SANS

THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY TRAINING

NETWORK SECURITY 2012

Las Vegas, NV | September 16-24, 2012

Hands-on immersion training programs
taught by the world's highest-rated instructors!

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Advanced Computer Forensic Analysis and Incident Response

Intrusion Detection In-Depth

Security Leadership Essentials for Managers with Knowledge Compression™

Web App Penetration Testing and Ethical Hacking

...and more than 35 other courses in network and
software security, forensics, legal, management, and IT audit.

"SANS, as always, delivers quality training that provides immediate real-world application."

-KEVIN MCLAUGHLIN,
UNIVERSITY OF CINCINNATI

Register at
www.sans.org/network-security-2012

SANS IT Security Training and Your Career Roadmap

SECURITY CURRICULUM

Incident Handling

- **SEC504** Hacker Techniques, Exploits, and Incident Handling — *GCIH*
- **SEC501** Advanced Security Essentials – Enterprise Defender — *GCED*
- **FOR508** Advanced Computer Forensic Analysis & Incident Response — *GCFA* (COURSE RELAUNCH)

Additional Incident Handling Courses
www.sans.org/security-training/curriculums/security

Penetration Testing

Additional Penetration Testing Courses
http://pen-testing.sans.org

- **SEC504** Hacker Techniques, Exploits, and Incident Handling — *GCIH*
- **SEC560** Network Pen Testing and Ethical Hacking — *GPEN*
- **SEC542** Web App Pen Testing and Ethical Hacking — *GWAPT*
- **SEC575** Mobile Device Security and Ethical Hacking (New!)
- **SEC660** Advanced Pen Testing, Exploits, and Ethical Hacking — *GXPN*
- **SEC642** Advanced Web App Pen Testing and Ethical Hacking (New!)
- **SEC617** Wireless Ethical Hacking, Pen Testing, and Defenses — *GAWN*

Beginners

SEC301 NOTE:
If you have experience in the field, please consider our more advanced course - SEC401.

- **SEC301** Intro to Information Security — *GISF*
- **SEC401** SANS Security Essentials Bootcamp Style — *GSEC*

Network Security

- **SEC501** Advanced Security Essentials – Enterprise Defender — *GCED*
- **SEC566** Implementing & Auditing the Twenty Critical Security Controls - In-Depth
- **SEC540** VoIP Security

Additional Network Security Courses
www.sans.org/security-training/curriculums/security

Intrusion Analysis

- **SEC501** Advanced Security Essentials – Enterprise Defender — *GCED*
- **SEC502** Perimeter Protection In-Depth — *GCFW*
- **SEC503** Intrusion Detection In-Depth — *GCIA*

Additional Intrusion Analysis Courses
www.sans.org/security-training/curriculums/security

System Administration

- **SEC501** Advanced Security Essentials – Enterprise Defender — *GCED*
- **SEC505** Securing Windows — *GCWN*
- **SEC579** Virtualization and Private Cloud Security (New!)
- **SEC506** Securing Linux/Unix — *GCUX*
- **SEC540** VoIP Security

Additional System Administration Courses
www.sans.org/security-training/curriculums/security

MANAGEMENT CURRICULUM

- **SEC301** Intro to Information Security — *GISF*
- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ — *GSLC*
- **SEC301** Intro to Information Security — *GISF*
- **SEC401** SANS Security Essentials Bootcamp Style — *GSEC*
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep — *GCPM*
- **MGT414** SANS® +S™ Training Program for the CISSP® Certification Exam — *GISP*

Additional Management Courses
www.sans.org/security-training/curriculums/management

FORENSICS CURRICULUM

- **FOR408** Computer Forensic Investigations - Windows In-Depth — *GCFE*
- **FOR508** Advanced Computer Forensic Analysis & Incident Response — *GCFA* (COURSE RELAUNCH)
- **FOR558** Network Forensics
- **FOR563** Mobile Device Forensics
- **FOR610** REM: Malware Analysis Tools & Techniques — *GREM*

Additional Forensic Courses
http://computer-forensics.sans.org

AUDIT CURRICULUM

- **SEC301** Intro to Information Security — *GISF*
- **SEC401** SANS Security Essentials Bootcamp Style — *GSEC*
- **AUD407** Foundations of Auditing Information Systems
- **AUD507** Auditing Networks, Perimeters, and Systems — *GSNA*
- **AUD566** Implementing & Auditing the Twenty Critical Security Controls – In-Depth

Additional Audit Courses
http://it-audit.sans.org

LEGAL CURRICULUM

- **SEC301** Intro to Information Security — *GISF*
- **SEC401** SANS Security Essentials Bootcamp Style — *GSEC*
- **LEG523** Law of Data Security and Investigations — *GLEG*

GIAC certification available for courses indicated with GIAC acronyms

SOFTWARE SECURITY CURRICULUM

Defense

- **DEV522** Defending Web Applications Security Essentials — *GWEB*

Attack

- **SEC542** Web App Pen Testing and Ethical Hacking — *GWAPT*
- **SEC642** Advanced Web App Pen Testing and Ethical Hacking (New!)

Secure Coding

JAVA
- **DEV541** Secure Coding in Java/JEE (4-Day Course) — *GSSP-JAVA*
- **DEV530** Essential Secure Coding in Java/JEE (2-Day Course)

.NET
- **DEV544** Secure Coding in .NET (4-Day Course) — *GSSP-.NET*
- **DEV532** Essential Secure Coding in ASP.NET (2-Day Course)

C & C++
- **DEV543** Secure Coding in C & C++

PCI
- **DEV536** Secure Coding for PCI Compliance

Additional Software Security Courses
http://software-security.sans.org

Dear Colleague,

I hope you'll join us this fall at the largest training event in our history! **SANS Network Security 2012 will be back at Caesars Palace in Las Vegas, September 16-24.** We return with the best in network security training, certification, and up-to-the-minute research on the most important topics in the industry today. Choose from 45 courses with a great selection from our IT security, pen testing, forensic, audit, appsec, and security management curricula. You'll meet hundreds of like-minded security professionals facing the same challenges and learning together how to implement effective solutions. SANS Network Security is your best annual networking opportunity!

If you are new to SANS Network Security 2012, SANS offers a high-energy program, hands-on labs, a huge *Vendor Solutions Expo*, bonus evening talks on the most timely security challenges, plus a myriad of networking and additional learning opportunities. If you have attended this event in the past, then you know how valuable the experience can be to your career and to the safety and preservation of your company's most critical assets.

At SANS Network Security 2012, you'll get hands-on, immersion training from SANS world-class instructors, and learn what it takes to stop cybercrime for your organization. Included in our lineup are several hot, new courses: Security 575: Mobile Device Security and Ethical Hacking and Security 642: Advanced Web App Penetration Testing and Ethical Hacking (an advanced class after SEC542) along with our new short course, Security 524: Cloud Security Fundamentals. If you have taken SEC401, consider SEC501 a follow on course to SANS Security Essentials with no overlap. Many of these hottest courses will sell out, so register today!

Not only can you select a job-based, full course to meet your training needs, but you can also select a short, skill-based course to maximize your training investment. You can start the week with a one-day security management course (which can help you better communicate security needs to management), and end the week with one of ten two-day courses that will fit with your longer course and intensify your training.

As an added value, don't miss *SANS @Night* presentations, evening talks with keynote speakers, and a variety of Vendor events. SANS Network Security 2012 *Vendor Expo* is being held on September 18-19, and provides a look at vendor products and solutions that can help address your organization's key security issues. In addition, we will be featuring *Lunch & Learn* sessions and *Cocktail Briefs* throughout this event. And don't forget *NetWars – Tournament Play* with Ed Skoudis. NetWars is a collection of computer and network security challenges designed to represent real-world security issues, their flaws, and their resolutions. Normally priced at $999, NetWars is free with any paid five- or six-day course at SANS Network Security 2012. NetWars' relevance to current security challenges makes it one of our most popular evening offerings. It was a big hit at SANS 2012 with a long waitlist, so don't miss the chance to secure your seat!

This industry changes daily, attacks continue making the national news, and you are facing increasingly complex challenges. If you have pen testers, forensics experts, and application and software developers on your staff, get them to come to Las Vegas. They will bring back tools and knowledge to defend your organization from the threats that really matter. SANS is the most trusted source for information security training, so why go anywhere else? Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office.

Can't make it to Network Security this year? You can still be part of the action! Students who register for a Simulcast course will attend remotely by logging into a virtual classroom and joining the live class. See page 72 for details.

It is our goal to help you get the most out of your SANS Network Security 2012 experience. If you have suggestions on how we can better help you find the information you need, then I would love to hear from you, **Stephen@sans.edu**.

See you in Las Vegas!

Stephen Northcutt
President
The SANS Technology Institute, a postgraduate computer security college

Stephen Northcutt

Here is what a few of last year's attendees had to say:

"I can't believe how much I'm learning – I've got a laundry list of things I'll be implementing as soon as I'm back in the office."
-James Hancock, Fickewirth & Associates

"I feel much more prepared to defend my network."
-Greg Toussaint, ITT Corporation

"Absolutely fantastic course. The instructor delivered a top-class explanation. The best class I have taken in 15+ years of my working life."
-Sarveshwar Rao, Alcatel-Lucent

Courses-at-a-Glance

Please check the website for an up-to-date course list at www.sans.org/network-security-2012

		SUN 9/16	MON 9/17	TUE 9/18	WED 9/19	THU 9/20	FRI 9/21	SAT 9/22	SUN 9/23	MON 9/24
AUD407	Foundations of Auditing Information Systems		PAGE 60							
AUD507	Auditing Networks, Perimeters & Systems		PAGE 62							
AUD521	Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant								PAGE 67	
DEV522	Defending Web Applications Security Essentials		PAGE 64							
DEV541	Secure Coding in Java/JEE: Developing Defensible Applications		PAGE 65							
DEV544	Secure Coding in .NET: Developing Defensible Applications		PAGE 65							
FOR408	Computer Forensic Investigations - Windows In-Depth		PAGE 46							
FOR508	Advanced Computer Forensic Analysis & Incident Response		PAGE 48							
FOR563	Mobile Device Forensics		PAGE 50							
FOR610	REM: Malware Analysis Tools and Techniques		PAGE 52							
LEG523	Law of Data Security and Investigations		PAGE 9							
MGT305	Technical Communication and Presentation Skills for Security Pros	P 68								
MGT414	SANS® +S™ Training Program for the CISSP® Cert Exam SIMULCAST		PAGE 54							
MGT433	Securing The Human: Building and Deploying an Effective Security Awareness Program SIMULCAST								PAGE 68	
MGT442	Information Security Risk Management								PAGE 68	
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™		PAGE 56							
MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep		PAGE 58							
SEC301	Intro to Information Security		PAGE 10							
SEC401	SANS Security Essentials Bootcamp Style SIMULCAST		PAGE 12							
SEC501	Advanced Security Essentials – Enterprise Defender		PAGE 14							
SEC502	Perimeter Protection In-Depth		PAGE 16							
SEC503	Intrusion Detection In-Depth		PAGE 18							
SEC504	Hacker Techniques, Exploits, and Incident Handling		PAGE 20							
SEC505	Securing Windows SIMULCAST		PAGE 22							
SEC506	Securing Linux/Unix		PAGE 24							
SEC509	Securing Oracle Databases		PAGE 26							
SEC524	Cloud Security Fundamentals *NEW!*								PAGE 66	
SEC540	VoIP Security		PAGE 28							
SEC542	Web App Penetration Testing and Ethical Hacking		PAGE 30							
SEC546	IPv6 Essentials								PAGE 67	
SEC560	Network Penetration Testing and Ethical Hacking		PAGE 32							
SEC566	Implementing & Auditing the 20 Critical Security Controls - In-Depth SIMULCAST		PAGE 34							
SEC575	Mobile Device Security and Ethical Hacking *NEW!*		PAGE 36							
SEC579	Virtualization and Private Cloud Security *NEW!*		PAGE 38							
SEC580	Metasploit Kung Fu for Enterprise Pen Testing								PAGE 66	
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses		PAGE 40							
SEC642	Advanced Web App Penetration Testing and Ethical Hacking *NEW!*		PAGE 42							
SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking		PAGE 44							
SEC710	Advanced Exploit Development								PAGE 67	
HOSTED	(ISC)²® CSSLP® CBK® Education Program		PAGE 69							
HOSTED	RMF for DoD IT Workshop		PAGE 70							
HOSTED	Physical Penetration Testing - Introduction								PAGE 71	
HOSTED	Offensive Countermeasures: Defensive Tactics That Actually Work								PAGE 71	
HOSTED	Advanced Vulnerability Scanning Techniques Using Nessus								PAGE 71	
	NetWars – Tournament Play					PAGE 6				

SANS Network Security 2012

SANS @Night Evening Talks

Attend these free talks as an added benefit to your training experience.

Linux Forensics for Non-Linux Folks *Hal Pomeranz*

Many forensic analysts approach analysis of Linux systems with fear and trepidation because the platform is unfamiliar and has a reputation for complexity. In many ways, however, forensic analysis of Linux systems is easier than other platforms because most of the data is in plain text formats and simple tools suffice for many investigations. This session will demonstrate where many of the important forensic artifacts are stored on a Linux system and suggest strategies for analyzing their contents.

Information Assurance Metrics: Practical Steps to Measurement *James Tarala*

Show up to a security presentation, walk away with a specific action plan. In this presentation, James Tarala, a senior instructor with the SANS Institute, will be presenting on making specific plans for information assurance metrics in an organization. Clearly, this is an industry buzzword at the moment when you listen to presentations on the 20 Critical Controls, NIST guidance, or industry banter. Security professionals have to know that their executives are discussing the idea. So exactly how do you integrate information assurance metrics into action in an organization and actually achieve value from the effort? Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, students will have a start integrating metrics into their information assurance program.

Everything They Told Me About Security Was Wrong *John Strand*

If you were to believe the vendors and the trade shows, you would think everything was "OK" with IT security. You would think AV works. You would think "plug and play" IDS was effective. You would think that Data Loss Prevention would prevent data loss. Why, then, is it that very large organizations are still getting compromised? Organizations with very large budgets and staff still get compromised in advanced and persistent ways. Something is very wrong in this industry.

Let's find out what is wrong and how we can fix it.

In this presentation we will have multiple live demonstrations including: hacking a Mac, and hacking a Linux system and bypassing AV. However, the most important thing about this presentation is that we will cover how we need to change our defensive mindset. After all, if information security was easy it would not take six days to cover the essentials.

New Legal Methods for Collecting and Authenticating Cyber Investigation Evidence *Ben Wright*

The source of evidence for digital investigations is changing. Previously digital evidence was extracted from a piece of hardware in the possession of the investigator, such as a hard drive or the flash memory on a smartphone. Now the evidence is on the web (Facebook!) or in the cloud (Google Docs!), and often the only practical way to access it is to capture what the investigator ascertains through a client such as a browser. Mr. Wright will share thoughts on how to capture and preserve cyber evidence.

Intrusion Detection is Dead *Dr. Johannes Ullrich*

Intrusion Detection Systems are still widely operated in a "black list mode," meaning that signatures and anomaly detection modules are searching vast amounts of traffic for known bad activity. The current threat landscape, however, doesn't provide us with the luxury of easy identifiable well-known exploits. Instead, we are hunting covert channels in standard protocols like HTTP that are hard to parse and identify. This talk will present an alternate approach to Intrusion Detection: Network Traffic Whitelisting.

Windows Exploratory Surgery with Process Hacker *Jason Fossen*

In this talk we'll rummage around inside the guts of Windows while on the lookout for malware, using a free tool named Process Hacker (similar to Process Explorer). Understanding processes, threads, drivers, handles and other OS internals is important for analyzing malware, doing forensics, troubleshooting, and hardening the OS. If you have a laptop, get Process Hacker from SourceForge.net and together we'll take a peek under the GUI to learn about Windows internals and how to use Process Hacker for combating malware.

Evolving Threats *Paul Henry*

For nearly two decades defenders have fallen into the "Crowd Mentality Trap" and have simply settled on doing the same thing everyone else was doing. While at the same time attackers have clearly evolved both in terms of malware delivery vectors and attack methodology. Today our defenses focus primarily on the gateway and upon attempting to outwit attackers delivery methods. This leaves us woefully exposed and, according to a recent Data Breach Report, has resulted in 3,765 incidents, 806 million records exposed and $157 billion (USD) in data-breach costs in only the past 6 years.

Visit www.sans.org/network-security-2012/night.php for additional events.

Malware Analysis Essentials using REMnux *Lenny Zeltser*

Though some tasks for analyzing Windows malware are best performed on Windows laboratory systems, there is a lot you can do on Linux with the help of free and powerful tools. REMnux is an Ubuntu distribution that incorporates many such utilities. This practical session presents some of the most useful REMnux tools. Lenny Zeltser, who teaches SANS' reverse-engineering malware course, will share how you can use the utilities installed on REMnux. If you haven't experimented with Linux-based tools for malware analysis, you've been missing out. And if you've been meaning to begin exploring the field of malware analysis, this talk will help you get started.

What's New in Windows 8 and Server 2012? *Jason Fossen*

Windows 8 and Server 2012 are major new releases, and the stakes for Microsoft are huge. Windows 8 is more than just a new touch-oriented graphical interface, it's a new direction for Microsoft as a whole. Come join the author of the Securing Windows course at SANS (SEC505) for an overview of the most important changes, especially for security, such as Windows on ARM tablets, booting from USB flash drives, Microsoft Account integration, secure boot with UEFI firmware, Metro Internet Explorer, picture password logon, and more. Will Windows 8 make or break Microsoft? Will iPad and Android fall before the Windows 8 juggernaut? Come and see!

The SANS360: The Security Crystal Ball *Rob Lee, Moderator*

10 Speakers - 10 Presentations - 360 Seconds Each

SANS is known for its density of talented professionals in the field of Information Security, Penetration Testing, Auditing, and Digital Forensics and Incident Response. SANS Network Security 2012 faculty brings you the SANS360: The Security Crystal Ball, focusing on predictions for information security of tomorrow and into the next several years. Learn the thoughts from many of the leading experts in the community as they each share their ideas on what we will be dealing with in the future.

SANS Network Security 2012

Vendor Expo

September 18, 2012 | 12:00pm - 1:30pm and 5:00pm - 7:00pm
September 19, 2012 | 12:00pm - 1:30pm

Given that virtually everything in security is accomplished with a tool, exposure to those tools is a very important part of the SANS Training Event learning experience. Leading solutions providers will be on hand for a two-day vendor expo, an added bonus to registered training event attendees.

Vendor-Sponsored Lunch Sessions

September 18, 2012 | 12:00pm - 1:30pm

Join these sponsoring vendors and others on the expo floor for an introduction to leading solutions and services that showcase the best options in information security.

Vendor Welcome Reception

September 18, 2012 | 5:00pm - 7:00pm

This informal reception allows you to visit exhibits and participate in some exciting activities. This is a great time to mingle with your peers and experience first-hand the latest in information security tools and solutions with interactive demonstrations. Enjoy appetizers and beverages while comparing experiences with other attendees regarding the solutions they are using to address security threats in their organization. Attendees can visit sponsors to receive raffle tickets and enter to win exciting prizes. Prize drawings occur throughout the expo.

Vendor-Sponsored Lunch & Learn Presentations

Throughout SANS 2012, vendors will provide sponsored lunch presentations where attendees can interact with peers and receive education on vendor solutions. Take a break and get up-to-date on security technologies!

For dates, times and complete information please visit www.sans.org/network-security-2012/vendor.php

How Are You Protecting Your

- **Data**
- **Network**
- **Systems**
- **Critical Infrastructure**

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, audit, and management.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

Learn more about GIAC and how to *Get Certified* at **www.giac.org**

Department of Defense

Come to SANS and take the training with the highest pass rate on 8570 required certifications.

www.sans.org/8570

DoD Baseline IA Certifications

IAT Level I	IAT Level II	IAT Level III
A+-CE	**GSEC**	**GCIH**
Network+CE	Security+CE	**GSE**
SSCP	SSCP	CISA
		CISSP (or Associate)

IAM Level I	IAM Level II	IAM Level III
GISF	**GSLC**	**GSLC**
GSLC	CAP	CISM
CAP	CISM	**CISSP** (or Associate)
Security+CE	**CISSP** (or Associate)	

IASAE I	IASAE II	IASAE III
CISSP (or Associate)	**CISSP** (or Associate)	CISSP - ISSEP
		CISSP - ISSAP

CNDSP Analyst	CNDSP Infrastructure Support
GCIA	SSCP
GCIH	CEH
CEH	

CNDSP Incident Responder	CNDSP Infrastructure Support
GCIH	**GSNA**
CSIH	CSIA
CEH	CEH

CNDSP Incident Responder
CISSP - ISSMP
CISM

SANS Training Courses for DoD Approved Certifications

SANS TRAINING COURSE	DoD APPROVED CERT
SEC301: Intro to Information Security	GISF
SEC401: SANS Security Essentials Bootcamp Style	GSEC
SEC503: Intrusion Detection In-Depth	GCIA
SEC504: Hacker Techniques, Exploits & Incident Handling	GCIH
AUD507: Auditing Networks, Perimeters and Systems	GSNA
MGT414: SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512: SANS Security Essentials for Managers with Knowledge Compression™	GSLC

DoD 8570 certification requirements are subject to change, please visit http://iase.disa.mil/eta/iawip for the most updated version.

For more information, contact us at 8570@sans.org or visit www.sans.org/8570

NETWARS

A True Hands-On Interactive Security Challenge!

NetWars is a computer and network security challenge designed to test participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals.

- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing

The NetWars competition will be played over two evenings: September 20-21. Prizes will be awarded at the conclusion of the games. REGISTRATION IS LIMITED AND IS FREE for students attending any long course at SANS Network Security 2012 *(NON-STUDENTS ENTRANCE FEE IS $999)*.

Register at www.sans.org/network-security-2012

How NetWars Works

At the outset of the challenge, each player must find hidden keys within a special image downloaded from the Internet and then use those keys to enter an online environment where knowledge of security vulnerabilities, their exploits, and their associated defenses can be turned into points.

NetWars has five separate levels, so players may quickly advance through earlier levels to their level of expertise. The entire challenge involves all five levels.

Levels:

1) **Played on CD image (Lin or Win), no superuser privs granted**
2) **Played on CD image (Lin or Win) with superuser**

3) **Played across the Internet, attacking DMZ**
4) **Played across the Internet, attacking internal network from DMZ**

5) **Played across the Internet, attacking other player's castles and defending your own**

Scoring

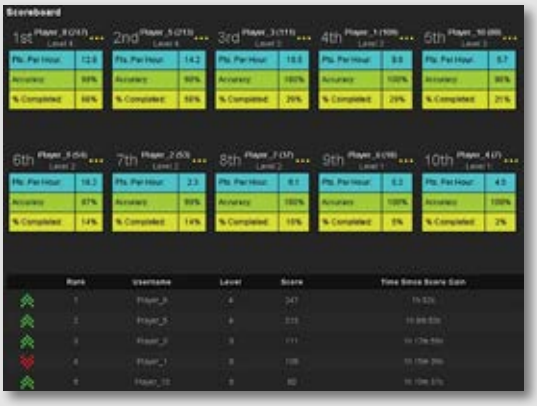
A comprehensive score card is generated for each player at the conclusion of the NetWars challenge. This detailed assessment illustrates the areas where participants have demonstrated skills and highlights other areas where skills can be refined or built.

Scoreboard

- Scoreboard shows progress in real-time
- Great challenge at-a-glance view, depicting:
  - Challenges conquered
  - Territory still available
  - Momentum and rank
  - Time since last score

Scoreboard Stats

- Scoreboard animation reveals other player stats
  - Accuracy
  - Speed
  - Percentage complete ***(Rank and momentum always remain on the screen)***



Benefits for Individuals

If you are a self-motivated security professional who really wants to put your knowledge to the test, then NetWars is an excellent opportunity for you to have fun and learn in a competition with other security professionals, practicing real world tactics that could happen at any time.

- **The detailed score card is an incomparable opportunity for you to analyze your security knowledge and decide in what other areas you would like to learn new skills or refine your existing ones.**
- **Demonstrate your experience to other security professionals.**
- **Stay on top of the latest attacks and see what your competition is doing.**
- **Participants that reach level three of NetWars will be eligible to receive 12 CMU credits towards GIAC certification renewal.**

Benefits for Organizations

How would your security team handle a real attack? Do they have the right skills and knowledge to defend vital systems? The NetWars simulation lets you see how your organization would react during an attack, but without the consequences.

- **Test the experience and skills of your current security team and assess areas where further training is needed.**
- **Evaluate the experience of potential new hires.**
- **Use the score card to create a customized training program for your security personnel.**

What's Your Next Career Move?

The information security field is growing and maturing rapidly; are you positioned to win?
A Master's Degree in Information Security from the SANS Technology Institute
will help you build knowledge and skills in management or technical engineering.

STI offers two master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

STI Cohort 2012-02 starts at Network Security 2012.
Enroll by August 15, 2012 to be eligible for a scholarship of up to 30% of your first year's tuition.

"The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience - you walk out of every class with skills you can use immediately."

-Courtney Imbert, MSISE Student

Please join us for a special graduation ceremony Friday, September 21, 2012.

22 of the courses being offered at SANS Network Security 2012 may be applied towards an STI Master's Degree.

SANS TECHNOLOGY INSTITUTE
KNOWLEDGE FOR PEACE
SCIENTIA PRO PACE

www.sans.edu
info@sans.edu
720.941.4932

Legal 523

Law of Data Security and Investigations

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop NOT Required • Instructor: Benjamin Wright

New laws regarding privacy, e-discovery, and data security are creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. The professional training needed to accomplish this is uniquely available in SANS' LEG523 series of courses, which is designed to build skills in the analysis and use of contracts, policies, and records management procedures.

Earning the GLEG certification for LEG523 demonstrates to employers that a professional has not only attended classes, but studied and absorbed the sophisticated content of these courses. Certification distinguishes any professional, whether an IT expert, an auditor, a paralegal, or a lawyer, and the value of certification will grow in the years to come as law and security issues become even more interlocked.

Legal 523 covers the law of business, contracts, fraud, crime, IT security, IT liability and IT policy – all with a focus on electronically stored and transmitted records. The course also teaches investigators how to prepare credible, defensible reports, whether for cyber, forensics, incident response, human resources or other investigations. LEG523 is a five-day package delivering the content of the following one-day courses:

- **Fundamentals of IT Security Law and Policy**
- **E-records, E-discovery, and Business Law**
- **Contracting for Data Security and Other Technology**
- **The Law of IT Compliance: How to Conduct Investigations**
  - *Lessons will be invaluable to the proper execution of any kind of internal investigation.*
- **Applying Law to Emerging Dangers: Cyber Defense**
  - *In-depth review of legal response to the major security breach at TJX.*
  - *Learn how to incorporate effective public communications into your cyber security program.*

Recent updates to the courses address hot topics such as risk, investigations and business records retention connected with cloud computing, and social networks like Facebook and Twitter. Updates also teach students how to analyze and respond to the risks and opportunities surrounding OSINT (open source intelligence gathering).

This course adopts an increasingly global perspective. Non-US professionals attend the Legal-523 course because there is no training like it anywhere else in the world.

Who Should Attend:

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology Managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy Officers

What Students Are Saying

"There is no other course like this. Many eye-opening revelations about the ever changing landscape for information security legal risks."

-Bill Ardern, Mecklenburg County

From the Author

These are five intense days covering the rapid development of law at the intersection of IT and security. Be prepared for insights and tips you've not heard before. -Ben Wright

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Security 301

Intro to Information Security

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop NOT Required • Instructor: Fred Kerby

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, SEC301 rocks!

We begin by covering basic terminology and concepts and then move to the basics of computers and networking, discussing Internet Protocol, routing Domain Name Service, and network devices. We cover the basics of cryptography and wireless networking; then we look at policy as a tool to effect change in your organization. In the final day of the course, we put it all together with an introduction to defense in depth.

If you're a newcomer to the field of information security, this is the course for you! You will develop the skills to bridge the gap that often exists between managers and system administrators and learn to communicate effectively with personnel in all departments and at all levels within your organization.

This is the course SANS offers for the professional just starting out in security. If you have experience in the field, please consider our more advanced offerings, such as SEC401: SANS Security Essentials Bootcamp Style.

Who Should Attend:

- Persons new to information technology (IT) who need to understand the basics of information assurance, computer networking, cryptography, and risk evaluation
- Managers and information security officers who need a basic understanding of risk management and the tradeoffs between confidentiality, integrity, and availability
- Managers, administrators, and auditors who need to draft, update, implement, or enforce policy

From the Author

A good friend of mine once said, "A little security is better than no security." If your organization is in either situation (little or no security) and you want to make a difference in a positive way, this course is a great place to start. If your organization has already made an investment in security, this is a great opportunity to compare notes with others and identify how to maximize the return on your investment. Twelve years ago I agreed to fill the position of "number one spear catcher" (the head security guy) for our organization. I asked about training and my predecessor told me that the agency would provide training, but suggested that I work for six months to get some "real-world experience to compare against the theory." It was a long and frustrating six months and the training was less than helpful. A few years later when SANS offered to let me help write and teach this course, I literally jumped at the opportunity. Every time I teach it, I'm excited and I enjoy it as much as the attendees. It's been very gratifying. - Fred Kerby

GIAC Certification
www.giac.org

DoD 8570 Required
www.sans.org/8570

What Students Are Saying

"This class is great for IT professionals looking for their first step towards security awareness. I have been in IT for 17 years and I learned a lot on this first day of class."

-Paul Beninati, EMC

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

301.1 A Framework for Information Security

Information security is based upon foundational concepts such as asset value, the CIA triad (confidentiality, integrity, and availability), principal of least privilege, access control, and separation. Day one provides a solid understanding of the terms, concepts, and tradeoffs that will enable you to work effectively within the information security landscape. If you have been in security for a while, these chapters will be a refresher, providing new perspectives on some familiar issues.

Topics: Basic Concepts (Value of Assets, Security Responsibilities, IA Pillars and Enablers, IA Challenges, Trust and Security); Principles (Least Privilege, Defense in Depth, Separation of Risk, Kerckhoff's Principle); Security as a Process (Analysis, Protection, Detection, Response)

301.2 Securing the Infrastructure

To appreciate the risks associated with being connected to the Internet one must have a basic understanding of how networks function. Day two covers the basics of networking (including a review of some sample network designs), including encapsulation, hardware and network addresses, name resolution, and address translation. We explore some typical attacks against the networking and computing infrastructure along with appropriate countermeasures.

Topics: Terms (Encapsulation, Ports, Protocols, Addresses, Network Reference Models - stacks); Addressing (Hardware, Network, Resolution, Transport Protocols, TCP, UDP); Other Protocols (ARP, ICMP, Routing Basics, The Local Network, Default Gateway); Network Components (Hubs, Switches, Routers, Firewalls, Component Management - SNMP); Attacks and Countermeasures (Attack Theory, Types of Attacks, Countermeasures)

301.3 Cryptography and Security in the Enterprise

Cryptography can be used to solve a number of security problems. Cryptography and Security in the Enterprise provides an in-depth introduction to a complex tool, (cryptography) using easy to understand examples and avoiding complicated mathematics. Attendees will gain meaningful insights into the benefits of cryptography (along with the pitfalls of a poor implementation of good tools). The day continues with an overview of the security organization in a typical company. Where does security fit in the overall organizational scheme? What is its charter? What other components of the larger organization must it interact with? We conclude the day with a whirlwind overview of wireless networking technology benefits and risks, including a roadmap for reducing risks in a wireless environment.

Topics: Cryptography (Cryptosystem Components, Cryptographic Services, Algorithms, Keys, Cryptographic Applications, Implementation); Security in the Enterprise (Organizational Placement, Making Security Possible, Dealing with Technology, Security Perspectives, Organizational Relationships, Building a Security Program); Wireless Network Security (Wireless Use and Deployments, Wireless Architecture and Protocols, Common Misconceptions, Top 4 Security Risks, Steps to Planning a Secure WLAN)

301.4 Information Security Policy

Day four will empower those with the responsibility for creating, assessing, approving, or implementing security policy with the tools and techniques to develop effective, enforceable, policy. Information Security Policy demonstrates how to bring policy alive by using tools and techniques such as the formidable OODA (Orient, Observe, Decide, Act) model. We also explore risk assessment and management guidelines and sample policies, as well as examples of policy and perimeter assessments.

Topics: The OODA Model; Security Awareness; Risk Management Policy for Security Officers; Developing Security Policy; Assessing Security Policy; Applying What We Have Learned on the Perimeter; Perimeter Policy Assessment

301.5 Defense In-Depth: Lessons Learned

The goal of day five is to enable managers, administrators, and those in the middle to strike a balance between "security" and "getting the job done." We'll explore how risk management deals with more than security and how the ISO-OSI model may have an eighth layer (political) impacting communications and transmission. It is replete with war stories from the trenches that illustrate the TSP protocol (the Tie to Sandal Protocol) used by successful security professionals worldwide.

Topics: The Site Security Plan; Computer Security; Application Security; Incident Handling; Making the Most of Your Opportunities with Others; Measuring Progress

SANS Senior Instructor

Fred Kerby

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than sixteen years. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security. A frequent speaker at SANS, Fred's presentations reflect his opinions and are not the opinions of the Department of the Navy.

"The course was very valuable in helping me better understand how to secure my company's network."

- Brett Cassidy, Mission Solutions Engineering

Security 401

SANS Security Essentials Bootcamp Style

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required • Instructor: Dr. Eric Cole

Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

Who Should Attend:

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Anyone new to information security with some background in information systems and networking

What Students Are Saying

"The quick pace is awesome! Moving forward and actively covering topics is invigorating!"

-Steven Park, Boeing

SPECIAL NOTE: This course is endorsed by the Committee on National Security Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).

Test your security knowledge with our SANS Security Essentials Assessment Test. Get your free test at **https://portal.sans.org/assessments**

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 72.***

Bootcamp

This program has extended hours.
Security 401 PARTICIPANTS ONLY
Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

Attendance is required for the evening bootcamp sessions as the information presented appears on the GIAC exams. These daily bootcamps give you the opportunity to apply the knowledge gained throughout the course in an instructor-led environment. It helps fill your toolbox with valuable tools you can use to solve problems when you go back to work. The material covered is based on Dr. Eric Cole's "Cookbook for Geeks," and most students find it to be one of the highlights of their Security Essentials experience! Students will have the opportunity to install, configure, and use the tools and techniques they have learned. CDs containing the software required will be provided for each student. Students should arrive with a laptop properly configured. A working knowledge of each operating system is recommended but not required. For students who do not wish to build a dual boot machine, SANS will provide a bootable Linux CD for the Linux exercises.

From the Author

One of the things I love to hear from students after teaching Security 401 is "I have worked in security for many years and after taking this course I realized how much I did not know." With the latest version of Security Essentials and the Bootcamp, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After attending Security 401, I am confident you will walk away with solutions to problems you have had for a while plus solutions to problems you did not even know you had.
-Eric Cole

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

401.1 Hands On: Networking Concepts

Day one teaches you how networks, routers, firewalls, and the related protocols like TCP/IP work so you'll be better prepared to determine hostile traffic and have a foundation for the succeeding days' training.

Topics: Network Fundamentals; IP Concepts; IP Behavior, IOS and Router Filters; Physical Security; Bootcamp

401.2 Hands On: Defense In-Depth

Day two covers security threats and their impact, including information warfare. It also covers sound security policies and password management tools, the six steps of incident handling, and web server security testing.

Topics: Defense in Depth; Security Policy and Contingency Planning; Access Control and Password Management; Incident Response; Information Warfare; Web Communications and Security; Bootcamp

401.3 Hands On: Internet Security Technologies

Day three gives you a roadmap that will help you understand the tools and options available for deploying systems for defense.

Topics: Attack Strategies and Mitigation; Vulnerability Scanning; Intrusion Detection Technologies; Intrusion Prevention Technologies; IT Risk Management; Bootcamp

401.4 Hands On: Secure Communications

Day four covers encryption, wireless security, and operations security.

Topics: Encryption 101; Encryption 102; Applying Cryptography; Wireless Network Security; VoIP; Operations Security; Bootcamp

401.5 Hands On: Windows Security

Day five is all about securing the current batch of Windows operating systems (Windows XP/2003/Vista/2008/Windows 7) and teaches the tools that simplify and automate the process.

Topics: Windows Security Infrastructure; Permissions and User Rights; Security Templates and Group Policy; Service Packs, Hotfixes, and Backups; Securing Windows Network Services; Automation and Auditing; Bootcamp

401.6 Hands On: Linux Security

Based on industry consensus standards, this course provides step-by-step guidance on improving the security of any Linux system. The course combines practical how-to instructions with background information for Linux beginners and security advice and best practices for administrators of all levels of expertise.

Topics: Linux Landscape; Linux Command Line; Linux OS Security; Linux Security Tools; Maintenance, Monitoring, and Auditing Linux

Security Essentials is our most popular training program and requires that you attend the evening bootcamp sessions with hands-on exercises. These extended hours really help to fill in the gaps in your information security knowledge. Everyone, except truly seasoned hands-on information security workers, can benefit from SANS Security Essentials Bootcamp Style. A GSEC Certification can add 6-9% to your bottom line salary.

SANS Faculty Fellow

Dr. Eric Cole

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Dr. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware, Hiding in Plain Site, Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting in which he provides state of the art security services and expert witness work. He also served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS faculty Fellow and course author.

Security 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Bryce Galbraith

Cyber security will continue to increase in importance as attacks become stealthier, have a greater financial impact on an organization, and cause reputational damage. While Security Essentials lays a solid foundation for the security practitioner, there is only so much that can be packed into a six-day course. SEC501 is a follow up to SEC401: SANS Security Essentials Bootcamp Style (with no overlap) and continues to focus on more technical areas needed to protect an organization. The course focus is on:

- **Prevention** - configuring a system or network correctly
- **Detection** - identifying that a breach has occurred at the system or network level
- **Reaction** - responding to an incident and moving to evidence collection/forensics

A key theme is that prevention is ideal, but detection is a must. We have to ensure that we constantly improve security to prevent as many attacks as possible. Attacks will continue to pose a threat to an organization as data becomes more portable and networks continue to be porous. Therefore a key focus needs to be on data protection both internally and externally - securing our critical information whether it resides on a server, in a robust network architecture, or on a portable device.

Despite our best effort at preventing attacks and protecting critical data, some attacks will still be successful. Therefore we need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic flowing on your networks and looking for indication of an attack. It also includes performing penetration testing and vulnerability analysis against an organization to identify problems and issues before a compromise occurs.

Finally, once an attack has been detected, we must react in a timely fashion and perform forensics. By understanding how the attacker broke in, this can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Who Should Attend:

- **Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401**
- **People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want a broad, advanced coverage of the core areas to protect their systems**
- **Anyone looking for detailed technical knowledge on how to protect against, detect, and react to the new threats that will continue to cause harm to an organization**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

From the Author

It is always a thrill after I finish teaching SEC401 to see students leave with a fire in their eyes and an excitement about them. They walked into class feeling overwhelmed that security is a lost cause, but now they leave class understanding what they need to do and have a focus and drive to do the right thing to secure their organizations. However the next question we receive on a constant basis is, what course should I take next? How do I continue my journey? Well, it depends on what your focus area is. Do you want to get more into perimeter protection, IDS, operating system security, etc? The challenge is that many students have positions that do not allow them to focus on one area — they need to understand all of the key areas across security. What students are telling us is that they want a Security Essentials part 2 or a 500-level continuation of Security Essentials covering the next level of technical knowledge. In Security 501, SANS has decided to give students just what they have been asking for, and I am beyond thrilled with the results. We have identified core foundation areas that compliment SEC401 with no overlap and continue to build a solid security foundation for network practitioners.

This is illustrated by one student who after a recent class ran up to me, gave me a big hug (he was a retired football player, so I did not argue), and said, "SANS is awesome. I have been frustrated in my job for over a year and had lost hope that you really could secure an organization and that anything I did made a difference. Just as my light of hope was burning out, I decided to take the Security Essentials course, figuring it was a lost cause. After this class the fire is burning brighter than it ever was. I feel like a kid again and cannot wait to go back to my company and make a difference. However, I think my boss is scared because I called him eight times throughout the week, telling him all of the great information and practical knowledge I learned."

After teaching thousands of students, I am confident you will have similar results and be just as excited. However, just for reference, hugs are optional. -Eric Cole

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

501.1 Hands On: Defensive Network Infrastructure

Protecting a network from attack starts with designing, building, and implementing a robust network infrastructure. Many aspects to implementing a defense-in-depth network are often overlooked since companies focus on functionality. Achieving the proper balance between business drivers and core protection of information is difficult. On the first day students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

Topics: Introducing Network Infrastructure as Targets for Attack; Implementing the Cisco Gold Standard to Improve Security; Advanced Layer 2 and 3 Controls

501.2 Hands On: Packet Analysis

Packet analysis and intrusion detection are at the core of timely detection. Detecting attacks is becoming more difficult as attacks become stealthier and more difficult to find. Only by understanding the core principles of traffic analysis can one become a skilled analyst and distinguish normal traffic from attack traffic. Security professionals must be able to detect new, advanced zero-day attacks before they compromise a network. Prevention, detection, and reaction must all be closely knit so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can continue to operate.

Topics: Architecture Design & Preparing Filters; Detection Techniques and Measures; Advanced IP Packet Analysis; Intrusion Detection Tools

501.3 Hands On: Pentest

An organization must understand the changing threat landscape and compare that against its own vulnerabilities. On day three students will understand the variety of tests that can be run and how to perform penetration testing in an effective manner. Students will learn about external and internal pen testing and the methods of black, gray, and white box testing. Penetration testing is critical to identify an organization's exposure points, but students will also learn how to prioritize and fix these vulnerabilities to increase the overall security of an organization.

Topics: Variety of Penetration Testing Methods; Vulnerability Analysis; Key Tools and Techniques; Basic Pen Testing; Advanced Pen Testing

501.4 Hands On: First Responder

Any organization connected to the Internet or with employees is going to have attacks launched against it. Security professionals need to understand how to perform incident response, analyze what is occurring, and restore their organization back to a normal state as soon as possible. Day four will equip students with a proven six-step process to follow in response to an attack – prepare, identify, contain, eradicate, recover, and learn from previous incidents. Students will learn how to perform forensic investigation and find indication of an attack. This information will be fed into the incident response process and ensure the attack is prevented from occurring again in the future.

Topics: Incident Handling Process and Analysis; Forensics and Incident Response

501.5 Hands On: Malware

As security professionals continue to build more proactive security measures, attackers' methods will continue to evolve. A common way for attackers to target, control, and break into as many systems as possible is through the use of malware. Therefore it is critical that students understand what type of malware is currently available to attackers and future trends and methods of exploiting systems. With this knowledge students can then learn how to analyze, defend, and detect malware on systems and minimize the impact to the organization.

Topics: Malware; Microsoft Malware; External Tools and Analysis

501.6 Hands On: Data Loss Prevention

Cyber security is all about managing, controlling, and mitigating risk to critical assets, which in almost every organization are composed of data or information. Perimeters are still important, but we are moving away from a fortress model and moving towards a focus on data. This is based on the fact that information no longer solely resides on servers where properly configured access control lists can limit access and protect our information; it can now be copied to laptops and plugged into networks. Data must be protected no matter where it resides.

Topics: Risk Management; Data Classification; Digital Rights Management; Data Loss Prevention (DLP)

SANS Certified Instructor

Bryce Galbraith

As a contributing author of the internationally bestselling book Hacking Exposed: Network Security Secrets & Solutions, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he and his team provide specialized vulnerability assessment and penetration testing services for clients. He teaches several of The SANS Institute's most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, he speaks at numerous conferences, and holds several security certifications and blogs about security issues at http://blog.layeredsec.com.

Security 502

Perimeter Protection In-Depth

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Seth Misenar

There is no single fix for securing your network. That's why this course is a comprehensive analysis of a wide breadth of technologies. This is probably the most diverse course in the SANS catalog, as mastery of multiple security techniques is required to defend your network from remote attacks. You cannot just focus on a single OS or security appliance. A proper security posture comprises multiple layers. This course was developed to give you the knowledge and tools necessary at every layer to ensure your network is secure.

The course starts by looking at common problems: Is there traffic passing by my firewall I didn't expect? How did my system get compromised when no one can connect to it from the Internet? Is there a better solution than anti-virus for controlling malware? We'll answer these questions and more.

We all know how to assign an IP address, but to secure your network you really need to understand the idiosyncrasies of the protocol. We'll talk about how IP works and how to spot the abnormal patterns. If you can't hear yourself saying "Hummm, there are no TCP options in that packet. It's probably forged," then you'll gain some real insight from this portion of the material.

Once you have an understanding of the complexities of IP, we'll get into how to control it on the wire. We focus on the underlying technology used by all of the projects rather than telling you which ones are good and which ones are bad. A side-by-side product comparison is only useful for that specific moment in time. By gaining knowledge of what goes on under the cover, you will be empowered to make good product choices for years to come. Just because two firewalls are stateful inspection, do they really work the same on the wire? Is there really any difference between stateful inspection and network-based intrusion prevention, or is it just marketing? These are the types of questions we address in this portion of the course.

We move on to a proper, wire-level assessment of a potential product as well as what options and features are available. We'll even get into how to deploy traffic control while avoiding some of the most common mistakes. Feel like your firewall is generating too many daily entries for you to review the logs effectively? We'll address this problem not by reducing the amount of critical data, but by streamlining and automating the back-end process of evaluating it.

Who Should Attend:

- Information security officers
- Intrusion analysts
- IT managers
- Network architects
- Network security engineers
- Network and system administrators
- Security managers
- Security analysts
- Security architects
- Security auditors

What Students Are Saying

"The course is valuable because it allows me to assess the defense in-depth tools being used in my organization with the latest industry standards and best practices."

-Stephanie Clark, Military Sealift Command

But you can't do it all on the wire. A properly layered defense needs to include each individual host – not just the hosts exposed to access from the Internet, but hosts that have any kind of direct or indirect Internet communication capability as well. We'll start with OS lockdown techniques and move on to third-party tools that can permit you to do anything from sandbox insecure applications to full-blown application policy enforcement.

Most significantly, I've developed this course material using the following guiding principles: learn the process, not just one specific product; you learn more by doing, so hands-on problem-solving is key; and always peel back the layers and identify the root cause. While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem solving and root cause analysis. While these are usually considered soft skills, they are vital to being an effective security architect. So along with the technical training, you'll receive risk management capabilities and even a bit of Zen empowerment.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

502.1 TCP/IP for Firewalls

This first section is more than an executive overview as we dig down into the bits and bytes of the problem. What can be secured at the network level, and which protection needs to be pushed back to the hosts? What are my packet level control devices really doing on the wire, and when can't I trust them? If you want to control traffic on the wire, you have to understand the IP protocol. It is for this reason a majority of the day is spent doing packet level analysis. While many protocol analyzers will tell you what they think is happening, if you cannot read the decodes for yourself, you will have no idea when the tool is leading you astray.

Topics: Common Threats; Windump/Tcpdump; OSI Layer 2; OSI Layer 3; Fragmentation; OSI Layer 4 through 6; IP Version 6 (IPv6)

502.2 Hands On: Firewalls, NIDS, and NIPS

The only way to understand if a network traffic control device is going to meet your requirements is to understand the technology underneath the hood. Do all stateful inspection firewalls handle traffic the same way? Is there really any difference between a stateful inspection firewall and a network-based intrusion prevention system (NIPS)? In today's material we will cut through the vendor marketing slicks and look at what their products are really capable of doing.

Topics: Static Packet Filters; Stateful Packet Filters; Stateful Inspection Filtering; Intrusion Detection and Prevention; Proxies; Cisco IOS

502.3 Hands On: Wire Products and Assessment

In today's material we will look at how each vendor has implemented the technology. We'll also discuss how to test these products on the wire so we know exactly how they are impacting traffic. Can the product stop a covert communication channel using ICMP error packets? What about a source route attack? These are the types of questions we'll strive to answer in this material. The number one problem students have with managing their environment is dealing with the firewall logs. Not only will we discuss what to look for, but through practical exercises you will learn how to optimize the log review process into something that takes less time to finish than your morning coffee.

Topics: Commercial Traffic Control Products; Open Source Traffic Control Products; Building A Firewall Rulebase; Perimeter Assessment; Firewall Log Analysis

502.4 Hands On: Host Level Security

In the early days of the Internet it was possible to secure a network right at the perimeter. Modern-day attacks, however, are far more advanced and require a multi-layered approach to security. This does not mean the perimeter no longer serves a useful role; it's just that now it is only part of the equation. So today we focus on the security posture of our individual hosts, look at what the OS vendors give us to work with and when we may need to turn to third-party tools. It is not enough to simply configure the hosts. We'll look at vulnerability scanning and audits in order to be able to validate continuous integrity. When the worst occurs, we'll talk about performing a forensic analysis as well. Finally, we will talk about security information management. The devices on your network really want to tell you what is going on, but you have to be able to sort through all of the data. We'll look at options for both daily reports as well as real-time alerting.

Topics: Securing Hosts and Services; Host-Based Intrusion Detection and Prevention; Vulnerability Assessment and Auditing; Forensics; Security Information Management

502.5 Hands On: Securing the Wire

It's not enough to control traffic flow; we also need to be able to secure the data inside of the packets. We will start with the basics, authentication and encryption, and learn how these technologies are combined into the modern day VPN. We'll discuss which of the technologies have been proved to be mathematically secure and which of them is a leap of faith. Further, we will discuss how to integrate encrypted dataflow into your overall architecture design so you are not blinded to attacks through these encrypted tunnels. Then we turn our attention to securing the internal network structure. We'll cover deploying wireless access points without creating (yet another) point of management. We'll also look at network access control (NAC) and discuss what it can do today as well as its potential in the future.

Topics: Authentication; Encryption; VPNs, Wireless; Network Access Control

502.6 Hands On: Perimeter Wrap-Up

The problems start off easy, like small organizations that need advice in order to make their environment more secure. The complexity quickly escalates to where you need to combine security, functionality, and political issues into the design. A healthy dose of risk assessment is also thrown in for good measure. You will also perform a series of labs that are hostile in nature. A majority of the previous labs were geared towards problem solving. You will be presented with a security issue and then given a hands-on process for resolving it.

Topics: Sizing Up A Network; Cool Tools

SANS Certified Instructor

Seth Misenar

Seth Misenar is a certified SANS instructor and also serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including SEC401, SEC504, and SEC542. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute.

Security 503

Intrusion Detection In-Depth

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Mike Poor

Learn practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This challenging track methodically progresses from understanding the theory of TCP/IP, examining packets, using Snort to analyze traffic, becoming familiar with the tools and techniques for traffic and intrusion analysis, to reinforcing what you've learned with a hands-on challenge of investigating an incident. Students should be able to "hit the ground running" once returning to a live environment where traffic analysis it required.

This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP (see **www.sans.org/conference/tcpip_quiz.php**) in order to fully understand the topics that will be discussed. Although others may benefit from this course, it is most appropriate for students who are or who will become intrusion detection/prevention analysts. Students generally range from novices with some TCP/IP background all the way to seasoned analysts. The challenging hands-on exercises are specially designed to be valuable for all experience levels. We strongly recommend that you spend some time getting familiar with tcpdump before coming to class.

Who Should Attend:

- Intrusion detection analysts (all levels)
- Network engineers
- System, security, and network administrators
- Hands-on security managers

What Students Are Saying

"This class heightens your security awareness on protecting your network and provides excellent examples, in detail, on how to accomplish this."

-Laura Freeman, DND

From the Author

When I was invited to be a member of a computer incident response team in the late 1990's (just after Al Gore invented the Internet), there was no formal cybersecurity training available. Consequently, I learned on the job and made my share, and then some, of mistakes. I was so naive that I tried to report an attack on our network by a host with an IP address in the 192.168 reserved private network, available for use by anyone. Needless to say, I got a very embarrassing enlightenment when someone clued me in.

With the benefit of experience and the passage of time, there are many lessons to be shared with you. This knowledge affords you the opportunity to learn and practice in the classroom to prepare you for the fast-paced always-interesting job of intrusion detection analysts.

-Judy Novak

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

503.1 TCP/IP for Intrusion Detection

Students will be able to translate native hexadecimal at the IP, transport layers, and some protocols such as DNS. The material presented in this day will give students the knowledge and understanding of TCP/IP and free tools, like tcpdump and wireshark, to assist them in troubleshooting all types of networking complaints from routing problems to firewall and critical server issues.

Topics: Refresher of TCP/IP; TCP/IP Communication Model; IP Fragmentation; Internet Control Message Protocol (ICMP); Stimulus and Response; Microsoft Protocols; Domain Name System (DNS); IPv6

503.2 & 503.3 Hands On – Parts 1 & 2: Network Traffic Analysis Using TCPdump*

In this two-day module, students will learn how to interpret header fields and values in a packet. We will build on that skill to learn traffic analysis with lab exercises to reinforce the theory. Tcpdump is the tool of choice selected to demonstrate the theory and is used in hands-on exercises. The intent of these days is to provide the foundation to enable the analyst perform packet/traffic interpretation.

Topics: Introduction to Tcpdump; Writing Tcpdump Filters; Tcpdump Filters; Examining Datagram Fields with Tcpdump; Analysis of Tcpdump Output; Advanced Analysis; Application Protocols and Detection; SiLK

503.4 Hands On: Intrusion Detection Snort Style*

On day four students will install, configure, and use the powerful and versatile freeware intrusion detection system Snort. In addition, they will learn to customize Snort for many special uses. Hands-on exercises that will challenge both the novice and seasoned Snort user are included so that students will feel confident in their ability to effectively utilize Snort for their site's specific needs when they get back to the office.

Topics: Introduction; Modes of Operation; Writing Snort Rules; Configuring Snort as an IDS; Output Analysis; Advanced Topics Hands-On - Part 1

503.5 Hands On: Intrusion Analysis*

This day starts to bring together the knowledge gained on previous days to help the student become a combat-ready analyst. Students will learn how to assess and prioritize the events generated by an IDS/IPS, including how to correlate events across multiple platforms and operating environments. Next students will participate in analyzing network traffic, including performing network traffic forensic analysis.

Topics: Analyst Toolkit; Wireshark; SiLK: Network Traffic Forensics; Network Architecture for Monitoring; Correlation

503.6 Hands On: IDS Challenge*

This day is the culmination and consummation of all the previous days where students use their knowledge for a hands-on exercise to investigate an actual attack. This challenge is a guided approach to discovering the network architecture, profiling traffic, identifying attacks, analyzing possible compromises, characterizing the enemy, tracking the hacker's activities, and correlation. This engaging activity allows students to work as a team, or individually, to reinforce what they've learned and challenges them to think analytically.

*This course is available to Security 503 participants only.

SANS Senior Instructor

Mike Poor

Mike is a founder and senior security analyst for the DC firm InGuardians, Inc. In the past he has worked for Sourcefire as a research engineer and for SANS leading their intrusion analysis team. As a consultant Mike conducts incident response, breach analysis, penetration tests, vulnerability assessments, security audits, and architecture reviews. His primary job focus, however, is in intrusion detection, response, and mitigation. Mike currently holds the GCIA certification and is an expert in network engineering and systems and network and web administration. Mike is an author of the international best selling *Snort* series of books from Syngress, a member of the Honeynet Project, and a handler for the SANS Internet Storm Center.

Security 504

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: John Strand

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

Who Should Attend:

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

What Students Are Saying

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."

-Joshua Anthony, West Virginia Army National Guard

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

It is imperative that you get written permission from the proper authority in your organization before using these tools and techniques on your company's system and also that you advise your network and computer operations teams of your testing.

From the Author

My favorite part of teaching Hacker Techniques, Exploits, and Incident Handling is watching students when they finally get it. It's usually a two-stage process. First, students begin to realize how truly malicious some of these attacks are. Some students have a very visceral reaction, occasionally shouting out "Oh, shoot!" when they see what the bad guys are really up to. But if I stopped the process at that point, I'd be doing a disservice. The second stage is even more fun. Later in the class, students gradually realize that, even though the attacks are really nasty, they can prevent, detect, and respond to them. Using the knowledge they gain in this track, they know they'll be ready when a bad guy launches an attack against their systems. And being ready to thwart the bad guys is what it's all about. -Ed Skoudis

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

504.1 Incident Handling Step-by-Step and Computer Crime Investigation

This session describes a detailed incident handling process and applies that process to several in-the-trenches case studies. Additionally, in the evening an optional 'Intro to Linux' mini-workshop will be held. This session provides introductory Linux skills you'll need to participate in exercises throughout the rest of SEC504. If you are new to Linux, attending this evening session is crucial.

Topics: Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record Keeping; Incident Follow-Up

504.2 Hands On – Part 1: Computer and Network Hacker Exploits*

It is imperative that system administrators and security professionals know how to control what outsiders can see. Students who take this class and master the material can expect to learn the skills to identify potential targets and be provided tools they need to test their systems effectively for vulnerabilities. This day covers the first two steps of many hacker attacks: reconnaissance and scanning.

Topics: Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools

504.3 Hands On – Part 2: Computer and Network Hacker Exploits*

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course covers the third step of many hacker attacks – gaining access. For each attack, the course explains vulnerability categories, how various tools exploit holes, and how to harden systems or applications against each type of attack. Students who sign an ethics and release form are issued a CD-ROM containing the attack tools examined in class.

Topics: Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Netcat: The Attacker's Best Friend; Hands-on Exercises with a List of Tools

504.4 Hands On – Part 3: Computer and Network Hacker Exploits*

Attackers aren't resting on their laurels, and neither can we. They are increasingly targeting our operating systems and applications with ever-more clever and vicious attacks. This session looks at increasingly popular attack avenues as well as the plague of denial of service attacks.

Topics: Password Cracking; Web Application Attacks; Denial of Service Attacks; Hands-on Exercises with a List of Tools

504.5 Hands On – Part 4: Computer and Network Hacker Exploits*

Once intruders have gained access into a system, they want to keep that access by preventing pesky system administrators and security personnel from detecting their presence. To defend against these attacks, you need to understand how attackers manipulate systems to discover the sometimes-subtle hints associated with system compromise. This course arms you with the understanding and tools you need to defend against attackers maintaining access and covering their tracks.

Topics: Maintaining Access; Covering the Courses; Five Methods for Implementing Kernel-Mode RootKits on Windows and Linux; the Rise of Combo Malware; Detecting Backdoors; Hidden File Detection; Log Editing; Covert Channels; Sample Scenarios

504.6 Hands On: Hacker Tools Workshop*

In this workshop you'll apply skills gained throughout the week in penetrating various target hosts while playing Capture the Flag. Your instructor will act as your personal hacking coach, providing hints as you progress through the game and challenging you to break into the laboratory computers to help underscore the lessons learned throughout the week. For your own attacker laptop, do not have any sensitive data stored on the system. SANS is not responsible for your system if someone in the class attacks it in the workshop. Bring the right equipment and prepare it in advance to maximize what you'll learn and the fun you'll have doing it.

Topics: Capture the Flag Contest; Hands-on Analysis; General Exploits; Other Attack Tools and Techniques

*This course is available to Security 504 participants only.

SANS Senior Instructor

John Strand

John Strand is a senior instructor with the SANS Institute. He teaches SEC504: Hacker Techniques, Exploits, and Incident Handling; SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464 and the co-author for SEC580. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing.

Security 505

Securing Windows

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

Will you be transitioning from Windows XP to Windows 7? The SEC505: Securing Windows course is fully updated for Windows Server 2008-R2 and Windows 7. Most of the content applies to Windows Server 2003 and XP too, but the focus is on 2008/Vista/7.

Concerned about the 20 Critical Security Controls of the Consensus Audit Guidelines? This course will help you implement , not just audit, the critical controls relevant to Windows systems and will also walk you through most of the tools step by step, too.

As a Windows security expert, how can you stand out from the crowd and offer management more than the usual apply-this-checklist advice? Be a security architect who understands the big picture. You can save your organization money, maintain compliance with regulations, secure your networks, and advance your career all at the same time. How? By leveraging the Windows infrastructure you've already paid for.

This program is a comprehensive set of courses for Windows security architects and administrators. It tackles tough problems like Active Directory forest design, how to use Group Policy to lock down desktops, deploying a Microsoft PKI and smart cards, pushing firewall and IPSec policies out to every computer in the domain, securing public IIS web servers, and PowerShell scripting.

PowerShell is the future of Windows scripting and automation. Easier to learn and more powerful than VBScript, PowerShell is an essential tool for automation and scalable management. If there is one skill that will most benefit the career of a Windows specialist, it's scripting. Most of your competition lacks scripting skills, so it's a great way to make your resume stand out. Scripting skills are also essential for being able to implement the 20 Critical Security Controls.

You are encouraged to bring a virtual machine running Windows Server 2008 Enterprise Edition configured as a domain controller, but this is not a requirement for attendance since the instructor will demo everything discussed on-screen. You can get a free evaluation version of Server 2008 from Microsoft's website (just do a Google search on "site:microsoft.com Server 2008 trial"). You can use VMware, Virtual PC, or any other virtual machine software.

This is a fun and fascinating course, a real eye-opener even for Windows administrators with years of experience. Come see why there's a lot more to Windows security than just applying patches and changing passwords; come see why a Windows network needs a security architect.

Who Should Attend:

- Windows network security engineers and architects
- Windows administrators with security duties
- Anyone with Windows machines who wants to implement the SANS 20 Critical Security Controls
- Active Directory designers and administrators
- Those who must enforce security policies on Windows hosts
- Those deploying or managing a PKI or smart cards
- IIS administrators and webmasters with web servers at risk
- Administrators who use the command line or scripting to automate their duties and must learn PowerShell (the replacement for CMD scripting and VBScript)

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 72.*

From the Author

I've happily been with SANS for over a decade, and the courses I write are always guided by two questions: 1) What do administrators need to know to secure their networks? and 2) What should administrators learn to advance their careers as IT professionals? I'm not a Microsoft employee or a Microsoft-basher, so you won't get either kind of propaganda here; my concern is with the health of your network and your career. As a security consultant I've seen it all (good, bad, and ugly), and my experience goes into the manuals I write for SANS and the stories I tell in seminars. The Securing Windows course is packed with interesting and useful advice that is hard or impossible to find on the Internet. We always have a good time, so I hope to meet you at the next training event! -Jason Fossen

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/
cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

505.1 Hands On: Securing Active Directory and DNS

On day one, we will quickly get you on top of what you need to know about Active Directory security and delegation of authority. Importantly, this course is not an introduction to AD or an overview of basic administration topics. This is a course for people who already manage AD, need to plan a redeployment, or must lock down what they've got.

Topics: Securing Domain Controllers; Active Directory Access Control Lists; Delegation of Authority; Forest Designs; Secure Dynamic DNS

505.2 Hands On: Enforcing Critical Controls With Group Policy

In this course, we'll see how to use Group Policy to lock down desktops and servers, implement many of the SANS 20 Critical Controls, enforce regulatory compliance changes, configure services and applications, and scale our work out to thousands of systems conveniently. If you've never seen Group Policy before, you're in for a shock (a good shock!) and if you've been using Group Policy for years, this course should expand your understanding even more since the emphasis is on security, not Group Policy in general.

Topics: Security Templates; What is Group Policy?; Fine-Tuning Group Policy; Updating Vulnerable Software; Pushing Out Scripts; Enforcing Critical Controls

505.3 Hands On: Windows PKI, EFS, and BitLocker

Planning a PKI or data encryption project isn't easy, and mistakes and redeployments can be costly, so this day is designed in part to assist in the planning process to help avoid these mistakes. If you're not encrypting laptops and portable drives now, you will be soon, and BitLocker/EFS can save your organization money while making the deployment relatively easy. Using Group Policy, you can manage most features of BitLocker and EFS on all your machines without having to configure each of them by hand.

Topics: Why Must I Have A PKI?; How To Install The Windows PKI; How To Manage Your PKI; Deploying Smart Cards; Encrypting File System; BitLocker Drive Encryption

505.4 Hands On: Windows Firewall, IPSec, Wireless, and VPNs

Day four is about how to use the Windows Firewall, IPSec, RADIUS, the RRAS VPN gateway service, and WPA2 for 802.11 wireless to secure the network layer in our Windows environments. Virtually all these client settings, including wireless settings, are manageable through Group Policy.

Topics: The New Windows Firewall; Why Use IPSec?; Creating IPSec Policies; RADIUS for Network Security; Virtual Private Networking; Securing Wireless Networks

505.5 Hands On: Securing IIS 7.5

The demand for IIS security personnel is great because IIS is so widely deployed. This course focuses on IIS 7.5 in Windows Server 2008-R2, but many of the principles discussed will apply to earlier versions of IIS as well. If you're new to IIS, this course will get you up to speed.

Topics: Server Hardening; XML Configuration System; IIS Authentication and Authorization; Web-Based Applications; Logging and Auditing; FTP Over SSL (FTPS)

505.6 Hands On: Windows PowerShell

You don't have to bring a laptop to attend the course, but if you do, get the latest version of PowerShell from Microsoft (**www.microsoft.com/powershell**). A CD-ROM will be handed out by the instructor with sample scripts and other files with which to experiment. During the course, we will walk through all the essentials of PowerShell together. The course presumes nothing, you don't have to have any prior scripting experience to attend. And, most importantly, be prepared to have fun: PowerShell is just plain cooooooool.

Topics: What is PowerShell?; Cmdlets; Running Scripts; Namespace Providers; Piping Objects; Parameter Binding; Regular Expressions; Functions and Filters; The .NET Class Library; Using Properties and Methods at the Command Line; Accessing COM Objects: WMI, ADSI, ADO, etc.; Security and Execution Policy; And lots and lots of sample scripts to walk through...

SANS Faculty Fellow

Jason Fossen

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS' week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401.5), and has been involved in numerous other SANS' projects since 1998. He graduated from the University of Virginia, received his master's degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas. Jason blogs about Windows Security Issues on the SANS Windows Security Blog. http://blogs.sans.org/windows-security

What Students Are Saying

"The course introduced a wide range of technologies and issues I was completely unaware of- great exposure to new ideas. Jason's depth of knowledge and examples are of great value."

-Jeff Ruff, AASKI Technologies

Security 506

Securing Linux/Unix

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Hal Pomeranz

Experience in-depth coverage of Linux and Unix security issues. Examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. This course provides specific configuration guidance and practical, real-world examples, tips, and tricks.

Throughout this course you will become skilled at utilizing freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS' practical approach with hands-on exercises every day ensures that you can start using these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

Who Should Attend:

- Security professionals looking to learn the basics of securing Unix operating systems
- Experienced administrators looking for in-depth descriptions of attacks on Unix systems and how they can be prevented
- Administrators needing information on how to secure common Internet applications on the Unix platform
- Auditors, incident responders, and InfoSec analysts who need greater visibility into Linux and Unix security tools, procedures, and best practices

A Sampling of Topics:

- **Memory Attacks, Buffer Overflows**
- **File System Attacks, Race Conditions**
- **Trojan Horse Programs and Rootkits**
- **Monitoring and Alerting Tools**
- **Unix Logging and Kernel-Level Auditing**
- **Building a centralized logging infrastructure**
- **Network Security Tools**
- **SSH for Secure Administration**
- **Server "lockdown" for Linux and Unix**
- **Controlling root access with sudo**
- **SELinux and chroot() for application security**
- **DNSSEC deployment and automation**
- **mod_security and Web Application Firewalls**
- **Secure Configuration of BIND, Sendmail, Apache**
- **Forensic Investigation**

What Students Are Saying

"It sparked my interest to get a deeper understanding of how to secure my systems at work and at home. Hal's experience as a forensics examiner is of great interest and a definite plus. Great experience."

- Tim Horne, Honeywell Aerospace

From the Author

A wise man once said, "How are you going to learn anything if you know everything already?" And yet there seems to be a quiet arrogance in the Unix community that we've figured out all of our security problems, as if to say, "Been there, done that." All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In fifteen plus years on the job, what I've learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students that say things like, "I've been using Unix for 20 years, and I still learned a lot in this class." That's really rewarding.
-Hal Pomeranz

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

506.1 Hands On – Part 1: Hardening Linux/Unix Systems

This course tackles some of the most important techniques for protecting your Linux/Unix systems from external attacks. But it also covers what those attacks are so that you know what you're defending against. This is a full-disclosure course with in-class demos of actual exploits and hands-on exercises to experiment with various examples of malicious software, as well as different techniques for protecting Linux/Unix systems.

Topics: Memory Attacks and Overflows; Vulnerability Minimization; Boot-Time Configuration; Encrypted Access; Host-Based Firewalls

506.2 Hands On – Part 2: Hardening Linux/Unix Systems

Continuing our exploration of Linux/Unix security issues, this course focuses in on local exploits and access control issues. What do attackers do once they gain access to your systems? How can you detect their presence? How do you protect against attackers with physical access to your systems? What can you do to protect against mistakes (or malicious activity) by your own users?

Topics: Rootkits and Malicious Software; File Integrity Assessment; Physical Attacks and Defenses; User Access Controls; Root Access Control With Sudo; Warning Banners; Kernel Tuning For Security

506.3 Hands On – Part 3: Hardening Linux/Unix Systems

Monitoring your systems is critical for maintaining a secure environment. This course digs into the different logging and monitoring tools available in Linux/Unix, and looks at additional tools for creating a centralized monitoring infrastructure such as Syslog-NG. Along the way, the course introduces a number of useful SSH tips and tricks for automating tasks and tunneling different network protocols in a secure fashion.

Topics: Automating Tasks With SSH; AIDE Via SSH; Linux/Unix Logging Overview; SSH Tunneling; Centralized Logging With Syslog-NG

506.4 Hands On – Part 1: Application Security

This course examines common application security tools and techniques. The SCP-Only Shell will be presented as an example of using an application under chroot() restriction, and as a more secure alternative to file sharing protocols like anonymous FTP. The SELinux application whitelisting mechanism will be examined in depth. Tips for troubleshooting common SELinux problems will be covered and students will learn how to craft new SELinux policies from scratch for new and locally developed applications. Significant hands-on time will be provided for students to practice these concepts.

Topics: chroot() for Application Security; The SCP-Only Shell; SELinux Basics; SELinux and the Reference Policy; Application Security Challenge Exercise

506.5 Hands On – Part 2: Application Security

This course is a full day of in-depth analysis on how to manage some of the most popular application level services securely on a Linux/Unix platform. We will tackle the practical issues involved with securing the three of the most commonly used Internet servers on Linux and Unix: BIND, Sendmail, and Apache. Beyond basic security configuration information, we will take an in-depth look at topics like DNSSec and Web Application Firewalls with mod_security and the Core Rules.

Topics: BIND; DNSSec; Sendmail; Apache; Web Application Firewalls with mod_security

506.6 Hands On: Digital Forensics for Linux/Unix

This hands-on course is designed to be an information-rich introduction devoted to basic forensic principals and techniques for investigating compromised Linux and Unix systems. At a high level, it introduces the critical forensic concepts and tools that every administrator should know and provides a real-world compromise for students to investigate using the tools and strategies discussed in class.

Topics: Tools Throughout; Forensic Preparation and Best Practices; Incident Response and Evidence Acquisition; Media Analysis; Incident Reporting

SANS Faculty Fellow

Hal Pomeranz

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is a SANS Faculty Fellow and the creator of the SANS/GIAC Securing Linux/Unix course (GCUX) as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog, and co-author of the weekly Command-Line Kung Fu blog. http://blog.commandlinekungfu.com

Security 509

Securing Oracle Databases

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Tanya Baccam

Experts agree that Oracle is one of the most complex software packages available today. Unfortunately, complexity often introduces an increased risk for vulnerabilities. These vulnerabilities are being increasingly targeted by attackers. It is not uncommon for the SANS Internet Storm Center to see hundreds of thousands of hack attempts against Oracle databases each month.

SANS recognizes the need for comprehensive Oracle security training to help organizations protect their most critical information resources. In this course, the student is lead through the process of auditing and securing Oracle by defining the risks to data, using techniques for detecting unauthorized access attempts, using Oracle access controls and user management functions, and developing reliable processes to secure the Oracle database, as well as applications.

Throughout the course the student will be exposed to the database as seen through the eyes of an attacker, including public and unreleased techniques that are used to compromise the integrity of the database or escalate a user's privileges. In this fashion, the student gains a better understanding of how an attacker sees a database as a target and how we can configure the database to be resistant to known and unknown attacks.

Who Should Attend:

- Oracle database administrators responsible for installation and management of Oracle databases
- Developers who wish to create secure data access applications and Web sites
- Security professionals who are concerned about the security of their organization's Oracle databases
- Auditors and penetration testers who need to evaluate the security of Oracle databases
- Security managers who need to understand the security risks with data held in an Oracle database

This course has been updated for versions of Oracle up to and including 11g on Unix and Windows operating systems.

What Students Are Saying

"It was refreshing to have a knowledgeable and confident instructor on this subject. It is a sharp contrast from the other Oracle classes I have taken."

-Sean Devitt, Harris Corporation

From the Author

Database compromises are a significant risk faced by organizations today. Data compromises seem to be constantly occurring, and many of the huge breaches that we know about today resulted because database security was improperly addressed. Databases are key targets because they store one of our most valuable resources - our data. The data needs to be protected. Oracle is one of the most exciting and challenging databases that exists. When it comes to securing an Oracle database, there are many challenges that Administrators and security professionals will face. This course is designed to be a fully comprehensive and intense introduction to planning, auditing, and securing an Oracle database. The course doesn't just mention the vulnerabilities, but it explains why the issues may exist and how an attacker could leverage them. Multiple hands-on exercises reinforce the content we learn in class. This aids the student in thinking like an attacker, which needs to be done to protect the databases. Students are often amazed at the many different ways an attacker might compromise an Oracle database! Ultimately, the goal is to teach how to protect one of the most important organizational assets - the data. This course is an exciting and interesting journey in protecting this critical organizational asset!
- Tanya Baccam

509.1 Hands On: Securing Oracle Foundations

The student is introduced to various techniques used by an attacker to compromise the database, including buffer overflows, SQL injection attacks, exploiting Oracle stored procedures, and cross-site scripting attacks. We look at the process of installing the database in a secure fashion after hardening the host operating system with strong file system permissions. An overview of all the Oracle offered security features will be covered.

Topics: Securing Oracle; Foundations; Oracle Attack Vectors and Security Features; Host Operating System Security; Identifying Passwords in the Environment

509.2 Hands On: Securing Oracle's Authentication Process

Oracle's authentication process has some significant weaknesses that need to be understood to secure the environment. Additionally, 11g made some significant changes to the authentication process. We review the authentication process in detail. Oracle default user accounts, roles, and grants will be reviewed, including audit techniques to identify user accounts with weak passwords. Multiple password cracking techniques and tools will be analyzed. Auditing user accounts and application schema accounts is discussed in detail covering third party authentication, shared accounts, and proxy authentication implemented in third party applications. The day concludes with a complete discussion of password management, including enforcing and creating a password management policy and utilizing profiles to control access to database resources.

Topics: Authentication Methods; Default Users and Password Audits; Schema and Application Owners; Implementing Password Management

509.3 Hands On: Oracle Access Controls — Configuration

Access control techniques are used to protect database objects. We cover many of the countless database configuration options with recommendations that make the database more resistant to common attacks, including both intentional and accidental incidents. We also dedicate time to the problems associated with the growing number of PUBLIC privileges including the techniques authenticated users can use to escalate their privilege levels. Tools such as Database Vault and Data Masking are also explored.

Topics: Access and Output; Roles and Users; Configuration; PUBLIC Privileges, Profiles, Packages, and Objects

509.4 Hands On: Auditing Oracle

Some organizations think auditing within Oracle's environment is difficult, if not impossible. This day delves into auditing the Oracle environment in a manageable and simple way. We examine the built-in Oracle auditing features, including Fine-Grained Auditing. Audit Vault will also be reviewed. Forensic assessment of Oracle databases is also covered in this day, including data recovery and retracing the steps of an attacker. If your organization is encumbered by federal restrictions and legal requirements in information management, this day will provide vital information that you can deploy immediately after completing this course.

Topics: Oracle Auditing - Myths and Facts; Reviewing the Audit Trail; Forensics; Fine Grained Audit; Securing Exposed Services

509.5 Hands On: Networking, Encryption, and Developer Tools

Since the Oracle listener can be the first recipient of attacks from adversaries seeking to compromise the database, we cover topics related to securing the listener. Network design recommendations for the database and administrative workstations are also addressed, including Oracle's Database Firewall. The day continues by discussing the challenges of encryption within the database or outside of the database. Encryption is looked at for both data at rest and data in transit. Finally, we conclude the day by looking at techniques to secure the SQL*Plus and iSQL*Plus tools, including techniques to enforce and restrict the use of specific applications that are allowed to connect to the database.

Topics: Auditing the Oracle Listener; Network Access to Oracle; Encryption; Restricting Developer and Access Tools

509.6 Hands On: Development and Securing Applications

End-user tools created with PL/SQL and Java can introduce their own security risks. This day covers secure programming for the database including protecting source code confidentiality and integrity and settings resource limits to prevent attacks. Security application roles and other techniques will be explored as options for protecting data. We also look at some of the common Web application vulnerabilities and the affect they can have on the Oracle database. The final module of this intense day covers where we think Oracle security is going, exploring early techniques in the design of viruses and worms specific to Oracle.

Topics: Oracle Programming Issues; Web Application Vulnerabilities; Controlling Applications; Controlling Application Internals; Oracle Security Future

SANS Senior Instructor

Tanya Baccam

Tanya is a SANS senior instructor, as well as a SANS courseware author. With more than 10 years of information security experience, Tanya has consulted with a variety of clients about their security architecture in areas such as perimeter security, network infrastructure design, system audits, web server security, and database security. Currently, Tanya provides a variety of security consulting services for clients, including system audits, vulnerability and risk assessments, database assessments, web application assessments, and penetration testing. She has previously worked as the director of assurance services for a security services consulting firm and served as the manager of infrastructure security for a healthcare organization. She also served as a manager at Deloitte & Touche in the Security Services practice. Tanya has played an integral role in developing multiple business applications and currently holds the CPA, GIAC GCFW, GIAC GCIH, CISSP, CISM, CISA, CCNA, and OCP DBA certifications. Tanya completed a bachelor of arts degree with majors in accounting, business administration and management information systems.

Security 540

VoIP Security

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Paul A. Henry

The promise of reduced costs obtainable through the use of VoIP (Voice over IP) can quickly be erased due to the inherent and often overlooked security risks. Whether your organization already utilizes VoIP communications or is only now considering deploying it, you need to master VoIP security best practices and technologies in order to design, deploy, and audit your trusted VoIP infrastructures. The best way to secure a VoIP network is to incorporate security into the design right from the beginning. However, even if you have security concerns about an existing VoIP network, this course will teach you all of the tips and tricks to protect your critical VoIP networks. You will learn practical tasks that you can directly apply immediately when you go back to work.

VoIP has become a widely adopted technology, and it's here to stay. VoIP protocols and technologies, and especially VoIP security, are among the most complex fields in IT today. This course offers the in-depth knowledge required to understand how VoIP technologies work at the protocol level (mainly focusing on SIP and RTP). A detailed in-class analysis of infrastructure, signaling, and media attacks will reveal the security risks of VoIP networks for service providers, carriers, and enterprises, and students will be shown how to mitigate these risks.

By helping you understand how VoIP protocols work and giving you hands-on experience with attack mechanisms that can impact your VoIP environment, this challenging course helps you design, build, and then provide ongoing assessment of a secure VoIP architecture.

We will cover various VoIP attacks from VoIP signaling and media eavesdropping, caller ID impersonation, and VoIP authentication cracking to man-in-the-middle call manipulation and media injection. We will then examine multiple cutting-edge solutions, security devices, standards, and countermeasures that can be used to alleviate these vulnerabilities and threats, detailing the strengths and weaknesses of each, while guiding you through the best tools for securing your VoIP network.

Who Should Attend:

- Network professionals who are responsible for designing and deploying secure VoIP infrastructures.
- Security professionals who are concerned about the weaknesses of VoIP environments.
- Members and leaders of incident handling teams who are interested in adding VoIP to their analysis and response capabilities.
- Service provider professionals who are interested in adding security to their VoIP offerings.
- Penetration testers who want to include VoIP security assessments in their organization's service offerings.
- Auditors who must evaluate VoIP infrastructures to ensure they meet an acceptable level of risk.

As part of the course, you will receive a software VoIP PBX based on Trixbox (Asterisk), an audio headset, and several VoIP analysis and attack tools. This toolkit will help you build your own VoIP infrastructure, gain hands-on experience, and learn the attack tools used to exploit VoIP vulnerabilities from the attacker perspective. You'll learn to understand the insight gained from VoIP penetration testing, which you will be able to apply to protect your VoIP infrastructure from attacks. The extensive hands-on labs, plus the instruction from industry VoIP security experts, provide you with the skills needed to architect and evaluate your VoIP infrastructure.

The course includes an extensive list of references for each module for further analysis and staying up to date in future VoIP security trends.

From the Author

When VoIP is mentioned, two main concepts emerge into people's minds: lowering telecommunication costs, and security. Obviously, VoIP provides a lot of advantages versus the legacy voice infrastructures, where reduction, computer application integration, and unified communications cost seem to be the most notorious. However, many organizations do not think of security when they implement VoIP. While VoIP has many benefits, it changes the rules on security. At the same time, it is interesting to analyze the level of trust we have in the legacy telephony infrastructures, like the PSTN or cellular networks (GSM, GPRS, or UMTS). We believe they are completely secure and that only law enforcement, or high-technology spies (like those in the movies), would be able to control our voice calls. This level of trust is associated with its closed and proprietary nature, versus the open and distributed nature of VoIP infrastructures, and it is what sets our expectation of privacy and level of trust in these networks making us think VoIP is inherently insecure.

However, nothing could be further from the truth. If implemented properly and securely, VoIP infrastructures can be more secure and trustworthy than the legacy voice networks. A couple of basic scenarios can exemplify this statement. Nowadays, caller ID spoofing is trivial and unavoidable in the PSTN; however, strong authentication methods are available in VoIP to mitigate impersonation attacks. Similarly, voice conversations crossing the PSTN travel in the clear, so anyone in the path between caller and callee can intercept and listen to the conversation. VoIP allows applying strong encryption techniques to protect the audio contents of a voice call and avoid eavesdropping attacks. The solutions are available; you only need to learn them and know how to deploy them. This advanced course is designed to provide you with the skills required to do so and master VoIP security. -Dr. Eric Cole

540.1 Hands On: VoIP Systems, Infrastructure and Design*

The VoIP field is very complex, with multiple technologies, standard and proprietary protocols, and components. This day starts with a brief introductory overview about VoIP concepts and devices and hands-on guidance to build the VoIP infrastructure used in the rest of the course. In order to gain hands-on experience, students will learn how to configure and secure Asterisk, an open source VoIP PBX. Configuring and designing a real VoIP server will help reinforce the security issues and countermeasures that have to be deployed.

Topics: Voice over Internet Protocol (VoIP); VoIP Deployment; Key Pitfalls to Avoid; Trixbox and Asterisk; Installing and Configuring Asterisk and Testing the Lab; Securing Asterisk

540.2 Hands On: VoIP Protocols and Analysis*

On day two, the course jumps directly into into the VoIP protocols world, introducing the main VoIP standards bodies and the most important VoIP signaling, media, and support protocols. One of the most critical skills for network engineers and security professionals is mastering the identification and analysis of network protocols. The course provides hands-on techniques to identify and analyze VoIP signaling and media protocols using Wireshark, focusing on SIP/SDP and RTP/RTCP. In order to understand all further VoIP attacks in detail, it is mandatory to be able to perform an in-depth analysis of the protocol's behavior, message types, call flow diagrams, and packet contents. The course dissects the SIP, SDP, RTP, and RTCP protocols to provide you with this in-depth knowledge. The main goal is to understand the details of the signaling and media protocols (SIP and RTP), the packets format, and how to analyze the stages of a SIP and RTP connection.

Topics: VoIP Standard Bodies; VoIP Signaling Protocols; VoIP Protocols Identification and Hands-on Analysis

540.3 Hands On – Part 1: VoIP Signaling Threats and Attacks*

Many organizations are deploying VoIP infrastructures, but few take the time to examine their deployment to ensure the infrastructure meets organizational requirements for security. This day examines the various threats that target VoIP environments, and multiple attack techniques and tools that leverage protocol and implementation weaknesses to compromise VoIP security. Taking an in-depth look at these techniques and tools, understanding how they work and the flaws they exploit, and practicing with them will help you make informed decisions to best accommodate the balance of usability, quality, performance, and security that is appropriate for your organization. This day explores in depth tools and techniques focused on the VoIP signaling threats.

Topics: VoIP Signaling Attacks: (SIP-based)

540.4 Hands On – Part 2: VoIP Signaling Threats and Attacks*

While understanding the attacks against signaling protocols is important, the real threat to a VOIP environment is compromise of the media protocols. The media protocol is where the "live" conversation is transmitted across the wire. Attacks against the media protocols can range from denial-of-service attacks to unauthorized recording of phone conversations.

Topics: VoIP Media Attacks: (RTP-based)

540.5 Hands On: VoIP Security*

After these attacks are dissected and understood, it is time to implement mitigation techniques, defenses, and countermeasures surrounding secure VoIP protocols and VoIP security devices. These elements provide multiple options to design and build a secure VoIP architecture. Only through an in-depth knowledge of the available VoIP secure protocols at the network, signaling, media, and key-exchange levels is it possible to protect the VoIP traffic and the sensitive contents exchanged through it. The protocols are complemented by VoIP security devices. New VoIP security standards are still being designed and ratified. The course dissects and compares all of them and their specific details because this is what makes the difference to determine the best solution for your environment. The current state of the art and best practices for all these secure VoIP protocols is analyzed. This VoIP defenses analysis is complemented with questions addressed to your VoIP vendor and service provider that guide you to select the best VoIP security solution based on your needs.

Topics: VoIP Security Devices

540.6 Hands On: VoIP Architecture*

The last day covers the most relevant VoIP infrastructure and network attacks with the goal of emphasizing how important it is to build a secure VoIP infrastructure on top of a secure network architecture. Some of the network-based attacks with a higher impact on the VoIP infrastructure are analyzed as well as the best architecture practices to protect the VoIP infrastructure against these threats. The VoIP security lectures are supplemented by hands-on labs focused on identifying devices on a VoIP infrastructure and complementing the initial reconnaissance results with more advanced vulnerability scanning and VoIP usernames and phone extensions enumeration techniques. Additionally, the signaling labs are rounded out with SIP-based manipulation attacks using advanced MitM tools and techniques. VoIP media vulnerabilities are demonstrated and practiced using eavesdropping and advanced RTP manipulation attacks. Finally, the VoIP countermeasures modules contain technical security checklists aimed to evaluate the VoIP security capabilities and supported features and protocols offered by your VoIP vendor(s) or service provider(s).

Topics: VoIP supporting infrastructure; VoIP Environment Awareness

*This course is available to Security 540 participants only.

SANS Certified Instructor

Paul A. Henry

Paul Henry is one of the world's foremost global information security and computer forensic experts with more than 20 years experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principle at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Henry has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Henry is frequently cited as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the *Information Security Management Handbook*. Paul serves as a keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

Security 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Justin Searle

Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate- to advanced-level class, you'll learn the art of exploiting web applications so you can find flaws in your enterprise's web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker so that you can be a powerful defender.

On day one, we will study the attacker's view of the web as well as learn an attack methodology and how the pen-tester uses JavaScript within the test. On day two we will study the art of reconnaissance, specifically targeted to web applications. We will also examine the mapping phase as we interact with a real application to determine its internal structure. During day three we will continue our test by starting the discovery phase using the information we gathered on day two. We will focus on application/server-side discovery. On day four we will continue discovery, focusing on client-side portions of the application, such as Flash objects and Java applets. On day five we will move into the final stage of exploitation. Students will use advanced exploitation methods to gain further access within the application. Day six will be a Capture the Flag event where the students will be able to use the methodology and techniques explored during class to find and exploit the vulnerabilities within an intranet site.

Who Should Attend:

- General security practitioners
- Penetration testers
- Ethical hackers
- Web application vulnerability
- Website designers and architects
- Developers

What Students Are Saying

"Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences." -Bobby Bryant, DoD

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization's web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

From the Author

Testing the security of web applications is not as simple as just knowing what SQL injection and cross-site scripting mean. Successful testers understand that methodical, thorough testing is the best means of finding the vulnerabilities within the applications. This requires a deep understanding of how web applications work and what attack vectors are available. This course provides that understanding by examining the various parts of a web application penetration. When teaching the class, I especially enjoy the use of real-world exercises and the in-depth exploration of web penetration testing. -Kevin Johnson

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

542.1 Hands On: The Attacker's View of the Web*

We begin by examining web technology – protocols, languages, clients, and server architectures – from the attacker's perspective. Then we cover the four steps of web application pen tests: reconnaissance, mapping, discovery, and exploitation.

Topics: Overview of the Web from a Penetration Tester's Perspective; Exploring the Various Servers and Clients; Discussion of the Various Web Architectures; Discover How Session State Works; Discussion of the Different Types of Vulnerabilities; Define a Web Application Test Scope and Process; Define Types of Penetration Testing

542.2 Hands On: Reconnaissance and Mapping*

Reconnaissance includes gathering publicly-available information regarding the target application and organization, identifying machines that support our target application, and building a profile of each server. Then we will build a map of the application by identifying the components, analyzing the relationship between them, and determining how they work together.

Topics: 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 Website; Scripting to Automate Web Requests and Spidering; Application Flow Charting; Relationship Analysis Within an Application; JavaScript for the Attacker

542.3 Hands On: Server-Side Discovery*

We will continue with the discovery phase, exploring both manual and automated methods of discovering vulnerabilities within the applications as well as exploring the interactions between the various vulnerabilities and the different user interfaces that web apps expose to clients.

Topics: Learn Methods to Discover Various Vulnerabilities; Explore Differences Between Different Data Back-ends; Explore Fuzzing and Various Fuzzing Tools; Discuss the Different Interfaces Websites Contain; Understand Methods for Attacking Web Services

542.4 Hands On: Client-Side Discovery*

Learning how to discover vulnerabilities within client-side code, such as Java applets and Flash objects, includes use of tools to decompile the objects and applets. We will have a detailed discussion of how AJAX and web service technology enlarges the attack surface that pen testers leverage.

Topics: Learn Methods to Discover Various Vulnerabilities; Learn Methods to Decompile Client-side Code; Explore Malicious Applets and Objects; Discovery Vulnerabilities in Web Application Through Their Client Components; Understand Methods for Attacking Web Services; Understand Methods for Testing Web 2.0 and AJAX-based Sites; Learn How AJAX and Web Services Change Penetration Tests; Learn the Attacker's Perspective on Python and PHP

542.5 Hands On: Exploitation*

Launching exploits against real-world applications includes exploring how they can help in the testing process, gaining access to browser history, port scanning internal networks, and searching for other vulnerable web applications through zombie browsers.

Topics: Explore Methods to Zombify Browsers; Discuss Using Zombies to Port Scan or Attack Internal Networks; Explore Attack Frameworks; 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

542.6 Hands On: Capture the Flag*

The goal of this event is for students to use the techniques, tools, and methodology learned in class against a realistic intranet application. Students will be able to use a virtual machine with the SamuraiWTF web pen testing environment in class and can apply that experience in their workplace.

Topics: Capture the Flag

*This course is available to Security 542 participants only.

SANS Instructor

Justin Searle

Justin is a managing partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and currently plays key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences, and is currently an instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top security conferences such as Black Hat, DEFCON, OWASP, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework, Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Security 560

Network Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Ed Skoudis

Security vulnerabilities, such as weak configurations, unpatched systems, and botched architectures, continue to plague organizations. Enterprises need people who can find these flaws in a professional manner to help eradicate them from our infrastructures. Lots of people claim to have penetration testing, ethical hacking, and security assessment skills, but precious few can apply these skills in a methodical regimen of professional testing to help make an organization more secure. This class covers the ingredients for successful network penetration testing to help attendees improve their enterprise's security stance.

We address detailed pre-test planning, including setting up an effective penetration testing infrastructure and establishing ground rules with the target organization to avoid surprises and misunderstanding. Then we discuss a time-tested methodology for penetration and ethical hacking across the network, evaluating the security of network services and the operating systems behind them.

Attendees will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, and social networking sites. We'll then turn our attention to scanning, experimenting with numerous tools in hands-on exercises. Our exploitation phase will include the use of exploitation frameworks, stand-alone exploits, and other valuable tactics, all with hands-on exercises in our lab environment. The class also discusses how to prepare a final report, tailored to maximize the value of the test from both a management and technical perspective. The final portion of the class includes a comprehensive hands-on exercise, following all of the steps to conduct a penetration test against a hypothetical target organization.

Who Should Attend:

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

The course also describes the limitations of penetration testing techniques and other practices that can be used to augment penetration testing to find vulnerabilities in architecture, policies, and processes. We also address how penetration testing should be integrated as a piece of a comprehensive enterprise information security program.

What Students Are Saying

"The best course in penetration testing in the industry. Ed's teaching and delivery allow him to shine and stand out from the rest of the crowd."

-Rudy Villalona, HP Enterprise Serivces

From the Author

Successful penetration testers don't just throw a bunch of hacks against an organization and regurgitate the output of their tools. Instead, they need to understand how these tools work in depth and conduct their test in a careful, professional manner. This course explains the inner workings of numerous tools and their use in effective network penetration testing and ethical hacking projects. When teaching the class, I particularly enjoy the numerous hands-on exercises culminating with a final pen-testing extravaganza lab. -Ed Skoudis

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

560.1 Hands On: Planning, Scoping, and Recon*

This course provides extensive details of penetration testing preparation and methodology, which are immensely useful in meeting the Payment Card Industry (PCI) Data Security Standard (DSS) Requirement 11.3 on penetration testing. We cover building a penetration testing and ethical hacking infrastructure that includes the appropriate hardware, software, network infrastructure, and test tools arsenal, with specific low-cost recommendations. This portion of the course also describes how to plan the specifics of a test, carefully scoping the project and defining the rules of engagement.

Topics: The Mindset of the Professional Pen Tester; Legal Issues; Reporting; Types of Penetration Tests and Ethical Hacking Projects; Detailed Recon; Mining Search Engine Results with Aura/Wikto/EvilAPI

560.2 Hands On: Scanning*

This component of the course focuses on the vital task of scanning a target environment, creating a comprehensive inventory of machines, and then evaluating those systems to find potential vulnerabilities. We'll look at some of the most useful scanning tools freely available today, experimenting with them in our hands-on lab. Because vulnerability-scanning tools inevitably give us false positives, we'll also look at techniques for false-positive reduction with hands-on exercises.

Topics: Overall Scanning Tips; tcpdump for the Pen Tester; Protocol Anomalies; The Nmap Scripting Engine; Version Scanning with Nmap and Amap; False Positive Reduction

560.3 Hands On: Exploitation and Post Exploitation*

In this section we look at the many kinds of exploits that a penetration tester or ethical hacker can use to compromise a target machine. We'll analyze in detail the differences between server-side, client-side, and local privilege escalation exploits, exploring some of the most useful recent exploits in each category. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. We'll also look at post-exploit analysis of machines and pivoting to find new targets.

Topics: Comprehensive Metasploit Framework Coverage with Exploits/Stagers/Stages; Bypassing the Shell vs. Terminal Dilemma; Installing VNC/RDP/SSH with Only Shell Access; Running Windows Commands Remotely with sc and wmic; Building Port Scanners and Password Guessers at the Command Line

560.4 Hands On: Password Attacks*

This component turns our attention to password attacks, analyzing password guessing, password cracking, and pass-the-hash techniques in depth. We'll go over numerous tips based on real-world experience to help penetration testers and ethical hackers maximize the effectiveness of their password attacks with some of the most powerful attack tools available today for gaining access to machines.

Topics: Pass-the-Hash Attacks Using Modified SMB Client Software; Patching John the Ripper to Squeeze Out Maximum Performance; Rainbow Tables Hands-on and In-depth; Cain – The Pen Tester's Dream Tool

560.5 Hands On: Wireless and Web Apps*

This section describes methodologies for finding common wireless weaknesses, including misconfigured access points, application of weak security protocols, and the improper configuration of stronger security technologies. The second half focuses on web application pen testing and looking for the flaws that impact commercial and homegrown web apps. Attendees will work hands on with tools that can find cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws, experimenting with each in several exercises.

Topics: Wireless Attacks; Discovering Access Points (Wire-Side and Wireless-Side); Wireless Crypto Flaws; Client-Side Wireless Attacks; Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection

560.6 Hands On: Penetration Testing Workshop and Capture the Flag Event*

This lively session represents the culmination of the network penetration testing and ethical hacking course, where attendees apply the skills mastered in the other sessions in a hands-on workshop. The rest of the course covers the overall process for successful testing with a series of hands-on exercises individually illustrating each point. But in this final workshop, all of the exercises converge in an overall network penetration-testing workout, where attendees will function as part of a pen test team.

Topics: Applying Penetration Testing and Ethical Hacking Practices End-to-end; Scanning; Exploitation; Pivoting; Analyzing Results

*This course is available to Security 560 participants only.

SANS Faculty Fellow

Ed Skoudis

Ed Skoudis is a founder and senior security consultant with InGuardians. He is also the founder of Counter Hack Challenges, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including NetWars, Cyber Quests, and Cyber Foundations. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in financial, high technology, healthcare, and other industries. Ed conducted a demonstration of hacker techniques against financial institutions for the United States Senate and is a frequent speaker on issues associated with hacker tools and defenses. He has published numerous articles on these topics as well as the Prentice Hall best sellers *Counter Hack Reloaded* and *Malware: Fighting Malicious Code*. Ed was also awarded 2004-2009 Microsoft MVP awards for Windows Server Security and is an alumnus of the Honeynet Project. Previous to InGuardians, Ed served as a security consultant with International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips. http://blog.commandlinekungfu.com

Security 566

Implementing and Auditing the Twenty Critical Security Controls - In Depth

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Randy Marchany

In the last couple of years it has become obvious that in the world of information security, the offense is outperforming the defense. Even though budgets increase and management pays more attention to the risks of data loss and system penetration, data is still being lost and systems are still being penetrated. Over and over people are asking, "What can we practically do to protect our information?" The answer has come in the form of 20 information assurance controls known as the Consensus Audit Guidelines (CAG), located at **www.sans.org/critical-security-controls/guidelines.php**.

This course has been written to help those setting/implementing/deploying a strategy for information assurance in their agency or organization by enabling them to better understand these guidelines. Specifically the course has been designed in the spirit of the offense teaching the defense to help security practitioners understand not only how to stop a threat, but why the threat exists and how later to audit to ensure that the organization is indeed in compliance with their standards. Walking away from this course, students should better understand how to create a strategy for successfully defending their data, implement controls to prevent their data from being compromised, and audit their systems to ensure compliance with the standard. And in SANS style, this course will not only provide a framework for better understanding, but also give you a hands-on approach to learning these objectives to ensure that what you learn today you'll be able to put into practice in your organization tomorrow.

This course helps you master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. These Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls found at **www.sans.org/critical-security-controls/guidelines.php**.

Who Should Attend:

- Information assurance auditors
- System implementers/ administrators
- Network security engineers
- IT administrators
- DoD personnel/contractors
- Federal agencies/clients
- Private sector organizations looking for information assurance priorities for securing their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD 440, SEC401, SEC501, SANS Audit classes, and MGT512

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 72.***

From the Author

As we've had the opportunity to talk with information assurance engineers, auditors, and managers over the past ten years, we've seen frustration in the eyes of these hardworking individuals who are trying to make a difference in their organizations by better defending their data systems. It has even come to the point where some organizations have decided that it's simply too hard to protect their information, and many have started to wonder, is the fight really worth it? Will we ever succeed? We see companies and agencies making headway, but the offense keeps pushing. The goal of this course is to give direction and a realistic hope to organizations attempting to secure their systems. The 20 Critical Security Controls: Planning, Implementing and Auditing offers direction and guidance from those in the industry that think through the eyes of the attacker as to what security controls will make the most impact. What better way to play defense than by understanding the mindset of the offense? By implementing our defense methodically and with the mindset of a hacker, we think organizations have a chance to succeed in this fight. We hope this course helps turn the tide.

-Dr. Eric Cole and James Tarala

What Students Are Saying

"The course material is put together in such a way that you will be able to follow it like a recipe in your real-life environment."

-Jane Citino, Verizon Wireless

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

566.1 Hands On – Part 1: Implementing and Auditing the Twenty Critical Security Controls – In Depth*

Day 1 will cover an introduction and overview of the 20 critical controls, laying the foundation for the rest of the class. For each control the following information will be covered and we will follow the same outline for each control:

- Overview of the Control
- How it is Compromised
- Defensive Goals
- Quick Wins
- Visibility & Attribution
- Configuration & Hygiene
- Advanced
- Overview of Evaluating the Control
- Core Evaluation Test(s)
- Testing/Reporting Metrics
- Steps for Root Cause Analysis of Failures
- Audit/Evaluation Methodologies
- Evaluation Tools
- Exercise to Illustrate Implementation or Steps for Auditing a Control

In addition, Critical Controls 1 and 2 will be covered in depth.

Topics: Critical Control 1 - Inventory of Authorized and Unauthorized Devices
Critical Control 2 - Inventory of Authorized and Unauthorized Software

566.2 Hands On – Part 2: Implementing and Auditing the Twenty Critical Security Controls – In Depth*

Day 2 will cover Critical Controls 3, 4, 5, and 6.

Topics: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security

566.3 Hands On – Part 3: Implementing and Auditing the Twenty Critical Security Controls – In Depth*

Day 3 will cover Critical Controls 7, 8, 9, 10, and 11.

Topics: Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability (validated manually)
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

566.4 Hands On – Part 4: Implementing and Auditing the Twenty Critical Security Controls – In Depth*

Day 4 will cover Critical Controls 12, 13, 14, and 15.

Topics: Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based On Need to Know

566.5 Hands On – Part 5: Implementing and Auditing the Twenty Critical Security Controls – In Depth*

Day 5 will cover Critical Controls 16, 17, 18, 19, and 20.

Topics: Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response Capability (validated manually)
Critical Control 19: Secure Network Engineering (validated manually)
Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

*This course is available to Security 566 participants only.

SANS Certified Instructor

Randy Marchany

Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. He is a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000.

"Real-world approach to auditing, a rare thing to find in our current environment."

-Richard Goldberg,
Aera Energy, LLC

Security 575

Mobile Device Security and Ethical Hacking

New Course!

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Joshua Wright

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from ERP to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

The security risks of mobile phone and tablet device use in the workplace

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **distributed sensitive data storage and access mechanisms**
- **lack of consistent patch management and firmware updates**
- **the high probability of device loss or theft, and more.**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

Who Should Attend:

- Security personnel whose job involves assessing, deploying, or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills

From mobile device security policy development, to design and deployment, and more

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

From the Author

I'm not sure exactly when it started, but laptops and PCs are quickly becoming legacy computing devices, replaced with mobile phones and tablets at an ever increasing rate. Just when I thought we were getting a much better handle on the security of Windows, Mac, and other Unix systems, there is an explosion of new devices joining our networks. Mobile device adoption has been so rapid that we're suddenly back in the wild west. Many organizations just don't have the policies, procedures, technical infrastructure, and skilled personnel needed to deal with these new technologies and devices. The devices themselves simply do not have the same security controls that we rely on in modern, secure enterprise and government networks. Even with their weaknesses, mobile phones are here to stay, and we are being called on to support them. Some organizations try to drag their feet on allowing mobile phones, but that ultimately contributes to the problem. If we don't address security, the threats continue to grow uncontrolled and unmonitored. Mobile tablets only exacerbate the problem. To address these concerns, this course will give you the blueprint, technical frameworks, and hard-core analysis skills needed to address these challenges head-on so that your organization's personnel can use their mobile devices more securely. Using the skills shared in this course, you'll have the knowledge to securely deploy, manage, and monitor mobile phones and tablets inside your organization through effective policy and careful network deployment and monitoring. You'll also build essential skills in analyzing the risks of data leakage in mobile code and the applications your end-users want to run from app stores, and we'll show you how to ethically hack your networks to identify the real threat and exposure of mobile phone weaknesses. I created this course to help people build their skills in all these areas, focusing on the topics and concepts that are most important and immediately useful. Every organization needs security professionals with the skills required to secure mobile phone and tablet environments. By taking this course, you'll become an even more valued part of your organization, you'll be prepared to lead your organization's efforts to securely embrace the new world of mobile devices... and we'll have lots of geeky fun in the process. -Joshua Wright

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

575.1 Hands On: Mobile Device Threats, Policies, and Security Models*

The first part of the course looks at the significant threats affecting mobile phone deployment and how organizations are being attacked through these systems. As a critical component of a secure deployment, we guide you through the process of defining mobile phone and tablet policies with sample policy language and recommendations for various vertical industries, taking into consideration the legal obligations of enterprise organizations. We'll also look at the architecture and technology behind mobile device infrastructure systems for Apple, Android, BlackBerry, and Windows devices, as well as the platform-specific security controls available including device encryption, remote data wipe, application sandboxing, and more.

Topics: Mobile Phone and Tablet Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Phone and Tablet Security Models; Legal Aspects of Mobile; Mobile Device Policy Considerations and Development

575.2 Hands On: Mobile Device Architecture Security & Management*

With an understanding of the threats, architectural components, and desired security methods, we can design and implement mobile device and infrastructure systems to defend against threats. In this part of the course, we examine the design and deployment of network and system infrastructure to support a mobile phone deployment including the selection and deployment of that meet the organization's requirements for administration and security.

Topics: Wireless Network Infrastructure; Remote Access Systems; Certificate Deployment Systems; Mobile Device Management (MDM) System Architecture; Mobile Device Management (MDM) Selection

575.3 Hands On: Mobile Code and Application Analysis*

With the solid analysis skills taught in this section of the course, we can evaluate apps to determine the type of access and information disclosure threats that they represent. Security professionals can use these skills not only to determine which outside applications the organization should allow, but also to evaluate the security of any apps developed by the organization itself for its employees or customers. In this process, we'll use jailbreaking and other techniques to evaluate the data stored on mobile phones.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Filesystem Application Modeling; Network Activity Monitoring; Mobile Code and Application Analysis; Approving or Disapproving Applications in Your Organization

575.4 Hands On: Ethical Hacking Mobile Networks*

Through ethical hacking and penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that could allow unauthorized access to data or supporting networks. By identifying and understanding the implications of these flaws, we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; WiFi Attacks; Bluetooth Attacks; Network Exploits

SANS Senior Instructor

Josh Wright

Joshua Wright is an independent information security analyst and senior instructor with the SANS Institute. A widely recognized expert in the wireless security field, Josh has worked with private and government organizations to evaluate the threat surrounding wireless technology and evolving threats. As an open-source enthusiast, Josh has developed a variety of tools that can be leveraged for penetration testing and security analysis. Josh publishes his tools, papers, and techniques for effective security analysis on his website at www.willhackforsushi.com.

575.5 Hands On: Ethical Hacking Mobile Phones, Tablets, and Applications*

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on individual mobile devices including iPhones, iPads, Android phones, Windows Phones and BlackBerry phones and tablets. We'll also examine platform-specific application weaknesses and look at the growing use of web framework attacks.

Topics: Mobile Device Exploits; Web Framework Attacks; Application Attacks; Cloud/Remote Data Accessibility Attacks

575.6 Hands On: Secure Mobile Phone Capture the Flag*

On the last day of class, we apply the skills, concepts, and technology covered in the course for a comprehensive Capture the Flag (CtF) event. In this day-long, in-depth final hands-on CtF exercise, you will:

- **Have the option to participate in multiple organizational roles related to mobile device security,**
- **Design a secure infrastructure for the deployment of mobile phones,**
- **Monitor network activity to identify attacks against mobile devices,**
- **Extract sensitive data from a compromised iPad, and**
- **Attack a variety of mobile phones and related network infrastructure components.**

In the CtF exercise, you will use the skills built throughout the course to evaluate real-world systems and defend against attackers, simulating the realistic environment you'll face when you get back to the office. You will leave the course armed with the knowledge and skills you'll need to securely integrate and deploy mobile devices in your organization.

*This course is available to Security 575 participants only.

Security 579

Virtualization and Private Cloud Security

New Course!

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop provided ***(Students will be provided a laptop for use during class)***
Instructor: Dave Shackleford

One of today's most rapidly evolving and widely deployed technologies is server virtualization. Many organizations are already realizing the cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management for virtualized systems. There are even security benefits of virtualization - easier business continuity and disaster recovery, single points of control over multiple systems, role-based access, and additional auditing and logging capabilities for large infrastructures.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits and presents new vulnerabilities that must be managed. In addition, there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams. Virtualization technologies also connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional security controls.

In addition, many organizations are evolving virtualized infrastructure into private clouds - internal shared services running on virtualized infrastructure. Security architecture, policies, and processes will need to adapt to work within a cloud infrastructure, as well, and there are many changes that security and operations teams will need to accommodate to ensure assets are protected.

Who Should Attend:

- Security personnel who are tasked with securing virtualization and private cloud infrastructure
- Network and systems administrators who need to understand how to architect, secure, and maintain virtualization and cloud technologies
- Technical auditors and consultants who need to gain a deeper understanding of VMware virtualization from a security and compliance perspective

The class starts out with two days of architecture and security design for both virtualization and private cloud infrastructure. The entire gamut of components will be covered ranging from hypervisor platforms to virtual networking, storage security to locking down the individual virtual machine files. We'll describe how to secure the management interfaces and servers, delve into virtual desktop infrastructure (VDI), and go in-depth on what to consider when building a private cloud from existing virtualization architecture. Finally, we'll look at integrating virtual firewalls and intrusion detection systems into the new architecture for access control and network monitoring.

The next two days will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. We'll show you how to design a foundational risk assessment program, and then build on this with policies, governance, and compliance considerations within your environment. We'll cover auditing and assessment of your virtualized assets, with a session on scripting that will help you put this into practice right away. Then we'll go in-depth into data security within a private cloud environment, discussing encryption and data lifecycle management techniques that will help you keep up with data that is much more mobile than ever before. Identity and Access Management (IAM) within a virtualized/cloud environment will be touched on, and we'll wrap up with a thorough session on disaster recovery and business continuity planning that leverages and benefits from virtualization and cloud-based technology.

The final two days go into detail on offense and defense - how can we assess virtualized environment using scanning and pen testing tools and techniques, and how do things change when we move to a cloud model? We'll cover a variety of scanners and vulnerability management tools and practices, and then take a hard look at virtualization vulnerabilities, exploits, and toolkits for pen testing that we can put to use in class. Once we cover the offense, we'll take the opposite approach and go into detail on performing intrusion detection and logging within the virtual environment, as well as covering anti-malware advances and changes within virtual infrastructure. We'll wrap up the session with coverage of incident handling within virtual and cloud environments, as well as adapting forensics processes and tools to ensure we can maintain chain-of-custody and perform detailed analysis of virtualized assets.

579.1 Hands On: Virtualization Security Architecture and Design*

We'll cover the foundations of virtualization infrastructure and clarify the differences between server virtualization, desktop virtualization, application virtualization, and storage virtualization. We'll start with hypervisor platforms, covering the fundamental controls that should be set within VMware ESX and ESXi, Microsoft Hyper-V, and Citrix XenServer. You'll spend time analyzing virtual networks. We'll compare designs for internal networks and DMZs Virtual switch types will be discussed, along with VLANs and PVLANs. We will cover virtual machine settings, with an emphasis on VMware VMX files. Tactics will be covered that help organizations better secure Fibre Channel, iSCSI, and NFS-based NAS technology.

Topics: Virtualization Components and Architecture Designs; Hypervisor Lockdown Controls for VMware; Microsoft Hyper-V, and Citrix Xen, Virtual Network Design Cases, Virtual Switches and Port Groups, Segmentation Techniques

579.2 Hands On: Virtualization and Private Cloud Infrastructure Security*

Today starts with virtualization management. VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), and Citrix XenCenter will be covered. Virtual Desktop Infrastructure (VDI) will be covered with emphasis on security principles. Specific security-focused use cases for VDI, such as remote access and network access control, will be reviewed. We will take an in-depth look at virtual firewalls. Students will build a virtualized intrusion detection model; integrating promiscuous interfaces and traffic capture methods into virtual networks; and then setting up and configuring a virtualized IDS sensor. Attention will be paid to host-based IDS, with considerations for multitenant platforms.

579.3 Hands On – Part 1: Virtualization Offense and Defense*

In this session, we'll delve into the offensive side of security specific to virtualization and cloud technologies. While many key elements of vulnerability management and penetration testing are similar to â€œtraditional environments, there are many differences that we will cover. First, we'll cover a number of specific attack scenarios and models that represent the different risks organizations face in their virtual environments. Then we'll go through the entire penetration testing and vulnerability assessment lifecycle, with an emphasis on virtualization tools and technologies. Students will then learn about monitoring traffic and looking for malicious activity within the virtual network, and numerous network-based and host-based tools will be covered and implemented in class. Finally, students will learn about logs and log management in virtual environments.

579.4 Hands On – Part 2: Virtualization Offense and Defense*

This session is all about defense! We'll start off with an analysis on anti-malware techniques. We'll look at traditional antivirus, whitelisting, and other tools and techniques for combating malware, with a specific eye toward virtualization and cloud environments. New commercial offerings in this area will also be discussed to provide context, as well. The majority of this session will focus on incident response and forensics in a virtualized or cloud-based infrastructure. We'll walk students through the 6-step incident response cycle espoused by NIST and SANS, and highlight exactly how virtualization fits into the "big picture." Students will discuss and analyze incidents at each stage, again with a focus on virtualization and cloud. We'll finish the incident response section with processes and procedures organizations can put to use right away to improve their awareness of virtualization-based incidents.

579.5 Hands On: Virtualization and Cloud Integration: Policy, Operations, and Compliance*

This session will explore how traditional security and IT operations changes with the addition of virtualization and cloud technology in the environment. Our first discussion will be a lesson on contrast! First, we'll present an overview of integrating existing security into virtualization. Then, we'll take a vastly different approach, and outline how virtualization actually creates new security capabilities and functions! This will really provide a solid grounding for students to understand just what a paradigm shift virtualization is, and how security can benefit from it, while still needing to adapt in many ways.

579.6 Hands On: Confidentiality, Integrity, and Availability with Virtualization and Cloud*

Today's session will start off with a lively discussion on virtualization assessment and audit. You may be asking - how will you possibly make a discussion on auditing lively? Trust us! We'll cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most important and critical things to take away from these to implement. We'll really put our money where our mouth is next - students will learn to implement audit and assessment techniques by scripting with the VI CLI, as well as some Powershell and general shell scripting! Although not intended to be an in-depth class on scripting, some key techniques and ready-made scripts will be discussed to get students prepared for implementing these principles in their environments as soon as they get back to work.

*This course is available to Security 579 participants only.

SANS Certified Instructor

Dave Shackleford

Dave Shackleford is the owner and principal consultant at Voodoo Security; senior vice president of research and CTO at IANS; and a SANS analyst, instructor, and course author. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft; CTO for the Center for Internet Security; and as a security architect, analyst, and manager for several Fortune 500 companies. Dave is a coauthor of *Hands-On Information Security* from Course Technology as well as the Managing Incident Response chapter in the Course Technology book *Readings and Cases in the Management of Information Security*. Recently, Dave coauthored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

Security 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Matthew Luallen

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, but it is growing in deployment and utilization with wireless LAN technology and WiFi as well as other applications, including cordless telephones, smart homes, embedded devices, and more. Technology such as ZigBee and WiMAX offer new methods of connectivity to devices, while other wireless technology, including WiFi, Bluetooth, and DECT, continue their massive growth rate, each introducing their own set of security challenges and attacker opportunities.

To be a wireless security expert, you need to have a comprehensive understanding of the technology, the threats, the exploits, and the defense techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems, including developing attack techniques leveraging Windows 7 and Mac OS X. We'll also examine the commonly overlooked threats associated with Bluetooth, ZigBee, DECT, and proprietary wireless systems. As part of the course, you'll receive the SWAT Toolkit, which will be used in hands-on labs to back up the course content and reinforce wireless ethical hacking techniques.

Who Should Attend:

- Ethical hackers and penetration testers
- Network security staff
- Network and system administrators
- Incident response teams
- Information security policy decision makers
- Technical auditors
- Information security consultants
- Wireless system engineers
- Embedded wireless system developers

Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

In terms of technical content, SEC617 ranks up at the top for in-depth, comprehensive information about wireless security. However, you don't need to be an expert in wireless technology to succeed in this course. To help students consume the course content, I've written extensive notes for every topic, complete with review question and answer sections and recommendations for additional reading if you want to dig deeper. Many students comment that their favorite part about the course is the hands-on time, which makes up a significant part of the course. Classroom labs are written such that even if you have never used wireless technology or a Linux system before, you'll be able to complete all exercises and reproduce your results against your own networks when you return to the office. Everyone can take this class and gain useful and valuable skills for attacking and defending wireless networks.

From the Author

It's been amazing to watch the progression of wireless technology over the past several years. WiFi has grown in maturity and offers strong authentication and encryption options to protect networks, and many organizations have migrated to this technology. At the same time, attackers are becoming more sophisticated, and we've seen significant system breaches netting millions of payment cards that start with a wireless exploit. This pattern has me very concerned, as many organizations, even after deploying WPA2 and related technology, remain vulnerable to a number of attacks that expose their systems and internal networks. In putting this class together, I wanted to help organizations recognize the multi-faceted wireless threat landscape and evaluate their exposure through ethical hacking techniques. Moreover, I wanted my students to learn critical security analysis skills so that, while we focus on evaluating wireless systems, the vulnerabilities and attacks we leverage to exploit these systems can be applied to future technologies as well. In this manner, the skills you build in this class remain valuable for today's wireless technology, tomorrow's technology advancements, and for other complex systems you have to evaluate in the future as well. If you have questions or comments about this course, I would be very happy to hear from you. Please e-mail me at **jwright@sans.org**. -Joshua Wright

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

617.1 Wireless Architecture and Analysis*

Students will identify the risks associated with modern wireless deployments as well as the characteristics of physical layer radio frequency systems, including 802.11a/b/g and pre-802.11n systems. Students will leverage open-source tools for analyzing wireless traffic and mapping wireless deployments.

Topics: Wireless Signal Exposure Threats; Identifying Threats in Wireless Networks; RF Signal Propagation and Transmission Characteristics; RF Antenna Gain Types and Concepts; Physical Layer Coding Mechanisms; Leveraging Tools Including Kismet, Wireshark, and gpsmap for Network Mapping and Identification

617.2 Hands On – Part 1: Wireless Security Exposed*

Students will develop an in-depth treatise on the IEEE 802.11 MAC layer and operating characteristics. Using passive and active assessment techniques, students will evaluate deployment and implementation weaknesses, auditing against common implementation requirements, including PCI and the DoD Directive 8100.2. Security threats introduced with rogue networks will be examined from a defensive and penetration-testing perspective. Threats present in wireless hotspot networks will also be examined, identifying techniques attackers can use to manipulate guest or commercial hotspot environment.

Topics: IEEE 802.11 Framing; AP Fingerprinting; Kismet Post-Processing; Assessing Information Disclosure Threats; Auditing Wireless Policy Compliance; Evading WIDS Systems with Custom Rogue APs; "Free Public WiFi" and Ad-Hoc Networks; Wireless Device Triangulation; Webmail Session Hijacking; Defensive Measures for Guest Network Deployment

617.3 Hands On – Part 2: Wireless Security Exposed*

Students will continue their assessment of wireless security mechanisms, such as the identification and compromise of static and dynamic WEP networks and exploiting weak authentication techniques, including the Cisco LEAP protocol. Next-generation wireless threats will be assessed, including attacks against client systems, such as network impersonation attacks and traffic manipulation. Students will evaluate the security and threats associated with common wireless MAN technology, including proprietary and standards-based solutions.

Topics: Introduction to The RC4 Cipher; Understanding Failures in WEP; Leveraging Advanced Tools to Accelerate WEP Cracking; Attacking MS-CHAPv2 Authentication Systems; Attacker Opportunities When Exploiting Client Systems; Manipulating Plaintext Network Traffic; Attacking the Preferred Network List on Client Devices; Network Impersonation Attacks; Risks Associated with WMAN Technology; Assessing WiMAX Flaws

617.4 Hands On – Part 3: Wireless Security Exposed*

Part three covers the evaluation of modern wireless encryption and authentication systems, identifying the benefits and flaws in WPA/WPA2 networks and common authentication systems. Upper-layer encryption strategies for wireless security using IPSec are evaluated with in-depth coverage of denial-of-service attacks and techniques.

Topics: Threats Associated with the WPA/TKIP Protocol; Implementing Offline Wordlist Attacks Against WPA/WPA2-PSK Networks; Understanding the PEAP Authentication Exchange; Exploiting PEAP Through RADIUS Impersonation; Recommendations for Securing Windows XP Supplicants; Exploiting Wireless Firmware for DoS Attack; Wireless Packet Injection and Manipulation Techniques; VPN Network Fingerprinting and Analysis Tools

617.5 Hands On – Part 4: Wireless Security Exposed*

Advanced wireless testing and vulnerability discovery systems will be covered, including 802.11 fuzzing techniques. A look at other wireless technology, including proprietary systems, cellular technology, and an in-depth coverage of Bluetooth risks, will demonstrate the risks associated with other forms of wireless systems and the impact to organizations.

Topics: Wireless Fuzzing Tools and Techniques; Vulnerability Disclosure Strategies; Discovering Unencrypted Video Transmitters; Assessing Proprietary Wireless Devices; Traffic Sniffing in GSM Networks; Attacking SMS Messages and Cellular Calls; Bluetooth Authentication and Pairing Exchange; Attacking Bluetooth Devices; Sniffing Bluetooth Networks; Eavesdropping on Bluetooth Headsets

617.6 Wireless Security Strategies and Implementation*

The final day of the course evaluates strategies and techniques for protecting wireless systems. Students will examine the benefits and weaknesses of WLAN IDS systems while gaining insight into the design and deployment of a public key infrastructure (PKI). Students will also examine critical secure network design choices, including the selection of an EAP type, selecting an encryption strategy, and the management of client configuration settings.

Topics: WLAN IDS Signature and Anomaly Analysis Techniques; Understanding PKI Key Management Protocols; Deploying a Private Certificate Authority on Linux and Windows Systems; Configuring Windows IAS for Wireless Authentication; Configuring Windows XP Wireless Settings in Login Scripts

*This course is available to Security 617 participants only.

SANS Certified Instructor

Matthew Luallen

Matthew E. Luallen is a well-respected information professional, researcher, instructor, and author. Mr. Luallen serves as the president and co-founder of CYBATI, a strategic and practical educational and consulting company. CYBATI provides critical infrastructure and control system cybersecurity consulting, education, and awareness. Prior to incorporating CYBATI, Mr. Luallen served as a co-founder of Encari and provided strategic guidance for Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office. In an effort to promote education and collaboration in information security, Mr. Luallen is an instructor and faculty member at several institutions. Mr. Luallen is adjunct faculty for DePaul University, teaching the Computer Information and Network Security Masters degree capstone course. He is also a certified instructor and CCIE for Cisco Systems, covering security technologies, such as firewalls, intrusion prevention, and virtual private networks, and general secure information architecture. As a certified instructor for the SANS Institute, Mr. Luallen teaches infrastructure architecture, wireless security, web application security, regulatory and standards compliance, and security essentials. Mr. Luallen is a graduate of National Technological University with a master's degree in computer science, and he also holds a bachelor of science degree in industrial engineering from the University of Illinois, Urbana.

Security 642

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Kevin Johnson

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag (CtF) event, which tests the knowledge you will have acquired the previous five days.

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real-world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

Who Should Attend:

- Web penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- System architects

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full-day Capture the Flag (CtF) event. This CtF event will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets as well as fulfill a need to teach more advanced techniques than can be covered in the foundational course, Security 542: Web Application Penetration Testing and Ethical Hacking.

From the Author

As web applications and their mobile counterparts become more complex and hardened against attack, penetration testers need to adjust the techniques they use to evaluate the security of these systems. This includes understanding how the various targets work, their usage of encryption and web application firewalling, and how to perform vulnerability discovery and exploitation against these items. This course is designed to expand past the methodology and focus on the how when we are presented with the challenges of web penetration testing.
-Kevin Johnson

642.1 Hands On: Advanced Discovery and Exploitation*

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle these targets. We will begin the class by exploring how Burp Suite works and more advanced ways to use it within your penetration-testing processes. The exploration of Burp Suite will focus on its ability to work within the traditional web penetration testing methodology and assist in manually discovering the flaws within the target applications. Following this discussion, we will move into studying specific vulnerability types. This examination will explore some of the more advanced techniques for finding server-based flaws such as SQL injection. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers show the risks the flaws expose an organization to.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Examine How to Use Burp Intruder to Effectively Fuzz Requests; Explore Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Learn Advanced Exploitation Techniques

642.2 Hands On: Discovery and Exploitation for Specific Applications*

On day two of 642, we will continue the exploration of advanced discovery and exploitation techniques. We'll start by exploring client-side flaws such as cross-site scripting (XSS) and cross-site request forgery (XSRF). We will explore some of the more advanced methods for discovering these issues. After finding the flaws, you will learn some of the more advanced methods of exploitation, such as scriptless attacks and building web-based worms using XSRF and XSS flaws within an application. During the next part of the day we'll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. This section of the class examines applications such as SharePoint and WordPress. These specific targets have unique needs and features that make testing them both more complex and more fruitful for the tester. This section of the class will help you understand these differences and make use of them in your testing.

Topics: Discovering XSRF Flaws Within Complex Applications; Learning About DOM-based XSS Flaws and How to Find Them Within Applications; Exploiting XSS Using Scriptless Injections; Bypassing Anti-XSRF Controls Using XSS/XSRF Worms; Attacking SharePoint Installations; How to Modify Your Test Based on the Target Application

642.3 Hands On: Web Application Encryption*

Cryptographic weaknesses are a common area where flaws are present, yet few penetration testers have the skill to investigate, attack and exploit these flaws. When we investigate web application crypto attacks, we typically target the implementation and use of cryptography in modern web applications. Many popular web programming languages or development frameworks make encryption services available to the developer, but do not inherently protect encrypted data from being attacked, or permit the developer to use cryptography in a weak manner. These implementation mistakes are going to be our focus in this section, as opposed to the exploitation of deficiencies in the cryptographic algorithms themselves. We will also explore the various ways applications use encryption and hashing insecurely. Students will learn how techniques such as identifying what the encryption technique is to how to exploit various flaws within the encryption or hashing.

Topics: Explore How to Identify the Cryptography in Use; Discover How to Attack the Encryption Keys; Learn How to Attack Electronic Codebook (ECB) Mode Ciphers; Exploit Padding Oracles and Cipher Block Chaining (CBC) Bit Flipping

642.4 Hands On: Web Application Firewall and Filter Bypass*

Today, applications are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques make it more difficult for penetration testers during their testing. These controls block many of the automated tools and simple techniques used to discover flaws today. On day four you will explore techniques used to map the control and how it is configured to block attacks. You'll be able to map out the rule sets and determine the specifics of how it detects attacks. This mapping will then be used to determine attacks that will bypass the control. You'll use HTML5, UNICODE and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Explore How to Determine the Rule Sets Protecting the Application; Learn How HTML5 Injections Work; Discover the Use of UNICODE and Other Encodings

642.5 Hands On: Mobile Applications and Web Services*

Web applications are no longer limited to the traditional HTML based interface. Web services and mobile applications have become more common and are regularly being used to attack client and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. During day five, you will learn how to build a test environment for mobile applications and web services. We will also explore various techniques to discover flaws within the applications and backend systems. These techniques will make use of tools such as Burp Suite and other automated toolsets.

Topics: Understanding the Mobile Platforms and Architecture; Intercepting Traffic to Web Services and from Mobile Applications; Building a Test Environment; Injecting Malicious Traffic into Web Services

642.6 Hands On: Capture the Flag*

During day six of the class you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this capture the flag event is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You'll be able to use these ideas and methods against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework web penetration-testing environment. You will be able to use this both in the class and after leaving and returning to your normal jobs.

*This course is available to Security 642 participants only.

SANS Senior Instructor

Kevin Johnson

Kevin Johnson is a security consultant and founder of Secure Ideas. Kevin came to security from a development and system administration background. He has many years of experience performing security services for fortune 100 companies, and in his spare time he contributes to a large number of open-source security projects. He is the founder of many different projects and has worked on others. He founded BASE, which is a web front-end for Snort analysis. He also founded and continues to lead the SamuraiWTF live DVD. This is a live environment focused on web penetration testing. He also founded Yokoso! and Laudanum, which are focused on exploit delivery. Kevin is a senior instructor for SANS and the author of Security 542: Web Application Penetration Testing and Ethical Hacking. He also presents at industry events, including DEFCON and ShmooCon, and for various organizations, like Infragard, ISACA, ISSA, and the University of Florida.

Security 660

Advanced Penetration Testing, Exploits, and Ethical Hacking

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)
46 CPE/CMU Credits • Laptop Required • Instructor: Stephen Sims

It is well-known that attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, one must have a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 engages attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

The course starts off by introducing advanced penetration concepts, which will become the focus throughout the course. The course quickly dives deep into modern operating system controls, which stump many attackers and penetration testers. There are often ways around controls, such as address space layout randomization (ASLR), data execution prevention (DEP), canaries, and many others. These controls are introduced on day one and defeated at various points throughout the course. The remainder of the day is spent using the Python programming language for penetration testing. Scripting skills are essential to automate and speed up scanning, perform fuzzing, as well as launch exploits. Evening labs each day are used to allow for additional time practicing the techniques learned.

Who Should Attend:

- Network and Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers

Day two jumps into accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, DHCP, 802.1X, CDP, VOIP, ARP, SNMP, and others. Day three takes a look at very successful attacks against Windows domain environments. Topics include breaking out of RDP sessions, performing MitM attacks against Kerberos and RDP, downgrading authentication protocols, harvesting passwords in unusual locations, and many others. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect code execution in debuggers, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls, such as ASLR and DEP. Client-side attacks are also covered, and you will understand how to perform vulnerability discovery and exploit development. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Bootcamp

This program has extended hours.

Evening Bootcamp Sessions:
5:15pm - 7:00pm (Days 1-5)

From the Author

As a perpetual student of information security, I am excited to offer this course on advanced penetration testing. Often, when conducting an in-depth penetration test, we are faced with situations that require unique or complex solutions to successfully pull off an attack, mimicking the activities of increasingly sophisticated real-world attackers. Without the skills to do so, you may miss a major vulnerability or not properly assess its business impact. Target system personnel are relying on you to tell them whether or not an environment is secured. Attackers are almost always one step ahead and are relying on our nature to become complacent with controls we work so hard to deploy. This course was written to keep you from making mistakes others have made, teach you cutting-edge tricks to thoroughly evaluate a target, and provide you with the skills to jump into exploit development. Contact me at stephen@deadlisting.com if you have any questions about the course! -Stephen Sims

What Students Are Saying

"Up-to-date hands-on content left me feeling confident I could start to apply my new skills back in the office."

-Rafe Pilling,
Dell SecureWorks

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

Security 660 Course Content

660.1 Hands On: Network Attacks for Penetration Testers*

Day one serves as an advanced network attack module, building on knowledge gained from SEC560: Network Penetration Testing and Ethical Hacking. The focus for day one will be on obtaining access to the network; manipulating the network to gain an attack position for eavesdropping and attacks, and for exploiting network devices; leveraging weaknesses in network infrastructure; and taking advantage of client frailty.

Topics: Bypassing Network Admission Control; Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD5 Authentication; IEEE 802.1X authentication; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; Exploiting OSPF Authentication to Inject Malicious Routing Updates; Using Evilgrade to Attack Software Updates; Overcoming SSL Transport Encryption Security with Sslstrip; Remote Cisco Router Configuration File Retrieval

660.2 Hands On: Crypto, Attacking the Domain, and Escaping Restricted Desktops*

Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We begin by building some fundamental knowledge on how ciphers operate without getting bogged down in complex mathematics, and then we move on to techniques for identifying, assessing, and attacking real-world crypto implementations. We finish the module with lab exercises that allow you to practice your new found crypto attack skill set against reproduced real-world application vulnerabilities.

Topics: Low Profile Enumeration of Large Windows Environments Without Heavy Scanning; Strategic Target Selection; Remote Desktop Protocol (RDP) and Man-in-the-Middle Attacks; Windows Network Authentication Attacks (e.g., MS-Kerberos, NTLMv2, NTLMv1, LM); Windows Network Authentication Downgrade; Discovering and Leveraging MS-SQL for Domain Compromise Without Knowing the sa Password; Metasploit Tricks to Attack Fully Patched Systems; Utilize LSA Secrets and Service Accounts to Dominate Windows Targets; Dealing with Unguessable/Uncrackable Passwords; Leveraging Password Histories; Gaining Graphical Access; Expanding Influence to Non-Windows Systems

660.3 Hands On: Python, Scapy, and Fuzzing*

Day three brings together multiple skill sets needed for creative analysis in penetration testing. The day starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation. Using Scapy, we examine techniques for transmitting and receiving network traffic beyond what canned tools can accomplish, including IPv6.

Topics: Becoming Familiar with Python Types; Leveraging Python Modules for Real-World Pen Tester Tasks; Manipulating Stateful Protocols with Scapy; Using Scapy to Create a Custom Wireless Data Leakage Tool; Product Security Testing; Using Taof for Quick Protocol Mutation Fuzzing; IDAPro; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring While Fuzzing with Sulley; Leveraging Microsoft Word Macros for Fuzzing .docx files; Block-Based Code Coverage Techniques Using Paimei

660.4 Hands On: Exploiting Linux for Penetration Testers*

Day Four begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. These topics are important to understand for anyone performing penetration testing at an advanced level. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. We will take a look at the Linux OS from an exploitation perspective and discuss the topic of privilege escalation. We continue by describing how to look for SUID programs and other likely points of vulnerabilities and misconfigurations. The material will focus on techniques that are critical to performing penetration testing on Linux applications.

Topics: Stack and Dynamic Memory Management and Allocation on the Linux OS; Disassembling a Binary and Analyzing x86 Assembly Code; Performing Symbol Resolution on the Linux OS; Identifying Vulnerable Programs; Code Execution Redirection and Memory Leaks; Return Oriented Programming (ROP); Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Defeating Stack Protection on the Linux OS; Defeating ASLR on the Linux OS

660.5 Hands On: Exploiting Windows for Penetration Testers*

On day five we start off with covering the OS security features (ALSR, DEP, etc.) added to the Windows OS over the years, as well as Windows specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS. We look at fuzzing skills, which are required to test remote services, such as TFTP and FTP, for faults. Once a fault is discovered, the student will work with Immunity Debugger to turn the fault into an opportunity for code execution and privilege escalation. Advanced stack-based attacks, such as disabling data execution prevention (DEP) and heap spraying for browser-based applications, are covered. Client-side exploitation will be introduced, as it is a highly common area of attack. The day will end with a look at shellcode and the differences between Linux and Windows.

Topics: The State of Windows OS Protections on XP, Vista, 7, Server 2003 and 2008; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS protections added to Windows; Dynamic and Static Fuzzing on Windows Applications or Processes; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Return Oriented Programming (ROP); Windows 7 and Windows 8; Porting Metasploit Modules; Client-side Exploitation; Windows and Linux Shellcode

660.6 Hands On: Capture the Flag*

This day will serve as a real-world challenge for students, requiring them to utilize skills obtained throughout the course, think outside the box, and solve simple-to-complex problems. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

*This course is available to Security 660 participants only.

SANS Senior Instructor

Stephen Sims

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works at Wells Fargo in San Francisco as a security architect. He has spent several years performing exploit development and reverse engineering. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC710: Advanced Exploit Development, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification, as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

Forensics 408

Computer Forensic Investigations - Windows In-Depth

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Chad Tilbury

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threat, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to piece together what happened in these cases.

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008), you will be exposed to well-known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

FOR408: COMPUTER FORENSIC INVESTIGATIONS - WINDOWS IN-DEPTH is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course with SANS we recommend that you start here.

Who Should Attend:

- Information technology professionals
- Incident Response Team Members
- Law enforcement officers, federal agents, or detectives
- Media Exploitation Analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

You will receive with this course: Free SANS Investigative Forensic Toolkit (SIFT) Essentials

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.

- **One Tableau T35es Write Blocker (Read-Only)**
- **IDE Cable/Adapters**
- **SATA Cable/Adapters**
- **FireWire and USB Cable Adapters**
- **Forensic Notebook Adapters (IDE/SATA)**

What Students Are Saying

"I've been doing forensics for almost 4 years. FOR408 is not a newbie course. Without 408, an investigator will be missing an incredible wealth of needed knowledge, and a disciplined methodology. Instead of 'looking for evil' by the time you finish the first run through the taught methodology, you will have found and proven 'the evil."

-Kris Courter,
Applied Signal Technology, Inc.

From the Author

SANS COMPUTER FORENSICS GRADUATE THWARTS BANK HEIST.
Headlines similar to these are now a reality, as former students have emailed me regularly about how they were able to use their digital forensic skills in very real situations. Graduates of Computer Forensics Windows In-Depth are the front line troops deployed when you need accurate digital forensic and media exploitation analysis. From analyzing terrorist laptops to investigating insider intellectual property theft and fraud, SANS digital forensic graduates are battling and winning the war on crime and terror. Graduates have directly contributed to solving some of the toughest cases out there because they learn how to conduct analysis and run investigations properly. Knowing that this course places the correct methodology and knowledge in the hands of responders who thwart the plans of criminals or foreign attacks brings me great comfort. Graduates are doing it. Daily. I am proud that the Computer Forensics Investigations-Windows In-Depth course at SANS helped prepare them to fight and solve crime. -Rob Lee

Forensics
http://computer-forensics.sans.org

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

408.1 Hands On: Digital Forensics Fundamentals and Evidence Acquisition*

Securing or "Bagging and Tagging" digital evidence can be tricky. Each computer forensic examiner should be familiar with different methods of successfully acquiring it maintaining the integrity of the evidence. Starting with the foundations from law enforcement training in proper evidence handling procedures, you will learn firsthand the best methods for acquiring evidence in a case. You will utilize the Tableau T35es write blocker, part of your SIFT Essentials kit, to obtain evidence from a hard drive using the most popular tools utilized in the field. You will learn how to utilize toolkits to obtain memory, encrypted or unencrypted hard disk images, or protected files from a computer system that is running or powered off.

Topics: Purpose of Forensics: Investigative Mindset, Focus on the Fundamentals; Evidence Fundamentals: Admissibility, Authenticity, Threats against Authenticity; Reporting and Presenting Evidence: Taking Notes, Report Writing Essentials, Best Practices for Presenting Evidence: Tableau Write Blocker Utilization, Access Data's FTK Imager, Access Data's FTK Imager Lite; Evidence Acquisition Basics; Preservation of Evidence: Chain of Custody, Evidence Handling, Evidence Integrity

408.2 Hands On: Core Windows Forensics Part I — String Search, Data Carving, and Email Forensics

You will learn how to recover deleted data from the evidence, perform string searches against it using a word list, and begin to piece together the events that shaped the case. Today's course is critical to anyone performing digital forensics to learn the most up-to-date techniques of acquiring and analyzing digital evidence. Email Forensics: Investigations involving email occur every day. However, email examinations require the investigator to pull data locally, from an email server, or even recover web-based email fragments from temporary files left by a web browser. Email has become critical in a case and the investigator will learn the critical steps needed to investigate Outlook, Exchange, Webmail, and even Lotus Notes email cases.

Topics: Recover Deleted Files: Automated Recovery, String Searches, Dirty Word Searches; Email Forensics: How Email Works, Locations, Examination of Email, Types of Email Formats; Microsoft Outlook/Outlook Express; Web-Based Mail; Microsoft Exchange; Lotus Notes; E-mail Analysis, E-mail Searching and Examination

408.3 Hands On: Core Windows Forensics Part II — Registry and USB Device Analysis

Each examiner will learn how to examine the Registry to obtain user profile data and system data. The course will also teach each forensic investigator how to show that a specific user performed key word searches, ran specific programs, opened and saved files, and list the most recent items that were used. Finally, USB Device investigations are becoming more and more a key part of performing computer forensics. We will show you how to perform in-depth USB device examinations on Windows 7, Vista, and Windows XP machines.

Topics: Registry Forensics In-Depth;Registry Basics; Core System Information; User Forensic Data; Evidence of Program Execution; Evidence of File Download; USB Device Forensic Examinations

408.4 Hands On: Core Windows Forensics Part III — Artifact and Log File Analysis

Suspects unknowingly create hundreds of files that link back to their actions on a system. Learn how to examine key files such as link files, the windows prefetch, pagefile/system memory, and more. The latter part of the section will center on examining the Windows log files and the usefulness in both simple and complex cases.

Topics: Memory, Pagefile, and Unallocated Space Analysis; Forensicating Files Containing Critical Digital Forensic Evidence; Windows Event Log Digital Forensic Analysis

408.5 Hands On: Core Windows Forensics Part IV — Web Browser Forensics

Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what an individual did while surfing via their Web browser. The results will give you pause the next time you use the web.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox

408.6 Hands On: Digital Forensic Challenge and Mock Trial

Windows Vista/7 Based Digital Forensic Challenge. There has been a murder-suicide and you are the investigator assigned to process the hard drive. This day is a capstone for every artifact discussed in the class. You will use this day to solidify the skills you have learned over the past week.

Topics: Digital Forensic Case; Mock Trial

*This course is available to Forensics 408 participants only.

SANS Certified Instructor

Chad Tilbury

Chad Tilbury has spent over ten years responding to computer intrusions and conducting forensic investigations. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and more recently as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, and CISSP certifications. He is currently a consultant specializing in incident response, E-Discovery, and computer forensics.

Forensics 508

Advanced Computer Forensic Analysis & Incident Response

Course Relaunch – Brand New!

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits • Laptop Required
Instructors: Rob Lee & Richard Salgado (1/2 of Day 5 – Legal Portion)

Over the past two years, we have seen a dramatic increase in sophisticated attacks against organizations. Cyber-attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data resulting in millions of dollars stolen. Hackivist groups attacking government and Fortune500 companies are becoming bolder.

FOR508: ADVANCED COMPUTER FORENSIC ANALYSIS AND INCIDENT RESPONSE will give you help you start to become a master of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, the advanced persistent threat, and complex digital forensic cases.

This course utilizes as uses the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. The free **SIFT Workstation** can match any modern forensic tool suite. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Who Should Attend:

- Incident response team members
- Experienced digital forensic analysts
- Law Enforcement Officers, Federal agents, or detectives
- Media exploitation analysts
- Red team members, penetration testers, and exploit developers
- Information security professionals

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME.

This course includes a Free SANS Investigative Forensic Toolkit (SIFT) Advanced

As part of this course you will receive the ***SANS Investigative Forensic Toolkit (SIFT) Advanced***. The SIFT Advanced Toolkit consists of:

- **SIFT Workstation Virtual Machine w/ plenty of hands on exercises in class**
- **F-RESPONSE TACTICAL**
  - **TACTICAL enables investigators to access physical drives and physical memory of a remote computer via the network**
  - **Able to use any tool to parse the live remote system including the SIFT Workstation**
  - **Perfect for Intrusion Investigations and Data Breach Incident Response situations**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Course DVD loaded with case examples, tools, and documentation**

From the Author

"There are people smarter than you, they have more resources than you, and they are coming for you. Good luck with that." Matt Olney said when describing the Advanced Persistent Threat. He was not joking. The results over the past several years clearly indicate that hackers employed by nation states and organized crime are racking up success after success. The Advanced Persistent Threat has compromised hundreds of organizations. Organized crime utilizing botnets are exploiting ACH fraud daily. Similar groups are penetrating banks and merchants stealing credit card data daily. Fortune 500 companies are beginning to detail data breaches and hacks in their annual stockholders reports.

The enemy is getting better, bolder, and their success rate is impressive.

We can stop them. We need to field more sophisticated incident responders and digital forensic investigators. We need lethal digital forensic experts that can detect and eradicate advanced threats immediately. A properly trained incident responder could be the only defense your organization has left in place during a compromise. Forensics 508: Advanced Computer Forensic Analysis and Incident Response is crucial training for you to become a lethal forensicator to step up to these advanced threats. The enemy is good. We are better. This course will help you become one of the best. -Rob Lee

Digital Forensics and Incident Response
http://computer-forensics.sans.org

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

508.1 Hands On: Windows File Systems – In-Depth*

File systems are the core to your understanding of computer forensics. As every forensic tool utilizes this knowledge, you will learn how hard drives are used to store data from the partitioning to how file systems work. Utilizing real-world intrusion scenarios, you will see how to respond to complex attacks through teaching you the background of how data is stored on a variety of operating systems. This knowledge will allow you to see beyond most anti-forensic techniques allowing you to gain the advantage while responding to breaches in your organization.

Topics: Computer Forensics for Incident Responders; Incident Response and Forensics Methodology; File System Essentials; Windows FAT and exFAT File Systems In-Depth; Windows NTFS File Systems In-Depth

508.2 Hands On: Incident Response and Memory Analysis*

The section starts focusing on advanced acquisition techniques teaching you to acquire system memory, volatile data, and a remote live drive images from a compromised systems. Forensic analysts responding to enterprise intrusions must also be able to scale their examinations from the traditional one analyst to one machine examination to one analyst to 1,000 machines. This main section of this section's material will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills in your security armory.

Topics: Windows Incident Response; Mounting Images for Examinations; Remote and Enterprise Forensic Examinations; Memory Acquisition and Analysis; Memory Analysis Techniques with Redline; Live Memory Forensics; Advanced Memory Analysis with Volatility

508.3 Hands On: Timeline Analysis*

Over the past 3 years, a renascence has occurred for the tool development for timeline analysis. SANS spearheaded the research and development by sponsoring some of the new tools that have been created recently, specifically log2timeline. As a result of the recent developments, many professionals have turned to timeline analysis as one of their core tools and capabilities. This section will step you through the two primary methods of creating and analyzing timelines created during advanced cases. Exercises will not only show how each analyst how to create a timeline, but key methods on how to use them effectively in their cases.

Topics: Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Windows Time Rules (File Copies vs. File Moves); Filesystem Timeline Creation using Sleuthkit and fls; Super Timeline Creation and Analysis; Super Timeline Artifact Rules; Timeline Creation with log2timeline; Super Timeline Analysis

508.4 Hands On: Filesystem Forensic Analysis*

A major criticism of digital forensic professionals surrounds that many tools simply require a few mouse clicks to have the tool automatically recover data for evidence. This "push button" mentality has led to inaccurate case results in the past few years in high profile cases such as the Casey Anthony Murder trial. You will stop being reliant on "push button" forensic techniques as we cover how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to accomplish it by-hand and show how automated tools should be able to recover the same data.

Topics: Windows XP Restore Point Analysis; VISTA; Windows 7; Server 2008 Shadow Volume Copy Analysis; File System and Data Layer Examination; Metadata Layer Examination; File Name Layer Examination; File Sorting and Hash Comparisons; Indicator of Compromise Analysis and Creation

508.5 Hands On – Part 1: Intrusion Analysis*

Focus: Finding Unknown Malware, Detecting Anti-Forensics Techniques, Step-By-Step Methodology to Analyze and Solve Challenging Cases

Note this is a half day section. This advanced session will demonstrate techniques used by first responders that they use to discover malware or artifacts related to an intrusion when very little information to their capabilities or hidden location. We will discuss techniques to help funnel the possible candidates down to the most likely candidate for our evil malware trying to hide on the system. The section concludes with a step-by-step approach on how to handle investigations surrounding the most difficult cases. You will learn the best ways to approach intrusion and spear phishing attack cases.

Topics: Step-by-Step Finding Unknown Malware; Anti-Forensics Detection Methodologies; Methodology to Analyze and Solve Challenging Cases

508.5 Hands On – Part 2: Computer Investigative Law For Forensic Analysts*

Focus: As a team lead, you will need to know where legal land mines might exist. This half day of material focuses on what a technical lead must know before they begin any digital forensic case to protect you and your team during an investigation.

Note this is a half day section. Learn to investigate incidents while minimizing the risk for legal trouble. This course is designed not for management, but for the Digital Forensic and Incident Response team leaders in charge of an investigation. The content focuses on challenges that every lead investigator needs to understand before, during, and post investigation. Since most investigations could potentially bring a case to either a criminal or civil courtroom, it is essential for you to understand how to perform a computer-based investigation legally and ethically.

Topics: Who Can Investigate and Investigative Process Laws; Evidence Acquisition/Analysis/Preservation Laws and Guidelines; Laws Investigators Should Know; Forensic Reports and Testimony

508.6 Hands On: The Intrusion Forensic Challenge*

This brand new exercise, updated in 2012, brings together some of the most exciting techniques learned from earlier in the week and leverage your new skills in a case that simulates an attack by an advanced adversary such as the APT. You will walk out of the course today with hands-on experience investigating scenarios put together by a cadre of experts who have had hands on experience fighting advanced threats today such as the APT.

Topics: Real-World Compromise Based on APT Tactics and Malware; Timeline Creation , String Searches; Unallocated Space Analysis; Data Recovery And Analysis; Finding Malware; Find Data Exfiltration; Find Evidence of Lateral Movement; Find Evidence of Anti-Forensics

*This course is available to Forensics 508 participants only.

SANS Faculty Fellow

Rob Lee

Rob Lee is an entrepreneur and consultant in the Washington D.C. area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years' experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team computer crime investigations and incident response. Over the next 7 years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book *Know Your Enemy*, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report *M-Trends: The Advanced Persistent Threat*. Rob frequently contributes articles at the SANS Blog http://computer-forensics.sans.org.

Forensics 563

Mobile Device Forensics

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required
Instructors: Heather Mahalik & Terrance Maguire

Mobile device forensics is a rapidly evolving field, creating exciting opportunities for practitioners in corporate, criminal, and military settings. Designed for students who are both new to and already familiar with mobile device forensics, this hands-on course provides the core knowledge and skills that a Digital Forensic Investigator needs to process cell phones, PDAs, and other mobile devices. Using state-of-the art tools, you will learn how to forensically preserve, acquire and examine data stored on mobile devices and utilize the results for internal investigations or in civil/criminal litigation. This course covers techniques and tools in the context of an overall forensic methodology, providing you with the ability to obtain and utilize digital evidence on mobile devices. In addition, by teaching lessons learned from years of experience, we will help you learn how to handle common challenges in the field.

With the increasing prevalence of mobile devices, Digital Forensic Investigators are encountering them in a wide variety of cases. Investigators within organizations can find stolen data and incriminating communications on devices used by rogue employees. In civil and criminal cases, investigators can extract useful evidence from mobile devices, can get a clearer sense of which individuals were in cahoots, and can even show the location of key suspects at times of interest. IT auditors, managers, and lawyers all need to understand the vast potential of mobile device forensics. Because mobile devices can contain details about who was doing what, where and when, their usefulness as a source of information in an investigation should never be underestimated.

Throughout this course we provide practical, hands-on exercises to give you ample opportunities to explore mobile devices and the data they contain.

By guiding you through progressively more intensive exercises with mobile devices, we familiarize you with the inner workings of these devices and show you the benefits and limitations of various approaches and tools. We not only demonstrate state-of-the-art mobile forensic tools and techniques, we peel back the layers of digital evidence on mobile devices to show what is going on behind the scenes. In this way, you obtain a deeper knowledge of the information you rely on when investigating cases involving mobile devices. This combination of teaching skills and knowledge will enable you to resolve investigations. The capstone exercise at the end of this course is designed to hone your mobile device forensics skills, and help you to apply them to an actual investigation.

From the Author

Mobile devices are becoming ubiquitous, delivering powerful technology into our pockets, keeping us connected wherever we are. Individuals store personal data on their PDAs, parents use GPS enabled devices to track their children, hospitals use handhelds to access medical data and support patient care, and companies give each employee a Blackberry to support their business. Being so closely tied to an individual's daily movements and activities, these portable devices are creating new security risks while providing valuable sources of evidence.

Corporate spies and data thieves have been caught using their mobile devices. Organized criminal groups have been infiltrated and unraveled through their use of mobile devices. A killer's mobile device showed his whereabouts at the time of the crime, and inadvertently recorded the sounds of his brutal acts. Sex offenders have video taped their crimes using mobile devices. Terrorists have been tracked down using traces of data recovered from cell phones attached to improvised explosive devices. Mobile devices have helped rescue kidnap victims before they came to harm. Many vice officers and courts consider mobile devices as an integral part of drug trafficking and dealing.

Using the proper methodology and tools, you can extract useful evidence from mobile devices and obtain records from network service providers to help avert an attack, further an investigation, or solve a crime. - Eoghan Casey

Who Should Attend:

- Information security professionals
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in mobile device forensics
- Information technology auditors

Digital Forensics and Incident Response
http://computer-forensics.sans.org

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

563.1 Hands On: Fundamentals of Mobile Device Forensics

Review of technology from a forensic perspective, forensic handling of mobile devices, and forensic acquisition and analysis methods and techniques. Hands-on introduction to leading mobile device forensic tools, including Cellebrite and XRY. Perform logical acquisitions, physical acquisitions and manual examination of mobile devices. Understand about the types of evidence on mobile devices and how to interpret the various data formats. Learn about the strengths and limitations of mobile device forensic tools, and how to overcome in-field challenges.

Topics: Mobile Network Investigations; Mobile Device Forensics; Forensic Handling of Mobile Devices; Forensic Documentation; Interacting with Mobile Devices; Hands-on Exercises

563.2 Hands On: Cell Phone Forensics & SIM Card Examination

Perform forensic acquisition and examination of SIM cards. Use mobile forensic tools, including BitPim, to acquire and analyze data from a variety of CDMA and GSM devices, including Motorola, Samsung and LG. Recover deleted data by delving into memory contents and extracting data structures on mobile devices. Compare forensic acquisition tools and validate completeness and accuracy of results.

Topics: Accessing Mobile Devices; Mobile Device Operating Systems; Mobile Device File Systems; Forensic Processing of SIM Cards; Forensic Examination of Data; Hands-on Exercises

563.3 Hands On: iPhone and Android Forensics

Smart phones are becoming more widely used and can be a valuable source of evidence in a variety of investigations. These portable devices can contain details about an individual's communications, contacts, calendar, online activities, and whereabouts at specific times. The third day of the course covers current effective practices for acquiring and examining data on iPhone/iPad, Android and Windows Mobile devices using both commercial and open source tools.

Topics: Forensic Acquisition Tools for Mobile Devices; Forensic Examination of Logical Data; Forensic Analysis of Internet Activities on Mobile Devices; Forensic Reconstruction of Activities on Mobile Devices; Hands-on Exercises

563.4 Hands On: Windows Mobile, Blackberry, Nokia, and Forensics

Apply forensic principles and tools to Blackberry and Nokia systems. Hands-on exploration of Blackberry and Nokia devices and data storage using various utilities and forensic tools. Perform logical and physical acquisitions and examinations of Nokia devices, including the use of Flasher boxes.

Topics: Forensic Acquisition of Physical Memory; Forensic Acquisition of Using Flasher Boxes; Forensic Examination of Physical Memory; Hands-on Exercises

563.5 Hands On: GPS Forensics and Mobile Device Forensic Challenge

Forensic acquisition and examination of GPS navigation devices, including location information saved on smart phones and EXIF data in multi-media files. Familiarization with other forensic acquisition and analysis techniques. Putting the pieces of a case together and presenting results in reports and testimony. A realistic hands-on investigative scenario bringing together lessons and techniques learned throughout the course.

Topics: Advanced Mobile Device Forensics Overview; Bringing It All Together; The Mobile Device Forensic Challenge; Hands-on Exercise

Throughout this course, we provide practical, hands-on exercises to give you ample opportunities to explore mobile devices and the data they contain.

*This course is available to Forensics 563 participants only.

SANS Certified Instructor

Heather Mahalik

Heather Mahalik is a senior digital forensics analyst at Basis Technology. As the on-site team lead, she uses her experience to manage the cell phone exploitation team and supports media and cell phone forensics efforts in the US government. Heather has worked in digital forensics for almost ten years and has performed thousands of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices, and portable media. Previously, Heather worked as a forensic examiner for Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. She has authored papers, presented at leading conferences, and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field. Heather's background is based on media forensics, and she currently specializes in BlackBerry, Nokia, knock-off, and iOS Forensics.

SANS Certified Instructor

Terrance Maguire

Terrance Maguire is a partner at cmdLabs. He has nearly twenty years of experience in physical and digital forensic investigations, has developed and led training programs in varied areas of law enforcement and digital evidence, and has experience implementing counterintelligence intrusion detection programs. His prior experience includes serving as a senior-level forensic computer analyst for the U.S. State Department. As a cyber operations specialist for the Department of Defense, he implemented network surveillance, network packet analysis, wireless surveys, and intrusion detection. In addition, at the Defense Computer Investigations Training Program (DCITP), Terrance developed and presented a broad range of instruction to federal law enforcement in the area of cybercrime. He served as a forensic detective with the Chesterfield County Police Department in Virginia. Subsequently, as a forensic scientist for the Virginia Division of Forensic Science, he conducted bloodstain pattern analysis in criminal cases and testified in court as an expert witness and he was the principal instructor at the Virginia Forensic Science Academy. He is a professorial lecturer at the George Washington University where he teaches graduate-level courses focusing on incident response and computer intrusion investigations involving network-based attacks.

Forensics 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Lenny Zeltser

Expand your capacity to fight malicious code by learning how to analyze bots, worms, and trojans.

LEARN R.E.M

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs-spyware, bots, trojans, etc.-that target or run on Microsoft Windows. This training also looks at reversing Web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

Learn Malware Analysis to Improve Incident Response and Forensics Skills

This unique course provides a rounded approach to reverse-engineering by covering both behavioral and code phases of the analysis process. As a result, the course makes malware analysis accessible even to individuals with a limited exposure to programming concepts. The materials do not assume that the students are familiar with malware analysis; however, the complexity of concepts and techniques increases as the course progresses.

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software. It also assists in determining how to contain the incident and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware present on compromised systems, including how to establish indicators of compromise (IOCs) for scoping and containing the intrusion.

Who Should Attend:

- Incident response team members
- Experienced digital forensic analysts
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Red team members, penetration testers, and exploit developers
- Application and software developers
- Information security professionals

A Methodical Approach to Reverse-Engineering

The course begins by covering fundamental aspects of malware analysis. You'll learn how to set up an inexpensive and flexible laboratory for understanding the inner-workings of malicious software and will understand how to use the lab for exploring characteristics of real-world malware. Then you'll learn to examine the program's behavioral patterns and code. Afterwards, you'll experiment with reverse-engineering compiled Windows executables and browser-based malware.

The course continues by discussing essential x86 assembly language concepts. You'll examine malicious code to understand the program's key components and execution flow. Additionally, you'll learn to identify common malware characteristics by looking at Windows API patterns and will examine excerpts from bots, rootkits, keyloggers, and downloaders. You'll understand how to work with PE headers and handle DLL interactions. Furthermore, you'll learn tools and techniques for bypassing anti-analysis capabilities of armored malware, experimenting with packed executables and obfuscated browser scripts.

Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents. Such documents act as a common infection vector and need to be understood by enterprises concerned about both large-scale and targeted attacks. The course also explores memory forensics approaches to examining rootkits. Memory-based analysis techniques also help understand the context of an incident involving malicious software.

Hands-On Training for Malware Analysis and Reversing

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine (REMnux) that includes tools for examining and interacting with malware.

Digital Forensics and Incident Response
http://computer-forensics.sans.org

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

610.1 Hands On: Malware Analysis Fundamentals*

Day one lays the groundwork for the course by presenting the key tools and techniques malware analysts use to examine malicious programs. You will learn how to save time by exploring malware in two phases. Behavioral analysis focuses on the specimen's interactions with its environment, such as the registry, the network, and the file system; code analysis focuses on the specimen's code and makes use of a disassembler and a debugger. You will learn how to build a flexible laboratory to perform such analysis in a controlled manner and will set up such a lab on your laptop. Also, we will jointly analyze a malware sample to reinforce the concepts and tools discussed throughout the day.

610.2 Hands On: Additional Malware Analysis Approaches*

Day two builds upon the fundamentals introduced earlier in the course, and discusses techniques for uncovering additional aspects of the malicious program's functionality. You will learn about packers and the analysis approaches that may help bypass their defenses. You will also learn how to patch malicious executables to change their functionality during the analysis without recompiling them. You will also understand how to redirect network traffic in the lab to better interact with malware, such as bots and worms, to understand their capabilities. You will also experiment with the essential tools and techniques for analyzing web-based malware, such as malicious browser scripts and Flash programs.

610.3 Hands On: Malicious Code Analysis*

Day three focuses on examining malicious executables at the assembly level. You will discover approaches for studying inner-workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. The day begins with an overview of key code reversing concepts and presents a primer on essential x86 assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The second half of the day discusses how malware implements common characteristics, such as keylogging, packet spoofing, and DLL injection, at the assembly level. You will learn how to recognize such characteristics in malicious Windows executables.

610.4 Hands On: Self-Defending Malware*

Day four begins by covering several techniques malware authors commonly employ to protect malicious software from being analyzed, often with the help of packers. You will learn how to bypass analysis defenses, such as structured error handling for execution flow, PE header corruption, fake memory breakpoints, tool detection, integrity checks, and timing controls. It's a lot of fun! As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises. The course completes by revising the topic of web-based malware, showing additional tools and approaches for analyzing more complex malicious scripts written in VBScript and JavaScript.

610.5 Hands On: Malicious Documents and Memory Forensics*

Day five represents the latest addition to the FOR610 course, discussing the more recent malware reverse-engineering approaches adopted by malware analysts. The topics covered during this day include analyzing malicious Microsoft Office and Adobe PDF document files. Exercises that demonstrate these techniques make use of tools, such as OfficeMalScanner, Offvis, PDF-parser, and PDF StructAzer. Another major topic covered during this day is the reversing of malicious Win32 executables using memory forensics techniques. This topic is explored with the help of tools, such as Volatility, malfind, moddump, and others, and brings us deeper into the world of user- and kernel-mode rootkits.

*This course is available to Forensics 610 participants only.

REM course on YouTube

http://www.youtube.com/watch?v=5AFdZ0v23YA

SANS Senior Instructor

Lenny Zeltser

Lenny Zeltser is a seasoned IT professional with a strong background in information security and business management. As a director at Radiant Systems (now part of NCR Corporation), he focuses on safeguarding IT environments of small and midsize businesses worldwide. Before Radiant, he led an enterprise security consulting team at a major IT hosting provider. Lenny's most recent work has focused on malware defenses and cloud-based services. He teaches how to analyze and combat malware at the SANS Institute, where he is a senior faculty member. He also participates as a member of the board of directors at the SANS Technology Institute and volunteers as an incident handler at the Internet Storm Center. Lenny frequently speaks on security and related business topics at conferences and industry events, writes articles, and has co-authored books on forensics, network security, and malicious software. He is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania. Lenny writes at blog.zeltser.com and twitter.com/lennyzeltser. More details about his projects are at www.zeltser.com.

Management 414

SANS® +S™ Training Program for the CISSP® Certification Exam

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 7:00pm (Day 1) • 8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6) • 46 CPE/CMU Credits
Laptop NOT Required • Instructor: Eric Conrad

The SANS® +S™ Training Program for the CISSP® Certification Exam will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

Domain 1: Access Controls
Domain 2: Telecommunications and Network Security
Domain 3: Information Security Governance & Risk Management
Domain 4: Software Development Security
Domain 5: Cryptography
Domain 6: Security Architecture and Design
Domain 7: Security Operations
Domain 8: Business Continuity and Disaster Recovery Planning
Domain 9: Legal, Regulations, Investigations and Compliance
Domain 10: Physical (Environmental) Security

Each domain of knowledge is dissected into its critical components. Every component is discussed in terms of its relationship to other components and other areas of network security. After completion of the course, the student will have a good working knowledge of the 10 domains of knowledge and, with proper preparation, be ready to take and pass the CISSP® exam.

Who Should Attend:

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 Domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified. Reinforce what you learned in training and prove your skills and knowledge with a GISP certification.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of Resume
- Passing the CISSP® 250 multiple-choice question exam with a scaled score of 700 points or greater
- Submitting a properly completed and executed Endorsement Form
- Period Audit of CPEs to maintain the credential

Bootcamp

This program has extended hours.

Evening Bootcamp Sessions:
5:00pm - 7:00pm (Days 1-5)

Morning Bootcamp Sessions:
8:00am - 9:00am (Days 2-6)

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 72.***

You Will Receive With This Course:

Free "CISSP® Study Guide" by Eric Conrad, Seth Misenar, and Joshua Feldman.

From the Author

The CISSP® certification has been around for almost ten years and covers security from a 30,000 foot view. CISSP® covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the CISSP® 10 domains of knowledge to life. By explaining important topics with stories, examples, and case studies, the practical workings of this information can be discovered. I challenge you to attend the SANS CISSP® training course and find the exciting aspect of the ten domains of knowledge. -Dr. Eric Cole

GIAC Certification
www.giac.org

DoD 8570 Required
www.sans.org/8570

What Students Are Saying

"This course was invaluable as a preparation tools for the CISSP exam."
-Matthew Slayton, Liberty Mutual Insurance

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

Management 414 Course Content

414.1 Introduction and Access Control*

Learn the specific requirements needed to obtain the CISSP® certification. General security principles needed in order to understand the 10 domains of knowledge are covered in detail with specific examples in each area. The first of 10 domains, Access Control is discussed using real-world scenarios to illustrate the critical points. Access control which includes AAA (authentication, authorization and accountability) will be covered with an emphasis on controlling access to critical systems.

Topics: Overview of Certification; Description of the 10 Domains: Introductory Material; Domain 1: Access Controls

414.2 Telecommunications*

Understanding network communications is critical to building a solid foundation for network security. All aspects of network security will be examined to include routing, switches, key protocols and how they can be properly protected on the network. The telecommunications domain covers all aspects of communication and what is required to provide an infrastructure that has embedded security.

Topics: Domain 2: Telecommunications and Network Security

414.3 Information Security Governance & Risk Management and Software Development Security*

In order to secure an organization, it is important to understand the critical components of network security and issues that are needed in order to manage security in an enterprise. Security is all about mitigating risk to an organization. The core areas and methods of calculating risk will be discussed. In order to secure an application it is important to understand system engineering principles and techniques. Software development life cycles are examined, including examples of what types of projects are suited for different life cycles.

Topics: Domain 3: Information Security Governance & Risk Management; Domain 4: Software Development Security

414.4 Cryptography and Security Architecture & Design*

Cryptography plays a critical role in the protection of information. Examples showing the correct and incorrect ways to deploy cryptography, and common mistakes made, will be presented. The three types of crypto systems are examined to show how they work together to accomplish the goals of crypto. A computer consists of both hardware and software. Understanding the components of the hardware, how they interoperate with each other and the software, is critical in order to implement proper security measures. We examine the different hardware components and how they interact to make a functioning computer.

Topics: Domain 5: Cryptography; Domain 6: Security Architecture and Design

414.5 Security Operations and Business Continuity & Disaster Recovery Planning*

Non-technical aspects of security are just as critical as technical aspects. Security operations security focuses on the legal and managerial aspects of security and covers components such as background checks and non-disclosure agreements, which can eliminate problems from occurring down the road. Business continuity planning is examined, comparing the differences between BCP and DRP. A life cycle model for BCP/DRP is covered giving scenarios of how each step should be developed.

Topics: Domain 7: Security Operations; Domain 8: Business Continuity and Disaster Recovery Planning

414.6 Legal, Regulations, Investigations and Compliance & Physical (Environmental) Security*

If you work in network security, understanding the law is critical during incident responses and investigations. The common types of laws are examined, showing how critical ethics are during any type of investigation. If you do not have proper physical security, it doesn't matter how good your network security is; someone can still obtain access to sensitive information. In this section various aspects and controls of physical security are discussed.

Topics: Domain 9: Legal, Regulations, Investigations and Compliance; Domain 10: Physical (Environmental) Security

*This course is available to Management 414 participants only.

SANS Certified Instructor

Eric Conrad

Certified SANS instructor Eric Conrad is lead author of the book The CISSP Study Guide. Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now president of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com.

Management 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program • Mon, Sept 17 - Fri, Sept 21
9:00am - 6:00pm (Days 1-4) • 9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits • Laptop NOT Required
Instructor: Stephen Northcutt

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to manage security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to US government managers and supporting contractors.

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security + 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

There are three goals for this course and certification:

- Establish a minimum standard for IT security knowledge, skills, and abilities. In a nutshell, this course covers all of the non-operating system topics that are in SANS Security Essentials, though not to the same depth. The goal is to enable managers and auditors to speak the same language as system, security, and network administrators.
- Establish a minimum standard for IT management knowledge, skills, and abilities. I keep running into managers that don't know TCP/IP, and that is OK; but then they don't know how to calculate total cost of ownership (TCO), leaving me quietly wondering what they do know.
- Save the up-and-coming generation of senior and rapidly advancing managers a world of pain by sharing the things we wish someone had shared with us. As the saying goes, it is OK to make mistakes, just make new ones.

Knowledge Compression™ uses specialized material, in-class reviews, examinations, and test-taking training to ensure that students have a solid understanding of the material that has been presented to them.

Who Should Attend:

- **All newly appointed information security officers**
- **Technically skilled administrators that have recently been given leadership responsibilities**
- **Seasoned managers that want to understand what your technical people are telling you**

From the Author

When SANS designed the Security Leadership for Managers course, we chose to emulate the format utilized by many executive MBA programs. While core source material is derived from our highly regarded SANS Security Essentials program, we decided to focus this program on the big picture of securing the enterprise: network fundamentals, security technologies, using cryptography, defense-in-depth, policy development, and management practicum. This course includes executive briefings designed to present a distilled summary of vitally important information security topics like operating system security and security threat forecasts. Ultimately, the goal of this program is to ensure that managers charged with the responsibility for information security can make informed choices and decisions that will improve their organization's security. -Stephen Northcutt

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

512.1 Managing the Plant, Network, and Information Architecture*

The course starts with a whirlwind tour of the information an effective IT security manager must know to function in today's environment. We will cover safety, physical security, and how networks and the related protocols, like TCP/IP, work and equip you to review network designs for performance, security, vulnerability scanning, and return on investment. You will learn more about secure IT operations in a single day than you ever thought possible.

Topics: Budget Awareness and Project Management; The Network Infrastructure; Computer and Network Addressing; IP Terminology and Concepts; Vulnerability Management; Managing Physical Safety, Security & the Procurement Process

512.2 Defense In Depth*

Learn information assurance foundations, which are presented in the context of both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. You will learn the methods of attack and the importance of managing attack surface.

Topics: Attacks Against the Enterprise; Defense in Depth; Managing Security Policy; Access Control and Password Management

512.3 Secure Communications*

Examine various cryptographic tools and technologies and how they can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered. Learn how malware and viruses often employ cryptographic techniques in an attempt to evade detection. We will learn about managing privacy issues in communications and investigate web application security.

Topics: Cryptography; Wireless Network Security; Steganography; Managing Privacy; Web Communications and Security; Operations Security, Defensive and Offensive Methods

512.4 The Value of Information*

On this day we consider the most valuable resource an organization has: its information. You will learn about intellectual property, incident handling, and to identify and better protect the information that is the real value of your organization. We will then formally consider how to apply everything we have learned, as well as practice briefing management on our risk architecture.

Topics: Managing Intellectual Property; Incident Handling Foundations; Information Warfare; Disaster Recovery/Contingency Planning; Managing Ethics; IT Risk Management

512.5 Management Practicum*

In the fifth and final day we pull it all together and apply the technical knowledge to the art of management. The management practicum covers a number of specific applications and topics concerning information security. We'll explore proven techniques for successful and effective management, empowering you to immediately apply what you have learned your first day back at the office.

Topics: The Mission; Globalization; IT Business and Program Growth; Security and Organizational Structure; The Total Cost of Ownership; Negotiations; Fraud; Legal Liability; Technical People

*This course is available to Management 512 participants only.

Security Leaders and Managers earn the highest salaries (well over six figures) in information security and are near the top of IT. Needless to say, to work at that compensation level, excellence is demanded. These days, security managers are expected to have domain expertise as well as the classic project management, risk assessment, and policy review and development skills.

SANS Faculty Fellow

Stephen Northcutt

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a post-graduate level IT security college (www.sans.edu). Stephen is author/coauthor of *Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security* 2nd Edition, *IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials*, and *Network Intrusion Detection* 3rd edition. He was the original author of the Shadow Intrusion Detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer.

Since 2007 Stephen has conducted over 34 in-depth interviews with leaders in the security industry, from CEOs of security product companies to the most well-known practitioners in order to research the competencies required to be a successful leader in the security field. He maintains the SANS Leadership Laboratory, where research on these competencies is posted as well as SANS Security Musings. He is the lead author for Execubytes, a monthly newsletter that covers both technical and pragmatic information for security managers. He leads the MGT512 Alumni forum, where hundreds of security managers post questions. He is the lead author/instructor for MGT512, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570, and he also is the lead author/instructor for MGT421. Stephen also blogs at the SANS Security Leadership blog.
www.sans.edu/research/leadership-laboratory

Management 525

IT Project Management, Effective Communication, and PMP® Exam Prep

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop NOT Required • Instructor: Jeff Frisk

Do you have the knowledge and tools you need to become a top-notch project manager and improve the success rate of your organization's IT projects? Do you need to improve your technical communication skills, risk analysis, and continuous monitoring processes?

The SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep course is a PMI Registered Education Provider (REP). REPs provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials. This course has been recently updated to fully align with the 2011 PMP® exam changes.

During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the PMBOK® Guide 4th edition and also provides specific techniques for success with information assurance initiatives.

Throughout the week, we will cover all aspects of project management- from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

A copy of the *PMP® Project Management Professional Exam Study Guide* (Sixth Edition) is provided to all participants. You can reference the and use your course material along with the knowledge you gain in class to prepare for the 2011 updated Project Management Professional (PMP®) Exam and the GIAC Certified Project Manager Exam.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in depth how cost, time, quality, and risk affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

Following the SANS promise, participants leave this course with specific tools that can be applied the day you get back to the office!

PMBOK® and PMP® are registered trademarks of the Project Management Institute.

Who Should Attend:

- Security professionals interested in understanding the concepts of project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/ design position who works regularly with project management staff.
- Individuals preparing for the Project Management Professional (PMP®) Exam

What Students Are Saying

"Jeff is very knowledgeable – he brings real-life examples which help explain material. Material is set up perfectly."

-Maria Saggiomo, DLA Information Operations Philadelphia

From the Author

Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential. -Jeff Frisk

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

525.1 Project Management Structure & Framework*

This course offers insight and specific techniques that both beginner and experienced project managers can utilize. The structure and framework section lays out the basic architecture and organization of project management. We will cover the common project management group processes, the difference between projects and operations, project life cycles, and managing project stakeholders.

Topics: Definition of Terms and Process Concepts; Group Processes; Project Life Cycle; Types of Organizations; PDCA Cycle

525.2 Project Charter and Scope Management*

During day two, we will go over techniques used to develop the project charter and formally initiate a project. The scope portion defines the important input parameters of project management and gives you the tools to ensure that from the onset your project is well defined. We cover tools and techniques that will help you define your project's deliverables and develop milestones to gauge performance and manage change requests.

Topics: Formally Initiating Projects; Project Charters; Project Scope Development; Work Breakdown Structures; Scope Verification and Control

525.3 Time and Cost Management*

Our third day details the time and cost aspects of managing a project. We will cover the importance of correctly defining project activities, project activity sequence, and resource constraints. We will use milestones to set project timelines and task dependencies along with learning methods of resource allocation and scheduling. We introduce the difference between resource and product-related costs and go into detail on estimating, budgeting, and controlling costs. You will learn techniques for estimating project cost and rates as well as budgeting and the process for developing a project cost baseline.

Topics: Process Flow; Task Lead and Lag Dependencies; Resource Breakdown Structures; Task Duration Estimating; Critical Path Scheduling; Cost Estimating Tools; Cost vs. Quality; Cost Base Lining; Earned Value Analysis and Forecasting

525.4 Communications and Human Resources*

During day four we cover methods for identifying, acquiring, developing, and managing your project team. Performance appraisal tools are offered as well as conflict management techniques. You will learn management methods to help keep people motivated and provide great leadership. The effective communication portion of the day covers identifying and developing key interpersonal skills. We cover organizational communication and the different levels of communication as well as common communication barriers and tools to overcome these barriers.

Topics: Acquiring and Developing Your Project Team; Organizational Dependencies and Charts; Roles and Responsibilities; Team Building; Conflict Management; Interpersonal Communication Skills; Communication Models and Effective Listening

525.5 Quality and Risk Management*

On day five you will become familiar with quality planning, quality assurance, and quality control methodologies as well as learning the cost of quality concept and its parameters. We define quality metrics and cover tools for establishing and benchmarking quality control programs. We go into quality assurance and auditing as well as using and understanding quality control charts. The risk section goes over known versus unknown risks and how to identify, assess, and categorize risk. We use quantitative risk analysis and modeling techniques so that you can fully understand how specific risks affect your project. You will learn ways to plan for and mitigate risk by reducing your exposure as well as how to take advantage of risks that could have a positive effect on your project.

Topics: Cost of Quality; Quality Metrics; Continual Process Improvement; Quality Baselines; Quality Control; Change Control; Risk Identification; Risk Assessment; Time and Cost Risks; Risk Probability and Impact Matrices; Risk Modeling and Response

525.6 Procurement and Project Integration*

We close out the week with the procurement aspects of project management and then integrate all of the concepts presented into a solid, broad-reaching approach. We cover contract basics and different types of contracts and then the make-versus-buy decision process. We go over ways to initiate strong request for quotations (RFQ) and develop evaluation criteria, then qualify and select the best partners for your project. The final session integrates everything we have learned by bringing all the topics together with the common process groups. Using detailed project management methodology, we learn how to finalize the project management plan and then execute and monitor the progress of your project to ensure success.

Topics: Contract Types; Make vs. Buy Analysis; Vendor Weighting Systems; Contract Negotiations; Project Execution; Monitoring Your Projects Progress; Finalizing Deliverables; Forecasting and Integrated Change Control

*This course is available to Management 525 participants only.

SANS Certified Instructor

Jeff Frisk

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the STI Curriculum Committee. Jeff holds the PMP certification from the Project Management Institute and GIAC GSEC credentials. He also is a certified SANS instructor and course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from The Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

Audit 407

Foundations of Auditing Information Systems

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: James Tarala

This course is designed for security and assurance professionals, system administrators, and business and operational auditors who want to develop the technical and operational knowledge of information system auditing. This course is a careful balance of the audit process, governance, and compliance regulations, as well a hands-on introduction to the latest technology tools. The auditing skills taught in AUD 407: Foundations of Auditing Information Systems are in great demand, as companies and agencies are required to comply with a growing number of regulations.

Students will learn the role of an auditor, the types of audits performed, and various information security and audit frameworks, as well as the tools and techniques of auditing technical controls, foundations of auditing operating systems, and foundations of auditing applications. Even seasoned professionals will learn the value of performing information system audits as well as the business value of information system auditing.

This information systems audit course focuses on the following areas and more:

- **Audit frameworks**
- **The information systems audit process**
- **Project management for auditors**
- **Data collection methodologies**
- **Regulations and compliance**
- **Auditing, vulnerability testing & penetration testing**
- **Auditing technical controls**
- **Auditing networks & operating systems**
- **Auditing business application systems**

Who Should Attend:

This class is designed for individuals who are tasked with auditing IT systems for implementation of organizational policies and procedures, risk, and policy conformance.

- **System implementers/administrators**
- **Network security engineers**
- **Internal auditors**
- **Assurance personnel**
- **Business and operational auditors**
- **DoD personnel/contractors**

What Students Are Saying

"The course gave me a new perspective on how to approach an audit."

-William Cummings, SRA International

From the Author

We believe auditors are the unsung heroes of organizations. Well planned information technology audits save companies time and money. Audits identify security risks and ways to reduce those risks. Being a good auditor is more than following a checklist. Great auditors have proficient technology skills. They are project managers, technical writers, persuaders, presenters, and subject matter experts. In this class, we provide students a solid foundation for understand the audit process. Let us teach you how to identify and evaluate security safeguards, and create a toolbox of automated technical auditing tools. Organizations are holding out for more audit heroes. Take the challenge!
-James Tarala

Looking for a great IT audit resource?

SANS IT Audit website is a community-focused site offering IT audit professionals a one-stop resource to learn, discuss, and share current developments in the field. It also provides information regarding SANS audit training, GIAC certification, and upcoming events. New content is added regularly, so please visit often. And don't forget to share this information with your fellow IT audit professionals.
http://it-audit.sans.org

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

407.1 Hands On: The Business of Auditing Information Systems*

During the first day of the course students will begin to be exposed to the business of auditing information systems and their role in such an effort. Students will learn the business purpose and value of information system audits, as well as understand the role of an auditor and the types of audits that could be performed. In addition, students will have the opportunity to consider audit and information security frameworks, which could serve as a foundation for audit programs or as a foundation for information assurance controls.

Topics: Define Audit Scope; Sample Information Systems Audits; Business Drivers for Audits; Internal Controls; Risk Management; Information Systems Governance

407.2 Hands On: Practical Concepts for Auditing Information Systems*

On this day students will continue their understanding of the foundational concepts of auditing information systems and begin to learn more about practical steps for performing and managing an audit. In addition, students will begin to examine the process of examining information assurance controls and the logistics necessary to effectively evaluate systems. Auditors will be confronted with the importance of auditing systems in light of regulatory guidance and how compliance plays a part in the audit process. Auditors will also be exposed to vulnerability and penetration testing concepts.

Topics: Characteristics of audits vs. characteristics of projects; Programs vs. Projects; The Project Management Process; Project Charters, WBSs, Project Scheduling / Cost; Critical Path & Diagrams, Crashing Projects; Project Management Offices

407.3 Hands On: Auditing & Governance, Risk, and Compliance (GRC)*

The third day of the course will introduce students to the importance of governance, risk, and compliance (GRC) concepts in the context of information system audits. This will lead students into an understanding of the relationship between business goals and information system controls used to manage risk. Formal risk management tools, frameworks, and techniques will be discussed and students will be exposed to available risk management programs during this day.

Topics: Elements of IT GRC; IT Governance Frameworks; COBIT; GTAG 15: Information Security Governance

407.4 Hands On: Auditing Technical Controls and Network Devices

On this day, students will learn the importance of auditing technical controls as a part of an overall audit and assurance program. Students will be exposed to a model for evaluating technical controls and how they fit into the bigger picture of control audits. Students will have the opportunity to perform examples of technical control assessments and will have the chance to try their skills by learning practically how to audit network devices - including configuration files and network access control lists.

Topics: Importance of Information System Controls; Governance Information System Controls; Technical Information System Controls: Network, Operating Systems, Application Controls; Role of the Auditor; Anatomy of a Technical Assessment

407.5 Hands On: Auditing Operating Systems: Windows, Unix

During this day of the course, students will continue their exploration of technical assurance controls. Specifically students will spend the day learning practical steps for auditing both Microsoft Windows and various flavors of Unix operating systems. Students will walk away from this day of the course with practical skills which will enable them to follow a repeatable process for auditing operating systems and the skills to identify risks in these systems. These skills will then be leveraged to consider how control audits of any system may be performed.

Topics: Common Operating System Audits; System Baselines; How to Complete an Operating System Audit; Data Gathering Tips / Philosophies; General System Baseline Tools

407.6 Hands On: Auditing Application Systems

The final day of this course will begin by examining the relationship between business goals and the application systems that are often used to enable those goals. Students will have the opportunity to learn practical skills for how to audit an application system from both a governance and technical control perspective. Students will be given hands-on opportunities to perform an assessment on application systems in order to be prepared to perform these audits in the real world. In addition, students will be provided resources for further study in the audit field and next steps for furthering their careers in the profession.

Topics: Why Audit Business Applications; Focus of an Application Audit; Information Security Controls; Scope of an Application Audit

*This course is available to Audit 407 participants only.

SANS Senior Instructor

James Tarala

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often times performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

Audit 507

Auditing Networks, Perimeters, and Systems

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: David Hoelzer

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. This course provides a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, you will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to any organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

While the primary audience for this course is auditors, system and security administrators will find very powerful techniques and processes for building continuous monitoring of systems and networks. Throughout the course, time is spent exploring how to determine what the correct "settings" are for an organization, how to abstract those settings into an automated process and how to ensure that the processes in the organization select and manage those settings correctly.

Every day of this course includes hands-on exercises. A variety of tools will be discussed and demonstrated during the lecture sections. These examples are then put into practice during labs so that you will leave knowing how to verify each and every control described in the class and know what to expect as audit evidence. Five of the hands-on days will give you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

Sign up for this course and experience the mix of theory, hands-on, and practical knowledge.

Who Should Attend:

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how they think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

What Students Are Saying

"By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. It is just like gaining real world experience."

-Jay Russell, U.S. Navy

From the Author

This advanced systems audit course stands alone in the information assurance arena as the only comprehensive source for hands on audit how-to. Past students have included long-time auditors and those new to the field, both of whom have found significant benefit from the refresher material. One individual, a vice president with the Institute of Internal Auditors, said, I've been auditing systems for a very long time, and no one ever actually gave me a formal process that I can apply to conducting technical audits. Thank you! While we don't require a high level of technical experience as a prerequisite to this course, we have worked hard to make sure that anyone who comes to the course walks away with a wealth of material that they can go back to their office and apply tomorrow. We realistically address the problem, How do I get there from here? by offering short-term goal solutions, which, when combined, will allow you to achieve your goal: identify, report on, and reduce risk in your enterprise. - David Hoelzer

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

DoD 8570 Required
www.sans.org/8570

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

507.1 Audit Principles, Risk Assessment, and Effective Reporting

In addition to filling in any foundational gaps that you might have in auditing principles, this day's material will give you two extremely useful risk assessment methods that are effective in measuring the security of a system and identifying weak or non-existent controls. Following this discussion, you will be able to analyze an existing set of controls, a business process, an audit exception, or a security incident, identify any missing or ineffective controls, and identify what corrective actions will eliminate the problem in the future.

Topics: Auditor's Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Benefits of Various Auditing Standards and Certifications; Basic Auditing and Assessing Strategies, Risk Assessment; The Six-step Audit Process

507.2 Hands On: Auditing the Perimeter

Focus on some of the most sensitive and important parts of our information technology infrastructure: routers and firewalls. In order to properly audit a firewall or router, we need to clearly understand the total information flow that is expected for the device. Diagrams will allow the auditor to identify what objectives the routers and firewalls are seeking to meet, thus allowing controls to be implemented that can be audited. Overall, this course will teach the student everything needed to audit routers, switches, and firewalls in the real world.

Topics: Overview; Detailed Audit of a Router; Auditing Switches; Testing the Firewall; Testing the Firewall Rulebase; Testing Third-Party Software; Reviewing Logs and Alerts; The Tools Used

507.3 Hands On: Network Auditing Essentials

This day continues where day two left off, extending network and perimeter auditing to internal system validation and vulnerability testing, helping network security professionals to see how to use the tools and techniques described to audit, assess, and secure a network in record time. Following a defense-in-depth approach, learn how to audit perimeter devices, create maps of active hosts and services, and assess the vulnerability of those services. Hands-on exercises are conducted throughout the day so students have the opportunity to use the tools.

Topics: Cloud Computing; Cloud architecture and deployments; Provider and Tenant responsibility considerations; Audit considerations for Iaas, Paas, and SaaS; Audit risk considerations and questions

507.4 Hands On: Web Application Auditing

We'll start with the underlying principles of web technology and introduce a set of tools that can be used to validate the security of these applications. Then we will build and work through a checklist for validating the existence and proper implementation of controls to mitigate the primary threats found in web applications.

Topics: Identify Controls Against Information Gathering Attacks; Process Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

507.5 Hands On: Advanced Windows Auditing

Systems based on the Windows NT line (XP, 2003, Vista, 2008 and Windows 7) make up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control. This class gives you the keys, techniques, and tools to build an effective long term audit program for your Microsoft Windows environment.

Topics: Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

507.6 Hands On: Auditing Unix Systems

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will get to explore, assess, and audit Unix systems hands-on. Neither Unix nor scripting experience is required for this day.

Topics: Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

SANS Faculty Fellow

David Hoelzer

David Hoelzer is a high-scoring certified SANS instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. David blogs about IT Audit issues at https://blogs.sans.org/it-audit

Developer 522

Defending Web Applications Security Essentials

Six-Day Program • Mon, Sept 17 - Sat, Sept 22
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Dr. Johannes Ullrich

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure it. DEV522 covers the OWASP Top 10 and will help you to better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class.

This class goes beyond classic web applications and includes coverage of Web 2.0 technologies, like AJAX and web services. We also arm you with knowledge to defend yourself against cutting-edge attackers, such as various protective HTTP headers and new generation of browser-based web application protections.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding level implementation.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

Who Should Attend:

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI compliant organizations who need to be trained to comply with PCI requirements

GIAC Certification Package Included

- Two Practice Tests
- One Certification Exam

GIAC Certification
www.giac.org

Dr. Johannes Ullrich *SANS Senior Instructor*

Dr. Johannes Ullrich is the Dean of Research and a faculty member of the SANS Technology Institute. In November of 2000, Johannes started the DShield.org project, which he later integrated into the Internet Storm Center. His work with the Internet Storm Center has been widely recognized. In 2004, Network World named him one of the 50 most powerful people in the networking industry. Secure Computing Magazine named him in 2005 one of the Top 5 influential IT security thinkers. His research interests include IPv6, Network Traffic Analysis and Secure Software Development. Johannes is regularly invited to speak at conferences and has been interviewed by major publications, radio as well as TV stations. He is a member of the SANS Technology Institute's Faculty and Administration as well as Curriculum and Long Range Planning Committee. As chief research officer for the SANS Institute, Johannes is currently responsible for the GIAC Gold program. Prior to working for SANS, Johannes worked as a lead support engineer for a Web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. He also maintains a daily security news summary podcast and enjoys blogging about application security. **http://software-security.sans.org/blog**

STI Graduate School
www.sans.edu

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

Developer 541

Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program | Mon, Sept 17 - Thu, Sept 20 | 9:00am - 5:00pm | 24 CPE/CMU Credits | Laptop Required | Instructor: Frank Kim

Great programmers have traditionally distinguished themselves by the elegance, effectiveness, and reliability of their code. That's still true, but elegance, effectiveness, and reliability have now been joined by security. Major financial institutions and government agencies have informed their internal development teams and outsourcers that programmers must demonstrate mastery of secure coding skills and knowledge through reliable third-party testing or lose their right to work on assignments for those organizations. More software buyers are joining the movement every week.

Such buyer and management demands create an immediate response from programmers, "Where can I learn what is meant by secure coding?" This unique SANS course allows you to bone up on the skills and knowledge required to prevent your applications from getting hacked.

This is a comprehensive course covering a huge set of skills and knowledge. It's not a high-level theory course. It's about real programming. In this course you will examine actual code, work with real tools, build applications, and gain confidence in the resources you need for the journey to improving the security of Java applications.

Who Should Attend:

- Developers who want to build more secure applications
- Java EE programmers
- Software engineers
- Software architects
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

Rather than teaching students to use a set of tools, we're teaching students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates in a Secure Development Challenge where you perform a security review of a real-world open source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that you have learned in class, implement fixes for these issues.

GIAC Certification Package Included

- Two Practice Tests
- One Certification Exam

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Developer 544

Secure Coding in .NET: Developing Defensible Applications

Four-Day Program | Mon, Sept 17 - Thu, Sept 20 | 9:00am - 5:00pm | 24 CPE/CMU Credits | Laptop Required | Instructor: Jason Montgomery

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. On the other hand, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET, 2.0 Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the onus is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

During this four-day course we will analyze the defensive strategies and technical underpinnings of the ASP.NET framework and learn where, as a developer, you can leverage defensive technologies in the framework, where you need to build security in by hand. We'll also examine strategies for building applications that will be secure both today and in the future.

Who Should Attend:

This class is focused specifically on software development but is accessible enough for anyone who's comfortable working with code and has an interest in understanding the developer's perspective:

- Software developers and architects
- Senior software QA specialists
- System and security administrators
- Penetration Testers

Rather than focusing on traditional web attacks from the attacker's perspective, this class will show developers first how to think like an attacker, and will then focus on the latest defensive techniques specific to the ASP.NET environment. The emphasis of the class is a hands-on examination of the practical aspects of securing .NET applications during development.

Have you ever wondered if ASP.NET Request Validation is effective? Have you been concerned that XML web services might be introducing unexamined security issues into your application? Should you feel un-easy relying solely only on the security controls built into the ASP.NET framework? Secure Coding in ASP.NET will answer these questions and far more.

GIAC Certification Package Included

- Two Practice Tests
- One Certification Exam

GIAC Certification
www.giac.org

New Course! Security 524: Cloud Security Fundamentals

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Dave Shackleford

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

Who Should Attend:

- Security personnel who are currently tasked with assessing the technical risks of cloud computing
- Network and systems administrators who currently manage private clouds or need to leverage hybrid and/or public cloud services
- Technical auditors and consultants who need to gain a deeper understanding of cloud computing and security concerns
- Security and IT managers who need to understand the risks of cloud computing and advise business management of the risks and various approaches to cloud computing

The first fundamental issue is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls that infosec professionals have come to rely on are not available in cloud environments, stripped down in many ways, or not able to be controlled by security teams. Security professionals must become heavily involved in the development of contract language and Service Level Agreements (SLAs) when doing business with Cloud Service Providers (CSPs). Compliance and auditing concerns are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent as audit and security teams require.

The SANS Cloud Security Fundamentals course starts out with a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types including: public, private, and hybrid. An overview of security issues within each of these models will be covered with in-depth discussions of risks to consider. Attendees will go in-depth on architecture and infrastructure fundamentals for private, public, and hybrid clouds. A wide range of topics will be covered including: patch and configuration management, virtualization security, application security, and change management. Policy, risk assessment, and governance within cloud environments will be covered with recommendations for both internal policies and contract provisions to consider. This path leads to a discussion of compliance and legal concerns. The first day will wrap-up with several fundamental scenarios for students to evaluate.

Attendees will start off the second day with coverage of audits and assessments for cloud environments. The day will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as evaluating audit and monitoring controls. Next the class will turn to protecting the data itself! New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in-depth. The challenges of identity and access management in cloud environments will be covered. The course will move into disaster recovery and business continuity planning using cloud models and architecture. Intrusion detection and incident response in cloud environments will be covered along with how best to manage these critical security processes and technologies that support them given that most controls are managed by the CSP.

Security 580: Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Bryce Galbraith

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit, are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an Open Source and easy to use framework. This course will help students get the most out of this free tool.

Who Should Attend:

- This class would be essential to any industry that has to test regularly as part of compliance requirements or regularly tests their security infrastructure as part of healthy security practices.
- Penetration testers
- Vulnerability assessment personnel
- Auditors
- General security engineers
- Security researchers

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

Security 546: IPv6 Essentials

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Dr. Johannes Ullrich

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the next years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

This course will introduce network administrators and security professionals to the basic concepts of IPv6. While it is an introduction to IPv6, it is not an introduction to networking concepts. You should understand and be aware of the basic concepts of IPv4, and networking in general.

Security 710: Advanced Exploit Development

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 7:00pm (Day 1) | 9:00am - 5:00pm (Day 2) | 14 CPE/CMU Credits
Laptop Required | Instructor: Stephen Sims

SANS SEC710 is an advanced two-day course on exploit development. Students attending this course should know their way around a debugger and have prior experience exploiting basic stack overflows on both Windows and Linux. Terms such as "jmp esp" and "pop/pop/ret" should be nothing new to you. We will move beyond these attack techniques to explore more advanced topics on heap exploitation, format string attacks, and Microsoft patch reversal and exploitation. We will be taking a real Microsoft security patch, reversing it to model the discovery of an undisclosed vulnerability, and developing a client-side exploit that defeats controls such as ASLR.

Who Should Attend:

- Network and systems penetration tester
- Application developer
- Incident handlers
- IDS engineers

Attendees can apply the skills developed in this class to create and customize exploits for penetration tests of homegrown software applications and newly discovered flaws in widespread commercial software. Understanding the process of exploit development can help enterprises analyze their actual business risks better than the ambiguous hypotheticals we often contend with in most traditional vulnerability assessments. This course is not for the faint of heart or those with modest skills. It is leading edge stuff for the best technical security professionals, security researchers, and pen testers. If you are able to absorb it, the knowledge gained throughout the course will help you write custom exploits to gain privileged system access and determine the real risk to your business. Precompiled exploits won't help you here!

Audit 521: Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Dave Hoelzer

The payment card industry has been working over the past several years to formalize a standard for security practices that are required for organizations who process or handle payment card transactions. The fruit of this labor is the Payment Card Industry Data Security Standard (currently at version 2.0).

This standard, which started life as the Visa Digital Dozen, is a set of focused comprehensive controls for managing the risks surrounding payment card transactions, particularly over the Internet. Of course, compliance validation is one of the requirements. This course was created to allow organizations to exercise due care by performing internal validations through a repeatable, objective process. While the course will cover all of the requirements of the standard, the primary focus is on the technical controls and how they can be measured. Every student will leave the class with a toolkit that can be used to validate any PCI/DSS environment technically and the knowledge of how to use it.

Management 433: Securing The Human: Building and Deploying an Effective Security Awareness Program

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop NOT Required | Instructor: Lance Spitzner

Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and changes to behaviors. In this challenging course you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant. In addition, you will develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.

SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 72.***

STI Graduate School
www.sans.edu

Management 442: Information Security Risk Management

Two-Day Course | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop NOT Required | Instructor: Evan Wheeler

This course will explore each phase of the risk management lifecycle, focusing on implementing assessment and analysis techniques that should be used to properly assess and mitigate information risk. Students will learn techniques for how to perform risk assessments for new vulnerabilities, compliance violations, new IT projects, and how to qualify the current risk level for presentation to executive level management. A series of case studies will be followed throughout the course to provide students with hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. Once students have mastered risk analysis techniques, the course will cover specific strategies for building and implementing an information security risk management program.

Hands-on labs and exercises will be assigned to be completed by students individually or in small groups, according to the day's topic. The assignments will follow a progression of a typical risk management process, showing students how to complete each step of a real-world scenario based on the case studies mentioned above. Each assignment will be based on the assessment of a fictional organization (such as a government agency, software development company, or regional bank) and other instructor-provided scenarios. Once students have learned to apply these techniques to assess risk as part of their information security management duties, the course will focus on a different approach to perform a focused risk assessment of an entire environment or specific project as an external consultant. Along the way, several popular security risk management frameworks and methodologies will be introduced and compared so that students understand how to best leverage existing risk models. The course concludes with a program level roadmap for building a security risk management program from scratch.

Management 305: Technical Communication and Presentation Skills for Security Professionals

One-Day Course | Sun, Sept 16 | 9:00am - 5:00pm | 6 CPE/CMU Credits | Laptop Required | Instructor: Dave Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills.

Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this material.

After writing a meaningful report, it is not uncommon to find that we must present the key findings from that report before an audience, whether that audience is our department, upper management, or perhaps even the entire organization. How do you transform an excellent report into a powerful presentation? We will work through a process that works to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

Writing the presentation is only half of the battle, though. How do you stand up in front of a group of five or even five thousand and speak? In the afternoon we will share tips and techniques of top presenters that you can apply to give the best presentation of your career. Additionally, students will have the opportunity to work up and deliver a short presentation to the class followed by some personal feedback from one of SANS' top speakers.

(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

Five-Day Program | Mon, Sept 17 - Fri, Sept 21 | 9:00am - 6:00pm | 35 CPE/CMU Credits
Laptop NOT Required | Instructor: Mano Paul

Presented by: (ISC)²®

Application vulnerabilities were ranked the #1 threat to information security professionals in the 2011 (ISC)² Global Information Security Workforce Study. Software and information security professionals need the tools and knowledge to mitigate from these constant and evolving threats.

The (ISC)² five-day CSSLP CBK Education Program is the exclusive way to learn security best practices and industry standards for the software lifecycle. This is where you will learn tools and processes on how security should be built into each phase of the software lifecycle. It will also detail security measures that need to take place beginning with the requirement phase, through software design all the way through software testing and ultimately disposal. This will ensure you're properly prepared to take on the constantly evolving vulnerabilities exposed in software development. Each software stakeholder is responsible for certain phase(s) of the SLC, but all phases must have security built into them. CSSLP is for all the stakeholders involved in the process. Each of the seven CSSLP Domains covers how to build security into the different phases.

The comprehensive (ISC)² CSSLP CBK Education program covers the following domains:

- **Secure Software Concepts – security implications in software development**
- **Secure Software Requirements – capturing security requirements in the requirements gathering phase**
- **Secure Software Design – translating security requirements into application design elements CSSLP Man**
- **Secure Software Implementation/Coding – unit testing for security functionality and resiliency to attack and developing secure code and exploit mitigation**
- **Secure Software Testing – integrated QA testing for security functionality and resiliency to attack**
- **Software Acceptance – security implication in the software acceptance phase**
- **Software Deployment, Operations, Maintenance, and Disposal – security issues around steady state operations and management of software**

Download a brochure to learn more about the CSSLP. www.isc2.org/csslpedu

Please note that the price of tuition does NOT include the CSSLP exam.

Who Should Attend:

- Software Architects
- Software Engineers/Designers
- Software Development Managers
- Requirements Analysts
- Project Managers
- Business and IT Managers
- Auditors
- Developers and Coders
- Security Specialists
- Auditors and Quality Assurance Managers
- Application Owners

Mano Paul *(ISC)² Instructor*

Mano Paul is the Software Assurance Advisor for (ISC)², the global leader in information security education and certification, representing and advising the organization on software assurance strategy, training, education and certification. His information security and software assurance experience includes designing and developing security programs from compliance-to-coding, security in the SDLC, writing secure code, risk management, security strategy, and security awareness training and education. Following his entrepreneurial acumen, he founded and serves as the CEO & President of Express Certifications, a professional certification assessment and training company that developed studISCope, (ISC)²'s official self-assessment offering for their certifications. He also founded SecuRisk Solutions, a company that specializes in security product development and consulting. Before Express Certifications and SecuRisk Solutions, Mr. Paul played several roles from software developer, quality assurance engineer, logistics manager, technical architect, IT strategist and security engineer/program manager/strategist at Dell Inc. Mr. Paul holds the following professional certifications – CSSLP, CISSP, AMBCI, MCSD, MCAD, CompTIA Network+ and the ECSA certification.

RMF for DoD IT Workshop

Five-Day Program | Mon, Sept 17 - Fri, Sept 21 | 9:00am - 5:00pm | 30 CPE/CMU Credits
Laptop Required | Instructor: Scott Byers

Presented by:

SecureInfo
A KRATOS Company

The Risk Management Framework for DoD Information Technology Workshop

SecureInfo is pleased to announce the release of the Risk Management Framework for DoD Information Technology (RMF for DoD IT or RDIT) Workshop. This intense Cybersecurity-based workshop blends lecture, discussion, and hands-on exercises to educate students on the new RDIT methodology. This workshop will prepare students to implement the Risk Management Framework for their IT systems as prescribed in the updated DoD series of publications, as well as the related NIST and CNSS publications. The workshop compares and contrasts numerous aspects of the current DoD C&A process (DIACAP), to the new methodology for categorizing information systems, selecting and implementing applicable security controls, and establishing a Continuous Monitoring program. This workshop breaks down the RDIT methodology (into steps, tasks, outputs, and responsible entities) and includes informative lectures, discussions, and exercises which provide a functional understanding of Cybersecurity, Risk Management, and the proper selection, implementation, and validation of the new Security Controls as outlined on the DIACAP Knowledge Service and complimented by NIST Special Publications.

Background

The Department of Defense has adopted and will transition to a new Cybersecurity Risk Management Framework (RMF) methodology [RDIT] as the replacement for DIACAP. The direction for this transformation comes from the latest set of both DoD and Committee for National Security Systems (CNSS) document replacements for DoDD 8500.1, DoDI 8500.2, DoDI 8510.01, CNSSP 22, and CNSSI 1253. The RDIT is supported and complimented through a suite of standards and guidelines: National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, 800-30, 800-39, 800-53, 800-53A, and 800-137.

Laptop Requirement

Laptops are required for this course, as each student will be asked to create documentation and participate in practical exercises that guide the students. The laptop must have Adobe Acrobat Reader, Excel, and Word. Resource Kits are provided via CDs for students attending the course, for in-class work, as well as supplemental materials.

Scott Byers *SecureInfo Corporation*

Scott Byers has been an educator for the past 14 years in the Information Security and Information Assurance (IA) fields. He has trained numerous government and civilian personnel in the intricacies of the Security Authorization process (formerly known as Certification and Accreditation), as well as the installation, configuration and usage of several security management, scanning, and automation tools. Scott also has an in-depth background as a security consultant, having completed multiple Security Authorization packages for USAF Information Systems taking them through the required process to successful Authorization to Operate (ATO) decisions. He is the primary instructor at SecureInfo, A Kratos Company, for the upcoming transition of DIACAP to the Risk Management Framework (RMF) for DoD IT Systems, and other associated courses.

Who Should Attend:

The curriculum covered in this course is appropriate for all government and contractor personnel who must understand and implement the new RDIT methodology; including, but not limited to, ISSMs, ISSOs, SCAs, PM/SMs, AO Reps, and IG/Auditors.

- **Individuals with information system and security management and oversight responsibilities.** (e.g., authorizing official representatives, chief information officers, senior information assurance officers, information system owners, or certifying authorities)
- **Individuals with information system and information assurance control assessment and monitoring responsibilities.** (e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, Inspectors General, or program managers)
- **Individuals with information assurance implementation and operational responsibilities.** (e.g., information system owners, information owners/stewards, mission/business owners, information system security managers/officers, security managers, or system administrators)

Please check the online course description for any updates, prerequisites, laptop requirements, or special notes.

Physical Penetration Testing - Introduction

Two-Day Program | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Deviant Ollam

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company's security posture or to augment their career as a penetration tester.

Took Kit Included with Class

- A lockpicking toolkit with a varied blend of hooks, rakes, diamonds, and tension tools
- A set of ten training and practice locks
- Wafer lock tools and a sample wafer lock
- A door latch bypassing tool
- A locksmith's impressioning file
- A pocket microscope & key gripper (also for impressioning)
- A bump key

Who Should Attend:

- Penetration testers, security auditors, IT professionals responsible for infrastructure oversight.
- Student Requirements, experience/expertise
- This course begins at the complete novice level, no prior knowledge of lockpicking is necessary.

Offensive Countermeasures: Defensive Tactics That Actually Work

Two-Day Program | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: John Strand

One of the big questions we get is why Offensive Countermeasures are so important. Well, to be honest, you will need it someday. The current threat landscape is shifting. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. Some of the things we talk about you may implement immediately, others may take you a while to implement. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, attribute who is attacking you and, finally, attack the attackers.

More to the point, the old strategies of security have failed us and will continue to fail us unless we start becoming more offensive in our defensive tactics.

Presented by:

Who Should Attend:

Security professionals and systems administrators who are tired of playing catch-up with attackers

Advanced Vulnerability Scanning Techniques Using Nessus

Two-Day Program | Sun, Sept 23 - Mon, Sept 24 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: SANS Staff

This course teaches advanced scanning techniques by using a real-world scenario to demonstrate how these techniques help to solve problems in a sample work environment.

In this course you (or you and your team) will take on the role of a brand new security engineer for a financial company. You will be tasked with configuring and auditing a system to be used within your network environment. The system and associated applications make up the environment used to manage the business. Currently, the old system is in place, and an upgrade is planned. The current vulnerability scanning process takes over a week to complete, and there is duplication of effort and a known false positive rate. Additionally, breaches have occurred on the network, and your company is in jeopardy of being fined due to compliance violations. The vulnerability management process is missing vulnerabilities that were exploited by attackers. A sample system has been provided for you that exactly mirrors what will be used in production, right down to the passwords and configuration.

Presented by:

Who Should Attend:

Students who are familiar with Nessus, but wish to learn a more advanced method of vulnerability scanning. This includes security engineers, penetration testers, and systems administrators.

You don't have to miss out on SANS' top-rated training. Attend select SANS Network Security 2012 courses remotely via SANS Simulcast!

How SANS Simulcast Works

Cutting-edge webcast technology and live instruction combine to deliver a fun and engaging remote learning experience. Remote students will also receive six months of access to an archived copy of the class to use as a reference tool or to catch up on a missed session. The platform is web-based so students simply need a solid internet connection to participate.

"This is the first web-based training course I have done and was wondering if it would actually be worthwhile. It surpassed my expectations! The software and technology worked really well, the presenter kept everything moving along nicely and was quick to pick up on participants' comments during the lecture segments. The IM component adds value – lots of good information/comments from the class." -Jeremy Gay, Montana State University

To register for a SANS Network Security 2012 Simulcast course, please visit www.sans.org/simulcasts

The following SANS Network Security 2012 courses will be available via SANS Simulcast:

Short Courses:
MGT433

Long Courses:
MGT414 SEC401
SEC505 SEC566

Additional Training Options

www.sans.org/ondemand

SANS OnDemand *Online Security Training & Assessments*

If you're a self-motivated learner whose schedule changes often, then SANS OnDemand is the right learning platform for you. Choose from more than 40 courses, and take them whenever and wherever you want. Each course gives you four months of access to our OnDemand computer-based training platform, which includes a mix of presentation slides, video demonstrations, and assessment tests supported with audio of SANS' top instructors teaching the material.

If you have questions about the material, our virtual mentors are available to help. You can also bundle OnDemand with any other SANS online or in-person training vehicle to diversify your learning experience or bolster your preparation for the GIAC certification exam.

www.sans.org/vlive

SANS vLive *Live Virtual Training from SANS' Top Instructors*

If you prefer a structured and interactive learning environment, vLive may be right for you! The vLive platform uses cutting-edge webcast technology and collaboration software to create a virtual classroom. vLive classes are taught in real time by SANS' top instructors. Most vLive classes meet two evenings a week from 7:00pm to 10:00pm EST.

- Interact with your instructor during class.
- Classes are recorded and can be reviewed online for six months.
- You can revisit individual class sessions to review challenging concepts or repeat exercises.

Training Events

SANS Training Events are recognized as the best place in the world to get IT security education, from intimate gatherings to our action-packed national events! Network with other information security professionals, hear world-class speakers, actively engage with providers of proven security solutions, and participate in challenges and contests.

www.sans.org/security-training/bylocation/index_all.php

Community *Community Training Events*

The SANS Community format offers our most popular security courses in a small classroom setting – most courses have fewer than 25 students. The course material is delivered over a six-day period, just like at larger SANS events, by instructors trained by SANS very best authors and instructors. We bring SANS to your community at a discounted tuition level while also saving you time and money on travel.

www.sans.org/community

OnSite *Information Security Training at Your Location*

With the SANS OnSite program you can bring a combination of high-quality content and world-recognized instructors to your location and realize significant savings in employee travel costs and course fees for larger classes.

www.sans.org/onsite

Mentor & @Work *Intimate Live Instruction*

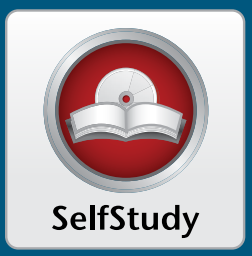
The SANS Mentor program offers the flexibility of live instruction with self-paced learning. Classes are conducted over the course of several weeks, much like a graduate level course. Students study on their own then work with the Mentor during class to discuss material, answer questions, and work on exercises and labs such as Capture the Flag.

www.sans.org/mentor

Summit Series *Your IT Security Connection*

SANS WhatWorks Summits are unique events that focus on the most current topics in computer security. User panels, debates, vendor demos, and short talks by industry experts help you get the most up-to-date security solutions in the least amount of time.

www.sans.org/summit



SelfStudy *Books & MP3s*

With each SelfStudy course, you'll receive a complete set of SANS course books, MP3s of lectures by SANS' top instructors, and when applicable, hands-on CDs and virtual labs.

www.sans.org/selfstudy

SANS CYBER GUARDIAN PROGRAM

www.sans.org/cyber-guardian

Stay ahead of cyber threats!

Join the SANS Cyber Guardian program today.

How the Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Contact us at onsite@sans.org to get started!

Program Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above)

or

- A CISSP certification

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

Learn more about the SANS Cyber Guardian Program at www.sans.org/cyber-guardian

Core Courses

SEC503 Intrusion Detection In-Depth (GCIA)

SEC504 Hacker Techniques, Exploits, and Incident Handling (GCIH)

SEC560 Network Penetration Testing and Ethical Hacking (GPEN)

FOR508 Advanced Computer Forensic Analysis & Incident Response (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

SEC502 Perimeter Protection In-Depth (GCFW)

SEC505 Securing Windows (GCWN)

SEC506 Securing Linux/Unix (GCUX)

Red Team Courses

SEC542 Web App Penetration Testing and Ethical Hacking (GWAPT)

SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)

SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

Future SANS Training Events

SANSFIRE 2012
Washington, DC
July 6-15, 2012
www.sans.org/sansfire-2012

Security Impact of IPv6 Summit 2012
Washington, DC
July 6, 2012
www.sans.org/ipv6-summit-2012

SANS San Francisco 2012
San Francisco, CA
July 30 – August 6, 2012
www.sans.org/san-francisco-2012

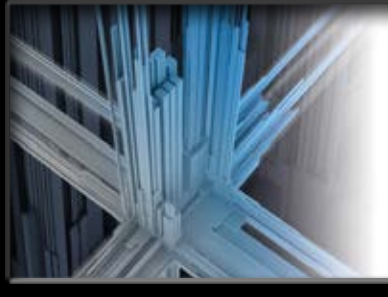
SANS Security Architecture Summit 2012
San Diego, CA
July 31 - August 1, 2012
www.sans.org/security-architecture-summit-2012

SANS Boston 2012
Boston, MA
August 6-11, 2012
www.sans.org/boston-2012

Vulnerability Management Summit 2012
San Antonio, TX
August 14 - 17, 2012
www.sans.org/vulnerability-summit-2012

SCADA Security Advanced Training 2012
The Woodlands, TX
August 20 - 24, 2012
www.sans.org/scada-sec-training-2012

SANS Virginia Beach 2012
Virginia Beach, VA
August 20-31, 2012
www.sans.org/virginia-beach-2012



SANS Crystal City 2012
Arlington, VA
September 6-11, 2012
www.sans.org/crystal-city-2012

SANS CyberCon 2012
Virtual Conference
October 8-13, 2012 | www.sans.org/cybercon-2012

SANS Seattle 2012
Seattle, WA
October 14-21, 2012
www.sans.org/seattle-2012

SANS Baltimore 2012
Baltimore, MD
October 15-22, 2012
www.sans.org/baltimore-2012

Future SANS Training Events

SANS Chicago 2012

Chicago, IL
Oct 29 – Nov 5, 2012
www.sans.org/chicago-2012

SANS San Diego 2012

San Diego, CA
November 12-17, 2012
www.sans.org/san-diego-2012

SANS London 2012

London, UK
Nov 26 - Dec 3, 2012
www.sans.org/london-2012

SANS San Antonio 2012

San Antonio, TX
Nov 27 - Dec 2, 2012
www.sans.org/san-antonio-2012

SANS Cyber Defense Initiative 2012

Washington, DC
December 7-16, 2012
www.sans.org/cyber-defense-initiative-2012

North American SCADA and Process Control Summit 2013

Lake Buena Vista, FL
February 5-15, 2013

SANS Community

The Community SANS format offers our most popular security courses in a small classroom setting in your own community - most courses have fewer than 25 students. The course material is delivered over a six-day period, just like it is at a larger SANS event, by instructors trained by SANS very best authors and instructors. For a complete list of events, please visit www.sans.org/community

Austin, TX
June 28-29 | SEC524

Albuquerque, NM
July 9-14 | SEC401

Anaheim, CA
July 9-14 | SEC401

Las Vegas, NV
July 16-21 | SEC401

Raleigh, NC
July 16-21 | SEC504

Minneapolis, MN
July 23-28 | SEC542

Springfield, IL
July 24-25 | SEC464

Dallas, TX
Jul 30 - Aug 4 | SEC542

Atlanta , GA
July 30-31 | SEC464

Fort Lauderdale, FL
July 30-31 | SEC464

Pensacola, FL
August 6-11 | SEC401

Baltimore, MD
August 6-10 | FOR610

Toronto, ON
August 13-18 | SEC401

Seattle, WA
August 13-18 | SEC560

Colorado Springs, CO
August 13-18 | SEC542

San Antonio, TX
August 20-25 | SEC401

Atlanta, GA
September 10-15 | SEC401

Annapolis, MD
September 10-15 | SEC560

Calgary, AB
September 10-15 | SEC579

Sunnyvale, CA
September 24-28 | SEC566

Montreal, QC
September 24-29 | SEC560

SANS Network Security 2012

Hotel & Travel Information

SANS Network Security 2012 will be located at

Caesars Palace
3570 Las Vegas Blvd.
Las Vegas, NV 89109
877-427-7243
www.caesars.com/index.shtml

Welcome to the most prestigious resort in the world. From the shops of world-renowned designers like Valentino and Louis Vuitton to the celebrity clientele at PURE nightclub, you'll discover legendary shopping and nightlife at Caesars Palace, plus a world of luxury at our extraordinary swimming pools and spa.

Caesars Palace wants to lavish you with all the amenities that will make your stay with us one you'll always remember. Discover indulgence beyond expectation at Qua Baths & Spa, featuring never before seen amenities like Roman baths, a dry-heat Laconium room and a stunning, snow-filled Arctic Ice room. Caesars Palace is also the home of celebrity stylist Michael Boychuck, "colorist to the stars." Every salon in town he's touched has become a must-visit destination, and now Color, a Salon by Michael Boychuck is exclusively at Caesars Palace. At the Garden of the Gods Pool Oasis, graceful fountains and classically inspired statuary surround three large swimming pools and two outdoor whirlpool spas so you can relax with friends around sparkling waters.

Top 5 reasons to stay at Caesars Palace

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at Caesars Palace, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the conference.
4. SANS schedules morning and evening events at Caesars Palace that you won't want to miss!
5. Everything is in one convenient location!

After exploring all that our spa, salon, and pools have to offer, you can shop at more than 120 stores in two elegant settings. The names on the storefronts are legendary, and the merchandise inside is the best the world has to offer. From Cartier and Roberto Cavalli to Salvatore Ferragamo, you can browse through the world's finest stores at the Forum Shops and Appian Way.

Then, cap off your night at PURE, our remarkable club that sets new standards for Las Vegas nightlife. Owned in part by Celine Dion, Shaquille O'Neal, Andre Agassi and Steffi Graf, PURE is three stylish venues in one, including a VIP room, a dance floor with progressive DJs and a large outdoor patio with cascading waterfalls, walls of fire and breathtaking views of the surrounding Strip.

Special Hotel Rates

A special discounted "Early Bird Rate" of $122.50 S/D will be honored until August 17, 2012. Then the special discounted rate of $175.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include In-Room high-speed Internet, a $14.99 value! To make reservations please call (866) 227-5944 and ask for the SANS special "Early Bird Rate."

NOTE: You must mention that you are attending the SANS Institute training event to get the discounted rate. The resort will require a major credit card to guarantee your reservation. To cancel your reservation, you must notify the resort at least 72 hours before your planned arrival date.

Avis is proud to offer special rates for SANS 2012. Make your reservations now and don't forget to use your special discount code: **J945620**. **www.avis.com**

Weather Conditions

September in Las Vegas is pleasant with highs around 95° and lows near 66°. For the latest weather conditions and forecast, please consult **www.weather.com**.

Come to Las Vegas!

Dear Colleagues and Friends,

SANS is back in Las Vegas, one of our most popular destinations, right in the heart of the world famous strip! The city has so much to offer, you will find famous attractions, shows, restaurants, and shopping all within walking distance. SANS Network Security 2012 will be offering more courses, night sessions, and vendor events than ever before. This includes NetWars, our virtual security challenge competition, which offers a perfect opportunity for you to get a report card on your abilities in cyber security.

The training event will be back at Caesars Palace (**www.caesarspalace.com**) which is an attraction in itself! This property features the Forum Shops with over 160 shops and 14 restaurants. The Garden of the Gods pool complex has just doubled in size. Rod Stewart, a true legend on the concert scene, is the scheduled performer during Network Security 2012. The hotel also has various dining options from high-end celebrity restaurants and all-you-can-eat buffets to the Market Street Grill, a food court that is quite popular for a quick bite!

Caesars Palace has the largest square footage of any hotel on the strip. Since it will take approximately 10 minutes to get from the front door to your classroom, we highly recommend staying inside the hotel. Please book early so you can take advantage of our special group rate. Most guest rooms at Caesars Palace are an elevator's ride away our classrooms, and you will not even need to walk through the casino. As an extra treat, you will receive complimentary high-speed Internet – but only if you book under the special SANS group rate.

Even though it will be warm outside, you still want to bring a jacket for the climate-controlled classrooms and cooler evenings. You will also want to check out the SANS Network Security 2012 program guide for all of the events as well as the social board for student gatherings around the city. Please feel free to send me an e-mail at **Brian@sans.org** if I can offer any additional tips to make sure you have the best time possible at SANS Network Security 2012.

We look forward to seeing you in Las Vegas!

Warm regards

Brian Correia

Brian Correia
Director, Business Development & Venue Planning

Five Reasons to Register

1. ***The best career move you will ever make!***
   That's how one SANS alumnus described the IT security education and networking opportunities offered by SANS. Attending SANS Network Security 2012 is a way of investing in your career. To reap the maximum benefit, read the course descriptions carefully. Check out the five- and six-day courses plus a wide variety of one- to four-day skill-based short courses.

2. ***Why settle for second best?***
   If you want to increase your understanding of information security and become more effective in your job, you need to be trained by the best. "SANS provides by far the most in-depth security training with the true experts in the field as instructors," says Mark Smith, Costco Wholesale.

3. ***Challenge yourself!***
   Consider attempting GIAC (Global Information Assurance Certification), the industry's most respected technical security certification. GIAC is the only information security certification for advanced technical subject areas, including audit, intrusion detection, incident handling, firewalls and perimeter protection, forensics, hacker techniques, and Windows and Unix operating system security.

4. ***Become part of an elite group.***
   We're referring to the group of technical, security-savvy professionals who have had hands-on training through SANS. Material taught in the SANS courses directly applies to real-world challenges in your IT environment. "Six days of training gave me six months of work to do," says Steven Marscovetra of Norinchukin Bank. "It is amazing how much of the training I can apply immediately at work."

5. ***Don't miss out on a good opportunity!***
   This is your chance to make a great career move, be taught by the cream of the crop, challenge yourself, and become part of an elite group during a full week of IT security education and networking opportunities. Come prepared to learn; we will come prepared to teach.

SANS Network Security 2012

Registration Information

Register online at
www.sans.org/network-security-2012

How to Register

1. To register, go to www.sans.org/network-security-2012.
Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. We do not take registrations by phone.

2. Provide payment information.
Even if you do not want to submit your payment information online, still complete the online form! There is an option to submit credit card information for payment by fax or phone once the online form is completed and you have your invoice number.

SANS ACCEPTS ONLY US and CANADIAN FEDERAL GOVERNMENT PURCHASE ORDERS

If you normally use a PO and are not part of the federal government, please see our additional PO information on the tuition information page:
www.sans.org/network-security-2012/tuition.php

3. Print your invoice.
If you need one, you must print YOUR OWN INVOICE at the end of the online registration process. The invoice will pop up automatically when the registration is successfully submitted. You may also access your invoice at **https://portal.sans.org/history**.

4. E-mail confirmation will arrive soon after you register.

To register for a SANS Network Security 2012 Simulcast course, please visit www.sans.org/simulcasts

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**8/8/12**	**$500.00**	**8/22/12**	**$250.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at **www.sans.org/security-training/discounts.php** prior to registering.

Get GIAC Certified!

- Only $549 when combined with SANS training
- Deadline to register is the last day of SANS Network Security 2012
- Price goes to $799 after deadline
- Register today at **registration@sans.org**!

Frequently Asked Questions

Frequently asked questions about SANS Training and GIAC Certification – the industry standard for security knowledge – are posted at **www.giac.org/overview/faq.php**.

Cancellation

You may subsitute another person in your place at any time by sending an e-mail request to **registration@sans.org** or a fax request to 301-951-0140. There is a $300 cancellation fee per registration. Cancellation requests must be received by Wednesday, August 29, 2012, by fax or mail-in order to receive a refund.

SANS Network Security 2012 Registration Fees

Register online at **www.sans.org/network-security-2012**

If you don't wish to register online,
please call 301-654-SANS(7267) 9:00am - 8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

Job-Based Long Courses

		Paid by 8/8/12	Paid by 8/22/12	Paid after 8/22/12	Add GIAC Cert	Add OnDemand
☐ AUD407	Foundations of Auditing Information Systems	$3,695	$3,945	$4,195		
☐ AUD507	Auditing Networks, Perimeters, and Systems	$3,695	$3,945	$4,195	☐ $549	☐ $449
☐ DEV522	Defending Web Applications Security Essentials	$3,695	$3,945	$4,195	Included	☐ $449
☐ FOR408	Computer Forensic Investigations - Windows In-Depth	$4,095	$4,345	$4,595	☐ $549	☐ $449
☐ FOR508	Advanced Computer Forensic Analysis and Incident Response	$4,095	$4,345	$4,595	☐ $549	☐ $449
☐ FOR563	Mobile Device Forensics	$3,745	$3,995	$4,245		
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$3,445	$3,695	$3,945	☐ $549	☐ $449
☐ LEG523	Law of Data Security and Investigations	$3,445	$3,695	$3,945	☐ $549	☐ $449
☐ MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	$3,495	$3,745	$3,995	☐ $549	☐ $449
☐ MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	$4,095	$4,345	$4,595	☐ $549	☐ $449
☐ MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	$3,695	$3,945	$4,195	☐ $549	
☐ SEC301	Intro to Information Security	$3,445	$3,695	$3,945	☐ $549	☐ $449
☐ SEC401	SANS Security Essentials Bootcamp Style	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC501	Advanced Security Essentials – Enterprise Defender	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC502	Perimeter Protection In-Depth	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC503	Intrusion Detection In-Depth	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC504	Hacker Techniques, Exploits, and Incident Handling	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC505	Securing Windows	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC506	Securing Linux/Unix	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC509	Securing Oracle Databases	$3,695	$3,945	$4,195		
☐ SEC540	VoIP Security	$3,695	$3,945	$4,195		
☐ SEC542	Web Application Penetration Testing and Ethical Hacking	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC560	Network Penetration Testing and Ethical Hacking	$4,095	$4,345	$4,595	☐ $549	☐ $449
☐ SEC566	Implementing & Auditing the Twenty Critical Security Controls - In-Depth	$3,445	$3,695	$3,945		☐ $449
☐ SEC575	Mobile Device Security and Ethical Hacking ***NEW!***	$4,095	$4,345	$4,595		
☐ SEC579	Virtualization and Private Cloud Security ***NEW!***	$4,095	$4,345	$4,595		
☐ SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	$3,895	$4,145	$4,395	☐ $549	☐ $449
☐ SEC642	Advanced Web App Penetration Testing and Ethical Hacking ***NEW!***	$3,895	$4,145	$4,395		
☐ SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking	$4,095	$4,345	$4,595	☐ $549	☐ $449
☐ HOSTED	(ISC)²® CSSLP® CBK® Education Program	$2,645	$2,895	$3,145		
☐ HOSTED	RMF for DoD IT Workshop Workshop	$3,495	$3,745	$3,995		

Skill-Based Short Courses

		If taking a 5-6 day course				
☐ AUD521	Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant	$1,150	$1,700	$1,700	$1,700	
☐ DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	N/A	$2,995	$3,245	$3,495	Included ☐ $239
☐ DEV544	Secure Coding in .NET: Developing Defensible Applications	N/A	$2,995	$3,245	$3,495	Included ☐ $239
☐ MGT305	Technical Communication and Presentation Skills for Security Professionals	$575	$995	$995	$995	
☐ MGT433	Securing The Human: Building and Deploying an Effective Security Awareness Program	$1,150	$1,700	$1,700	$1,700	
☐ MGT442	Information Security Risk Management	$1,150	$1,700	$1,700	$1,700	☐ $199
☐ SEC524	Cloud Security Fundamentals	$1,150	$1,700	$1,700	$1,700	
☐ SEC546	IPv6 Essentials	$1,150	$1,700	$1,700	$1,700	
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$1,150	$1,700	$1,700	$1,700	☐ $239
☐ SEC710	Advanced Exploit Development	$1,250	$1,800	$1,800	$1,800	☐ $239
☐ HOSTED	Physical Penetration Testing - Introduction	N/A	$1,850	$1,850	$1,850	
☐ HOSTED	Offensive Countermeasures: Defensive Tactics That Actually Work	$1,150	$1,700	$1,700	$1,700	
☐ HOSTED	Advanced Vulnerability Scanning Techniques Using Nessus	$1,150	$1,700	$1,700	$1,700	
☐ SPECIAL	NetWars – Interactive Security Challenge Entrance Fee	FREE	$999	$999	$999	

Individual Courses Available

	MON 9/17	TUE 9/18	WED 9/19	THU 9/20	FRI 9/21	SAT 9/22
AUD507	☐ 507.1	☐ 507.2 & 507.3		☐ 507.4	☐ 507.5	☐ 507.6
LEG523	☐ 523.1	☐ 523.2	☐ 523.3	☐ 523.4	☐ 523.5	
SEC301	☐ 301.1	☐ 301.2	☐ 301.3	☐ 301.4	☐ 301.5	
SEC401	☐ 401.1	☐ 401.2	☐ 401.3	☐ 401.4	☐ 401.5	☐ 401.6
SEC501	☐ 501.1	☐ 501.2	☐ 501.3	☐ 501.4	☐ 501.5	☐ 501.6
SEC502	☐ 502.1	☐ 502.2	☐ 502.3	☐ 502.4	☐ 502.5	☐ 502.6
SEC503	☐ 503.1					
SEC504	☐ 504.1					
SEC505	☐ 505.1	☐ 505.2	☐ 505.3	☐ 505.4	☐ 505.5	☐ 505.6

Individual Course Day Rates If Not Taking a Full Course

☐ One Full Day	$1,350
☐ Two Full Days	$2,075
☐ Three Full Days	$3,025
☐ Four Full Days	$3,675
☐ Five Full Days	$4,375
☐ Six Full Days	$4,875
☐ Seven Full Days	$5,475
☐ Eight Full Days	$5,995

REMINDER: **When you register, please use the promo code located on the back cover.**

SANS 5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this Promo Code and receive a Special invitation to the **SANS Hosted President's Reception**

Setting the Standard for Security Training

SANS

SANS is the most trusted and by far the largest source for information security training, certification, and research in the world.

Five Tips to Get Approval for SANS Training

1. EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (inside cover) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.
- Note that the core, job-based courses can be complemented by short, skill-based courses of one or two days. We also offer deep discounts for bundled course packages. Consider a *GIAC Certification*, which will show the world that you have achieved proven expertise in your chosen field.

2. RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Promise to share what you've learned with your colleagues.

3. SAVE

- The earlier you sign up, the more you save, so explain the benefit of signing up early.
- Save even more with group discounts! See inside for details.

Scan the QR code and register by August 8th to ***SAVE $500*** *on SANS Network Security 2012 courses.*

www.sans.org/info/104665

4. ADD VALUE

- Share with your boss that you can add value to your experience by meeting with network security experts – people who face the same type of challenges that you face every single day.
- Explain how you will be able to get and share great ideas on improving your IT productivity and efficiency.
- Enhance your SANS training experience with *SANS @Night* talks and the *Vendor Expo*, which are free and only available at live training events.
- Take advantage of the special SANS host-hotel rate so you will be right where the action is!

5. ACT

- With the fortitude and initiative you have demonstrated thus far, you can confidently seek approval to attend SANS training!

Return on Investment: SANS training events are recognized as the best place in the world to get information security education. With SANS, you will gain significant return on investment (ROI) for your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

Remember: SANS is your first and best choice for information and software security training. The SANS Promise is *"You will be able to apply our information security training the day you get back to the office!"*