

# SANS

THE MOST TRUSTED NAME IN INFORMATION  
AND SOFTWARE SECURITY TRAINING

*"This course is helping  
me solidify my security  
knowledge and it will  
allow me to apply it  
back at work."*

-EDMUND CHEUNG, SoCAL EDISON



GIAC Approved Training

# Network Security 2014

Las Vegas, NV | October 19-27, 2014

*Hands-on immersion training courses  
taught by the nation's highest-rated instructors*

## Security Essentials Bootcamp Style

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

**Network Penetration Testing and Ethical Hacking**

**Windows Forensic Analysis**

**Web App Penetration Testing and Ethical Hacking**

**Intrusion Detection In-Depth**

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

*...and dozens of other courses on network and software security,  
forensics, cybersecurity and the law, management, IT audit,  
industrial control systems, and more.*

Register at

[sans.org/event/network-security-2014](http://sans.org/event/network-security-2014)



Dear Colleague,

Please accept our invitation to attend **SANS Network Security 2014** from **October 19-27**. SANS will bring you the best in network security training, certification, and up-to-the-minute research on the most important topics in the industry today. Use this brochure to review more than 40 courses with a great selection from our IT security and security management curricula, along with forensics, IT audit, data security law, and three secure coding offerings. We will again be using **Caesars Palace** in Las Vegas for our campus.

If you have attended this event in the past, then you know how valuable it can be to your career and to the safety of your company's online and computerized resources. If you are new to SANS Network Security 2014, we promise you a high-energy program with hands-on labs, a huge **Vendor Expo**, evening talks on the most timely security challenges, and a myriad of networking opportunities.

At SANS Network Security 2014, you'll get hands-on, immersion training from SANS' world-class instructors and learn what it takes to stop cybercrime for your organization. Our line-up includes several new courses: **SEC511: Continuous Monitoring and Security Operations**; **SEC760: Advanced Exploit Development for Penetration Testers**; **FOR526: Memory Forensics In-Depth**; **FOR572: Advanced Network Forensics and Analysis**; **FOR585: Advanced Smartphone Forensics**; and **ICS410: ICS/SCADA Security Essentials**. Many of the hottest courses will sell out quickly, so register today!

SANS Network Security 2014 is rich with options. You can select a job-based full course to meet your training needs, but you can also select a short skill-based course to maximize your training investment. SANS courses prepare you for **GIAC** certification, which proves that you have the network security skills, training, and experience to protect critical IT infrastructure. Are you considering earning a master's degree in your field? Many of the courses offered at SANS Network Security 2014 can be applied toward a master's degree or a graduate certificate through the **SANS Technology Institute**. See page 74 to learn more.

You can also choose to take part in the **Core NetWars Tournament** or **DFIR NetWars Tournament** on the evenings of October 23 and 24. NetWars is growing in popularity at each event due to its relevance to current security challenges. Both tournament events are hands-on, interactive learning scenarios that enable information security and DFIR professionals to develop and master real-world, in-depth skills:

- **Core NetWars** is a computer and network security challenge designed to test a participant's experience and skills in a safe environment while having a little fun with your fellow IT security professionals.
- **DFIR NetWars** is an incident simulator packed with a vast amount of forensic and incident response challenges, enabling players to learn the skills to stop data breaches and solve complex crimes.

NetWars was a big hit last year, so don't miss the chance to secure your seat!

Be sure to check out the new **SANS Brochure Challenge** on the next page.

If you have penetration testers, forensics experts, and application and software developers on your staff, get them to Las Vegas for SANS Network Security 2014. They will bring back tools and knowledge to protect your assets!

The cybersecurity industry changes daily—attacks make national news all the time and enterprises everywhere are facing increasingly complex challenges. Nothing beats a SANS live training event to bring you face to face with industry leaders who are uniquely equipped to give you the best training available to meet those challenges head on. You will be able to use what you learn the day you return to work!

SANS Network Security is your annual networking opportunity. **See you in Las Vegas!**

Here's what  
Network Security 2013  
attendees had to say about  
the value of their training

**"I would like to thank  
all the SANS staff  
and instructors for  
continuing to make  
this training event an  
excellent source for  
balanced, timely, and  
high-quality education  
and interaction.**

**Well done!"**

**-SHARON O'BRYAN, DeVry Inc.**

**"Keeping material  
relevant is what SANS  
has been doing.  
Keep up the good  
work!"**

**-B. TAYLOR, U.S. NAVY**

**"Once again, blown away  
by the in-depth content  
– just when I thought I  
got it, there was more  
info to dissect."**

**-MATTHEW BRITTON, BCBSLA**



**AWARDS  
2014  
WINNER**  
Honored in the U.S.



**@SANSInstitute**

**Join the conversation: #SANSNetworkSecurity**



**SANS**  
IT SECURITY  
TRAINING  
AND YOUR  
CAREER  
ROADMAP

# Information Security

Information security professionals are responsible for research and analysis of security threats that may affect an organization's assets, products, or technical specifications. This security professional will dig into technical protocols and specifications for a greater understanding of security threats than most of his/her peers, identifying strategies to defend against attacks by gaining an intimate knowledge of the threats.

**SAMPLE JOB TITLES**

- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect

**CORE COURSES**

**TECHNICAL INTRODUCTORY**

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

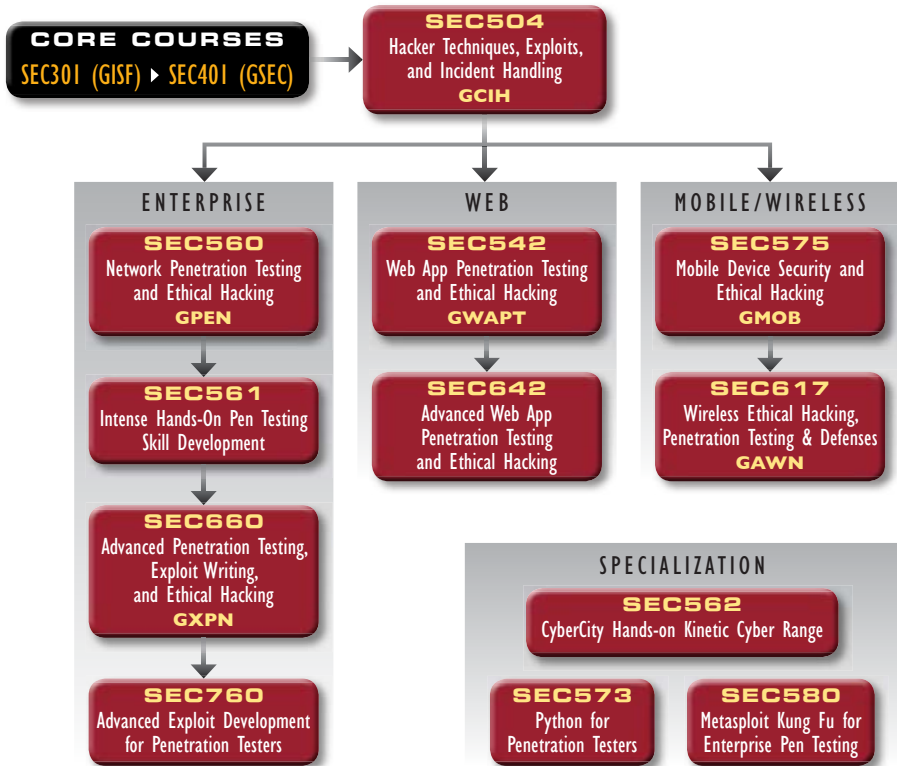
**CORE**

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

**IN-DEPTH**

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

## Penetration Testing/Vulnerability Assessment



Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, write modern exploits, and recommend mitigations before they are exploited by real-world attackers.

**SAMPLE JOB TITLES**

- Penetration tester
- Vulnerability assessor
- Ethical hacker
- Red/Blue team member
- Cyberspace engineer

## Risk and Compliance/Auditing/Governance Titles

**SEC566**  
Implementing and Auditing the Critical Security Controls – In-Depth  
**GCCC**

**AUD507**  
Auditing Networks, Perimeters, and Systems  
**GSNA**

These experts assess and report risks to the organization by measuring compliance with policies, procedures, and standards. They recommend recommendations for improvements to make the organization more efficient and profitable through continuous monitoring of risk management.

**SAMPLE JOB TITLES**

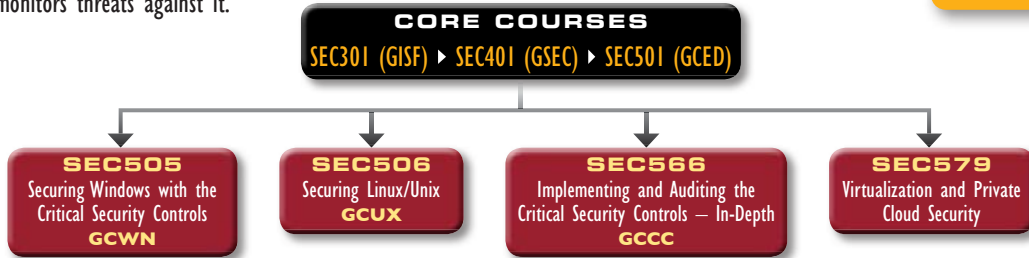
- Auditor
- Compliance officer

## Network Operations Center, System Admin, Security Architecture

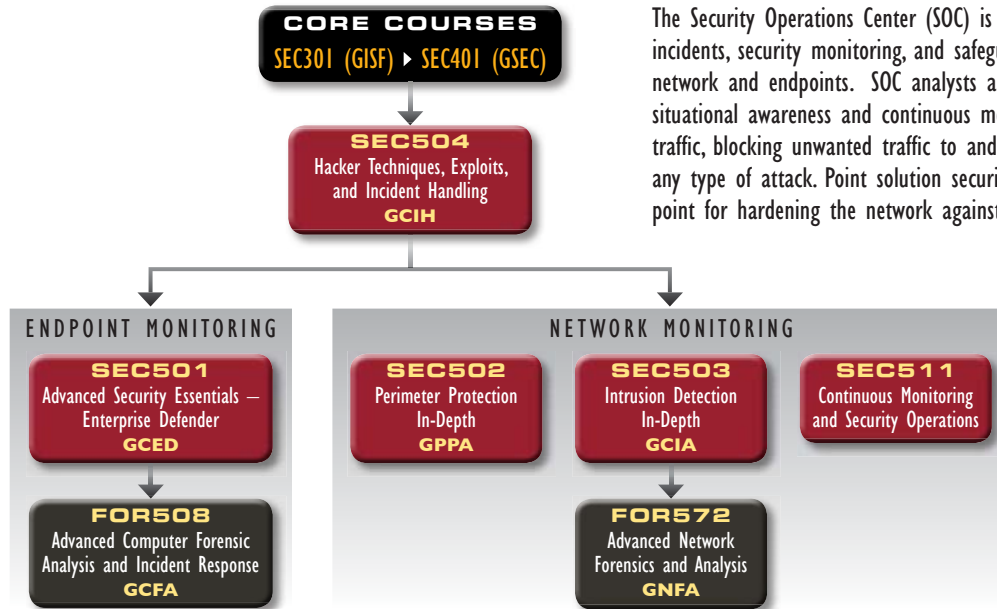
A Network Operations Center (NOC) is the location where IT professionals supervise, monitor, and maintain the enterprise network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC works hand-in-hand with the Security Operations Center, which safeguards the enterprise and continuously monitors threats against it.

### SAMPLE JOB TITLES

- System/IT administrator
- Security administrator
- Security architect/engineer



## Security Operations Center/Intrusion Detection



The Security Operations Center (SOC) is the focal point of cyber-related incidents, security monitoring, and safeguarding assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous monitoring, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

### SAMPLE JOB TITLES

- Intrusion detection analyst
- Security operations center analyst/engineer
- CERT member
- Cyber threat analyst

## Development – Secure Development



The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

### SAMPLE JOB TITLES

- Developer
- Software architect
- QA tester
- Development manager

# NETWARS

**In-Depth,  
Hands-On InfoSec Skills**

[sans.org/netwars](http://sans.org/netwars)

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

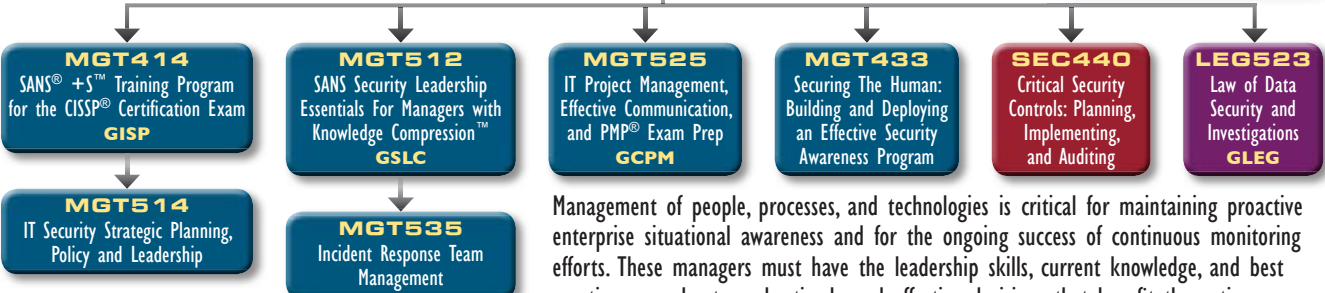
- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing
- Intrusion Detection

## Cyber or IT Security Management

**CORE COURSES**  
SEC301 (GISF) ▶ SEC401 (GSEC)

**SAMPLE JOB TITLES**

- CISO
- Cybersecurity manager/officer
- Security director



Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. These managers must have the leadership skills, current knowledge, and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

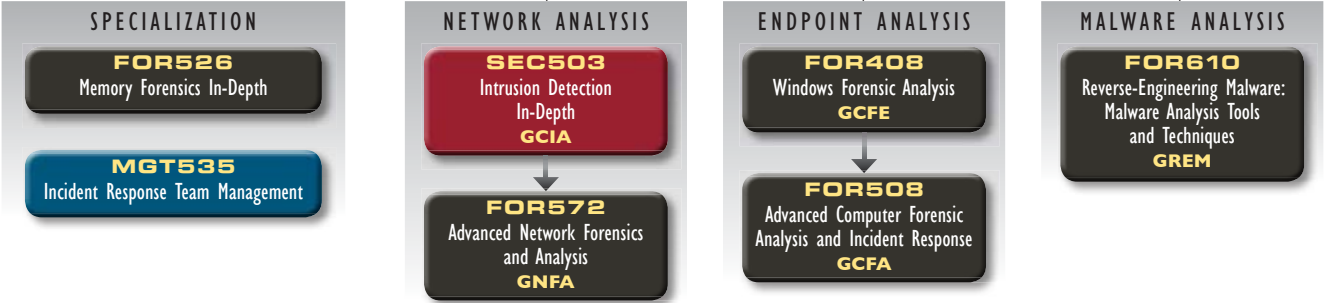
## Incident Response

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and mitigate a security incident.

**SAMPLE JOB TITLES**

- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst

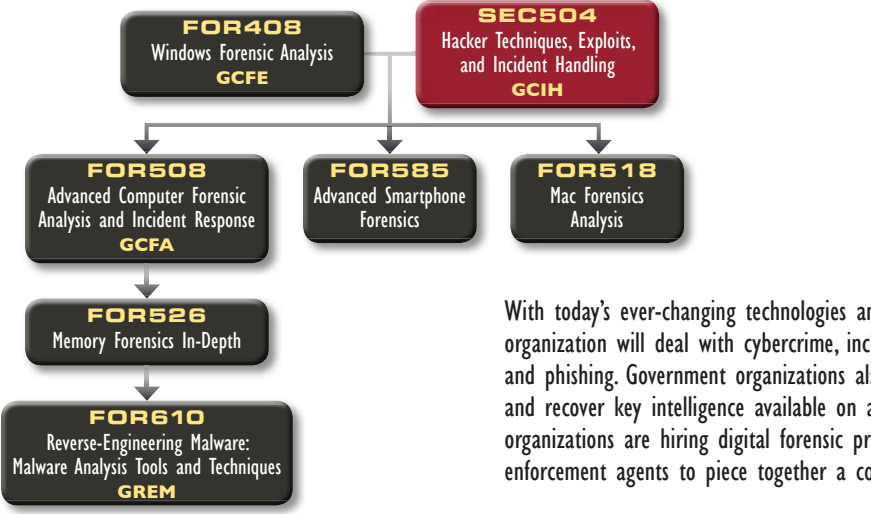
**CORE COURSES**  
SEC301 (GISF) ▶ SEC401 (GSEC) → SEC504  
Hacker Techniques, Exploits,  
and Incident Handling  
GCIH



## Digital Forensic Investigations and Media Exploitation

**SAMPLE JOB TITLES**

- Computer crime investigator
- Law enforcement
- Digital investigations analyst
- Media exploitation analyst
- Information technology litigation support and consultant
- Insider threat analyst



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. Government organizations also need the skills to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.



# SANS Brochure Challenge

SANS is introducing a new kind of challenge – one that unfolds from the pages of the brochure itself. This challenge will take you across many domains of knowledge, including (but not limited to!) the following:

**Infosec Fundamentals | Digital Forensics Knowledge | Steganography | Social Media | Mobile Devices | And much, much more!**

You'll enjoy all these and more from the comfort of your brochure and local computer, along with everyone's favorite global network, the Internet itself. You'll be able to advance all the way through this challenge from anywhere in the world.

### ***If this sounds a bit overwhelming, don't worry!***

If you need a smidgeon of help, we'll be releasing a series of hints in future brochures and on the SANS website to help you along. Make sure to get all your answers in by **October 27, 2014 to be eligible for prizes!**

So, how can you win and earn the undying respect of all your friends? There are three ways to win, though for each of them you'll need to finish the challenge. We'll award prizes to the first person to complete the challenge, the person with the best technical write-up, and one lucky person who wins a random draw from all entries.

**Assemble all the numbers found throughout this brochure to begin the challenge.**



### ***What will you win?***

The person with the best technical write-up will receive a signed copy of "Counter Hack Reloaded," as will the winner of the random drawing. And, the first person to finish the challenge will receive the **GRAND PRIZE** – a free four-month subscription to NetWars Continuous, valued at over \$2,000! You'll have plenty of opportunities to develop your skills, especially with our automated hint system to ensure a Stuck-Free™ experience!

### **Rules of Engagement:**

- ▶ No denial of service attacks
- ▶ No brute force attacks – though you won't gain access in this way, you could slow down the experience for other players
  - ▶ No attacks against the web server or its underlying operating system
  - ▶ No sharing of challenge links, hints, or write-ups before the contest deadline has passed

***Have fun with our first official brochure challenge!***

-The SANS Institute

Check out the following brochures for challenge hints:  
SANS Albuquerque  
SANS Baltimore  
SANS Seattle

**The Core NetWars Tournament and the DFIR NetWars Tournament will be held simultaneously at Network Security 2014!**

# NETWARS

## **Core NetWars Tournament**

### **Topics Include:**

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

## **DFIR NetWars Tournament**

### **Topics Include:**

- Host Forensics
- Malware Analysis
- Network Forensics
- Memory Analysis

**Both NetWars competitions will be played over two evenings: October 23-24, 2014**

*Prizes will be awarded at the conclusion of the games.*

**REGISTRATION IS FREE**

**for students attending any long course at NS 2014 (NON-STUDENTS ENTRANCE FEE IS \$1,249).**

**Registration is limited, so sign up soon!**

Register at [sans.org/event/network-security-2014/courses](http://sans.org/event/network-security-2014/courses)

# Courses-at-a-Glance

For an up-to-date course list please check the website at [sans.org/event/network-security-2014/schedule](http://sans.org/event/network-security-2014/schedule)

	SUN 10/19	MON 10/20	TUE 10/21	WED 10/22	THU 10/23	FRI 10/24	SAT 10/25	SUN 10/26	MON 10/27
SEC301 <b>Intro to Information Security</b>							<b>PAGE 4</b>		
SEC401 <b>Security Essentials Bootcamp Style</b> <i>SIMULCAST</i>							<b>PAGE 6</b>		
SEC440 <b>Critical Security Controls: Planning, Implementing and Auditing</b>								<b>PAGE 70</b>	
SEC501 <b>Advanced Security Essentials – Enterprise Defender</b> <i>SIMULCAST</i>							<b>PAGE 8</b>		
SEC502 <b>Perimeter Protection In-Depth</b> <i>SIMULCAST</i>							<b>PAGE 10</b>		
SEC503 <b>Intrusion Detection In-Depth</b> <i>SIMULCAST</i>							<b>PAGE 12</b>		
SEC504 <b>Hacker Techniques, Exploits, and Incident Handling</b>							<b>PAGE 14</b>		
SEC505 <b>Securing Windows with the Critical Security Controls</b>							<b>PAGE 16</b>		
SEC506 <b>Securing Linux/Unix</b>							<b>PAGE 18</b>		
SEC511 <b>Continuous Monitoring and Security Operations</b> <b>NEW!</b>							<b>PAGE 20</b>		
SEC542 <b>Web App Penetration Testing and Ethical Hacking</b>							<b>PAGE 22</b>		
SEC546 <b>IPv6 Essentials</b>								<b>PAGE 70</b>	
SEC560 <b>Network Penetration Testing and Ethical Hacking</b>							<b>PAGE 24</b>		
SEC561 <b>Intense Hands-on Pen Testing Skill Development</b>							<b>PAGE 26</b>		
SEC566 <b>Implementing and Auditing the Critical Security Controls – In-Depth</b>							<b>PAGE 28</b>		
SEC573 <b>Python for Penetration Testers</b>							<b>PAGE 30</b>		
SEC575 <b>Mobile Device Security and Ethical Hacking</b>							<b>PAGE 32</b>		
SEC579 <b>Virtualization and Private Cloud Security</b>							<b>PAGE 34</b>		
SEC580 <b>Metasploit Kung Fu for Enterprise Pen Testing</b>								<b>PAGE 70</b>	
SEC617 <b>Wireless Ethical Hacking, Penetration Testing, and Defenses</b>							<b>PAGE 36</b>		
SEC642 <b>Advanced Web App Penetration Testing and Ethical Hacking</b>							<b>PAGE 38</b>		
SEC660 <b>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</b>							<b>PAGE 40</b>		
SEC760 <b>Advanced Exploit Development for Penetration Testers</b> <b>NEW!</b>							<b>PAGE 42</b>		
FOR408 <b>Windows Forensic Analysis</b>							<b>PAGE 44</b>		
FOR508 <b>Advanced Computer Forensic Analysis and Incident Response</b>							<b>PAGE 46</b>		
FOR526 <b>Memory Forensics In-Depth</b> <b>NEW!</b>							<b>PAGE 48</b>		
FOR572 <b>Advanced Network Forensics and Analysis</b> <b>NEW!</b> <i>SIMULCAST</i>							<b>PAGE 50</b>		
FOR585 <b>Advanced Smartphone Forensics</b> <b>NEW!</b>							<b>PAGE 52</b>		
FOR610 <b>Reverse-Engineering Malware: Malware Analysis Tools and Techniques</b>							<b>PAGE 54</b>		
MGT305 <b>Technical Communication and Presentation Skills for Security Professionals</b>	<b>P 71</b>								
MGT414 <b>SANS® +S™ Training Program for the CISSP® Certification Exam</b>							<b>PAGE 56</b>		
MGT415 <b>A Practical Introduction to Risk Assessment</b>	<b>P 71</b>								
MGT433 <b>Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program</b> <i>SIMULCAST</i>								<b>PAGE 71</b>	
MGT512 <b>SANS Security Leadership Essentials for Managers with Knowledge Compression™</b> <i>SIMULCAST</i>							<b>PAGE 58</b>		
MGT514 <b>IT Security Strategic Planning, Policy, and Leadership</b>							<b>PAGE 60</b>		
MGT525 <b>IT Project Management, Effective Communication, and PMP® Exam Prep</b>							<b>PAGE 62</b>		
AUD507 <b>Auditing Networks, Perimeters, and Systems</b>							<b>PAGE 64</b>		
LEG523 <b>Law of Data Security and Investigations</b>							<b>PAGE 65</b>		
DEV522 <b>Defending Web Applications Security Essentials</b>							<b>PAGE 66</b>		
DEV541 <b>Secure Coding in Java/JEE: Developing Defensible Applications</b>							<b>PAGE 67</b>		
DEV544 <b>Secure Coding in .NET: Developing Defensible Applications</b>							<b>PAGE 67</b>		
ICS410 <b>ICS/SCADA Security Essentials</b> <b>NEW!</b>							<b>PAGE 68</b>		
HOSTED (ISC)® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program							<b>PAGE 69</b>		
HOSTED <b>Offensive Countermeasures: The Art of Active Defenses</b>								<b>PAGE 69</b>	
HOSTED <b>Physical Penetration Testing – Introduction</b>								<b>PAGE 69</b>	
HOSTED <b>Embedded Device Security Assessments for the Rest of Us</b>								<b>PAGE 69</b>	
<b>NetWars Tournaments (Core &amp; DFIR)</b>							<b>PAGE 2</b>		

## CONTENTS

Bonus Sessions . . . . .	72	Cyber Talent . . . . .	75	Hotel Information . . . . .	78
Vendor Events . . . . .	73	Securing the Human Program . . . . .	75	Come to Las Vegas . . . . .	79
Simulcast . . . . .	74	DoD Directive 8570 Information . . . . .	75	Registration Information . . . . .	80
SANS Technology Institute . . . . .	74	Future SANS Training Events . . . . .	76	Registration Fees . . . . .	81
		SANS Training Formats . . . . .	77		

# Intro to Information Security

Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 5:00pm

Laptop Required

30 CPE/CMU Credits

Instructors: Fred Kerby &

Keith Palmgren

▶ GIAC Cert: GISF

**COURSE NOW  
INCLUDES  
HANDS-ON LABS**

**SANS**



## 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

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!

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 technology, 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.

If you're a newcomer to the field of information security, this course will start you off with a solid foundation. SEC301 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.

**"I enjoyed the connection between real-life scenarios and training material."**

-Stephanie Westbrook,  
Offensive Logic-LLC

**"Fred is an excellent instructor who blends theory with practical examples."**

-Kwabby Gyasi IMF

**"SEC301 does an excellent job of giving you an idea of how well your security policy is written."**

-Terry Benes,  
University of Nebraska Foundation



**Fred Kerby** SANS Senior Instructor

Fred Kerby 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.



**Keith Palmgren** SANS Certified Instructor

Keith Palmgren is an IT Security professional with 26 years of experience in the field. He began his career with the U.S. Air Force working with cryptographic keys & codes management. He also worked in, what was at the time, the newly-formed computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a senior security architect working on engagements with the DoD and the National Security Agency. As security practice manager for both Sprint and Netigy, Keith built and ran the security consulting practice — responsible for all security consulting world-wide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. As a trainer, Keith has satisfied the needs of nearly 5,000 IT professionals and authored a total of 17 training courses. Keith currently holds the CISSP, GSEC, CEH, Security+, Network+, A+, and CTT+ certifications.



### 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), principle of least privilege, access control, and separation of risks. 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, Kerckhoffs's Principle); Security as a Process, Configuration Management, Backups, Auditing, Detection, and 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 of the various types of malware and associated delivery mechanisms. We conclude with a review of some typical attacks against the networking and computing infrastructure as well as discussing human-based attacks.

**Topics:** Terms (Encapsulation, Ports, Protocols, Addresses, Network Reference Models — Stacks); Addressing (Hardware, Network, Name Resolution); Transport Protocols (TCP, UDP); Other Protocols (ARP, ICMP); Routing Basics and The Default Gateway; Network Components (Switches, Routers, Firewalls); Network Attacks and Malware; Application and Human-Based Attacks

### 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 poor implementation of good tools). The day continues with an overview of Operational Security (OPSEC) as well as Safety and Physical Security. 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); Operations Security (OPSEC), Physical Security, Safety; Wireless Network Technology (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 HANDS ON: 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 just security. We discuss the six phases of incident handling as well as some techniques that organizations can use to develop meaningful metrics.

**Topics:** The Site Security Plan; Computer Security; Application Security; Incident Handling; Measuring Progress

### You Will Be Able To

- ▶ Discuss and understand risk as a product of vulnerability, threat, and impact to an organization
- ▶ Apply basic principles of information assurance (e.g., least privilege, separation of risk, defense in depth, etc.)
- ▶ Understand how networks work (link layer communications, addressing, basic routing, masquerading)
- ▶ Understand the predominant forms of malware and the various delivery mechanisms that can place organizations at risk
- ▶ Grasp 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



giac.org

# Security Essentials Bootcamp Style

## Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

Laptop Required

46 CPE/CMU Credits

Instructor: Bryce Galbraith

▶ GIAC Cert: GSEC

▶ Cyber Guardian

▶ Masters Program

▶ DoDD 8570

**“The flagship SANS course, SEC401, has an exceptional blend of security essential theory and hands-on experience.”**

-Ed Concepcion, USMC

**“SEC401 lets me go back and improve my organization’s security. It has given me tools, more insights, and an overall refreshment of my knowledge. Excellent trainer in every aspect!!!!”**

-Jerry Robels de Medina Godo

**“Coming right out of college with a computer science background, this fills in a lot of gaps in my security knowledge.”**

-Jack Mulrey, SWIFT

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 cybersecurity. Most importantly, your organization will be secure because its employees 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 cybersecurity. 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 cybersecurity, three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. What is 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.

## 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 specialists, penetration testers, and auditors who need a solid foundation of security principles to be as effective as possible at their jobs
- ▶ Anyone new to information security with some background in information systems and networking



## Bryce Galbraith SANS Principal Instructor

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

**401.1 HANDS ON: Networking Concepts**

A key way attackers gain access to an organization's resources is through a network connected to the Internet. An organization wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine hostile traffic. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials, and more, will be covered to provide a firm foundation for the days of training that follow.

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

**401.2 HANDS ON: Defense In-Depth**

In order to secure an enterprise network, you must have an understanding of the general principles of network security. On day two, you will learn about six key areas of network security.

**Topics:** Information Assurance Foundations; Computer Security Policies; Contingency and Continuity Planning; Business Impact Analysis; Password Management; Incident Handling; Offensive and Defensive Information Warfare

**401.3 HANDS ON: Internet Security Technologies**

Military agencies, banks and retailers offering electronic commerce programs, and as well as dozens of other types of organizations, are demanding to know what threats they are facing and what they can do to address those threats. On this day, you will be provided with a roadmap to help you understand the paths available to organizations that are considering or planning to deploy various security devices and tools such as intrusion detection systems and firewalls.

**Topics:** Host-Based Intrusion Detection and Prevention; Network-Based Intrusion Detection and Prevention; Honey pots; Methods of Attacks; Firewalls and Perimeters; Risk Assessment and Auditing

**401.4 HANDS ON: Secure Communications**

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few organizations use it. This technology is encryption. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day four looks at various aspects of encryption and how it can be used to secure a company's assets.

**Topics:** Cryptography; Steganography; PGP; Wireless; Operations Security

**401.5 HANDS ON: Windows Security**

Windows is the most widely-used and hacked operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. Day five will help you quickly master the world of Windows security while showing you the tools you can use to simplify and automate your work.

**Topics:** The Security Infrastructure; Permissions and User Rights; Security Policies and Templates; Service Packs, Patches, and Backups; Securing Network Services; Auditing and Automation

**401.6 HANDS ON: Linux Security**

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

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

**You Will Be Able To**

- ▶ Design and build a network architecture using VLANs, NAC and 802.1x based on APT indicator of compromise
- ▶ Run Windows command line tools to analyze the system looking for high-risk items
- ▶ Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- ▶ Install VMWare and create virtual machines to operate a virtual lab to test and evaluate tools/security of systems
- ▶ Create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness
- ▶ Identify visible weaknesses of a system utilizing various tools to include dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure
- ▶ Determine overall scores for systems utilizing CIS Scoring Tools and create a system baseline across the organization
- ▶ Build a network visibility map that can be used for hardening of a network – validating the attack surface and covering ways to reduce it through hardening and patching
- ▶ Sniff open protocols like telnet and ftp and determine the content, passwords and vulnerabilities utilizing WireShark



**ATTEND REMOTELY**

**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.  
*More info on page 74.*

# Advanced Security Essentials – Enterprise Defender

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Paul A. Henry

▶ GIAC Cert: GCED

▶ Masters Program

▶ DoDD 8570



## Who Should Attend

- ▶ Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- ▶ Students who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want 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 increase in importance as attacks become stealthier; have a greater financial impact on 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 efforts to prevent attacks and protect 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 prevention and detection measures, completing the security lifecycle.

**“SEC501 is helping me expand my security knowledge by putting the history and the information in an explanation of real-world technologies.”**

-Gerald Servidio, General Electric

**ATTEND  
REMOTELY**



**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.

**More info on page 74.**



## 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.

### 501.1 HANDS ON: Defensive Network Infrastructure

Protecting a network from attack starts with designing, building, and implementing a robust network infrastructure. Many aspects of implementing a defense-in-depth network are often overlooked because organizations 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: Penetration Test

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 penetration 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 as well as the 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

Cybersecurity 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 compromises networks 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 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 deploy data loss prevention solutions at both a host and network level



giac.org



sans.edu



DoDD 8570 Required  
sans.org/8570

# Perimeter Protection In-Depth

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Tanya Baccam  
 ▶ GIAC Cert: GPPA  
 ▶ Cyber Guardian  
 ▶ Masters Program

**“Great instructor.  
 So valuable to have  
 real experts who  
 work in the field teaching  
 the material.  
 Very appreciative.  
 Thank you!”**  
 -Jennifer Kurzawa, Lockheed Martin

**“Excellent material and  
 course as always! That’s  
 why I keep coming back!”**  
 -Bo Jonsson, Borenis AB

**ATTEND  
 REMOTELY**



**SIMULCAST**

If you are unable to attend  
 this event, this course is also  
 available in SANS Simulcast.

**More info on page 74.**



## 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.

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

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

We spend quite a bit of time learning about IP. Sure we all know how to assign an IP address, but to secure your network you really need to understand the idiosyncrasies of the protocol. We’ll talk about how IP works and how to spot the abnormal patterns. If you can’t hear yourself saying “Hmmm, there are no TCP options in that packet, it’s probably forged,” then you’ll gain some real insight from this portion of the material.

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

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

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

Most significantly, the course material has been developed using the following guiding principles:

- **Learn the process, not one specific product.**
- **You learn more by doing, so hands-on problem-solving is key.**
- **Always peel back the layers and identify the root cause.**

While technical knowledge is important, what really matters are the skills to properly leverage it. This is why the course is heavily focused on problem-solving and root-cause analysis. While these are usually considered soft skills, they are vital to being effective in the role of security architect. So along with the technical training, you’ll receive risk management capabilities and even a bit of Zen empowerment.

## Who Should Attend

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

### 502.1 HANDS ON: TCP/IP for Firewalls

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

**Topics:** Threat Vectors; OSI Layer 2; OSI Layer 3; OSI Layers 4 and 5; Packet Decoding; Labs

### 502.2 HANDS ON: Firewalls, NIDS, and NIPS

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

**Topics:** IPv6; Static Filters; Stateful Filters; Stateful Inspection; Network Address Translation; Network-based Intrusion Detection and Prevention; Proxies, Border Routers; Cisco IOS; Wireshark; Labs

### 502.3 HANDS ON: Wire Products and Assessment

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

**Topics:** Perimeter Deployment Options; Snort: A Real-life Example; Building a Firewall Rulebase; Web Application and Database Firewalls; Firewall Assessment; Firewall Log Analysis; Labs

### 502.4 HANDS ON: Host-Level Security

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

**Topics:** Securing an Operating System; Securing Exposed Services; Web Application Security; Host-based Intrusion Detection and Prevention; Vulnerability Assessment; Baseline Audits; Forensics; Security Information Management; Labs

### 502.5 HANDS ON: Securing the Wire

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

**Topics:** Encryption; Authentication; VPN Options; VPN Architecture; Wireless; Network Access Control; Labs

### 502.6 HANDS ON: Perimeter Wrap-Up

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

**Topics:** Sizing Up a Network; Cool Tools; Cloud Security Considerations

## You Will Be Able To

- ▶ Apply perimeter security solutions in order to identify and minimize weaknesses to properly protect your perimeter
- ▶ Deploy and utilize multiple firewalls to understand the strengths and weaknesses that each present
- ▶ Use built-in tools to audit, protect and identify if systems have been compromised
- ▶ Utilize tcpdump to analyze network traffic in detail to understand what packets are communicating and how to identify potential covert channels
- ▶ Understand and utilize techniques to compromise and protect against application layer attacks such as XSS, CSRF, SQL injection and more
- ▶ Utilize tools to evaluate packets and identify legitimate and illegitimate traffic
- ▶ Use tools to evaluate and identify the risks related to Cloud Computing
- ▶ Inspect the intricate complexities of IP, including identifying malicious packets
- ▶ Evaluate and secure SSL, wireless networks, VPNs, applications and more
- ▶ Implement a logging solution that properly identifies risk and is manageable



giac.org



sans.org/  
cyber-guardian



sans.edu

# Intrusion Detection In-Depth

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Mike Poor  
 ▶ GIAC Cert: GCIA  
 ▶ Cyber Guardian  
 ▶ Masters Program  
 ▶ DoDD 8570

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 compromise at a high-profile company. 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 create an environment 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 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.

Industry expert and instructor Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. Packetrix is supplemented with demonstration "pcaps" – files that contain network traffic. This allows students to follow along on their laptops with the class material and demonstrations. Additionally, these pcaps provide a good library of network traffic to use when reviewing the material, especially for certification.

There are several hands-on exercises each day to reinforce the course book material, allowing you to transfer the knowledge in your head to execution at your keyboard.

Exercises have two different approaches. The first is 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 more challenging experience for a student who may already know the material or who has quickly mastered new material. Additionally, there is an "extra credit" stumper question for exercises 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 overflowing with course book material that didn't quite get absorbed into your brain during this intense week of learning. This will enable you to hit the ground running once returning to a live environment.

The challenging hands-on exercises are specially designed to be valuable for all experience levels. The Packetrix VMware used in class is a Linux distribution so we strongly recommend that you spend some time getting familiar with a Linux environment that uses the command line for entry, along with learning some of the core Unix commands, before coming to class.

## Who Should Attend

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

**"SEC503 is a great eye-opener, and I'm excited to bring the knowledge I learned back to my organization."**

-John Neff, Sotera Defense Solutions

**"I can get the content anywhere, but Mike's ability to deliver the material is why I would recommend SEC503. He kept things interesting."**

-Chris Kachigan, Lockheed Martin

**"Mike does an excellent job balancing dry technical info with enough personal anecdotes to keep it lively."**

-Benjamin Jones, U.S. Navy



### Mike Poor SANS Senior Instructor

Mike Poor is a founder and senior security analyst for the Washington, 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 on 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. @Mike\_Poor



**503.1 HANDS ON: Fundamentals of Traffic Analysis: PART 1**

Day 1 provides a refresher or introduction to TCP/IP, depending on your background, 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; and 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: Layer 2; IP Layer: Layer 3, IPv4, and IPv6

**503.2 HANDS ON: Fundamentals of Traffic Analysis: PART 2**

Day 2 continues where Day 1 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; Writing tcpdump 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: Open-Source IDS: Snort and Bro**

We take a unique approach of teaching both open-source IDS solutions by presenting them in their operational life-cycle phases from planning to updating. This will offer you a broader view of what is entailed for the production operation of each of these open-source tools. This is more than just a step-by-step discussion of install, configure, and run the tools. This approach provides a recipe for a successful deliberate deployment, not just a haphazard “download and install the code and hope for the best.”

**Topics:** Operational Lifecycle of Open-Source IDS; Introduction; Snort; Bro; Comparing Snort and Bro to Analyze Same Traffic

**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 exercise that challenges you to 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 because 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



**ATTEND REMOTELY**

**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.

*More info on page 74.*

# Hacker Techniques, Exploits, and Incident Handling

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

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

**“John Strand is clear, energetic, and has a great depth of knowledge.”**

-Jason MacDonald, DOD Canada

**“Excellent training, excellent presentation, and applicable direct lab examples.”**

-Rodney Lindemann, I43 IOS

**“This is day 4 and our SANS instructor, John Strand, is bringing the same level of high energy and enthusiasm to every topic as he did on day one. Great course!”**

-Christopher Wilson, USAF

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



### John Strand SANS Senior Instructor

Along with SEC504, John Strand 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.

@strandjs

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

This session describes a detailed incident-handling process and applies that process to several in-the-trenches case studies. Additionally, an optional "Intro to Linux" mini-workshop held on the evening of this session will provide 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



giac.org



sans.org/  
cyber-guardian



sans.edu



DoDD 8570 Required  
sans.org/8570

### You Will Be Able To

- ▶ Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- ▶ Analyze the structure of common attack techniques in order to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- ▶ Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- ▶ Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- ▶ Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- ▶ Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- ▶ Gain access to a target machine using Metasploit, and then detect the artifacts and impacts of exploitation through process, file, memory, and log analysis
- ▶ Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- ▶ Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- ▶ Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
- ▶ Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choose appropriate response actions based on each attacker's flood technique
- ▶ Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

# Securing Windows with the Critical Security Controls

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Jason Fossen

▶ GIAC Cert: GCWN

▶ Cyber Guardian

▶ Masters Program

**“SEC505 should be required for anyone administering windows domains.”**

-Tom Gonzales,

Credit Union of Colorado

**“Jason’s way of explaining objects in Powershell is both unique and was easy to understand. The best explanation I’ve heard since Powershell came out.”**

-Mark Lucas, Caltech

**“This was by far the best class I’ve ever taken for Windows!”**

-Rob Trujillo, U.S. Courts

How can we deal with pass-the-hash attacks, token abuse, administrator account compromise, and the lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that lead to malware infections? These are tough problems, but we tackle them in SEC505.

While forensics and incident response are great for detection and remediation, the goal of this course is to prevent those infections in the first place (after all, first things first). Hacking tools are fun, but having a bunch of hacking tools doesn't help in securing a large Active Directory network against their use. We need different tools to implement security, and these tools have to scale without spending a fortune. Examples of workable tools are Group Policy and PowerShell.

Learning PowerShell is probably the single best new skill for the careers of Windows administrators, especially with the trend towards cloud computing. Because most of your competition lacks scripting skills, it's a great way to make your résumé stand out. This course devotes an entire day to PowerShell, but you don't need any prior scripting experience, we'll start with the basics.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to help prove your security skills and Windows security expertise. The GCWN certification counts towards getting a Master's Degree in information security from the SANS Technology Institute ([sans.edu](http://sans.edu)) and also satisfies the Department of Defense 8570 computing environment (CE) requirement

This is a fun course and a real eye-opener even for Windows administrators with years of experience.



## Who Should Attend

- ▶ Windows security engineers and system administrators
- ▶ Anyone who wants to learn PowerShell
- ▶ Anyone who wants to implement the 20 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
- ▶ Anyone who needs to prevent malware infections
- ▶ Anyone implementing the Australian Directorate's Four Controls



### 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.

**505.1 HANDS ON: Windows Operating System and Applications Hardening**

We start by choosing malware-resistant software and Windows operating systems, then we regularly update that software, limit what software users can run, and then configure that software so that its exploitable features are disabled or at least restricted to work-only purposes. Nothing is guaranteed, of course, but what if you could reduce your malware infection rate by more than half? What if your next penetration test wasn't an exercise in embarrassment? The trick is hardening Windows in a way that is cost-effective, scalable, and with minimal user impact.

**Topics:** Going Beyond Just Anti-Virus Scanning; OS Hardening with Security Templates; Hardening with Group Policy; Enforcing Critical Controls for Applications

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

Today's course continues the theme of resisting malware and APT adversaries, but with a special focus on securing the keys to the kingdom: Administrative Power. If a member of the Domain Admins group is compromised, the entire network is lost. How can we better prevent the compromise of administrative accounts and contain the harm when they do get compromised? What can we do about pass-the-hash and token abuse attacks? Remember, as a network administrator, you are a high-value target and your adversaries will try to take over your user account and infect the computers you use at work (and at home).

**Topics:** Compromise of Administrative Powers; Active Directory Permissions and Delegation; Updating Vulnerable Software

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

Public Key Infrastructure (PKI) is not an optional security service anymore. Windows Server includes a complete built-in PKI for managing certificates and making their use transparent to users. You can be your own private Certification Authority and generate as many certificates as you want at no extra charge. It's all centrally managed through Group Policy. Digital certificates play an essential role in Windows security: IPSec, BitLocker, S/MIME, SSL/TLS, smart cards, script signing, etc. They all use digital certificates. Everything needed to roll out a smart card solution, for example, is included with Windows except for the cards and readers themselves, and generic cards are available in bulk for cheap. You might already have a smart card built into your motherboard as a TPM chip.

**Topics:** Why Have a PKI?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards, BitLocker Drive Encryption and 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 look at 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:** Why IPSec?; Creating IPSec Policies; Windows Firewall; Securing Wireless Networks; RADIUS for Wireless and Ethernet

**505.5 HANDS ON: Server Hardening and Dynamic Access Control**

What are the best practices for hardening servers, especially servers exposed to the Internet? How can we remotely manage our servers in a secure way, especially our virtualized servers hosted by third-party cloud providers? If I have Internet-exposed servers, how can I more safely make them Active Directory domain members? If I have service accounts or scheduled jobs running as Domain Admin, what are the risks and what can I do about it? Today's course is all about server hardening.

**Topics:** Dangerous Server Protocols; Server Hardening; Internet-Exposed Member Servers; Dynamic Access Control (DAC)

**505.6 HANDS ON: Windows PowerShell Scripting**

PowerShell is Microsoft's object-oriented command shell and scripting language. Unlike in the past, virtually everything can be managed from the command line and scripts now. Server 2012-R2, for example, has over 3,000 PowerShell tools for nearly everything, including Active Directory, IIS, Exchange, SharePoint, System Center, AppLocker, Hyper-V, firewall rules, event logs, remote command execution, and much more.

**Topics:** Overview and Security of Powershell; Getting Around Inside PowerShell; Example Commands; Write Your Own Scripts; Windows Management Instrumentation (WMI)

**You Will Be Able To**

- ▶ Harden the configuration settings of Internet Explorer, Google Chrome, Adobe Reader, Java, and Microsoft Office applications to better withstand client-side exploits
- ▶ Use Group Policy to harden the Windows operating system by configuring DEP, ASLR, SEHOP, EMET and AppLocker whitelisting by applying security templates and running custom PowerShell scripts
- ▶ Deploy a WSUS patch server with third-party enhancements to overcome its limitations
- ▶ Implement Server 2012 Dynamic Access Control permissions, file tagging and auditing for Data Loss Prevention (DLP)
- ▶ Use Active Directory permissions and Group Policy to safely delegate administrative authority in a large enterprise to better cope with token abuse, pass-the-hash, service/task account hijacking, and other advanced attacks
- ▶ Install and manage a full Windows PKI, including smart cards, Group Policy auto-enrollment, and detection of spoofed root CA certificates
- ▶ Configure BitLocker drive encryption with a TPM chip using graphical and PowerShell tools
- ▶ Harden SSL, RDP, DNSSEC and other dangerous protocols using Windows Firewall and IPSec rules managed through Group Policy and PowerShell scripts
- ▶ Install the Windows RADIUS server (NPS) for PEAP-TLS authentication of 802.11 wireless clients and hands-free client configuration through Group Policy
- ▶ Learn how to automate security tasks on local and remote systems with the PowerShell scripting language and remoting framework



giac.org



sans.org/  
cyber-guardian



sans.edu

# Securing Linux/Unix

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Hal Pomeranz

▶ GIAC Cert: GCUX

▶ Cyber Guardian

▶ Masters Program

**“This course goes beyond securing Linux/Unix. It explains the reasons why as well as how the attacker is able to penetrate the system. I recommend this for anyone who is involved in administering these systems.”**

-Jeremy Kilgore, BancFirst

**“I’ve been a Unix systems administrator for a couple of decades, but in SEC506, I learned something new every day.”**

-Sheryl Coppenger, NCI Inc.

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

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

## Topics

- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Unix Logging and Kernel-Level Auditing
- Building a Centralized Logging Infrastructure
- Network Security Tools
- SSH for Secure Administration
- Server Lockdown for Linux and Unix
- Controlling Root Access with sudo
- SELinux and chroot() for Application Security
- DNSSEC Deployment and Automation
- mod\_security and Web Application Firewalls
- Secure Configuration of BIND, Sendmail, Apache
- Forensic Investigation



### Hal Pomeranz SANS Faculty Fellow

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the U.S. and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is the creator of the SANS Linux/Unix Security course (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.

## Who Should Attend

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

**506.1 HANDS ON: Hardening Linux/Unix Systems – PART 1**

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

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

**506.2 HANDS ON: Hardening Linux/Unix Systems – PART 2**

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

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

**506.3 HANDS ON: Hardening Linux/Unix Systems – PART 3**

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

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

**506.4 HANDS ON: Application Security – PART 1**

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

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

**506.5 HANDS ON: Application Security – PART 2**

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

**Topics:** BIND; DNSSEC; Sendmail; Apache; Web Application Firewalls with mod\_security

**506.6 HANDS ON: Digital Forensics for Linux/Unix**

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

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

**You Will Be Able To**

- ▶ Significantly reduce the number of vulnerabilities in the average Linux/Unix system by disabling unnecessary services
- ▶ Protect your systems from buffer overflows, denial-of-service, and physical access attacks by leveraging OS configuration settings
- ▶ Configure IP Tables and ipfilter host-based firewalls to block attacks from outside
- ▶ Deploy SSH to protect administrative sessions, and leverage SSH functionality to securely automate routine administrative tasks
- ▶ Use sudo to control and monitor administrative access
- ▶ Create a centralized logging infrastructure with Syslog-NG, and deploy log monitoring tools to scan for significant events
- ▶ Use SELinux to effectively isolate compromised applications from harming other system services
- ▶ Securely configure common Internet-facing applications such as Apache, BIND, and Sendmail
- ▶ Investigate compromised Unix/Linux systems with the Sleuthkit, lsof, and other open-source tools
- ▶ Understand attacker rootkits and how to detect them with AIDE and rkhunter/chkrootkit



giac.org



sans.org/  
cyber-guardian



sans.edu

# Continuous Monitoring and Security Operations

NEW

SANS

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Eric Conrad

We continue to underestimate the tenacity of our adversaries! Organizations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM), and Continuous Security Monitoring (CSM) taught in this course will best position your organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and day five of this course will greatly increase your understanding and enhance your skills in implementing CM utilizing the NIST framework.

SANS is uniquely qualified to offer this course. Course authors Eric Conrad (GSE #13) and Seth Misenar (GSE #28) hold the distinguished GIAC Security Expert Certification (GSE). Both are experienced, real-world, practitioners who apply the concepts and techniques they teach in this course on a daily basis. SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. The course authors have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

## Who Should Attend

- ▶ Security architects
- ▶ Senior security engineers
- ▶ Technical security managers
- ▶ SOC analysts
- ▶ SOC engineers
- ▶ SOC managers
- ▶ CND analysts
- ▶ Individuals working to implement Continuous Diagnostics and Mitigation (CDM), Continuous Security Monitoring (CSM), or Network Security Monitoring (NSM)



### Eric Conrad SANS Principal 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, GCFE, GAWN, and GSEC certifications. Eric also blogs about information security at [ericconrad.com](http://ericconrad.com).



**511.1 HANDS ON: Current State Assessment, SOC, and Security Architecture**

The prevention-dominant security model has failed. Given the frequency and extent of significant intrusions, this should not come as a surprise. In order to address the root of the problem, we must understand the current architecture and the design gaps that facilitate the adversary's dominance. What do we need to address to begin to make things better? Can we ever hope to win? What would winning look like? These are important questions that we must answer if we hope to substantially improve our security posture.

**Topics:** Current State Assessment, Security Operations Centers (SOCs), and Security Architecture; Modern Security Architecture Principles; Frameworks and Enterprise Security Architecture; Security Architecture – Key Techniques/Practices; Security Architecture Design Tools/Strategies; SOC

**511.2 HANDS ON: SOC and Defensible Network Security Architecture**

Understanding the problems with the current environment and realizing where we need to get to is far from sufficient: we need a detailed roadmap to bridge the gap between the current and desired state. Day 2 introduces and details the components of our infrastructure that become part of a defensible network security architecture and SOC. We are long past the days where a perimeter firewall and ubiquitous antivirus were sufficient security. There are many pieces and moving parts that comprise a modern defensible security architecture.

**Topics:** SOC/Security Architecture – Key Infrastructure Devices; Segmented Internal Networks; Defensible Network Security Architecture Principles Applied

**511.3 HANDS ON: SOC and Defensible Endpoint Security Architecture**

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Day 3 details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

**Topics:** Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching; Current Architectural Challenges

**511.4 HANDS ON: Continuous Monitoring**

Designing a SOC or security architecture that enhances visibility and detective capabilities represents a paradigm shift for most organizations. However, the design is simply the beginning. The most important element of a modern security architecture is the emphasis on detection. The architecture presented in days 1-3 emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise.

**Topics:** Continuous Monitoring and the 20 Critical Security Controls; Continuous Monitoring Overview; Network Security Monitoring (NSM); Network Security Monitoring and Design

**511.5 HANDS ON: Continuous Security Monitoring**

Network Security Monitoring (NSM) is the beginning; we need to not only detect active intrusions and unauthorized actions, but also know when our systems, networks, and applications are at an increased likelihood for compromise. A strong way to achieve this is through Continuous Security Monitoring (CSM) or Continuous Diagnostics and Mitigation (CDM). Rather than waiting for the results of a quarterly scan or an annual penetration test to determine what needs to be addressed, continuous monitoring insists on proactively and repeatedly assessing and reassessing the current security posture for potential weaknesses that need be addressed.

**Topics:** Scripting and Automation; Continuous Security Monitoring; Putting It All Together

**511.6 HANDS ON: Capstone Design/Detect/Defend**

The course culminates in a team-based capstone project that is a full day of hands-on work applying the principles taught throughout the week.

**Topics:** Security Architecture; Assess Provided Architecture; \$0 CAPEX Security Architecture; \$\$\$\$ CAPEX Security Architecture; Continuous Security Monitoring; Using Tools/Scripts Assess the Initial State; Quickly/Thoroughly Find All Changes Made

**You Will Be Able To**

- ▶ Analyze a security architecture for deficiencies
- ▶ Apply the principles learned in the course to design a defensible security architecture
- ▶ Understand the importance of a detection-dominant security architecture and security operations centers (SOC)
- ▶ Identify the key components of Network Security Monitoring (NSM)/ Continuous Diagnostics and Mitigation (CDM)/ Continuous Monitoring (CM)
- ▶ Determine appropriate security monitoring needs for organizations of all sizes
- ▶ Implement a robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- ▶ Determine requisite monitoring capabilities for a SOC environment
- ▶ Determine capabilities required to support continuous monitoring of key Critical Security Controls
- ▶ Utilize tools to support implementation of Continuous Monitoring (CM) per NIST guidelines SP 800-137



# Web App Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Seth Misenaar

- ▶ GIAC Cert: GWAPT
- ▶ Cyber Guardian
- ▶ Masters Program

## 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 developers
- ▶ Website designers and architects

**“Seth is an amazing instructor. He clearly has a passion for security, evident by his crazy amount of knowledge. His real-world examples relate well to the course content and make it easier to understand.”**

-Lee Slaughter, F5 Networks

**“The SEC542 tools and course presentation are top-notch. I'll be using this material extensively.”**

-Jeremy Pierson, Academy Mortgage



### Seth Misenaar SANS Principal Instructor

Seth Misenaar is a lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security through 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, GCFE, and MCSE. @sethmisenaar



### 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 using 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.

### You Will Be Able To

- ▶ Apply a detailed, four-step methodology to your web application penetration tests, including Recon, Mapping, Discovery and Exploitation
- ▶ Analyze the results from automated web testing tools to remove false positives and validate findings
- ▶ Use python to create testing and exploitation scripts during a penetration test
- ▶ Create configurations and test payloads within other web attacks
- ▶ Use FuzzDB to generate attack traffic to find flaws such as Command Injection and File Include issues
- ▶ Assess the logic and transaction flow within a target application to find logic flaws and business vulnerabilities
- ▶ Use the rerelease of Durzosploit to obfuscate XSS payloads to bypass WAFs and application filtering
- ▶ Analyze traffic between the client and the server application using tools such as Ratproxy and Zed Attack Proxy to find security issues within the client-side application code
- ▶ Use BeEF to hook victim browsers, attack the client software and network and evaluate the potential impact XSS flaws have within an application
- ▶ Perform a complete web penetration test during the Capture the Flag exercise to pull all of the techniques and tools together into a comprehensive test



giac.org



sans.org/  
cyber-guardian



sans.edu

# Network Penetration Testing and Ethical Hacking

## Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 6:30pm (Day 1)

9:00am - 5:00pm (Days 2-6)

37 CPE/CMU Credits

Laptop Required

Instructor: Ed Skoudis

- ▶ GIAC Cert: GPEN
- ▶ Cyber Guardian
- ▶ Masters Program

**“Ed Skoudis successfully combines expertise, real-world experiences, and even humor to deliver an incredibly effective learning experience...Thank you!”**

-George Huang,

Nationwide Insurance

**“This type of training is fantastic, all new penetration testers and personnel who interact with testers or set up assessments should take this SEC560.”**

-Christopher Duffy,

Knowledge Consulting Group



## Ed Skoudis SANS Faculty Fellow

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular InfoSec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions that help train cyber warriors how to defend the kinetic assets of a physical, miniaturized city. Ed's expertise includes hacker attacks and defenses, incident response, and malware analysis, with over 15 years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over 3,000 information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. @edskoudis

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SANS SEC560, our flagship course for penetration testing, fully arms you to address this duty head-on.

## The Must-Have Course for Every Well-Rounded Security Professional

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled InfoSec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job masterfully, safely, and efficiently.

## Learn the Best Ways to Test Your Own Systems Before the Bad Guys Attack

The whole course is designed to get you ready to conduct a full-scale, high-value penetration test, and on the last day of the course, you'll do just that. After building your skills in awesome labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

## Equipping Security Organizations with Comprehensive Penetration Testing and Ethical Hacking Know-How

You will learn how to perform detailed reconnaissance, learning about a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You'll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. We won't just cover run-of-the-mill options and configurations, we'll also go over less-well-known-but-super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post exploitation, password attacks, wireless, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth. The final portion of the class includes a comprehensive hands-on lab, conducting a full-day penetration test against a target organization.

## Who Should Attend

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

## Course Day Descriptions

### 560.1 HANDS ON: Comprehensive Pen Test Planning, Scoping, and Recon

In this section of the course, you'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you'll need for conducting great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, with a role-playing exercise where you'll build an effective scope and rules of engagement. We also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on document metadata analysis to pull sensitive information about a target environment.

**Topics:** The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Effective Reporting; Detailed Recon Using the Latest Tools; Mining Search Engine Results; Document Metadata Extraction and Analysis

### 560.2 HANDS ON: In-Depth Scanning

We next focus on the vital task of mapping the attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We'll look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We'll also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the day covering vital techniques for false-positive reduction so you can focus your findings on meaningful results and avoid the sting of a false positive, as well as how to conduct your scans safely and efficiently.

**Topics:** Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth; the Nmap Scripting Engine; Version Scanning with Nmap and Anmap; Vulnerability Scanning with Nessus and Retina; False Positive Reduction; Packet Manipulation with Scapy; Enumerating Users; Netcat for the Pen Tester; Monitoring Services During a Scan

### 560.3 HANDS ON: Exploitation and Post-Exploitation

In this section, we look at the many kinds of exploits that penetration testers use to compromise target machines, including client-side exploits, service-side exploits, and local privilege escalation. We'll see how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You'll learn in-depth how to leverage Metasploit and the Meterpreter to compromise target environments, search them for information to advance the penetration test, and pivot to other systems, all with a focus on determining the true business risk of the target organization. We'll also look at post-exploitation analysis of machines and pivoting to find new targets, finishing the section with a lively discussion of how to leverage the Windows shell to dominate target environments.

**Topics:** Comprehensive Metasploit Coverage with Exploits/Stagers/Stages; In-Depth Meterpreter Hands-On Labs; Implementing Port Forwarding Relays for Merciless Pivots; Bypassing the Shell vs. Terminal Dilemma; Installing VNC/RDP/SSH with Only Shell Access; Windows Command Line Kung Fu for Penetration Testers

### 560.4 HANDS ON: Password Attacks & Merciless Pivoting

This component of the course turns our attention to password attacks, analyzing password guessing, password cracking, and pass-the-hash techniques in depth. We'll go over numerous tips based on real-world experience to help penetration testers and ethical hackers maximize the effectiveness of their password attacks. You'll patch and custom-compile John the Ripper to optimize its performance in cracking passwords. You'll look at the amazingly full-featured Cain tool, running it to crack sniffed Windows authentication messages. You'll also perform multiple types of pivots to move laterally through our target lab environment, and pluck hashes and cleartext passwords from memory using the Mimikatz tool. We'll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And, we'll finish the day with an exciting discussion of powerful "pass-the-hash" attacks, leveraging Metasploit, the Meterpreter, and SAMBA client software.

**Topics:** Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Massive Pivoting Through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz; Password Cracking with John the Ripper & Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More

### 560.5 HANDS ON: Wireless and Web Apps Penetration Testing

This in-depth section of the course is focused on helping you become a well-rounded penetration tester. Augmenting your network penetration testing abilities, we turn our attention to methods for finding and exploiting wireless weaknesses, including identifying misconfigured access points, cracking weak wireless protocols, and exploiting wireless clients. We then turn our attention to web application pen testing, with detailed hands-on exercises that involve finding and exploiting cross-site scripting (XSS), cross-site request forgery (XSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

**Topics:** Wireless Attacks; Discovering Access; Attacking Wireless Crypto Flaws; Client-Side Wireless Attacks; Finding and Exploiting Cross-Site Scripting; Cross-Site Request Forgery; SQL Injection; Leveraging SQL Injection to Perform Command Injection; Maximizing Effectiveness of Command Injection Testing

### 560.6 HANDS ON: Penetration Testing Workshop and Capture the Flag Event

This lively session represents the culmination of the network penetration testing and ethical hacking course, where you'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop. You'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work with a team to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) is at risk. And, as a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

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

## You Will Be Able To

- ▶ Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- ▶ Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- ▶ Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- ▶ Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- ▶ Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization
- ▶ Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- ▶ Utilize the Windows and Linux command to plunder target systems for vital information that can further the overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- ▶ Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- ▶ Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- ▶ Utilize wireless attack tools for Wifi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a project's scope
- ▶ Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection



giac.org



sans.org/  
cyber-guardian



sans.edu

# Intense Hands-on Pen Testing Skill Development

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Tim Medin

## Topics addressed in the course include:

- ▶ Applying network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- ▶ Manipulating common network protocols to reconfigure internal network traffic patterns, as well as defenses against such attacks
- ▶ Analyzing Windows and Linux systems for weaknesses using the latest enterprise management capabilities of the operating systems, including the super powerful Windows Remote Management (WinRM) tools
- ▶ Applying cutting-edge password analysis tools to identify weak authentication controls leading to unauthorized server access
- ▶ Scouring through web applications and mobile systems to identify and exploit devastating developer flaws
- ▶ Evading Anti-Virus tools and bypassing Windows UAC to understand and defend against these advanced techniques
- ▶ Honing phishing skills to evaluate the effectiveness of employee awareness initiatives and your organization's exposure to one of the most damaging attack vectors widely used today



### Tim Medin SANS Certified Instructor

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security, where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog ([pen-testing.sans.org/blog](http://pen-testing.sans.org/blog)) and the Command Line Kung Fu Blog ([blog.commandlinekungfu.com](http://blog.commandlinekungfu.com)). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. @timmedin

To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS' top instructors engineered **SEC561: Intense Hands-on Pen Testing Skill Development** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises and labs, maximizing keyboard time during in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to address today's pen test and vulnerability assessment projects in enterprise environments.

*To get the most out of this course, students should have at least some prior hands-on vulnerability assessment or penetration testing experience (at least six months) or have taken at least one other penetration testing course (such as SANS SEC504, SEC560, or SEC542). The course will build on that background, helping participants ramp up their skills even further across a broad range of penetration testing disciplines.*

Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios, using skills that they can apply the day they get back to their jobs.

A lot of people can talk about these concepts, but this course teaches you how to actually apply them hands-on and in-depth. SEC561 shows security personnel, including penetration testers, vulnerability assessment personnel, auditors, and operations personnel, how to leverage in-depth techniques to get powerful results in every one of their projects. The course is overflowing with practical lessons and innovative tips, all with direct hands-on application. Throughout the course, students interact with custom-developed scenarios built just for this course on the innovative NetWars challenge infrastructure, which guides them through the numerous hands-on labs providing questions, hints, and lessons learned as they build their skills.



## Who Should Attend

- ▶ Security professionals who want to expand their hands-on technical skills in new analysis areas such as packet analysis, digital forensics, vulnerability assessment, system hardening, and penetration testing
- ▶ Systems and network administrators who want to gain hands-on experience in information security skills to become better administrators
- ▶ Incident response analysts who want to better understand system attack and defense techniques
- ▶ Forensic analysts who need to improve their analysis through experience with real-world attacks
- ▶ Penetration testers seeking to gain practical hands-on experience for use in their own assessments

### 561.1 HANDS ON: Security Platform Analysis

The first day of the course prepares students for real-world security challenges by giving them hands-on practice with essential Linux and Windows server and host management tools. First, students will leverage built-in and custom Linux tools to evaluate the security of host systems and servers, inspecting and extracting content from rich data sources such as image headers, browser cache content, and system logging resources. Next, students will turn their focus to performing similar analysis against remote Windows servers using built-in Windows system management tools to identify misconfigured services, scrutinize historical registry entries for USB devices, evaluate the impact of malware attacks, and analyze packet capture data. By completing these tasks, students build their skills in managing systems, applicable to post-compromise system host analysis, or defensive tasks such as defending targeted systems from persistent attack threats. By adding new tools and techniques to their arsenal, students are better prepared to complete the analysis of complex systems with greater accuracy in less time.

**Topics:** Linux Host and Server Analysis; Windows Host and Server Analysis

### 561.2 HANDS ON: Enterprise Security Assessment

In this section of the class, students investigate the critical tasks for a high-quality penetration test. We'll look at the safest, most efficient ways to map a network and discover target systems and services. Once the systems are discovered, we look for vulnerabilities and reduce false positives with manual vulnerability verification. We'll also look at exploitation techniques, including the use of the Metasploit Framework to exploit these vulnerabilities, accurately describing risk and further reducing false positives. Of course, exploits are not the only way to access systems, so we also leverage password-related attacks, including guessing and cracking techniques to extend our reach for a more effective and valuable penetration test.

**Topics:** Network Mapping and Discovery; Enterprise Vulnerability Assessment; Network Penetration Testing; Password and Authentication Exploitation

### 561.3 HANDS ON: Web Application Assessment

This section of the course will look at the variety of flaws present in web applications and how each of them is exploited. Students will solve challenges presented to them by exploiting web applications hands-on with the tools used by professional web application penetration testers every day. The websites students attack mirror real-world vulnerabilities including Cross-Site Scripting (XSS), SQL Injection, Command Injection, Directory Traversal, Session Manipulation and more. Students will need to exploit the present flaws and answer questions based on the level of compromise they are able to achieve.

**Topics:** Recon and Mapping; Server-side Web Application Attacks; Client-side Web Application Attacks; Web Application Vulnerability Exploitation

### 561.4 HANDS ON: Mobile Device and Application Analysis

With the accelerated growth of mobile device use in enterprise networks, organizations find an increasing need to identify expertise in the security assessment and penetration testing of mobile devices and the supporting infrastructure. In this component of the course, we examine the practical vulnerabilities introduced by mobile devices and applications, and how they relate to the security of the enterprise. Students will look at the common vulnerabilities and attack opportunities against Android and Apple iOS devices, examining data remnants from lost or stolen mobile devices, the exposure introduced by common weak application developer practices, and the threat introduced by popular cloud-based mobile applications found in many networks today.

**Topics:** Mobile Device Assessment; Mobile Device Data Harvesting; Mobile Application Analysis

### 561.5 HANDS ON: Advanced Penetration Testing

This portion of the class is designed to teach the advanced skills required in an effective penetration test to extend our reach and move through the target network. This extended reach will provide a broader and more in-depth look at the security of the enterprise. We'll utilize techniques to pivot through compromised systems using various tunneling/pivoting techniques, bypass anti-virus and built-in commands to extend our influence over the target environment, and find issues that lesser testers may have missed. We'll also look at some of the common mistakes surrounding poorly or incorrectly implemented cryptography and ways to take advantage of those weaknesses to access systems and data that are improperly secured.

**Topics:** Anti-Virus Evasion Techniques; Advanced Network Pivoting Techniques; Exploiting Network Infrastructure Components; Exploiting Cryptographic Weaknesses

### 561.6 HANDS ON: Capture the Flag Challenge

This lively session represents the culmination of the course, where attendees will apply the skills they have mastered throughout all the other sessions in a hands-on workshop. They will participate in a larger version of the exercises presented in the class to independently reinforce skills learned throughout the course. Attendees will apply their newly developed skills to scan for flaws, use exploits, unravel technical challenges, and dodge firewalls, all while guided by the challenges presented by the NetWars Scoring Server. By practicing the skills in a combination workshop in which multiple focus areas are combined, participants will have the opportunity to explore, exploit, pillage, and continue to reinforce skills against a realistic target environment.

**Topics:** VoIP Supporting Infrastructure; VoIP Environment Awareness

## You Will Be Able To

- ▶ Use network scanning and vulnerability assessment tools to effectively map out networks and prioritize discovered vulnerabilities for effective remediation
- ▶ Use password analysis tools to identify weak authentication controls leading to unauthorized server access
- ▶ Evaluate web applications for common developer flaws leading to significant data loss conditions
- ▶ Manipulate common network protocols to maliciously reconfigure internal network traffic patterns
- ▶ Identify weaknesses in modern anti-virus signature and heuristic analysis systems
- ▶ Inspect the configuration deficiencies and information disclosure threats present on Windows and Linux servers
- ▶ Bypass authentication systems for common web application implementations
- ▶ Exploit deficiencies in common cryptographic systems
- ▶ Bypass monitoring systems by leveraging IPv6 scanning and exploitation tools
- ▶ Harvest sensitive mobile device data from iOS and Android targets

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

Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 5:00pm

30 CPE/CMU Credits

Laptop Required

Instructor: James Tarala

▶ GIAC Cert: GCCC

▶ Masters Program

**“James goes into great detail in his explanations and examples. At first I thought this might become tedious, but I soon realized that some things I knew well, I didn’t know as well as I thought. His breadth of knowledge is impressive.”**

-Kenneth Eichman,  
Chemical Abstracts Service

**“SEC566 is very valuable. This course allows me to understand the importance of managing risk as it relates to these control categories.”**

-Ian Perry-Okpara,  
Federal Reserve Bank of Atlanta

Cybersecurity attacks are increasing and evolving so rapidly that it 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 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.

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.

## 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



### James Tarala SANS Senior Instructor

James Tarala is a principal consultant with Enclave Security and is based in 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 in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.





## 566.1 HANDS ON: Introduction and Overview of the 20 Critical Controls

Day 1 will cover an introduction and overview of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

- 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 networks 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 the Controls
- ▶ Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- ▶ Audit each of the Critical Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

**“Topics addressed real-world and current threats – gives great suggestions to assist an organization to better protect their IP space.”**

–Bill Coffey, Shaw AFB



giacc.org



sans.edu

# Python for Penetration Testers

Five-Day Program  
 Mon, Oct 20 - Fri, Oct 24  
 9:00am - 5:00pm  
 30 CPE/CMU Credits  
 Laptop Required  
 Instructor: Mark Baggett

**“SEC573 is vital for anyone who considers themselves to be a pen tester.”**

-Jeff Turner, Lexis Nexis Risk Solutions

**“Mark has a very effective and thorough teaching style – great for learning new material.”**

-Roswitha MacLean, SELF

**“Scripting is a necessity for any serious pen tester. SEC573 provides useful hands-on knowledge.”**

-Jeffrey Moy, Atlas Air

## You Will Receive

- ▶ A virtual machine with sample code and working examples
- ▶ A copy of “Violent Python”

Your target has been well hardened. So far, your every attempt to compromise their network has failed. But you did find evidence of a vulnerability, a break in their defensive posture. Sadly, all of your tools have failed to successfully exploit it. Your employers demand results. What do you do when off-the-shelf tools fall short? You write your own tool.

The best penetration testers can customize existing open-source tools or develop their own tools. The ability to read, write, and customize software is what distinguishes the good penetration tester from the great penetration tester. This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools to put you on the path of becoming a great penetration tester. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it.

Unfortunately, many penetration testers do not have these skills today. The time and effort required to develop programming skills may seem overwhelming. But it is not beyond your reach. This course is designed to meet you at your current skill level, appealing to a wide variety of backgrounds ranging from people without a drop of coding experience all the way up to skilled Python developers looking to increase their expertise and map their capabilities to penetration testing. Because you can't become a world-class tool builder by merely listening to lectures, the course is chock full of hours of hands-on labs every day that will teach you the skills required to develop serious Python programs and how to apply those skills in penetration testing engagements. Join us and learn Python in-depth and fully weaponized!

The course begins with an introduction to SANS pyWars, a four-day Capture the Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own individualized pace. This allows experienced programmers to quickly progress to more advanced concepts while novice programmers spend time building a strong foundation. This individualized approach allows everyone to hone their current skills to make them the most lethal weapon they can be.

After introducing pyWars the course covers the essential skills required to get the most out of the Python language. The essential skills workshop labs will teach those who are new to software development the concepts and techniques required to develop their own tools. The workshop will also teach shortcuts that will make experienced developers even more deadly. Then we turn to applying those skills in today's real-world penetration testing scenarios. You will develop a port scanning, antivirus evading, client infecting backdoor for placement on target systems. You will develop a SQL injection tool to extract data from websites that fail with off-the-shelf tools. You will develop a multi-threaded password guessing tool and a packet assembling network reconnaissance tool. The course concludes with a one-day Capture the Flag event that will test your ability to apply your new tools and coding skills in a penetration testing challenge.

## Who Should Attend

- ▶ Security professionals who want to learn how to develop Python applications
- ▶ Penetration testers who want to move from being a consumer of security tools to the creator of security tools
- ▶ Technologists who need custom tools to test their infrastructure and desire to create those tools themselves

**573.1 HANDS ON: Essentials Workshop – PART 1**

The course begins with a brief introduction to Python and the pyWars Capture-the-flag game. We set the stage for students to learn at their own pace in the 100% hands-on pyWars lab environment. As more advanced students take on Python-based Capture-the-flag challenges, students who are new to programming will start from the very beginning with Python essentials.

**Topics:** Variables; Math Operators; Strings; Functions; Modules; Compound Statements; Introspection

**573.2 HANDS ON: Essentials Workshop – PART 2**

You will never learn to program by staring at Powerpoint slides. The second day continues the hands-on lab-centric approach established on day one. This section continues covering the essentials of the language, including data structures and programming concepts. With the essentials of the language under your belt, the pyWars challenges and the in-class labs start to cover more complex subjects.

**Topics:** Lists; Loops; Tuples; Dictionaries; The Python Debugger; System Arguments & OptParser; File Operations

**573.3 HANDS ON: Pen Testing Applications – PART 1**

Day 3 shifts gears. With a core set of skills established, we can begin developing penetration testing tools that you can use in your next engagement. You will develop a backdoor command shell that evades antivirus software and provides you with that critical initial foothold in the target environment. You will then develop a customizable SQL injection tool that you can use to extract all the data from a vulnerable database when off-the-shelf tools fail. Finally, we will discuss how to speed up your code with multi-threading.

**Topics:** Network Sockets; Exception Handling; Process Execution; Metasploit Integration; Antivirus; IDS Evasion; Introduction to SQL; Blind SQL Injection Techniques; Developing Web Clients; Multi-Threaded Applications; Mutexes and Semaphores; Message Queues; Thread Communications

**573.4 HANDS ON: Pentesting Applications – PART 2**

In this section you will develop more tools that will make you a more lethal penetration tester. First, you will develop a custom web-based password guesser. This will teach you how to get the most out of Python's web-based libraries and interact with websites using cookies, proxies, and other features to p0wn the most difficult web-based authentication systems. Then, you'll write a network reconnaissance tool that will demonstrate the power of Python's third-party libraries.

**Topics:** HTTP Form Password Guessing; Advanced Web Client Techniques; HTTP Proxies/HTTP Cookies; Session Hijacking; TCP Packet Reassembly With Scapy; Extracting Images from TCP Streams; Analyzing Image Metadata

**573.5 HANDS ON: Capture the Flag**

In this final section you will be placed on a team with other students. Working as a team, you will apply skills you have mastered in a series of penetration testing challenges. Participants will exercise the skills and code they have developed over the previous four days as they exploit vulnerable systems, break encryption cyphers, and remotely execute code on target systems. Test your skills! Prove your might!

**You Will Be Able To**

- ▶ Write a backdoor that uses Exception Handling, Sockets, Process execution, and encryption to provide you with your initial foothold in a target environment. The backdoor will include features such as a port scanner to find an open outbound port, the ability to evade antivirus software and network monitoring and the ability to embed payload from tools such as Metasploit.
- ▶ Write a SQL injection tool that uses standard Python libraries to interact with target websites. You will be able to use different SQL attack techniques for extracting data from a vulnerable target system.
- ▶ Develop a tool to launch password guessing attacks. While developing this tool you will also make your code run faster by using multi-threading. You will handle a modern authentication system by finding cookies and bypassing CAPTCHAs. You will know how to enhance your program with local application proxies and how to create and use target customized password files.
- ▶ Write a network reconnaissance tool that uses SCAPY, cStringsIO and PIL to reassemble TCP packet streams, extract data payloads such as images, display images, extract Metadata such as GPS coordinates and link those images with GPS coordinates to Google maps.

**“I benefited from not only the excellent course material of SEC573 but also from the additional info and very satisfactory percentage of hands-on time.”**

-Roswitha MacLean, Self



**Mark Baggett** SANS Certified Instructor

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. He has served in a variety of roles from software developer to Chief Information Security Officer. Mark is the author of SANS' Python for Penetration Testers course (SEC573) and the pyWars gaming environment. Mark teaches several classes in the SANS Penetration Testing curriculum including SEC504 (Incident Handling), SEC560 (Penetration Testing) and his Python course. Mark is very active in the information security community. Mark is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter, which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. As part of the Pauldotcom Team, Mark generates blog content for the “pauldotcom.com” podcast. In January 2011, Mark assumed a new role as the Technical Advisor to the DoD for SANS. Today he assists various government branches in the development of information security training programs.



# Mobile Device Security and Ethical Hacking

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Christopher Crowley

▶ GIAC Cert: GMOB

▶ Masters Program

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.

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or a 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.

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 from mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

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

## Who Should Attend

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

**“In the fast-paced world of BYOD and mobile device management, SEC575 is a must course for InfoSec managers.”**

-Jude Meche, DSCC

**“The content of SEC575 is simply eye-opening. Organizations are so busy trying to roll out their BYOD projects without any understanding of the risks. This course is a must for security professionals rolling out BYOD projects.”**

-Vijay Kora,

Open Solutions Consulting Inc.



### 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, GMOB, 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. @CCrowMontance

### 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 against 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 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
- 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.

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/event/network-security-2014/courses](https://sans.org/event/network-security-2014/courses)

## You Will Be Able To

- ▶ Develop effective policies to control employee-owned (Bring Your Own Device, BYOD) and enterprise-owned mobile devices, including the enforcement of effective passcode policies and permitted application
- ▶ Utilize jailbreak tools for Apple iOS and Android systems such as redsn0w & Absinthe
- ▶ Conduct an analysis of iOS and Android filesystem data using SqliteSpy, Plist Editor, and AXMLPrinter to plunder compromised devices and extract sensitive mobile device use information such as the SMS history, browser history, GPS history, and user dictionary keywords
- ▶ Analyze Apple iOS and Android applications with reverse-engineering tools including class-dump, JD-GUI, dextranslater, and apktool to identify malware and information leakage threats in mobile applications
- ▶ Conduct an automated security assessment of mobile applications using iAuditor, Cycript, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications
- ▶ Use wireless network analysis tools to identify and exploit wireless networks, crack WEP and WPA/ WPA2 access points, bypass enterprise wireless network authentication requirements, and harvest user credentials
- ▶ Intercept and manipulate mobile device network activity using Burp to manipulate the actions taken by a user in an application and to deliver mobile device exploits to vulnerable devices



giac.org



sans.edu

# Virtualization and Private Cloud Security

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Dave Shackelford

**“The rush for virtualization is difficult for security sensitive environments. SEC579 helps demonstrate which risks are valid.”**

-Paul Mayers, Lloyds Banking Group

**“SEC579 actually provides pertinent information outside what is freely available and is applicable to securing my organization’s virtual infrastructure.”**

-David Richardson, ManTech

**“Dave is one of the best instructors on the face of the planet! SEC579 is the absolute best virtualization security information available! And it’s immediately usable.”**

-Leonard Lyons, Northrop Grumman

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.

## 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



### Dave Shackelford SANS Senior Instructor

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

### 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; Virtual Machine Security Configuration Options; Storage Security and Design Considerations

### 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

### 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 an 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; integrate promiscuous interfaces and traffic capture methods into virtual networks; and then set up and configure 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 of 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. Most of this session will focus on incident response and forensics in a virtualized or cloud-based infrastructure. We'll walk students through the six-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 change 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.

# Wireless Ethical Hacking, Penetration Testing, and Defenses

## Six-Day Program

Mon, Oct 20 - Sat, Oct 25

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.

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and 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. You'll also develop attack techniques leveraging Windows 7 and Mac OS X. We'll 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.

## 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

**"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. The instructor has stretched me and my skills this week and I am better for it!"**

-John Fruge, B&W Technical Services

**"SEC617 was great. I am still impressed with the consistency from day 1-6 of Larry Pesce keeping a high level of energy and knowledge throughout."**

-Phillip Mein, JCCC



## 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 802.11 a/b/g 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 environments.

**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 the exploitation of 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

This section 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 Attacks; 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, selection of 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

## You Will Be Able To

- ▶ Identify and locate malicious rogue access points using free and low-cost tools
- ▶ Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- ▶ Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- ▶ Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organization
- ▶ Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- ▶ Utilize wireless fuzzing tools including Metasploit file2air, and Scapy to identify new vulnerabilities in wireless devices



giac.org



sans.org/  
cyber-guardian



sans.edu

# Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Justin Searle

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

## Who Should Attend

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

We will begin by exploring advanced techniques and attacks to which modern, complex applications are vulnerable. We will then explore encryption as it relates to web applications, digging deep into practical cryptography including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing this encryption. We will spend some time looking at alternate front ends to web applications and web services such as mobile applications. The final portion of the class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets and fulfills a need to teach more advanced techniques than can be covered in the foundational course, **SEC542: Web Application Penetration Testing and Ethical Hacking.**

## You Will Be Able To

- ▶ Assess and attack complex modern applications
- ▶ Understand the special testing and exploits available against content management systems such as SharePoint and WordPress
- ▶ Use techniques to identify and attack encryption within applications
- ▶ Identify and bypass web application firewalls and application filtering techniques to exploit the system
- ▶ Use exploitation techniques learned in class to perform advanced attacks against web application flaws such as XSS, SQL injection and CSRF



**“SEC642 is a great way to take your testing to the next level. I can’t wait to try everything when I get back to work.”**

-Sara Dunnack, Aetna

**“SEC642 is very relevant to the work I do every day, and provides a lot of insight into technologies I thought I was familiar with.”**

-John Lincoln, Nordstrom

**“Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences.”**

-Bobby Bryant, DoD



## Justin Searle SANS Certified Instructor

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

### 642.1 HANDS ON: Advanced Discovery and Exploitation

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

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

### 642.2 HANDS ON: Discovery and Exploitation for Specific Applications

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

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

### 642.3 HANDS ON: Web Application Encryption

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

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

### 642.4 HANDS ON: Mobile Applications and Web Services

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

**Topics:** Attacking CBC Chosen Plaintext; Exploiting CBC with Padding Oracles; Understanding the Mobile Platforms and Architectures; Intercepting Traffic to Web Services and from Mobile Applications; Building a Test Environment; Penetration Testing of Web Services

### 642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

**Topics:** Understanding of Web Application Firewalling and Filtering Techniques; Exploring How to Determine the Rule Sets Protecting the Application; Learning How HTML5 Injections Work; Discovering the Use of UNICODE and Other Encodings

### 642.6 HANDS ON: Capture the Flag

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

# Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

## Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 7:00pm (Days 1-5)

9:00am - 5:00pm (Day 6)

Laptop Required

46 CPE/CMU Credits

Instructor: James Lyne

- ▶ GIAC Cert: GXPN
- ▶ Cyber Guardian
- ▶ Masters Program

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, Return Oriented Programming (ROP), Windows exploit-writing, and much more!

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

SEC660 starts off by introducing the advanced penetration concept, and provides an overview to help prepare students for what lies ahead. The focus of day one is on network attacks, an area often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Attacks are performed against NAC, VLANs, OSPF, 802.1X, CDP, IPv6, VOIP, SSL, ARP, SNMP, and others. Day two starts off with a technical module on performing penetration testing against various cryptographic implementations. The rest of the day is spent on network booting attacks, escaping Linux restricted environments such as chroot, and escaping Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using Return Oriented Programming (ROP) and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

## Who Should Attend

- ▶ Network and systems penetration testers
- ▶ Incident handlers
- ▶ Application developers
- ▶ IDS engineers

**“Looking at everything I have learned from SANS, I definitely feel I have gained an edge when it comes to the augmentation of my pentest skills.”**

-Alexander Cobblah,  
Booz Allen Hamilton

**“James Lyne demonstrates a great mastery knowledge and has a great personality.”**

-Brian Anderson,  
Northrop Grumman Corporation



## James Lyne SANS Certified Instructor

James Lyne is the Director of EMEA at SANS and the Director of Technology Strategy at the security firm Sophos. James comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed “massive geek”.

Eventually James escaped dark rooms and learned some social skills, and today is a keen presenter at conferences and industry events. With a wide range of experience working in a technical and strategic capacity from incident response to forensics with some of the world's largest organizations, James participates in industry panels, policy groups, and is a frequently-called-upon expert advisor all over the world. James is a frequent guest lecturer and often appears on national TV and other media outlets. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify and develop new talent. @jameslyne

### 660.1 HANDS ON: Network Attacks for Penetration Testers

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

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

### 660.2 HANDS ON: Crypto, Network Booting Attacks, and Escaping Restricted Environments

Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

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

### 660.3 HANDS ON: Python, Scapy, and Fuzzing

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

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

### 660.4 HANDS ON: Exploiting Linux for Penetration Testers

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

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

### 660.5 HANDS ON: Exploiting Windows for Penetration Testers

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

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

### 660.6 HANDS ON: Capture the Flag

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

#### You Will Be Able To

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



giac.org



sans.org/  
cyber-guardian



sans.edu

# Advanced Exploit Development for Penetration Testers

NEW

SANS

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Stephen Sims

## What You Will Receive

- ▶ Various preconfigured \*NIX virtual machines
- ▶ A course DVD with various tools that are required for use in class

“SEC760 is the kind of training we couldn’t get anywhere else. It’s not all theory, we got to implement and to exploit everything we learned.”

-Jenny Kitaichit, Intel

“Stephen Sims is super skilled! SANS has the brightest!!!”

-Mike Evans, Alaska Airlines

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. **SEC760:Advanced Exploit Development for Penetration Testers** teaches the skills required to reverse-engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

## You Will Learn:

- ▶ How to write modern exploits against the Windows 7 and 8 operating systems
- ▶ How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- ▶ The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- ▶ How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed.
- ▶ How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

## Who Should Attend

- ▶ Senior network and system penetration testers
- ▶ Secure application developers (C & C++)
- ▶ Reverse-engineering professionals
- ▶ Senior incident handlers
- ▶ Senior threat analysts
- ▶ Vulnerability researchers
- ▶ Security researchers



## Stephen Sims SANS Senior Instructor

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

@Steph3nSims

### 760.1 HANDS ON: Threat Modeling, Reversing and Debugging with IDA

Many penetration testers, incident handlers, developers, and other relative professionals lack reverse-engineering and debugging skills. This is a different skill than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDLC, developers and exploit writers should have experience using IDA Pro to debug and reverse their code when finding bugs or when identifying potential risks after static code analysis or fuzzing.

**Topics:** Security Development Lifecycle (SDL); Threat Modeling; Why IDA Is the #1 Tool for Reverse Engineering; IDA Navigation; IDA Python and the IDA IDC; IDA Plug-ins and Extensibility; Local Application Debugging with IDA; Remote Application Debugging with IDA

### 760.2 HANDS ON: Advanced Linux Exploitation

The ability to progress into more advanced reversing and exploitation requires an expert-level understanding of basic software vulnerabilities, such as those covered in SEC660. Heap overflows serve as a rite of passage into modern exploitation techniques. This day is aimed at bridging this gap of knowledge in order to inspire thinking in a more abstract manner; necessary for continuing further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows.

**Topics:** Linux Heap Management, Constructs, and Environment; Navigating the Heap; Abusing Macros such as `unlink()` and `frontlink()`; Function Pointer Overwrites; Format String Exploitation; Abusing Custom Doubly-Linked Lists; Defeating Linux Exploit Mitigation Controls; Using IDA for Linux Application Exploitation

### 760.3 HANDS ON: Patch Diffing, One-Day Exploits, and Return Oriented Shellcode

Attackers generally download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Often, vulnerabilities are disclosed privately, or even discovered in-house, allowing the vendor to more silently patch the vulnerability. This also allows the vendor to release limited or even no details at all about a patched vulnerability. Attackers are well aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems. This technique is also performed by incident handlers, IDS administrators and vendors, vulnerability and penetration testing framework companies, government entities, and others.

**Topics:** The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with `BinDiff`, `patchdiff2`, `turbodiff`, and `darungrim3`; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules; Triggering Patched Vulnerabilities; Writing One-Day Exploits; Handling Modern Exploit Mitigation Controls

### 760.4 HANDS ON: Windows Kernel Debugging and Exploitation

The Windows Kernel is very complex and intimidating. This day aims to help you understand the Windows kernel and the various exploit mitigations added into recent versions. You will perform Kernel debugging on various versions of the Windows OS, such as Windows 7 and 8, and learn to deal with its inherent complexities. Exercises will be performed to analyze vulnerabilities, look at exploitation techniques, and get a working exploit.

**Topics:** Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows Kernel; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques

### 760.5 HANDS ON: Windows Heap Overflows and Client-Side Exploitation

The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser, so browser techniques will also be taught, including modern heap spraying to deal with IE 8/9/10 and other browsers such as Firefox and Chrome. You will work towards writing exploits in the Use-After-Free/Dangling Pointer vulnerability class.

**Topics:** Windows Heap Management, Constructs, and Environment; Browser-Based and Client-Side Exploitation; Remedial Heap Spraying; Understanding C++ vtable/vtable Behavior; Modern Heap Spraying to Determine Address Predictability; Use-After-Free Attacks and Dangling Pointers; Determining Exploitability; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls

### 760.6 HANDS ON: Capture the Flag

Day 6 will serve as a capture the flag day with different types of challenges from material taught throughout the week.

## You Will Be Able To

- ▶ Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems
- ▶ Create exploits to take advantage of vulnerabilities through a detailed penetration testing process
- ▶ Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts
- ▶ Perform remote debugging of Linux and Windows applications
- ▶ Understand and exploit Linux heap overflows
- ▶ Write Return Oriented Shellcode
- ▶ Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities
- ▶ Perform Windows heap overflows and use-after-free attacks
- ▶ Use precision heap sprays to improve exploitability
- ▶ Perform Windows Kernel debugging up through Windows 8 64-bit
- ▶ Jump into Windows kernel exploitation

# Windows Forensic Analysis

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Chad Tilbury  
 ▶ GIAC Cert: GCFE  
 ▶ Masters Program

“FOR408 is going to help me obtain my GCFE certification, and will help me in my day-to-day job as a digital forensic associate.”

-Christine Casey, Stroz Friedberg

“FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations.”

-Nathan Lewis, KPMG



## Master Computer Forensics. What Do You Want to Uncover Today?

Every organization will deal with cyber-crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

**FOR408: Windows Forensic Analysis** focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

## FOR408 Windows Forensic Analysis will teach you to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, XP, and Windows Server 2008/2012
- Identify artifact and evidence locations that will answer key questions, including questions about program execution, file opening, external device usage, geo-location, file download, anti-forensics, and system usage
- Focus your capabilities on analysis instead of how to use a specific tool
- Extract key answers by utilizing proper analysis via a variety of free, open-source, and commercial tools in the Windows SIFT Workstation

**Updated FOR408 Course in 2014:** This course utilizes a brand-new Windows 8.1 based case exercise that took over 6 months to create the data. Realistic example case data takes months to create in real time correctly. The example case is a Windows 8.1 based image that has the subject utilize Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. Our development team has created an incredibly realistic scenario. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook, will detail step-by-step what each investigator needs to know to examine the latest Windows 8.1.

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



### Chad Tilbury SANS Senior Instructor

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. 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 60 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 GCFE, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury



**408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage**

The Windows Forensics course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

**Topics:** Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; FAT and NTFS File System Overview; Key Word Searching and Forensics Suites (FTK, EnCase, and Autopsy); Document and File Metadata; File Carving

**408.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 – Registry and USB Device Analysis**

This day focuses on Windows XP, Windows 7, and Windows 8/8.1 Registry Analysis, and USB Device Forensics. Throughout the section, investigators will use their skills in a real hands-on case, exploring evidence and analyzing evidence.

**Topics:** Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; External and Bring Your Own Device (BYOD) Forensic Examinations; Tools Utilized

**408.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 – Email Forensics**

You will learn how major forensic suites can facilitate and expedite the investigative process, and how to recover and analyze email, the most popular form of communication. Client-based, server-based, mobile, and web-based email forensic analysis are discussed in-depth.

**Topics:** Evidence of User Communication; How Email Works; Determining Sender's Geographic Locations; Examination of Email; Types of E-Mail Formats

**408.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 – Windows 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 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome**



This section looks at Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what individuals 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 Forensic Challenges**

This section revolves around a Digital Forensic Challenge based on Windows Vista/7. It is a capstone exercise for every artifact discussed in the class. You will use this section to consolidate the skills that you have learned over the past week.

**Topics:** Digital Forensic Case; Mock Trial

**You Will Be Able To**

- ▶ Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/8.1
- ▶ Use full-scale forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- ▶ Uncover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- ▶ Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), e-mail analysis, and Windows Registry parsing
- ▶ Use automated analysis techniques via AccessData's Forensic ToolKit (FTK), NuiX, and Internet Evidence Finder (IEF)
- ▶ Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and accomplish detailed damage assessments
- ▶ Use Windows shellbags analysis tools to articulate every folder and directory that a user opened up while browsing local, removable, and network drives
- ▶ Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- ▶ Use event log analysis techniques to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- ▶ Determine where a crime was committed using registry data to pinpoint the geo-location of a system by examining connected networks and wireless access points
- ▶ Use free browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts and flash cookies to identify the web activity of suspects, even if privacy cleaners and in-private browsing are used



giac.org



sans.edu



http://computer-forensics.sans.org

# Advanced Computer Forensic Analysis and Incident Response

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Rob Lee

▶ GIAC Cert: GCFA

▶ Cyber Guardian

▶ Masters Program

▶ DoDD 8570

“This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession.”

-Naveel Koya,

A C-DAC - Trivandrum

“FOR508 has an interesting curriculum delivered flawlessly, with hands-on labs that reinforce the material covered.”

-Everett Sherlock, Kapstone Paper



## Rob Lee SANS Faculty Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC 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 seven 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.” @robtee,sansforensics

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.

*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?

FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats. 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.



### 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

### 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 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 APT groups or crime syndicate groups that 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 incident response 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 are 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 established 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.



giac.org



sans.org/  
cyber-guardian



sans.edu



DoDD 8570 Required  
sans.org/8570

## You Will Be Able To

- ▶ Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hacktivists
- ▶ Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- ▶ Use the SIFT Workstation's capabilities, and perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- ▶ Use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- ▶ Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- ▶ Track the exact footprints of an attacker crossing multiple systems and observe data the attacker has collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- ▶ Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- ▶ Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS \$130 directory file indexes, journal parsing, and detailed Master File Table analysis
- ▶ Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, and recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- ▶ Discover an adversary's persistence mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autoruns, psexec, jobparser, group policy, triage-ir, and IOCfinder

# Memory Forensics In-Depth

NEW

SANS

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Alissa Torres

“Very valuable for what my group is doing at JPL. With the acquisition of MIR and RAM in first response, this is exactly the skill set we need to master.”

-Rick Smith, Jet Propulsion Lab

“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



## Alissa Torres SANS Certified Instructor

Alissa Torres specializes 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 an 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 the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught 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 B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT, and CTT+ certifications. @sibertor

Digital Forensics and Incident Response (DFIR) professionals view the acquisition and analysis of physical memory as critical to the success of an investigation, be it a criminal case, employee policy violation, or enterprise intrusion. Investigators who do not look at volatile memory are *leaving evidence on the table*. The valuable contents of RAM hold evidence of user actions as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to deftly analyze captured memory images and live response audits. By using the most effective freeware and open-source tools in the industry today and delivering a deeper understanding of how these tools work, this five-day course shows DFIR professionals how to unravel the real story of what happened on a system. It is a critical course for any serious investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

Just as it is crucial to understand disk and registry structures to substantiate findings in traditional system forensics, it is equally critical to understand memory structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. This course draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with hands-on, real-world, and malware-laden memory images.

### FOR526 – Windows Memory Forensics In-Depth will teach you:

- **Proper Memory Acquisition:** Demonstrate targeted memory capture ensuring data integrity and combating anti-acquisition techniques
- **How to Find Evil in Memory:** Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- **Effective Step-by-Step Memory Analysis Techniques:** Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- **Best Practice Techniques:** Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

**Remember: “Malware can hide, but it must run.”** It is this malware paradox that is the key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible for them to hide their footprints completely from a skilled incident responder performing memory analysis. FOR526 will ensure that you and your team are ready to respond to the challenges inherent in DFIR by using cutting-edge memory forensics tools and techniques.

### 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

### 526.1 HANDS ON: Foundations in Memory Analysis and Acquisition

Simply put, memory analysis has become a **required skill** for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first hit – the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

**Topics:** Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT Workstation; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

### 526.2 HANDS ON: Unstructured Analysis and Process Exploration

Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

**Topics:** Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

### 526.3 HANDS ON: Investigating the User via Memory Artifacts

An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

**Topics:** Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

### 526.4 HANDS ON: Internal Memory Structures (PART I)

Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, “Spotting Rootkit Behaviors” and “Extracting Suspicious Binaries,” it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

**Topics:** Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction

### 526.5 HANDS ON: Internal Memory Structures (PART II) and Memory Analysis Challenges

Sometimes an investigator’s luck runs out and he or she does not complete a memory acquisition before the target system is taken offline or shut down. In these cases, where else can system memory captures be found? Hibernation files and Windows crashdump files can be valuable sources of information, regardless of whether or not you find yourself with a current memory capture. This section covers the structure of the hibernation and crashdump files, as well as how to convert both into raw memory images that can easily be parsed using Volatility and other tools in our memory forensics weapons arsenal. In addition, we will analyze a crash dump file, discovering just how Windows responds and what information is captured when a system crashes.

**Topics:** Hibernation Files; Crash Dump Files; Memory Analysis Challenges

### 526.6 HANDS ON: Final Day Memory Analysis Challenge

This final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen the students’ ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

**Topics:** Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OSX Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

## You Will Be Able To

- ▶ Utilize stream-based data parsing tools to extract AES-encryption keys from a physical memory image to aid in the decryption of encryption files, volumes such as TrueCrypt, and BitLocker
- ▶ Gain insight into the current network activity of the host system by retrieving network packets from a physical memory image and examining them with a network packet analyzer
- ▶ Inspect a Windows crash dump to discern processes, process objects and current system state at the time of crash through use of various debugging tools such as kd, WinDBG, and livekd
- ▶ Conduct Live System Memory Analysis with the powerful SysInternals tool, Process Explorer, to collect real-time data on running processes allowing for rapid triage
- ▶ Use the SIFT workstation and in-depth knowledge of PE File modules in physical memory, extract and analyze packed and non-packed PE binaries from memory and compare them to their known disk-bound files.
- ▶ Discover key features from memory such as the BIOS keyboard buffer, Kernel Debugging Data Block (KDBG), Executive Process (EPROCESS) structures, and handles based on signature and offset searching, gaining a deeper understanding of the inner workings of popular memory analysis tools.
- ▶ Analyze memory structures using high-level and low-level techniques to reveal hidden and terminated processes and extract processes, drivers, and memory sections for further analysis
- ▶ Use a variety of means to capture memory images in the field, explaining the advantages and limitations of each method

# Advanced Network Forensics and Analysis

NEW

SANS

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Philip Hagen  
 ▶ GIAC Cert: GNFA

**“I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware than a more traditional approach does.”**

-Niklas Vilhelm, Norwegian National Security Authority

ATTEND  
 REMOTELY



**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.  
 More info on page 74.

Coming Fall of 2014



giac.org

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career; but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

**FOR572: Advanced Network Forensics and Analysis** was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpextract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through hundreds and thousands of data records.



## Who Should Attend

- ▶ Incident response team members
- ▶ Law enforcement officers, federal agents, and detectives
- ▶ Information security managers
- ▶ Network defenders
- ▶ IT professionals
- ▶ Network engineers
- ▶ IT lawyers and paralegals
- ▶ Anyone interested in computer network intrusions and investigations



### Philip Hagen SANS Instructor

Philip Hagen has over 14 years of experience in creating and deploying strategic and ad-hoc IT and InfoSec solutions. He has managed small, tactical projects and large government contracts. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a Communications Officer, and was assigned to a base-level Year 2000 project management office. The plans he helped create were later used during California's rolling power blackouts. At the Pentagon, he managed a support team serving 200 analysts. In 2003, Phil shifted to a government contractor, providing technical services for exotic IT security projects. These included systems that demanded 24x7x365 functionality. He supported the design, deployment, and support of a specialized network for 100 security engineers in 10 offices. He later managed a team of 85 computer forensic professionals in the National Security sector. Most recently, Phil formed Lewes Technology Consulting, LLC. He applies his IT and security experience to small and medium-size businesses as they track toward their business goals, and performs forensic casework and InfoSec training. @PhilHagen

### 572.1 HANDS ON: Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server; then go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

**Topics:** Goals of Forensic Investigation; Hypothesis Management Fundamentals; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Sources and Types; Case Management and Evidence Collection/Handling; Web Proxy Server Examination; Network Architectural Challenges and Opportunities; Packet Capture Applications and Data

### 572.2 HANDS ON: Netflow Analysis, Commercial Tools, and Visualization

In this section, you will learn what data items NetFlow can provide, and the various means of collecting those items. As with many such monitoring technologies, both commercial and open-source solutions exist to query and examine NetFlow data. We will review both categories and discuss the benefits and drawbacks of each. Finally, we will address the forensic aspects of wireless networking. We will cover similarities with and differences from traditional wired network examination, as well as what interesting artifacts can be recovered from wireless protocol fields. Some inherent weaknesses of wireless deployments will also be covered, including how attackers can leverage those weaknesses during an attack, and how they can be detected.

**Topics:** Introduction to NetFlow; NetFlow Collection Approaches; Open-Source Flow Tools; Commercial Flow Analysis Suites; Profiling and Behavior Analysis; Visualization Techniques and Tools; Wireless Network Forensics

### 572.3 HANDS ON: Network Protocols and Investigations

This section covers some of the most common and fundamental network protocols that you will likely face during an investigation. We will cover a broad range of protocols including the Dynamic Host Configuration Protocol, which glues together layers two and three on the OSI model, and Microsoft's Remote Procedure Call protocol, which provides all manners of file, print, name resolution, authentication, and other services.

**Topics:** Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS); Hypertext Transfer Protocol (HTTP); Secure HTTP (HTTPS) and Secure Sockets Layer (SSL); File Transfer Protocol (FTP); Network Time Protocol (NTP); Commercial Network Forensics; Microsoft Protocols; Simple Mail Transfer Protocol (SMTP)

### 572.4 HANDS ON: Logging, OPSEC, and Footprint

In this section, you will learn about various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You will learn various solutions that accomplish this, from tactical to enterprise-scale.

**Topics:** Syslog; Microsoft Event Logging; HTTP Server Logs; Firewall and Intrusion Detection Systems; Log Data Collection, Aggregation, and Analysis; Investigation OPSEC and Footprint Considerations

### 572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

**Topics:** Introduction to Encryption; Man-in-the-Middle; Encrypted Traffic Flow Analysis; Payload Reconstruction; Network Protocol Reverse Engineering; Automated Tools and Libraries

### 572.6 HANDS ON: Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

**Topics:** Network Forensic Case

## You Will Be Able To

- ▶ Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- ▶ Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- ▶ Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- ▶ Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- ▶ Use data from typical network protocols to increase the fidelity of the investigation's findings
- ▶ Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- ▶ Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- ▶ Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- ▶ Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- ▶ Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- ▶ Analyze wireless network traffic to find evidence of malicious activity
- ▶ Use visualization tools and techniques to distill vast, complex data sources into management-friendly reports
- ▶ Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- ▶ Apply the knowledge you acquire during the week in a full-day capstone exercise, modeled after real-world nation-state intrusions

# Advanced Smartphone Forensics

**NEW****SANS**

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: Heather Mahalik



It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individual's movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

**FOR585: Advanced Smartphone Forensics** focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. FOR585, originally conceptualized by Eoghan Casey, Heather Mahalik, and Terrance Maguire, has been updated to address today's smartphone technologies and threats by studying real-life investigative scenarios.

**Don't miss the NEW FOR585!**

The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlooked. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals.

**YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!**

**Who Should Attend**

- ▶ Experienced digital forensic analysts who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- ▶ Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices by learning how individuals used their smartphones, who they communicated with, and files they accessed
- ▶ Information security professionals who respond to data breach incidents and intrusions
- ▶ Incident response teams tasked with identifying the role that smartphones played in a breach
- ▶ Law enforcement officers, federal agents, or detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- ▶ IT auditors who want to learn how smartphones can expose sensitive information
- ▶ SANS SEC575, FOR563, FOR408, and FOR508 graduates looking to take their skills to the next level

**"This is the most advanced mobile device training that I know of and is greatly needed. It is currently the only course being taught at this level!"**

-Scott McNamee, DoS/CACI

**"Heather is a great instructor. The only downside will be not being able to bring her back to my office so we can pick her brain every day!"**

-C. McCollom,

Clark County Sheriff's Office

**Heather Mahalik** SANS Certified Instructor

Heather Mahalik is a senior digital forensics analyst at Basis Technology. As the on-site project manager, she uses her experience to manage the cell phone exploitation team and supports media and cell phone forensics efforts in the U.S. government. Heather has worked in digital forensics for over 10 years and has performed thousands of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices, and portable media. Previously, Heather worked as a forensic examiner for Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high-profile cases. She has authored papers, presented at leading conferences, and instructed classes focused on Mac forensics, mobile device forensics, and computer forensics to practitioners in the field.

Heather's background is based on media forensics, and she currently specializes in BlackBerry, Nokia, knock-off, Android, and iOS Forensics. @HeatherMahalik



### 585.1 HANDS ON: Smartphone Forensics Fundamentals

Although smartphone forensic concepts are similar to those in digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. Today you will apply what you already know to smartphone forensic handling, device capabilities, acquisition methods, and data encoding concepts of smartphone components. You will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures.

**Topics:** Introduction to Smartphones; Smartphone Handling; Forensic Acquisition of Smartphones; Smartphone Forensics Tool Overview; Smartphone Components

### 585.2 HANDS ON: Android and Malware Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. Without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on the devices, you will be unprepared for the rapidly evolving world of smartphone forensics. Malware affects not only Androids, but also a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones, and how to identify it.

**Topics:** Android Forensics Overview; Android File System Structures; Android Evidentiary Locations; Handling Locked Android Devices; Traces of User Activity on Android Devices; Malware and Spyware Forensics

### 585.3 HANDS ON: iOS Forensics

Apple iOS devices are no longer restricted to the United States, but are in use worldwide. iOS devices contain substantial amounts of data, including deleted records, that can be decoded and interpreted into useful information. Proper handling and parsing skills are required for bypassing locked iOS devices and correctly interpreting the data. Without the iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

**Topics:** iOS Forensics Overview and Acquisition; Handling Locked iOS Devices; iOS File System Structures; iOS Evidentiary Locations; Traces of User Activity on iOS Devices

### 585.4 HANDS ON: Blackberry and Backup File Forensics

Blackberry smartphones are designed to protect user privacy, but techniques taught in this section will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of the file system of Blackberry devices. Backup files are commonly found on external media and can be the only forensic acquisition method for newer iOS devices that are locked. Learning how to access and parse data from encrypted backup files may be the only lead to smartphone data relating to your investigation.

**Topics:** Backup File Forensics Overview; Creating and Parsing Backup Files; Evidentiary Locations on Backup Files; Locked Backup Files; Blackberry Forensics Overview; Blackberry Forensic Acquisition and Best Practices; Blackberry File System and Evidentiary Locations; Blackberry Forensic Analysis

### 585.5 HANDS ON: Third-Party Application and Other Smartphone Device Forensics

Given the prevalence of other types of smartphones around the world, it is critical for examiners to develop a foundation of understanding about data storage on multiple devices. Nokia smartphones running the Symbian operating system may no longer be manufactured, but it doesn't mean that they do not exist in the wild. You must acquire skills for handling and parsing data from uncommon smartphone devices. This day of instruction will prepare you to deal with "misfit" smartphone devices and provide you with advanced methods for decoding data stored in third-party applications across all smartphones.

**Topics:** Third-Party Applications on Smartphones Overview; Third-Party Application Locations on Smartphones; Decoding Third-Party Application Data on Smartphones; Knock-off Phone Forensics; Nokia (Symbian) Forensics; Windows Phone/Mobile Forensics

### 585.6 HANDS ON: Smartphone Forensic Capstone Exercise

This section will test all that you have learned during this week. In small groups, you will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

## You Will Be Able To

- ▶ Extract and use information from smartphones and mobile devices, including Android, iOS, Blackberry, Windows Phone, Symbian, and Chinese knock-off devices
- ▶ Understand how to detect hidden malware and spyware on smartphones and extract information related to security breaches, cyber espionage, and advanced threats involving smartphones
- ▶ Prevent loss or destruction of valuable data on smartphones by learning proper handling of these devices
- ▶ Learn a variety of acquisition methods for smartphones with an understanding of the advantages and limitations of each acquisition approach
- ▶ Interpret file systems on smartphones and locate information that is not generally accessible to users
- ▶ Recover artifacts of user activities from third-party applications on smartphones
- ▶ Recover location-based and GPS information from smartphones
- ▶ Perform advanced forensic examinations of data structures on smartphones by diving deeper into underlying data structures that many tools do not interpret
- ▶ Analyze SQLite databases and raw data dumps from smartphones to recover deleted information
- ▶ Perform advanced data-carving techniques on smartphones to validate results and extract missing or deleted data
- ▶ Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (who communicated with whom, locations at particular times)
- ▶ Decrypt locked backup file and bypass smartphone locks
- ▶ Apply the knowledge you acquire during the six days to conduct a full-day smartphone capstone event involving multiple devices and modeled after real-world smartphone investigations

# Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Lenny Zeltser

▶ GIAC Cert: GREM

▶ Masters Program

**“If you are serious about understanding reverse-engineering malware, FOR610 is the perfect course. Lenny is very thorough and meticulous – you will not get lost!”**

-Tom Cook, USMA

**“FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats.”**

-Paul Gunnerson, U.S. Army



## 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 member of the Board of Directors 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. @lennyzeltser

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining malicious programs that target and infect Windows systems. Knowing how to understand capabilities of malware is critical to an organization's ability to derive the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to understand the inner workings of malicious software and uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. Additionally, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

This course will teach you how to handle self-defending malware, learning to bypass the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts and deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will also learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if it exhibits rootkit characteristics.

The course culminates with a series of capture-the-flag challenges designed to reinforce the techniques learned in class and to provide additional opportunities for learning practical malware analysis skills in a fun setting.

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.



## Who Should Attend

- ▶ Individuals who have dealt with incidents involving malware and want to learn how to understand key aspects of malicious programs
- ▶ Technologists who have informally experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their expertise in this area
- ▶ Forensic investigators and IT practitioners looking to expand their skillsets and learn how to play a pivotal role in the incident response process

### 610.1 HANDS ON: Malware Analysis Fundamentals

Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program'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 debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner; and set up such a lab on your laptop using the supplied windows and Linux (REMinux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab – with guidance and explanations from the instructor – to reinforce the concepts discussed throughout the day.

**Topics:** Assembling a Toolkit for Effective Malware Analysis; Examining Static Properties of Suspicious Programs; Performing Behavioral Analysis of Malicious Windows Executables; Performing Static and Dynamic Code Analysis of Malicious Windows Executables; Contributing Insights to the Organization's Larger Incident Response Effort

### 610.2 HANDS ON: Malicious Code Analysis

Section two focuses on examining malicious Windows 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 section begins with an overview of key code-reversing concepts and presents a primer on essential x86 Intel 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 remaining part of the section discusses how malware implements common characteristics, such as keylogging and DLL injection, at the assembly level. You will learn how to recognize such characteristics in suspicious Windows executable files.

**Topics:** Core Concepts for Analyzing Malware at the Code Level; x86 Intel Assembly Language Primer for Malware Analysts; Identifying Key x86 Assembly Logic Structures with a Disassembler; Patterns of Common Malware Characteristics at the Windows API Level (DLL Injection, Function Hooking, Keylogging, Communicating over HTTP, etc.)

### 610.3 HANDS ON: In-Depth Malware Analysis

Section three builds upon the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. You will learn about packers and the techniques that may help analysts bypass their defenses. Additionally, you will understand how to redirect network traffic in the lab to better interact with malware to understand its capabilities. You will also learn how to examine malicious websites and deobfuscate browser scripts, which often play a pivotal role in malware attacks.

**Topics:** Recognizing Packed Malware; Automated Malware Unpacking Tools and Approaches; Manual Unpacking of Using OllyDbg, Process Dumping Tools and Imports-Rebuilding Utilities; Intercepting Network Connections in the Malware Lab; Interacting with Malicious Websites to Examine their Nature; Deobfuscating Browser Scripts Using Debuggers and Runtime Interpreters; JavaScript Analysis Complications

### 610.4 HANDS ON: Self-Defending Malware

Section four focuses on the techniques malware authors commonly employ to protect malicious software from being examined, often with the help of packers. You will learn how to recognize and bypass anti-analysis measures, such as tool detection, string obfuscation, unusual jumps, breakpoint detection and so on. We will also discuss the role that shellcode plays in the context of malware analysis and will learn how to examine this aspect of attacks. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

**Topics:** Bypassing Anti-Analysis Defenses; Recovering Concealed Malicious Code and Data; Unpacking More Sophisticated Packers to Locate the Original Entry Point (OEP); Identifying and Disabling Methods Employed by Malware to Detect Analysts' Tools; Analyzing Shellcode to Assist with the Examination of Malicious Documents and other Artifacts

### 610.5 HANDS ON: Malicious Documents and Memory Forensics

Section five starts by exploring common patterns of assembly instructions often used to gain initial access to the victim's computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner and exploring steps for analyzing malicious PDF documents with practical tools and techniques. 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 as 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 analyze malware more efficiently.

**Topics:** Analyzing Malicious Microsoft Office (Word, Excel, PowerPoint) Documents; Analyzing Malicious Adobe PDF Documents; Analyzing Memory to Assess Malware Characteristics and Reconstruct Infection Artifacts; Using Memory Forensics to Analyze Rootkit Infections

### 610.6 HANDS ON: Malware Reverse-Engineering Tournament

Section 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 hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student's ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, 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. The students who score the highest in the malware reverse-engineering challenge will be awarded the coveted SANS' Digital Forensics Lethal Forensicator coin. Game on!

**Topics:** Behavioral Malware Analysis; Dynamic Malware Analysis (Using a Debugger); Static Malware Analysis (Using a Disassembler); JavaScript Deobfuscation; PDF Document Analysis; Office Document Analysis; Memory Analysis

## You Will Be Able To

- ▶ Build an isolated, controlled laboratory environment for analyzing code and behavior of malicious programs
- ▶ Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes in a Windows environment
- ▶ Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- ▶ Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- ▶ Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- ▶ Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- ▶ Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- ▶ Assess the threat associated with malicious documents, such as PDF and Microsoft Office files in the context of targeted attacks
- ▶ Derive Indicators of Compromise (IOCs) from malicious executables to perform incident response triage
- ▶ Utilize practical memory forensics techniques to examine capabilities of rootkits and other malicious program types.



giac.org



sans.edu

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

## Six-Day Program

Mon, Oct 20 - Sat, Oct 25

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: Dr. Eric Cole

▶ GIAC Cert: GISP

▶ DoDD 8570



**“Great course and well worth it if you are considering taking the CISSP exam.”**

-David Raymond, U.S. Army

This course will cover the security concepts needed to pass the CISSP® exam. This is an accelerated review course that assumes the student has a basic understanding of networks and operating systems and focuses solely on the 10 domains of knowledge of the CISSP®:

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

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

## Who Should Attend

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

## You Will Receive With This Course:

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

## Obtaining Your CISSP® Certification Consists of:

- ▶ Fulfilling minimum requirements for professional work experience
- ▶ Completing the Candidate Agreement
- ▶ Review of your 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.**

**“I will become a CISSP again! I learned quite a bit outside of what’s required. Eric is inspiring me to take my career to another level! Great guy!”**

-Chimere Murrill, TASC

**“MGT414 offers a good top-level look at the information – it helps to know what to focus on.”**

-Paul Gunnerson, U.S. Army



## 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 Cybersecurity 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. @drecicole

### 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 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 and 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, and how they interact 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 and 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, and Physical (Environmental) Security

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

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



giac.org



DoDD 8570 Required  
sans.org/8570

### You Will Be Able To

- ▶ Understand the 10 domains of knowledge that are covered on the CISSP® exam
- ▶ Analyze questions on the exam in order to select the correct answer
- ▶ Apply the knowledge and testing skills learned in class to pass the CISSP® exam
- ▶ Apply the skills learned across the 10 domains to solve security problems when you return to work
- ▶ Understand and explain all of the concepts covered in the 10 domains of knowledge

Take advantage of SANS  
CISSP® Get Certified Program  
currently being offered.

[sans.org/special/  
cissp-get-certified-program](https://sans.org/special/cissp-get-certified-program)

# SANS Security Leadership Essentials For Managers with Knowledge Compression™

## Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 6:00pm (Days 1-4)

9:00am - 4:00pm (Day 5)

33 CPE/CMU Credits

Laptop NOT Needed

Instructor: G. Mark Hardy

▶ GIAC Cert: GSLC

▶ Masters Program

▶ DoDD 8570

**“Excellent instruction. I will be sending more managers to MGT512, and requesting Hardy.”**

-Jason Payne, Alert Logic

**“MGT512 is awesome! Lots of material covered, so I will need to go back and read the notes and study more. The course was very structured, relevant, and concise.”**

-Juan Canino, SWIFT

**“G. Mark Hardy was very knowledgeable on the subject matter and delivered the course material clearly.”**

-Carl Ford, Burke & Herbert Bank

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.

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.

## Knowledge Compression™

### Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class that 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!

## 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 their technical people are telling them



### G. Mark Hardy SANS Certified Instructor

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

### 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, and the Procurement Process

### 512.2 IP Concepts, Attacks Against the Enterprise, and Defense-in-Depth

You will learn about 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 also learn the methods of the 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 how 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 into 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.



giac.org



sans.edu



DoD 8570 Required  
sans.org/8570

**ATTEND REMOTELY**



**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.  
*More info on page 74.*

### You Will Be Able To

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

# IT Security Strategic Planning, Policy, and Leadership

Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 5:00pm

30 CPE/CMU Credits

Laptop Recommended

Instructors: Stephen Northcutt,

Frank Kim

► Masters Program



**Frank Kim**  
SANS Certified Instructor

Frank Kim is a security leader with over 16 years of experience in information security, risk management, and enterprise IT. He has a passion for developing security strategies and building teams focused on practical solutions to business risks. He currently serves as the curriculum lead for application security at the SANS Institute and is the author and an instructor for the Secure Coding in Java course. Frank is a popular public speaker and has presented at security, software development, and leadership events around the world.

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.

Another 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.

## 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.



**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. @StephenNorthcutt



### 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 that 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, or anyone assigned to review, write, assess or support security policy and procedure, can benefit from this section. 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 Policies, 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

### You Will Be Able To

- ▶ Calculate the half life of information
- ▶ Establish a strategic planning horizon appropriate for your organization
- ▶ Conduct any of the well-known environmental scans (SWOT, Porters 5, Pest and many others)
- ▶ Facilitate out-of-the-box thinking (brainstorming, reverse brainstorming, synergetics)
- ▶ Select between candidate initiatives and perform back-of-the-envelope planning
- ▶ Understand how policy is used and when it is needed or not needed
- ▶ Manage the policy creation process
- ▶ Develop policy for difficult topics such as social media
- ▶ Evaluate policy using using the SMART methodology
- ▶ Understand the use of leadership competencies in developing leadership skills
- ▶ Select a few competencies to work on to further your effectiveness



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

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop NOT Needed

Instructor: Jeff Frisk

▶ GIAC Cert: GCPM

▶ Masters Program



Recently updated course contents to fully prepare you for the 2014 PMP® Exam! The **SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** course is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide* (Fifth Edition) is provided to all participants. You can reference the guide and use your course material along with the knowledge you gain in class to prepare for the 2014 updated PMP® Exam and the GIAC Certified Project Manager Exam.

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

## Who Should Attend

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

**“I am in a role where I need to manage and contribute to a number of projects. The things I learned in MGT525 will have exponential benefits.”**

-Sandy Dunn, Hewlett Packard

**“MGT525 is solid project management training with real-world examples taught by an instructor with significant PM and technical knowledge.”**

-Rich Graves, Carleton College



### Jeff Frisk SANS Certified Instructor

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

### 525.1 Project Management Structure & Framework

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

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

### 525.2 Project Charter and Scope Management

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

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

### 525.3 Time and Cost Management

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

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

### 525.4 Communications and Human Resources

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

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

### 525.5 Quality and Risk Management

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

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

### 525.6 Procurement, Stakeholder Management and Project Integration

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

**Topics:** Contract Types; Make vs. Buy Analysis; Vendor Weighting Systems; Contract Negotiations; Stakeholder Communication and Stakeholder Management Strategies; Project Execution; Monitoring Your Project's Progress; Finalizing Deliverables; Forecasting and Integrated Change Control

### You Will Be Able To

- ▶ Recognize the top failure mechanisms related to IT and InfoSec projects, so that your projects can avoid common pitfalls
- ▶ Create a project charter that defines the project sponsor and stakeholder involvement
- ▶ Document project requirements and create a requirements traceability matrix to track changes throughout the project lifecycle
- ▶ Clearly define the scope of a project in terms of cost, schedule and technical deliverables
- ▶ Create a work breakdown structure defining work packages, project deliverables and acceptance criteria
- ▶ Develop a detailed project schedule, including critical path tasks and milestones
- ▶ Develop a detailed project budget including cost baselines and tracking mechanisms
- ▶ Develop planned and earned value metrics for your project deliverables and automate reporting functions
- ▶ Effectively manage conflict situations and build communication skills with your project team
- ▶ Document project risks in terms of probability and impact, and assign triggers and risk response responsibilities
- ▶ Create project earned value baselines and project schedule and cost forecasts



giac.org



sans.edu

# Auditing Networks, Perimeters, and Systems

Six-Day Program  
 Mon, Oct 20 - Sat, Oct 25  
 9:00am - 5:00pm  
 36 CPE/CMU Credits  
 Laptop Required  
 Instructor: David Hoelzer  
 ▶ GIAC Cert: GSNA  
 ▶ Masters Program  
 ▶ DoDD 8570

**“AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!”**

-Carlos Everfield, U.S. Army

**“Providing value to businesses is an important part of my company’s work. AUD507 is showing me ways to provide value. David’s professional experience is evident and his lecture style is entertaining and interactive.”**

-Michael Decker, CNS Security



## David Hoelzer SANS Faculty Fellow

David Hoelzer is the author of more than 20 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 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow in the Center for Cybermedia Research and also a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. 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\_hoelzer

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 specifically organized 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 helping management understand the relationship between the technical controls and the risks to the business that these controls address. 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 auditors 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



giac.org



sans.edu



DoDD 8570 Required  
 sans.org/8570

# Law of Data Security and Investigations

Five-Day Program  
 Mon, Oct 20 - Fri, Oct 24  
 9:00am - 5:00pm  
 30 CPE/CMU Credits  
 Laptop NOT Needed  
 Instructor: Benjamin Wright  
 ▶ GIAC Cert: GLEG  
 ▶ Masters Program

**“Coming from an intense IT operations background, it was extremely valuable to receive an understanding of my security role from a legal point of view.”**

-John Ochman, BD

**“LEG523 was an excellent use of time. Benjamin Wright knows material very well. He has excellent flow and is right on target with course description.”**

-Sharon O'Bryan, DeVry Inc

**“LEG523 provides a great foundation and introduction into the legal issues involving cybersecurity.”**

-Tracey Kinslow,  
 TN Air National Guard



## Benjamin Wright SANS Senior Instructor

Benjamin Wright is the author of several technology law books, including *Business Law and Computer Security*, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery and has been quoted in publications around the globe, from the Wall Street Journal to the Sydney Morning Herald. Mr. Wright is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for experience and advice on the law of cyber investigations and electronic payments. [@benjaminwright](#)

### **New legal tips on confiscating and interrogating mobile devices. Includes the public response by retailer Target since January 2014 to a major payment card security incident.**

New law on privacy, e-discovery, and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. The needed professional training is uniquely available in the LEG523 series of courses, including skills in the analysis and use of contracts, policies, and records management procedures.

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

This course covers the law of business, contracts, fraud, crime, IT security, IT liability and IT policy – all with a focus on electronically stored and transmitted records. The course also teaches investigators how to prepare credible, defensible reports, whether for cyber, forensics, incident response, human resources or other investigations.

This course provides training and continuing education for many compliance programs under InfoSec and privacy mandates such as GLBA, HIPAA, FISMA and PCI-DSS.

Each successive day builds upon lessons from the earlier days. The lessons will help any enterprise (public or private sector) cope with such problems as hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

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

This course adopts an increasingly global perspective. Non-U.S. professionals attend the LEG523 course because there is no training like it anywhere else in the world. A lawyer from a European police agency recently attended and expressed high praise for the course when it was over: Another lawyer – from the national tax authority in an African country – sought out the course because electronic filings, evidence and investigations have become so important to her work. Students like the European and African lawyers help the instructor, U.S. attorney Benjamin Wright, improve the course and include more non-U.S. content as he constantly revises it.

### **Who Should Attend**

- ▶ Investigators
- ▶ Security and IT professionals
- ▶ Lawyers
- ▶ Paralegals
- ▶ Auditors
- ▶ Accountants
- ▶ Technology managers
- ▶ Vendors
- ▶ Compliance officers
- ▶ Law enforcement
- ▶ Privacy officers
- ▶ Penetration testers



[giac.org](http://giac.org)



[sans.edu](http://sans.edu)

# Defending Web Applications Security Essentials

Six-Day Program

Mon, Oct 20 - Sat, Oct 25

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Dr. Johannes Ullrich

▶ GIAC Cert: GWEB

▶ Masters Program

**“What you don’t know about web app defense is most likely killing you and you wouldn’t know it.”**

-Michael Malarkey, Bank of America

**“This course really proved to me that ignorance is bliss. I learned a lot that I could immediately take back to the office.”**

-Shawn Shirley, Ferrum College



giac.org



sans.edu

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

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

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

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

**DEV522: Defending Web Applications Security Essentials** is intended for anyone tasked with implementing, managing, or protecting Web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, and auditors who are interested in recommending proper mitigations to web security issues and infrastructure security professionals who have an interest in better defending their web applications.

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

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

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

## Who Should Attend

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



## Dr. Johannes Ullrich SANS Senior Instructor

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

## Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program  
 Mon, Oct 20 - Thu, Oct 23  
 9:00am - 5:00pm  
 24 CPE/CMU Credits  
 Laptop Required  
 Instructor: Gregory Leonard  
 ▶ Masters Program

### Who Should Attend

- ▶ Developers who want to build more secure applications
- ▶ Java EE programmers
- ▶ Software engineers
- ▶ Software architects
- ▶ Application security auditors
- ▶ Technical project managers
- ▶ Senior software QA specialists
- ▶ Penetration testers who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options
- ▶ Developers who need to be trained in secure coding techniques to meet PCI compliance

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

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

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

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

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



sans.edu

## Secure Coding in .NET: Developing Defensible Applications

Four-Day Program  
 Mon, Oct 20 - Thu, Oct 23  
 9:00am - 5:00pm  
 24 CPE/CMU Credits  
 Laptop Required  
 Instructor: Eric Johnson  
 ▶ Masters Program

### Who Should Attend

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

- ▶ ASP.NET developers who want to build more secure web applications
- ▶ .NET framework developers
- ▶ Software engineers
- ▶ Software architects
- ▶ Developers who need to be trained in secure coding techniques to meet PCI compliance

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

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

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

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



sans.edu

Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 5:00pm

30 CPE/CMU Credits

Laptop Required

Instructor: Graham Speake

▶ GIAC Cert: GICSP

**Who Should Attend**

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- ▶ IT (includes operational technology support)
- ▶ IT security (includes operational technology security)
- ▶ Engineering
- ▶ Corporate, industry, and professional standards

**“Excellent content and very informative.”**

-Khalid Alsomaly, Saudi Aramco



giac.org

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

*The course will provide you with:*

- **An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints**
- **Hands-on lab learning experiences to control system attack surfaces, methods, and tools**
- **Control system approaches to system and network defense architectures and techniques**
- **Incident-response skills in a control system environment**
- **Governance models and resources for industrial cybersecurity professionals.**

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

Because of the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as does system reliability throughout the system lifecycle.

When personnel working in one of the domains above complete this course, they will have an appreciation, understanding and common language for industrial control system security that will enable them to work together with others in these domains to better secure their common ICS environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

***“ICS410 bridges the gap in knowledge between ICS and information security. It is useful to engineers and information security professionals.”***

—YEE CHING, E-COP (S) PTE LTD

**Graham Speake** SANS Instructor

Graham Speake is principal systems architect for Yokogawa Electric Corporation, ISCI Marketing Chair, and an IEC62443 editor. Graham is an engineer with over 30 years' experience, the last 15 of which have been in the industrial cybersecurity arena for both end-user companies and vendors. Graham has spent 10 years in BP looking at control systems security in both upstream and downstream business areas. Additionally, he has 5 years' experience in designing safety systems at Industrial Control Services. Graham is the author of a number of books and is a frequent contributor to magazine articles.



## HOSTED COURSES

SANS Hosted is a series of courses presented by other educational providers to complement your needs for training outside of our current course offerings.

### HOSTED

## (ISC)<sup>2</sup>® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program

Five-Day Program

Mon, Oct 20 - Fri, Oct 24

9:00am - 5:00pm

35 CPE/CMU Credits

Laptop NOT Needed

Instructor: (ISC)<sup>2</sup> Staff

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.

**Notice:** Please note that the price of tuition does NOT include the CSSLP® exam.

### Who Should Attend

- ▶ Software architects
- ▶ Software engineers/designers
- ▶ Software development managers
- ▶ Requirements analysts
- ▶ Project managers
- ▶ Business and IT managers
- ▶ Auditors
- ▶ Developers and coders
- ▶ Security specialists
- ▶ Auditors and quality-assurance managers
- ▶ Application owners

### HOSTED

## Offensive Countermeasures: The Art of Active Defenses

Two-Day Program

Sun, Oct 26 - Mon, Oct 27

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop Required

Instructors: John Strand,  
Mick Douglas

Active Defenses have been capturing a large amount of attention in the media lately. There are those who thirst for vengeance and want to directly attack the attackers. There are those who believe that any sort of active response directed at an attacker is wrong. We believe the answer is somewhere in between.

You will learn how to force an attacker to take more moves to attack your network – moves that can increase your ability to detect them. You will learn how to gain better attribution as to who is attacking you and why. You will also find out how to get access to a bad guy's system. And most importantly, you will find out how to do the above legally.

### Who Should Attend

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

### HOSTED

## Physical Penetration Testing – Introduction

Two-Day Program

Sun, Oct 26 - Mon, Oct 27

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop NOT Needed

Instructor: Deviant Ollam

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions.

You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

You will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company's security posture or to augment their career as a penetration tester.

### Who Should Attend

- ▶ Penetration testers
- ▶ Security auditors
- ▶ IT professionals responsible for infrastructure oversight

### HOSTED

## Embedded Device Security Assessments for the Rest of Us

Two-Day Program | Sun, Oct 26 - Mon, Oct 27 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Paul Asadoorian

The Internet of Things has grown large enough to affect us all in a variety of ways (both positively and negatively!). The goal of this course is to enable you to uncover embedded systems vulnerabilities as part of your duties as a security professional.

SECURITY 440

**Critical Security Controls: Planning, Implementing and Auditing**

Two-Day Course | Sun, Oct 26 - Mon, Oct 27 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop NOT Needed | Instructor: James Tarala

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

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

SECURITY 546

**IPv6 Essentials**

Two-Day Course | Sun, Oct 26 - Mon, Oct 27 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop Required | Instructor: Dr. Johannes Ullrich

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how to apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.



SECURITY 580

**Metasploit Kung Fu for Enterprise Pen Testing**

Two-Day Course | Sun, Oct 26 - Mon, Oct 27 | 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.

MANAGEMENT 305

**Technical Communication and Presentation Skills for Security Professionals**



One-Day Course | Sun, Oct 19 | 9:00am - 5:00pm

6 CPE/CMU Credits | Laptop Required

Instructor: David Hoelzer

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Attendees will also get a crash course on advanced public speaking skills.



sans.edu

MANAGEMENT 415

**A Practical Introduction to Risk Assessment**

One-Day Course | Sun, Oct 19 | 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 it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.



MANAGEMENT 433

**Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program**

Two-Day Course | Sun, Oct 26 - Mon, Oct 27 | 9:00am - 5:00pm | 12 CPE/CMU Credits | Laptop NOT Needed | Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little, if anything, into securing the human element. As a result, people are now the weakest link; the simplest way for cyber attackers to hack into any organization is to target your employees. One of the most effective ways to secure the human element is to build an active awareness and education program that goes beyond just compliance and changes behaviors. In this challenging course you will learn how to do just that. You will learn the key concepts and skills needed to build, maintain and measure a high-impact

security awareness program. All course content is based on lessons learned from hundreds of organizations around the world. In addition, you will learn not only from extensive interaction with the instructor, but from working with your peers, as well. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so that you can immediately implement your own customized awareness program upon returning to your organization.

ATTEND REMOTELY



**SIMULCAST**

If you are unable to attend this event, this course is also available in SANS Simulcast.

More info on page 74.



sans.edu

# 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.

### **Real-Time Network Monitoring in Industrial Control Systems** *Graham Speake*

Industrial control systems have become more IT over the years. However, traditional IT monitoring tools are not designed and built with these real-time networks in mind. These networks are running TCP/IP, usually with special protocols not usually found on IT networks. New monitoring tools are now available that can visualize protocols that will enable non-IT engineers to easily monitor and spot erroneous traffic quickly and easily. This talk will explain the principals and demonstrate such a tool.

### **Evolving Threats** *Paul A. Henry*

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

### **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 its 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 these 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.

### **How Not to Suck at Pen Testing** *John Strand*

In this presentation, John will cover some key components that many penetration tests lack, including why it is important to get caught, why it is important to learn from real attackers, and how to gain access to organizations without sending a single exploit. Additionally, John will show you how to bypass “all powerful” white listing applications that are often touted as an impenetrable defense. Bit9? Palo Alto? Yea, we will talk about bypassing those too.

### **Sushi-Grade Smartphone Forensics on a Ramen Noodle Budget** *Heather Mahalik*

One of the biggest questions we get in FOR585 is “What can I do with open-source tools because my lab can’t afford to buy all of this equipment?” This talk will answer those questions specific to Android forensics. Acquisition, analysis, and memory capture are possible using open-source methods and tools. Is data missed if the examiner relies on open-source tools for Android forensics? A comparison of what is recovered from an Android using open-source and popular commercial tools will be discussed.

### **SANS 8 Mobile Device Security Steps**

*Christopher Crowley*

Every organization is challenged to rapidly deploy mobile device security. The SANS 8 Mobile Device Security Steps is a community-driven project to provide the most up-to-date information on the most effective strategies for securing mobile infrastructure. Chris Crowley will discuss the guidance provided in the 8 Steps, including user authentication and restricting unauthorized access, OS and application management, device monitoring, and key operational components for mobile device management.

### **The Law of Offensive Countermeasures, Active Defense or Whatever You Wanna Call It**

*Benjamin Wright*

The range of steps that a good guy might take relative to a bad guy is limited only by imagination. As our imagination invents new steps, we use metaphors like “honeypot,” “sinkhole” and “hacking back” to describe what’s going on. But when we try to fit these metaphors into law, confusion erupts. This presentation will only compound the confusion. Come join the raucous discussion.

### **The Great Browser Schism: How to Analyze IE10 & IE11** *Chad Tilbury*

Changes to Internet Explorer have been slowly occurring since Windows 7, but the introduction of IE10 with Windows 8 and IE11 with Windows 8.1 has been nothing short of cataclysmic. Take everything you knew about Internet Explorer and file it away, because it won’t help you now. This talk will cover Internet Explorer 10 & 11 artifact by artifact, giving you the tools and techniques necessary to do a full analysis. Learn to parse the ESE database, where your Index.dat files went, and why device synchronization will make browser forensics more important than ever (smart watch’s reminder list).

# BONUS SESSIONS

## Weaponizing Digital Currency

G. Mark Hardy

Satoshi Nakamoto wasn't stupid. In the early days, he (they) mined over 1,000,000 Bitcoins when nobody really cared. If Bitcoin continues to increase in value at the rate it did last year, someone will be holding a massive currency weapon. George Soros destabilized the British Pound in 1992 and made over \$1 billion profit. In the largest counterfeiting operation in history, Nazi Germany devised Operation Bernhard to destabilize the British economy by dropping millions of pounds from Luftwaffe aircraft. If the holder of the megabitcoin has a currency digital weapon that works frictionlessly in milliseconds, against whom will he target it? Can it destabilize an entire government? Can it be continuously reused for blackmail? What should governments be doing now to plan for this contingency and fight back? We'll discuss an entirely new class of information weapon – digital cryptocurrency – and how it might either change the course of history, or be relegated to the ash heap of failure.

## Malware Analysis Essentials Using REMnux

Lenny Zeltser

Though some tasks for analyzing Windows malware are best performed on Windows laboratory systems, there is a lot you can do on Linux with the help of free and powerful tools. REMnux is an Ubuntu distribution that incorporates many such utilities. This practical session presents some of the most useful REMnux tools. Lenny Zeltser, who teaches SANS' reverse-engineering malware course, will share how you can use the utilities installed on REMnux to:

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

If you haven't experimented with Linux-based tools for malware analysis, you've been missing out. And if you've been meaning to begin exploring the field of malware analysis, this talk will help you get started.

## The Bot Inside the Machine

Dr. Johannes Ullrich

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

## Windows Exploratory Surgery with Process Hacker

Jason Fossen

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

<http://processhacker.sourceforge.net>

Find complete details at [sans.org/event/network-security-2014/bonus-sessions](http://sans.org/event/network-security-2014/bonus-sessions)

## Vendor Expo

Wednesday, October 22, 2014

12:00pm - 1:30pm and 5:00pm - 7:00pm

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

## Vendor-Sponsored Lunch Sessions

Wednesday, October 22, 2014 | 12:00pm - 1:30pm

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

## Vendor-Sponsored Lunch & Learn Presentations

Throughout Network Security 2014, vendors will provide sponsored lunch presentations where attendees can interact with peers and receive education on vendor solutions. Take a break and get up-to-date on security technologies!

## Vendor Welcome Reception

Wednesday, October 22, 2014 | 5:00pm - 7:00pm

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





**You don't have to miss out on SANS' top-rated training. Attend your choice of seven popular courses remotely via SANS Simulcast!**

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.

**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.

The following  
NS 2014  
courses will be  
available via  
SANS Simulcast:

**LONG COURSES**

SEC401  
SEC501  
SEC502  
SEC503  
FOR572  
MGT512

**SHORT COURSE**

MGT433

To register for a Network Security 2014 Simulcast course, please visit [sans.org/event/network-security-2014/attend-remotely](http://sans.org/event/network-security-2014/attend-remotely)

**The information security field is growing and maturing rapidly.  
Are you positioned to grow with it?**

**A Master's Degree in Information Security from the SANS Technology Institute (STI) will help you build knowledge and skills in management or technical engineering.**

**Master's Degree Programs:**

- ▶ **M.S. IN INFORMATION SECURITY ENGINEERING**
- ▶ **M.S. IN INFORMATION SECURITY MANAGEMENT**

**Specialized Graduate Certificates:**

- ▶ **PENETRATION TESTING & ETHICAL HACKING**
- ▶ **INCIDENT RESPONSE**
- ▶ **CYBERSECURITY ENGINEERING (CORE)**

SANS Technology Institute, an independent subsidiary of SANS, is accredited by The Middle States Commission on Higher Education. 3624 Market Street | Philadelphia, PA 19104 | 267.285.5000 an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



Learn more at [sans.edu](http://sans.edu) | [info@sans.edu](mailto:info@sans.edu)



# 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 26 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



Get Certified at [giac.org](http://giac.org)



## SECURITY AWARENESS



For a free trial, visit us at [securingthehuman.org](http://securingthehuman.org)

### FOR THE 21<sup>ST</sup> CENTURY

End User - Utility - Engineer - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of computer-based training modules:
  - STH.End User is mapped against the Critical Security Controls.
  - STH.Utility fully addresses NERC-CIP compliance.
  - STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems.
  - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
  - Compliance modules cover various topics including PCI DSS, Red Flags, FERPA, and HIPAA, to name a few.
- Test your employees and identify vulnerabilities through STH.Phishing emails.

## Department of Defense Directive 8570 (DoDD 8570)

[sans.org/8570](http://sans.org/8570)



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 requirements.

### 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

### Compliance/Recertification

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

Go to [giac.org](http://giac.org) to learn more about certification renewal.

DoDD 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](mailto:8570@sans.org) or visit [sans.org/8570](http://sans.org/8570)

# FUTURE SANS TRAINING EVENTS

Information on all events can be found at [sans.org/security-training/by-location/all](http://sans.org/security-training/by-location/all)




SANS  
**San Antonio**  
San Antonio, TX  
Aug 11-16, 2014




**Security Awareness**  
SUMMIT & TRAINING  
Dallas, TX  
Sept 8-17, 2014



SANS  
**Cyber Defense**  
SUMMIT & TRAINING  
Nashville, TN  
Aug 13-20, 2014



SANS  
**Albuquerque**  
Albuquerque, NM  
Sept 15-20, 2014



SANS  
**Virginia Beach**  
Virginia Beach, VA  
Aug 18-29, 2014



SANS  
**Baltimore**  
Baltimore, MD  
Sept 22-27, 2014



SANS  
**Chicago**  
Chicago, IL  
Aug 24-29, 2014



SANS  
**Seattle**  
Seattle, WA  
Sept 29 - Oct 6, 2014



SANS  
**Crystal City**  
Arlington, VA  
Sept 8-13, 2014



SANS  
**Network Security**  
Las Vegas, NV  
Oct 19-27, 2014



**Retail Cyber Security**  
SUMMIT & TRAINING  
Dallas, TX  
Sept 8-17, 2014



SANS  
**Cyber Defense San Diego**  
San Diego, CA  
Nov 3-8, 2014



# FUTURE SANS TRAINING EVENTS

Information on all events can be found at [sans.org/security-training/by-location/all](http://sans.org/security-training/by-location/all)



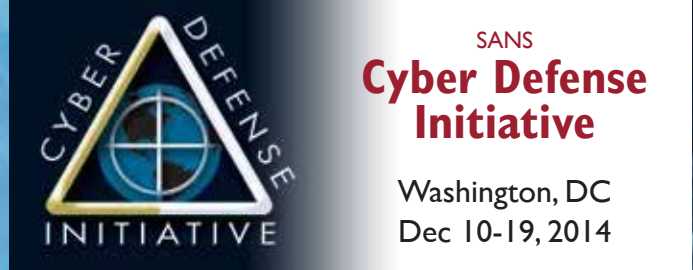
Fort Lauderdale, FL    Nov 3-8, 2014



SANS  
**Healthcare Cyber Security**  
SUMMIT & TRAINING  
San Francisco, CA  
Dec 3-10, 2014



Washington, DC    Nov 13-20



SANS  
**Cyber Defense Initiative**  
Washington, DC  
Dec 10-19, 2014

## SANS TRAINING FORMATS

### LIVE CLASSROOM TRAINING

### ONLINE TRAINING



#### Training Events

*Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with your Peers*  
[sans.org/security-training/by-location/all](http://sans.org/security-training/by-location/all)



#### OnDemand

*E-learning Available Anytime, Anywhere, at Your Own Pace*  
[sans.org/ondemand](http://sans.org/ondemand)



#### Community SANS

*Live Training in Your Local Region with Smaller Class Sizes*  
[sans.org/community](http://sans.org/community)



#### vLive

*Online Evening Courses with SANS' Top Instructors*  
[sans.org/vlive](http://sans.org/vlive)



#### OnSite

*Live Training at Your Office Location*  
[sans.org/onsite](http://sans.org/onsite)



#### Simulcast

*Attend a SANS Training Event without Leaving Home*  
[sans.org/simulcast](http://sans.org/simulcast)



#### Mentor

*Live Multi-Week Training with a Mentor*  
[sans.org/mentor](http://sans.org/mentor)



#### OnDemand Bundles

*Extend Your Training with an OnDemand Bundle Including Four Months of E-learning*  
[sans.org/ondemand/bundles](http://sans.org/ondemand/bundles)



#### Summit

*Live IT Security Summits and Training*  
[sans.org/summit](http://sans.org/summit)

# Hotel Information

## Training Campus

### Caesars Palace

3570 Las Vegas Blvd.

Las Vegas, NV 89109

[sans.org/event/network-security-2014/location](http://sans.org/event/network-security-2014/location)

The grandest of Las Vegas hotels, Caesars Palace is famous worldwide for its magnificent beauty and impeccable service. This majestic Las Vegas hotel offers a 129,000 square foot casino, 26 restaurants and cafes, sprawling gardens and pools, a world-class spa, and the renowned Colosseum spotlighting world-class stars.

### Special Hotel Rates Available

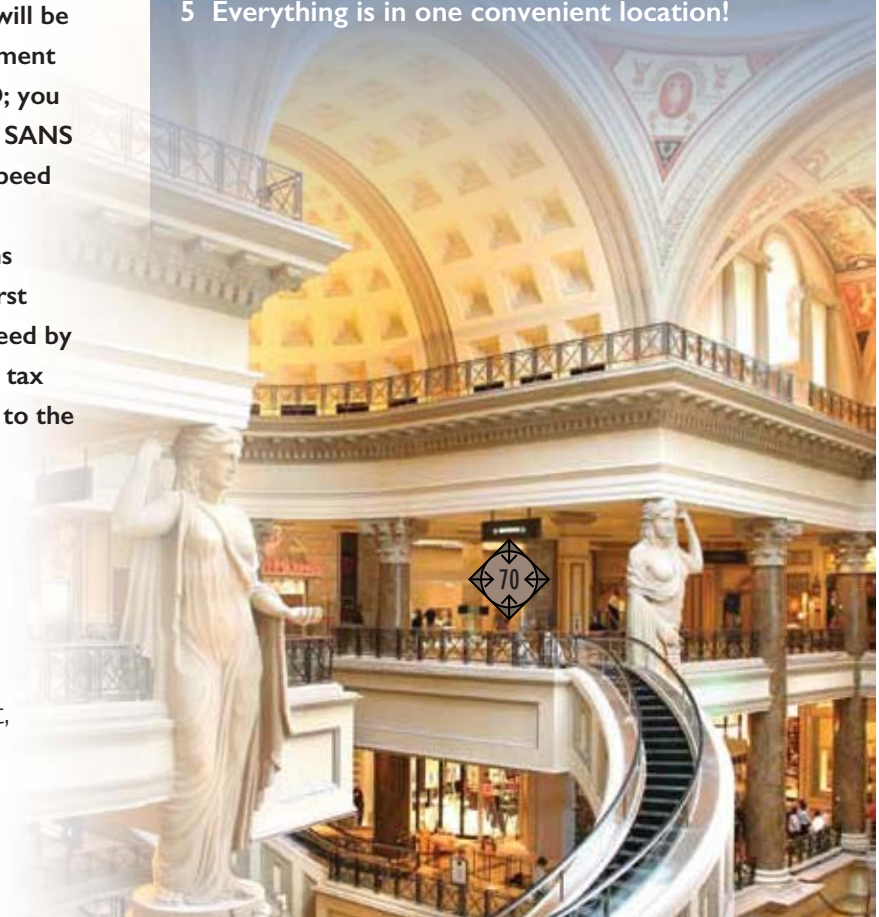
A special discounted Early Bird Rate of \$122.50 will be available until September 5, 2014. After that time, a discounted rate of \$175.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through September 24, 2014. All reservations must be guaranteed with a deposit for the first night's guestroom and tax charge. If guaranteed by a credit card, the first night's guestroom and tax charge, per room, will be billed immediately to the cardholder's account.

### Weather Conditions

October in Las Vegas is pleasant with highs around 82° and lows near 54°. For the latest weather conditions and forecast, please consult [weather.com](http://weather.com).

### Top 5 reasons to stay at Caesars Palace

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



# COME TO LAS VEGAS!

Dear Colleagues and Friends,

Network Security 2014 is back in Las Vegas right in the heart of the world famous strip! The city has so much to offer; you will find world-famous attractions, shows, restaurants, and shopping all within walking distance. SANS Network Security 2014 will be offering more courses, bonus sessions, and vendor events than ever before including NetWars, SANS' hands-on, interactive learning scenarios that enable you to develop and master real-world, in-depth skills. And we now offer a DFIR version of NetWars!

The training event will take place at Caesars Palace which is an attraction in itself! ([caesarspalace.com](http://caesarspalace.com)) **If you book by September 5th we have an additional 30% discount off of our already special group rate.**

This property features the Forum Shops with over 160 shops and 14 restaurants. The Garden of the Gods pool complex has five pools that span over 4.5 acres. The hotel has various dining options from high-end celebrity restaurants and an all-you-can-eat buffet (considered the best in Vegas) to the Market Street Grill, a food court that is quite popular for a quick bite!

Across the street from Caesars Palace is a brand new 550-foot tall observation wheel known as the largest in the world. It is part of a new dining and entertainment complex of LINQ ([caesars.com/linq](http://caesars.com/linq)), featuring bowling lanes, music venues, and an updated version of O'Shea's Irish Bar. Britney Spears is scheduled to perform at Planet Hollywood and Caesars Palace has a brand new Gordon Ramsey Pub and Grill.

Caesars Palace has the largest square footage of any hotel on the strip. **Since it will take approximately 10 minutes alone to get from the front door to your classroom, we highly recommend staying inside the hotel.** We also highly recommend you book early since we will not be able to guarantee our special group rate after the deadline. Most guest rooms at Caesars Palace are close to our classrooms, and you won't even need to walk through the casino. **As an extra treat, you will receive complimentary high-speed Internet – but only if you book under the special SANS group rate.**

Even though it will be warm outside, you still want to bring a jacket for the climate-controlled classrooms. You will also want to check out the SANS Network Security 2014 program guide for all of our events including more SANS@Night talks than ever. Please feel free to send me an email at [Brian@sans.org](mailto:Brian@sans.org) if I can be of any assistance with your travel plans.

*Brian Correia*

Director, Business Development & Venue Planning

## Five Reasons to Register

### 1. The best career move you will ever make!

That's how one SANS alumnus described the IT security education and networking opportunities offered by SANS. Attending Network Security 2014 is a way of investing in your career. To reap the maximum benefit, read the course descriptions carefully. Check out the five- and six-day courses plus a wide variety of one- to four-day skill-based short courses.

### 2. Why settle for second best?

If you want to increase your understanding of information security and become more effective in your job, you need to be trained by the best. "SANS provides by far the most in-depth security training with the true experts in the field as instructors," says Mark Smith, Costco Wholesale.

### 3. Challenge yourself!

Consider attempting GIAC (Global Information Assurance Certification), the industry's most respected technical security certification. GIAC is the only information security certification for advanced technical subject areas, including audit, intrusion detection, incident handling, firewalls and perimeter protection, forensics, hacker techniques, and Windows and Unix operating system security.

### 4. Become part of an elite group!

We're referring to the group of technical, security-savvy professionals who have had hands-on training through SANS. Material taught in the SANS courses directly applies to real-world challenges in your IT environment. "Six days of training gave me six months of work to do," says Steven Marscovetra of Norinchukin Bank. "It is amazing how much of the training I can apply immediately at work."

### 5. Don't miss out on a good opportunity!

This is your chance to make a great career move, be taught by the cream of the crop, challenge yourself, and become part of an elite group during a full week of IT security education and networking opportunities. Come prepared to learn; we will come prepared to teach.



# REGISTRATION INFORMATION

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

## How to Register

1. To register, go to [sans.org/event/network-security-2014/courses](http://sans.org/event/network-security-2014/courses).

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.

3. Print your invoice.

4. An email confirmation will arrive soon after you register.

## Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	8/27/14	\$400.00	9/17/14	\$200.00

Some restrictions apply.

## Group Savings (Applies to tuition only)

**10% discount** if 10 or more people from the same organization register at the same time

**5% discount** if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at [sans.org/security-training/discounts](http://sans.org/security-training/discounts) prior to registering.



To register for a Network Security 2014 Simulcast course, please visit [sans.org/event/network-security-2014/attend-remotely](http://sans.org/event/network-security-2014/attend-remotely)



## Group Discounts for SANS Security Training

[sans.org/vouchers](http://sans.org/vouchers)

### SANS Universal Voucher Credit Program

The **SANS Universal Voucher Credit Program** provides organizations of all sizes with a 12-month online account that is convenient and easy to manage. SANS will maximize your training investment by providing you with bonus credits. SANS Universal Voucher Credits can be used for any SANS live or online training format as well as GIAC certification exams. This will give you maximum flexibility and an easy one-time procurement process.



## Get GIAC Certified!

- Only \$599 when combined with SANS training
- Deadline to register at this price is the last day of SANS NS 2014
- Price goes to \$899 after deadline
- Register today at [registration@sans.org](mailto:registration@sans.org)

## Frequently Asked Questions

Frequently asked questions about SANS Training and GIAC Certification are posted at [giac.org/overview/faq.php](http://giac.org/overview/faq.php).

## Cancellation Policy

If an attendee must cancel, a substitution request may be made at any time. Processing fees will apply. All substitution requests must be submitted by email to [registration@sans.org](mailto:registration@sans.org).

If an attendee must cancel without substitution, a refund can be issued for any received payments. All cancellation requests must be submitted in writing by mail or fax and postmarked by Oct 1, 2014. Payments will be refunded by the method that they were submitted. Processing fees will apply. No refunds will be given after the stated deadline. Accessed online materials cannot be transferred to a substitute nor have payments refunded.

# NETWORK SECURITY 2014 REGISTRATION FEES

Register online at [sans.org/event/network-security-2014/courses](http://sans.org/event/network-security-2014/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 8/27/14	Paid by 9/17/14	Paid after 9/17/14	Add GIAC Cert	Add OnDemand
<input type="checkbox"/> SEC301	Intro to Information Security	\$3,995	\$4,195	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC401	Security Essentials Bootcamp Style	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC501	Advanced Security Essentials – Enterprise Defender	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC502	Perimeter Protection In-Depth	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC503	Intrusion Detection In-Depth	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC504	Hacker Techniques, Exploits, and Incident Handling	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC505	Securing Windows with the Critical Security Controls	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC506	Securing Linux/Unix	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC511	Continuous Monitoring and Security Operations <b>NEW!</b>	\$4,495	\$4,695	\$4,895		
<input type="checkbox"/> SEC542	Web Application Penetration Testing and Ethical Hacking	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC560	Network Penetration Testing and Ethical Hacking	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC561	Intense Hands-on Pen Testing Skill Development	\$4,695	\$4,895	\$5,095		
<input type="checkbox"/> SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	\$3,995	\$4,195	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC573	Python for Penetration Testers	\$3,995	\$4,195	\$4,395		
<input type="checkbox"/> SEC575	Mobile Device Security and Ethical Hacking	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC579	Virtualization and Private Cloud Security	\$4,695	\$4,895	\$5,095		<input type="checkbox"/> \$599
<input type="checkbox"/> SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC642	Advanced Web App Penetration Testing and Ethical Hacking	\$4,495	\$4,695	\$4,895		<input type="checkbox"/> \$599
<input type="checkbox"/> SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> SEC760	Advanced Exploit Development for Penetration Testers <b>NEW!</b>	\$4,695	\$4,895	\$5,095		
<input type="checkbox"/> FOR408	Windows Forensic Analysis	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> FOR508	Advanced Computer Forensic Analysis and Incident Response	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> FOR526	Memory Forensics In-Depth <b>NEW!</b>	\$4,695	\$4,895	\$5,095		<input type="checkbox"/> \$599
<input type="checkbox"/> FOR572	Advanced Network Forensics and Analysis <b>NEW!</b>	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> FOR585	Advanced Smartphone Forensics <b>NEW!</b>	\$4,695	\$4,895	\$5,095		<input type="checkbox"/> \$599
<input type="checkbox"/> FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	\$4,695	\$4,895	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	\$3,795	\$3,995	\$4,195	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	\$4,495	\$4,695	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> MGT514	IT Security Strategic Planning, Policy, and Leadership	\$3,995	\$4,195	\$4,395		<input type="checkbox"/> \$599
<input type="checkbox"/> MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	\$3,795	\$3,995	\$4,195	<input type="checkbox"/> \$599	
<input type="checkbox"/> AUD507	Auditing Networks, Perimeters, and Systems	\$4,270	\$4,470	\$4,670	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> DEV522	Defending Web Applications Security Essentials	\$4,270	\$4,470	\$4,670	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> LEG523	Law of Data Security and Investigations	\$3,995	\$4,195	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> ICS410	ICS/SCADA Security Essentials <b>NEW!</b>	\$3,995	\$4,195	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$599
<input type="checkbox"/> HOSTED	(ISC)® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program	\$3,145	\$3,145	\$3,145		
<b>Skill-Based Short Courses</b>		<b>If taking a 5-6 day course</b>				
<input type="checkbox"/> SEC440	Critical Security Controls: Planning, Implementing, and Auditing	\$1,250	\$2,000	\$2,000	\$2,000	
<input type="checkbox"/> SEC546	IPv6 Essentials	\$1,250	\$1,885	\$1,885	\$1,885	
<input type="checkbox"/> SEC580	Metasploit Kung Fu for Enterprise Pen Testing	\$1,250	\$1,885	\$1,885	\$1,885	
<input type="checkbox"/> MGT305	Technical Communication and Presentation Skills for Security Professionals	\$575	\$1,045	\$1,045	\$1,045	
<input type="checkbox"/> MGT415	A Practical Introduction to Risk Assessment	\$750	\$1,095	\$1,095	\$1,095	
<input type="checkbox"/> MGT433	Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program	\$1,250	\$1,885	\$1,885	\$1,885	
<input type="checkbox"/> DEV541	Secure Coding in Java/JEE: Developing Defensible Applications	N/A	\$3,550	\$3,750	\$3,950	<input type="checkbox"/> \$599
<input type="checkbox"/> DEV544	Secure Coding in .NET: Developing Defensible Applications	N/A	\$3,550	\$3,750	\$3,950	<input type="checkbox"/> \$599
<input type="checkbox"/> HOSTED	Offensive Countermeasures: The Art of Active Defenses	N/A	\$1,700	\$1,700	\$1,700	
<input type="checkbox"/> HOSTED	Physical Penetration Testing – Introduction	N/A	\$1,900	\$1,900	\$1,900	
<input type="checkbox"/> HOSTED	Embedded Device Security Assessments for the Rest of Us	N/A	\$1,900	\$1,900	\$1,900	
<input type="checkbox"/> SPECIAL	Core NetWars – Tournament Entrance Fee	FREE	\$1,249	\$1,249	\$1,249	
<input type="checkbox"/> SPECIAL	DFIR NetWars – Tournament Entrance Fee	FREE	\$1,249	\$1,249	\$1,249	

## Individual Courses Available

	MON 10/20	TUE 10/21	WED 10/22	THU 10/23	FRI 10/24	SAT 10/25
AUD507	<input type="checkbox"/> 507.1	<input type="checkbox"/> 507.2	<input type="checkbox"/> 507.3	<input type="checkbox"/> 507.4	<input type="checkbox"/> 507.5	<input type="checkbox"/> 507.6
LEG523	<input type="checkbox"/> 523.1	<input type="checkbox"/> 523.2	<input type="checkbox"/> 523.3	<input type="checkbox"/> 523.4	<input type="checkbox"/> 523.5	
SEC301	<input type="checkbox"/> 301.1	<input type="checkbox"/> 301.2	<input type="checkbox"/> 301.3	<input type="checkbox"/> 301.4	<input type="checkbox"/> 301.5	
SEC401	<input type="checkbox"/> 401.1	<input type="checkbox"/> 401.2	<input type="checkbox"/> 401.3	<input type="checkbox"/> 401.4	<input type="checkbox"/> 401.5	<input type="checkbox"/> 401.6
SEC501	<input type="checkbox"/> 501.1	<input type="checkbox"/> 501.2	<input type="checkbox"/> 501.3	<input type="checkbox"/> 501.4	<input type="checkbox"/> 501.5	<input type="checkbox"/> 501.6
SEC503	<input type="checkbox"/> 503.1					
SEC504	<input type="checkbox"/> 504.1					
SEC505	<input type="checkbox"/> 505.1	<input type="checkbox"/> 505.2	<input type="checkbox"/> 505.3	<input type="checkbox"/> 505.4	<input type="checkbox"/> 505.5	<input type="checkbox"/> 505.6

## Individual Course Day Rates If Not Taking a Full Course

<input type="checkbox"/> One Full Day	\$1,350
<input type="checkbox"/> Two Full Days	\$2,145
<input type="checkbox"/> Three Full Days	\$3,025
<input type="checkbox"/> Four Full Days	\$3,952
<input type="checkbox"/> Five Full Days	\$4,395
<input type="checkbox"/> Six Full Days	\$5,100
<input type="checkbox"/> Seven Full Days	\$5,475
<input type="checkbox"/> Eight Full Days	\$5,995

RE M I N D E R : When you register, please use the promo code located on the back cover.



SANS is the most trusted and by far the largest source for information security training, certification, and research in the world.

## Five Tips to Get Approval for SANS Training

### 1. EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (inside cover) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.
- Note that the core, job-based courses can be complemented by short, skill-based courses of one or two days. We also offer deep discounts for bundled course packages. Consider a *GIAC Certification*, which will show the world that you have achieved proven expertise in your chosen field.

### 2. RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Promise to share what you've learned with your colleagues.

### 3. SAVE

- The earlier you sign up, the more you save, so explain the benefit of signing up early.
- Save even more with group discounts! See inside for details.



Scan the QR code and register by August 27th to **SAVE \$400** on SANS NS 2014 courses.

[sans.org/info/160227](http://sans.org/info/160227)

### 4. ADD VALUE

- Share with your boss that you can add value to your enterprise by meeting with network security experts – people who face the same type of challenges that you face every single day.
- Explain how you will be able to get and share great ideas on improving your IT productivity and efficiency.
- Enhance your SANS training experience with *SANS@Night* talks and the *Vendor Expo*, which are free and only available at live training events.
- Take advantage of the special SANS host-hotel rate so you will be right where the action is!

### 5. ACT

- With the fortitude and initiative you have demonstrated thus far, you can confidently seek approval to attend SANS training!

**Return on Investment:** SANS training events are recognized as the best place in the world to get information security education. With SANS, you will gain significant returns on your InfoSec investment. Through our intensive immersion classes, our training is designed to help your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited.

**Remember:** SANS is your first and best choice for information and software security training. The SANS Promise is “You will be able to apply our information security training the day you get back to the office!”