Washington, DC | December 7-16, 2012

# SANS

THE MOST TRUSTED SOURCE FOR INFORMATION
AND SOFTWARE SECURITY TRAINING

# CYBER DEFENSE INITIATIVE

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

**Security Essentials Bootcamp Style**

**Hacker Techniques, Exploits & Incident Handling**

**Security Leadership Essentials for Managers with Knowledge Compression™**

**Virtualization and Private Cloud Security**

**Computer Forensic Investigations – Windows In-Depth**

**Intrusion Detection In-Depth**

**Mobile Device Forensics**

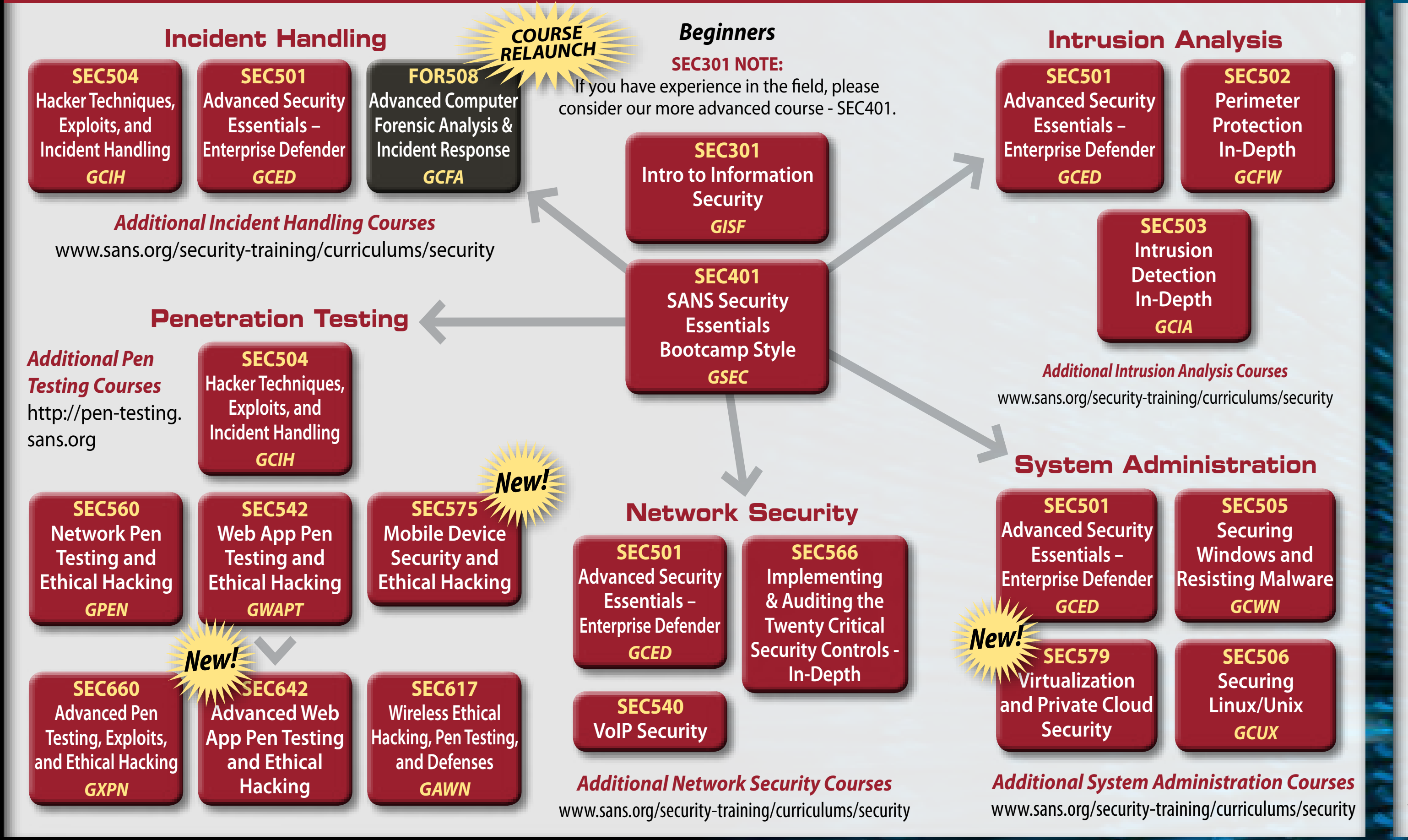
***...and much more!***

> *"SANS, as always, delivers quality training that provides immediate real-world application."*
>
> -KEVIN MCLAUGHLIN,
> UNIVERSITY OF CINCINNATI

**Register at**
**www.sans.org/cyber-defense-initiative-2012**

# SANS IT Security Training and Your Career Roadmap

## SECURITY CURRICULUM



### Incident Handling

COURSE RELAUNCH

**SEC504** Hacker Techniques, Exploits, and Incident Handling *GCIH*

**SEC501** Advanced Security Essentials – Enterprise Defender *GCED*

**FOR508** Advanced Computer Forensic Analysis & Incident Response *GCFA*

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

### 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*

### Penetration Testing

*Additional Pen 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*

New!
**SEC575** Mobile Device Security and Ethical Hacking

**SEC660** Advanced Pen Testing, Exploits, and Ethical Hacking *GXPN*

New!
**SEC642** Advanced Web App Pen Testing and Ethical Hacking

**SEC617** Wireless Ethical Hacking, Pen Testing, and Defenses *GAWN*

### 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*

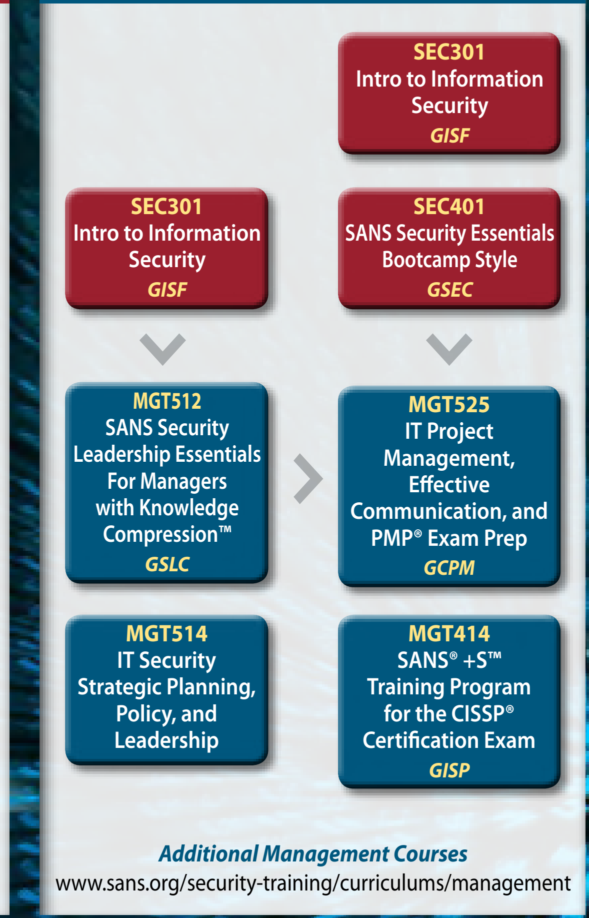
**SEC505** Securing Windows and Resisting Malware *GCWN*

New!
**SEC579** Virtualization and Private Cloud Security

**SEC506** Securing Linux/Unix *GCUX*

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

## MANAGEMENT CURRICULUM



**SEC301** Intro to Information Security *GISF*

**SEC301** Intro to Information Security *GISF*

**SEC401** SANS Security Essentials Bootcamp Style *GSEC*

**MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ *GSLC*

**MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep *GCPM*

**MGT514** IT Security Strategic Planning, Policy, and Leadership

**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*

COURSE RELAUNCH
**FOR508** Advanced Computer Forensic Analysis & Incident Response *GCFA*

**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*

**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*

### Secure Coding

JAVA

**DEV541** Secure Coding in Java/JEE *GSSP-JAVA*

.NET

**DEV544** Secure Coding in .NET *GSSP-.NET*

C & C++

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

PCI

**DEV536** Secure Coding for PCI Compliance

### Attack

**SEC542** Web App Pen Testing and Ethical Hacking *GWAPT*

New!
**SEC642** Advanced Web App Pen Testing and Ethical Hacking

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

Dear Colleague,

**SANS Cyber Defense Initiative** (CDI) is one of our most important events of the year. It is my hope that you will join me in **Washington, DC on December 7-16**. We are bringing more than 25 courses, SANS' most interesting and challenging educational programs, to meet the needs of the sophisticated cyber security community in the nation. SANS has proven to be uniquely capable of developing security skills now most in need, because SANS courses are taught by many of the nation's most accomplished security practitioners. Hands-on training is the hallmark of SANS' events along with the promise that you will be able to put what you learn in SANS courses to work as soon as you get back to the office. Our updated courses reflect the newest attacks, how they work, and what will and what won't work to stop the attacks or mitigate them. You already know these new attacks are really testing your skills. Learn about and try the effective tools to find, block, and decipher the latest hacking attacks.

SANS CDI 2012 is offering these new cutting-edge courses: Security 579: Virtualization and Private Cloud Security, Security 642: Advanced Web App Penetration Testing and Ethical Hacking, Security 575: Mobile Device Security and Ethical Hacking, and Forensics 508: Advanced Computer Forensic Analysis and Incident Response. The rest of our lineup includes basic and advanced courses in penetration testing, auditing, forensics, security management, web app developer, CISSP, and more.

**SANS CDI 2012 is powered by Netwars – Tournament Play.** We'll be running an exciting NetWars competition, available FREE to CDI attendees taking a five or six day class, while seats last. To add extra excitement, SANS CDI 2012 will include our FIRST-EVER NetWars Tournament of Champions, where the best-of-the-best NetWars participants from the past eighteen months will face off to see who comes out on top. Whether you are a first-time NetWars participant looking to have fun and build your skills, or a seasoned champion, remember that seating is limited. Please make sure you sign up for NetWars when you register for a CDI long course.

NetWars Tournaments are a two-evening simulation featuring real-world computer and network security challenges. Participants have fun conquering these challenges as they build skills and demonstrate their abilities in this safe, informal, and engaging event. Many NetWars participants comment about how NetWars really reinforces the lessons they are learning in their courses and expands their vision into other information security arenas. Space is limited, so please register early.

This year, our campus for the main event is the Hilton Washington & Towers. The campus for all of our Forensics courses is the DuPont Circle Hotel, just a short walk away. Both hotels have guestrooms available at the same great rate. This is your opportunity to get unmatched training and sightseeing from either location. See our *Hotel & Travel Information* page for details.

I look forward to seeing you in Washington, DC in December.

Kind regards,

Alan Paller

Alan Paller
Director of Research
The SANS Institute

**Alan Paller**

Here is what some of our 2012 alumni have had to say about their SANS training:

*"Got SANS? SANS always is one of the first places I look for information. Not only because of the quantity – but also the quality."*
-Jarrod Frates, ACS, Inc.

*"It was great to test my skills and to see where I needed more work. I had never participated in anything like that before, and am so glad I did."*
-Sean Nixon,
Morris Communications

*"As always, this SANS course offers information I can immediately apply to my organization!"*
-Leon Noseworthy,
Collect of North Alantic-Qatar

## Contents

# Courses-at-a-Glance

| Please check the website for an up-to-date course list at<br>www.sans.org/cyber-defense-initiative-2012 | | FRI<br>12/7 | SAT<br>12/8 | SUN<br>12/9 | MON<br>12/10 | TUE<br>12/11 | WED<br>12/12 | THU<br>12/13 | FRI<br>12/14 | SAT<br>12/15 | SUN<br>12/16 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AUD507 | Auditing Networks, Perimeters, and Systems | | | PAGE 22 | | | | | | | |
| DEV522 | Defending Web Applications Security Essentials | | | PAGE 24 | | | | | | | |
| FOR408 | Computer Forensic Investigations – Windows In-Depth | | | PAGE 26 | | | | | | | |
| FOR508 | Advanced Computer Forensic Analysis and Incident Response *NEW!* | | | PAGE 28 | | | | | | | |
| FOR563 | Mobile Device Forensics | | | PAGE 30 | | | | | | | |
| FOR610 | Reverse-Engineering Malware: Malware Analysis Tools and Techniques | | | PAGE 32 | | | | | | | |
| MGT305 | Technical Communication and Presentation Skills for Security Professionals | | P 44 | | | | | | | | |
| MGT414 | SANS® +S™ Training Program for the CISSP® Certification Exam *SIMULCAST* | | | PAGE 34 | | | | | | | |
| MGT433 | Securing The Human: Building and Deploying an Effective Security Awareness Program *SIMULCAST* | P 43 | | | | | | | | | |
| MGT512 | SANS Security Leadership Essentials For Managers with Knowledge Compression™ | | | | PAGE 36 | | | | | | |
| MGT514 | IT Security Strategic Planning, Policy, and Leadership | | | | PAGE 38 | | | | | | |
| SEC401 | SANS Security Essentials Bootcamp Style *SIMULCAST* | | | PAGE 2 | | | | | | | |
| SEC434 | Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting | | | | | | | | | P 42 | |
| SEC501 | Advanced Security Essentials – Enterprise Defender *SIMULCAST* | | | PAGE 4 | | | | | | | |
| SEC503 | Intrusion Detection In-Depth | | | PAGE 6 | | | | | | | |
| SEC504 | Hacker Techniques, Exploits, and Incident Handling *SIMULCAST* | | | PAGE 8 | | | | | | | |
| SEC505 | Securing Windows and Resisting Malware | | | PAGE 10 | | | | | | | |
| SEC524 | Cloud Security Fundamentals | P 41 | | | | | | | | | |
| SEC546 | IPv6 Essentials | P 41 | | | | | | | | | |
| SEC560 | Network Penetration Testing and Ethical Hacking | | | PAGE 12 | | | | | | | |
| SEC566 | Implementing and Auditing the Twenty Critical Security Controls – In-Depth | | | | PAGE 14 | | | | | | |
| SEC575 | Mobile Device Security and Ethical Hacking *NEW!* | | | PAGE 16 | | | | | | | |
| SEC579 | Virtualization and Private Cloud Security *NEW!* | | | PAGE 18 | | | | | | | |
| SEC642 | Advanced Web App Penetration Testing and Ethical Hacking *NEW!* | | | PAGE 20 | | | | | | | |
| SEC580 | Metasploit Kung Fu for Enterprise Pen Testing | | | | | | | | | P 42 | |
| Hosted | (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program | | | PAGE 40 | | | | | | | |
| Hosted | Offensive Countermeasures – Defensive Tactics That Actually Work | P 44 | | | | | | | | | |

Security 401

# SANS Security Essentials Bootcamp Style

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**9:00am - 7:00pm (Days 1-5) • 9:00am - 5:00pm (Day 6)**
**46 CPE/CMU Credits • Laptop Required**
**Instructor: Bryce Galbraith**

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.

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

**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).**

## 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**

## SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 45.*

## Bootcamp

**This program has extended hours for 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.

## Bryce Galbraith *SANS Certified Instructor*

As a contributing author of the internationally best-selling 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**.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

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

## 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 will help you quickly master the world of Windows security while showing you the tools you can use to simplify and automate your work. You will complete the day with a solid grounding in Windows security, including the important new features in Windows 8 and Server 2012.

**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

### What Students Are Saying

*"The quick pace is awesome! Moving forward and actively covering topics is invigorating!"* -Steven Park, Boeing

**SANS Security Essentials Bootcamp Style** 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.

Security 501

# Advanced Security Essentials – Enterprise Defender

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**9:00am - 5:00pm • 36 CPE/CMU Credits**
**Laptop Required • Instructor: Eric Conrad**

## Cyber Security Survival Course – Security Enterprise Defender

Cyber security continues to be a critical area for organizations and 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. Security 501 is a follow up to SEC401: SANS Security Essentials (with no overlap) and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course 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 need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts – externally and internally. 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, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting their 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 that is 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 is detected we must react to it 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**

### SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 45.*

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

### What Students Are Saying

*"If you want to be a technology and security leader, this is the course for you!"*
-Andrew Longsworth, Priscoll's

## Eric Conrad *SANS Certified 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**.

GCED

GIAC Certification
**www.giac.org**

SANS INSTITUTE

STI Graduate School
**www.sans.edu**

## 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

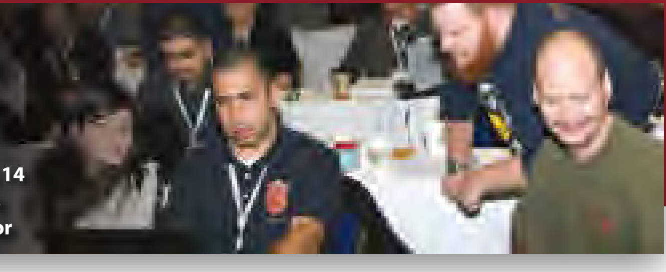
Cyber security is all about managing, controlling, and mitigating risk to critical assets, which in almost every organization are composed of data or information. Perimeters are still important, but we are moving away from a fortress model and moving towards a focus on data. This is based on the fact 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)

Security 503

# Intrusion Detection In-Depth

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**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 **(http://www.sans.org/security-training/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**

## A Sampling of Topics

**TCP/IP**
- Tcpdump Overview and TCP/IP concepts
- ICMP
- Fragmentation
- Stimulus - Response
- Microsoft Protocols
- Domain Name System (DNS)
- IPv6

- **Hands-On tcpdump Analysis**
- Mechanics of running tcpdump
- General network traffic analysis

**Hands-On Snort Usage**
- Various modes of running Snort
- Writing Snort rules

**Intrusion Analysis**
- Intrusion Detection Architecture
- Intrusion Detection/Prevention Analysis

### 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

## Mike Poor *SANS Senior Instructor*

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.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

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

## 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

## 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

## 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

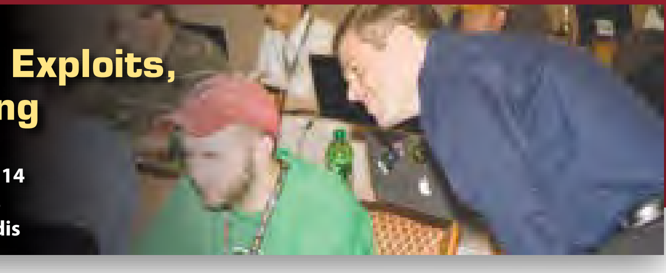
## 503.6 Hands On: IDS Challenge*

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.

Security 504

# Hacker Techniques, Exploits, and Incident Handling



Six-Day Program • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Ed Skoudis

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.

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.**

## 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

## SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 45.*

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

## Ed Skoudis *SANS Faculty Fellow*

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**

## 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.

Security 505

# Securing Windows and Resisting Malware

Six-Day Program • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Jason Fossen

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The Securing Windows and Resisting Malware course is fully updated for Windows Server 2012, Windows 8, Server 2008-R2, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact on users of these changes. You'll see the instructor demo the important steps live, and, if you bring a laptop, you can follow along too. The manuals are filled with screenshots and step-by-step exercises, so you can do the steps alongside the instructor in seminar or later on your own time if you prefer.

We've all got anti-virus scanners, but what else needs to be done to combat malware and intruders using Advanced Persistent Threat (APT) techniques? Today's weapon of choice for hackers is stealthy malware with remote control channels, preferably with autonomous worm capabilities, installed through client-side exploits. While other courses focus on detection or remediation, the goal of this course is to prevent the infection in the first place (after all, first things first).

Especially in Server 2012 and beyond, PowerShell dominates Windows scripting and automation. It seems everything can be managed through PowerShell now. And if there's a needed skill that will most benefit the career of a Windows specialist, it's being able to write PowerShell scripts because most of your competition will lack scripting skills, so it's a great way to make your resume stand out. This course devotes an entire day to PowerShell scripting, but you don't need any prior scripting experience.

This course will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows expertise.

You are encouraged to bring a virtual machine running Windows Server 2012 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 2012 from Microsoft's web site (just do a search on "site:microsoft.com Server 2012 evaluation trial"). You can use Hyper-V, VMware, VirtualBox, or any other virtual machine software you wish.

This is a fun course and a real eye-opener even for Windows administrators with years of experience. Whether you're taking SEC505 live or in OnDemand, get the PowerShell scripts now for the course from **www.sans.org/windows-security** (go to the Downloads link). There is no prior registration required, and all scripts are in the public domain.

## Who Should Attend:

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the SANS Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- IIS administrators and webmasters with servers at risk

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

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

## Jason Fossen *SANS Faculty Fellow*

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**

## 505.1 Hands On: Windows Operating System and Applications Hardening

We start by choosing malware-resistant software and Windows operating systems, then we regularly update that software, limit what software users can run, and then configure that software so that its exploitable features are disabled or at least restricted to work-only purposes. The trick is hardening Windows in a way that is cost-effective, scalable, and with minimal user impact. In this course we'll look at tools like Group Policy, security templates, WSUS, and SCWCMD.EXE to hopefully make it easier. In today's course and during the week, we'll see how to implement many of the 20 Critical Controls.

**Topics:** Metro Apps; WinRT API; UEFI Firmware Vulnerabilities; DEP; ASLR; SEHOP; WSUS; BYOD Issues; OS Hardening; Group Policy; Critical Controls

## 505.2 Hands On: Dynamic Access Control & Restricting Administrative Compromise

Today's course also includes more recommendations for thwarting malware and APT adversaries. Hackers and malware love it when users are members of the local Administrators group on their computers because it makes it easier to compromise the computer. We will talk about what's so dangerous about the Administrators group and how to either get users out of that group or secretly curtail the power of that group.

**Topics:** Dynamic Access Control (DAC); Active Directory; Administrative Powers; Kerberos; Windows Credential Manager vs. KeePass

## 505.3 Hands On: Windows PKI, BitLocker, and Secure Boot

With Windows Certificate Services you can be your own private Certification Authority (CA). BitLocker is manageable through Group Policy and from the command line. BitLocker has automatic encryption key archival features for recovery, requires little or no user training, and can be used to encrypt portable USB drives. With UEFI firmware and Windows 8, you can also use Secure Boot to help fight off bootkits and other malware too.

**Topics:** PKI; Windows PKI; Group Policy; BitLocker, Biometrics; Smart Cards

## 505.4 Hands On: Dangerous Protocols, IPSec, Windows Firewall, and Wireless

Today's course is on securing wireless and wired network access, hardening vulnerable protocols and ports, and using the Windows Firewall with IPSec. IPSec can authenticate users in Active Directory to implement share permissions for TCP and UDP ports based on the user's global group memberships. And as more of our servers are moved out to the cloud, we will rely on SSL, RDP and IPSec even more.

**Topics:** SSL; RDP; SMBv3; NetBIOS; LLMNR; DNS; Group Policy; IPSec; Windows Firewall; WPA2; RADIUS

## 505.5 Hands On: Securing IIS Web Servers

In this course, we will talk about how to harden the OS, how to strip IIS down to its essentials to reduce its attack surface, how to enforce authentication and authorization rules, how to implement application-layer HTTP/FTP filtering rules, and in general how to help keep your website from becoming another victim statistic. We will also see how to require SSL/TLS for the greatly improved FTP service and how to configure an FTP server farm to provide secure remote access to internal file servers.

**Topics:** Server Hardening; WebDEV; IPSec; XML Configuration; IIS Authentication and Authorization; Web-Based Applications; Logging and Auditing; FTPS

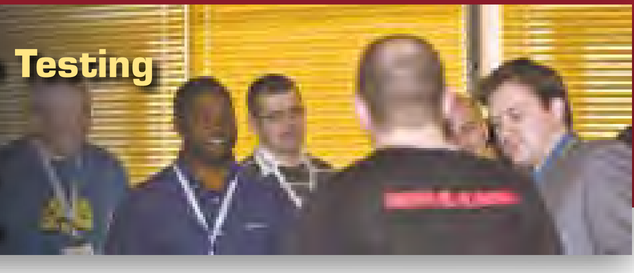
## 505.6 Hands On: Windows PowerShell Scripting

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:** PowerShell; Windows Management Instrumentation (WMI); Writing Your Own Scripts

Security 560

# Network Penetration Testing and Ethical Hacking



**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**9:00am - 5:00pm • 36 CPE/CMU Credits**
**Laptop Required • Instructor: John Strand**

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.

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.

## 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**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

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

## What Students Are Saying

*"Can't overemphasize the value in getting wisdom from a seasoned, experienced penetration tester."*

-Sean Verity, MSUFCU

## John Strand *SANS Senior Instructor*

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: Hacker Detection for System Administrators and the co-author for SEC580: Metasploit Kung Fu for Enterprise Pen Testing. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He also is also 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.

## 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.

Security 566

# Implementing and Auditing the Twenty Critical Security Controls - In-Depth

**Five-Day Program • Mon, Dec 10 - Fri, Dec 14**
**9:00am - 5:00pm • 30 CPE/CMU Credits**
**Laptop Required • Instructor: James Tarala**

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

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

## James Tarala *SANS Senior Instructor*

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.

## 566.1 Hands On: Introduction and Overview of the 20 Critical Controls*

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: Critical Controls 3,4,5, and 6*

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: Critical Controls 7, 8, 9, 10, and 11*

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: Critical Controls 12, 13, 14, and 15*

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: Critical Controls 16, 17, 18, 19, and 20*

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.

Security 575

# Mobile Device Security and Ethical Hacking

New Course!

Six-Day Program • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Peter Szczepankiewicz

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**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

## 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.

## Peter Szczepankiewicz *SANS Certified Instructor*

Formerly working with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a senior security engineer with IBM. People lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. Peter expounds, "Putting together networks only to tear them apart, is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place."

## 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

## 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 • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
*Laptop Provided For Class Use* • Instructor: Paul A. Henry

## For the SEC579: Virtualization and Private Cloud Security course, a laptop will be provided for class use.

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.

### 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

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.

The class starts out with two days of architecture and security design for both virtualization and private cloud infrastructure. The next two days will help you adapt your existing security policies and practices to the new virtualized or cloud-based infrastructure. 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?

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

## Paul A. Henry *SANS Senior Instructor*

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.

## 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*

Today, 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 traditional 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*

Today 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*

Today, we 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, we 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.

Security 642

# Advanced Web App Penetration Testing and Ethical Hacking

New Course!

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**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 the 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.

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 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.

## Who Should Attend:

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

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

## Kevin Johnson *SANS Senior Instructor*

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. Kevin's involvement in open-source projects is spread across a number of projects and efforts. 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 certified instructor for SANS and the author of SEC542: Web App Pen 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.

## 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.

Audit 507

# Auditing Networks, Perimeters, and Systems

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**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

## David Hoelzer *SANS Faculty Fellow*

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**.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

## 507.1 Audit Principles, Risk Assessment & 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

Developer 522

# Defending Web Applications Security Essentials

**Six-Day Program • Sun, Dec 9 - Fri, Dec 14**
**9:00am - 5:00pm • 36 CPE/CMU Credits**
**Laptop Required • Instructor: Jason Lam**

## 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**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

## What Students Are Saying

*"I really appreciate the world experience that the instructor brings. Showing real logs and other demos make for a rich learning experience." -*

-Diane Johnson Nordstrom, Inc.

## Jason Lam *SANS Certified Instructor*

Jason is a senior security analyst at a major financial institution in Canada. His recent SANS Institute courseware development includes Defending Web Application Security Essentials and Web Application Pen Testing Hands-On Immersion. Jason started his career as a programmer before moving on to ISP network administration, where he handled network security incidents, which sparked his interest in information security. Jason specializes in web application security, penetration testing, and intrusion detection. He currently holds a BA in computer science from York University in Toronto, Ontario, as well as the CISSP, GCIA, GCFW, GCUX, GCWN, and GCIH certifications.

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

## 522.1 Hands On: Web Basics and Authentication Security*

We begin with an overview of the software development life cycle and security. Proper security control and process during development is essential to having secure applications, as well as the essential technologies that are at play in web applications. You can't win the battle if you don't understand what you are trying to defend. Learn how web applications work and the security concepts related to them. We discuss the authentication aspect of web applications in depth, including the vulnerabilities, followed by examples of exploitation and the mitigations that could be implemented in the short and long term. Learn the right way of planning for access during the development life cycle and the common pitfalls with access control by starting with the vulnerabilities, mitigation and testing, followed by a section on the best practice on authorization.

**Topics:** HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

## 522.2 Hands On: Web Application Common Vulnerabilities and Mitigations*

Since the Internet does not guarantee secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. We cover the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security. We discuss session management in web applications and a hacker's technique in attacking the session mechanism and related defense strategies. The best practices of session security and cross-site request forgery are discussed to ensure your application's session management is as strong as possible. Then we cover business logic flaws and concurrency; the difficult topics to detect by automated scanners. The day ends with input-related flaws and SQL injection, the basic mechanics of these vulnerabilities, followed by the real-world attack trends. We delve into the mitigation and the best practice in avoiding these critical vulnerabilities.

**Topics:** SSL vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrency; Input Related Flaws and Related Defense; SQL Injection Vulnerabilities, Testing, and Defense

## 522.3 Hands On: Proactive Defense and Operation Security*

Day three begins with a detailed discussion on cross-site scripting, related mitigation, and testing strategy, as well as HTTP response splitting. Defending the platform and host by locking down the web environment is an essential topic. We will discuss the correct approach to handling incidents and handling logs and the intrusion detection aspect of web application security. Then we will turn our focus to the proactive defense mechanism so that we stay ahead of the bad. Topics such as file upload handling, intrusion detection, honeypot, redirection, in-depth authentication information, and practical input validation strategy will be covered. This information will give you the extra edge in defending your application.

**Topics:** Web Environment Configuration Security; Intrusion Detection in Web Application; Incident Handling; Honeytoken

## 522.4 Hands On: AJAX and Web Services Security*

Day four is dedicated to AJAX and web services security. Asynchronous JavaScript and XML (AJAX) and web services are currently the most active areas in web application development. Security issues continue to arise as organizations are diving head first into insecurely implementing new web technologies without first understanding them. We cover the security issues, mitigation strategies, and general best practices for implementing AJAX and web Services. We also examine real-world attacks and trends to give you a better understanding of exactly what you're protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

**Topics:** Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

## 522.5 Hands On: Cutting-Edge Web Security*

Day five has a strong focus on cutting-edge web application technologies and current research area. Clickjacking and DNS rebinding are difficult to defend against and require multiple defense strategies to be successful. We cover the new generation of single sign on solutions such as OpenID and the implication of using these authentication systems and the common gotchas to avoid. The Web2.0 adoption, the use of Java applet, Flash, ActiveX, and Silverlight are on the increase. The security strategies of defending these technologies are discussed so these client-side technologies can be locked down properly.

**Topics:** Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single Sign On Solution and Security; IPv6 Impact on Web Security

## 522.6 Hands On: Capture & Defend the Flag Exercise*

Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. The major focus is a large lab, which ties the lessons learned during the week together and reinforces the lessons by practicing them hands on. You are provided with a virtual machine implementing a complete database driven dynamic website. A custom tool is used to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. It will be up to you to decide which vulnerabilities are real and which are false positives. You are then asked to mitigate the vulnerabilities. The scanner will score students as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. You will learn hands on how to secure the web application, starting with the operating system, the web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

**Topics:** Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

*This course is available to Developer 522 participants only.

Forensics 408

# Computer Forensic Investigations – Windows In-Depth

Six-Day Program • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Rob Lee

**Please Note:**

**This course will be taught at the Digital Forensics Campus – The DuPont Circle Hotel**

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.

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

## 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)**

## Rob Lee *SANS Faculty Fellow*

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**.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

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

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

## 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.

Forensics 508 BRAND NEW!

# Advanced Computer Forensic Analysis and Incident Response

Six-Day Program • Sun, Dec 9 - Fri, Dec 14
9:00am - 5:00pm • 36 CPE/CMU Credits
Laptop Required • Instructor: Chad Tilbury

**Please Note:**

**This course will be taught at the Digital Forensics Campus – The DuPont Circle Hotel**

***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.

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

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

The SIFT Advanced Toolkit consists of:

- **F-Response Tactical**
  - **Tactical enables investigators to access remote system via the network**
  - **Perfect for incident response investigating compromised systems**
- **SANS VMware based Forensic Analysis Workstation (SIFT Workstation)**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Bootable Forensic Distribution**
- **Course DVD loaded with case examples, tools, and documentation**

*Our adversaries are good and getting better. Are we learning how to counter them? Yes we are. Learn how.*

## Chad Tilbury *SANS Certified Instructor*

Chad Tilbury has spent over twelve 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 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, GREM, and CISSP certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics.

## 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

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

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

GIAC Certification
**www.giac.org**

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

STI Graduate School
**www.sans.edu**

## 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.

Forensics 563

# Mobile Device Forensics

Five-Day Program • Sun, Dec 9 - Thu, Dec 13
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Terrance Maguire and Donnie Tindall

**Please Note:**

**This course will be taught at the Digital Forensics Campus – The DuPont Circle Hotel**

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.

## 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

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

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

## Terrance Maguire *SANS Certified Instructor*

Terrance Maguire is the chief scientist and managing member of Digital Forensics Academy LLC, conducting digital forensic investigations, research and development in computer forensics and provides training to the government and commercial sectors. He has over 21 years of experience in physical and digital forensics investigations. Mr. Maguire is a professional lecturer at The George Washington University and a certified SANS instructor in computer forensics.

## Donnie Tindall *SANS Instructor*

Donnie Tindall is a Digital Forensics Analyst at Basis Technology, where he provides on-site mobile device forensic support for the U.S. Government, including development and teaching of mobile forensic courses to government and military users. Previously, he worked as a consultant to the FBI Terrorist Explosive Device Analytical Center, where he was responsible for mobile device forensics on media associated with Improvised Explosive Devices. Prior to that, Donnie served in the United States Marine Corps for 5 years as an electronics technician; this experience has benefited him greatly in performing chip-off extractions, as well as allowing him to develop custom hardware solutions to solve forensic challenges. Donnie has performed hundreds of mobile device extractions, including Nokia, BlackBerry, Android and iPhones. He is also an IACIS Certified Forensic Computer Examiner.

## 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: iOS 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

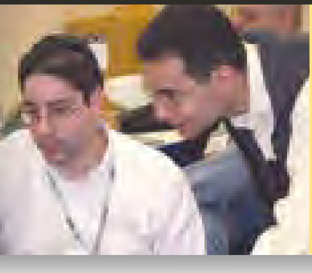
***Throughout this course, we provide practical, hands-on exercises to give you ample opportunities to explore mobile devices and the data they contain.***

*This course is available to Forensics 563 participants only.

Forensics 610

# Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Program • Sun, Dec 9 - Thu, Dec 13
9:00am - 5:00pm • 30 CPE/CMU Credits
Laptop Required • Instructor: Lenny Zeltser



**Please Note:**

**This course will be taught at the Digital Forensics Campus – The DuPont Circle Hotel**

**This malware analysis course prepares forensic investigators, incident responders, and malware specialists to reverse-engineer malicious software using practical tools and techniques.**

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!

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.

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity.

Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts navigate through malicious executables using a debugger and a disassembler.

## Lenny Zeltser *SANS Senior Instructor*

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**.

## 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

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

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

GIAC Certification
**www.giac.org**

STI Graduate School
**www.sans.edu**

## 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.

### What Students Are Saying

*"Highly valuable content, greatly increased my understanding of malware and techniques to reverse engineer."*

-Kenneth Miltenberger, US Coast Guard

### REM course on YouTube

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

Management 414

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

Six-Day Program • Sun, Dec 9 - Fri, Dec 14
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: Dr. Eric Cole

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.

## SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. *More info on page 45.*

## 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)**

## 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**

## Dr. Eric Cole *SANS Faculty Fellow*

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.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
**www.giac.org**

## You Will Receive With This Course:

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

## 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 and Network Security*

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 & Compliance, and 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.

Management 512

# SANS Security Leadership Essentials For Managers with Knowledge Compression™

**Five-Day Program • Mon, Dec 10 - Fri, Dec 14**
**9:00am - 6:00pm (Days 1-4) • 9:00am - 5:00pm (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.

**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**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

## There are three goals for this course and certification:

**1) Establish a minimum standard for IT security knowledge, skills, and abilities.**

**2) Establish a minimum standard for IT management knowledge, skills, and abilities.**

**3) 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.**

## Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a postgraduate 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**

## 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 IP Concepts, Attacks Against the Enterprise and 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.

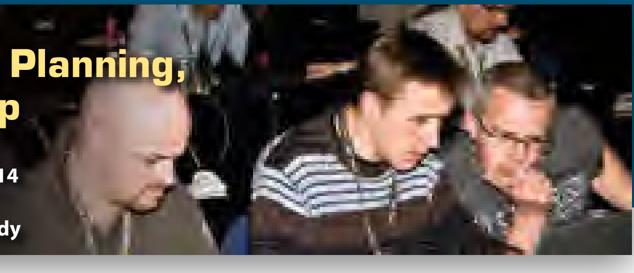
**Security Leaders and Managers** earn the highest salaries (well over six figures) in information security and are near the top of IT. Needless to say, to work at that compensation level, excellence is demanded. These days, security managers are expected to have domain expertise as well as the classic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

### What Students Are Saying

*"This course covers a wide array of concerns and ties IT security to operational and business objectives."* -Eugene Templet, LAMMICO

Management 514

# IT Security Strategic Planning, Policy, and Leadership



**Five-Day Program • Mon, Dec10 - Fri, Dec 14**
**9:00am - 5:00pm • 30 CPE/CMU Credits**
**Laptop Required • Instructor: G. Mark Hardy**

You know the expression, "What got you here, won't keep you here." I have met many people who were successful in terms of being technical, but they have struggled in management, especially in senior management positions. This course is designed to help with the transition from technical person to manager to leader and give you the tools to be successful as a senior IT strategic planner, policy author, and leader.

Strategic planning is hard for people in IT and IT Security because we spend so much time responding and reacting. Some of us have been exposed to a SWOT or something similar in an MBA course, but we almost never get to practice until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack.

In this course you will learn the entire strategic planning process: what it is and how to do it; what lends itself to virtual teams, and what needs to be done face to face. We will practice building those skills in class. Topics covered in depth include how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. We will also discuss the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, and revising the plan.

## Who Should Attend:

**This course is designed and taught for existing, recently appointed, and aspiring IT and IT Security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.**

Policy is a manager's opportunity to express expectations for the workforce, to set the boundaries of acceptable behavior and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that." Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy successfully.

The third focus of the course is on management and leadership competencies. Leadership is a capability that must be learned, exercised and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and the vision to see and effectively use available resources toward the end goal. However, leaders and followers influence each other toward the goal; it is a two-way street where all parties perform their functions to reach a common objective.

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

Effective leadership entails persuading team members to accomplish their objectives while removing obstacles and maintaining the well-being of the team in support of the organization's mission. Grooming effective leaders is critical to all types of organizations, as the most effective teams are cohesive units that work together toward common goals with camaraderie and a can-do spirit!

Leadership tends to be a bit "squishy" and courses covering the topic are often based upon the opinions of people who were successful in the marketplace. However, success can be as much a factor of luck as skill, so we base this part of the course on five decades of the research of social scientists and their experiments going as far back as Maslow and on research as current as Sunstein and Thaler. We discuss leadership skills that apply to commercial business, non-profit, not-for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

## G. Mark Hardy *SANS Instructor*

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

## 514.1 Hands On: An Approach to Strategic Planning*

Our approach to strategic planning is that there are activities that can be done virtually in advance of a retreat, and then other activities are best done in a retreat setting. On the first day, we will talk about some of the activities that can be done virtually.

**Topics:** How to Plan the Plan; Historical Analysis; Horizon Analysis; Visioning; Environmental Scans (SWOT, PEST, Porters etc.); Mission, Vision, and Value Statements

## 514.2 Hands On: Planning To Ensure Institutional Effectiveness*

This will include the retreat section of the course where we do the core planning activities of candidate selection, prioritization, and development of the roadmap.

## 514.3 Hands On: Security Policy Development*

You will experience the most in-depth coverage of security policy ever developed. By the end of the course your head will be spinning. Students and other SANS instructors who have seen the scope of the material have the same comment, "I never realized there is so much to know about security policy." Any security manager, anyone assigned to review, write, assess or support security policy and procedure, can benefit from Policy in Depth. You will learn what policy is, positive and negative tone, consistency of policy bullets, how to balance the level of specificity to the problem at hand, the role of policy, awareness and training, and the SMART approach to policy development and assessment. We cover different levels of policy from Information Security Management System (ISMS) governing policy to detailed issue-specific policies like acceptable use, approved encryption and end of life disposal of IT assets.

**Topics:** Policy Establishes Bounds for Behavior; Policy Empowers Users to do the Right Thing; Should and Shall, Guidelines, and Policy; ISMS as Governing Policy; Policy Versus Procedure; Policy Needs Assessment Process; Organizational Assumptions, Beliefs and Values (ABVs); Relationship of Mission Statement to Policy; Organizational Culture

## 514.4 Hands On: Comprehensive Security Policy Assessment*

In the policy section of the course, you will be exposed to over 100 different policies through an instructional delivery methodology that balances lecture, labs, and in-class discussion. We will emphasize techniques to create successful policy that users will read and follow; policy that will be accepted by the business units because it is sensitive to the organizational culture; and policy that uses the psychology of information security to guide implementation.

**Topics:** Using the Principles of Psychology to Implement Policy; Applying the SMART Method to Policy; How Policy Protects People, Organizations and Information; Case Study, the Process to Handle a New Risk (Sexting); Policy Header Components and How to Use Them; Issue-Specific Policies; Behavior-Related Polices, Acceptable Use, and Ethics; Warning Banners; Policy Development Process; Policy Review and Assessment Process; Wrap-up, the Six Golden Nuggets of Policy

## 514.5 Hands On: Leadership and Management Competencies*

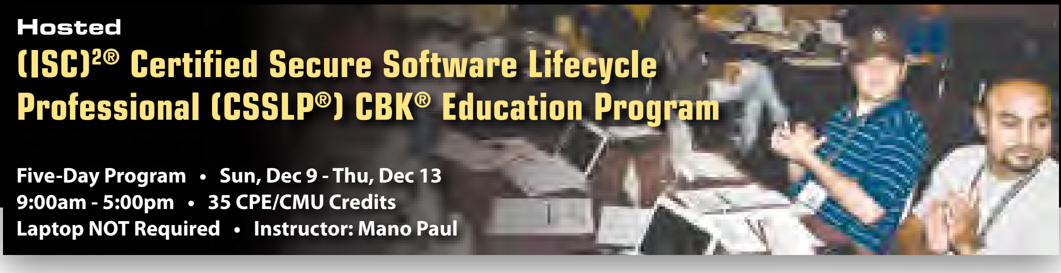
In the fifth and final day we pull it all together and apply the technical knowledge to the art of management. The management practicum covers a number of specific applications and topics concerning information security. We'll explore proven techniques for successful and effective management, empowering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

***There are three goals for the leadership component of this course:***

- **Establish a minimum standard for knowledge, skills, and abilities required to develop leadership**
- **Understand and leverage the motivational requirements of employees**
- **Establish a baseline understanding of the skills necessary to migrate from being a manager to being a leader**

**Topics:** Leadership Building Blocks; Coaching & Training; Change Management; Team Development; Motivating; Developing the Vision; Leadership Development; Building Competencies; Importance of Communication; Self-direction; Brainstorming; Relationship Building; Teamwork Concepts; Leader Qualities; Leadership Benefits

*This course is available to Management 514 participants only.



Hosted

# (ISC)$^{2®}$ Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

**Five-Day Program • Sun, Dec 9 - Thu, Dec 13**
**9:00am - 5:00pm • 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.

## 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

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**
- **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**

**Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.**

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.***

## 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.

## Security 524
# Cloud Security Fundamentals

**Two-Day Course • Fri, Dec 7 - Sat, Dec 8 • 9:00am - 5:00pm • 12 CPE/CMU Credits**
**Laptop Required • Instructor: Paul A. Henry**

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.

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. 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.

***Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.***

## Security 546
# IPv6 Essentials

**Two-Day Course • Fri, Dec 7 - Sat, Dec 8 • 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.

## Security 434

# Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting

**Two-Day Course • Sat, Dec 15 - Sun, Dec 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits**
**Laptop Required • Instructor: Dr. Eric Cole**

This first-ever dedicated log management class teaches system, network, and security logs, their analysis and management and covers the complete lifecycle of dealing with logs: the whys, hows and whats. You will learn how to enable logging and then how to deal with the resulting data deluge by managing data retention, analyzing data using search, filtering and correlation as well as how to apply what you learned to key business and security problems. The class also teaches applications of logging to forensics, incident response and regulatory compliance.

In the beginning, you will learn what to do with various log types and provide brief configuration guidance for common information systems. Next, you will learn a phased approach to implementing a company-wide log management program, and go into specific log-related tasks that needs to be done on a daily, weekly, and monthly basis in regards to log review and monitoring. Everyone is looking for a path through the PCI DSS and other regulatory compliance maze and that is what you will learn in the next section of the course. Logs are essential for resolving compliance challenges; this class will teach you what you need to concentrate on and how to make your log management compliance-friendly. And people who are already using log management for compliance will learn how to expand the benefits of you log management tools beyond compliance. You will learn to leverage logs for critical tasks related to incident response, forensics, and operational monitoring. Logs provide one of the key information sources while responding to an incident and this class will teach you how to utilize various log types in the frenzy of an incident investigation.

Finally, the class author, Dr. Anton Chuvakin, probably has more experience in the application of logs to IT and IT security than anyone else in the industry. This means he and the other instructors chosen to teach this course have made a lot of mistakes along the way. You can save yourself a lot of pain and your organization a lot of money by learning about the common mistakes people make working with logs.

***Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.***

## Security 580

# Metasploit Kung Fu for Enterprise Pen Testing

**Two-Day Course • Sat, Dec 15 - Sun, Dec 16 • 9:00am - 5:00pm • 12 CPE/CMU Credits**
**Laptop Required • Instructor: Kevin Johnson**

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.

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.

## Management 433

# Securing The Human: Building & Deploying an Effective Security Awareness Program

**Two-Day Course • Fri, Dec 7 - Sat, Dec 8 • 9:00am - 5:00pm • 12 CPE/CMU Credits**
**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.

## Who Should Attend:

- Security awareness training officers
- Chief Security Officers (CSO's) and security management
- Security auditors, governance, and compliance officers
- Training, human resources and communications staff
- Organizations regulated by HIPAA, FISMA, FERPA, PCI-DSS, ISO/IEC 27001, FERPA, SOX, or any other compliance-driven standards.
- Anyone responsible for planning, deploying, or maintaining an awareness program

## SANS SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast. ***More info on page 45.***

www.securingthehuman.org

SANS SECURING THE HUMAN

MANAGEMENT SKILL-BASED COURSE

Management 305

# Technical Communication and Presentation Skills for Security Professionals

**One-Day Course • Sat, Dec 8 • 9:00am - 5:00pm • 6 CPE/CMU Credits**
**Laptop Required • Instructor: David 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.

### Who Should Attend:

- All SANS Masters students
- Auditors
- Security architects
- Managers
- Incident handlers
- Forensic examiners
- Any individual seeking to improve his technical writing, presentation and reporting skills
- Individuals who write reports or make presentations to management
- Awareness trainers, local mentors
- Management should strongly consider sending individuals who must write and present reports and project plans to this course.

HOSTED SKILL-BASED COURSE

# Offensive Countermeasures: Defensive Tactics That Actually Work

**Two-Day Program • Fri, Dec 7 - Sat, Dec 8 • 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:

PaulDotCom

### Who Should Attend:

- Security professionals and systems administrators who are tired of playing catch-up with attackers.

***Please check the online course description for any updates, prerequisites, laptop requirements, or special notes at www.sans.org/cyber-defense-initiative-2012/event.php.***

SANS Simulcast

# You don't have to miss out on SANS' top-rated training. Attend select SANS CDI 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 four 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

The following SANS CDI 2012 courses will be available via SANS Simulcast:

***Short Courses:***
MGT433

***Long Courses:***
MGT414 SEC401
SEC501 SEC504

## SANS Event Simulcast classes are:

**COST-EFFECTIVE** - You can save thousands of dollars on travel costs, making Event Simulcast an ideal solution for students working with limited training budgets or travel bans.

**ENGAGING** - Event Simulcast classes are live and interactive, allowing you to ask questions and share experiences with your instructor and classmates.

**CONDENSED** - Complete your course quickly; all SANS Event Simulcast classes take no longer than six days to complete.

**REPEATABLE** - Event Simulcast classes are recorded and placed in an online archive in case you have to miss part of the class or just wish to view the material again at a later date.

**COMPLETE** - You will receive the same books, discs, and MP3 audio files that conference students receive, and you will see and hear the same information as it is presented at the live event.

To register for a SANS CDI 2012 Simulcast course, please visit www.sans.org/simulcasts

POWERED BY NETWARS

*Tournament for CDI course attendees includes*

**TOURNAMENT OF CHAMPIONS**

December 12-13, 2012

## 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: December 12 & 13.

Prizes will be awarded at the conclusion of the games.
REGISTRATION IS LIMITED AND IS FREE
for students attending any long course at SANS CDI 2012
*(NON-STUDENTS ENTRANCE FEE IS $999).*

**Register at**
**www.sans.org/cyber-defense-initiative-2012**

*In-Depth, Hands-On InfoSec Skills – Embrace the Challenge*

# NETWARS TOURNAMENT OF CHAMPIONS

*SANS is hosting the first ever Tournament of Champions where the best-of-the-best from past NetWars Competitions as well as the winners of this year's Cyber Defense Exercise (CDX), National Collegiate Cyber Defense Competition (NCCDC), CyberLympics and Cyber Patriot have been invited to face off. We have also invited some of the top high school and college students from the Cyber Camps and Cyber Foundations to participate as well. We expect to have some of the most capable security professional in the country matching wits with each other in our ultimate tournament!*

**NetWars Tournament of Champions
will be held at
SANS CDI 2012 on December 12-13
at the Washington Hilton Towers.**

**Awards will be given for the
top three professionals and the top three students.
We will also be giving special awards
based on individual achievements in the tournament.
Army Cyber Commander Lieutenant General Hernandez
invited to present awards.**

**Members of the national press have been invited and we expect this to be well attended and publicized.**

**Space is limited.
If you believe you qualify for this Tournament,
please contact us at netwars@sans.org
and we will validate and register you.
The $999 fee will be waived for all individuals
who qualify for the Tournament of Champions!**

# SANS CDI 2012 Special Events

## SANS @Night Evening Talks

**Enrich your SANS training experience! Evening talks given by our instructors and selected subject matter experts help you broaden your knowledge, get the most for your training dollar, and hear from the voices that matter in computer security.**

### Keynote: Future Trends in Network Security *Dr. Eric Cole*

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work. Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible. Dr. Cole's in-depth, cross-industry experience allows him to give relevant examples in every instance. This presentation covers security issues that are relevant to IT managers and administrators alike.

### Why our Defenses are Failing Us – One Click is All it Takes *Bryce Galbraith*

Organizations are spending unprecedented amounts of money in an attempt to defend their assets – yet all too often, one click is all it takes for it all to come toppling down around them. Every day we read in the news about national secrets, intellectual property, financial records and personal details being exfiltrated from the largest organizations on Earth. How is this being done? How are they bypassing our defenses (e.g. strong passwords, non-privileged accounts, anti-virus, firewalls/proxies, IDS/IPS, logging, etc.) And most importantly, what can we do about it? A keen understanding of the "true" risks we face in today's threatscape is paramount to our success.

### Gone in 60 Minutes: *60 minutes from discovery through exploitation - how fast is your patching process?* *David Hoelzer*

In this fast paced talk, David Hoelzer will walk you through the process a hacker might go through to discover a flaw, engineer a working proof of concept and then convert that into a working Metasploit exploit module... All in 60 minutes. If you're not a technical person, don't worry. There's still plenty to take away from this talk. If you are a technical person come along and see if there's a trick or two that you can use!

### Building a Portable Private Cloud *Paul A. Henry*

Security researchers, forensics practitioners and those IP Pros simply aspiring to learn virtualization "hands-on" typically had only two choices: build an expensive rack of servers; put up with the noise and pay huge power bills or to try working within the constraints of VMware Workstation and suffering the performance problems while also missing the real-world bare-metal virtualization experience. Today, there is perhaps a better alternative available - the Apple Mac Mini Server makes a great bare-metal VMware 5.0 workhorse. This presentation will demonstrate how it can be done.

### 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 to:

- Assess suspicious Windows executable files
- Explore infection artifacts in a network capture file
- Examine malicious document and media files

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.

### Tactical SecOps: A Guide to Precision Security Operations *Kevin Johnson*

Security has become a major part of what our organizations expect and require. Our operations teams are being bombarded from everyone including the audit/legal teams, security teams and the upstart hactivist script kiddie that found the low hanging fruit of our network. But all of this happens on top of the daily grind we have in just keeping our systems running.

In this talk, we will be exploring how operational teams can embed security testing within their current activities. By using an understanding of attacks and history of operational responsibilities, Kevin has built a guide for IT operations which includes security testing and verification techniques. This guide uses their professionally evil approach to security and provides understandable and open source methods and tools that can provide the precision information that is needed for response instead of the flood of noise most admins get from the tools being pushed on them today.

### 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.

### What's New in Server 2012 and Windows 8 *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, 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!

***For the latest info on SANS @Night evening talks, please visit***
***www.sans.org/cyber-defense-initiative-2012/night.php***

SANS CDI 2012

## Vendor Expo

**Tuesday, December 11, 2012**
**12:00pm - 1:30pm and 5:00pm - 7:00pm**

**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 one-day vendor expo, an added bonus to registered training event attendees.**

# 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

**13 of the courses being offered at SANS CDI 2012 may be applied towards an STI Master's Degree.**

The Master of Science degree programs of study leading to proficiency in Information Security Engineering (MSISE) and Management (MSISM) are developed and delivered for you using a scholar-practitioner philosophy. *Scholar-practitioner* means they are designed to provide a sound theoretical experience delivered through practitioner's lens. The focus of the programs is solutions at the enterprise level, meaning you will be able to make an impact at on an organization, total system or sovereign entity.

***The MSISE prepares you to:***

- Architect security approaches
- Establish adaptive security paradigms
- Ensure adaptive anticipatory detection
- Guide adaptive measured response strategies

***The MSISM prepares you to:***

- Develop and manage secure organizations
- Sponsor of adaptive security paradigms
- Foster adaptive anticipatory detection
- Advocate capacity for adaptive measured response strategies

## The STI Difference

***With an STI degree you will:***

- Build the necessary technical, leadership and communication skills needed in the information security industry;
- Earn seven or more highly revered Global Information Assurance Certifications (GIAC);
- Build your reputation in the industry through the publication of papers and projects.

**www.sans.edu | info@sans.edu**

**720.941.4932**

***New cohorts begin in January at SANS Security East 2013 and in September at SANS Network Security 2013 in Las Vegas. Learn more about STI Cohorts at www.sans.edu/interest/cohort***

# 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 Approved Baseline 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 |

| CND Analyst | CND Infrastructure Support |
|---|---|
| **GCIA** | SSCP |
| **GCIH** | CEH |
| CEH | |

| CND Incident Responder | CND Auditor |
|---|---|
| **GCIH** | **GSNA** |
| CSIH | CSIA |
| CEH | CEH |

| CN-SP Manager |
|---|
| CISSP - ISSMP |
| CISM |

## SANS Training Courses for DoD Approved Certifications

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

***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***

# 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*
  CISSP certification

### 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 and Resisting Malware (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) |

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.

# SANS Future

## SANS **CyberCon** 2012

Virtual Conference
October 8-13, 2012
www.sans.org/cybercon-2012

## SANS **Seattle** 2012

Seattle, WA
October 14-19, 2012
www.sans.org/seattle-2012

## SANS **Baltimore** 2012

Baltimore, MD
October 15-20, 2012
www.sans.org/baltimore-2012

## SANS **Chicago** 2012

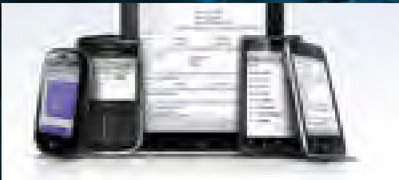
Chicago, IL
October 27 - November 5, 2012
www.sans.org/chicago-2012

## SANS **San Diego** 2012

San Diego, CA
November 12-17, 2012
www.sans.org/san-diego-2012

## SANS **San Antonio** 2012

San Antonio, TX
November 27 - December 2, 2012
www.sans.org/san-antonio-2012



## SANS **Mobile Device Security** Summit 2013

Anaheim, CA | January 7-14, 2013
www.sans.org/mobile-device-security-summit-2013

## SANS **Virtualization and Cloud Computing** Summit 2013

Anaheim, CA | January 7-14, 2013
www.sans.org/virtualization-cloud-summit-2013

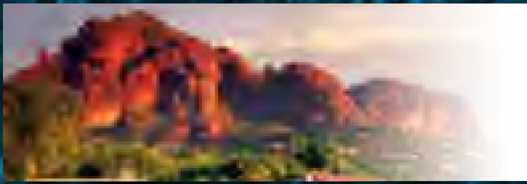
## SANS **North American SCADA and Process Control** Summit 2013

Lake Buena Vista, FL | February 6-15, 2013
www.sans.org/north-american-scada-2013

# Training Events

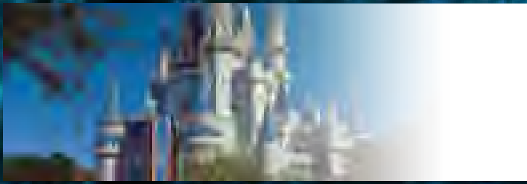
## SANS **Security East** 2013

New Orleans, LA
January 16-21, 2013
www.sans.org/security-east-2013



## SANS **Scottsdale** 2013

Scottsdale, AZ
February 17-23, 2013
www.sans.org/scottsdale-2013



## **SANS** 2013

Orlando, FL
March 6-16, 2013
www.sans.org/sans-2013

## SANS **Monterey** 2013

Monterey, CA
March 22-27, 2013
www.sans.org/monterey-2013

## SANS **Northern Virginia** 2013

Reston, VA
April 14-20, 2013
www.sans.org/northern-virginia-2013

## SANS **Cyber Guardian** 2013

Baltimore, MD
April 15-20, 2013
www.sans.org/cyber-guardian-2013

## SANS **Security West** 2013

San Diego, CA
May 8-15, 2013
www.sans.org/security-west-2013

## **SANSFIRE** 2013

Washington, DC
June 13-23, 2013
www.sans.org/sansfire-2013

## SANS **Rocky Mountain** 2013

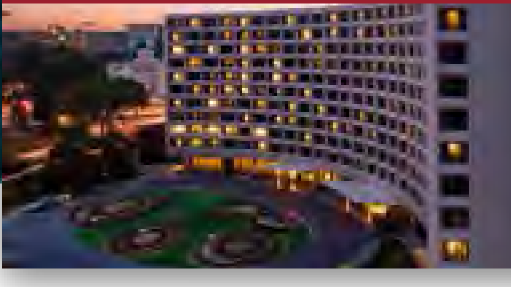
Denver, CO
July 15-22, 2013
www.sans.org/rocky-mountain-2013

SANS CDI 2012

# Hotel & Travel Information

***Please Note: There are two Campus Locations for SANS CDI 2012***

*Main-Event Campus* – Hilton Washington *Digital-Forensics Campus* – The DuPont Circle Hotel



*Main-Event Campus*

## Hilton Washington & Towers

1919 Connecticut Avenue NW
Washington, DC 20009
Tel: (202) 232-0438
www.thewashingtonhilton.com

Stay at the Hilton Washington, a recently-restored urban retreat where legendary hospitality, thoughtful amenities and exceptional experiences awaits guests in a location unmatched in the nation's capital. The hotel's contemporary accommodations feature a range of modern conveniences and amenities to ensure your trip is relaxing and stress-free. Workout, relieve stress, or relax in the LivingWell Health Club. Dine or meet with friends in one of the hotel's restaurants and lounges. Or take a walk and visit the boutiques, spas, pubs, and bistros in nearby DuPont Circle, Georgetown District, or the up-and-coming U-Street Corridor.

### Special Rates Available

**A special discounted rate of $199.00 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 high-speed Internet in your room and are only available through November 15, 2012. To make reservations please call (800) HILTONS (800-445-8667) and ask for the SANS Institute group rate.**

*Digital-Forensics Campus*

## The DuPont Circle Hotel

1500 New Hampshire Ave, NW
Washington, DC 20036
Tel: (855) 523-6953
www.doylecollection.com/locations/washington_dc_hotels/the_dupont_circle_hotel.aspx

The Dupont Circle Hotel is the new standard bearer for an energetic and vibrant Washington, DC that's rapidly claiming its place among the most happening of cities in the world. Ideally located overlooking Washington, DC's Dupont Circle, it is within easy walking distance of leafy, European-style avenues with their embassies, cafés and bookshops. It is the perfect base from which to explore the history of this great city and to enjoy its vibrant and hip social scene.

### Special Rates Available

**A special discounted rate of $199.00 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 high-speed Internet in your room and are only available through November 15, 2012. To make reservations please call (855) 523-6953) and ask for the SANS Institute group rate.**

### Top 5 Reasons to Stay at an Event Campus

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS Block.
2. No need to factor in daily cab fees, parking expense and the time associated with travel to alternate hotels.
3. By staying at Hilton Washington or The DuPont Circle Hotel, 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 Hilton Washington that you won't want to miss!
5. Most Special Events & SANS @Night Presentations will be held at the Hilton Washington – Main Event Campus! In addition, you will also be able to enjoy some Digital Forensics Special Events at The Dupont Circle Hotel – Digital Forensics Campus.

SANS CDI 2012

# Registration Information

*We recommend you register early to ensure you get your first choice of courses.*

**Register online at www.sans.org/cyber-defense-initiative-2012**

SANS
The Most Trusted Source for Information and Software Security Training

## How to Register

**1. To register, go to www.sans.org/cyber-defense-initiative-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/cyber-defense-initiative-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 CDI 2012 Simulcast course, please visit www.sans.org/simulcasts***

## Register Early and Save

| | DATE | DISCOUNT | DATE | DISCOUNT |
|---|---|---|---|---|
| Register & pay by | 10/24/12 | $500.00 | 11/7/12 | $250.00 |

Discount applies to 5- or 6-day courses only.

## 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, November 14, 2012**, by fax or mail-in order to receive a refund.

# SANS Training Options

Training

## Multi-Course Training Events

www.sans.org/security-training/bylocation/index_all.php

Community

## Community SANS

*Live Training in Your Local Region with Smaller Class Sizes*

www.sans.org/community

OnSite

## OnSite

*Live Training at Your Office Location*

www.sans.org/onsite

Mentor

## Mentor

*Live Multi-Week Training with a Mentor*

www.sans.org/mentor

Summit

## Summit Series

*Live IT Security Summits and Training*

www.sans.org/summit

OnDemand

## OnDemand

*All the Course Content at Your Own Pace*

www.sans.org/ondemand

vLive

## vLive

*Virtual Live Training from Your Home or Office*

www.sans.org/virtual-training/vlive

Simulcast

## Simulcast

*Attend Event Training From Your Location*

www.sans.org/virtual-training/event-simulcast
www.sans.org/virtual-training/custom-simulcast

SelfStudy

## SelfStudy

*Independent Study with Books and MP3s*

www.sans.org/selfstudy

# SANS CDI 2012 Registration Fees

**Register online at www.sans.org/cyber-defense-initiative-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 10/24/11 | Paid by 11/7/11 | Paid after 11/7/11 | Add GIAC Cert | Add OnDemand |
|---|---|---|---|---|---|---|
| □ 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 | □ FREE | □ $449 |
| □ FOR408 | Computer Forensic Investigations - Windows In-Depth | $4,095 | $4,345 | $4,595 | □ $549 | |
| □ FOR508 | Advanced Computer Forensic Analysis and Incident Response ***NEW!*** | $4,095 | $4,345 | $4,595 | □ $549 | |
| □ 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 |
| □ 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 |
| □ MGT514 | IT Security Strategic Planning, Policy and Leadership | $3,445 | $3,695 | $3,945 | | |
| □ 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 | |
| □ SEC503 | Intrusion Detection In-Depth | $3,895 | $4,145 | $4,395 | □ $549 | |
| □ SEC504 | Hacker Techniques, Exploits, and Incident Handling | $3,895 | $4,145 | $4,395 | □ $549 | □ $449 |
| □ SEC505 | Securing Windows and Resisting Malware | $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 | | |
| □ 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 | | |
| □ SEC642 | Advanced Web App Penetration Testing and Ethical Hacking ***NEW!*** | $3,895 | $4,145 | $4,395 | | |
| □ HOSTED | (ISC)²® CSSLP® CBK® Education Program | $2,645 | $2,895 | $3,145 | | |

## Skill-Based Short Courses

| | | If taking a 5-6 day course | Paid by 10/24/11 | Paid by 11/7/11 | Paid after 11/7/11 | Add GIAC Cert | Add OnDemand |
|---|---|---|---|---|---|---|---|
| □ MGT305 | Technical Communication and Presentation Skills for Security Professionals | $575 | $995 | $995 | $995 | | □ $129 |
| □ MGT433 | Securing The Human: Building and Deploying an Effective Security Awareness Program | $1,150 | $1,700 | $1,700 | $1,700 | | |
| □ SEC434 | Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting | $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 |
| □ HOSTED | Offensive Countermeasures: Defensive Tactics That Actually Work | $1,150 | $1,700 | $1,700 | $1,700 | | |

## Special Events

| | | | | | |
|---|---|---|---|---|---|
| □ NetWars - Tournament Play | FREE | $999 | $999 | $999 | |

## Individual Courses Available

| | SUN 12/9 | MON 12/10 | TUE 12/11 | WED 12/12 | THU 12/13 | FRI 12/14 |
|---|---|---|---|---|---|---|
| AUD507 | □ 507.1 | □ 507.2 & 507.3 | | □ 507.4 | □ 507.5 | □ 507.6 |
| 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 |
| 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 Day of Courses | $1,350 | □ Five Days of Courses | $3,825 |
| □ Two Days of Courses | $2,075 | □ Six Days of Courses | $4,375 |
| □ Three Days of Courses | $3,025 | □ Seven Days of Courses | $4,975 |
| □ Four Days of Courses | $3,575 | □ Eight Days of Courses | $5,575 |

**REMINDER:**

**When you register, please use the promo code located on the back cover.**