SANS

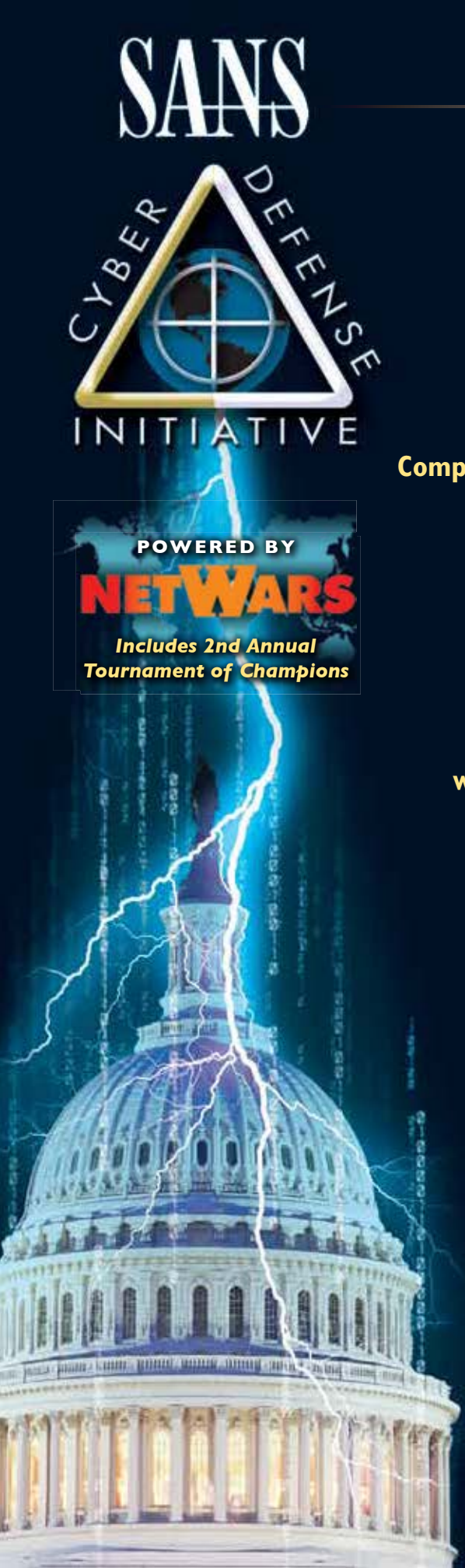
Washington, DC

December 12-19, 2013

CYBER DEFENSE INITIATIVE

POWERED BY NETWARS

Includes 2nd Annual Tournament of Champions



Choose from these popular courses:

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Computer Forensic Investigations – Windows In-Depth

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

SANS Security Leadership Essentials For Managers with Knowledge Compression™

REM: Malware Analysis Tools and Techniques

"This training increases my marketability in the job market. It also adds value to my organization."

-Phillip Baca, Drive Savers Data Recovery

GIAC Approved Training

Register at www.sans.org/event/cyber-defense-initiative-2013

Dear Colleague,

I am pleased to invite you to **SANS Cyber Defense Initiative (CDI) in Washington DC on December 12-19**. We are bringing more than 25 of our most interesting and challenging courses to meet your needs - from beginning practitioners to the most sophisticated professionals in the cyber security community. 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.

At SANS CDI 2013, you'll enjoy an extraordinarily rich training experience; you will meet other information security professionals, discuss new products with vendors, participate in **NetWars Tournament**, and listen to world-class guest speakers.

The course schedule for SANS CDI 2013 features a full lineup of SANS courses. We've also rolled out these new highly focused courses: **SEC505: Securing Windows and Resisting Malware** (GCWN) with Jason Fossen, **FOR526: Windows Memory Forensics In-Depth** with Alissa Torres, **MGT415: A Practical Introduction to Risk Assessment** with James Tarala, **AUD444: Auditing Security and Controls of Active Directory and Windows** with Tanya Baccam, and **AUD445: Auditing Security and Controls of Oracle Databases** with Tanya Baccam.

SANS CDI 2013 is powered by **NetWars Tournament**. We'll be running an exciting NetWars competition over two evenings, available FREE to CDI attendees taking a five- or six-day class, while seats last. This year will include a **DFIR NetWars** as well. And back by popular demand, our **Second Annual Invitational NetWars Tournament of Champions** draws best-of-the-best winners from previous years to the ultimate challenge. Whether you are a first time NetWars participant looking to have fun and build your skills, or a veteran trying to beat your own best score, make sure you sign up for NetWars when you register for a CDI long course!

This year, our campus is the **Washington Hilton**. See our **Hotel & Travel Information** page for details.

I look forward to seeing you in Washington in December.

Kind regards,

Alan Paller

Alan Paller
Director of Research
SANS Institute

Alan Paller

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

"Combination of course information, instructor insights, and networking opportunities is incredibly beneficial."
-Blake Roth,
Guide One Insurance,

"SANS continues to out perform all other training providers. You can train anywhere, but you can excel with SANS."
-John Lindsay,
Dept. of National Defence

"Practical hands-on training. It was awesome having Netwars available with this course."
-Colin Kinsella,
Dept. of Defense

"SANS is the gold standard in information security training – plain and simple."
-Scott Hilts, Bruce Power

SANS IT SECURITY TRAINING AND YOUR CAREER ROADMAP

SECURITY CURRICULUM

Beginners

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

SEC301 Intro to Information Security **GISF**

Penetration Testing

SEC401 Security Essentials Bootcamp Style **GSEC**

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**

SEC561 Hands-on Penetration Testing for the InfoSec Pro NEW

SEC573 Python for Penetration Testers NEW

SEC575 Mobile Device Security and Ethical Hacking **GMOB**

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

SEC642 Advanced Web App Pen Testing and Ethical Hacking NEW

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

SEC760 Advanced Exploit Development NEW

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

Incident Handling

SEC401 Security Essentials Bootcamp Style **GSEC**

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

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

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

Intrusion Analysis

SEC401 Security Essentials Bootcamp Style **GSEC**

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

SEC502 Perimeter Protection In-Depth **GCFW**

SEC503 Intrusion Detection In-Depth **GCIA**

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

System Administration

SEC401 Security Essentials Bootcamp Style **GSEC**

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**

Network Security

SEC401 Security Essentials Bootcamp Style **GSEC**

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

SEC566 Implementing & Auditing the Twenty Critical Security Controls – In-Depth

SEC540 VoIP and Unified Communications Security

AUDIT CURRICULUM

SEC566 Implementing & Auditing the Twenty Critical Security Controls – In-Depth

AUD507 Auditing Networks, Perimeters, and Systems *GSNA*

Specialized Audit Courses

AUD444 Auditing Security and Controls of Active Directory and Windows NEW

AUD445 Auditing Security and Controls of Oracle Databases NEW

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

MANAGEMENT CURRICULUM

SEC301 Intro to Information Security **GISF**

SEC401 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**

Specialization

MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam **GISP**

MGT433 Securing The Human: Building and Deploying an Effective Security Awareness Program

MGT514 IT Security Strategic Planning, Policy and Leadership

Additional Management Courses
www.sans.org/courses/management

DEVELOPER CURRICULUM

Core

STH.DEVELOPER Application Security Awareness Modules
www.securingthehuman.org/developer
CBT

DEV522 Defending Web Applications Security Essentials **GWEB**

Secure Coding

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

DEV544 Secure Coding in .NET (4-Day Course) **GSSP-.NET**

DEV543 Secure Coding in C & C++

Specialization

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

SEC642 Advanced Web App Pen Testing and Ethical Hacking NEW

Additional information on Developer Courses
http://software-security.sans.org

FORENSICS CURRICULUM

Core

FOR408 Computer Forensic Investigations – Windows In-Depth **GCFE**

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

Advanced and In-Depth

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

FOR572 Advanced Network Forensics and Investigations NEW

FOR610 Reverse Engineering Malware: Malware Analysis Tools & Techniques **GREM**

Specialization

FOR526 Windows Memory Forensics In-Depth NEW

FOR585 Advanced Smartphone and Mobile Device Forensics NEW

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

LEGAL CURRICULUM

SEC401 Security Essentials Bootcamp Style **GSEC**

LEG523 Law of Data Security and Investigations **GLEG**

GIAC certification available for courses indicated with GIAC acronyms

COURSES-AT-A-GLANCE

Please check the website for an up-to-date course list at www.sans.org/cyber-defense-initiative-2013		THU 12/12	FRI 12/13	SAT 12/14	SUN 12/15	MON 12/16	TUE 12/17	WED 12/18	THU 12/19
SEC301	Intro to Information Security SIMULCAST	PAGE 2							
SEC401	Security Essentials Bootcamp Style SIMULCAST	PAGE 4							
SEC434	Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting							P 42	
SEC501	Advanced Security Essentials – Enterprise Defender	PAGE 6							
SEC503	Intrusion Detection In-Depth	PAGE 8							
SEC504	Hacker Techniques, Exploits, and Incident Handling	PAGE 10							
SEC505	Securing Windows and Resisting Malware NEW!	PAGE 12							
SEC542	Web App Penetration Testing and Ethical Hacking	PAGE 14							
SEC566	Implementing and Auditing the Twenty Critical Security Controls – In-Depth	PAGE 16							
SEC575	Mobile Device Security and Ethical Hacking	PAGE 18							
SEC579	Virtualization and Private Cloud Security	PAGE 20							
SEC580	Metasploit Kung Fu for Enterprise Pen Testing							P 42	
SEC617	Wireless Ethical Hacking, Penetration Testing, & Defenses	PAGE 22							
FOR408	Computer Forensic Investigations – Windows In-Depth SIMULCAST	PAGE 24							
FOR508	Advanced Computer Forensic Analysis and Incident Response SIMULCAST	PAGE 26							
FOR526	Windows Memory Forensics In-Depth NEW!	PAGE 28							
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques SIMULCAST	PAGE 30							
MGT305	Technical Communication and Presentation Skills for Security Professionals							P 43	
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam SIMULCAST	PAGE 32							
MGT415	A Practical Introduction to Risk Assessment NEW!							P 43	
MGT433	Securing The Human: Building and Deploying an Effective Security Awareness Program							P 43	
MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	PAGE 34							
MGT514	IT Security Strategic Planning, Policy and Leadership	PAGE 36							
MGT535	Incident Response Team Management							P 44	
AUD444	Auditing Security and Controls of Active Directory and Windows NEW!	PAGE 40							
AUD445	Auditing Security and Controls of Oracle Databases NEW!				PAGE 40				
AUD507	Auditing Networks, Perimeters, and Systems	PAGE 38							
HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program	PAGE 41							
HOSTED	(ISC)²® Systems Security Certified Practitioner – SSCP® Review							P 44	
	NetWars – Tournament of Champions				P 46				

CONTENTS

SECURITY 301

Intro to Information Security

Course updated to include hands-on labs!

SANS

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 5:00pm
Laptop Required
30 CPE/CMU Credits
Instructor: Fred Kerby
- GIAC Cert: GISF

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management. Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

Who Should Attend

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

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

This course will help you develop the skills to bridge the gap that often exists between managers and system administrators, and learn to communicate effectively with personnel in all departments and at all levels within your organization.

"If you are just starting out in information security, this course has all the basics needed to get you started."
-Sherrie Aud, Deltha Corporation

"The information is immediately usable in the organization. Moreover, Mr. Kerby makes the presentation interesting and real-world, as well as practical and beneficial."
-Robert Smith, CMS

"Great crash-course and immersion for security and technology! From the logistics to the IS and OS, the necessary pieces of the cyber security puzzle have come together."
-Ansley LaBarre, EWA/IIT

Fred Kerby *SANS Senior Instructor*

Fred is an engineer, manager, and security practitioner whose experience spans several generations of networking. He was the Information Assurance Manager at the Naval Surface Warfare Center, Dahlgren Division for more than 16 years and has vast experience with the political side of security incident handling. His team is one of the recipients of the SANS Security Technology Leadership Award as well as the Government Technology Leadership Award. Fred received the Navy Meritorious Civilian Service Award in recognition of his technical and management leadership in computer and network security.

301.1 HANDS ON: A Framework for Information Security

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

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

301.2 HANDS ON: Securing the Infrastructure

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

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

301.3 HANDS ON: Cryptography and Security in the Enterprise

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

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

301.4 HANDS ON: Information Security Policy

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

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

301.5 Defense In-Depth: Lessons Learned

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

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

You Will Be Able To

- Discuss and understand risk as a product of vulnerability, threat, and impact to an organization
- Understand and apply basic principles of information assurance (e.g., least privilege, separation of risk, defense in depth, etc.)
- Explain the fundamentals of networking (link layer communications, addressing, basic routing, masquerading)
- Describe the predominant forms of malware and the various delivery mechanisms that can place organizations at risk
- Understand the capabilities and limitations of cryptography
- Evaluate policy and recommend improvements
- Identify and implement meaningful security metrics
- Identify and understand the basic attack vectors used by intruders

www.giac.org

SANS SIMULCAST

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

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPE/CMU Credits
Instructor: Seth Misenar

- GIAC Cert: GSEC
- Cyber Guardian
- Masters Program
- DoDD 8570

"I'm a newbie to security. This course presented a ton of information on this subject in a fast-paced, easy-to-understand manner."
-Michael Horkan, Rockwell Automation

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**
- **Operations personnel who do not have security as their primary job function but need an understanding of security to be effective**
- **IT engineers and supervisors who need to know how to build a defensible network against attacks**
- **Administrators responsible for building and maintaining systems that are being targeted by attackers**
- **Forensic, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs**
- **Anyone new to information security with some background in information systems and networking**

It seems wherever you turn organizations are being broken into, and the fundamental question that everyone wants answered is: Why? Why is it that some organizations get broken into and others do not? Organizations are spending millions of dollars on security and are still compromised. The problem is they are doing good things but not the right things. Good things will lay a solid foundation, but the right things will stop your organization from being headline news in the Wall Street Journal. SEC401's focus is to teach individuals the essential skills, methods, tricks, tools and techniques needed to protect and secure an organization's critical information assets and business systems. This course teaches you the right things that need to be done to keep an organization secure. The focus is not on theory but practical hands-on tools and methods that can be directly applied when a student goes back to work in order to prevent all levels of attacks, including the APT (advanced persistent threat). In addition to hands-on skills, we will teach you how to put all of the pieces together to build a security roadmap that can scale today and into the future. When you leave our training we promise that you will have the techniques that you can implement today and tomorrow to keep your organization at the cutting edge of cyber security. Most importantly, your organization will be secure because students will have the skill sets to use the tools to implement effective security.

With the APT, organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in cyber security. What has worked and will always work is taking a risk-based approach to cyber defense. Before your organization spends a dollar of its IT budget or allocates any resources or time to anything in the name of cyber security, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared 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 cutting-edge 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.

SANS SIMULCAST

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

401.1 HANDS ON: Networking Concepts

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

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

401.2 HANDS ON: Defense In-Depth

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

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

401.3 HANDS ON: Internet Security Technologies

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

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

401.4 HANDS ON: Secure Communications

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

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

401.5 HANDS ON: Windows Security

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

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

401.6 HANDS ON: Linux Security

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

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

Seth Misenar *SANS Certified Instructor*

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

www.giac.org

www.sans.org/cyber-guardian

www.sans.edu

DoDD 8570 Required
www.sans.org/8570

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Dr. Eric Cole

- GIAC Cert: GCED
- Masters Program

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

Cybersecurity 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. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

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 become 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 its 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. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

"Great course. Best training I have attended. This is my first SANS course and I can't wait to attend more."
-Leonard Crull, MI ANG

"Great course! I'm disturbed/impressed at how much the instructors know. Top-notch instructors are what makes SANS!"
-Chris Robinson, Sempra Energy

"Very knowledgeable. Top-tier training and industry leading."
-Herbert Monford, Regions Bank

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. He 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, where 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.

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)

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Learn the tools that can be used to analyze a network to both prevent and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary companies works and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Understand the six steps in the incident handling process and be able to create and run an incident handling capability
- Learn how to use various tools to identify and remediate malware across your organization
- Create a data classification program and be able to deploy data loss prevention solutions at both a host and network level

www.giac.org

www.sans.edu

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Mike Poor

- GIAC Cert: GCIA
- Cyber Guardian
- Masters Program
- DoDD 8570

"This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis."
-Thomas Kelly, DIA

"This course is valuable for anyone interested in IDS. Mike's knowledge and willingness to help you understand the material are unlike any other training I've been to. Great course and instructor."
-Dannie Arnold, U.S. Army

"Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts."
-Hector Araiza, USAF

Who Should Attend

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

If you have an inkling of awareness of security (even my elderly aunt knows about the perils of the Interweb!), you often hear the disconcerting news about another high-profile company getting compromised. The security landscape is continually changing from what was once only perimeter protection to a current exposure of always-connected and often-vulnerable. Along with this is a great demand for security savvy employees who can help to detect and prevent intrusions. That is our goal in the Intrusion Detection In-Depth course - to acquaint you with the core knowledge, tools, and techniques to prepare you to defend your networks.

This course spans a wide variety of topics from foundational material such as TCP/IP to detecting an intrusion, building in breadth and depth along the way. It's kind of like the "soup to nuts" or bits to bytes to packets to flow of traffic analysis.

Hands-on exercises supplement the course book material, allowing you to transfer the knowledge in your head to your keyboard using the Packetrix VMware distribution created by industry practitioner and SANS instructor Mike Poor. As the Packetrix name implies, the distribution contains many of the tricks-of-the-trade to perform packet and traffic analysis. All exercises have two different approaches. A more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a student who may already know the material or who has quickly mastered new material a more challenging experience. Additionally, there is an "extra credit" stumper question for each exercise intended to challenge the most advanced student.

By week's end, your head should be overflowing with newly gained knowledge and skills; and your luggage should be swollen with course book material that didn't quite get absorbed into your brain during this intense week of learning. This course will enable you to "hit the ground running" once returning to a live environment.

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 its 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.

503.1 HANDS ON: Fundamentals of Traffic Analysis: PART I

Day 1 provides a refresher or introduction, depending on your background, to TCP/IP covering the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, an introduction to Wireshark, the IP layer, both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network access/link layer; IP Layer

503.2 HANDS ON: Fundamentals of Traffic Analysis: PART II

Day 2 continues where Day1 ended in understanding TCP/IP. Two essential tools – Wireshark and tcpdump – are explored to give you the skills to analyze your own traffic. The focus of these tools on Day 2 is filtering traffic of interest in Wireshark using display filters and in tcpdump using Berkeley Packet Filters. We proceed with our exploration of the TCP/IP layers covering TCP, UDP, and ICMP. Once again, we describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Wireshark display filters; TCP; UDP; ICMP

503.3 HANDS ON: Application Protocols and Traffic Analysis

Day 3 culminates the examination of TCP/IP with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols – HTTP, SMTP, DNS, and Microsoft communications. Our focus is on traffic analysis, a key skill in intrusion detection.

Topics: Advanced Wireshark; Detection methods for application protocols; Microsoft Protocols; HTTP; SMTP; DNS; Packet crafting and nmap OS identification; IDS/IPS evasion theory; Real-world traffic analysis

503.4 HANDS ON: Intrusion Detection Snort Style

The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days - Intrusion Detection: Snort Style. Snort is a widely deployed open source IDS/IPS that has been a standard in the industry for over a decade. Knowing how to configure, tune and use it are indispensable skills.

Topics: Introduction; Modes of operation; Writing Snort rules; Configuring Snort as an IDS; Miscellaneous; Snort GUIs and analysis

503.5 HANDS ON: Network Traffic Forensics and Monitoring

On the penultimate day, you'll become familiar with other tools in the "analyst toolkit" to enhance your analysis skills and give you alternative perspectives of traffic. The open source network flow tool SiLK is introduced. It offers the capability to summarize network flows to assist in anomaly detection and retrospective analysis, especially at sites where the volume is so prohibitively large that full packet captures cannot be retained for very long, if at all.

Topics: Analyst toolkit; SiLK; Network Forensics; Network architecture for monitoring; Correlation of indicators

503.6 HANDS ON: IDS Challenge

The week culminates with a fun hands-on Challenge where you find and analyze traffic to a vulnerable honeynet host using many of the same tools you mastered during the week. Students can work alone or in groups with or without workbook guidance. This is a great way to end the week since it reinforces what you've learned by challenging you to think analytically, gives you a sense of accomplishment, and strengthens your confidence to employ what you've learned in the Intrusion Detection In-Depth course in a real-world environment.

You Will Be Able To

- Identify the security solutions that are most important for protecting your perimeter
- Understand attacks that affect security for the network
- Understand the complexities of IP and how to identify malicious packets
- Understand the risks and impacts related to Cloud Computing and security solutions to manage the risks
- Understand the process for properly securing your perimeter
- Identify and understand how to protect against application and database risks
- Use tools to evaluate the packets on your network and identify legitimate and illegitimate traffic

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu


DoDD 8570 Required
www.sans.org/8570

SECURITY 504

Hacker Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPE/CMU Credits
Laptop Required
Instructor: John Strand

- GIAC Cert: GCIH
- Cyber Guardian
- Masters Program
- DoDD 8570

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 and 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.

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

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

"This class teaches you all of the hacking techniques that you need as an incident handler."
-Demonique Lewis, TerpSys

John Strand *SANS Senior Instructor*

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

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: Computer and Network Hacker Exploits – PART 1

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: Computer and Network Hacker Exploits – PART 2

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: Computer and Network Hacker Exploits – PART 3

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: Computer and Network Hacker Exploits – PART 4

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

"John's experiences and teaching method reinforce concepts learned in this course. Also, on many occasions, John offered advice to students that can be directly applied to their own organization."

-James Browning, Dept. of Justice

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu

DoDD 8570 Required
www.sans.org/8570

SECURITY 505

Securing Windows and Resisting Malware

NEW

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Cyber Guardian
- Masters Program

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-R2, Server 2008-R2, and Windows 8.1, and Windows 7.

This course is about the most important things to do to secure Windows and how to minimize the impact of these changes on users of these changes. You'll see the instructor demo the important steps live, and you can follow along on your laptop. 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.

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

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

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, we'll start with the basics.

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.

"If you think you know Windows, take this Windows security class – your review of your own skills and understanding will be challenged, for the better!!"
-Matthew Stoeckle,
Nebraska Public Power District

"All Windows administrators responsible for securing IIS should attend this course."
-Billy Taylor,
Naval Sea Logistics Center

"You will know and be confident how to enable Windows PKI after taking this course. I had no practical experience, but plenty of theory. Jason broke down the pros and cons of the whole process. Excellent!!"
-Othello Swanston, DTRA-DOD

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

This course is about strategies for resisting malware infection. Malware is used by hackers and thieves in Advanced Persistent Threat (APT) scenarios to maintain stealthy remote control of your networks. By hardening the Windows operating system and the applications typically exploited by attackers, we hope to block the initial compromise which grants our adversaries a foothold inside the LAN. The trick, of course, is to do it in a cost-effective and scalable way with the least impact on users.

Topics: Security Templates; Group Policy; Hardening Internet Explorer, Adobe Reader, Java, Google Chrome and MS Office; Going Beyond AV Scanning; Application Whitelisting

505.2 HANDS ON: High-Value Targets and Restricting Admin Compromise

Hackers and malware often rely upon excessive administrative powers in the hands of users and even our own IT personnel. With pass-the-hash and token abuse attacks, a network can quickly be brought to its knees. We will see how to manage these powers and delegate authority safely. Active Directory permissions and auditing can also be used for delegating power to non-IT personnel, but how to do it? Finally, patch management is critically important for securing Windows environments, but it can be expensive when done correctly, so we will see how to make it easier without sacrificing security.

Topics: What Makes a High-Value Target ; Forms of Power in the Windows Kernel and its Group Policy Management; Mitigating Pass-the-Hash and Token Abuse Attacks; Role-Based Delegation of Authority with Active Directory Permissions and Auditing; Effective Patch Management

505.3 HANDS ON: Windows PKI, BitLocker, and Secure Boot

Windows provides a comprehensive Public Key Infrastructure (PKI) for managing certificates and making their use as transparent to users as possible. Windows PKI uses Active Directory to store certificates, Group Policy for hands-free deployment, and a special PKI database for private key archival and recovery. Everything you need for a full PKI, such as for smart cards, SSL/TLS, wireless WPA and VPNs, is built into Windows for free. BitLocker provides sector-level whole drive encryption and, with an optional TPM chip, can verify boot-up integrity too. BitLocker key recovery can be managed through Group Policy, which is important for preventing data loss and allowing forensics analysis. Secure Boot protects against bootkits on UEFI systems.

Topics: PKI Benefits; PKI Installation and Management; Installing Certificates Through Group Policy; Certificate Revocation; How To Issue Smart Cards; Managing BitLocker; BitLocker Key Recovery; UEFI Secure Boot

505.4 HANDS ON: IPSec, Windows Firewall, DNS, and Wireless

IPSec is not just for VPNs. IPSec provides authentication and encryption of packets in a way that is transparent to users and applications. IPSec is tightly integrated into the Windows Firewall, and this host-based firewall can be managed through Group Policy, NETSH.EXE or PowerShell. DNSSEC and DNS sinkholing can secure name resolution traffic. In the afternoon, we will then see how to use RADIUS for securing access to WPA 802.11 wireless networks using PEAP and digital certificates from your PKI. Wireless security best practices will also be covered, including wireless tethering issues.

Topics: IPSec beyond VPNs; DNSSEC; DNS Sinkholes; Group Policy Management of Windows Firewall; Windows RADIUS Service; 802.1X and WPA2; Wireless Best Practices

505.5 HANDS ON: Server Hardening and Dynamic Access Control

After attending this course you will know how to shrink the attack surface of Windows Server against determined attackers. The techniques discussed will apply to most types of servers, especially those using RDP, SMB, SSL and NTLM. Dynamic Access Control (DAC) is designed for managing and auditing the access to millions of files across many file servers. Claims associated with users and computers can be combined with traditional group memberships to define who has access to what. Files can be classified according to your own custom rules. DAC can be part of your Data Loss Prevention (DLP) infrastructure.

Topics: Server Hardening; Insecure Protocols like SSL and RDP; SMBv3 Encryption; File Classification Infrastructure; User and Device Claims; Kerberos Armoring; Conditional Expressions; Central Access Policy for Auditing

505.6 HANDS ON: Windows PowerShell Scripting

Everything is all PowerShell now. PowerShell is Microsoft's command shell and scripting language. PowerShell is available as a free download and is built into Server 2008, Windows 7 and later by default. How to stand out from the crowd? Learn PowerShell! Don't worry, we will walk through all the essentials of PowerShell together, the course presumes nothing, you don't have to have any prior scripting experience. And, most importantly, be prepared to have fun!

Topics: Running PowerShell Cmdlets and Scripts; Writing Your Own Functions and Scripts; Flow Control in Scripts; .NET Object Piping; Windows Management Instrumentation (WMI); Managing Events Logs and Active Directory; Walking Through Lots of Example Scripts Together

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu

SECURITY 542

Web App Penetration Testing and Ethical Hacking

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Kevin Johnson

- GIAC Cert: GWAPT
- Cyber Guardian
- Masters Program

"SEC542 is a step-by-step introduction to testing and penetrating web applications, a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, ii2P LLC

"Without a doubt, this was the best class for my career."
-Don Brown, Lockheed Martin

"Fun while you learn! Just don't tell your manager. Every class gives you invaluable information from real world testing you cannot find in a book."
-David Fava, The Boeing Company

Assess Your Web Apps in Depth

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

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

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

Who Should Attend

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

Kevin Johnson *SANS Senior Instructor*

Kevin Johnson is a Senior Security Consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture, and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises, and penetration testing everything from government agencies to Fortune 100 companies. Kevin is an instructor and author for the SANS Institute and a contributing blogger at TheMobilityHub. Kevin has performed a large number of trainings, briefings, and presentations for both public events and internal trainings. Kevin teaches for the SANS Institute on a number of subjects. He is the author of three classes- SEC542: Web Application Penetration Testing and Ethical Hacking, SEC642: Advanced Web Application Penetration Testing, and SEC571: Mobile Device Security. Kevin has presented at a large number of conventions, meetings, and industry events. Some examples of these are: DerbyCon, ShmooCon, DEFCON, Blackhat, ISACA, Infragard, and ISSA. In addition, Kevin is very involved in the open source community and runs a number of open source projects. These include SamuraiWTF, a web pen-testing environment; Laudanum, a collection of injectable web payloads; Yokoso!, an infrastructure fingerprinting project; and a number of others. Kevin is also involved in MobiSec and SH5ARK. Kevin was the founder and lead of the BASE project for Snort before transitioning that to another developer.

542.1 HANDS ON: The Attacker's View of the Web

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

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

542.2 HANDS ON: Reconnaissance and Mapping

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

Topics: Discover the Infrastructure Within the Application; Identify the Machines and Operating Systems; SSL Configurations and Weaknesses; Explore Virtual Hosting and its Impact on Testing; Learn Methods to Identify Load Balancers; Software Configuration Discovery; Explore External Information Sources; Google Hacking; Learn Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Application Flow Charting; Relationship Analysis Within an Application; JavaScript for the Attacker

542.3 HANDS ON: Server-Side Discovery

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

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

542.4 HANDS ON: Client-Side Discovery

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

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

542.5 HANDS ON: Exploitation

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

Topics: Explore Methods to Zombify Browsers; Discuss Using Zombies to Port Scan or Attack Internal Networks; Explore Attack Frameworks; Walk Through an Entire Attack Scenario; Exploit the Various Vulnerabilities Discovered; Leverage the Attacks to Gain Access to the System; Learn How to Pivot our Attacks Through a Web Application; Understand Methods of Interacting with a Server Through SQL Injection; Exploit Applications to Steal Cookies; Execute Commands Through Web Application Vulnerabilities

542.6 HANDS ON: Capture the Flag

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

Topics: Capture the Flag

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu

SECURITY 566

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

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: James Tarala

"This class is extremely valuable for any organization wanting to know where they stand on security."
-David Obrien, Costco

"James does an outstanding job of providing an overview of each control as well as offering his perspective and experience which adds a lot of value."
-Danny Tomlinson, Kapstone Paper

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. Specifically, by the end of the course students will know how to:

- Create a strategy to successfully defend their data
- Implement controls to prevent data from being compromised
- Audit systems to ensure compliance with Critical Control standards.

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

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

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

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

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

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)

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of network and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how critical controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the critical security controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

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 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.

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Christopher Crowley
▸ GIAC Cert: GMOB

"Wow! This course is everything you need to know about mobile device deployment, risks and more. Don't deploy your mobile devices without taking this course first."
-Bryan Simon, INTEGRIS Credit Union

"With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations."
-Dean Altman, Discount Tire

Now with enhanced coverage of BlackBerry 10, Apple iOS, and Android devices

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 by 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 enterprise resource planning 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.

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

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.

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 from 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.

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

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 device and infrastructure systems to defend these threats. In this part of the course, we'll examine the design and deployment of network and system infrastructure to support a mobile phone deployment including the selection and deployment of Mobile Device Management (MDM) systems.

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 event. In this day-long, in-depth final hands-on 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 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.

GMOB

www.giac.org

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2013/courses

SECURITY 579

Virtualization and Private Cloud Security

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Paul A. Henry

"AWESOME class thus far. I will be able to take a lot back to apply to our Hyper-V environment!!!"
-Craig VanHuss, Crutchfield Corp.

"Class continues to be spot-on. I'm really enjoying class and taking a lot from it as it's forcing me to think about architectural items we hadn't considered as an organization."
-Glenn Galang,
Lake Villa District Library

"This is an essential course for anyone considering or developing a virtualized environment."
-Barry Wudel, Fluor Corp.

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

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

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

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

You Will Be Able To

- Lock down and maintain a secure configuration for all components of a virtualization environment
- Design a secure virtual network architecture
- Evaluate virtual firewalls, intrusion detection and prevention systems, and other security infrastructure
- Evaluate security for private cloud environments
- Perform vulnerability assessments and pen tests in virtual and private cloud environments, and acquire forensic evidence
- Perform audits and risk assessments within a virtual or private cloud environment

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 principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and 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. Paul is frequently cited by major and trade print publications 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. In addition, 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*, where he is a consistent contributor. Paul serves as a featured and 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: Virtualization Offense and Defense – PART 1

In this session, we'll delve into the offensive side of security specific to virtualization and cloud technologies. While many key elements of vulnerability management and penetration testing are similar to 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: Virtualization Offense and Defense – PART 2

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

579.5 HANDS ON: Virtualization and Cloud Integration: Policy, Operations, and Compliance

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

579.6 HANDS ON: Confidentiality, Integrity, and Availability with Virtualization and Cloud

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

"Excellent combination of theory and hands-on really exposes you to security advantages and disadvantages of virtual environment."
-Scott Boaman, Naval Reactors

SECURITY 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Larry Pesce

- GIAC Cert: GAWN
- Cyber Guardian
- Masters Program

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

Who Should Attend

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

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

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

"The labs were great and provided a good means to practice the material. An excellent course for all levels of professionals who are dealing with wireless in the organization. Not knowing this information is like having your head in the sand. Easy to follow, but difficult to master...the instructor has stretched me and my skills this week and I am better for it!"
-John Fruge, B&W Technical Services

"This class will not only give you a basic understanding of wireless threats and vulnerabilities, but it can be as advanced as you want to make it with the questions that you ask."
-Daniel Mayernik,
Integrity Applications Incorporated

Larry Pesce *SANS Certified Instructor*

Larry is a senior security analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second leatherman. Larry also co-authored "Linksys WRT54G Ultimate Hacking" and "Using Wireshark and Ethereal" from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge.

617.1 HANDS ON: Wireless Data Collection & WiFi MAC Analysis

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

Topics: Understanding the Wireless Threat; Wireless LAN Organizations and Standards; Using the SANS Wireless Auditing Toolkit; Sniffing Wireless Networks: Tools, Techniques and Implementation; IEEE 802.11 MAC: In-Depth

617.2 HANDS ON: Wireless Tools and Information Analysis

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

Topics: Wireless LAN Assessment Techniques

617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

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

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

617.4 HANDS ON: Advanced WiFi Attack Techniques

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

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

617.5 HANDS ON: Bluetooth, DECT and ZigBee Attacks

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

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

617.6 HANDS ON: Wireless Security Strategies and Implementation

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

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

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Chad Tilbury

- GIAC Cert: GCFE
- Masters Program

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 threats, 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 an calling cybercrime law enforcement agents to piece together what happened in these cases.

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

FOR408: Computer Forensic Investigations – Windows In-Depth focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

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 8 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. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!"
-Jason Jones, USAF

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."
-Alexander Applegate, Auburn Univ.

"Definitely my most favorite SANS course I have attended! Very valuable skills to correlate or validate findings."
-Terrie Myerchin, DIRECTV, Inc.

"With Chad's background and his excellent teaching skills I would recommend FOR408."
-Brett Smetanka, KeyBank

SANS SIMULCAST

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

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 ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics.

408.1 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 while 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 E-mail 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: Windows 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

What You Will Receive With This Course

- Windows version of the SIFT Workstation Virtual Machine
- Windows 8 Standard Full Version License and Key for the Windows SIFT Workstation
- Full License to AccessData FTK and Guidance Software EnCase for a 3 month trial
- Full License to MagnetForensics Internet Evidence Finder for a 15 day trial
- Two full real-world cases to examine during class
- Course DVD loaded with case examples, tools, and documentation
- Wiebetech Ultradock v5 Write Blocker Kit

www.giac.org www.sans.edu

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

FORENSICS 508

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Rob Lee

- GIAC Cert: GCFA
- Cyber Guardian
- Masters Program
- DoDD 8570

"Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience."
-John Alexander, US Army

"Totally awesome, relevant and eye opening. I want to learn more every day."
-Matthew Britton,
Blue Cross Blue Shield of Louisiana

SANS SIMULCAST

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

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508: Advanced Computer Forensic Analysis and Incident Response will help you determine:

- How did the breach occur?
- What systems were compromised?
- What did they take? What did they change?
- How do we remediate the incident?

The updated FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

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 crime investigations and an incident response team. 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.

508.1 HANDS ON: Enterprise Incident Response

Incident responders should be armed with the latest tools, memory analysis techniques, and enterprise scanning methodologies in order to identify, track and contain advanced adversaries, and remediate incidents. Incident response and forensic analysts responding must be able to scale their examinations from the traditional one analyst per system toward one analyst per 1,000 or more systems. Enterprise scanning techniques are now a requirement to track targeted attacks by an APT group or crime syndicate groups which propagate through thousands of systems.

Topics: SIFT Workstation Overview; Incident Response Methodology; Threat and Adversary Intelligence; Intrusion Digital Forensics Methodology; Remote and Enterprise IR System Analysis; Windows Live Incident Response

508.2 HANDS ON: Memory Forensics

Critical to many IR teams detecting advanced threats in the organization, memory forensics has come a long way in just a few years. It can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. While traditionally solely the domain of Windows internals experts, recent tools now make memory analysis feasible for anyone. Better interfaces, documentation, and built-in detection heuristics have greatly leveled the playing field. This section will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills to your incident response and forensics armory.

Topics: Memory Acquisition and Analysis; Memory Analysis Techniques with Redline; Live Memory Forensics; Advanced Memory Analysis with Volatility

508.3 HANDS ON: Timeline Analysis

Timeline Analysis will change the way you approach digital forensics and incident response... forever. Learn advanced analysis techniques uncovered via timeline analysis directly from the developers who pioneered timeline analysis tradecraft. Temporal data is located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and, Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time based artifacts. Analysis that once took days now takes minutes. This section will step you through the two primary methods of creating and analyzing timelines created during advanced incidents and forensic 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: Deep Dive Forensics and Anti-Forensics Detection

A major criticism of digital forensic professionals is 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; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; FAT/exFAT Filesystem Overview

508.5 HANDS ON: Intrusion Forensics – The Art of Finding Unknown Malware

The adversaries are good, we must be better. Over the years, we have observed that many incident responders have a challenging time finding malware without effective indicators of compromise (IOCs) or threat intelligence gathered prior to a breach. This is especially true in APT group intrusions. This advanced session will demonstrate techniques used by first responders to discover malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

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

508.6 HANDS ON: The Incident Response & Intrusion Forensic Challenge

This brand new exercise brings together some of the most exciting techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary such as an APT. This challenge brings it all together using a simulated intrusion into a real enterprise environment consisting of multiple Windows systems. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic scenarios, which were put together by a cadre of individuals with many years of experience fighting advanced threats such as an APT group.

www.giac.org

www.sans.org/
cyber-guardian

www.sans.edu


DoDD 8570 Required
www.sans.org/8570


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

FORENSICS 526

Windows Memory Forensics In-Depth

NEW

SANS

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required
Instructor: Alissa Torres

"Totally awesome, relevant and eye opening. I want to learn more every day."
-Matthew Britton, Blue Cross Blue Shield of Louisiana

"The presentation, exercises, labs, and data provided are the best in the computer forensics industry."
-Rebecca Passmore, FBI

"This is the best SANS course I have taken so far with the best instructor. I hope to take more classes in the future."
-Jonathan Hinson, Duke Energy

FOR526: Memory Analysis In-Depth is a critical course for any serious investigator who wishes to tackle advanced forensic and incident response cases. Memory analysis is now a crucial skill for any investigator who is analyzing intrusions.

Malware can hide, but it must run – the malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis. Learn how memory analysis works by learning about memory structures and context, memory analysis methods, and the current tools used to parse system ram.

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide in plain sight avoiding detection by standard host-based security measures. Every action that adversaries make will leave a trace; you merely need to know where to look. Memory analysis will give you the edge that you need in order to discover advanced adversaries in your network.

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- Anybody who plays a part in the acquisition, preservation,forensics, or analysis of Microsoft Windows computers

FOR526: Memory Analysis In-Depth is one of the most advanced courses in the SANS Digital Forensics and Incident Response Curriculum. This cutting-edge course covers everything you need to step through memory analysis like a pro.

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

Alissa Torres *SANS Certified Instructor*

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

526.1 HANDS ON: Unstructured Memory

Memory forensics is the study of operating systems, and operating systems, in turn, work extensively with the processor and its architecture. Before we can begin a meaningful analysis of the operating system, we must therefore understand how the underlying components work and fit together. This section explains a number of technologies that are used in modern computers and how they have evolved to where they are today. Computer memory is a fantastic resource for the forensic investigator even without considering any operating system structures. There are data in memory that are simply not found anywhere else. Without even knowing which operating system was being used, an examiner can glean information that could be critical to a case. These data are generated by the underlying architecture or standards outside of the operating system. In particular, we focus on encryption keys and network packets. These two resources are not part of traditional forensics, but can provide invaluable data to the memory forensics investigator! While conducting brute force searches for these structures, we are also starting to gather data for examining the operating system later on. Unlike disk forensics, there is no volume header to parse in memory. Instead, we must find values created by the operating system by searching for them manually. There are a number of structures that we can search for which will help us determine what operating system was being used, and the values particular to this execution.

Topics: Computer Architectures; Virtual Memory Models; Implementing the Virtual Memory Model; Process Memory; System Memory; BIOS Keyboard Buffer; Encryption Keys; Network Packets; Traditional Data; Preparing for Structured Analysis; The SIFT Workstation; Pool Memory; Walking vs. Scanning

526.2 HANDS ON: User Visible Structures

Most users are familiar with processes on a Windows system, but not necessarily with how they work under the hood. In this section, we will talk about the operating system components that make up a process, how they fit together, and how they can be exploited by malicious software. We will start with the basics of each process, how it was started, where the executable lives, and what command line options were used. Next will be the Dynamic Link Libraries (DLLs) used by a program and how they are found and loaded by the operating system. Finally, we will talk about the operating system structures involved with threads, the actual blocks of executing code that make up the interactive portion of every process.

Topics: Processes; Dynamic-link Libraries (DLLs); Drivers; Sockets; Kernel Objects; Threads

526.3 HANDS ON: Operating System Internals

There are a tremendous number of structures used in Microsoft Windows. To understand what the operating system is doing, we have to understand these components. In this section we will begin to explore the complex web of interconnected data structures which make up the operating system. To that end we start with a basic introduction to C structures and how they are put together. From there we talk about which of them are used in Windows and the documentation Microsoft publishes about them. In this section we will explore, in-depth, all of the components which constitute Microsoft Windows operating systems. We will start with processes and all of the data they contain. From there we will discuss DLLs, drivers, sockets, kernel objects, threads, modules, and virtual address descriptors. For each of these areas we will talk about how these systems work, what data the operating system maintains, which of those are relevant for forensics, and how to determine if there is something suspicious occurring.

Topics: Introduction to C Structures; Microsoft Structures; Tools for Structures; Modules; Injected and Unpacked Code; Finding hidden DLLs; Finding Hidden Processes; Driver Hooking

526.4 HANDS ON: Memory Forensics in the Real World

Knowing the basics of memory forensics allows us to begin doing it in the real world. First, we must acquire memory images. On any given system there may already be memory images, from the machine's past, which contain highly valuable information. In this section we will discuss how to find and recover such memory images. We'll also cover some of the tools to capture memory images and how to choose the one which is best for you.

Topics: The Windows Registry; Hibernation Files; Crash Dump Files; Memory Imaging; Traditional Imaging Programs; Suspended Virtual Machine; USB; Firewire; Cold Boot Method

526.5 HANDS ON: Memory Challenges

This section will present a number of challenges for the memory forensic examiner. We do not want to spoil all of the surprises by listing them in the outline, but we can give you a sense of what you will be working on. These memory images may contain some kind of malicious software or data of interest. Each challenge will provide a little information to go on. (As with real-world examinations, of course, it's never enough information!) Your job will be to determine if there is anything of interest, and if so, what it is.

"Labs were extremely well done and easy to follow. By far the best of any SANS class I have taken."

-Jonathan Hinson, Duke Energy

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

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Lenny Zeltser

- GIAC Cert: GREM
- Masters Program

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!

Who Should Attend

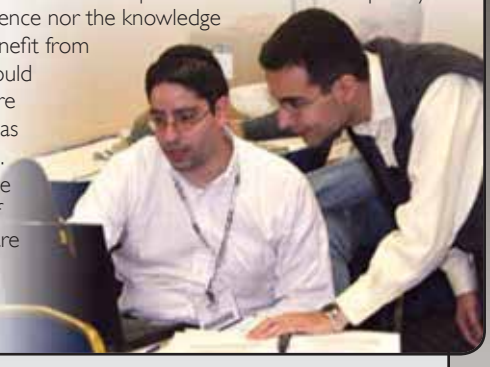
- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise

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.

The course begins by covering fundamental aspects of malware analysis. The course continues by discussing essential x86 assembly language concepts. Towards the end of the course, you'll learn to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents.

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

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 to navigate through malicious executables using a debugger and a disassembler.



"Lenny Zeltser is an outstanding instructor who cares about his students. His expertise combined with his teaching skills makes for an outstanding class."
-Ryan Kelley, Diebold, Inc.

"This class gave me essential tools that I can immediately apply to protect my organization."
-Don Lopez, Valley National Bank

SANS SIMULCAST

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

Lenny Zeltser *SANS Senior Instructor*

Lenny Zeltser is a seasoned business leader with extensive experience in information technology and security. As a product management director at NCR Corporation, he focuses on safeguarding IT infrastructure of small and midsize businesses world-wide. Before NCR, Lenny led the enterprise security consulting practice at a major IT hosting provider. In addition, Lenny is a Board of Directors member at SANS Technology Institute and a volunteer incident handler at the Internet Storm Center. Lenny's expertise is strongest at the intersection of business, technology and information security practices and includes incident response, cloud services and product management. He frequently speaks at conferences, writes articles and has co-authored books on network security and malicious software defenses. Lenny is one of the few individuals in the world who've earned the prestigious GIAC Security Expert designation. He 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.

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.

Topics: Configuring the malware analysis lab; Assembling the toolkit for malware forensics; Performing behavioral analysis of malicious Windows executables; Performing static and dynamic code analysis of malicious Windows executables; Additional learning resources for reverse-engineering malware

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. And you'll experiment with the essential tools and techniques for analyzing web-based malware, such as malicious browser scripts and Flash programs.

Topics: Reinforcing the dynamic analysis concepts learned in 610.1; Patching compiled malicious Windows executables; Analyzing packed malicious executable files; Intercepting network connections in the malware lab; Analyzing Web browser malware implemented in JavaScript and Flash

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.

Topics: Core concepts for reverse-engineering malware at the code level; x86 Intel assembly language primer; Handling anti-disassembling techniques; Identifying key x86 assembly logic structures with a disassembler; Patterns of common malware characteristics at the Windows API level (DLL injection, hooking, keylogging, sniffing, etc.)

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.

Topics: Identifying packers; Manual unpacking of packed and otherwise protected malicious Windows executables; Tips and tricks for bypassing anti-analysis mechanisms built into malware; Additional techniques for analyzing obfuscated browser scripts using tools such as SpiderMonkey

610.5 HANDS ON: Malicious Documents and Memory Forensics

Day five starts by exploring common patterns of assembly instructions often used to gain initial access to the victims computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner and explore steps for analyzing malicious PDF documents with utilities such as Origami and PDF Tools. Another major topic covered in this section is the reversing of malicious Windows executables using memory forensics techniques. We will explore this topic with the help of tools such the Volatility Framework and associated plug-ins. The discussion of memory forensics will bring us deeper into the world of user and kernel-mode rootkits and allow us to use context of the infection to reverse-engineer malware more efficiently.

Topics: Analyzing malicious Microsoft Office (Word, Excel, PowerPoint) and Adobe PDF documents; Examining shellcode in the context of malicious files; Analyzing memory to assess malware characteristics and reconstruct infection artifacts; Using memory forensics to analyze rootkit infections

610.6 HANDS ON: Malware Reverse-Engineering Challenge NEW CONTENT ADDED

Day six assigns students to the role of a malware reverse engineer, working as a member of an incident response and malware analysis team. Students are presented with a variety of challenges involving real-world malware. These challenges validate students' ability to respond to typical malware reversing tasks in an instructor-led lab environment and offers additional learning opportunities. The challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (using a debugger); Static Malware Analysis (using a disassembler); JavaScript Deobfuscation; PDF Document Analysis; Office Document Analysis; Flash File Analysis; Memory Analysis

www.giac.org

www.sans.edu

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

MANAGEMENT 414

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

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
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 Needed
Instructor: Eric Conrad

- GIAC Cert: GISP
- DoDD 8570

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

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.

Obtaining your CISSP® certification consists of:

- Fulfilling minimum requirements for professional work experience
- Completing the Candidate Agreement
- Review of résumé
- 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
- Periodic Audit of CPEs to maintain the credential

Note: CISSP® exams are not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam.

"The course covers a great deal of government and industry-specific content that is necessary for passing the CISSP."
-Rob Oatman, U.S. Coast Guard Academy

"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."
-Jeff Jones,
Constellation Energy Group

"This class focuses like a laser on the key concepts you'll need to understand the CISSP exam. Don't struggle with thousand page textbooks – let this course be your guide!"
-Carl Williams, Harris Corporation

SANS SIMULCAST

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

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.

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 which includes AAA (authentication, authorization, and accountability), using real-world scenarios 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 including routing, switches, key protocols, and how they can be properly protected on the network. The telecommunications domain covers all aspects of communication and what is required to provide an infrastructure that has embedded security.

Topics: Domain 2: Telecommunications and Network Security

414.3 Information Security Governance & Risk Management and Software Development Security

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

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

414.4 Cryptography and Security Architecture & Design

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

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

414.5 Security Operations and Business Continuity & Disaster Recovery Planning

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

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

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

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

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

www.giac.org

DoDD 8570 Required
www.sans.org/8570

MANAGEMENT 512

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPE/CMU Credits
Laptop NOT Needed
Instructor: Stephen Northcutt

- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

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 U.S. government managers and supporting contractors.

Who Should Attend

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

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, and 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.

"Every IT security professional should attend no matter what their position. This information is important to everyone."
-John Flood, NASA

"Gives a good understanding of what knowledge our employees need to have to be successful."
-Teddie Steele,
State Department of FCU

"Mr. Northcutt is able to disseminate the technical information in a way that is very easy to digest without getting overloaded."
-Christian Kopacsi, Chemical Bank

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class which aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

Stephen Northcutt *SANS Faculty Fellow*

Stephen Northcutt founded the GIAC certification and served as president of the SANS Technology Institute. 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 40 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 leads the Management 512 Alumni Forum, where hundreds of security managers post questions. He is the lead author/instructor for Management 512: SANS Security Leadership Essentials for Managers, a prep course for the GSLC certification that meets all levels of requirements for DoD Security Managers per DoD 8570. He also is the lead author/instructor for Management 514: IT Security Strategic Planning, Policy, and Leadership. Stephen blogs at the SANS Security Laboratory. www.sans.edu/research/security-laboratory

512.1 Managing the Enterprise, Planning, Network, and Physical Plant

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

On 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

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.

"The content was excellent and Stephen did an excellent presentation that included real-life examples."
-Stephen Kramper, MED3000

www.giac.org

www.sans.edu


DoDD 8570 Required
www.sans.org/8570

MANAGEMENT 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Recommended
Instructor: Mark Williams
▸ Masters Program

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.

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.

We will see examples and hear stories from businesses, especially IT and security oriented businesses, and then work together on labs. Business needs change, the environment changes, new risks are always on the horizon, and critical systems are continually exposed to new vulnerabilities. Strategic planning is a never-ending process. The planning section is hands-on and there is exercise-intensive work on writing, implementing, and assessing strategic plans.

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.

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, 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.

www.sans.edu

Mark Williams *SANS Instructor*

Mark Williams currently holds the position of principal systems security officer at BlueCross BlueShield of Tennessee. Mark holds multiple certifications in security and privacy including CISSP, CISA, CRISC, and CIPP/IT. He has authored and taught courses at undergraduate and graduate levels, as well as public seminars around the world. He has worked in public and private sectors in the Americas, Canada, and Europe in the fields of security, compliance, and management. Mark has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms. During this career Mark has consulted on issues of privacy and security, lead seminars, and developed information security, privacy, and compliance related programs.

514.1 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 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 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 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, ethics; Warning banners; Policy development process; Policy review and assessment process; Wrap-up, the six golden nuggets of policy

514.5 Leadership and Management Competencies

Essential leadership topics covered here include: leadership development, coaching and training, employee involvement, conflict resolution, change management, vision development, motivation, communication skills, self-direction, brainstorming techniques, benefits, and the ten core leadership competencies. In a nutshell, you'll learn the critical processes that should be employed to develop the skills and techniques to select, train, equip, and develop a team into a single cohesive unit with defined roles that operate together in harmony toward team-objective accomplishment.

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2013/courses

AUDIT 507

Auditing Networks, Perimeters, and Systems

SANS

Six-Day Program
Thu, Dec 12 - Tue, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: David Hoelzer

- GIAC Cert: GSNA
- Masters Program
- DoDD 8570

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is organized specifically to provide 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, the students 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 an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is assisting management to understand the relationship between the technical controls and the risks to the business that these affect. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives 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.

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. Sign up for this course and experience the mix of theoretical, 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

"By far, this is the most hands-on, technical tool-oriented auditing class I have ever seen. I cannot imagine another class that forces you to use real tools in real situations. It is just like gaining real world experience."
-Jay Russell, U.S. Navy

"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."
-Brooks Adams,
Georgia Southern University

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 the 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.

507.1 Effective Auditing, Risk Assessment, Reporting & Cloud Computing

After laying the foundation for the role and function of an auditor in the information security field, this days material will give you two extremely useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and assisting you to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions when dealing with virtualization and with Cloud Computing.

Topics: Auditor's Role in Relation to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Six-Step Audit Process; Virtualization and Cloud Computing

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: Web Application Auditing

Web Applications have consistently rated one of the top five vulnerabilities that enterprises face for the past several years. Unlike the other top vulnerabilities, however, our businesses continue to accept this risk since most modern corporations need an effective web presence to do business today. One of the most important lessons that we are learning as an industry is that installing an application firewall is not enough!

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

507.4 HANDS ON: Advanced Windows Auditing

Microsofts business class system make up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control because of the enormous number of controls and settings within the operating system. This class gives you the keys, techniques and tools to build an effective long term audit program for your Microsoft Windows environment. More importantly, during the course a continuous monitoring and reporting system is built out, allowing you to easily and effectively scale the testing discussed within your enterprise when you return home.

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

507.5 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 have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as, access controls and security models.

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

507.6 HANDS ON: Audit the Flag: A NetWars Experience

This final day of the course presents a capstone experience with additional learning opportunities. Leveraging the well known NetWars engine, students have the opportunity to connect to a simulated enterprise network environment. Building on the tools and techniques learned throughout the week, each student is challenged to answer a series of questions about the enterprise network, working through various technologies explored during the course.

Topics: Technologies Included in the Capstone Challenges:
Network Devices, Servers, Applications, and Workstations

www.giac.org

www.sans.edu

DoDD 8570 Required
www.sans.org/8570

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/cyber-defense-initiative-2013/courses

NEW

AUD444 Auditing Security and Controls of Active Directory and Windows

Three-Day Course
Thu, Dec 12 - Sat, Dec 14
9:00am - 5:00pm
18 CPE/CMU Credits
Laptop Required
Instructor: Tanya Baccam

Who Should Attend

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

Auditors need to be able to understand how Active Directory operates and the key business risks that are present. This course was written to teach auditors how to identify and assess those business risks. Active Directory and Windows systems are typically well known and utilized within organizational infrastructures. However, they can be difficult to audit since there are a large number of settings on the end system. This course provides the tools and techniques to effectively conduct an Active Directory and Windows audit, and while doing so identify key business process controls that may be missing. Students have the opportunity to look at the business process controls and then how those can be verified by looking at Active Directory and the Windows systems that exist. Plus, students are taught how to add additional value to their audits by being able to identify the technology risks that may have been overlooked. The hands-on exercises reinforce the topics discussed in order to give students the opportunity to conduct an audit on their own Windows systems, as well as understand the different security options that Windows provides.

Tanya Baccam *SANS Senior Instructor*

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

NEW

AUD445 Auditing Security and Controls of Oracle Databases

Three-Day Course
Sun, Dec 15 - Tue, Dec 17
9:00am - 5:00pm
18 CPE/CMU Credits
Laptop Required
Instructor: Tanya Baccam

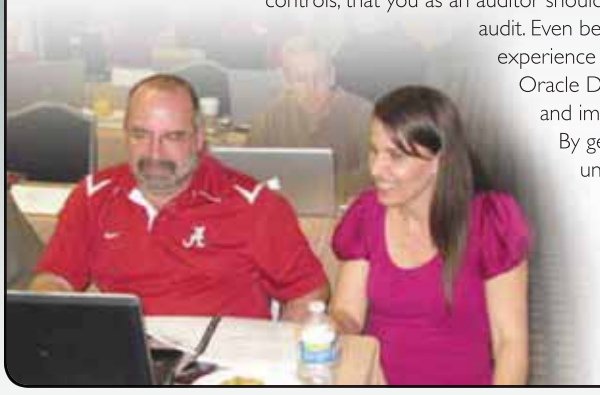
Who Should Attend

- Internal auditors
- IT specialist auditors
- IT auditors
- IT audit managers
- Information system auditors
- Information security officers

Over the past few years we have seen attackers target data since there is a financial incentive to being able to compromise valuable data. The media seems to be reporting new data compromises constantly. That means auditors need to be effectively auditing the controls that should exist to protect this valuable organizational asset.

Oracle Databases often store the data that's being targeted. Oracle Databases are very complex and challenging to audit! Auditors need to be able to effectively audit the processes and controls in place around the database to ensure the asset is being properly protected and the risks properly managed.

This course provides all of the details, including the IT process, procedural and technical controls, that you as an auditor should look for when conducting an Oracle database audit. Even better, you have the opportunity to get firsthand experience extracting and interpreting data from a live Oracle Database which allows you to be able to return and immediately conduct an Oracle Database audit. By getting hands-on experience, you get a better understanding of exactly how an Oracle Database operates and what data is available for audit purposes. The course is also put together in such a way that you can add additional value to the business and provide further security recommendations and benefits for the database being audited.



SANS Hosted are a Series of Classes presented by other educational providers to complement your needs for training outside of our current course offerings.

(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

Five-Day Program
Thu, Dec 12 - Mon, Dec 16
9:00am - 5:00pm
35 CPE/CMU Credits
Laptop NOT Needed
Instructor: Frank Shirmo

Notice: Please note that the price of tuition does NOT include the CSSLP® exam. SANS Hosted are a series of classes presented by other educational providers to complement your needs for training outside of our current course offerings.

This course will help you advance your software development expertise by ensuring you're properly prepared to take on the constantly evolving vulnerabilities exposed in the SDLC. It will train you on every phase of the software lifecycle detailing security measures and best practices for each phase. The CSSLP® Education Program is for all the stakeholders involved in software development. By taking this course, not only will you enhance your ability to develop software with more assurance you will understand how to build security within each phase of the software lifecycle.

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 CSSLP® man
- Secure Software Implementation/Coding - unit testing for security functionality and resiliency to attack, and developing secure code and exploit mitigation
- Secure Software Testing - integrated QA testing for security functionality and resiliency to attack
- Software Acceptance - security implication in the software acceptance phase
- Software Deployment, Operations, Maintenance and Disposal - security issues around steady state operations and management of software

Frank Shirmo *(ISC)² Instructor*

Mr. Frank Shirmo is a veteran information technology executive and an accomplished information security manager. Frank's diverse technology background and extensive years of experience in the software world has spanned all phases of the development lifecycle. He has effectively established, led, and managed small and large engineering teams. As a CTO, VP of engineering, general manager and director of information security practice, Frank has had overall responsibilities for software product portfolio strategies, software product line maintenance, and IT security services offerings. Frank is well versed on various platforms, technologies, protocols, frameworks, and standards. As an information security professional, Frank has maintained a focus on secure software development lifecycle and is considered a subject matter expert in his field. Throughout his tenure as an information security professional, he has gained the solid experience needed for the effective management of information security programs and has had the opportunity to gain the hands-on experience of security code reviews, threat modeling, attack surface analysis, and security testing. Frank has also acted as the program/project manager on small and large scale vulnerability assessment and penetration testing projects. Frank's progressive career is augmented with his solid academic background. He has earned his B.S and M.S in Computer Science and Engineering from Towson and Loyola Universities and pursued a Doctorate in Management and Leadership at University of Maryland. Frank possesses decades of experience as a teacher, and as a trainer. His powerful and unique style of training delivery has gained him a good deal of popularity in the classroom environment, both virtual and physical. Frank is a proud husband and father of three, currently living in the suburbs of Annapolis, Maryland.

SEC434 Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting

Two-Day Course
Wed, Dec 18 - Thu, Dec 19
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, how's 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.

"SANS training is like a catalyst. It not only boosts your knowledge but also inspires you to learn more."
-Tan Koon Yaw

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 your 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.

The class also includes an in-depth look at deploying, configuring and operating an open source tool OSSEC for log analysis, alerting and event correlation.

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.

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course
Wed, Dec 18 - Thu, Dec 19
9:00am - 5:00pm
12 CPE/CMU Credits
Laptop Required
Instructor: Eric Conrad

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.

Who Should Attend

- This class would be essential to any industry that has to test regularly as part of compliance requirements or regularly tests their security infrastructure as part of healthy security practices.
- Penetration testers
- Vulnerability assessment personnel
- Auditors
- General security engineers
- Security researchers

MGT305 Technical Communication and Presentation Skills for Security Professionals

One-Day Course
Wed, Dec 18
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Required
Instructor: David Hoelzer
▸ Masters Program

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. We will share tips and techniques of top presenters that you can apply to give the best presentation of your career.

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

www.sans.edu

NEW

MGT415 A Practical Introduction to Risk Assessment

One-Day Course
Wed, Dec 18
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Required
Instructor: James Tarala

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Who Should Attend

- Any security engineers, compliance directors, managers, auditors – basically any SANS alumni potentially
- Auditors
- Directors of security compliance
- Information assurance management
- System administrators

MGT433 Securing The Human: Building and Deploying an Effective Security Awareness Program

Two-Day Course
Wed, Dec 18 - Thu, Dec 19
9:00am - 5:00pm
12 CPE/CMU Credits
Laptop NOT Needed
Instructor: Lance Spitzner
▸ Masters Program

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 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

www.sans.edu

MANAGEMENT SKILL-BASED COURSE

MGT535 Incident Response Team Management

One-Day Course
Wed, Dec 18
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Recommended
Instructor: Christopher Crowley

Who Should Attend

- Information security engineers and managers
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

This course will take you to the next level of managing an incident response team. Given the frequency and complexity of today's attacks, incident response has become a critical function for organizations. Detecting and efficiently responding to incidents, especially those where critical resources are exposed to elevated risks, has become paramount, and to be effective, incident response efforts must have strong management processes to facilitate and guide them. Managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. Furthermore, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

This course was developed by an information security professional with over 26 years of experience, much of it in incident response. He was the founder of the first U.S. government incident response team. Students will learn by applying course content through hands-on skill-building exercises. These exercises range from: writing and evaluating incident response procedures, to the table-top validation of procedures, incident response management role playing in hypothetical scenarios, and hands-on experience in tracking incident status in hypothetical scenarios.

HOSTED SKILL-BASED COURSE

HOSTED (ISC)²® Systems Security Certified Practitioner – SSCP® Review

Two-Day Course
Wed, Dec 18 - Thu, Dec 19
9:00am - 5:00pm
12 CPE/CMU Credits
Laptop NOT Required
Instructor: Adam Gordon

Who Should Attend

- Network security engineers
- Security administrators
- System administrators
- Application programmers
- Database administrators
- Systems analysts
- Non-security specific technical positions that require an understanding of security concepts

This course is geared toward individuals who hold technical and engineering related information technology positions such as network security engineers, systems security analysts, security administrators as well as non-security specific technical positions that require an understanding of security concepts and of best security practices including system administrators, application programmers, database administrators and systems analysts. This course will use best practice methodologies for a constructive learning environment. In employing this framework, concepts will be shared with the class in a traditional format in order to expand their frame of reference, but learners will also share their individual experiences, in and from the workplace, based upon these concepts. The individual learners in the classroom have varied experiences, workplace tasks, and hands-on knowledge that will allow others to comprehend and increase their own understandings in order to grow, retain, and transfer this newly attained knowledge.

The course was developed by an information security professional with over 25 years of experience as both an educator and IT professional, Adam holds over 150 Professional IT Certifications including CISA, CISSP, SSCP, CRISC, CHFI, CEH, VCP, and SCNA. He is the author of several books and has achieved many awards, including ECCouncil Instructor of Excellence for 2006-07 and Top Technical Instructor Worldwide, 2002-2003. Adam holds his Bachelors Degree in International Relations and his Masters Degree in International Political Affairs from Florida International University.

Core material to be addressed based on the 7 domains of the SSCP® CBK:

1. Access Controls
2. Security Operations and Administration
3. Monitoring and Analysis
4. Risk, Response, and Recovery
5. Cryptography
6. Networks and Communication
7. Malicious Code and Activity

You don't have to miss out on SANS' top-rated training. Attend your choice of six popular 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 courses will be available via SANS Simulcast:

SEC301

SEC401

MGT414

FOR408

FOR508

FOR610

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 Cyber Defense Initiative 2013 Simulcast course, please visit www.sans.org/event/cyber-defense-initiative-2013/attend-remotely

Powered by

NETWARS

A True Hands-On Interactive Security Challenge!

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

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

The NetWars competition will be played over two evenings: December 15 & 16.

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 2013

(NON-STUDENTS ENTRANCE FEE IS $1,249).

Register at

www.sans.org/event/cyber-defense-initiative-2013

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

There will be two additional NetWars Tournament events held simultaneously at SANS CDI 2013:

DFIR NetWars

NetWars Tournament of Champions

(Invite only)

SANS DFIR NETWARS TOURNAMENT

DFIR NetWars Tournament is designed to help participants develop skills in several critical DFIR areas:

- **Malware Analysis**
- **Digital Forensics**
- **Incident Response**
- **File and Packet Analysis**

SANS NETWARS TOURNAMENT of CHAMPIONS

2nd Annual NetWars Tournament of Champions

December 15 & 16, 2013 | Invite Only

If you believe you qualify for this Tournament, please contact us at netwars@sans.org and we will validate and register you. The $1249 fee will be waived for all individuals who qualify for the Tournament of Champions!

CDI BONUS SESSIONS

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, hear from the voices that matter in computer security, and get the most for your training dollar.

KEYNOTE: APT: It is Time to Act *Dr. Eric Cole*

Albert Einstein said "We cannot solve our problems with the same thinking we used when we created them." With the new advanced and emerging threat vectors that are breaking into networks with relative ease, a new approach to security is required. The myth that these attacks are so stealthy they cannot be stopped is just not true. There is no such thing as an unstoppable adversary. It is time to act. In this engaging talk one of the experts on APT, Dr. Cole, will outline an action plan for building a defensible network that focuses on the key motto that "Prevention is Ideal but Detection is a Must". Better understand what the APT really is and what organizations can do to be better prepared. The threat is not going away, so the more organizations can realign their thinking with solutions that actually work, the safer the world will become.

An Introduction to PowerShell for Security Assessments *James Tarala*

With the increased need for automation in operating systems, every platform now provides a native environment for automating repetitive tasks via scripts. Since 2007, Microsoft has gone "all in" with their PowerShell scripting environment, providing access to every facet of the Microsoft Windows operating system and services via a scriptable interface. Administrators can completely administer and audit not only an operating system from this shell, but most all Microsoft services, such as Exchange, SQL Server, and SharePoint services as well. In this presentation James Tarala of Enclave Security will introduce students to using PowerShell scripts for assessing the security of the Microsoft services. Auditors, system administrators, penetration testers, and others will all learn practical techniques for using PowerShell to assess and secure these vital Windows services.

New School Forensics: Latest Tools and Techniques in Memory Analysis *Chad Tilbury*

Whether you are just getting started with memory forensics, or you have been at it since the early days, the last year produced a wealth of new memory analysis capabilities. Notably, nearly all of the progress has been accomplished in free and open source tools. Learn about the latest and greatest additions to the memory forensics arsenal:

- In-memory registry forensics
- Mac and Linux memory analysis
- Building and analyzing memory object timelines
- The advantages of live memory analysis

Sharing Without Borders: Attacking and Testing SharePoint *Kevin Johnson*

SharePoint has become one of the most common platforms in organizations today. Originally designed for simple content management, it has grown into a workflow, CMS, and communication powerhouse that runs on the Internet and intranets all over the world. While it is powerful, most organizations do not realize the risks it exposes within their organization. Kevin Johnson will be walking attendees through the systems available under the SharePoint name, as well as showing ways that penetration testers are able to assess and exploit them. He will also be releasing a series of tools and guidelines to help organizations assess their SharePoint systems.

Effective Phishing that Employees Like *Lance Spitzner*

One of the toughest challenges in establishing a high-impact security awareness program is measuring the impact. Are you changing behavior and reducing risk? Phishing assessments are a powerful way to measure such change, while addressing one of the most common human risks. As more organizations use phishing assessments, many of them are doing it wrong, not only negatively impacting their metrics but generating resentment among employees. In this short presentation, learn how to create a fun, engaging phishing program that not only effectively measures and reinforces key behaviors, but is also truly enjoyed by employees.

Introducing the CompTIA® CASP™ Exam *Eric Conrad and Seth Misenar*

Eric Conrad and Seth Misenar, coauthors of "Syngress CISSP® Study Guide", will introduce you to the new CompTIA® Advanced Security Practitioner certification, a hands-on technical exam with a mix of deeper technical questions, as well as higher-level management questions. The CASP™ was recently added to DoD 8570 for the following roles: IAT level III, IAM II, and IASAE level I and II. Will this cert be a valuable addition to your resume? Will this cert bleed significant market share from the CISSP®? Now that it has been added to DoD8570, will CASP™ become the go to DoD cert? Come find out where CASP™ fits into the security certification landscape and see if Eric and Seth's new SANS prep course for the CASP™ is right for you.

For dates, times, and complete information, please visit
www.sans.org/event/cyber-defense-initiative-2013/bonus-sessions

CDI BONUS SESSIONS

Securing The Kids *Lance Spitzner*

Technology is an amazing tool. It allows our kids to access a tremendous amount of information, meet new people, and communicate with friends around the world. In addition, for them to be successful in the 21st century they have to know and understand how to leverage these new tools. However, with all these capabilities come a variety of new risks, risks that as parents you may not understand or even be aware of. In this one hour presentation we cover the top three risks to kids online and the top five steps you can take to protect them. This course is based on the experiences and lessons learned from a variety of SANS top instructors who not only specialize in security, but are parents just like you. This talk is sponsored and delivered by SANS Securing The Human program.

Using RE to Turn the Tables! *David Hoelzer*

In this 60-minute presentation we will examine the discovery of a piece of targeted malware, discover hidden features, and use the malware's own libraries to turn the tables on the attacker to recover the passwords used to safeguard the "hidden features" and administrative interfaces that the malware contains! While the presentation will demonstrate reverse engineering, including binary disassembly, the discussion is always at a level that anyone attending can walk away with useful information, whether you are deeply technical or a C-level executive! Come and help us turn the tables on this attacker!

Windows Exploratory Surgery with Process Hacker *Jason Fossen*

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

Who's Watching the Watchers? *Mike Poor*

We have instrumented our networks to the Nth degree. We have firewalls, IDS, IPS, Next Gen Firewalls, Log correlation, and aggregation...but do we know if we have it right? Will we detect the NextGen™ attackers? In this talk we will explore ways that we improve the signal/noise ratio in our favor, and help identify the needle in the needlestack.

GIAC Program Overview

GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. Find out why this is important to your career.

SANS Technology Institute Open House

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery. If you aspire to help lead your organization's or your country's information security program and you have the qualifications, organizational backing, and personal drive to excel in these challenging degree programs, we will welcome you into the program.

Lunch & Learns

Short presentations given during the lunch break.

How to Become a SANS Instructor *Eric Conrad*

Have you ever wondered what it takes to teach for SANS? Wondering why our SANS Instructors do what they do? Join us for a lunch and learn where well share with you what it takes to become a Certified SANS Instructor. Space is limited and registration is required. Lunch is provided.

Vendor Expo

December 13, 2013 | 10:30am-10:50am | 12:30pm-1:15pm | 3:00pm-3:20pm

Our events incorporate external vendor partners showcasing some of the best security solutions available. Take advantage of the opportunity to interact with the people behind the products and learn what they have to offer you and your organization.

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 unique master's degree programs:

Master of Science in Information Security Engineering

Master of Science in Information Security Management

"The STI master's degree program combines the best of administrative and technical security into the curriculum. When you achieve your degree, you're well versed and can address any and all challenges placed before you."

-Kevin Fuller, MSISE Student

Apply today!
Cohorts are forming now.
www.sans.edu

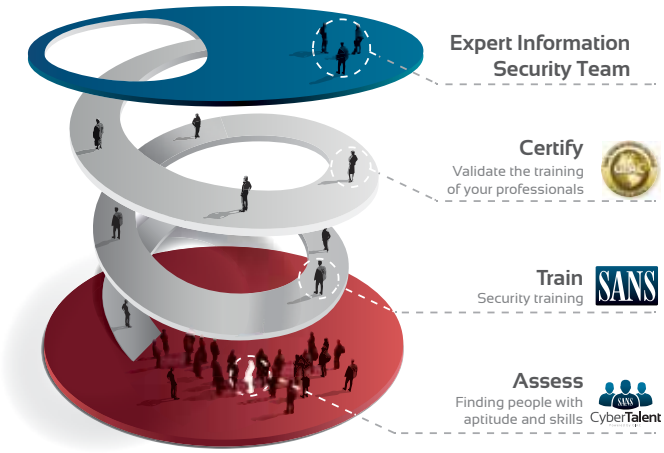
www.sans.edu
info@sans.edu
855-672-6733

Contact Us to Learn More

www.sans.org/cybertalent

A Web-Based Recruitment and Talent Management Tool

Introducing SANS CyberTalent Assessments, a new web-based recruitment and talent management tool that helps validate the skills of information security professionals. This unique tool may be used during the recruitment process of new information security employees and to assess the skills of your current staff to create a professional development plan. This tool will save you money and time, as well as provide you with the information required to ensure you have the right skills on your information security team.



Benefits of SANS CyberTalent Assessments

For Recruiting

- Provides a candidate ranking table to compare the skills of each applicant
- Identifies knowledge gaps
- Saves time and money by identifying candidates with the proper skillset

For Talent Management

- Determines baseline knowledge levels
- Identifies knowledge gaps
- Helps develop a professional development plan

US and Canada 301.654.SANS (7267) | www.sans.org/cybertalent
EMEA and APAC inquiries: + 44 (0) 20 3598 2363

How Are You Protecting Your

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, IT audit, management, and IT security law.

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

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

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

Department of Defense Directive 8570 *(DoDD 8570)*

www.sans.org/8570

DoDD 8570 is changing to 8140 in 2013

Department of Defense Directive 8570 (DoDD 8570) provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC provides the most options in the industry for meeting 8570/8140 requirements.

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CND Service Provider Manager
GCIA **GCIH** CEH	SSCP CEH	**GCIH** CSIH CEH	**GSNA** CISA CEH	CISSP - ISSMP CISM

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN **GCUX**

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

Compliance/Recertification:

To stay compliant with DoD 8570 requirements, you must maintain your certifications. GIAC certifications are renewable every four years.

Go to www.giac.org to learn more about certification renewal.

SANS Training Courses for DoDD Approved Certifications

SANS TRAINING COURSE		DoDD APPROVED CERT
SEC401	Security Essentials Bootcamp Style	GSEC
SEC501	Advanced Security Essentials – Enterprise Defender	GCED
SEC503	Intrusion Detection In-Depth	GCIA
SEC504	Hacker Techniques, Exploits, and Incident Handling	GCIH
AUD507	Auditing Networks, Perimeters, and Systems	GSNA
FOR508	Advanced Computer Forensic Analysis and Incident Response	GCFA
MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	CISSP
MGT512	SANS Security Essentials for Managers with Knowledge Compression™	GSLC

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 & Resisting Malware (GCWN)
SEC506	Securing Linux/Unix (GCUX)

Red Team Courses

SEC542	Web App Penetration Testing & 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.

SECURITY AWARENESS FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.
- Training is mapped against the 20 Critical Controls framework.
- Create your own program by choosing a variety of End User awareness modules.
- Enhance training by adding compliance topics, such as NERC-CIP, PCI DSS, HIPPA, FERPA, and Red Flags, to name a few.
- Test your employees and identify vulnerabilities through phishing emails.
- For a free trial visit us at www.securingthehuman.org

FUTURE SANS TRAINING EVENTS

SANS Network Security 2013

Las Vegas, NV | September 14-23

www.sans.org/event/network-security-2013

SANS Seattle 2013

Seattle, WA | October 7-14

www.sans.org/event/seattle-2013

SANS Baltimore 2013

Baltimore, MD | October 14-19

www.sans.org/event/baltimore-2013

SANS Chicago 2013

Chicago, IL | Oct 28 - Nov 2

www.sans.org/event/chicago-2013

SANS South Florida 2013

Fort Lauderdale, FL | November 4-9

www.sans.org/event/south-florida-2013

SANS Pen Test Hackfest
TRAINING EVENT AND SUMMIT

Washington, DC | November 7-14

www.sans.org/event/pen-test-hack-fest-2013

SANS San Diego 2013

San Diego, CA | November 18-23

www.sans.org/event/san-diego-2013

SANS San Antonio 2013

San Antonio, TX | December 3-8

www.sans.org/event/san-antonio-2013

FUTURE SANS TRAINING EVENTS

SANS **Golden Gate** 2013

San Francisco, CA | December 16-21

www.sans.org/event/golden-gate-2013

SANS **Security East** 2014

New Orleans, LA | January 20-25

www.sans.org/event/security-east-2014

SANS **AppSec** 2014
TRAINING EVENT AND SUMMIT

Austin, TX | February 3-8

www.sans.org/event/app-sec-2014

SANS **Cyber Guardian** 2014

Baltimore, MD | March 3-8

www.sans.org/event/cyber-guardian-2014

SANS **DFIRCON** 2014
DFIR-FOCUSED TRAINING EVENT

Monterey, CA | March 5-10

www.sans.org/event/dfircon-monterey-2014

NORTH AMERICAN **ICS/SCADA Security** 2014
TRAINING EVENT AND SUMMIT

Monterey, CA | March 11-20

www.sans.org/event/north-american-ics-scada-summit-2014

SANS 2014

Orlando, FL | April 8-14

www.sans.org/event/sans-2014

SANSFIRE 2014

Baltimore, MD | June 19-30

www.sans.org/event/sansfire-2014

SANS TRAINING FORMATS

LIVE CLASSROM TRAINING

Multi-Course Training Events
Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers
www.sans.org/security-training/by-location/all

Community SANS
Live Training in Your Local Region with Smaller Class Sizes
www.sans.org/community

OnSite
Live Training at Your Office Location
www.sans.org/onsite

Mentor
Live Multi-Week Training with a Mentor
www.sans.org/mentor

Summit
Live IT Security Summits and Training
www.sans.org/summit

ONLINE TRAINING

OnDemand
E-learning available anytime, anywhere, at your own pace
www.sans.org/ondemand

vLive
Convenient online instruction from SANS' top instructors
www.sans.org/vlive

Simulcast
Attend a SANS training event without leaving home
www.sans.org/simulcast

CyberCon
Live online training event
www.sans.org/cybercon

SelfStudy
Self-paced online training for the motivated and disciplined infosec student www.sans.org/selfstudy

Hotel Information

Training Campus
Washington Hilton

1919 Connecticut Ave. NW
Washington, DC 20009
www.sans.org/event/cyber-defense-initiative-2013/location

Special Hotel 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 14, 2013.

To make reservations, use the following link:
www.hilton.com/en/hi/groups/personalized/D/DCAWHHH-SANSCD-20131210/index.jhtml.
You can also call (800) HILTONS (800-445-8667) and ask for the SANS group rate.

Located in the heart of Washington, DC, the Washington Hilton hotel is situated near the capital's most sought-after neighborhoods. Enjoy the best entertainment and nightlife Washington has to offer at the nearby Adams Morgan, Woodley Park and the U Street Corridor. This Washington, DC hotel is one mile from the Smithsonian National Zoo and only four blocks from Dupont Circle Metro. Discover iconic Washington attractions including the White House, National Monument and Lincoln Memorial.

Experience a memorable hotel dining experience in The District Line Restaurant, offering regionally inspired comfort foods and seasonal dishes with locally sourced ingredients. Enjoy traditional American favorites, delicious seafood and healthy salads. Meet with friends over cocktails in the stylish TDL Bar or unwind with your favorite drink and watch sports on one of 15 flat-screen TVs in the comfortable McClellan's Sports Bar.

Stay in shape during your stay at this Washington, DC hotel in the heated outdoor pool and fully equipped fitness center. Unwind in the beautiful Heights Courtyard and Gardens and enjoy flickering fire pits, calming water features and a stunning view of Washington's skyline.

Top 5 reasons to stay at the Washington Hilton

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Washington Hilton, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Washington Hilton that you won't want to miss!
5. Everything is in one convenient location!

Registration Information

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

Register online at www.sans.org/event/cyber-defense-initiative-2013

How to Register

1. To register, go to www.sans.org/event/cyber-defense-initiative-2013.

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 U.S. 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/event/network-security-2013/attendee-info**

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 Cyber Defense Initiative 2013 Simulcast course, please visit www.sans.org/event/cyber-defense-initiative-2013/attend-remotely

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	10/23/13	$500.00	11/6/13	$250.00

Some restrictions apply.

Group Savings (Applies to tuition only)

15% discount if 12 or more people from the same organization register at the same time
10% discount if 8 - 11 people from the same organization register at the same time
5% discount if 4 - 7 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at www.sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: **registration@sans.org** or fax: **301-951-0140**. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by **November 13, 2013** – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your Fiscal Year. The SANS Voucher Discount Program pays you credits and delivers flexibility. **www.sans.org/vouchers**

SANS CDI 2013 REGISTRATION FEES

Register online at **www.sans.org/event/cyber-defense-initiative-2013/courses**

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 10/23/13	Paid by 11/6/13	Paid after 11/6/13	Add GIAC Cert	Add OnDemand
☐ SEC301	Intro to Information Security	$3,675	$3,925	$4,175	☐ $579	☐ $449
☐ SEC401	Security Essentials Bootcamp Style	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ SEC501	Advanced Security Essentials – Enterprise Defender	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ SEC503	Intrusion Detection In-Depth	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ SEC504	Hacker Techniques, Exploits, and Incident Handling	$4,345	$4,595	$4,845	☐ $579	☐ $449
☐ SEC505	Securing Windows and Resisting Malware **NEW!**	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ SEC542	Web Application Penetration Testing and Ethical Hacking	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ SEC566	Implementing & Auditing the Twenty Critical Security Controls – In-Depth	$3,675	$3,925	$4,175		☐ $449
☐ SEC575	Mobile Device Security and Ethical Hacking	$4,345	$4,595	$4,845	☐ $579	☐ $449
☐ SEC579	Virtualization and Private Cloud Security	$4,345	$4,595	$4,845		☐ $449
☐ SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	$4,145	$4,395	$4,645	☐ $579	
☐ FOR408	Computer Forensic Investigations – Windows In-Depth	$4,345	$4,595	$4,845	☐ $579	☐ $449
☐ FOR508	Advanced Computer Forensic Analysis and Incident Response	$4,345	$4,595	$4,845	☐ $579	☐ $449
☐ FOR526	Windows Memory Forensics In-Depth **NEW!**	$3,675	$3,925	$4,175		
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$4,145	$4,395	$4,645	☐ $579	☐ $449
☐ MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	$3,495	$3,745	$3,995	☐ $579	☐ $449
☐ MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	$4,245	$4,495	$4,745	☐ $579	☐ $449
☐ MGT514	IT Security Strategic Planning, Policy, and Leadership	$3,675	$3,925	$4,175		☐ $449
☐ AUD507	Auditing Networks, Perimeters, and Systems	$3,945	$4,195	$4,445	☐ $579	☐ $449
☐ HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program	$3,145	$3,145	$3,145		

Skill-Based Short Courses

		If taking a 5-6 day course	Paid by 10/23/13	Paid by 11/6/13	Paid after 11/6/13	Add GIAC Cert	Add OnDemand
☐ SEC434	Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting	$1,350	$2,045	$2,045	$2,045		
☐ SEC580	Metasploit Kung Fu for Enterprise Pen Testing	$1,250	$1,800	$1,800	$1,800		
☐ MGT305	Technical Communication and Presentation Skills for Security Professionals	$575	$1,045	$1,045	$1,045		
☐ MGT415	A Practical Introduction to Risk Assessment **NEW!**	$575	$1,045	$1,045	$1,045		
☐ MGT433	Securing The Human: Building and Deploying an Effective Security Awareness Program	$1,250	$1,800	$1,800	$1,800		
☐ MGT535	Incident Response Team Management	$575	$1,045	$1,045	$1,045		
☐ AUD444	Auditing Security and Controls of Active Directory and Windows **NEW!**	N/A	$2,400	$2,400	$2,400		
☐ AUD445	Auditing Security and Controls of Oracle Databases **NEW!**	N/A	$2,400	$2,400	$2,400		
☐ HOSTED	(ISC)²® Systems Security Certified Practitioner – SSCP® Review	N/A	$975	$975	$975		
☐ SPECIAL	NetWars – Tournament of Champions Entrance Fee	FREE	$1,249	$1,249	$1,249		

Individual Course Day Rates If Not Taking a Full Course

☐ One Full Day	$1,350
☐ Two Full Days	$2,075
☐ Three Full Days	$3,025
☐ Four Full Days	$3,775
☐ Five Full Days	$4,575
☐ Six Full Days	$4,875
☐ Seven Full Days	$5,475
☐ Eight Full Days	$5,995

REMINDER:

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