



Security University

510 Spring Street suite 130
Herndon VA 20170

Sondra Schneider,
President SU
109 Weed Ave, Stamford Ct 06902
Direct: 203-249-8364
877-357-7744
s0ndra@securityuniversity.net
Sept 2022

Supra Qualified



never
never
never
give
up

(winston churchill)

The SU Course Catalog is edited & published by the President of SU a non-degree granting intuition. 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. *except where indicated. SU is located at 510 Spring Street, Herndon VA 20170, 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 Credential Assistance Program approved.

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

"This institution is approved to classes approved by the 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.benefits.va.gov/gibill>."

Table of Contents	Page
Welcome	3
SU Mission	4
SU History	5
SU Approvals	5
SU Overview	6
SU Courses & Fees	7-9
SU Admission Information	10
SU Refund Policy	10
Veteran Education Benefits	11-12
Satisfactory Academic Progress	13
SU Course Descriptions	14
Student Services and School Policies	15-16
Grievance Policy	17
	18-19
Q/ISP Program Description Q/ISP Program Overview Q/SA Qualified/Security Analyst, Q/LPT & Qualified/Penetration Tester License, Q/EH Qualified/Ethical Hacker Certification + CEH Training, Q/FE Qualified/Forensics Expert, Q/ND Qualified/Network Defender, ISC ² CISSP Certified Information System Security Professional Cert Training Class, CompTIA Security+, CASP CompTIA Advanced Security Practitioner	20-40
Q/IAP Program Description Q/IAP Program Overview Qualified/Information Assurance Professional (CPoM) Certificate Program of Mastery, Qualified/Access, Authentication & PKI Professional, Q/NSP Qualified Network Security Policy Admin, Q/CandA Qualified/Certification and Accreditation Professional, ISACA CISA Training Class, CISM Certified Information Security Manager Training Class, CMMC PMP Project Manager Class, ITIL IV, Scrum, Qualified/Internet Security Awareness & Compliance for MGT, Qualified/Security Awareness Training SSCP Systems Security Certified Practitioner, ISSEP Certification Training Class,	41-63
Security+, CASP	64-71
Cybersecurity Hacking for Managers	71-74
Q/WP Program Description Q/WPP Program Overview SU Wireless Certification (CPoM) Certificate Program of Mastery, Q/WP Qualified/Wireless Professional Certification CWNA Exam, Q/WSP Qualified/ Wireless Security Professional CWSP Exam, Qualified Wireless Professional (CWNA & CWSP) Qualified Wireless Security Professional, QWAD Qualified/Wireless Analyst and Defender Bootcamp, Q/WLANPD Qualified/ Wireless Local Area Network Planning Design	75-90
ISO001 Certified ISO 27001 ISMS Lead Auditor Class, ISO002 Certified ISO 27001 ISMS Implementation Class,	91-93
Q/SSE Program Description and overview Q/SSE Program Overview SU Qualified/ Software Security Expert Q/SSE (CPoM) Certificate Program of Mastery, Q/SSE Qualified/SW Security Expert Bootcamp, Q/SSPT License Qualified/SW Security Penetration Tester, Q/ST Qualified/Software Testing Bootcamp, How to Break & Fix Web (Application) Security, How to Break and Fix Software Security, Fundamentals of Secure Software Programming, Qualified Software Hacker/Defender, Qualified/Software Security Tester Best Practices, Introduction to Reverse Engineering	94-118
Q/CDA Q/ISP Program Description Q/ISP Program Overview Qualified/ Cyber Network Defense Training (CPoM) Certificate Program of Mastery, Catching The Hackers – Introduction to Intrusion Detection, Catching The Hackers – Introduction to Intrusion Detection, Catching The Hackers II: Systems to Defend Networks, Linux/Unix Security, Mission Critical Planning, Qualified/Security Hacking Certificate for Managers	119-127
Faculty & Administrations	128-134

welcome

Dear Future Cyber Professional,

Let me be the first to welcome you to SU... and to the hot cybersecurity profession.



This catalog is designed to provide you as much information as we can about your course, certifications and certificate offerings, regulations, and list of the student services at your disposal. We have made every effort to make this information 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 Instructional Team will be glad to answer you.

I truly hope that you will work to get the most out of your SU education. CyberSecurity is by far the hottest job in tech. There will be a lot of great cyber educational opportunities available to you in the future and I urge you to take full advantage of it. I think you will find our hands-on competency-based cyber courses, quiz engine, ebooks, and team of amazing instructors teaching SU's stacked methodology to be very useful to your cyber learning.

I hope you will really focus on your cyber career in ways you have not before attending SU. Our qualified cyber courses will enrich your skills & portfolio to achieve a better lifestyle for you and your family. Remember, while it is important to learn great technical cyber skills... it is even more essential for you to learn about how to communicate with your cyber peers, C-level management and the community of cyber professionals. If you master those skills, you will find that "anything is possible" on your future cyber success.

Lastly, I urge you to really get involved with your school's ethos, beliefs, philanthropy and aspirations. Learning cyber is really fun. Helping others through cyber charity events, giving back at association events - you have the opportunity to meet lots of new cyber people and gives you great satisfaction.

I wish you the best of luck and success in the coming months... and for the rest of your cyber career. I look forward to meeting you in the future and personally welcoming you to the hottest job in tech.

With warmest regards,
Sondra Schneider

SU Mission

The mission of SU is striving to provide our students with the highest quality information security education available through our CyberSecurity, 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
- To offer accelerated learning scheduling options to accommodate the distinctive needs of the adult nontraditional students
- To assist students in realizing their potential by establishing basic skills assessment, with an escalating step by step learning and hands-on performance based competencies based on assessment and 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 cybersecurity education, skills and techniques to become successful in the cybersecurity profession.

SU History

Since 1999 SU has led the cybersecurity professional education industry in hands-on 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 *sneakernet* was a solvable communication issue she focused on Fiber connectivity and what could be run on fiber. Before starting SU Sondra worked at Fujitsu networks. They funded the first e-community. Then Datapoint created the first p2p video to provide full motion video to the desktop over copper. Early 1990 Sondra worked at MFS Datanet to sell fiber connections to AOL, PSINet, Mindspring, Earthlink, Prodigy clients developing a eastern seaboard fiber backbone, today's east coast internet. She left MFS for ATT's first internet tech. Tasked with increasing 800 dial revenue she drafted the first 1800 flowers webpage before browsers existed, there was no wallet side technology. While skiing she met BBN (Bolt Beranek, Newan) and installed the first firewall to an ATT client and the White House. In 1996 Sondra left ATT for the WheelGroup/ USAF Warfare group with the first intrusion detection tool, Netranger. The first scanning tool to kill network bad guys. Wheelgroup was acquired and Sondra left to start the first information security practice that ran tiger teams in NYC – IFSec. 3 years later after losing staff to clients, Sondra started SU (SU) "Center for Qualified CyberSecurity Excellence & Mastery" after selling IFSec to Price Waterhouse.

In 1999 the challenge was lack of cyber talent. SU was first to deliver hands-on performance based "security analysis penetration testing skills and methodologies" classes, certifications and licenses to validate student cybersecurity skills. SU was first to deliver hands-on Software Security Coder Training and Certification, and SU was the first to provide Qualified Forensic Professionals Validated Skills Licenses. SU courses and exam provide critical cyber skills.

22 years later. There are 27,000 cyber professionals with hands-on validated SU cyber skills and credentials working in every agency, defense contractors and many fortune 100 company.

The SU's Qualified Certificates Programs of Mastery [like the Q/ISP®] 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 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 labs. This provides corporations and governmental agencies worldwide the opportunity to hire highly *qualified, certified* and *validated* cybersecurity practitioners who have mastered hands-on cybersecurity skills. Former student C. Mercer say's once he earned (a number of) performance based SU cybersecurity certifications he had a higher earning potential with expanded career opportunities. Being *qualified, certified with validated* with hands on cybersecurity skills makes a statement about who you are and recognized as a serious, knowledgeable and dedicated cyber threat professional – part of a globally recognized family of qualified and validated cybersecurity professionals.

SU Overview

Since 1999, SU has qualified and validated over 27,000 cybersecurity professionals. SU's Qualified/ Information Security Professional Certificate Program of Mastery Credential (Q/ISP CPoM) validates cybersecurity skills for IS & IA professionals that qualify and validates our nation's workforce. SU's Q/ISP Certificate Programs of Mastery include 3/ 72 hr practicums to validate student's cyber skills in the job role.

In 1999 SU became the first cyber security school opened in NYC and moved to Northern Virginia in 2000 finding the market to be a good match. SU is a woman owned small business that is a leading provider of hands-on performance based qualified cybersecurity certificates and certification training in the world.

SU has a tastefully decorated interior, two spacious classrooms, and modern equipment for high tech classes. The student classroom is designed so that students acquire practical experience through servicing guests with a complete menu of cyber skills to help student gain employment.

SU's Qualified Cybersecurity Certificate Programs of Mastery methodology comes from 22 years of cyber education using the accelerated stacked and latticed "Schneider Method" of successively more challenging step by step. Students have up to seven years to complete the qualified certificate programs of mastery that develop key cyber skills and cyber habits.

SU's Certificate Programs of Mastery (Q/ISP, Q/IAP, Q/WP, Q/SSE, Q/CDA) *rigorously* qualify and validate cybersecurity 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 courses and programs of mastery are designed to teach a cybersecurity vocational objectives through an accelerated learning experience - from hands-on workshops, certifications, with deep dives on cyber topic and tech. Every class is structured to give you expertise in a critical cyber skills you can immediately put to use.

SU houses a library of continuing education aids, which include copies of textbooks, periodicals, DVD's, and other reference materials that support the education process. Students receive an access to e-books and a private online quiz engine containing quizzes for use throughout their program. Classes covering networks, access, penetration testing and forensics techniques as well as career readiness, and cyber resume review are incorporated into the curriculum. Top professional educators assist SU student at local job fares.

SU's goal is strategic, so cybersecurity professionals achieve at a high level. A specific and measurable vocational result is described in each class to help you reach and achieve your cybersecurity goals.





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

SU Courses and Fees

SU Center for Qualified CyberSecurity Excellence & Mastery 5 CyberSecurity Qualified Certificate Programs of Mastery Course Listing

SU programs and classes are career technical. SU Q/ISP program is SCHEV approved for both face-to-face or hybrid modalities. Welcome to the Q/ISP, Q/IAP, Q/WP, Q/SSE, Q/CND Certificate Programs of Mastery.



SU Course Listing 2022 - 2023

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.				
R-Required E-Elective	Course Title	Class fee includes exam – exams are required to graduate	Course Hours	Retail Costs
SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery				Program
* This is the cost of the program when you pay tuition up front or pay by class.			936 hrs	\$26,500*
The SU Q/ISP® Certificates 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 <i>defending network mission assurance</i> .				
R	Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class & Exam		72	\$3,990
R	Q/PTL® Qualified/ Penetration Tester License workshop		72	\$4,500
R	Q/EH® Qualified/ Ethical Hacker Certification Class & Exam		72	\$3,990
R	Q/ND® Qualified/ Network Defender Certification Class & Exam		72	\$3,990
R	Q/FE® Qualified/ Forensic Expert Certification Class & Exam		72	\$3,990
R	SU CISSP® Certified Information Security Systems Professional Class & Exam		72	\$4,190
R	SU Security+® CompTIA Certification Class & Exam		72	\$3,990
R	SU CASP® - CompTIA Advance Security Professional Certification Class & Exam		72	\$3,990
R	Linux/UNIX® Security Certification Class & Exam		72	\$3,990
R	Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & Exam		72	\$3,990
R	Q/PTL® Qualified/ Penetration Tester License Practical required to graduate		72	\$3,990
R	Q/ND® Qualified/ Network Defender Certification Practical required to graduate		72	\$3,990
R	Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate		72	\$3,990
E	SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class & Exam		72	\$3,990
E	Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam		72	\$3,990
E	TCP/IP and Key Features of Wireshark & Exam		72	\$3,990
E	How to Conduct Network Vulnerability Analysis & Exam		72	\$3,990
E	Python Forensics Certification Class & Exam		72	\$3,990
E	PowerShell Forensics Certification Class & Exam		72	\$3,990
E	Python/Powershell Incident Response Certification Class & Exam		72	\$3,990
SU Q/IAP® Qualified/ Information Assurance Professional Certificate Program of Mastery				Program
* This is the cost of the program when you pay tuition up front or pay by class.			936 hrs	\$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 & Exam	72	\$3,990
R	Q/NSP® Qualified/ Network Security Policy Administrator & Exam	72	\$3,990
R	Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam	72	\$3,990
R	SU Security+® CompTIA Certification Class & Exam	72	\$3,990
R	SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam	72	\$4,190
R	SU CASP® - CompTIA Advance Security Professional Certification Class & Exam	72	\$3,990
R	SU CISA® Certified Information Security Auditor Certification Class & Exam	72	\$3,990
R	SU CISM® Certified Information Security Manager Certification Class & Exam	72	\$3,990
R	Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam	72	\$3,990
R	Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam	72	\$4,490
R	SU CMMC Cybersecurity Maturity Model Practicum	72	\$3,990
R	PMP Project Manager Professional Certification Class & Exam	72	\$3,990
R	SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam	72	\$3,990
E	Scrum Master Certification Class & Exam	72	\$3,990
E	ITIL V3 Certification Class & Exam	72	\$3,990
E	SU CIPP® Certified Information Privacy Professional Certification Class & Exam	72	\$3,990
E	SU Q/CSO Qualified/Cyber Security Officer Certification Class & Exam	72	\$3,990
E	ISSEP® ISC2® Information Security Systems Engineer Certification Class & Exam	72	\$3,990
E	ISC2 SSCP Systems Security Certified Practitioner Certification Class & Exam	72	\$3,990
E	Qualified/ Internet Threat Security Awareness Training and Compliance for Mgt	72	\$3,990
E	SSCP ISC2 System Security Certified Professional	72	\$3,990
E	Qualified/ Security Hacking Certificate for Managers	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 pay by class.		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 Class & Exam	72	\$3,990
R	Q/ WP® Qualified/ Wireless Professional Certification Class & Exam	72	\$3,990
R	Q/WSP® Qualified/ Wireless Security Professional Certification Class & Exam	72	\$3,990
R	Q/WAD® Qualified/ Wireless Analyst & Defender Practicum	72	\$3,990
R	Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ Qualified Wireless / Qualified Wireless Security Professional Certification Class & Exams	144	\$6,990
R	SU Security+® CompTIA Certification Class & Exam	72	\$3,990
R	SU CASP® Certified Advance Security Professional Certification Class & Exam	72	\$3,990
R	PMP Project Manager Professional Certification & Exam	72	\$3,990
R	Q/WLANPD Qualified/ Wireless Local Area Network Planning and Design & 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 & Exam	72	\$3,990
R	Q/WDNO Qualified/ Wireless Deceptive Network Optimization & Exam	72	\$3,990
E	ITIL V3 Certification Class & Exam	72	\$3,990
E	Scrum Master Certification Class & 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 pay by class.		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 Bootcamp Certification Class & Exam	72	\$3,990
R	Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class & Exam	72	\$3,990
R	Q/STP® Qualified Software Testing Bootcamp Certification Class & Exam	72	\$3,990
R	How to Break & FIX Web Security Certification Class & Exam	72	\$3,990
R	How to Break & FIX Software Security Certification Class & Exam	72	\$3,990
R	Fundamentals of Secure Software Programming Certification Class & Exam	72	\$3,990
R	Q/SH/D® Qualified/ Software Hacker / Defender Certification Class & Exam	72	\$3,990
R	Q/STBP® Qualified/ Software Tester Best Practices Certification Class & Exam	72	\$3,990
R	Introduction to Reverse Engineering Certification Class & Exam	72	\$3,990
R	SU Security+® CompTIA Certification Class & Exam	72	\$3,990

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.		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 & Exam	72	\$3,990
R	IDS II Catching the Hackers II: Systems to Defend Networks Cert Class & Exam	72	\$3,990
R	IDS III: On-site Log Analysis, Event Correlation and Response Cert Class & Exam	72	\$3,990
R	Q/MC® Qualified/ Mission Critical Certification Class & Exam	72	\$3,990
R	Q/CDA Qualified/ Cyber Defense Analyst Certification Class & Exam	72	\$3,990
R	SU Security+® CompTIA Certification Class & Exam	72	\$3,990
R	SU CASP® Certified Advance Security Professional Certification Class & Exam	72	\$3,990
R	SU CISSP® Certified Information Security Systems Professional Class & Exam	72	\$4,190
R	Linux/UNIX® Security Certification Class & Exam	72	\$3,990
R	SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class & Exam	72	\$3,990
R	Cloud Computing Security Knowledge Certification Class & Exam	72	\$3,990
R	Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam	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 & Exam	72	\$3,990
E	How to Conduct Network Vulnerability Analysis & Exam	72	\$3,990
E	Microsoft Certified Solutions Expert & Exams	360	\$10,990
E	Python Forensics Certification Class & Exam	72	\$3,990
E	PowerShell Forensics Certification Class & Exam	72	\$3,990
E	Python/Powershell Incident Response Certification Class & Exam	72	\$3,990
<p>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. Practical required CPoM designation "validation" after class completion. Practicals are mastery evidence to support the claim of knowing something.</p> <p>SU Accelerated Qualified/ Registered Cyber Apprenticeship Program. 100% eligible for veteran education benefits. Earn 8 Cyber Certs/ 24 mo/ attend 8 courses of 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® Certificate Program of Mastery Exams/ SUT Q/ISP®, Q/IAP®, Q/WP®, Q/SSE® Q/CND® Certification exams by TESTRAC are high stakes, on site, on-line, on-demand testing.</p>			

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

NONSTANDARD TERM DEFENITION

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 hour contact hours.

ADMISSIONS REQUIREMENTS

SU is committed to equal educational opportunity and 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
- Demonstrate sufficient knowledge of the Transmission Control Protocol/Internet Protocol (TCP/IP).
- Verified 2 months of work experience or employer enrollment.
- Interview with the school president who confirms the students work history and TCP/IP knowledge.
- A resume can verify 2 months of work experience using TCP/IP.
- A school transcript is requested for prior credit.

STUDENT ORIENTATION

All incoming Students must attend Orientation which will be held prior to the start of the program. During Orientation, the Student will learn about responsibilities and standards, the format of the program, the progression of the program, and how performance will be measured.

All classes are taught in English. All face-to-face courses begin @7:45am first day and 8am thereafter 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 3 classrooms, 2 classrooms seat 50 students, 1 seat class room seats 15 students. 95% attendance is expected of all students. An instructor may remove any student who exceeds 3 two hours of absences. Faculty members must include in the course syllabus any attendance policies that will affect student outcomes, including those concerning tardiness and early departures from class.

STUDENT RESPONSIBILITIES

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. Furthermore, 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 unit course or subject or combination of courses or subjects which is pursued by a veteran, dislocated worker, non-traditional student or service member at an educational institution, which is a combination of cyber courses pursued at SU. The combination of cybersecurity classes is accepted as necessary to meet requirements for a predetermined educational, professional or vocational objective for 5 Certificate Programs of Mastery. It may consist of subjects or courses which fulfill requirements for more than one cyber certificate objective related to a cybersecurity career field. Including an approved full-time program of apprenticeship or on-job training;

FINANCIAL AID, CANCELLATION AND TUITION REFUNDS POLICY

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.

A prospective or current student may cancel their Certificate Program of Mastery enrollment through the last day of class and receive a 100% refund of all tuition and fees paid (excluding exam fees). Any student who paid by credit card is responsible for a 6% credit card processing fee. If a student has pre-paid tuition for the entire program (\$26,500 for 13 courses), they will be refunded the actual amount of the tuition and exam fees not used. The refund would equal the tuition paid minus the cost of the courses completed along with the applicable exam fees. Applicants and students must request a refund via email or phone call. SU refunds are within 45 days after receipt of a written request or the date the student last attended classes whichever is sooner. SU reserves the right to cancel a class at any time. If this happens, SU will refund the class fee in full. SU's liability is limited to the class fees only. SU cannot be held liable for other related expenses, i.e., airfare, airline penalties, lodging, etc. Should a prospective or current student request to re-schedule for extenuating or unforeseen circumstances, SU requests the student re-register for the next class date at no additional charge.

An applicant must demonstrate the character readiness, and commitment to successfully complete the academic program for which admission is requested. In determining whether to grant or deny admission, SU will consider information about the applicant's prior postsecondary educational experiences, employment record, credit record and any criminal record. 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.

TRANSFER

This School may accept appropriate credit from previous education after enrollment. This School does not guarantee the transferability of its credits unless there is a written articulation agreement with the institution. This School may accept credit hours for valid credential. An official transcript will be used to determine the appropriate entry point into the curriculum to provide a better educational experience.

VA ELIGIBILITY:

Students who are eligible for VA benefits must provide a copy of their VA Certificate of Eligibility letter or Entitlement Information print-out from “eBenefits” (for Chapter 33) or form 28-1905 (for Chapter 31) on or before the first day of Class to have their VA Educational Benefits included in their Estimated Financial Plan. Delay of VA Disbursement to School: Due to a delay in disbursement funding from VA under Chapter 31 or 33, SU will not:

- Prevent a student from enrolling
- 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

Any student who attends a course under chapter 31 or 33 certificate of eligibility may attend from the beginning on the date the student provides a COE until the VA provides payment to the school or 90 days after the school certifies tuition and fees. Exam fees are line items and noted as included or not included in the class fee on each invoice and receipt “as noted above” No penalty’s late fees of denial of access to classes libraries or school facilities, or require the student borrow additional funds die 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 their sudden withdrawal or pro-longed absence from their enrollment, will be eligible to re-enroll at the school by consulting with the President.

PRIOR CREDIT POLICY:

Per, 38CFR 21.4254 (c)(4), VA eligible Students must provide a copy of all post-secondary transcripts (not just those for cyber programs). The school will maintain written records of pervious education and training. Appropriate credit will be granted by the school for previous education and training, with the training period shortened proportionately, and the Student and VA so notified.

VA ATTENDANCE POLICY

Attendance is evaluated each day of class. If attendance falls below 95% upon formal evaluation, the student will be asked 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 documented mitigating circumstances will not be terminated. Alternate arrangements for continuing attendance, without termination from the school may be made to make up hours, at the discretion of the President. However, veterans may not be certified to the VA 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 Certifying Official.

VA 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.

VA 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 possible termination of veteran’s educational benefits, and possible dismissal from SU. Re-admittance after conduct dismissal requires reapplication to the school.

VA 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 that includes costs, 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 data 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 program was paid in full the appropriate refund will be refunded.

PII - By policy SU does not provide (unencrypted) PII to anyone.

SATISFACTORY ACADEMIC PROGRESS (SAP)

Satisfactory Academic Progress (SAP) is required for *all enrolled Students*. All students are provided access to the SAP policy during enrollment. SAP periods are based on student's original certificate program class registration agreement and subsequent class registrations. Students meeting the minimum requirement attendance (95%) of each class are considered to be making SAP of their qualified cyber certificate program of mastery program.

Standards of Progress Policy: SU provides non-college degree (NCD) programs and vocational objectives based on hours, not credits. Students agreements include the following:

- SU conducts course eligibility screening with *every new* student prior to enrollment
- Students must disclose transfers credit hours asap after registering in a qualified certificate program of mastery
- Students review policies regarding the award of [academic] credit hours for prior 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 credits and awards learning acquired for specialized military training of cybersecurity occupational experience when applicable.

1. Each course registration is a student agreement to attend the course. A syllabus is distributed to students at class registration which contains information on how students meet course completion. Any student arriving to class more than three hours late will be considered absent and asked to make up the time or reschedule class.
2. Student progress is measured daily for progress evaluation. Student attendance and progress reviewed by the faculty and the president daily. Students are expected to attend 95% of the 72 hours of class 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.
3. At the end of every 72-hour class, the president and faculty review attendance and academic data to determine who have completed class and award participation agreements.

SU demonstrates a student's progress (SOP) in learning the materials and 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 taking a required cyber exams. Students earn a participation certificate documenting their class completion and a transcript of their continued pursuit of their cybersecurity qualified cybersecurity certificate program of mastery.

GRADING PROCEDURE

Grading Policy/Standards of Progress/Practical - 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, grades on quizzes to support the learning process and encourage student success, and ensures accuracy, consistency and fairness in scoring for each student. *Exams (100-70% passing grade) are not include to determine a final pass/fail grade.* The goal of a practical assessment is to measure competency. Ample practice and feedback will be given generously as students are on site in labs. Students will be periodically evaluated based upon performance and attendance. In case of a failure, the student can update or retake the assessment. The first passing grade will be recorded. The enrichments practical's are evaluated on a Pass or Not Passed basis.

COURSE DESCRIPTION

Each Qualified Cybersecurity Certificate Program of Mastery consists of 13 required instructor led courses and practicals prepare students with the technical skills you need to be an effective cybersecurity professional.

Instructor led courses involve performing advanced procedures and services on live systems for defensive and offensive security. Each course will provide students with an understanding of the Fundamentals and Procedures of cybersecurity, system administration, networks and network security, defensive and offensive security skills necessary to complete a successful cybersecurity job task. SU training is developed by a global team of cybersecurity experts. Training covers the full spectrum of cybersecurity 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 cybersecurity roles. Match today's threat landscape with the right skills.

EDUCATIONAL OBJECTIVES / GOALS:

Upon completion of 13 required courses in a Qualified Certificate Program of Mastery a student graduates.

Students will have the following:

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

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

Proficiency to advance your cybersecurity career

Earned valuable Certificate of Completion and cyber certification credentials for cyber careers

SU's NICE publication provides a fundamental reference in support of building a workforce capable of meeting a student's vocation objective and cybersecurity needs by using a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role using a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks necessary for each cyber work role. SU supports the NICE Framework for cybersecurity 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. All classes are approved for face to face or hybrid. This 72 hour accelerated class is taught using face to face modality or hybrid modality. Class includes 72 hours of contact studies, labs, reading assignments and final exam - passing the final exam is a requirement for graduation.

INSTRUCTIONAL METHODS

In a student-centered classroom, Educators will instruct and coach students to achieve competency in all the various skill sets, through problem solving, self-paced study, 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. Enrichment and practical's gives the student more time to study concepts with greater depth, breadth, and complexity. Enrichment also 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 order to graduate and receive a certificate, Students must meet the following requirements:

- Complete the required hours of training
- Complete curriculum requirements
- Fulfill all financial obligations to the school

Upon completion of all course requirements, successful completion of the certification classes, exams and practicals is required to obtain a participation certificate making you eligible for cyber employment.

TUITION

Each Qualified Cybersecurity Certificate Program of Mastery fee is \$26,500 and consists of 13 required instructor led courses. The CPoM \$26,500 class fee includes all “R” required classes listed on the course fee sheet above – exams are required to graduate. Students enrolled in a CPoM using a pay as you go payment method can select from the CPoM fee chart where all classes are priced separately – exams are required to graduate. Students using veteran benefits are charged the entire \$26,500 tuition rate pro-rated per class.

STUDENT SERVICES

During career planning interviews and Student orientation, students receive information about the qualified cybersecurity certificate instructional programs, goals of each 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 graduate in obtaining a career-related position. Employment opportunities are available for review from 3rd party cybersecurity 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. Career advising, placement services and employment opportunities. SU does not provide job placement services however SU does provide independent training plan consultation (upon request) to determine student’s certification path to increase their interview opportunities before/ after class registration. SU is frequently requested to post cyber job openings and career links to SU websites, advertise job opportunities and host career fairs. (<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 eligibility to determine an effective independent training plan that review cyber credentials 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 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.

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 sOndra@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.

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.

Testimonial 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. ADuby Captain, USA - Department of Computer Science, University of Colorado at Colorado Springs



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

Q/SA® Qualified/ Security Analyst and Penetration Testing Certification

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 Penetration Tester Certification Class & exam
Q/PTL® Qualified/ Penetration Tester License workshop
Q/EH® Qualified/ Ethical Hacker Certification Class & exam
Q/ND® Qualified/ Network Defender Certification Class & exam
Q/FE® Qualified/ Forensic Expert Certification Class & exam
SU CISSP® Certified Information Security Systems Professional Class & exam
SU Security+® CompTIA Certification Class & exam
SU CASP® - CompTIA Advance Security Professional Certification Class & exam
Linux/UNIX® Security Certification Class & exam
Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & exam
Q/PTL® Qualified/ Penetration Tester License Practical required to graduate
Q/ND® Qualified/ Network Defender Certification Practical required to graduate
Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate

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 "Practical", fully detailed management report. Your report is due to SU 60 days from the start of class. This practical shows your penetration testing skills and validates 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
Time:	72 hrs
Learning Level:	Intermediate
Contact Hours:	40 hr Lecture 32 hr labs
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 Practical for CPoM Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid 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 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, CRYPTO tool, 'Curl'

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 scripts to extract information from target systems
- Configure and launch a vulnerability scanners, like Nessus, Metasploit , 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 lines 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 20 hr Lecture 30 hr labs

Penetration concepts you will master during this hands on class

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

Expectations You 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

10 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. SU Q/SA® class is CNSS-approved. 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, C&A
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 14 hr Lecture & labs

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 14 hr Lecture & labs

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 14 hr Lecture & labs

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 14 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 Lesson 5 14 hr Lecture & labs

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

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practical 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



Super Qualified



Q/PTL QUALIFIED/ PENETRATION TESTER LICENSE

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/PTL 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 practical provides adequate evidence to support the claim of knowing something.

Class Fee: \$4,500
Time: 72 hrs
Learning Level: Intermediate
Contact Hours: 72 hours
Prerequisites: Understanding of TCP/IP Protocols
Credits: 30 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 Practical for CPoM
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 72 hour accelerated class is taught using face to face modality or hybrid 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 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 ,Ncat , 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 72 hrs labs

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 1 14 hrs 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 access
 - 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. 1 Hr 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 14 hrs 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. SNMP 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 14 hrs Lecture & Labs

4. .5 Hr 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. .5 Hr 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. .5 Hr 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. .5 Hr 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 Plan3 14 hrs Lecture & Labs**
8. .5 Hr 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. .5 Hr 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. .5 Hr 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. .5 Hr 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 14 hrs Lecture & Labs**
12. .5 Hr 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. .5 Hr 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. .5 Hr 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. .5 Hr 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 2-5pm 1 hr gather data 6pm

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the practical 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 + CEH Training



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 72 hour 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: 42 hrs lecture/ 30 hrs labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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 ,Ncat , 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.

- 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 identify 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. **31 hrs lecture/ 41 hrs labs**

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

Lesson Plan 1

Qualified Ethical Hacker /Defender (QEH/D) Module 1: Ethics and Legality **1 hrs Lecture 1 hr 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 **2 hrs Lecture 2 hr 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
2 hrs Lecture 2 hr 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 **2 hrs Lecture 3 hr Labs**

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

Qualified Ethical Hacker /Defender (QEH/D)) Module 6: Trojans and Backdoors **1 hrs Lecture 2 hr 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 **2 hrs Lecture 3 hr 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 **1 hrs Lecture 1 hr Labs**

- Understand the types of DoS Attacks
- Understand how DDoS attack works
- Understand how BOTs/BOTNETS work
- What is "smurf" attack

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

Qualified Ethical Hacker /Defender (QEH/D) Module 4: Enumeration **2 hrs Lecture 2 hr 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

- What is "SYN" flooding
- Describe the DoS/DDoS countermeasures

Qualified Ethical Hacker /Defender (QEH/D)) Module 9: Social Engineering **1 hrs Lecture 1 hr 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 **1 hrs Lecture 2 hr 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 **1 hrs Lecture 2 hr 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 **1 hrs Lecture 2 hr Labs**

- Understanding how web application works
- Objectives of web application hacking
- QSAAatomy 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 **1 hrs Lecture 2 hr 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 **1 hrs Lecture 2 hr 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 **2 hrs Lecture 2 hr 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 **1 hrs Lecture 2 hr 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 **1 hrs Lecture 0 hr 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 **2 hrs Lecture 0 hr 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 **2 hrs Lecture 3 hr 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 **1 hrs Lecture 2 hr 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 **2 hrs Lecture 1 hr 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 **2 hrs Lecture 3 hr 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 practical 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 Penetration Tester Certification Class & exam
Q/PTL® Qualified/ Penetration Tester License workshop
Q/EH® Qualified/ Ethical Hacker Certification Class & exam
Q/ND® Qualified/ Network Defender Certification Class & exam
Q/FE® Qualified/ Forensic Expert Certification Class & exam
SU CISSP® Certified Information Security Systems Professional Class & exam
SU Security+® CompTIA Certification Class & exam
SU CASP® - CompTIA Advance Security Professional Certification Class & exam
Linux/UNIX® Security Certification Class & exam
Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & exam
Q/PTL® Qualified/ Penetration Tester License Practical required to graduate
Q/ND® Qualified/ Network Defender Certification Practical required to graduate
Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate



Q/ISP Qualified/ Information Security Professional Certificate of Mastery



Q/ND- QUALIFIED/ NETWORK DEFENDER

Q/ND® Qualified/ Network Defender

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 misconfigurations, 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: 18 hr Lecture 22 hr labs
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 Practical
Fail > 95% Attendance

This 72 hour accelerated class is taught using face to face modality or hybrid 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, Digital 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

I Lecture 38 Lab 34

1 hr Lecture

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

1 hr Lecture

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

1 hr Lecture 1 hr labs

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

2 hr Lecture 2 hr labs

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 applications

Lesson Plan 2

1 hr Lecture 1 hr labs

5. 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

1 hr Lecture 1 hr labs

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 IPv6s
- How to configure
- How to integrate with firewalls & VPN's
- What VPN's to use with which firewalls
- Gartner's report on IPv6 & IPv6 matrix

1 hr Lecture 1 hr labs

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 hr lecture

1. Preparation - Laying the groundwork for effective malware

1 hr Lecture 1 hr labs

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

1 hr Lecture 1 hr labs

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

1 hr Lecture 1 hr labs

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

1 hr Lecture 1 Hr lab

11. Firewall, VPN & Prevention Management

assessing the firewall, VPN & IPv6 vendors
independent certification of firewall & VPN products
installation, training and after sales support
assigning resources for firewall, VPN & IPv6

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, & IPv6 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

1 hr lecture 2 hr 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

1 hr lecture 2 hr labs

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

1 hr Lecture 2 hr labs

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

Defining a recovery strategy and restoring a system
Defining incident management goals and metrics

Lesson Plan 5

1 hr Lecture 2 hr labs

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.

1 hr Lecture 2 hr labs

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

2 hr lab Class Exercises

- 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
-

Exam 75 Questions Online exam, begins at 1pm

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practical 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 you're mitigating the threat step by step. All books are provided during class.



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

Q/FE QUALIFIED/ FORENSICS EXPERT CERTIFICATION

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 practical 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.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 42 hr Lecture 30 hr labs
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 Practical for CPoM
Fail > 95% Attendance

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

This 72 hour accelerated class is taught using face to face modality or hybrid 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.

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:

- 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: 20 hrs lecture/ 20 hrs labs

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.

2 hr Lecture 1 hr labs

Detecting Computer Crime

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

2 hr Lecture 2 hr 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

4 hr Lecture 5 hr 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

3 hr Lecture 3 hr 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

3 hr Lecture 6 hr 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

2 hr Lecture 2 hr 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

2 hr Lecture 1 hr 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

1 hr Lecture 0 hr 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

SU Q/ISP® Qualified/ Information Security Professional Certificate Program of Mastery CPoM / non degree-
Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class & exam
Q/PTL® Qualified/ Penetration Tester License workshop
Q/EH® Qualified/ Ethical Hacker Certification Class & exam
Q/ND® Qualified/ Network Defender Certification Class & exam
Q/FE® Qualified/ Forensic Expert Certification Class & exam
SU CISSP® Certified Information Security Systems Professional Class & exam
SU Security+® CompTIA Certification Class & exam
SU CASP® - CompTIA Advance Security Professional Certification Class & exam
Linux/UNIX® Security Certification Class & exam
Cloud Computing Security Knowledge Certification (CCSK & Plus) Class & exam
Q/PTL® Qualified/ Penetration Tester License Practical required to graduate
Q/ND® Qualified/ Network Defender Certification Practical required to graduate
Q/FE® Qualified/ Forensic Expert Certification Class Practical required to graduate

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

Q/AAP Qualified/ Access, Authentication & PKI Professional



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 72 hour 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: 41 hr Lecture 31 hr labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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.

KU Outcomes:

- * Students shall be 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: 41 hrs lecture/ 31 labs

- 1. Cryptography Refresher: concepts, algorithms, key management 1 hr Lecture 0 hr labs**
- 2. Public Key Infrastructure (PKI) 3 hr Lecture 2 hr labs**
- 3. Network Security Refresher**
 - Network Defense and Countermeasure
 - Penetration Testing
 - Transmission Security
 - Security Roles and Responsibilities
- 4. Digital Certificates and Digital Signatures 3 hr Lecture 2 hr 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 4 hr Lecture 5 hr 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 3 hr Lecture 5 hr 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 3 hr Lecture 2 hr labs**
 - Pitfalls of remembered password systems
 - Encryption: Digital certificates and digital signatures
 - Smart cards
 - Tokens
 - Biometrics
 - Combining authentication mechanisms for multi-factor authentication
 - Hands-on exercises: using smart cards and biometric authentication tools
- 8. Overcoming Pitfalls in Encryption and Certificate Management 2hr Lecture 1 hr labs**
 - Avoiding common pitfalls in the use of encryption and PKI

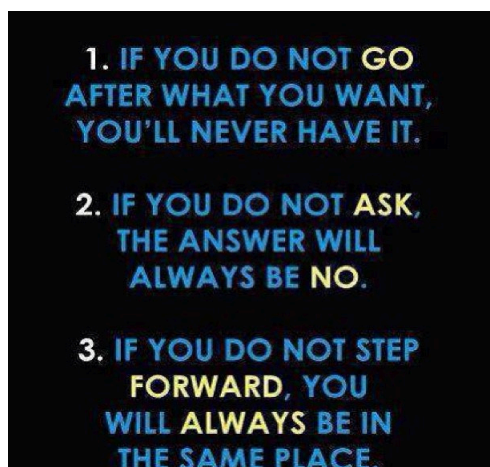
- How to avoid underestimating the complexity of a PKI rollout
- Challenges associated with encryption
- Key management
- Case Studies: An examination of how PKI and CAs have been used in real organizations

8. Deploying a PKI 3 hr Lecture 2 hr 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 practical 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 & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class and Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum
PMP Project Manager Professional Certification Class & Exam
SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam



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

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



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: 45 hr Lecture 27 hr labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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.

Lesson Plan 45 hrs lecture/ 27 hrs labs

5 hr Lecture 3 hr 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

4 hr lecture 3 hr labs

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 hrs Lecture 2 hr Labs

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

6 hr Lecture 2 hr labs

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

3 hrs Lecture 0hr 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

1 hrs Lecture 2 hr Labs

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 practical 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 practical 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 available 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 & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum

PMP Project Manager Professional Certification Class & Exam
SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam

Q/CandA® RMF - Qualified/ Certification and Accreditation Administration

This class is designed for key personnel responsible for the management and implementation of the NIST SP800-37 Certification and Accreditation process. This course will provide a practical and 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.  **Note:** This class can be easily tailored to meet the certification and accreditation needs of any organization.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry to Intermediate
Contact Hours: 72 hrs lecture/ 22 hrs labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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.

Learning Objectives **50 hrs lecture/ 22 hrs labs**

- Information System Security Administration, Management, 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 Accredited
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 28 hrs lecture/ 12 hrs labs:

Domain 1: Describe the Risk Management Framework (RMF)

6 hrs Lecture 0 hr Labs

- 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

6 hrs Lecture 0 hr Labs

- 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

6 hrs Lecture 3 hr Labs

- 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 Controls

6 hrs Lecture 2 hr Labs

- 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

6 hrs Lecture 2 hr Labs

- 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

6 hrs Lecture 2 hr Labs

- 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

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

Domain 7 - RMF Step 6: Monitor Security Controls

6 hrs Lecture 3 hr Labs

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

The Q/CA 10 hr practical measures of the knowledge, skills and abilities required for C&A / A&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 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 practical 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/IAP Qualified/ Information Assurance Professional Certificate Program of Mastery

DoD Information Tech Security Cert / Accreditation Process DITSCAP

This class is designed for key personnel responsible for the management and implementation of the NIST SP800-37 Certification and Accreditation process. This course will provide a practical and 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 on the DoD Information Assurance Certification and Accreditation Process (DIACAP) is the United States Department of Defense (DoD) process to ensure that risk management is applied on information systems (IS). DIACAP defines a DoD-wide formal and standard set of activities, general tasks and a management structure process for the certification and accreditation (C&A) of a DoD IS that will maintain the information assurance (IA) posture throughout the system's life cycle..



Note: This class can be easily tailored to meet the certification and accreditation needs of any organization.

Class Materials: NIST SP800-37 C and A Process Materials
Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 72 hr Lecture 0 Labs
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 & Practical Fail > 95% Attendance

Sample Job Titles
Contracting Officer (CO)
IA Manager
IA Program Manager
IA Security Officer
IS Program Manager
IS Manager (ISSM)
IS Security Officer (ISSO)
IS Security Operator

This 72 hour accelerated class is taught using face to face modality or hybrid 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 4M Ram, 350 Gig drives, running MS OS, linux, and VMWare Workstation.

Who Should Attend 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, Information Security Analysts, Consultants and Contractors; Security and Certification Officials responsible for developing C&A packages

KU outcomes:

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

Scope & Objectives 52 hrs lecture/ 20 hrs labs

Conduct a Non-Technical Assessment of Information Security
Review Documentation and the Origin of Specific Requirements
Evaluation of System Architecture Including Defense-in-Depth (DiD)
Coordinating and Identifying Collateral Resources to Facilitate the C&A Process
Constructing and Tailoring the C&A Plan
Consolidating C&A Collateral Documentation
Preparing Security Test and Evaluation Plans and Correlating Testing
Identifying Evaluation Techniques

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

Business Needs / Course Goals for C&A DITSCAP Process 52 hrs Lecture 20 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

The **DoD Information Assurance Certification and Accreditation Process (DIACAP)** is the [United States Department of Defense](#) (DoD) process to ensure that [risk management](#) is applied on [information systems](#) (IS). DIACAP defines a DoD-wide formal and standard set of activities, general tasks and a management structure process for the [certification](#) and [accreditation](#) (C&A) of a DoD IS that will maintain the [information assurance](#) (IA) posture throughout the [system's life cycle](#).

One major change in DIACAP from [DITSCAP](#) is the embracing of the idea of [information assurance](#) controls (defined in DoDD 8500.1 and DoDI 8500.2) as the primary set of security requirements for all automated information systems (AISs). The IA Controls are determined based on the system's [mission assurance](#) category (MAC) and confidentiality level (CL).

Process

System Identification Profile Lesson 1 8hrs

DIACAP Implementation Plan Lesson 2 8hrs

Validation

Certification Determination Lesson 3 4hrs

DIACAP Scorecard Lesson3 4hrs

POA&M Lesson 4 8hrs

Authorization to Operate Decision Lesson 5 4hrs

Residual Risk Acceptance Lesson 5 2hrs 2hr Exam

References

- [DIACAP Guidance at the DoD Information Assurance Support Environment](#)
- [DIACAP Knowledge Service](#) (requires DoD [PKI](#) certificate)
- [Full list of DIACAP Phases](#) with instructions at GovITwiki.
- [DPT. Of Defense Instruction 8510.01: DoD Information Assurance Certification and Accreditation Process](#)
- [Department of Defense Directive 8500.1: Information Assurance \(IA\)](#)
- [Department of Defense Instruction 8500.2: Information Assurance \(IA\) Implementation](#)

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practical 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.

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

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

ISC2 Certification Class - ISC² CISSP® Training Class (The Official SU CISSP Training)

ISC2 ISSP Certified Information System Security Professional CERTIFICATION Training Class

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: \$4,190 incl exam fee
Time: 72 hrs
Learning Level: Entry
Contact Hours: 51 hr Lecture 21 quiz labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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.com 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: 31 hrs lecture/ 9 hrs labs Lesson Plan 1-5 / 2 domains with online quizzes

Domain 1 – Security and Risk Management

- Information Security Concepts and Objectives
 - 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

Directory Management of Identity and Access Control Information
Attacks on Access Controls
Access Control Management

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

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 Considerations for Commercial Off-The-Shelf Software
Artificial Intelligence

- **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

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:**

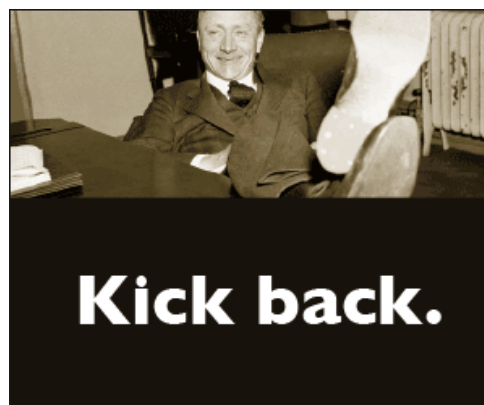
- Backup and Fault Tolerance
- Business Continuity and Disaster Recovery

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 practical 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: 48 hr Lecture 14 hr labs
Prerequisites: None - need 4 yrs in IT to exam
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 72 hour accelerated class is taught using face to face modality or hybrid 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.

58 hrs lecture/ 14 hrs labs

Lesson Plan 1 2 hrs Lecture & Labs 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 12 hrs Lecture & Labs Administration - Identification of information assets and documentation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability.

Lesson Plan 3 12 hrs Lecture & Labs 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 12 hrs Lecture & Labs 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 12 hrs Lecture & Labs 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 12 hrs Lecture & Labs 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 12 hrs Lecture & Labs 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 practical 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® Bootcamp up to one year

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

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Intermediate
Contact Hours: 51 hr Lecture 21 hr labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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 Bootcamp
- 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 Schedule 14 hr lecture & hr labs each 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 practical 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® Training Class

CISA Certified Information Security Auditor

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Basic
Contact Hours: 72 hr Lecture No labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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*

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 4 hrs -

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 4 hrs

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 8 hrs

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 8 hrs

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 8 hrs

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 8 hrs

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
Human 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 practical 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

CISM® Training 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.

A One-of-a-Kind Credential

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 Bootcamp is 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.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 52 hr Lecture 20 Quiz Labs
Prerequisites: None
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

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 72 hour accelerated class is taught using face to face modality or hybrid 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 72 hrs lecture:

1 Information Security Governance & Strategy 14 hrs

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 14 hrs

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 14 hrs

- 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 14 hrs

- 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 14 hrs

- Incident Management and Response Overview
- Incident Management
- Concepts Scope and Charter of Incident Management
- Information Security Manager
- Incident Management Objectives

Post event Reviews

- 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



Grades -All students must ordinarily take all quizzes, lab, final exam and submit the class practical 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/ISP Qualified/ Information Security Professional Certificate Program of Mastery

SECURITY+ CompTIA Certification

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: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 51 hr Lecture 21 hr labs
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
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 72 hour accelerated class is taught using face to face modality or hybrid 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

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 - 31 hrs lecture/ 9 hrs labs

Tips for taking the exam & SU Pre-class Study Techniques

1.0 Security Governance, Risk, and Compliance (Risk Management) 21%

2.0 CyberSecurity 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 CyberSecurity 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 an enterprise network, on-site or in the cloud, with security in mind

Lesson Plan 51 hr lecture 21 labs/quizzes

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

4 hrs Lecture 2 hr Labs

1.1 CyberSecurity Concepts

- Confidentiality, integrity, availability
- Business drivers for cybersecurity: risk, compliance
- Roles in CyberSecurity management
- Regulatory compliance overview

1.2 CyberSecurity 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 CyberSecurity Controls

- Types of security controls - administrative, technical, physical
- CyberSecurity control intent

1.4 Policies, Standards, Procedures, and Administrative Controls for CyberSecurity

- 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 CyberSecurity Incident Response Procedures

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

1.7 Fundamentals of CyberSecurity 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

5 hrs Lecture 2 hr Labs

2.0 CyberSecurity Threats, Attacks and Vulnerabilities

2.1 Identifying and Characterizing Threat Actors

Types of actors

- Attributes of actors

2.2 Types of CyberSecurity 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 CyberSecurity Frameworks and Configuration Baselines

- Benchmarks/secure configuration guides
 - Defense-in-depth/layered security
- ### 3.2 Implementing Network CyberSecurity 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

5 hrs Lecture 2 hr Labs

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 CyberSecurity Technologies and Tools

4 hrs Lecture 2 hr Labs

6.1 Install and Configure CyberSecurity 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 CyberSecurity Assessment Tools

- Protocol analyzer
- Network scanners
- Command line tools

6.3 Troubleshooting CyberSecurity 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 CyberSecurity 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 28hr lecture 12 hr labs/quizzes

2 hrs 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.

2 hrs Administration - Identification of information assets and documentation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability.

2 hrs 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.

2 hrs 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

2 hrs 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.

2 hrs Data Communications - The network structure, transmission methods and techniques, transport formats and security measures used to operate both private and public communication networks.

2 hrs 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 practical 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

CASP CompTIA Advanced Security Practitioner (CASP) Course

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

CASP is CompTIA's first mastery-level certification for enterprise technical security leads. CASP 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 CASP certified confirms that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. CASP 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.

CASP 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 CASP certification is included in the approved list of certifications that meet the DoD Directive 8570.1 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 + \$411 Exam fee
Time: 72 hrs
Learning Level: Advanced
Contact Hours: 72 hr Lecture 22 hr labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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 Advanced Security Practitioner (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

Learning Objectives - 40 hrs lecture/ 32 hrs labs

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 Advanced Security Practitioner (CASP) Course Outline 6 hr lecture 2 hr lab

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 6 hr lecture 2 hr lab

Lesson 2A: Cryptographic Concepts Techniques

Lesson 2B: Host and Storage Security controls;

Lesson 2C: Application Security;

Lesson 2D: Network Security Components

Domain 3 Technical Integration of Enterprise Components 6 hr lecture 2 hr lab

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 6 hr lecture 2 hr lab

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 6 hr lecture 2 hr lab

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 CASP Certified?

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

- | | |
|---|--|
| <p>1. Managing Risk</p> <ul style="list-style-type: none"> Identify the Importance of Risk Management Assess Risk Mitigate Risk Integrate Documentation into Risk Management | <p>Enterprise</p> <ul style="list-style-type: none"> Analyze Scenarios to Secure the Enterprise |
| <p>2. Integrating Computing, Communications, and Business Disciplines</p> <ul style="list-style-type: none"> Facilitate Collaboration across Business Units Secure Communications and Collaboration Solutions Implement Security Activities throughout the Technology Life Cycle | <p>4. Integrating Advanced Authentication and Authorization Techniques</p> <ul style="list-style-type: none"> Implement Authentication and Authorization Technologies Implement Advanced Identity Management |
| <p>3. Using Research and Analysis to Secure the Enterprise</p> <ul style="list-style-type: none"> Determine Industry Trends and Effects on the | <p>5. Implementing Cryptographic Techniques</p> <ul style="list-style-type: none"> 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 practical 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/ISP Qualified/ Information Security Professional Certificate Program of Mastery

QUALIFIED/ SECURITY HACKING CERTIFICATE FOR MANAGERS



This 72 hour Qualified Security Hacking Certificate class 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: 48 hr Lecture 24 hr lab
Prerequisites: none
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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: 36 hrs lecture/ 36 hrs labs

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

4 hrs Lecture 4 labs

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 Hacker: Footprinting 3 hrs Lecture 3 hr labs**

- 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 3 hrs Lecture 5 hrs labs**

- 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 perimeter
- **1 hr lecture 3 hr labs**
- You will examine the weaknesses of firewall architectures
- Securing mail with VPN
- Examine E-shoplifting
- Hack SSL-enabled sites

- 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

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

- Reverse WWW Shell
- **How to detect the crime, track the criminal, and assemble the evidence. 3 hrs Lecture 4 hr labs**
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
- **Understanding Computer Investigations 2 hr Lecture 5 hr labs**
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
- Preparing for Computing Investigations
- Understanding Enforcement Agency Investigations
- Understanding Corporate Investigations
- Maintaining Professional Conduct
- 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

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

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

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 practical 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/WP Qualified/ Professional Certificate Program of Mastery

Q/WLANPD Qualified/ Local Area Network Planning and Design

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 35 hr Lecture 37 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 practical 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 2 hr lecture

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

- 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 Organizations and Standards 3 hr lecture

- 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 Security & Compliance 3 hr lecture

- 802.11 Legacy Security Methods
- Encryption – TKIP/CCMP
- Authentication Passphrases & 802.1X/EAP
- WPA/WPA2-Personal
- WPA/WPA2-Enterprise
- WPS Pushbutton/ PIN
- RoE-Based Access Control (RBAC)
- VPN Security
- Intrusion

Wi-Fi Hardware & Software 2 hr lecture

- Protection Systems (WIPS)
- PCI Compliance
- HIPAA Compliance
- Enforcing Compliance

Wi-Fi Site Surveying 3 hrs lecture 10 hrs labs

- 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 2 lectures 2 hr labs

- 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 2 hr lecture 2 hr labs

- 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

Classroom Demonstrations & 30 hr labs

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.

- 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 5 hr labs

- 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 3 hr labs

- 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 3 hr labs

- 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

Q/WP QUALIFIED/ PROFESSIONAL CERTIFICATION

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 the MOST RESPECTED 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:	35 hr Lecture 37 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 security. 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:

Lesson Plan 18 hrs lecture/ 27hrs labs:

1. Lesson Plan 1 12hrs Lecture & Lab

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 enhance 802.11 WLAN

2. **2 hrs lecture/ 1.5 hrs labs**

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. **14 hrs Lecture & Lab**

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 two 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 **12hrs Lecture & Lab**

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 **14hrs Lecture & Lab**

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 4 **14hrs Lecture & Lab**

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 practical 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 of Mastery CoM non degree (4 Q/WP® + Security+®, CASP®)
Q/WAD® Qualified/ Analyst & Defender Class & Exam
Q/ WP® Qualified/ Professional Certification Class & Exam
Q/WSP® Qualified/ Security Professional Certification Class & Exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ Qualified / Qualified Security Professional Certification Class & Exams
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
PMP Project Manager Professional Certification & Exam
Q/WLANPD Qualified/ Local Area Network Planning & Design & Exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing & Exam
Q/WDNO Qualified/ Deceptive Network Optimization & Exam

QWSP® QUALIFIED/ SECURITY PROFESSIONAL

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. Practical 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: 51 hr Lecture 21 hr labs
 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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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:

- 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 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

2.5 hrs Lecture 2 hr Labs

WLAN Intrusion

- 1.1. Intrusion Tools
- 1.2. Intrusion Techniques
- 1.3. LAB – WLAN Intrusion Tools and Techniques

2. 1hrs Lecture

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. 2hrs Lecture 2 hr Labs

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-depth 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 802.1X/EAP solutions changed to 802.11i/RSN solutions
- 3.10. 802.11i frame format explanations and graphics

Lesson Plan 2

4. .5hrs Lecture

The 802.11i amendment

5. 2hrs Lecture 2 hr Labs

IP Security – Network Layer Security

5.1. PPTP VPN

5.2. IP Framework and implementation discussion and graphical detail

Lesson Plan 3

6. 2 hr Labs

LAB – 802.1X/EAP & VLAN based Security Solutions

7. 2hrs Lecture 2 hr Labs

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. 2hrs Lecture 3 hr Labs

Lab Exercises

- 8.1. Secure WLAN Bridging
- 8.2. WLAN Switching
- 8.3. Enterprise Encryption Gateways (EEGs)
- 8.4. Enterprise Wireless Gateways (EWGs)
- 8.5. SOHO/SMB solutions
- 8.6. WLAN Routers

9. 2hrs Lecture 2 hr Labs

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. 2hrs Lecture 3 hr Labs

Authentication, Authorization, and Accounting (AAA) Systems

- 10.1. Local Authentication in APs, EWGs, WLAN switches, and WLAN routers
- 10.2. RADIUS authentication and proxy services
- 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. 3hrs Lecture 4 hr Labs

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

2hrs Lecture 2 hr Labs

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 practical 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 of Mastery CoM non degree (3 Q/WP® - Q/WP, Q/WSP, (or Q/WP-Q/WSP Bootcamp) Q/WAD + Security+®, CASP®, Q/WTE)
Q/WAD® Qualified/ Analyst & Defender Class & Exam
Q/ WP® Qualified/ Professional Certification Class & Exam
Q/WSP® Qualified/ Security Professional Certification Class & Exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ Qualified / Qualified Security Professional Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
PMP Project Manager Professional Certification & Exam
Q/WLANPD Qualified/ Local Area Network Planning & Design & Exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing & Exam
Q/WDNO Qualified/ Deceptive Network Optimization & Exam





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: \$3,490
Time: 72 hrs
Contact Hours: 42 hr Lecture 30 hr labs
Learning Level: Basic
Prerequisites: Understanding of TCP/IP Protocols
Credits: 45 CPE / 4 CEU
Instructor: TBD
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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.

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

1. A proven advanced skill set.
 - o Intimate knowledge of the inter-workings of IEEE 802.11 standards
 - o Understanding of the use of common tools found in LAN protocol analyzers
 - o Detailed knowledge of appropriate application of a protocol analyzer
 - o A thorough understanding of LAN troubleshooting from performance and security perspectives
2. A unique and uniquely recognized certification.
 - o The CWAP is the only vendor neutral LAN analysis certification.
 - o 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.
 - o Performance and security analysis to the maximum potential of the available protocol analyzer.
 - o Troubleshooting from various perspectives in a variety of LAN implementations.
 - o Verification of Layer 2, 3 & 7 security solutions during security audits.
 - o 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 23 hrs lecture/ 22 hrs labs:

The following list contains the materials covered in the lecture portion of the course:

Lesson Plan Day 1

2hrs Lecture 0 hr Labs

Physical Layer

- PLCP and PMD Sub-layers
- PLCP header fields and subfields

1hrs Lecture 0hr Labs

DCF Mode

- Interframe Spacing
- Backoff Algorithms
- Frame exchange processes

1hrs Lecture 0hr Labs

PCF Mode

- Media access rules
- Frame exchange processes

MAC frame fields and subfields

1hrs Lecture 1hr Labs

MAC layer addressing

- BSS
- ESS
- WDS

1hrs Lecture 0hr Labs

802.11e topical coverage

1hrs Lecture 1hr Labs

Wired connectivity standards for access points and bridges

- 802.1h
- RFC1042

2hrs Lecture 3hr Labs

Using LAN

protocol analyzers

- Performance analysis
- Security analysis
- Distributed analysis
- Protocol decode analysis
- Site Surveying
- Application Analysis

Lesson Plan Day 2

1hrs Lecture 2hr Labs

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 | • Scalable VPN Solutions |
| • Rogue Hardware & Default Settings | • EAP - Cisco (LEAP) |
| • RF Jamming & Data Flooding | • Layered Security |
| • Information Theft | • Bridging Security |
| • Hijacking and DoS Attacks | • 802.1x and EAP-TTLS |
| • Access Point VPNs | • SSH2 Tunneling & Local Port Redirection |

Class Outline

Lesson Plan 3

1hrs Lecture 1hr Labs
Risk Assessment

- Assets to protect
- Threats to protect against
- Legal protection
- Costs
- Basic security measures
- Threat analysis
- Impact analysis

2hrs Lecture 1hr Labs

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

1hrs Lecture 2hr Labs

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

2hrs Lecture 2hr Labs
Advanced Security Measures

- security policy
- Authentication & encryption
- DMZ and VLANs
- Audits
- Traffic pattern analysis
- Authenticated DHCP

1hrs Lecture 3hr Labs

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
Rogue hardware & default settings
RF Jamming & data flooding

Lesson Plan5

1hrs Lecture 2hr Labs
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

1hrs Lecture 1hr Labs

Prevention & Countermeasures

- 802.1x
- 802.11i
- TKIP
- AES
- Intrusion detection
- US Federal and state laws

1hrs Lecture 0hr Labs

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 practical 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 of Mastery CoM non degree (3 Q/WP® - Q/WP, Q/WSP, (or Q/WP-Q/WSP Bootcamp) Q/WAD + Security+®, CASP®, Q/WTE)
Q/WAD® Qualified/ Analyst & Defender Class & Exam
Q/ WP® Qualified/ Professional Certification Class & Exam
Q/WSP® Qualified/ Security Professional Certification Class & Exam
Q/WAD® Qualified/ Analyst & Defender Practicum
Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ Qualified / Qualified Security Professional Certification Class & Exams
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
PMP Project Manager Professional Certification & Exam
Q/WLANPD Qualified/ Local Area Network Planning & Design & Exam
Q/WLANPD Qualified/ Local Area Network Planning Design Practicum
Q/WNST Qualified/ Network and IoT Security Testing & Exam
Q/WDNO Qualified/ Deceptive Network Optimization & Exam



Q/WP & Q/WSP Qualified/ Professional and Qualified/ Security Professional (144 hours classb)

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 as well as testing for the CWNA™ & CWSP™ Exams.

SU's Qualified Professional & Security Professional Bootcamp course consists of hands on learning using the latest enterprise LAN security and auditing equipment. This 144 hour course bootcamp 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.



With the burgeoning growth of LAN installations, all IT professionals must become knowledgeable about security, security in particular. Q/WSP™ WLAN Security, the preparation course for the CWSP™ certification, teaches students the necessary skills for implementing and managing 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 products from vendors. 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. And 4 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: 64 hr Lecture 68 hr labs
Prerequisites: Understanding of TCP/IP Protocols
Credits: 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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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

- 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 18 hrs lecture/ 22 hrs labs:

12. 1 hrs lecture/ 0 hrs labs

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 enhance 802.11 WLAN

13. 2 hrs lecture/ 1 hrs labs

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. 1 hrs lecture/ 3 hrs labs

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. 1 hrs lecture/ 1 hrs labs

16. 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. 1 hrs lecture/ 1 hrs labs

Power over Ethernet

- 17.1. Recognize the two types of devices used in Power over Ethernet (PoE)
- 17.2. Recognize the differences between the two 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. 1 hrs lecture/ 2 hrs labs

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. 2 hrs lecture/ 3 hrs labs

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. 2 hrs lecture/ 2 hrs labs

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. 2 hrs lecture/ 2 hrs labs

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. 1 hrs lecture/ 2 hrs labs

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. 2 hrs lecture/ 3 hrs labs

Antennas

- 23.1. Antenna characteristics and behaviors

- 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. 2 hrs lecture/ 2 hrs labs

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.

Qualified/ Security Professional

Certification Q/WP002 QUALIFIED/ SECURITY PROFESSIONAL



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 16 hrs lecture/ 24 hrs labs:

All attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 security

- 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

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 3 hrs Lecture 7 hr Labs

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-depth 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 802.1X/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 Framework and implementation discussion in detail
LAB – 802.1X/EAP & VLAN based Security Solutions

Lesson 2 2hrs Lecture 6 hr Labs

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 Wireless Gateways (EWGs)
SOHO/SMB solutions
WLAN Routers

Lesson 3 2hrs Lecture 10 hr Labs

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 3 hrs 7 hr Labs

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

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

ISMS® Lead Auditor Class

ISMS Lead Auditor (72 hours)

The ISO 27001 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: 43 hr Lecture 29 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 6 hrs Lecture 2hr labs

Communication during the audit

Audit Procedures

Drafting of conclusions and non-conformity reports

Lesson 4: Conclude the audit 6 hrs lecture 2 hrs lab

Audit Documentation Review of the Audit Notes

Audit Conclusions

Managing an audit program

The competence and evaluation of auditors

Training Closure

Lesson 5: Examination 8 hrs (5 hrs lecture 3 hrs exam)

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 basic knowledge 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 practical 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, CASP & Security+ , ISMS ISO 27001) Practicals * below
Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class & Exam
Q/NSP® Qualified/ Network Security Policy Administrator & Exam
Q/CA CMMC Cybersecurity Maturity Model Certification class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CISSP® ISC2® Certified Information Security Systems Professional Class & Exam
SU CASP® - CompTIA Advance Security Professional Certification Class & Exam
SU CISA® Certified Information Security Auditor Certification Class & Exam
SU CISM® Certified Information Security Manager Certification Class & Exam
Certified ISO 27001 SU ISMS® Lead Auditor Class & Exam
Certified ISO 27001 SU ISMS® Lead Implementer Certification Class & Exam
SU CMMC Cybersecurity Maturity Model Practicum
PMP Project Manager Professional Certification Class & Exam
SU Q/ISO Qualified/ Chief Information Security Officer Certification Class & Exam

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

Certified ISO 27001 Implementation Class

ISMS Lead Implementer (72 hours)

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 seven-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: 41 hr Lecture 21 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 initiation 14 hr Lecture & labs

Introduction to management systems

Presentation of ISO 27001 and ISO 27002 standards

Fundamental Principles of Information Security

Preliminary analysis

Project management

Lesson 2 : Plan 14 hr Lecture & labs

Governance

Risk analysis

Statement of applicability

Lesson 3 : Do 14 hr Lecture & labs

Document management program

Controls and processes design

Controls implementation Formation, awareness and communication

Incidents management

Lesson 4 : Check, Act and certification audit 14 hr Lecture & labs

Monitoring

Metrics and dashboards

Internal audit

Management review

Continual improvement

Certification audit

Lesson 5 : Practical and Examination 14 hr Lecture & labs

Risk analysis practical

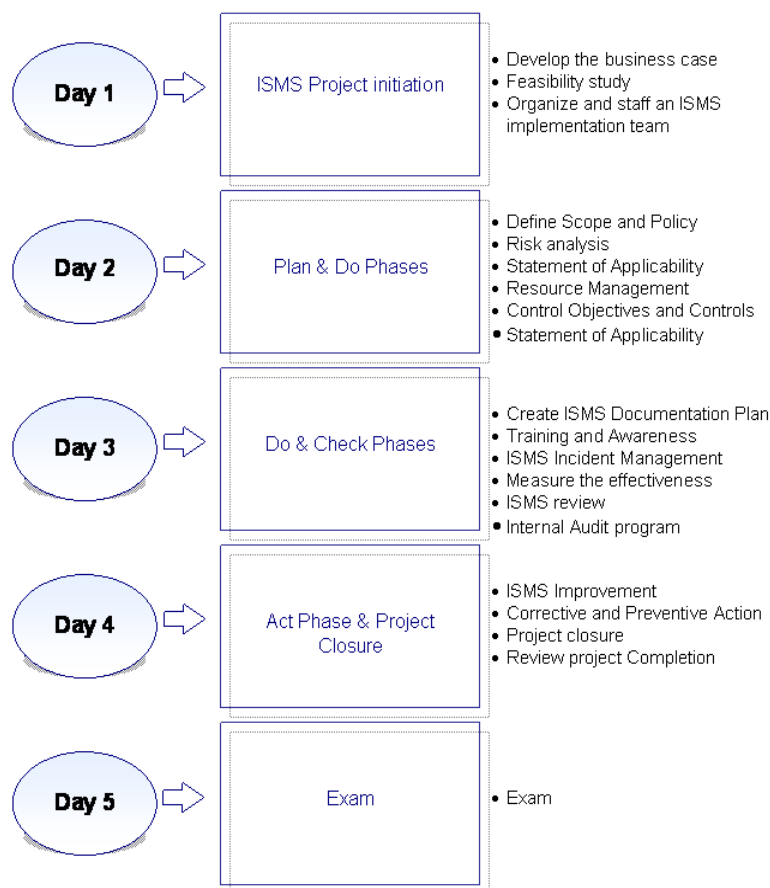
Statement of applicability practical

2 hrs3-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.

Grades -All students must ordinarily take all quizzes, labs, final exam and submit the class practical 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



Q/SSE Qualified/ Software Security Expert Certificate Program of Mastery

Q/SSE® Qualified/ SW Security Expert 72 hour Bootcamp 



SU Q/SSE® Qualified/ Software Security Expert Certification Certificate of Mastery CoM nondegree (9 Q/SSE classes + Security+, CASP)
Q/SSE® Qualified/ Software Security Expert Certification Class & Exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class & Exam
Q/STP® Qualified Software Testing Bootcamp Certification Class & Exam
How to Break & FIX Web Security Certification Class & Exam
How to Break & FIX Software Security Certification Class & Exam
Fundamentals of Secure Software Programming Certification Class & Exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class & Exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class & Exam
Introduction to Reverse Engineering Certification Class & Exam
SU Security+® CompTIA Certification Class & 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 3 part, 72 hour 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: 23 hr Lecture 28 hr labs
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 Practical Fail > 95% Attendance
This 72 hour accelerated class is taught using face to face modality or hybrid 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 *Class handbook, lab, SU resource and 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

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...), ebgoat, Ounce, Foritfy, X Wget, Cyprio 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 24 hrs lecture/ 16 hrs labs

Lesson 1 Part A

Know your Code 8 hrs Lecture 3 hr Labs

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 8 hrs Lecture 5 hr Labs

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 6 hrs Lecture 8 hr Labs

Know your Security Solutions

Lesson 5 C 6 hrs Lecture 8 hr Labs

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 practical 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.





New Rules to Attack Software

This 72 hour hands-on workshop 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 programmers 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 Lecture 32 hr labs
Prerequisites: Understanding of TCP/IP Protocols
Credits: 72 CPE / 3 CEU
Method of Delivery: Residential (100% face-to-face) or Hybrid
Instructor: TBD
Class Materials: SU textbook and testing software
Method of Evaluation: 95 % attendance 100 % completion of Lab
Grading: Pass = Attendance + Labs and Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 ,Ncat , 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 lecture/ 32 hrs labs

Lesson 1 & 2

8 hrs Lecture 5 hr Labs

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

2 hrs Lecture 0 hr Labs 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

2 hrs Lecture 2 hr Labs 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 31 hrs Lecture 5 hr Labs

IV. Software Testing Learn the two most important factors to ensure great testing

2 hrs Lecture 1 hr Labs

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

Lesson 4 3 hrs Lecture 3 hr Labs

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

Lesson 5 1 hrs Lecture 2 hr Labs

UI Area 3 -Stored Data Explore how stored data can become corrupted

Learn how to successfully apply four stored data attacks

1 hrs Lecture 2 hr Labs

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 practical 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 of Mastery CoM nondegree (9 Q/SSE classes + Security+, CASP)
Q/SSE® Qualified/ Software Security Expert 5 Day Bootcamp Certification Class & Exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class & Exam
Q/STP® Qualified Software Testing Bootcamp Certification Class & Exam
How to Break & FIX Web Security Certification Class & Exam
How to Break & FIX Software Security Certification Class & Exam
Fundamentals of Secure Software Programming Certification Class & Exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class & Exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class & Exam
Introduction to Reverse Engineering Certification Class & Exam
SU Security+® CompTIA Certification Class & 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/ST® Qualified/ Software Testing Bootcamp](#) 



This class is unique in the security industry. As a follow on to the class How to Break and FIX Software Security, this 72 hour 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 bootcamp 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 Lecture 32 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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: 40 hrs Lecture 32 hr Labs

Programming 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, Fortify, IDA pro Helix, X Wget, Cyprio 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 40 hrs lecture/ 32 hrs labs

Self Study and Nightly Assignments. Students will need to complete required reading and analyze how specific security issues correspond to their area of testing focus of the application.

Lesson 1 - 32 hrs Lecture & Labs

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 – 40 hrs Lecture 15 hr Labs

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 practical 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 of Mastery CoM nondegree (9 Q/SSE classes + Security+, CASP)
Q/SSE® Qualified/ Software Security Expert Certification Class & Exam
Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class & Exam
Q/STP® Qualified Software Testing Bootcamp Certification Class & Exam
How to Break & FIX Web Security Certification Class & Exam
How to Break & FIX Software Security Certification Class & Exam
Fundamentals of Secure Software Programming Certification Class & Exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class & Exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class & Exam
Introduction to Reverse Engineering Certification Class & Exam
SU Security+® CompTIA Certification Class & 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 & Fix Web Application Security



In this 72 hour 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 Lecture 32 hr labs
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 Practical Fail > 95% Attendance
Text Materials: Class handbook, lab, SU resource CD's and 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 72 hour accelerated class is taught using face to face modality or hybrid 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, 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, Cyprio 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 40 hrs lecture/ 32 hrs labs

Lesson 1

3 hrs Lecture 3 hr Labs

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

3 hrs Lecture 3 hr Labs

Attacking the client

- The need for a rich UI
- Attack 4: Selections outside of ranges
- Attack 5: Client side validation

Lesson 3

3 hrs Lecture 3 hr Labs

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

3 hrs Lecture 3 hr Labs

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 4 & ½ Lesson 5

3 hrs Lecture 3 hr Labs

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

2 hrs Lecture 2 hr Labs

Web Services

- Moving to web services
- Common Attacks
- Constraints on input and output
- Attack 22: web services specific attacks

1 hrs Lecture 1 hr Labs

Privacy

- Who you are, where have you been
- Methods for gathering data

2 hrs Lecture 2 hr Labs

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



This 72 hour hands-on workshop 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 and software tools using real software.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 40 hr Lecture 32 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 40 hrs lecture/ 32 hrs labs

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 10 hrs Lecture 10 hr Labs

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 3 hrs Lecture 7 hr Labs IV. 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 2 hrs Lecture 5 hr Labs

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 5 hrs Lecture 8 hr Labs

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 .5 hr Labs

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 1 hr Labs

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 practical 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)

SU Q/SSE* Qualified/ Software Security Expert Certification Certificate of Mastery CoM
Q/SSE* Qualified/ Software Security Expert Certification Class & Exam

Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class & Exam
Q/STP® Qualified Software Testing Bootcamp Certification Class & Exam
How to Break & FIX Web Security Certification Class & Exam
How to Break & FIX Software Security Certification Class & Exam
Fundamentals of Secure Software Programming Certification Class & Exam
Q/SH/D® Qualified/ Software Hacker / Defender Certification Class & Exam
Q/STBP® Qualified/ Software Tester Best Practices Certification Class & Exam
Introduction to Reverse Engineering Certification Class & Exam
SU Security+® CompTIA Certification Class & 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

FUNDEMENTAS OF SECURE SOFTWARE PROGRAMMING



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: 37 hr Lecture 35 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 40 hrs lecture/ 32 hrs labs

Lesson I Introduction to Software Security -16 hrs Lecture & Labs

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 –Systems 14 hrs Lecture & Labs

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 14 hrs Lecture & Labs

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 14 hrs Lecture & Labs

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 – 14 hrs Lecture & Labs

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 practical 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 



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: 37 hr Lecture 35 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 ,Ncat , 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, Cyprio 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

- 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 Plan 40 hrs lecture/ 32 hrs labs 75 question Online exam last day of class

Lesson 1 and ½ Lesson 2

12 hrs Lecture & Labs

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

12 hrs Lecture & Labs

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

12 hrs Lecture & Labs

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

12 hrs Lecture & Labs

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

12 hrs Lecture & Labs

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.

Grades -All students must ordinarily take all quizzes, labs, final exam, and submit the class practical 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

QUALIFIED/ SOFTWARE SECURITY TESTER BEST PRACTICES



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.

Class Fee: \$3,990
Time: 72 hrs
Learning Level: Entry
Contact Hours: 40 hr Lecture 32 hr labs
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 Practical Fail > 95% Attendance

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

This 72 hour accelerated class is taught using face to face modality or hybrid 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.

KU Outcomes

- * Students will 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 40 hrs lecture/ 32 hrs labs

Lesson 1 & ½ Lesson 2 – 12 hrs Lecture & Labs

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 and 1 /2 Lesson 3 16 hrs Lecture & Labs

II. Methodology

- Security testing roles
- Threat modeling
- Risk assessments
- Security test planning
- Test team organization and management.
- Reporting

Lesson 3 & 4 - 12 hrs Lecture & Labs

III. In-Depth Look at Security Vulnerabilities

each vulnerability will be analyzed for cause, symptoms, prevention and tools to test in software.

1. System-Level

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 4/5 - 12 hrs Lecture & Labs

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



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.

Class Fee: \$3,990
Time: 472 hrs
Learning Level: Intermediate
Contact Hours: 40 hr Lecture 32 hr labs
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 Practical Fail > 95% Attendance
This 72 hour accelerated class is taught using face to face modality or hybrid 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

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

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 40 hrs lecture/ 32 hrs labs

Lesson 1 14 hrs Lecture & Labs

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 14 hrs Lecture & Labs

III. The Reverse Engineers Toolset

Debuggers
Disassemblers
Editors
Utilities
Virtual Machines

Lesson 3 14 hrs Lecture & Labs

IV. Vulnerability analysis and exploitation using reverse engineering techniques

Intro to IDAPro
Using IDA
DA scripts

Lesson 4 14 hrs Lecture & Labs

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 practical 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 14 hrs Lecture & Labs s

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

1 hrs Lecture 0 hr Labs

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/ISP Qualified/ Information Security Professional Certificate of Mastery

Qualified/ Internet Security Awareness Training and Compliance for MGT

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: 39 lecture 24 labs
Prerequisites: None
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 Fail > 95% Attendance

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

This 72 hour accelerated class is taught using face to face modality or hybrid 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:

38hrs Lecture 24 Labs

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.

- 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 practical 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/ISP Qualified/ Information Security Professional Certificate Program of Mastery

Qualified/ Computer Security Awareness Training

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. 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.

Class Fee: \$3,999
Time: 72 hrs
Learning Level: Entry
Contact Hours: 72 hr Lecture
Prerequisites: None
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 + quizzes Fail > 95% Attendance

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 72 hour accelerated class is taught using face to face modality or hybrid 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: 72 *hrs lecture/ 0 hrs labs*

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

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 practical 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/CND Qualified/ Cyber Network Defense Certificate Program of Mastery

IDS I CATCHING THE HACKERS I -Introduction to Intrusion Detection

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 & Exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert & Exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class & Exam
Q/MC® Qualified/ Mission Critical Certification Class & Exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
SU CISSP® Certified Information Security Systems Professional Class & Exam
Linux/UNIX® Security Certification Class & Exam
SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class & Exam
Cloud Computing Security Knowledge Certification (CCSK) Class & Exam
Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam
IDS III: On-site Log Analysis, Event Correlation and Response Practicum

This 72 hour 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, including Cisco, ISS RealSecure, NFR - Network Flight Recorder, SNORT, Tripwire Enterprise (and shareware), SYMANTEC, and more. 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: 37 hr Lecture 35 hr labs
Prerequisites: Basic 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 72 hour accelerated class is taught using face to face modality or hybrid 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

KU 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

2hrs Lecture 0 hr Labs

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

2hrs Lecture 2 hr Labs

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

1hrs Lecture 0 hr Labs

3. Managed /Insourcing vs. Outsourcing Options

2 hrs Lecture 3 hr Labs

4. Implementing IDS

- choosing an intrusion detection system
- host-based and network-based IDS
- key attributes of IDS
- placement determination
- who administers the IDS

4 hrs Lecture 4 hr Labs

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

10. Essential Tools and Resources

11. What You Can Expect in the Future

Cyber threat evasion and threat mitigation 4 hr Labs

Validating the Threats: Hacker Attack Methods

- integrating IDS and firewalls

2 hrs Lecture 0 hr Labs

5. IDS and threat management: staff roles --clearly define responsibilities

- law enforcement contact
- overall coordinator
- documentation
- logging

2 hrs Lecture 2 hr Labs

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

2 hrs Lecture 4 hr Labs

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

- filtering rules
- routing information
- active attacks
- bug exploitation
- buffer overruns
- race condition
- trust exploitation
- denial of service
- social engineering
- physical access

- 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 4 hr Labs **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 practical 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**





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.

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 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 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, 72 hour 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: \$3,995
Time: 72 hrs
Learning Level: Entry
Contact Hours: 27 hr Lecture 35 hr labs
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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. *Labs, SU Pen Testing*

Lesson 1

Role and Operating Characteristics of IDS

2 hr Lecture 1 hr labs

- Identifying major IDS functions
- Defining the role of IDS related to firewalls and other network perimeter security safeguards

1. Choosing an Intrusion Detection System

2 hr Lecture 2 hr labs

- Host-based vs. network-based IDS
- Key attributes for positioning IDS in the network
- Determining who administers the IDS

2. Lesson 2

IDS Architecture

2 hr Lecture 2 hr labs

- Integrating IDS and firewalls
- Sensors
- Collectors
- Management consoles
- IDS in the weeds

3. Lesson 3

IDS Operation

2 hr Lecture 3 hr labs

- 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 2 hr Lecture 2 hr labs

- 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

2 hr Lecture 3 hr labs

- 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

2 hr Lecture 3 hr labs

- 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

3 hr Lecture 3 hr labs

- 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 practical 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 



Q/CND® Qualified/ Cyber Network Defense Certificate of Mastery CoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, CASP or CISSP)
IDS I Catching the Hackers Intro to Intrusion Detection Certification Class & Exam
IDS II Catching the Hackers II: Systems to Defend Networks Cert Class & Exam
IDS III: On-site Log Analysis, Event Correlation and Response Cert Class & Exam
Q/MC® Qualified/ Mission Critical Certification Class & Exam
Q/CDA Qualified/ Cyber Defense Analyst Certification Class & Exam
SU Security+® CompTIA Certification Class & Exam
SU CASP® Certified Advance Security Professional Certification Class & Exam
SU CISSP® Certified Information Security Systems Professional Class & Exam
Linux/UNIX® Security Certification Class & Exam
SU CompTIA CySA+ Cybersecurity Analyst+ Certification Class & Exam
Cloud Computing Security Knowledge Certification (CCSK and CCSK Plus) Class & Exam
Advanced Cloud Security and Applied SecDevOps (CCSK Advanced) Class & Exam
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: 41hr Lecture 31 hr labs
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 72 hour accelerated class is taught using face to face modality or hybrid 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 & Linux 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 ,Ncat , 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: **41 hrs Lecture 31 hr Labs:**

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 6 hrs Lecture 2 hr Labs

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: 3 hrs Lecture 5 hr Labs

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: 4 hrs Lecture 4 hr Labs 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 3 hrs Lecture 5 hr Labs 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-ftp.

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 2 hrs Lecture 6 hr Labs

Webmail on Unix operating system. While vulnerabilities are very uncommon, they tend to bring extreme consequences, both because Webmail I 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 practical 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

MISSION CRITICAL PLANNING

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: \$3,999
Time: 72 hrs
Learning Level: Entry
Contact Hours: 72 hr Lecture
Prerequisites: None
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 Practical 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 72 hour accelerated class is taught using face to face modality or hybrid 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 **42 hrs lecture/ 30 hrs labs:**

Phase I — Establishing Baseline 7hrs Lecture 4 hr Labs

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 7 hrs Lecture 9 hr Labs

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 6hrs Lecture 8 hr Labs

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 practical 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** - No books are required for this course. However, you may want to supplement your preparation.



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 practical's 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 as a Q/ISP Certificate Program of Mastery your not require you to attend SU classes, however you are required to pass all 4 Q/ISP Program exams and develop the 3 practica. The practica "validates" your qualified cybersecurity 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 cybersecurity 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 cybersecurity 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 & Penetration Testing Methods /](#)
- [3. Q/PTL Qualified/ Penetration Tester License](#)
- [4. Q/FE Qualified Forensic Expert](#)
- [5. Q/ND Qualified/ Network Defense](#)



To accomplish this standard, Q/ISP goes beyond theory and terminology and tests the processes and methodology of tactical security skills. A Qualified/ Cybersecurity Professional Certification Program of Mastery (CPoM) 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 Certification 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 cybersecurity 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 20 years and still leading the way for security professionals to validate tactical security skills to reach their career & personal potential.

M. Lynch - Testimonial - 2021

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 cybersecurity 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 cybersecurity 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!



Sondra J. Schneider

Founder & President/ Administrator

Instructor, CISSP, CEH/ Q/EH, ESCA/ Q/SA, Q/PTL, CHFI/ Q/FE, Q/ND, ISO 27001 Lead Auditor.



A 20-year information security industry veteran, Sondra Schneider is the President of SU, an Information Security & Assurance Certification and Training Company. For the past 19 years Sondra has been traveling around the world training network professionals to be network *and* security professionals. In 2006-2007 Sondra worked tirelessly to update the SU 2000 AIS certifications (Advanced Information Security Cert) to the new performance based Q/ISP "hands-on" security certifications for the information & assurance community. The new "Qualified" Q/ISP certification, and related Q/EH, Q/SA-Q/PTL, Q/FE & Q/ND Certifications have been selected to be approved by the DoD 8570 proposal committee in early 2011.

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 works closely with the vendor community to provide information security certification training to comply with the 8570 DoDM mandate.

Ms. Schneider specializes in password and identity management – access, authentication and PKI systems, biometrics, networks and security, network perimeter architecture and security, vulnerability auditing, intrusion detection, and broad band networks. Prior to founding SU, she was a founding partner of the first information security consulting practice located in New York City (since acquired by Price Waterhouse/True Secure) where she developed information security consulting, training & certifications processes for Fortune 500 customers and developed and managed Federal IA/IS consulting projects. Ms. Schneider has been a pioneer in information security technologies since 1992 when she began her career delivering 45 mega bit broadband services along the eastern seaboard for first implementation of the "internet" with MFS DataNet. While with MFS DataNet she was part of the team that built the first "downstream ISP provider" market - AOL, PSI Net & Earthlink etc.

After MFS DataNet was acquired in 1993, she left to pursue a new Internet role at ATT as the first ATT Internet Specialist where she used her MFS Datanet internet skills to create and deliver the first internet sites for ATT. Ms Schneider was tasked with educating large (10M+) ATT client accounts about internet access as a business process tool. And in 1995 she was involved with the first ATT branded firewall (Site Patrol) from BBN to protect corporate networks as they deployed Internet access across closed networks. In 1996, she accepted the Director of Business Development position in the Northeast for the WheelGroup Corporation (since acquired by CISC O in 1997) , where she was responsible for the "introduction and implementation" of the CISC O/ WheelGroup NetRanger intrusion detection and NetSonar network auditing tools product line with large customers and VARs . Capitalizing on her earlier product experience with ATT, she brought real-time intrusion detection systems and tools to financial institutions telcos, healthcare, and Fortune 500 customers.

Kevin Cardwell ([Resume](#)) Instructor, CEH/QEH, ECSA/QSA, CHFI/QFE Q/ISP Director



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 free-lance 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.

**Ken Cutler CISSP, CISM, Dir. Q/ISP**

Sr. Security Instructor & CISSP® Curriculum Manager, Security+, Q/EH, Q/SA

Senior Security Evangelist and Security Curriculum Manager SU

Ken Cutler is Director, Professional Training Classes for SU (SU). His responsibilities include CyberSecurity 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 (Moore McCormack Resources). 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.

David Spivey Instructor Security CSE Q/AAP 2013

David brings over 20 years of security related experience with the last 15 with Cisco in a multitude of different security roles. David brings 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 for 15 years while working full time for CISCO, now Palo Alto networks.

Randy Kholer Instructor Security + Q/EH, CASP 2020

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.

Amy Pflug Instructor Q/AAP

Ms. Pflug has over 18 years of experience in the development and implementation of specialized software. Ms. Pflug was a member of the Key Management Infrastructure (KMI) Working Group. This working group had the task of reexamining DOD existing and evolving approaches for provisioning cryptographic key products and services for military, intelligence, governments, allied, contracting and business customers. This Working Group provided an integrated and focused activity to define the KMI architecture and drive future investment. Ms. Pflug conducts Operational Test and Evaluations (OT&E) based on a OT&E Plan and Procedures document that are written to test each new version of the Certification Authority software for class 4 Public Key Infrastructure (PKI) certificates. This test demonstrated the operational readiness of the Motorola NSM software. NSM software is currently using FORTEZZA® algorithms.

Michael Pender Instructor ISO 27001

(1) 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);

Wanted Sr. QISP Instructor(s)

Sr. Instructors Qualified/ Information Security Professional QISP

this person is a full time employee working in the Northern VA area. Responsibilities are teaching Q/EH Qualified/ Ethical Hacking classes, Q/SA Qualified Security Analyst Penetration Testing, Q/NA Qualified/ Network Defender, and Q/FE Qualified/ Forensic Expert with a Forensic & incident response background.

On Sabbatical: **H. Morrow Long**, CISSP, CEH, CHFI Instructor - Qualified/ Information Security Professional Class (Q/ISP)

H. Morrow Long is Director Qualified/ Information Security Professional (Q/ISP) Classes @ SU. Morrow has been a presenter at (and organizer of) several conferences as well as an instructor at Yale University, Fairfield University, the University of New Haven, Gateway Community Technical College and a number of private training institutes. H. Morrow Long (CISSP, CISM, CEH, Q/EH, Q/SA - Q/PTL, Q/FE, Q/ND) 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 23 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 and over 13 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).

Morrow has taught computer science, networking and information security courses at several Universities (including Yale, the University of New Haven and Fairfield University) and private seminar institutes (including SU). Mr. Long was one of the original participants in the Infragard program in Connecticut. Morrow was on the executive board of CUIISP (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). 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.

Chris Pugrud Instructor Q/CA

Chris is an information security professional with over fifteen years of progressive experience working for Fortune 500 companies and the Federal Government. Chris has expertise in Certification and Accreditation (C&A) work, specifically C&A based on National Institute of Standards and Technology (NIST) guidelines and has taught on this subject matter. Some of the other projects he has completed include Gap Analysis of security infrastructure, security baseline development, firewall/intrusion detection system (IDS) deployment, security assessments, and security awareness training. Chris has supported a wide range of clients that have spanned the globe as well as business sectors including Energy/Power, Healthcare, and Finance/Banking. Most recently, Chris has focused on information security program

development, providing this service to his clients as well as internally within his own organization. Mr. Alward also has experience developing security policies for large organizations.

Glen Strutz Instructor Q/CA,

Mr. Strutz is an information security professional with over ten years of progressive experience working for Fortune 500 companies and the Federal Government. In addition to experience and has continually pursued technical and non-technical industry certifications as appropriate including the CISSP (ISC2). Throughout his career, Glen has supported a wide range of clients that have spanned the globe as well as business sectors including , Healthcare, and Finance/Banking, Energy/Power. Most recently, has focused on information security program development, providing this service to his clients. Glen has expertise in Certification and Accreditation (C&A) work, specifically C&A based on National Institute of Standards and Technology (NIST) guidelines and has taught on this subject matter. Some of the other projects he has completed include Gap Analysis of security infrastructure, security baseline development, firewall/intrusion detection system (IDS) deployment, security assessments, and security awareness training. Glen also has experience developing security policies for large organizations

Char Sample - Advisor

Dr. Char Sample is has over 23 years of experience in the information security industry, and presently works for CERT at Carnegie Mellon University where she supports various cyber efforts. 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.

Gale Pomper - Advisor

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.

Dan Conroy - Advisor CTO UTC

Previous head of Strategy, Planning and Governance Citi

Daniel Conroy was 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. In 2010, he was a speaker at the RSA Conference & delivered a presentation on integrating SEIM with network access control. 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. In 2011 Daniel presented at numerous high-profile conferences & events across the United States such as the FS-ISAC conference in Miami, FL, IT-GRC summit in Boston, MA & IT Roadmap conferences nationwide & is recognized as an expert in his field. Once again, Daniel & his team were finalists in the ISE North America competition. Daniel has been guest lecturer at the Institute of Technology, Tallaght for several years. In April '11, Daniel featured in CIO Digest magazine with an article titled "Preparing & Adapting".

Steve Boddy <http://steve-boddy.strikingly.com/>

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.
