
Cloud Data Security Lifecycle
Summary

Earning the CCSK will provide you with the knowledge to effectively develop a holistic cloud security program relative to globally accepted standards. It covers key areas, including best practices for IAM, cloud incident response, application security, data encryption, SecaaS, securing emerging technologies, and more. If you want to learn more, you can the CCSK guide.
Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President.

SU Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

IDS II ON-SITE LOG ANALYSIS, EVENT CORRELATION AND RESPONSE PRACTICUM

Real-Time Tools and Methodologies for Discovering and Reacting to Network Intrusion Attempts

Q/CND® Qualified/ Cyber Network Defense Certificate program of Mastery CPoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, SecurityX or CISSP) Practicals as evidence to support the claim of knowing something
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class w/exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert w/exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class w/exam
Q/MC® Qualified/ Mission Critical Certification Class w/exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class w/exam
SU Security+® CompTIA Certification Class w/exam
SU SecurityX ® [formerly CASP] Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
Linux/UNIX® Security Certification Class w/exam
SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class w/exam
Cloud Computing Security Knowledge Certification (CCSK) Class w/exam
IDS II: On-site Log Analysis, Event Correlation and Response Practicum
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This 72 hour practicum investigates how to strengthen network and enterprise threats. You will compare managed services to make informed decisions about which is best suited to your organization. You will explore the pros and cons of perimeter defenses and deep internal defenses. Hacker attack labs will enrich your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you complete this performance based practicum you will know where to position sensors and consoles to reduce risk across the entire enterprise; write scripts to reduce risk, understand the types of responses you will receive; and how to react to alerts using live countermeasures.

Class Fee:	$3,990
Time:	72hrs
Learning Level:	Advanced
Contact Hours:	72 hours 4 weeks
Prerequisites:	m Basic competency with TCP/IP &
Credits:	Linux. 72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD

Method of Evaluation: 95 % attendance 2. 100 % completion of Lab
Grading: Pass = Attendance+ labs & quizzes Fail > 95% Attendance

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/ Security Engineer
Security Solutions Architect
Systems Engineer/ Systems Security Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, and final practicum.
KU Outcomes

* Students will be able to write a system incidence response policy.
* Students will be able to describe and write various risk analysis methodologies.
* Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
* Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Cyber Threat Vector on live cyber range
Validating the Threats: Hacker Attack Methods

- cyber range threats
- reconnaissance
- mapping networks
- access points
- relationships between systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

IDS II Insider threat on-site Log Analysis, Event Correlation and Response Practicum
Insider threat is one of the most dangerous security threat, and a much more complex issue. These insiders can be a former or a disgruntled employee or any business associate that has or had an authorized access to information for any particular organization. They have control and security measures. Hence continuous monitoring is essential to track each and every activity within the network. Log management is a strong technique which includes both Log analysis with event correlation which provides the root cause of any attack and network can be protected from security violations. Though intrusion detection is complex process, while checking the ability to detect intrusive behavior within the internal environment, it has to take care of suppressing the false alarm rate. Some strong approach is required on the basis of which decisions can be taken fast.

This 72 hour practicum class investigates how to strengthen network- and host-based intrusion detection systems (IDS). You will use and report on tools that log data risk and review and compare threats to make informed decisions about which is best suited to the task at hand. You will decide what best works for perimeter defenses and deep internal defenses. You will build unique Hacker attack scenarios to demonstrate your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you leave this cutting-edge class, you will provide a schematic of where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. **Books** - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below

SU Q/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

Hands On

IDS III ON-SITE LOG ANALYSIS, EVENT CORRELATION AND RESPONSE PRACTICUM

Real-Time Tools and Methodologies for Offensive Reaction to Network Intrusion Attempts

This 72 hour class investigates how to offensive countermeasures strengthen network. You will explore the leading offensive security products on the market today, You will compare managed services to make informed decisions about which is best suited to your organization. You will explore the pros and cons of perimeter defenses and deep internal defenses. Hacker attack labs will teach you offensive methodologies, master your port scanning skills, learn advanced level exploitation of buffer overruns, and other network assaults in action. When you leave this mastery level practicum, you will how to defend the network, how best to position sensors and consoles; the types of responses you will receive; and how to react to alerts using todays advanced offensive countermeasures.

Class Fee:	$3,990
Time:	72hrs
Learning Level:	Advanced
Contact Hours:	72 hrs
Prerequisites:	Basic competency with TCP/IP & Linux.
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 2. 100 % completion of Lab
Grading:	Pass = Attendance+ labs & quizzes Fail > 95% Attendance

Sample Job Titles
Information Assurance (IA) Architect
Information Security Architect
Information Systems Security Engineer
Network Security Analyst
Research & Development Engineer
Security Architect/ Security Engineer
Security Solutions Architect
Systems Engineer/ Systems Security Analyst

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, and final practicum.
KU Outcomes

* Students will be able to write a system incidence response poliy and define offensive countermeasure for the entire enterprise.
* Students will be able to describe and write various risk analysis methodologies and offensive countermeasures..
* Students will be able to evaluate and categorize risk 1) with respect to offensive technology; 2) with respect to individual threats, and 3) in the enterprise, and recommend appropriate offensive responses.
* Students will be able to compare the advantages and disadvantages of various offensive attack methodologies.
* Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

11. What You Can Expect in the Future

Cyber threat evasion and threat mitigation
Validating the Threats: Hacker Attack Methods

- hacker attacks: a demo
- reconnaissance
- mapping networks
- access points
- relationships between systems
- physical and logical locations of systems
- types of systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

Cyber Threat Vector on live cyber range
Validating the Threats: Hacker Attack Methods

- cyber range threats
- reconnaissance
- mapping networks
- access points
- relationships between systems
- system configuration
- services offered
- user information• security mechanisms
- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

IDS III On-site Log Analysis, Event Correlation and Response Certification Class Practicum
Insider threat is one of the most dangerous security threat, and a much more complex issue. These insiders can be a former or a disgruntled employee or any business associate that has or had an authorized access to information for any particular organization. They have control and security measures. Hence continuous monitoring is essential to track each and every activity within the network. Log management is a strong technique which includes both Log analysis with event correlation which provides the root cause of any attack and network can be protected from security violations. Though intrusion detection is complex process, while checking the ability to detect intrusive behavior within the internal environment, it has to take care of suppressing the false alarm rate. Some strong approach is required on the basis of which decisions can be taken fast.

This 72 hour practicum class investigates how to strengthen network- and host-based intrusion detection systems (IDS). You will use and report on tools that log data risk and review and compare threats to make informed decisions about which is best suited to the task at hand. You will decide what best works for perimeter defenses and deep internal defenses. You will build unique Hacker attack scenarios to demonstrate your skills of port scanning, exploit buffer overruns, and other network assaults in action. When you leave this cutting-edge class, you will provide a schematic of where to position sensors and consoles; the types of responses you will receive; and how to react to alerts using industry-standard IDS countermeasures.

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. **Books** - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery Hands On
HOW TO CONDUCT NETWORK VULNERABILITY ANAYLSIS CLASS W/EXAM

This course will teach you how to find vulnerabilities in systems and software by teaching the process that a hacker uses when they target an organization. One of the critical things for anyone who wants to learn either how to defend or even attack a network, is the ability to find and analyze system or network vulnerabilities. In this course, How to Conduct a Network Vulnerability Analysis, you will learn to how to follow a systematic methodology to identify potential vulnerabilities. Using passive and active vulnerability scanning methods you evaluate what threats vectors are on your network, and learn how to take the results of this data and analyze it to determine the vulnerabilities that can be used to attack, or identify the risk that needs to be mitigated. This science teaches you best practices and how to deploy three of the most popular vulnerability scanners and conduct comparisons of them. When you complete this course you'll have the knowledge and skills needed to identify vulnerabilities and act appropriately to mitigate cyber risk.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of labs

Grading: Pass = Attendance +Labs& Quizzes   Fail > 95% Attendance
This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Class Materials – SU class textbook, Labs and resources CD
KU Outcomes - this course will teach you how to find vulnerabilities
Students will be able to evaluate and categorize risk using 3 scanning tools

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Did you hear about North Korea hacking Sony Pictures? Or about Stuxnet, one of the most sophisticated APT affecting nuclear plants in Iran? This exciting certification will require clearing CMSD first to be able to start learning how to dissect nation-state-sponsored attacks! You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware!

Learning Objectives -

You will learn techniques to dynamically instrument Student projects include performing vulnerability assessments. You cannot talk about vulnerability assessments without also mentioning penetration testing. Although both processes serve to protect a networked environment, they are not the same thing. The two terms are sometimes incorrectly used interchangeably. In a vulnerability assessment, an exploitable flaw is identified and alleviated. The process is mostly automated to cover a wide variety of unpatched vulnerabilities. Penetration testing, is focused on real-life cyberattacks to see how a hacker can breach defenses. This testing involves both automated tools and a human to mimic an attacker. Penetration testing can help identify even the most minute security problem, such as unencrypted passwords and inadequate security settings. And because penetration testing is also a vulnerability test, it should be conducted regularly to ensure consistent IT and network security management.

The different types of vulnerability assessments
Vulnerability assessments can help you find potential exploits before hackers start snooping, ensure your systems remain up to date and patched, create a proactive focus on information security, and ultimately help your organization maintain its reputation.
There are various types of vulnerability assessments. They include: Network-based assessment As the name suggests, this scan helps pinpoint possible flaws on wired and wireless networks. Database assessment -This assessment involves locating security loopholes in a database to prevent malicious attacks, such as distributed denial-of-service (DDoS), SQL injection, brute force attacks, and other network

vulnerabilities. Web application assessment - This scan involves a careful evaluation of web applications and their source code to find any security holes. The process can be done manually or automated. -Host-based assessment This type of assessment examines any possible weaknesses or threats in server workstations and other network hosts. It also involves a meticulous examination of ports and services. Wireless network assessment -This scan validates whether an organization's wireless infrastructure is securely configured to prevent unauthorized access.

Lesson 1
Class covers the physical layers of the file system (from the physical platters to the file name layer that contains file names and a directory
Course Lessons -

Lesson 2 Intro and lab set up

- Introduction
- Course Virtual Machines
- Downloading and Installing Nmap
- Demo: Downloading and Installing Nmap

Lesson 3 Performing the Scanning Methodology

- Introduction
- Demo: Non-intrusive Target Search
- Defining Intrusive Target Search
- Demo: Finding Live Systems
- Identifying Ports and Services
- Demo: Scanning Ports and Services
- Enumerating and Identifying Vulnerabilities
- Demo: Enumerating System Information
- Module Summary

Lesson 4 Leveraging the Internet to Find Vulnerabilities

- Overview
- Demo: Exploring Search Engine Capability
- Examining Common Vulnerability Sites
- Demo: Leveraging Vulnerability Sites
- Module Summary
- Module Summary 2

Lesson 5 Understanding the Types of Vulnerability Scanning
Overview and Passive Analysis

- Demo: Conducting Passive Analysis
- Actively Scanning for Flaws
- Demo: Conducting Active Scanning
- Reviewing Vulnerability Scanning Tools
- Module Summary

Lesson 6 Executing Vulnerability Scanning

- Overview
- Demo: Nessus
- Introducing Nexpose
- Demo: Nexpose
- Introducing OpenVAS
- Demo: OpenVAS
- Vulnerability Scanner Comparison
- Module Summary

Lesson 7 Conclusion

- Course Conclusion and Next Steps

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
PYTHON FORENSIC CERTIFICATION CLASS W/EXAM

Nowadays it is common practice amongst ethical hackers to write nifty scripts and automate any structured process, ranging from small network scans to wide area network packet sniffing. In recent years, Python has become the language of choice for such tasks, and there are good reasons for this. In this class you will learn ethical hacking using Python, we will discuss the reasons that make these two such a brilliant couple. Below is the list of topics we shall be going over: What is ethical hacking? What is Python? Why use Python for thical hacking? Simple dictionary attack using Python What is Ethical Hacking? The term hacking goes a long way back. To be exact, it all started at the Railroad Club of MIT, where both the term 'hacking' and 'hacker' were first coined. It's been almost 50 years now, and hacking has evolved into a discipline in the current day and age. With the increase in awareness regarding data protection and data privacy, hacking has been deemed as an illegal activity today. If caught, there's a good chance that you will be prosecuted for quite some time depending on the degree of harm caused. None the less, to protect themselves from hackers of all sorts, employment of Ethical Hackers has become a common practice amongst organizations. Ethical hackers are given the responsibility of finding and fixing security flaws for a certain organization before black hat hackers find them.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	TCP/IP knowledge
Credits:	72 CPE / 3 CEU
Method of Delivery:	face-to-face
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab
Grading: Pass = Attendance +Labs& Quizzes	Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Class Materials – SU class textbook, Labs and resources CD

KU Outcomes

Students will be able to hack using python.

Students will be able to describe how to use python to write break code

Students will be able to evaluate and categorize risk using Pthon coding

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Below is the list of topics we shall be going over: What is ethical hacking? What is Python? Why use Python for thical hacking? Simple dictionary attack using Python What is Ethical Hacking? The term hacking goes a long way back. To be exact, it all started at the Railroad Club of MIT, where both the term 'hacking' and 'hacker' were first coined. It's been almost 50 years now, and hacking has evolved into a discipline in the current day and age. With the increase in awareness regarding data protection and data privacy, hacking has been deemed as an illegal activity today. If caught, there's a good chance that you will be prosecuted for quite some time depending on the degree of harm caused. None the less, to protect themselves from hackers of all sorts, employment of Ethical Hackers has become a common practice amongst organizations. Ethical hackers are given the responsibility of finding and fixing security flaws for a certain organization before black hat hackers find them

Learning Objectives -

You will leais a general-purpose scripting language that has gained immense popularity amongst professionals and beginners for its simplicity and powerful libraries. Python is insanely versatile and can be used for almost any kind of programming. From building small scale scripts that are meant to do banal tasks, to large scale system applications – Python can be used anywhere and everywhere. In fact, NASA actually uses Python for programming their equipment and space machinery. Python can also be used to process text, display numbers or images, solve scientific equations, and save data. In short, Python is used behind the scenes to process a lot of elements you might need or encounter on your devices.

Lesson 1
Why use Python for Ethical Hacking?
Python for super users skills
Python for use libraries.
Building python libraries
AI artificial intelligence has Pytorch and Tensorflow
Data Science has Pandas, Numpy, Matplotlib.

Lesson 2
Similarly, Python is brilliant for ethical hacking for the following;
Cyber Security Training
Nifty python libraries like Pulsar,
NAPALM, NetworkX etc make developing network tools a breeze
Ethical hackers generally develop small scripts
Python scripting language for juice performance - small programs - big programs
Python as a community tool
Learning Python for career opportunities

Lesson 3
Dictionary Attack using Python
Let us create a small Python program that can be used to crack a password using the dictionary attack

Lesson 3-
Python is a very simple language yet powerful scripting language, it’s open-source and object-oriented and it has great libraries that can be used for both for hacking and for writing very useful normal programs other than hacking programs. In the future and present era python is very popular and it’s easy to learn, learning to hack with python will be fun and you will learn python programming in the best way. What you will learn Code your own reverse shell (TCP and HTTP).

Lesson 4
Learn various concepts such as cryptography, computer networks & security, application security, idAM (identity & access management), vulnerability analysis, malware threats, sniffing, SQL injection, DoS, session hijacking, and various security practices for businesses from scratch with hands-on demonstrations. Enroll in this Cyber Security certification training program to learn from experienced industry professionals, work on real-time projects and become a certified expert..

Lesson 5
Root - since Python is basically part of every single Linux install, you could do a shitton retrieving system and user information by just using the normal packages. You won't even need to install nmap or similar; using plain Python packages, you could check which services are running and such.).

Lesson 6
Gives information on useful tools every penetration tester/hacker should have in their arsena
snippet of codes to fix and learn
everything from writing network sniffers,
stealing email credentials,
bruteforcing directories
crafting mutation fuzzers
investigating virtual machines,
creating stealthy trojans.

Lesson 7
Python 3.x bit shifting
code hygiene
offensive forensics with the Volatility Framework
expanded explanations of the Python libraries ctypes, struct, lxml, and Beautiful Soup,
offensive hacking strategies like splitting bytes, leveraging computer vision libraries, and scraping websites.

- Create a trojan command-and-control server using GitHub
- Detect sandboxing and automate common malware tasks like keylogging and screenshotting
- Extend the Burp Suite web-hacking tool
- Escalate Windows privileges with creative process control
- Use offensive memory forensics tricks to retrieve password hashes and find vulnerabilities on a virtual machine
- Abuse Windows COM automation
- Exfiltrate data from a network undetected

When it comes to offensive security, you need to be able to create powerful tools on the fly. You will not find a lab this extensive anywhere else! Overall: All in all this course is so relevant and so practicum that there is no reason not to put this one on your wishlist

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
PYTHON POWERSHELL INCIDENT RESPONSE CERTIFICATION CLASS W/EXAMC

Hands On

Nowadays most of the windows-based attacks are happening around PowerShell. As an Incident Responders, you should know your way around PowerShell especially on how the attackers can leverage PowerShell in various ways within the attack lifecycle. The aim of this article is to give a glimpse of different techniques in the PowerShell arsenal which can aid responders in hunting activities. This course focus is on battling the much maligned Advanced Persistent Threat (APT). This course is up to date with the latest forensics techniques. Incident management is an often-debated, frequently misunderstood topic that can quickly befuddle even the most advanced security teams. So to clear things up, we took “lessons learned” from successes and failures over the years. And while it may not answer every question you may have about modern incident response, we hope that it sets the wheels in motion for something better than what you have today.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (face-to-face) or Hybrid TBD
Instructor: TBD	
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs& Quizzes Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation. Class Materials – SU class textbook, Labs and resources CD

KU Outcomes

Students will be able to write a script in powershell.

Students will be able to describe how to use powershell to write various risk incident and analysis methodologies.

Students will be able to evaluate and categorize risk using powershell incident response

Text Materials: labs, SU Pen Testing Materials, resource CD’s and attack handouts -Machines a Dual Core 486M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Did you hear about North Korea hacking Sony Pictures? Or about Stuxnet, one of the most sophisticated APT affecting nuclear plants in Iran? This exciting certification will require clearing CMSD first to be able to start learning how to dissect nation-state-sponsored attacks! You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware!

Learning Objectives -

You will learn techniques to dynamically instrument binaries during execution with PinTool, or how to create Immunity Debugger plugins to hook malicious APIs. You will have the chance to understand and practice how to dissect the most sophisticated APT in our era, The Equation Group and see how they are able to hide their presence within hard drives by reprogramming the firmware! This course is a enrichment style lab immersion concept:

This class has recently been retooled to focus on battling the much maligned Advanced Persistent Threat (APT). The class motto is "APT is in your network, start hunting". The APT focus makes it 100% relevant to not just forensic investigators, but to anyone wanting to learn to defend their network. The Material - this course is a smorgasbord of valuable skills and information for incident responders, system administrators, and forensicators alike.

Lesson 1

Class covers the physical layers of the file system (from the physical platters to the file name layer that contains file names and a directory structure), and how to properly mount images for analysis (e.g. read only). Just when you think the first day couldn't cover any more information the class jumps into the exciting world of Enterprise Analysis and Live System Incident Response (my favorite!!). This portion teaches students about domain authentication, how to secure domain administrator credentials, and many methods of accessing system information on remote of hosts (Many of my future blog posts will revolve around utilizing PowerShell for "Live System 'Enterprise' Incident Response" for lack of a better term).

Lesson 2
The second day is spent covering memory forensics. Memory Forensics covers the details of memory (memory structures and such), and how to implement memory forensics TODAY. Students will learn how to acquire memory, as well as, how to provide in depth analysis of the memory once acquired. Memory forensics is absolutely necessary when combating APT as it is one of the best, if not only, methods to detect rootkits. The best part of lesson 2 is that it doesn't focus on one method of analyzing memory. We spend the time to teach students the pros and cons to different tools, and even different methods of using the same tool.

Lesson 3
is dedicated to timeline analysis. No one should be considered a forensicator or incident responder if they do not have an intimate knowledge of timeline analysis (Specifically using log2timeline). Log2timeline came out of a GCFA Gold Paper written by Kristinn Guðjónsson, and the community has never looked back. Log2timeline is really a cultural shift in the way we perform investigations, as it aggregates almost every forensic artifact into one timeline that truly tells the story of actions taken on a machine. We will interpret a specific artifact, then you lose fidelity in your timeline (possibly the opportunity to spot malicious activity).

Lesson 4 and 5
begin with XP Restore Point and Volume Shadow Copy analysis which can be harnessed for some really cool stuff. We can use these snapshots to add fidelity and depth to our timeline, and we can use them to recover deleted files. Then deep dive forensics (This is where the class dives into the weeds of file system analysis). The class dives into $MFT analysis which introduces us to a second set of timestamps ($STDINFO), and new artifacts like the NTFS TriForce (David Cowen's baby). These artifacts are presented in this class –and we wraps up with methods and techniques of finding unknown malware. Assuming anti-virus fails to detect a threat, what are some methods we can use for detection? This class end introduces and spends half a day discussing the concept of malware funneling which is the process of reducing data through a series of automated tasks until you have a small enough data set that you can perform manual analysis. Labs (1-6): After the lesson students spend the rest of the lesson in the lab as a team exercise. The team investigates a set of hosts that were part of an intrusion, however this is not your normal everyday exercise....this is where it gets interesting!

This course is developed around an "as real as it gets" scenario. The scenario is about an R&D firm that makes a great discovery, only to be hacked by APT. Students are given four hosts to conduct forensic investigations to determine what happened. Questions like the initial infection vector, when the initial infection occurred, what data was lost, and the current state of the network can be answered.
When we talk about this lab it is important to understand the level of detail used to create this virtual network. Not only did the network have 100s of hosts and 1000s of users, we ensure this network was as real looking as possible. We hired a professional Red Team and trained them up to act like APT, he hired domain architects to build the domain in a professional/secure manner, and he even loaded the systems with some of the latest security tools. You will not find a lab this extensive anywhere else!
Overall: All in all this course is so relevant and so practical that there is no reason not to put this one on your wishlist.

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery non-degree
Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Workshop
Q/EH® Qualified/ Ethical Hacker Certification Class w/exam
Q/ND® Qualified/ Network Defender Certification Class w/exam
Q/FE® Qualified/ Forensic Expert Certification Class w/exam
SU CISSP® Certified Information Security Systems Professional Class
SU Security+® CompTIA Certification Class w/exam
SU SecurityX® - [formerly CASP] Certification Class w/exam
Linux/UNIX® Security Certification Class w/exam
Cloud Computing Security Knowledge Certification Class w/exam
Q/PTL® Qualified/ Penetration Tester License Practicum
Q/ND® Qualified/ Network Defender Practicum
Q/FE® Qualified/ Forensic Expert Practicum

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
POWERSHELL FORENSIC CERTIFICATION CLASS W/EXAM

Even for seasoned PowerShell users, a deep and robust understanding of the language fundamentals can be incredibly powerful for writing more efficient, readable, and usable code. Section 1 of the course focuses on building a solid foundation upon which more complex use cases can then be constructed. With a focus on Blue Team specific functions, well frame the discussion around the PowerShell basics in terms that will be immediately useful for students. For example, common data structures are discussed as a fundamental aspect of PowerShell and immediately applied as Blue Team triage and analysis tactics. This base is built from the ground up and accessible to students with no prior scripting experience, but with enough nuance to shed light on the "why does it work this way" question for more seasoned PowerShell users. For professionals already familiar with the basic concepts, PowerPlay offers an interactive, out-of-band challenge system for students to drill various concepts and techniques related to the course material.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	TBD
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance +Labs & Quizzes   Fail > 95% Attendance

Text Materials: labs, SU Pen Testing Materials, resource CD's and attack handouts

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

This course Effective Blue Teams work to harden infrastructure, minimize time to detection, and enable real-time response to keep pace with modern adversaries. Automation is a key component to facilitate these capabilities, and PowerShell can be the glue that holds together and enables the orchestration of this process across disparate systems and platforms to effectively act as a force multiplier for Blue Teams. This course will enable Information Security professionals to leverage PowerShell to build tooling that hardens systems, hunts for threats, and responds to attacks immediately upon discovery.
Now that we have a strong understanding of the fundamentals, this course section focuses on ways to weaponize PowerShell both from an offensive and defensive perspective. The section begins with a focus on offensive PowerShell use cases. Threat actors have long used PowerShell as an attack platform, delivering fileless malware and living off the land using built-in capabilities. The next section turns this discussion around and focuses on the Blue Team aspects of controlling PowerShell execution.
The section then dives deep into log analysis and data parsing and discovery. The goal is to maximize the utility of native features of operating systems and applications while fully understanding how to find important data. If Blue Teams can identify sensitive data in unexpected locations, those data can be handled or protected properly. The section concludes with a discussion of PowerShell as a platform to enable Blue Teams to work within DevOps development practices. As modern development teams transition practices, Blue Teams must adapt. Automation plays an important role in this process, as Blue Teams fight to scale capabilities to match modern development frameworks. PowerShell provides this automation platform and can be the catalyst to enable continuous assurance of critical business services. PowerShell is uniquely positioned for this task of enabling Blue Teams. It acts as an automation toolset that functions across platforms and it is built on top of the .NET
Students will learn scripting fundamentals from the ground up with respect to the capabilities of PowerShell as a defensive toolset

- Ways to maximize performance of code across dozens, hundreds, or thousands of systems
- Modern hardening techniques using Infrastructure-as-Code principles
- How to integrate disparate systems for multi-platform orchestration
- PowerShell-based detection techniques ranging from Event Tracing for Windows to baseline deviation to deception
- Incident Response techniques leveraging PowerShell-based automation

This course is meant to be accessible to beginners who are new to the PowerShell scripting language as well as to seasoned veterans looking to round out their skillset. Language fundamentals are covered in-depth, with hands-on labs to enable beginning students to become comfortable with the platform. For skilled PowerShell users who already know the basics, the material is meant to solidify knowledge of the underlying mechanics while providing additional challenges to further this understanding.

The PowerPlay platform built into the lab environment enables practical, hands-on drilling of concepts to ensure understanding, promote creativity, and provide a challenging environment for anyone to build on their existing skillset. PowerPlay consists of challenges and questions mapping back to and extending the course material. Between the course material and the PowerPlay bonus environment, students will leave the course well equipped with the skills to automate everyday cyber defense tasks. You will return to work ready to implement a new set of skills to harden your systems and accelerate your capabilities to more immediately detect and respond to threats. Exercises - Hands-on PowerShell: Get comfortable with PowerShell cmdlets, objects, and the pipeline to start making meaningful tools. Triage the VM: Quickly understand the state of a system, from networking details to process execution and removable devices Scripting in PowerShell: Leverage an understanding of the language basics to build high-quality tooling that will be supportable by Blue Teams. Debugging: Save time and frustration, easily identifying complex bugs in PowerShell through built-in debugging capabilities and Pester tests Source Control: Become familiar with Git concepts to effectively manage version control

Lesson1
Getting to Know PowerShell
Background and history
Why PowerShell is such a good fit for Blue Teams
How to use commands and find them
Objects and pipelines as PowerShell differentiators
Extending PowerShell with .NET

Lesson 2
Blue Team Use Cases
Network inspection
Triage at the operating system level
File discovery and inspection
Language Basics

Lesson 3
Variables, data structures, and flow control
Input and output
Functions and script blocks
PowerShell Environment
Customizing the console
Common development environments

Lesson 4
Debugging
Static code analysis
Tracing and breakpoints
Helpful tools like Pester and PSScriptAnalyzer
Source Control
Git terminology

Lesson 5
Creating repositories and branches
Managing code with pull requests
Driving release pipelines from source control

Lesson 6
Exercises
Offensive PowerShell: Build a fileless keylogger that automatically exfiltrates keystrokes to cloud storage
Controlling PowerShell: Analyze the impact of a stronger security posture surrounding PowerShell usage in the enterprise.
Efficient Log Analysis: Understand how to efficiently analyze and filter Windows events and plaintext log files, and find attacks within sample log files

Parsing and Discovery: Build tools to extract important data from unstructured text-based logs and use these same techniques for sensitive data discovery
DevOps: Leverage PowerShell as an orchestration engine, building containers for automated web application scanning and identifying potentially compromised containers in the environment

Lesson 7
Offensive PowerShell
Common tactics used by attackers leveraging PowerShell
Fileless implementation techniques
NET utilization by PowerShell-based attack tools
Controlling PowerShell
Limiting attack surface on PowerShell-enabled systems
Controlling, not attempting to block, PowerShell in the enterprise
Just Enough Administration for enabling secure usage of administrative PowerShell sessions
Log Analysis
Enabling appropriate logging
Reading and filtering Windows Event Logs
Reading and filtering plaintext logs
Text Parsing
Regular expressions and string operations to enable efficient parsing
DevOps
Automating static and dynamic application security testing
Pipeline assurance automation
Container interaction, security assessment, and triage

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
ADVANCED CLOUD SECURITY AND APPLIED SECDEVOPS CERTIFICATION CLASS W/EXAM

This class provides the advanced knowledge needed to implement cloud services and enables you to gain critical insights into topics such as data security, key management, and identity and access management and speak with confidence about cloud security concerns.

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2hr exam
Prerequisites:	Understanding of TCP/IP Protocols
Credits:	72 CPE/ 3 Credit
Method of Delivery:	Residential (face-to-face) or Hybrid TBD
Instructor:	
Method of Evaluation:	95 % attendance 100 % completion of Lab

This accelerated class is taught using face to face modality or hybrid modality [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.
Machines a Dual Core 16M Ram, 1TGig drives, running MS OS, linux, and VMWare Workstation.

Who Is This Program For?
Cloud Computing Analyst, Cloud Administrator, Cloud Architect, Cloud Engineer, Enterprise Architect, Security Administrators, Security Architect and Systems Engineer are cloud security job roles.

This 72hr in-depth fully immersed cloud platform technology class provides a hands-on review of how the services are built and managed, and the security implications. We will then quickly start building out a sandbox environment and deploying security controls.
Some of the topics and techniques covered will include (at a minimum):

Use of accounts for managing blast radius.
Building out advanced cloud virtual networks.
Leveraging inherent cloud capabilities for network security.
Use of DNS management, auto scale groups, load balancers, and other technologies for immutable infrastructure. Advanced Identity and Access management for cloud, including setting up SAML federation across providers. Privileged user management, MFA, and other access essentials.
Securing serverless, PaaS and mixed IaaS/PaaS architectures.

Focuses on designing secure architectures, integrate with evOps, and build your own SecDevOps toolkit for managing cloud security at scale:
Fundamentals of SecDevOps.
Building secure deployment pipelines.
Integrating automated security testing into deployment pipelines.
Cloud security architectural patterns for major application types.
Cloud data security and encryption.
Automating continuous security monitoring and alerting using cloud native capabilities.
Security automation through the console.
Security automation through code.
Scaling your security operations to hundreds (or thousands) of accounts through automation.

Students should have basic familiarity with at least one public cloud provider (Amazon or Azure) and hands-on experience launching and managing basic instances/services. They should also be comfortable with the command line and basic scripting. Additionally we highly encourage students to understand basic Ruby programming for the coding portions. Code snippets will be provided, so students with experience in other languages should be able to keep up. This is a very broad, advanced training that requires a diverse skills set to complete all the labs. Students may fall behind in certain sections due to the rapid pace but the labs can all be completed outside of the training environment if needed. Only about 10% of those who take the class have the background to complete every hands-on portion but we ensure through lecture that everyone gains the needed knowledge.

Q/ISP Qualified/ Information Security Professional Certificate Program of Mastery
TCP/IP AND KEY FEATURE OF WIRESHARK CERTIFICATION CLASS W/ EXAM

One of the critical things for anyone who wants to learn either how to defend or even attack a network, is the ability to find and analyze system or network vulnerabilities. Wireshark is a free open-source packet analyzer that is the number one tool for network analysis, troubleshooting, software and communications protocol development, and related education in networking. When you are finished with this course, you will be able to perform network analysis for communications troubleshooting and forensics. Students will learn the contents & concepts of TCP/IP and Wireshark and how they should work together to provide true in-depth cyber security.

Sample Job Title
Chief Information Security Officer (CISO)
Common Control Provider/ Cybersecurity Officer
Enterprise Security Officer /Facility Security Officer
Information Systems Security Manager (ISSM)
Information Technology (IT) Director
Principal Security Architect/ Risk Executive
Security Domain Specialist
Senior Agency Information Security (SAIS) Officer

Class Fee:	$3,990
Time:	72 hrs
Learning Level:	Entry
Contact Hours:	40 hr 1 wk + 32 hr pre-study & 2h exam
Prerequisites:	TCP/IP Protocols Knowledge
Credits:	72 CPE / 3 CEU
Method of Delivery:	Residential (100% face-to-face) or Hybrid
Instructor:	register at Pearson Vue Testing Center
Method of Evaluation:	95 % attendance 100 % completion of Lab

Grading: Pass = Attendance + Completion of Labs and Practicum for CPoM Fail > 95% Attendance

This accelerated class is taught using face to face modality or hybrid modality, [excluding veterans using the Veterans Education benefits, can only attend in the face to-face modality]. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

Text Materials: SU TCP/IP class handbook, labs, online quizzes SU resource CD's and 500 exam questions.
No tools for this class, students bring on their own laptop machines with www.freepractice test.com and exam force pre installed.

Becoming a Wireshark Certified Network Analyst™ validates your ability to use Wireshark to perform network analysis for communications troubleshooting and forensics. Achieving Wireshark certification also demonstrates that you have experience troubleshooting, optimizing, and securing a network based on evidence found by analyzing traffic captured with Wireshark. It indicates your aptitude in TCP/IP network communications and is an ideal complement to CISSP, CCIE, CompTIA Network+, and other industry certifications.
Who Should Attend? Anyone interested in learning to troubleshoot and optimize TCP/IP networks and analyze network traffic with Wireshark, especially network engineers, information technology specialists, security analysts, and those preparing for the Wireshark Certified Network Analyst exam.

About Wireshark: Wireshark is a widely deployed open-source program that enables users to inspect hundreds of protocols and perform live capture and offline analysis. It has a broad set of features and runs on a variety of platforms, including Windows, OS X, and Linux. With more than 500,000 downloads per month, the Wireshark network analyzer is quickly becoming the industry standard.
Our Wireshark Training Optimize TCP/IP networks with Wireshark®. This hands-on, in-depth course provides the skills to isolate and fix network performance issues. Learn how Wireshark can solve your TCP/IP network problems by improving your ability to analyze network traffic. Our course emphasizes hands-on labs (27 in all) and real-world scenarios that will help you put theory into practice and give you the classroom experience to implement what you learn as soon as you get back to the office. Our Wireshark training class includes traffic capturing and filtering, 10 key troubleshooting steps, and case studies delivered by instructors with years of packet-level experience.

The certification exam is based on four, primary areas:
Wireshark functionality
TCP/IP network communications
Network troubleshooting
Network security

Required Exams -You'll take one action-packed course to prepare for the Wireshark Certified Network Analyst Exam. In addition, through a simple Wireshark experiment, you will see the TCP/IP packets and security systems in action that are serving your PC/laptop, that serves you.

Here's an overview of what we cover in our TCP/IP Prep Training Course:

Lesson 1.

Introduction to Network Analysis and Wireshark
TCP/IP Analysis Checklist
Top Causes of Performance Problems
Get the Latest Version of Wireshark
Capturing Traffic
Opening Trace Files
Processing Packets
The Qt Interface Overview
Using Linked Panes
The Icon Toolbar
Master the Intelligent Scrollbar
The Changing Status Bar
Right-Click Functionality
General Analyst Resources
Your First Task When You Leave Class

2.

Learn Capture Methods and Use Capture Filters Analyze Switched Networks
Walk-Through a Sample SPAN Configuration
Analyze Full-Duplex Links with a Network TAP Analyze Wireless Networks
USB Capture
Initial Analyzing Placement
Remote Capture Techniques
Available Capture Interfaces
Save Directly to Disk
Capture File Configurations
Limit Your Capture with Capture Filters
Examine Key Capture Filters

3.

Customize for Efficiency: Configure Your Global Preferences
First Step: Create a Troubleshooting Profile Customize the User Interface
Add Custom Columns for the Packet List Pane
Set Your Global Capture Preferences
Define Name Resolution Preferences
Configure Individual Protocol Preferences

4.

Navigate Quickly and Focus Faster with Coloring Techniques
Move Around Quickly: Navigation Techniques
Find a Packet Based on Various Characteristics
Build Permanent Coloring Rules
Identify a Coloring Source
Use the Intelligent Scrollbar with Custom Coloring Rules
Apply Temporary Coloring
Mark Packets of Interest

5.

Spot Network and Application Issues with Time Values and Summaries
Examine the Delta Time (End-of-Packet to End-of-Packet)
Set a Time Reference
Compare Timestamp Values
Compare Timestamps of Filtered Traffic
Enable and Use TCP Conversation Timestamps
Compare TCP Conversation Timestamp Values Determine the Initial Round Trip Time (iRTT) Troubleshooting Example Using Time
Analyze Delay Types

6.

Create and Interpret Basic Trace File Statistics
Examine Trace File Summary Information
View Active Protocols
Graph Throughput to Spot Performance Problems Quickly
Locate the Most Active Conversations and Endpoints Other Conversation Options
Graph the Traffic Flows for a More Complete View
Burst Statistics
Numerous Other Statistics are Available
Quick Overview of VoIP Traffic Analysis
SIP and RTP Analysis Overview
SIP Call Setup
Analyzing Call Setup with SIP
Session Bandwidth and RTP Port Definition

7.

Focus on Traffic Using Display Filters
Display Filters
Filter on Conversations/Endpoints
Build Filters Based on Packets
Display Filter Syntax
Use Comparison Operators and Advanced Filters
Filter on Text Strings
Build Filters Based on Expressions
Watch for Common Display Filter Mistakes
Share Your Display Filters

TCP/IP Communications and Resolutions Overview
TCP/IP Functionality
When Everything Goes Right
The Multi-Step Resolution Process
Resolution Helped Build the Packet
Where Faults Can Occur
Typical Causes of Slow Performance

8.

Analyze DNS Traffic

DNS Overview
DNS Packet Structure
DNS Queries
Filter on DNS Traffic
Analyze Normal/Problem DNS Traffic

10.
Analyze ARP Traffic
ARP Overview
ARP Packet Structure
Filter on ARP Traffic
Analyze Normal/Problem ARP Traffic

11. Analyze IPv4 Traffic
IPv4 Overview
IPv4 Packet Structure
Analyze Broadcast/Multicast Traffic
Filter on IPv4 Traffic
IP Protocol Preferences
Analyze Normal/Problem IP Traffic

12. Analyze ICMP Traffic
ICMP Overview
ICMP Packet Structure
Filter on ICMP Traffic
Analyze Normal/Problem ICMP Traffic

13. Analyze UDP Traffic
UDP Overview
Watch for Service Refusals
UDP Packet Structure
Filter on UDP Traffic
Follow UDP Streams to Reassemble Data
Analyze Normal/Problem UDP Traffic

14. Analyze TCP Protocol
TCP Overview
The TCP Connection Process
TCP Handshake Problem
Watch Service Refusals
TCP Packet Structure
The TCP Sequencing/Acknowledgment Process
Packet Loss Detection in Wireshark
Fast Recovery/Fast Retransmission Detection in Wireshark
Retransmission Detection in Wireshark
Out-of-Order Segment Detection in Wireshark
Selective Acknowledgement (SACK)
Window Scaling
Window Size Issue: Receive Buffer Problem
Window Size Issue: Unequal Window Size Beliefs
TCP Sliding Window Overview
Troubleshoot TCP Quickly with Expert Info
Filter on TCP Traffic and TCP Problems
Properly Set TCP Preferences
Follow TCP Streams to Reassemble Data 16. Examine
Advanced Trace File Statistics
Build Advanced IO Graphs
Graph Round Trip Times
Graph TCP Throughput
Find Problems Using TCP Time-Sequence Graphs

15. Graph Traffic Characteristics
Advanced I/O Graphing
Graph Round Trip Times
Graph TCP Throughput
Find Problems Using TCP Time Sequence Graphs

16. Analyze HTTP Traffic
HTTP Overview
HTTP Packet Structure
Filter on HTTP Traffic
Reassembling HTTP Objects
HTTP Statistics
HTTP Response Time
Overview of HTTP/2
HTTP/2 Analysis Fundamentals
HTTP /2 Frame Format
Analyze Normal/Problem HTTP Traffic

17. Analyze TLS-Encrypted Traffic (HTTPS)
Analyze HTTPS Traffic
Encrypted Alerts
Decryption Steps
Filter on SSL

18. Review Your 10 Key Troubleshooting Steps
Baseline "NormalTraffic
Use Color
Look Who's Talking: Examine Conversations and Endpoints
Focus by Filtering
Create Basic IO Graphs
Examine Delta Time Values
Examine the Expert System
Follow the Streams
Graph Bandwidth Use, Round Trip Time, and TCP
Time/Sequence Information
Watch Refusals and Redirections

Grades -All students must ordinarily take all quizzes, labs, exams and submit the class practicum in order to be eligible for a Q/ISP, Q/IAP, Q/SSE, or Q/WP credential unless granted an exception in writing by the President. Know that Q/ISP classes draws quite the spectrum of students, including "those less comfortable," "those more comfortable," and those somewhere in between. The course is graded as a pass or fail solely on your attendance and participation. Those less comfortable and somewhere in between are not at a disadvantage vis-à-vis those more comfortable. Escalating labs help you prepare for real world scenarios. Each labs escalates upon itself, increasing in intensity, rising to the next level, while you're mitigating the threat step by step. **Books** - No books are required for this course. However, you may want to supplement your preparation for or review of some lectures with self-assigned readings relevant to those lectures' content from either of the books below. The first is intended for those inexperienced in (or less comfortable with the idea of) hacking. The second is intended for those experienced in (or more comfortable with the idea of) hacking. Both are available at sites like Amazon.com. Both are avail at the SU Hacker Library. Realize that free, if not superior, resources can be found on the SU website.

Welcome to the Q/ISP® Qualified/Information Security Professional Certificate Program of Mastery Information

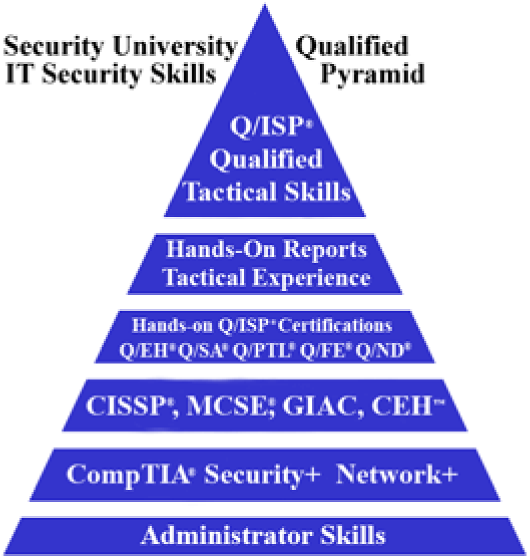
What is a Q/ISP "Qualified" Information Security Professional Certificate of Mastery?
A Q/ISP is a person who successfully passed the Q/ISP online 125 question certification exam and successfully completed 3 practicals of the Q/ISP Certificate Program of Mastery. The Q/ISP exam fee is $450.00 US dollars. A Q/ISP exam is delivered online from anywhere. You need a camera and remote access using a SU Qualified proctor.

To earn a designation you are required to pass all 4 Q/ISP Program exams and develop the 3 practicums. The practicum "validates" your qualified cyber security skills and grants you the official use of SU's "Qualified" symbol as your trust mark.

Q/ISP Certificate Program of Mastery is obtained through SU for the purpose of recognizing qualified individuals who have distinguished themselves as knowledgeable and proficient cyber security practitioners with validated hands-on tactical security skills. The Q/ISP Certificate Program of Mastery designation provides the only means of identifying and certifying *qualified persons* who subscribe to a rigorous requirement for maintaining their knowledge and proficiency in cyber security with "validated" hands-on tactical security skills.

Q/ISP Qualified/ Information Security Professional Certification Classes

1. Q/EH Qualified/ Ethical Hacker
2. Q/SA Qualified/ Security Analyst
3. Q/PTL Qualified/ Penetration Tester License
4. Q/FE Qualified Forensic Expert
5. Q/ND Qualified/ Network Defense


Security University IT Security Skills Qualified Pyramid

Q/ISP® Qualified Tactical Skills

Hands-On Reports Tactical Experience

Hands-on Q/ISP® Certifications Q/EH® Q/SA® Q/PTL® Q/FE® Q/ND®

CISSP®, MCSE; GIAC, CEH™

CompTIA® Security+ Network+

Administrator Skills

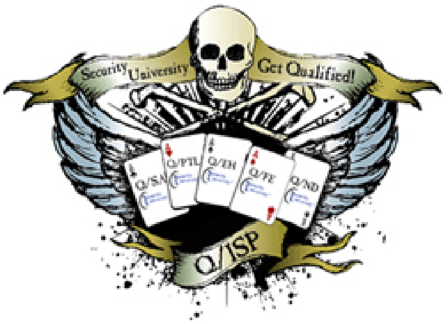
To accomplish this standard, Q/ISP goes beyond theory and terminology and tests the processes and methodology of tactical security skills. A Qualified/ Cyber Security Professional Certification Program of Mastery for Individuals is:

- For system and network administrators and security professionals, the class offers added proof that you know have the security skills needed to protect systems and networks and that you have validated those security skills needed to carry out those tasks.
- Q/ISP courses provide an over -arching baseline of information security skills ensuring that dangerous threats to your networks and critical assets - threats that at are actively being exploited - are thoroughly addressed.
- Q/ISP CPoM ensures that qualified professionals can keep their security skills and practical knowledge current through 120 continuing education credits every 3 years (no less than 120 hours annually).
- Many large private companies and government agencies are reviewing the Q/ISP Certificate Program of Mastery for new job students and has been added to the 8570 IA WIP Certification list.

The Q/ISP Certificate Program of Mastery is for IT & IS security professionals, Sys Admins, Security Auditors, Network Auditors, CISO's who are looking to validate tactical security skills, earn a vocational cyber security certificate, advance their cyber careers and increase their income. Each 72 hour class is packed with hours of hands-on tactical labs with leading edge security tools and technologies setting the stage for your "Qualified" Information Security Professional credential. Once you have mastered the 4 Q/ISP classes & certification exams, or passed the Q/ISP certification exam and submitted completed and reviewed/ approved practical's, you have validated your tactical security skills of an information security professional and are "qualified".

Passing the Q/EH, Q/SA, Q/ND and Q/FE classes are NOT mandatory for taking the Q/ISP Certification exam to earn your Q/ISP Certification. Contact info@securityuniversity.net for more information or call 1.203-249-8364.

You may ask... What does the Q/ISP Logo Represent?
SU's Q/ISP logo represents the highest commitment for Security professionals in the world. It is a custom logo created to honor security professionals who aspire to earn the most valued tactical hands-on security skills training, certifications and licenses in the world. It shows you have earned "tactical hands-on security skills" not only a "certification".



The skull represents brains.
The ribbons symbolize integrity and honor.
The wings exemplify the ability to soar towards your true potential (and above the turkeys you work with).
The playing cards attest that you've mastered the security skills to win at mitigating security.

SU has led the wave of tactical hands-on security skills training & certifications since 1999. From pioneering to establishing the highest standard for performance based information security training & certifications for the past 25 years and still leading the way for security professionals to validate tactical security skills to reach their career & personal potential.

M. Lynch - Testimonial - 2017
The certifications that I have received through SU (1 CompTIA Security+, 4 Q/ISP related certs, and 1 Q/PTL License) have done two main things that have benefited my career transition to my second career. First, these certifications have opened additional job opportunities that I can apply to since they require Security+ or cyber security related certs that the Q/ISP certs demonstrate.
Secondly, these certs have allowed me to enhance my resume with recent certs to complement my resume filled with experience.
These certs and training has allowed me to obtain new detailed technical skills and knowledge that builds confidence in what I can offer to a new employer since I have both passed exams along with completing practicum assignments via the Q/ISP class that allowed me to obtain hands on skills and demonstrates that I can perform similar task if assigned in future employment.

For my career prospects, I am now seeing more active contact from employers due to either recruiters or hiring manager seeing the recent certs. My resume has been pulled for further contact via phone interviews and face-to-face interviews. In one recent interview, the hiring manager informed me directly that I was selected to be interviewed due to my cyber security certs even when these were not listed as part of the qualifications for the position. In a recent phone interview, I was informed that in addition to the position I was being interviewed for, the hiring manager was going to recommend to the customer that I be considered for a cyber security specialist. Thus, more chances to be hired have occurred by having these certs.

Finally, I expect these certs to provide additional confidence within the prospective employer as they eventually decide to provide a job offer. Their confidence will be enhanced both by the actual interview process and having seen the actual security certs indicating to them that I can perform well on the job starting day one. I am appreciative of the quality of training provided to me by SU and their instructors and I am thankful for the opportunity provided to me for the new skill training at SU via the grants available for displaced workers.

Q/EH Testimonial
I have over 20 years' experience in both teaching and information security. I am very particular about both and highly concerned with the decline in real training revolving around the current challenges which we face. I was honestly impressed with both the level of expertise and the instructor's ability to relay this information to the students. This is not simply another idiot boot camp but a well-reasoned and directed classroom experience which prepares the student for the real world. I was impressed with the hands-on exercises. These combined with the instructor's elevated knowledge base made the class enjoyable and extremely topical. When you compare SU to other training groups in the region, they are infinitely superior in both talent and developmental materials. I think that SU has the right mindset in the development of their classes. They are working to impart valuable knowledge and not simply to push students through. Whereas, I believe that any student could pass any applicable exam after attending these courses, the test is not the focal point. They deserve to be commended for both their mindset and the efforts that they've made to enhance the knowledge base of their students. I sincerely appreciate my time learning with SU and would recommend it to any organization which actually wants to develop real IA professionals. PSparks DoD/DISA/JITC

This CISSP® course with Ken Cutler was a life changing experience! I now know I can pass the exam and I now know what to study. I highly recommend this course to anyone wishing to forward there career in IT security, IT management, or IT auditing. [MMassy] I really enjoyed this course and in the near future I need continuing education courses I would consider taking classes at SU!

HERE RESTS IN
HONORED GLORY
AN AMERICAN
SOLDIER

Sondra J. Schneider (Resume) Founder & President / Administrator

Full Time Professor, Lead PKI Instructor, CISSP, CEH/ Q/EH, ESCA/ Q/SA, Q/PTL, CHFI/ Q/FE, Q/ND, ISO 27001 Lead Auditor, Grant Officer.

A 31-year information security industry veteran, Sondra Schneider is the President of SU and the Director of SU's Center for Qualified Cyber Security Excellence & Mastery. Since 1999 Sondra and the SU Instructor team have been training IT Professionals to be Cyber Security Professionals. SU's Q/ISP - Qualified/ Information Security Professional Certificate Program and micro credentials [Q/EH, Q/SA-Q/PTL, Q/FE & Q/ND] earned the prestigious NSA CNNS 4011, 4012, 4013A, 4014, 4015 and 4016A approval from 2008 to 2018 until the NSA expired CNSS for CAE Center for Academic Excellence in Cyber Operations standards.

In 2004 Ms. Schneider was awarded "Entrepreneur of the year" for the First Annual Woman of Innovation Awards from the CT Technology Council. She is an active advisor for the CT Technology Counsel, and advisers 3 computer security internet (start-up) technology companies and a frequent speaker at computer security and industry events. She is a founding member of the NYC HTCIA and IETF, and the vendor community to provide information security certification training to comply with the 8570/ 8140 DoD mandates.

SU is 36,000 strong. Since 1999 SU's Center for Qualified Cyber Security Excellence & Mastery trains and certifies Cyber/IT professionals in hands-on performance based, stacked cyber credentials. Success is doing it once. Mastery is the ability to do it repeatedly at the same level of excellence. Many people will experience success, but few will experience cyber mastery. In 1985 Sondra Schneider crafted the first sneakernet system for Equitrac [tape data collection] to solve client backups *sneakernet* was a solvable communications issue. She focused on fiber connectivity and what could be run on fiber over the next decade. Before founding Security University, Sondra worked at Fujitsu Networks UK which funded the first e-community pilot pre internet. Sondra worked for Datapoint Systems who created Intel's 8080 data chip-set [Intel inside] and the first p2p video [30 frames full-motion video over copper]. In 1990 Sondra worked at MFS Datanet (Metropolitan Fiber Systems) selling & installing the fiber backbone [internet] to AOL, PSINet, Mindspring, Earthlink, and Prodigy on the eastern seaboard. After MFSDatanet was acquired by UUNET, Sondra worked for ATT deploying the digital internet fiber backbone. She developed the first webpage [1-800 Flowers] 24 months before the Netscape browser [existed] and 36 months before wallet side technology existed. In 1994 Sondra contracted BBN to install the first firewall at the White House.

In 1996 Sondra left ATT for the WheelGroup, a USAF Information Warfare group start-up selling the new Netranger network intrusion detection tool that scanned live systems for bad actors. In 1996 CISCO acquired the Wheelgroup and Sondra used the stock proceeds to start the first information security practice in the USA called IFSec. IFSec created "tiger teams' to mitigate digital threats against networks and welcome banners. In 1999 Sondra sold IFSec to PriceWaterhouse and started Security University (SU). Sondra created the "Center for Qualified Cyber Security Excellence & Mastery" using the Qualified /Hacking/ Security Analysis/ Penetration Testing/ Forensics' skills class methodologies she developed at IFSec staff to teach her staff essential cyber skills to reduce risk. Sondra personally experienced the IT/ Cyber talent shortage with her security practice. When she sold IFSec it was to create SU to develop the IT/Cyber talent necessary to protect our nations assets and address the IT/ Cyber talent shortage. SU's performance based curriculums provide IT/cyber professionals with escalating hands-on performance based programs, classes and certifications. In 2001 SU was first to deliver hands-on Software Security Expert Training and Certification for Microsoft, and in 2004 SU was the first to provide the Qualified/ Forensic Professionals Validated Skills Program and License. For 25 years, SU's Center for Qualified Cyber Security Excellence & Mastery courses, live cyber ranges and Security University Tests [exams] provide critical cyber security skills to assess, qualify and validate the cyber security workforce.

Greg Ecklin (Resume) CTO - SU Chief Technology Officer

Security University is 36,000 strong. As CTO of Security University Greg has been pivotal in qualifying and upskilling SU's cybers ecurity workforce framework. Greg earned a BS in Computer Science from West Point Military Academy Graduating class of 2013. Greg brings his Army Cyber Warrior experience leading a national incident response team of 23 cyber professionals conducting defensive cyberspace operations after standing up the first US Cyber Protection Brigade. The need for a highly trained civilian with cyber-warfare skills to monitor and respond to unauthorized activity against information systems and computer networks is intensifying. After the service Greg joined MITRE and managed 2 cyber assessment teams for 4 years. In 2019 Greg joined SU as a part-time adjunct professor/ advisor and CTO in 2021.

At SU Greg manages all SU technology to advance SU's 5 Qualified Cyber Security Programs of Mastery hands-on labs at the highest level for the NSA CNSS approved [expired] Q/ISP curriculum's [Qualified Cyber Security Certificate Program of Mastery] performance based programs. Greg's MITRE experience building and leading cyber teams in offensive and defensive cyber security assessments against national security interests is instrumental in defining the level of rigor for SU "live" cyber ranges that provide essential skills to qualify and validate students mastery practicum's. Greg's extensive experience helps SU identify skills that qualify and validate SU's cyber framework to advance our nation's cyber security.

Gregs role as CTO ensures there are enough well-trained people to protect critical computer systems from cyber attacks. Greg is a seasoned cyber security professional who is an innovative, results-oriented leader with 12 years of building and leading technical teams in cyber security and IT to defend your organization from adversaries before it's too late. Greg roles focus on operational "adaptability" and agility across all 5 Qualified Cyber Security Certificate Programs. A technically proficient cyber security professional and SME, Greg is a strong leader with exceptional communication skills with significant experience in leading large-scale programs, and a practical approach to problem solving. Greg leverages his cyber security knowledge across SU curriculums focused on threat exposure & third-party risk.

Additionally, Greg is the President of Big Bytes, a veteran owned small business serving small/ medium IT cyber clients. Greg drives the modernization and cyber transformation of his clients streamlining services and reducing IT/Cyber complexity while enabling business while decreasing the attack surface.

Ken Cutler CISSP, CISM, CISA, Security, CASP (Resume)
Director Professional Cyber Security Certification Programs / Instructor

Ken Cutler is Director, Professional Training Certification classes. His responsibilities include Cyber Security and professional certification curriculum development and senior lead instructor for SU. He is an internationally recognized consultant, lecturer, and hands-on trainer in the Information Security and IT audit fields. Previously, Ken founded the Information Security curriculum for MIS Training Institute in 1993 and served as training department head, conference/symposium chair, and lead instructor for over 18 years. He has delivered a wide array of lecture and hands-on courses throughout the United States, including numerous US government agencies, as well as, in Russia, United Kingdom, Netherlands, Finland, Nigeria, Ghana, Tunisia, South Africa, Serbia, Mexico, United Arab Emirates, Oman, Greece, Singapore, and Hong Kong. Previously, Ken has headed major Information Security and Quality Assurance programs at American Express Travel Related Services and Lockheed-Martin (Martin Marietta) and has been a Fortune 500 company Chief Technology Officer. His industry experience includes: insurance, banking, financial services, healthcare, natural resources, manufacturing, government contracting, security and audit software product design and utilization, consulting and training.

Mr. Cutler has been a long-time active participant and advisor in US federal, international government, and industry security standards initiatives and co-authored NIST SP 800-41, “Guidelines on Firewalls and Firewall Policy”. Ken has also published works on the intricacies of Information Security, security architecture, disaster recovery planning, security, vulnerability testing, firewalls, and single sign-on. In addition, he has been frequently quoted in popular trade publications such as *Healthcare Information Security Newsletter, Computerworld* , *Information Security Magazine* , *Infoworld, InformationWeek, CIO Bulletin, and MIS TransMISsion.* Mr. Cutler was featured in a special TV program entitled, *“The Electronic Battlefield”*, on Abu Dhabi, UAE Public TV. Mr. Cutler is also the Founder and Principal Consultant of KCA InfoSec Assurance, an independent consulting firm delivering a wide array of Information Security and IT Audit management and technical professional services. His input on vulnerability and risk assessment tools has been frequently sought out by major software vendors. Ken served as a Certified Weather Forecaster in the US Air Force and was decorated for his exemplary performance during his overseas duty assignment in Alaska. Mr. Cutler is also the Founder and Principal Consultant of KCA InfoSec Assurance, an independent consulting firm delivering a wide array of Information Security and IT Audit management and technical professional services. His input on vulnerability and risk assessment tools has been frequently sought out by major software vendors. Ken served as a Certified Weather Forecaster in the US Air Force and was decorated for his exemplary performance during his overseas duty assignment in Alaska.

Kevin Cardwell (Resume) Director of SU Qualified/ Cyber Security Certificate Programs of Mastery Q/ISP, Q/IAP, Q/WP, Q/CND / Instructor

Kevin Cardwell spent 22 years in the U.S. Navy, during this time he tested and evaluated Surveillance and Weapon system software, some of this work was on projects like the Multi- Sensor Torpedo Alertment Processor (MSTRAP), Tactical Decision Support System (TDSS), Computer Aided Dead Reckoning Tracer (CADRT), Advanced Radar Periscope Discrimination and Detection (ARPDD), and the Remote Mine Hunting System (RMHS). He has worked as both software and systems engineer on a variety of Department of Defense projects and was selected to head the team that built a Network Operations Center (NOC) that provided services to the command ashore and ships at sea in the Norwegian Sea and Atlantic Ocean. He served as the Leading Chief of Information Security at the NOC for six years prior to retiring from the U.S. Navy. During this time he was the leader of a 5 person Red Team that had a 100% success rate at compromising systems and networks. He currently works as a freelance consultant and provides consulting services for companies throughout the US, UK and Europe . He is an Adjunct Associate Professor for the University of Maryland University College where he participated in the team that developed the Information Assurance program for Graduate Students which is recognized as a Center of Excellence program by the National Security Agency (NSA). He is an Instructor and Technical Editor for Computer Forensics, and Hacking courses. He has presented at the Blackhat USA Conference. He is a Certified Ethical Hacker (CEH), and holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas. His current research projects are in Computer Forensic evidence collection on "live" systems, Professional Security Testing and Advanced Rootkit technologies.

Randy Kohler (Resume) Director of Cyber Security Training and Curriculum Development / Instructor, Security +, SecurityX , Q/EH, C|EH 2024
Randy brings over 20 years of security related experience with the last 15 with institutional instruction in a multitude of different security roles. Randy's clients included corporate executives, small businesses, U.S. Air Force & Navy, non-profit organizations, colleges, and local radio stations. Senior Consultant & Senior Technical Instructor & Senior Penetration Tester • Assisted in the process of getting over 10,000+ students certified from Network+,Security+,CySA+,CASP+,CEH,CHFI and many more since 2001. He has high energy and encouraging outlook with a compelling desire for team continuity• Exceptional presentation and customer service skills • Superb competency in IT security, network design, maintenance & project management • Impeccable work ethic, steadfast dedication, and high integrity • Noteworthy ambitious attitude • Self-motivated, quick-witted and inspiring.

DRs. Char Sample - Adjunct & Advisor (Resume)
Highly experienced cyber security professional with over 23 years of experience in network security and software engineering. Internet security experiences include expertise with firewalls, IDS, IPS, Anomaly Detection, DNS, DNSSEC, Mail, routing, authentication, encryption, secure network architectures, cloud computing (IaaS, PaaS) and Unix internals. Experienced in designing and developing Internet security products. Additional experiences in relating cultural influences in computer network attack behaviors. Published author. Invited speaker at international conferences and forums. Dr. Sample recently defended her dissertation on "Culture and Computer Network Attack Behaviors" at Capitol College in Laurel, Maryland." Other areas of research interest include: Cloud Computing, Anomaly Detection methods, Big Data, and DNS.

Doctor of Science, Information Assurance, Capitol College (Laurel, Maryland) May 2013 Title: Culture and Computer Network Attack Behaviors, Master of Science, Systems Management, Capitol College (Laurel, Maryland) May 1995 - Telecommunications Systems. Bachelor of Science, University of Pittsburgh, August 1984. Major: Computer Science Minor: Math. RESEARCH AREAS: Interdisciplinary research combining social sciences and cyber security, data fidelity, artificial intelligence, malicious use of artificial intelligence, machine learning, adversarial machine learning, fake news, threat intelligence, metrics, cyber operations modeling and simulation, cyber mission force development and preparation, DNS security, routing security, security architecture issues, anomaly detection techniques, big data, cloud security analytics, quantifying behaviors, firewalls, IDS and monitoring solutions.

PUBLICATIONS:

· *ZTA: Zero Trust, But Verify, European Conference on Cyber Security and Warfare, June 2022*· *Interdisciplinary Lessons Learned While Researching Fake News,* Frontiers, December 2020.· *Data Resilience: An Interdisciplinary Approach,* IEEE Resilience Week, 2020.· *A Cross-discipline Approach to Countering 4th Generation Espionage,* European Conference on CyberSecurity and Warfare, 2019.· *Fake News: A Method for Measuring Distance from Fact,* Big Data Disinformation Workshop December 2018.· *A Model for Evaluation Fake News,* US Army Cyber Defense Journal, December 2018.

· *A Model for Evaluating Fake News,* CyCon US 2018, November 2018.· *Simulations in Cybersecurity: A Review of Cognitive Modeling of Network Attackers, Defenders and Users,*Frontiers in Psychology, section Cognitive Science.

· *A Cultural Exploration of Social Media Manipulators,* European Conference on Cyber Security & Warfare, 2018.

· *Data Fidelity in the Post Truth Era Part 1: Network Data,* International Conference on Cyber Security & Warfare, 2018.

· *Psychological Behavioral Examinations in Cyber Security,* Book Chapter, 2018.· *Culture + Cyber: Exploring the Relationship,* Applied Human Factors and Ergonomics Conference,2017.· *Cultural Observations on Social Engineering Victims*, European Conference on Cyber Security and Warfare, 2017.· *Data Fidelity: Security's Soft Underbelly*, Recent

Challenges in Information Science (RCIS) 2017. ・ *Cultural Exploration of Attack Vector Preferences for Self-Identified Attackers* (RCIS) 2017. ・ *What's in a Name? Cultural Observations on Nationally Named Hacking Groups*, International Conference on Cyber Security and Warfare, 2017.・ *Re-thinking Threat Intelligence*, CyCon October 2016. ・ *Cyber + Culture Early Warning Study*, SEI 2015.

Papers: Using Hofstede's Cultural Dimensions to Gain Insight into Social Networking Site Adoption Rates,book chapter in Analyzing the Strategic Role of Social Media in Firm Growth and Productivity. Culture and Cyber Behaviours: DNS Defending, European Conference on Cyber Warfare and Security,July 2015. Application of Hofstede's Cultural Dimensions in Social Networking, European Conference on Social Media (ECSM) 2014, July 2014. Attribution Beyond the IP, e-Forensics, March 2014. Hofstede's Cultural Markers in Computer Network Attack Behaviors, ICCWS 2014. A Different Perspective on Attribution, CyberTalk, Spring 2014. Applicability of Cultural Markers in Computer Network Attack Attribution, ECIW 2013. An Overview of Anomaly Detection, IT Professional IEEE January 2013. Cloud computing security: Routing and DNS Threats, TechTarget 2012. IaaS security puts spotlight on hypervisor security, tenant management, TechTarget 2012. An examination of PaaS security challenges, TechTarget, 2012. Types of DNS Attacks Reveal DNS Defense Tactics, TechTarget, 2012. PRESENTATIONS: RSAC 2020, San Francisco, CA IEEE Big Data Disinformation Workshop, Seattle, Washington NATO MARCOMM, Fake News, Northwood, UK NATO CyCon US, Washington, DC (2016, 2018) University of New South Wales & DSTG, Canberra, Australia. COSAC, Naas, Ireland (2011 – 2022) International Conference on Cyber Warfare and Security, (2014 – 2019) (track chair 2017 - 2021). NATO – Norfolk State University Cyber Security Workshop, 2017, Norfolk, VA British Computing Society, Cambridge, UK and London UK, 2017 Recent Challenges in Information Science, 2017, Brighton, UK Cyber Security Practitioner's Workshop, (2014 – 2018) York, UK European Conference on Cyber Warfare and Security, 2013 - 2020 (track chair 2016-2021), Dublin, Ireland Applied Human Factors and Ergonomics, 2017, Los Angeles, CA Cardiff University, 2017, Cardiff, UK Suits and Spooks 2015, Washington DC and London, UK. ISACA Conference, October 2014, Dublin, Ireland 2nd Annual Psyber Security Workshop, August 2014, Ft. Meade, Maryland European Conference on Social Media, July 2014, University of Brighton, Brighton, UK ISACA Dublin, March 2014, Dublin, Ireland ISACA Belfast, March 2014, Belfast, Ireland 44Con, September 2013, London, England National Information Security Conference, June 2013, Glasgow Scotland Shmoocon, January 2012, Washington, DC PATENTS and HONORS: Resilience Week, Data Fidelity: An Interdisciplinary Approach, 2020 Best PhD Paper and Presentation, European Conference on Information Warfare and Security 2013 Recognized inventor of Web Host Intrusion Prevention System (WHIPS), Verizon awarded patent in 2006 Recognized inventor of Console Host Resource Management System (CHRMS); Verizon awarded patent in 2006

DRs. Gale Pomper - Adjunct & Advisor (Resume)

Gale Pomper has over 27 years of experience installing and designing computer networks. She holds numerous certifications from Microsoft, Novell, and CompTIA, including Server+, MCT, MCSE, MCTS for SharePoint, and MCTS and EMA for Exchange 2007. She is the principal author for an exam guide for Windows 2000 Active Directory published in December 2001, and a contributing author for Windows XP Power Pack published in March 2003. For the past 15 years, Gale has been an independent consultant providing network design services, customized training, and SharePoint implementation services. In 2007, Ms. Pomper took a position working for the Department of Defense as a Global Exploitation and Vulnerability Analyst and is currently a Program Director for her office. She is a CISSP.

David Spivey - Instructor, Systems Engineer, Major Accounts Palo Alto Network CSE Q/AAP

David brings over 20 years of security related experience with the last 18 with Cisco in a multitude of different security roles. David bring's real-world deployment, implementation, root cause analysis, security posture assessments, and architectures for some of the largest global organizations. Some security engagements that David has been involved with include Microsoft, Intel, GM, Ford, Best Buy, Target, CAT, State Farm, Eli Lilly, Cummins, Wellpoint, United Healthcare and the largest financial institutions. These engagements have included but not limited to IPS, DDoS, PKI, 802.1x/Radius Control Planes, Firewall, Botnet Filtering, Security Posture Audit & Assessments. David has been instructing for clients, internal Cisco and at external conferences like Secure360 for the last 10 years. He brings real-world examples and experiences to the classroom often discussing what he can in detail for your information analysis. David graduated from WKU with a Bachelor of Science in Mathematics/Computer Science and has extensive Graduate work within Mathematics Topology and Group Theory disciplines.

Behzad Salimi - Instructor (Resume)

Frederick Haggerty - SU Advisor Forensics, Security+, CEH, CHFI, Q/FE
Frederick Haggerty is an accomplished Senior Java/J2EE Developer with 15+ years of experience in providing technical solutions that improve scalability, performance, and productivity for a variety of organizations. Fred is a Senior Java/J2EE Developer with extensive experience in building mission critical web-based systems — providing enterprise application integration, designing and implementing solutions using SOA and Web Services, and integrating technologies like JAAS and JSF, Spring and Hibernate, and a variety of other Java frameworks. He has also been involved in all phases of Software Development Life Cycle (SDLC) for small and large scale projects. Frederick's areas of technical expertise include designing and implementing secure web-based systems, using middleware technologies, implementing the Role Based Access Control (RBAC) security model using Java Authentication and Authorization Service (JAAS) to secure Java applications, and building Enterprise Service Bus (ESB) applications. His experience also includes designing, developing, and building secure web services with JAX-WS/JAXB and SAML authentication (X509 Certificates, LDAP), which allows for logging, monitoring and alerting, and ensuring strict compliance to the Privacy Act for PII data. hroughout his career, Frederick has supported a wide range of clients that have spanned many areas such as DOD, law enforcement (FBI/NCIS), and DOI, as well as non-profit organizations. Most recently, Frederick has focused primarily on digital forensics and information security program development, to include security policy development for small and medium organizations. He has combined his expert knowledge in building complex systems and his technical proficiency in information security to help companies achieve an overall better security posture.

Michael Penders - SU Instructor CMMC & ISO 27001 Lead Auditor / Lead Implementer (Resume**)**
Chairman/ President, Environmental Security International L3C (ESI) (2001 to Present)
Founding Principal and Chief Executive Officer of consulting firm which conducts assessments, investigations, and designs compliance programs; ESI implements Environmental and Security Management Systems conforming to standards for Best Practices; ESI provides training in the implementation and enforcement of environmental laws and best practices in risk assessment and security management; ESI offers facilitation, mediation, policy and legal services. Clients have included: NATO; EPA; DOD; DOE; WCO; Port Authorities and Public Utilities; Government Agencies, Associations and Corporations in North America, Europe, Asia and the Middle East.
Select Accomplishments, Leadership Positions, and Publications:
Transportation Research Board (TRB) Critical Infrastructure Protection Committees;
Chair, US-Israel Working Group of Experts in Management Systems, Standards and Security. Facilitated agreement on first international standard for integrated Security Management System (SMS) now

reflected in ISO 28000 standards and DHS Regulations;

US Technical Advisory Groups (TAG) ISO TC8 for ISO DIS 20858 for Maritime Port Facility Assessment and Security Plan Development; ISO 28000, US ANSI Strategic Advisory Group (SAG) on Integrated Management System Standards; ANSI DHS Homeland Security Panel;

Judge, Secretary of Defense Environmental Excellence Awards (2006 to present);

Testified before Chairman of the Senate Judiciary Committee on environmental law enforcement, homeland security policy, audit and risk management system standards;

Lead Investigator of pilot projects testing integrated security assessments, management system design, and implementation at critical infrastructure facilities, including ports;

Chairman, Homeland Security Committee, American Bar Association (ABA), Section of Environment, Energy, and Natural Resources (SEER) (August, 2007 to 2010);

John Ellwood Saurbaugh - Instructor (Resume**)**

Steven B. Wyllie - Instructor (Resume**)**

Daniel Conroy - Advisor (Resume**)**

Chief Technology Officer (CTO) - Digital & AI, at RTX & Chief Information Security Officer (CISO) (4x).
Daniel Conroy is CTO of Rayethon. As the Chief Technology Officer - Digital at Raytheon Technologies (RTX), I am at the forefront of pioneering digital transformation and leveraging AI to scale operations, enhancing the technical and strategic landscape of the company. My role encompasses safeguarding the technical interests of RTX's digital and Global Information Services, driving the implementation of our ambitious technology strategy and vision, and ensuring the robustness and integrity of our infrastructure and resources. Under my leadership, my team is dedicated to ensuring that critical systems and business operations are resilient and available, empowering RTX to achieve its strategic objectives and maintain its competitive edge. My responsibilities extend beyond the operational to the strategic, as I oversee the security posture of the company, ensuring the confidentiality, availability, and integrity of not only RTX's assets but also those of our global customers. This role leverages my deep expertise in core security principles to protect against and mitigate cyber threats, ensuring trust and reliability in our digital environment. Before ascending to my current position, I was entrusted with the global security of the company's and customers' assets, a testament to my comprehensive understanding of the complex cybersecurity landscape and my ability to effectively manage and mitigate risks. Beyond my executive duties, I am an experienced keynote speaker and a recognized voice in the Information Security community. My contributions extend to notable Information Security events and publications, where I share insights on emerging technologies, cybersecurity trends, and the strategic implementation of AI and digital transformation initiatives to safeguard and propel businesses forward. In an era where technology evolves at an unprecedented pace, I am committed to leading RTX's digital journey, ensuring that our technological advancements and security measures not only meet but exceed the demands of the modern digital world.

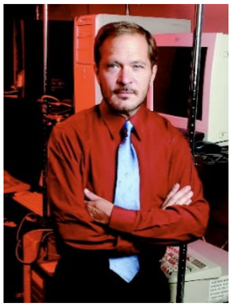
Prior to RTX, Daniel held positions as CISO Synchrony Financial, head of Strategy, Planning and Governance Citibank, MD & Chief Information Security Officer at The Bank of New York Mellon for four years. In 2009 he received the 'Best in Class' BNYM award which recognizes individuals/ teams who demonstrate a spirit of dedication & ingenuity. Daniel enhanced monitoring, identification & control within the information security environment through the procurement & implementation of additional software & toolsets. Daniel focused on the increased involvement of organized crime in this arena:* State sponsored cyber threats* Growing insider threats* Legislative initiatives. Daniel's group had responsibility for threat & vulnerability assessments, incident response, security architecture, network monitoring, data loss prevention, policies & standards, security awareness, client assessment/communications, information classification & database monitoring. Daniel's project regarding the governance & control of Internal Social Media was awarded a national honor, Best Project in the Information Security category, at Technology Managers Forum in 2010. Also in 2010, Daniel was a finalist for Information Security Executive of the Year (Northeast Sector) for 2010 at T.E.N.

Steve Boddy

Ambitious thought leader with a tech-savvy approach towards collaborative innovation. Lead the best of breed technologists at tip of the spear on high value mission-critical programs designed to safeguard information essential to maintain national security in identity and access management of the cyber frontier. •Results-driven Program Manager actualizing strategies to identify cadence and synchronization requirements to create complex software products. Combine strong team leadership, consensus building and talent development to create agile teams that transform business objectives into effective solutions using Scrum, Kanban, Lean and the Scaled Agile Framework.

More than three decades of experience in increasingly challenging information technology, management, and administrative positions. Exceptionally talented at leading cooperative efforts for creating solutions to overcome IT issues with cross-integration of system implementation, information security, and technical management in agile DevOps environments.

H. Morrow Long - CISSP, CEH, CHFI
Instructor - Qualified/ Information Security Professional Program (Q/ISP) (On Sabbatical)



Morrow Long is the Yale University Information Security Officer, Director of the Information Security Office and DMCA Notification Agent for Yale University. He has been with Yale University for the past 25 years, participating in many campus and IT projects (Y2K Planning, Business Continuity/DR, Oracle Financials/HR Business Modernization Project, Yale's Windows NT to Windows 2000 Active Directory Migration Project, HIPAA Security). Morrow Long is also a Visiting Scientist with the Carnegie Mellon University Software Engineering Institute's in the CERT/Networked Systems Survivability group. Mr. Long is a UNIX, NT and TCP/IP security expert, an author, consultant and educator with more than 26 years of experience with the IP (Internet Protocol) networking protocols with 2 decades years of experience designing Internet/Intranet firewalls and information security solutions. Morrow has written and released several information security software programs into the public domain (including one of the first TCP port scanners and the first audio Web server CGI cited in Wired magazine). Mr. Long was one of the original participants in the Infragard program in Connecticut. Morrow was on the executive board of CUISP (Campus University & Information Security Professionals) and also participates in the EDUCAUSE/I2 Computer/Network Security Task Force (a founder of the annual Educause Security Professionals Conference), CISDG (CT InfoSec Discussion Group) and is President of the Connecticut ISSA Chapter.

Prior to working at Yale University Mr. Long was a Member Technical Staff at the ITT Advanced Technology Labs in Stratford and Shelton (1984-6) Connecticut and a Lead Programmer Analyst developing INVESTWARE(TM) at New England Management Systems (NEMS 1982-84).Mr. Long holds a B.S. in Communications from the Boston University School of Communication (1981) and a M.S. C.I.S. (Computing and Information Systems) from the University of New Haven (1986 as well as CISSP®, CISM® and CEH™ certification. Morrow has contributed to several papers and books on computer security, computer crime, digital forensics, network survivability and information assurance.