

SANS

THE MOST TRUSTED NAME IN INFORMATION
AND SOFTWARE SECURITY TRAINING

SANS 2014
will be held at the
**Walt Disney
World Dolphin
Resort**

*"One of the most relevant
and informational
courses I've ever taken.
I'll be back for more. "*

-RACHEAL STRIDER, PATELCO CREDIT UNION



GIAC Approved Training

Register at
**[www.sans.org/
sans-2014](http://www.sans.org/sans-2014)**

2014

Orlando, FL

April 5-14, 2014

*Our most comprehensive information security
training event of the year...something for everyone!*

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Computer Forensic Investigations – Windows In-Depth

Web App Penetration Testing and Ethical Hacking

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

*And more than 30 additional courses in
network and software security, forensics, software development,
legal, management, and IT audit.*

**Save \$400
by registering early!**
See page 80 for more details.



SANS IT SECURITY TRAINING AND YOUR CAREER ROADMAP

SECURITY CURRICULUM

Beginners

SEC301 NOTE:

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

SEC301
Intro to
Information Security
GISF

Penetration Testing

SEC401
Security Essentials Bootcamp Style
GSEC

SEC504
Hacker Techniques, Exploits, and
Incident Handling
GCIH

SEC560
Network Pen
Testing and
Ethical Hacking
GPEN

SEC542
Web App Pen
Testing and
Ethical Hacking
GWAPT

SEC561
Hands-on Pen Testing
Skill Development

SEC573
Python for Penetration
Testers

SEC575
Mobile Device
Security and
Ethical Hacking
GMOB

SEC660
Advanced Pen
Testing, Exploits,
and Ethical Hacking
GXPN

SEC642
Advanced Web
App Pen Testing
and Ethical
Hacking

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

SEC617
Wireless Ethical
Hacking, Pen Testing,
and Defenses
GAWN

SEC760
Advanced Exploit
Development

Incident Handling

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials –
Enterprise Defender
GCED

SEC504
Hacker Techniques, Exploits,
and Incident Handling
GCIH

FOR508
Advanced Computer Forensic
Analysis & Incident Response
GCFA

Intrusion Analysis

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security
Essentials –
Enterprise Defender
GCED

SEC502
Perimeter
Protection
In-Depth
GPPA

SEC503
Intrusion
Detection
In-Depth
GCIA

FOR508
Advanced Computer
Forensic Analysis &
Incident Response
GCFA

System Administration

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security
Essentials –
Enterprise Defender
GCED

SEC505
Securing Windows
and Resisting
Malware
GCWN

SEC579
Virtualization
and Private Cloud
Security

SEC506
Securing
Linux/Unix
GCUX

Network Security

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security
Essentials –
Enterprise Defender
GCED

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

SEC540
VoIP and Unified
Communications
Security

AUDIT CURRICULUM

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

AUD507
Auditing Networks,
Perimeters, and Systems
GSNA

Specialized Audit Courses

AUD444
Auditing Security and
Controls of Active Directory
and Windows

AUD445
Auditing Security
and Controls of
Oracle Databases

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

MANAGEMENT CURRICULUM

SEC301
Intro to
Information Security
GISF

SEC401
Security Essentials
Bootcamp Style
GSEC

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

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

Specialization

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

MGT433
Securing The Human:
How to Build,
Maintain and Measure
a High-Impact
Awareness Program

MGT514
IT Security
Strategic
Planning,
Policy, and
Leadership

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

DEVELOPER CURRICULUM

Core

**STH.
DEVELOPER**
Application Security
Awareness Modules
[www.securingthehuman.org/
developer](http://www.securingthehuman.org/developer)

DEV522
Defending Web
Applications
Security Essentials
GWEB

Secure Coding

DEV541
Secure Coding
in Java/JEE
GSSP-JAVA

DEV544
Secure Coding
in .NET
GSSP-.NET

DEV543
Secure Coding
in C & C++

Specialization

SEC542
Web App Pen Testing
and Ethical Hacking
GWAPT

SEC642
Advanced Web App
Pen Testing and
Ethical Hacking

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

FORENSICS CURRICULUM

Core

FOR408
Computer Forensic Investigations –
Windows In-Depth
GCFE

SEC504
Hacker Techniques, Exploits,
and Incident Handling
GCIH

Advanced and In-Depth

FOR508
Advanced Computer
Forensic Analysis &
Incident Response
GCFA

FOR572
Advanced
Network Forensics
and Investigations

FOR610
Reverse Engineering
Malware: Malware Analysis
Tools & Techniques
GREM

Specialization

FOR526
Windows Memory Forensics
In-Depth

FOR585
Advanced Smartphone
and Mobile Device Forensics

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

LEGAL CURRICULUM

SEC401
Security Essentials
Bootcamp Style
GSEC

LEG523
Law of Data Security and
Investigations
GLEG



GIAC certification available
for courses indicated with
GIAC acronyms

We are pleased to invite you to **SANS 2014** from **April 5-14** in **Orlando, Florida**. We will be returning to the **Walt Disney World Dolphin** right in the heart of the Walt Disney World® Resort.

At SANS, we're serious about training. We want you to be successful at protecting your company's most important asset: its data. SANS instructors are industry experts who provide a unique brand of intensive, immersion-training courses designed to help you master the practical steps necessary to defend systems and networks. Register online today.

You will receive the best computer security training available anywhere, with more than 40 courses packed with immediately useful techniques and tools. SANS 2014 will also feature a number of new courses, including:

- **SEC503: Intrusion Detection In-Depth** (*Simulcast available*)
- **SEC561: Intense Hands-on Pen Testing Skill Development**
- **FOR572: Advanced Network Forensics and Analysis**
- **MGT415: A Practical Introduction to Risk Assessment**

Always on the cutting edge, our courses will give you the critical knowledge that you need right now.

During the evenings of April 10 and 11, we are offering **NetWars** and **DFIR NetWars**, an intense interactive, Internet-based competition for computer attacks and defenses. Show off your skills or gain them as you play! You must register, but both NetWars and DFIR NetWars are free with a 5-6 day course.

To complement your training, our **SANS@Night Series** features presentations on the most current topics in information security by some of the best speakers in the industry.

Have you considered what **GIAC Certification** can do for you? It's no secret that employers are looking for certified information security personnel, and they know that GIAC cert holders have strong, hands-on skills. Earn your credentials by signing up for a corresponding GIAC certification attempt when registering for your SANS course.

Do you need to meet **DoD Directive 8570** requirements? SANS 2014 offers seven courses that align with the requirements for **Baseline IA Certification**. See the DoD page for detailed information about how SANS courses help prepare you for your certification.

Have you thought about earning your master's degree? Some of the courses offered at SANS 2014 may count for either the **Masters of Science in Information Security Engineering** or the **Masters of Science in Information Security Management** once you apply to pursue your master's degree with the SANS Technology Institute. See the **STI Master's Degree** page to find out which courses at SANS 2014 may be used for your STI Master's Degree.

The event campus, the **Walt Disney World Dolphin**, is located between Epcot® and Disney's Hollywood Studios™ in the heart of the Walt Disney World® Resort. It is close to both Disney's Animal Kingdom® Theme Park and Magic Kingdom® Park. See the **Hotel Information** page to find out more.

At SANS 2014, you'll learn more than you can imagine and have countless opportunities to expand your network of security experts and friends. Start making your training and travel plans now and meet us at Disney in April! Register today for SANS 2014.

Our alumni of
SANS 2013 say it all:

**"I thoroughly
enjoyed FOR508. It
will be a massive
resource for me.
Thanks!"**

-CHRIS TORRENCE, BRUNSWICK

**"MGT433 has been
an eye-opening
experience and will
provide valuable
tools to take back
to the work place."**
-CRAIG MYERS, USACASCOM

**"This is my first
formal computer
training and
first SANS event.
Extremely valuable
and current
information was
shared from the
first day."**
-ERIC WATT,
U.S. NAVAL ACADEMY

**"This is my second
SANS workshop from
Eric Cole. The last
one was 9 years
ago and he is still
enthusiastic and
very up-to-date in
this field. Excellent!"**
-KYLE CUNNINGHAM,
MAYO CLINIC

Courses-at-a-Glance

Please check the website for an up-to-date course list at www.sans.org/event/sans-2014/schedule

	SAT 4/5	SUN 4/6	MON 4/7	TUE 4/8	WED 4/9	THU 4/10	FRI 4/11	SAT 4/12	SUN 4/13	MON 4/14
AUD444 Auditing Security and Controls of Active Directory and Windows			PAGE 58							
AUD445 Auditing Security and Controls of Oracle Databases					PAGE 58					
AUD507 Auditing Networks, Perimeters, and Systems			PAGE 50							
AUD521 Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant								PAGE 57		
DEV522 Defending Web Applications Security Essentials <i>SIMULCAST</i>			PAGE 52							
DEV541 Secure Coding in Java/JEE: Developing Defensible Applications			PAGE 53							
DEV544 Secure Coding in .NET: Developing Defensible Applications			PAGE 53							
FOR408 Computer Forensic Investigations - Windows In-Depth			PAGE 34							
FOR508 Advanced Computer Forensic Analysis & Incident Response			PAGE 36							
FOR526 Windows Memory Forensics In-Depth			PAGE 38							
FOR572 Advanced Network Forensics and Analysis <i>NEW!</i>			PAGE 40							
FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques			PAGE 42							
LEG523 Law of Data Security and Investigations			PAGE 54							
MGT305 Technical Communication and Presentation Skills for Security Pros	P59									
MGT414 SANS® +S™ Training Program for the CISSP® Certification Exam			PAGE 44							
MGT415 A Practical Introduction to Risk Assessment <i>NEW!</i>	P59									
MGT433 Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program <i>SIMULCAST</i>	PAGE 60									
MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™			PAGE 46							
MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep			PAGE 48							
MGT535 Incident Response Team Management	P60									
SEC301 Intro to Information Security			PAGE 2							
SEC401 Security Essentials Bootcamp Style <i>SIMULCAST</i>			PAGE 4							
SEC434 Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting	PAGE 56									
SEC501 Advanced Security Essentials – Enterprise Defender			PAGE 6							
SEC502 Perimeter Protection In-Depth			PAGE 8							
SEC503 Intrusion Detection In-Depth <i>NEW!</i> <i>SIMULCAST</i>			PAGE 10							
SEC504 Hacker Techniques, Exploits, and Incident Handling			PAGE 12							
SEC505 Securing Windows and Resisting Malware			PAGE 14							
SEC542 Web App Penetration Testing and Ethical Hacking			PAGE 16							
SEC546 IPv6 Essentials	PAGE 56									
SEC560 Network Penetration Testing and Ethical Hacking <i>SIMULCAST</i>			PAGE 18							
SEC561 Intense Hands-on Pen Testing Skill Development <i>NEW!</i>			PAGE 20							
SEC566 Implementing & Auditing the 20 Critical Security Controls – In-Depth			PAGE 22							
SEC575 Mobile Device Security and Ethical Hacking			PAGE 24							
SEC579 Virtualization and Private Cloud Security			PAGE 26							
SEC580 Metasploit Kung Fu for Enterprise Pen Testing								PAGE 57		
SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses			PAGE 28							
SEC642 Advanced Web App Penetration Testing and Ethical Hacking			PAGE 30							
SEC660 Advanced Penetration Testing, Exploits, and Ethical Hacking			PAGE 32							
HOSTED (ISC)²® (CSSLP®) CBK® Education Program			PAGE 55							
HOSTED Physical Penetration Testing - Introduction								PAGE 55		
NetWars – Tournament							PAGE 66			
DFIR NetWars Tournament							PAGE 67			

CONTENTS

Simulcast.....61	Securing The Human Program69	SANS Training Formats75
Bonus Sessions.....62	GIAC Certification.....70	Future SANS Training Events76
Vendor Events63	CyberTalent Program71	Hotel Information78
NetWars.....64	DoD Directive 8570 Information ..72	Come to Orlando.....79
SANS Security Operations Center 66	SANS Technology Institute73	Registration Information80
Cyber Defense Curriculum68	Cyber Guardian Program74	Registration Fees81

Intro to Information Security

Five-Day Program

Mon, Apr 7 - Fri, Apr 11

9:00am - 5:00pm

Laptop Required

30 CPE/CMU Credits

Instructor: Fred Kerby

▶ GIAC Cert: GISF

**COURSE NOW
INCLUDES
HANDS-ON LABS**

SANS

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

-Sherrie Audrict, Deltha Corporation

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

-Robert Smith, CMS

"Great crash-course and immersion for security and technology! From the logistics to the IS and OS, the necessary pieces of the cybersecurity puzzle have come together."

-Ansley LaBarre, EWA/IIT

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.

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



Fred Kerby SANS Senior Instructor

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

301.1 HANDS ON: A Framework for Information Security

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

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

301.2 HANDS ON: Securing the Infrastructure

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

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

301.3 HANDS ON: Cryptography and Security in the Enterprise

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

Topics: Cryptography (Cryptosystem Components, Cryptographic Services, Algorithms, Keys, Cryptographic Applications, Implementation); Security in the Enterprise (Organizational Placement, Making Security Possible, Dealing with Technology, Security Perspectives, Organizational Relationships, Building a Security Program); Wireless Network 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 security and how the ISO-OSI model may have an eighth layer (political) impacting communications and transmission. The day is replete with war stories from the trenches that illustrate the TSP protocol (the Tie to Sandal Protocol) used by successful security professionals worldwide.

Topics: The Site Security Plan; Computer Security; Application Security; Incident Handling; 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



www.giac.org

Security Essentials Bootcamp Style

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

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

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

Laptop Required

46 CPE/CMU Credits

Instructor: Dr. Eric Cole

▶ 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 is the best InfoSec training bar none. The value for the money is unbeatable!"

-Ron Fought,

Sirius Computer Solutions

"SEC401 is an eye opener to the broader aspects of network/Security admin roles. You see things from a different paradigm."

-Rod Campbell, CITEC



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.

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 students will have the skill sets to use the tools to implement effective security.

With the APT, organizations are going to be targeted. Whether the attacker is successful penetrating an organization's network depends on the organization's defense. While defending against attacks is an ongoing challenge with new threats emerging all of the time, including the next generation of threats, organizations need to understand what works in 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. Is it the most cost-effective way of reducing the risk?

Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security so that you will be prepared if you are given the responsibility for securing systems and/or organizations. This course meets both of the key promises SANS makes to our students: (1) You will gain cutting-edge knowledge you can put into practice immediately upon returning to work; and, (2) You will be taught by the best security instructors in the industry.

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

401.1 HANDS ON: Networking Concepts

A key way attackers gain access to a company's resources is through a network connected to the Internet. A company 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 dozens of other types of organizations are demanding to know what threats they are facing and what they can do to alleviate those threats. On this day, you will obtain a roadmap that will 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; Honeypots; 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 companies 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 of 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 create a virtual lab to test and evaluate tools/security of systems
- ▶ Create an effective policy that can be enforced within an organization and design a checklist that can be used 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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu



www.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 61.

Advanced Security Essentials – Enterprise Defender

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Paul A. Henry

▶ GIAC Cert: GCED

▶ Masters Program

“Great course. Best training I have attended. This is my first SANS course and I can’t wait to attend more.”

-Leonard Crull, MI ANG

“Very knowledgeable. Top-tier training and industry leading.”

-Herbert Monford, Regions Bank

“It identifies and demonstrates a wide variety of attack factors that can be leveraged to steal my company’s data.”

-Corey Bidne, USDA



Who Should Attend

- ▶ Students who have taken Security Essentials and want a more advanced 500-level course similar to SEC401
- ▶ People who have foundational knowledge covered in SEC401, do not want to take a specialized 500-level course, and still want 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 an organization, and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

A key theme is that prevention is ideal, but detection is a must. We need to be able to ensure that we constantly improve our security to prevent as many attacks as possible. This prevention/protection occurs on two fronts - externally and internally. Attacks will continue to pose a threat to an organization as data become more portable and networks continue to be porous. Therefore a key focus needs to be on data protection, securing our critical information no matter whether it resides on a server, in a robust network architecture, or on a portable device.

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

Finally, once an attack is detected we must react to it in a timely fashion and perform forensics. Understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.



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 companies focus on functionality. Achieving the proper balance between business drivers and core protection of information is difficult. On the first day students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

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

501.2 HANDS ON: Packet Analysis

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

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

501.3 HANDS ON: Pentest

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

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

501.4 HANDS ON: First Responder

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

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

501.5 HANDS ON: Malware

As security professionals continue to build more proactive security measures, attackers' methods will continue to evolve. A common way for attackers to target, control, and break into as many systems as possible is through the use of malware. Therefore it is critical that students understand what type of malware is currently available to attackers 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 companies works and how to respond to attacks
- ▶ Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- ▶ Understand the six steps in the incident handling process and be able to create and run an incident handling capability
- ▶ Learn how to use various tools to identify and remediate malware across your organization
- ▶ Create a data classification program and be able to deploy data loss prevention solutions at both a host and network level



www.giac.org



www.sans.edu

Perimeter Protection In-Depth

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Bryce Galbraith

▶ GIAC Cert: GPPA

▶ Cyber Guardian

▶ Masters Program

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 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 learn risk-management capabilities and even a bit of Zen empowerment.

The course starts by looking at common problems we need to resolve. 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. Then we'll learn how to control it on the wire. We focus on the underlying technology used by both good and bad products. 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 the next 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 learn how to deploy traffic control while avoiding some of the most common mistakes.

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

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

"The course is very valuable because it shows you the techniques and methods attackers use and how to defend against them."

-Curtis Greer, U.S. Navy

"SEC502 opened my eyes so wide it scared me!"

-George Scarborough,
Defense Logistics Agency

"As an analyst, these courses are the most relevant in the industry."

-Louis Robichaud,
Atlantic Lottery Corp.



Bryce Galbraith SANS Certified 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, he holds several security certifications and speaks at conferences around the world.



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: Common Threats; Windump/Tcpdump; OSI Layer 2; OSI Layer 3; Fragmentation; OSI Layers 4 and 5

502.2 HANDS ON: Firewalls, NIDS, and NIPS

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

Topics: Static Packet Filters; Stateful Packet Filters; Stateful Inspection Filtering; Intrusion Detection and Prevention; Proxies; Cisco IOS; IP Version 6 (IPv6)

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: Traffic Control Products; Building A Firewall Rulebase; Perimeter Assessment; Web Application and Database Firewalls; Firewall Log Analysis

502.4 HANDS ON: Host-Level Security

In the early days of the Internet it was possible to secure a network right at the perimeter. Modern-day attacks, however, are far more advanced and require a multi-layered approach to security. This does not mean the perimeter no longer serves a useful role; it's just that now it is only part of the equation. So today we focus on the security posture of our individual hosts, 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 Hosts and Services; Host-Based Intrusion Detection and Prevention; Vulnerability Assessment and Auditing; Forensics; Security Information Management

502.5 HANDS ON: Securing the Wire

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

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

502.6 HANDS ON: Perimeter Wrap-Up

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

Topics: Sizing Up A Network; Cool Tools; 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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu

Intrusion Detection In-Depth

NEW

SANS

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Mike Poor
 ▶ GIAC Cert: GCIA
 ▶ Cyber Guardian
 ▶ Masters Program
 ▶ DoDD 8570



Who Should Attend

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

“This course provides a good basis of knowledge and presents important tools which will be at the core of any intrusion analysis.”

-Thomas Kelly, DIA

“This course is valuable for anyone interested in IDS. Mike’s knowledge and willingness to help you understand the material are unlike any other training I’ve been to. Great course and instructor.”

-Dannie Arnold, U.S. Army

“Course was designed around real-world intrusions and is highly needed for network security administrators and/or analysts.”

-Hector Araiza, USAF

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

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

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

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



Mike Poor SANS Senior Instructor

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

503.1 HANDS ON: Fundamentals of Traffic Analysis: PART I

Day 1 provides a refresher or introduction 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; both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network access/link layer; IP Layer; IPv6

503.2 HANDS ON: Fundamentals of Traffic Analysis: PART II

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

The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days – Open Source IDS: Snort and Bro. Snort and Bro are widely deployed open source IDS/IPS solutions that have been industry standards for over a decade.

Topics: Operational life-cycle 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 Challenge where you find and analyze traffic to a vulnerable honeynet host using many of the same tools you mastered during the week. Students can work alone or in groups with or without workbook guidance. This is a great way to end the week 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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu



DoDD 8570 Required
www.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 61.

Hacker Techniques, Exploits, and Incident Handling

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

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

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

-Anthony Liu, Scotia Bank

"This class teaches you all of the hacking techniques that you need as an incident handler."

-Demonique Lewis, TerpSys

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

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

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

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

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

504.2 HANDS ON: Computer and Network Hacker Exploits – PART 1

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

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

504.3 HANDS ON: Computer and Network Hacker Exploits – PART 2

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

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

504.4 HANDS ON: Computer and Network Hacker Exploits – PART 3

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

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

504.5 HANDS ON: Computer and Network Hacker Exploits – PART 4

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

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

504.6 HANDS ON: Hacker Tools Workshop

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

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

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 to be able 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 choosing appropriate response actions based on each attacker's flood technique
- ▶ Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu



DoDD 8570 Required
www.sans.org/8570

Securing Windows and Resisting Malware

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Jason Fossen
 ▶ GIAC Cert: GCWN
 ▶ Cyber Guardian
 ▶ Masters Program

"If you think you know Windows, take this Windows security class – your review of your own skills and understanding will be challenged, for the better!!"

-Matthew Stoeckle,
 Nebraska Public Power District

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

-Orhella Swanston, DTRA-DOD

In April of 2014, Microsoft will stop releasing any new security patches for Windows XP. Like it or not, migrating off Windows XP is no longer optional, the clock is counting down. The **Securing Windows and Resisting Malware** course is fully updated for Windows Server 2012-R2, Server 2008-R2, Windows 8.1, and Windows 7.

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

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

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

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

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



Jason Fossen SANS Faculty Fellow

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

505.1 HANDS ON: Windows Operating System and Applications Hardening

We start by choosing malware-resistant software and Windows operating systems, then we regularly update that software, limit what software users can run, and then configure that software so that its exploitable features are disabled or at least restricted to work-only purposes. 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 to 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 (CA) 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 then see how to use RADIUS for securing access to WPA 802.11 wireless networks using PEAP and digital certificates from your PKI. Wireless security best practices will also be covered, including wireless tethering issues.

Topics: 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 the past, virtually everything can be managed from the command line and scripts now. Server 2012-R2, for example, has over 3000 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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu

Web App Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Kevin Johnson

▶ GIAC Cert: GWAPT

▶ Cyber Guardian

▶ Masters Program

SANS



Who Should Attend

- ▶ General security practitioners
- ▶ Penetration testers
- ▶ Ethical hackers
- ▶ Web application developers
- ▶ Website designers and architects

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.

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

-Brad Milhorn, ii2P LLC

"Without a doubt, this was the best class for my career."

-Don Brown, Lockheed Martin

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

-David Fava, The Boeing Company



Kevin Johnson SANS Senior Instructor

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

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

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

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

542.2 HANDS ON: Reconnaissance and Mapping

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

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

542.3 HANDS ON: Server-Side Discovery

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

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

542.4 HANDS ON: Client-Side Discovery

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

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

542.5 HANDS ON: Exploitation

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

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

542.6 HANDS ON: Capture the Flag

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

Topics: Capture the Flag

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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu

Network Penetration Testing and Ethical Hacking

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

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

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend."

-Mark Hamilton, McAfee

**ATTEND
REMOTELY**



SIMULCAST

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

More info on page 61.



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 which help train cyber warriors in 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 fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SEC560) and incident response (SEC504), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in 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.

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. **SANS SEC560: Network Penetration Testing and Ethical Hacking** truly prepares you to conduct successful penetration testing and ethical hacking projects. 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 detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course.

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

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

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

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

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

Who Should Attend

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

560.1 HANDS ON: Network Penetration Testing: Planning, Scoping, and Recon

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

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

560.2 HANDS ON: Network Penetration Testing: Scanning

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

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

560.3 HANDS ON: Network Penetration Testing: Exploitation and Post Exploitation

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

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

560.4 HANDS ON: Network Penetration Testing: Password Attacks

This component of the course turns our attention to password attacks, analyzing password guessing, password cracking, and pass-the-hash techniques in depth. Because passwords remain the dominant authentication scheme of most enterprises, professional penetration testers and ethical hackers need to understand how to find password weaknesses in a target environment. 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. We'll cover one of the best automated password-guessing tools available today, THC Hydra, and run it against target machines to guess Windows SMB and Linux SSH passwords. We'll then zoom in on the password representation formats for most major operating systems, discussing various cracking tools in-depth.

Topics: The primacy of passwords; Password attack tips; Account lockout and strategies; Password Guessing with THC-Hydra; Password representation formats in depth; John the Ripper features for penetration testers; Cain: The pen tester's dream tool; Rainbow table attacks in depth; Pass-the-hash attacks against Windows: Using hashes without even cracking a password

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

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

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

560.6 HANDS ON: Penetration Testing Workshop & Capture the Flag Event

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/sans-2014/courses

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 projects scope
- ▶ Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and less risk faced by an organization



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu

Intense Hands-on Pen Testing Skill Development

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

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

To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS top instructors engineered SANS SEC 561: 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 on in-class labs 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 hands-on 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 6 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 that they can apply the day that they get back to their jobs.

A lot of people can talk about these concepts, but this course teaches you how to actually do them hands-on and in-depth. The SANS SEC561 course 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 brand new, 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



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) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing.

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. Attendees 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 to you by the NetWars Scoring Server. By practicing the skills in a combination workshop where 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 Twenty Critical Security Controls – In-Depth

Five-Day Program

Mon, Apr 7 - Fri, Apr 11

9:00am - 5:00pm

30 CPE/CMU Credits

Laptop Required

Instructor: James Tarala

“This class is extremely valuable for any organization wanting to know where they stand on security.”

-David O'Brien, Costco

“James does an outstanding job of providing an overview of each control as well as offering his perspective and experience which adds a lot of value.”

-Danny Tomlinson, Kapstone Paper

Cybersecurity attacks are increasing and evolving so rapidly that 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 Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

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 to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

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

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

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

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

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

566.2 HANDS ON: Critical Controls 3, 4, 5, and 6

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)

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

–Bill Coffey, Shaw AFB

You Will Be Able To

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

Mobile Device Security and Ethical Hacking

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Joshua Wright

▶ GIAC Cert: GMOB

▶ Masters Program

“SEC575 offers invaluable material. Josh Wright’s energy and enthusiasm are incomparable!”

-Randy Pauli, Chelan County PUD

“With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations.”

-Dean Altman, Discount Tire



Joshua Wright SANS Senior Instructor

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational mission cyber warriors in the U.S. military, government agencies, and critical infrastructure providers.

Now covering BlackBerry 10, Apple iOS 7, and Android 4.3 devices

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

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

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

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

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and 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

575.1 HANDS ON: Mobile Device Threats, Policies, and Security Models

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

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

575.2 HANDS ON: Mobile Device Architecture Security & Management

With an understanding of the threats, architectural components and desired security methods, we can design and implement device and infrastructure systems to defend these threats. In this part of the course, we'll examine the design and deployment of network and system infrastructure to support a mobile phone deployment including the selection and deployment of Mobile Device Management (MDM) systems.

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

575.3 HANDS ON: Mobile Code and Application Analysis

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

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

575.4 HANDS ON: Ethical Hacking Mobile Networks

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

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

575.5 HANDS ON: Ethical Hacking Mobile Phones, Tablets, and Applications

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

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

575.6 HANDS ON: Secure Mobile Phone Capture the Flag

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

- Have the option to participate in multiple organizational roles related to mobile device security
- Design a secure infrastructure for the deployment of mobile phones
- Monitor network activity to identify attacks against mobile devices
- Extract sensitive data from a compromised iPad
- 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 www.sans.org/event/sans-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, Cycrypt, 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



www.giac.org



www.sans.edu

Virtualization and Private Cloud Security

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Dave Shackelford

“AWESOME class thus far. I will be able to take a lot back to apply to our Hyper-V environment!!!”

-Craig VanHuss, Crutchfield Corp.

“Class continues to be spot-on. I’m really enjoying class and taking a lot from it as it’s forcing me to think about architectural items we hadn’t considered as an organization.”

-Glenn Galang,
 Lake Villa District Library

“This is an essential course for anyone considering or developing a virtualized environment.”

-Barry Wudel, Fluor Corp.

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.

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

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 emphasis on security principles. Specific security-focused use cases for VDI, such as remote access and network access control, will be reviewed. We will take an in-depth look at virtual firewalls. Students will build a virtualized intrusion detection model; integrating promiscuous interfaces and traffic capture methods into virtual networks; and then setting up and configuring a virtualized IDS sensor. Attention will be paid to host-based IDS, with considerations for multitenant platforms.

579.3 HANDS ON: Virtualization Offense and Defense – PART 1

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

579.4 HANDS ON: Virtualization Offense and Defense – PART 2

This session is all about defense! We'll start off with an analysis 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. The majority of this session will focus on incident response and forensics in a virtualized or cloud-based infrastructure. We'll walk students through the 6-step incident response cycle espoused by NIST and SANS, and highlight exactly how virtualization fits into the "big picture." Students will discuss and analyze incidents at each stage, again with a focus on virtualization and cloud. We'll finish the incident response section with processes and procedures organizations can put to use right away to improve their awareness of virtualization-based incidents.

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

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

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

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

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Larry Pesce

▶ GIAC Cert: GAWN

▶ Cyber Guardian

▶ Masters Program

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

-John Fruge, B&W Technical Services

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, the threats, the exploits, and the defense techniques along with hands-on experience in evaluating and attacking wireless technology. Not limiting your skill-set to WiFi, you'll need to evaluate the threat from other standards-based and proprietary wireless technologies as well. This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques attackers use to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems. 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



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 environment.

Topics: Wireless LAN Assessment Techniques

617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

Students will continue their assessment of wireless security mechanisms, such as the identification and compromise of static and dynamic WEP networks and 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

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

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

617.5 HANDS ON: Bluetooth, DECT and ZigBee Attacks

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

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

617.6 HANDS ON: Wireless Security Strategies and Implementation

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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu

Advanced Web App Penetration Testing and Ethical Hacking

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Justin Searle

"Thank you for offering this class. It has been a tremendous assistance to me in strengthening my web app pen testing skills. Kevin is awesome!"

-Mark Geeslin, Citrix

"Subject material is current. Instructor is a pro. Great stuff. I'll be back."

-Brian Houlihan,
 National Credit Union Administration

"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

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

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.

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



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. He is currently a certified instructor for the SANS Institute. 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).

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; Examine How to Use Burp Intruder to Effectively Fuzz Requests; Explore Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Learn Advanced Exploitation Techniques

642.2 HANDS ON: Discovery and Exploitation for Specific Applications

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 how techniques such as identifying what the encryption technique is to how to exploit various flaws within the encryption or hashing.

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

642.4 HANDS ON: Mobile Applications and Web Services

Web applications are no longer limited to the traditional HTML based interface. Web services and mobile applications have become more common and are regularly being used to attack client and organizations. As such, it has become very important that penetration testers understand how to evaluate the security of these systems. 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

Today, applications are using more security controls to help prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. These controls block many of the automated tools and simple techniques used to discover flaws today. On day 5 you will explore techniques used to map the control and how it is configured to block attacks. You'll be able to map out the rule sets and determine the specifics of how it detects attacks. This mapping will then be used to determine attacks that will bypass the control. You'll use HTML5, UNICODE and other encodings that will enable your discovery techniques to work within the protected application.

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

642.6 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. You will be able to use this both in the class and after leaving and returning to your jobs.

Advanced Penetration Testing, Exploits, and Ethical Hacking

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

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

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

Laptop Required

46 CPE/CMU Credits

Instructor: Stephen Sims

▶ GIAC Cert: GXPN

▶ Cyber Guardian

▶ Masters Program

"This course is an excellent tour into the advanced skills needed for current/effective penetration."

-Matthew Smith,

U.S. Dept. of Homeland Security

"Most comprehensive coverage of fuzzing. I would have signed up for the course for that alone."

-Adam Kliarsky,

Cedars-Sinai Medical Center

"The breadth and depth of information that this course covers in spectacular detail shines with the glory of a thousand suns."

-Jacob Horne, Dept. of Defense

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 advanced penetration concepts, and 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



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.

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; Utilize LSA Secrets and Service Accounts to Dominate Windows Targets; Dealing with Unguessable/Uncrackable Passwords; Leveraging Password Histories; Gaining Graphical Access; Expanding Influence to Non-Windows Systems

660.3 HANDS ON: Python, Scapy, and Fuzzing

Day three 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 (ASLR, 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



www.gjac.org



www.sans.org/cyber-guardian



www.sans.edu

Computer Forensic Investigations – Windows In-Depth

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Ovie Carroll
 ▶ GIAC Cert: GCFE
 ▶ Masters Program

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

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



<http://computer-forensics.sans.org>



Ovie Carroll SANS Certified Instructor

Ovie Carroll has over 20 years of federal law enforcement experience. Ovies was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national-level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit where he was responsible for all computer intrusion investigations and for providing all computer forensic analysis in support of USPS-OIG investigations. Ovies is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. In addition to his career fighting computer crime, Ovies has conducted investigations into a variety of offenses including murder, fraud, bribery, theft, gangs and narcotics.

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

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

This course covers the fundamental steps of the in-depth computer forensic and media exploitation methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 8 and Server 2008) you will be exposed to well-known computer forensic tools such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that students can take with them.



Who Should Attend

- ▶ Information technology professionals
- ▶ Incident response team members
- ▶ Law enforcement officers, federal agents, or detectives
- ▶ Media exploitation analysts
- ▶ Information security managers
- ▶ Information technology lawyers and paralegals
- ▶ Anyone interested in computer forensic investigations

What You Will Receive With This Course

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

408.1 HANDS ON: Digital Forensics Fundamentals and Evidence Acquisition

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

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

408.2 HANDS ON: CORE WINDOWS FORENSICS PART I – String Search, Data Carving, and E-mail Forensics

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

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

408.3 HANDS ON: CORE WINDOWS FORENSICS PART II – Registry and USB Device Analysis

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

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

408.4 HANDS ON: CORE WINDOWS FORENSICS PART II – 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; Forensically Files Containing Critical Digital Forensic Evidence; Windows Event Log Digital Forensic Analysis

408.5 HANDS ON: CORE WINDOWS FORENSICS PART IV – Web Browser Forensics

Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what 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 Digital Forensic Challenge and Mock Trial

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

Topics: Digital Forensic Case; Mock Trial

You Will Be Able To

- ▶ Perform proper Windows forensic analysis by applying key analysis techniques covering Windows XP through Windows 8
- ▶ Use full-scale forensic tools and analysis methods to detail every action a suspect accomplished on a Windows system, including how and who placed an artifact on the system, 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 analysis, Windows artifact analysis, and e-mail 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)
- ▶ Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information that the suspect was interested in finding and to accomplish damage assessments
- ▶ Use shellbags analysis tools to articulate every folder and directory that a user opened up while browsing the hard drive
- ▶ 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
- ▶ Learn event log analysis techniques and use them to determine when and how users logged into a Windows system via a remote session, at the keyboard, or simply by unlocking their screensaver
- ▶ Determine where a crime was committed using FTK Registry Viewer to pinpoint the geo-location of a system by examining connected networks, browser search terms, and cookie data
- ▶ Use Mandiant Web Historian, parse raw SQLite databases, and leverage browser session recovery artifacts and flash cookies to identify web activity of suspects, even if privacy cleaners and in-private browsing are used



www.giac.org



www.sans.edu



<http://computer-forensics.sans.org>

Advanced Computer Forensic Analysis and Incident Response

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: Rob Lee
 ▶ GIAC Cert: GCFA
 ▶ Cyber Guardian
 ▶ Masters Program
 ▶ DoDD 8570

“Excellent course, invaluable hands-on experience taught by people who not only know the tools and techniques, but know their quirkiness through practical, real-world experience.”

-John Alexander, US Army

“Totally awesome, relevant and eye opening. I want to learn more every day.”

-Matthew Britton,
 Blue Cross Blue Shield of Louisiana



<http://computer-forensics.sans.org>



Rob Lee SANS Faculty Fellow

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



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

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?

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

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

508.1 HANDS ON: Enterprise Incident Response

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

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

508.2 HANDS ON: Memory Forensics

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

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

508.3 HANDS ON: Timeline Analysis

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

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

508.4 HANDS ON: Deep Dive Forensics and Anti-Forensics Detection

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

Topics: Windows XP Restore Point Analysis; VISTA , Windows 7, Server 2008 Shadow Volume Copy Analysis; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; FAT/exFAT Filesystem Overview

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

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

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

508.6 HANDS ON: The Incident Response & Intrusion Forensic Challenge

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



www.giac.org



www.sans.org/cyber-guardian



www.sans.edu



DoDD 8570 Required
www.sans.org/8570

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 they have 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 timestamping, 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

Windows Memory Forensics In-Depth

Five-Day Program
 Mon, Apr 7 - Fri, Apr 11
 9:00am - 5:00pm
 30 CPE/CMU Credits
 Laptop Required
 Instructor: Alissa Torres

“The presentation, exercises, labs, and data provided are the best in the computer forensics industry.”

-Rebecca Passmore, FBI

“This is the best SANS course I have taken so far with the best instructor. I hope to take more classes in the future.”

-Jonathan Hinson, Duke Energy



<http://computer-forensics.sans.org>



Alissa Torres SANS Certified Instructor

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on 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.

Malware Can Hide, But It Must Run

Acquiring and analyzing physical memory is seen by Digital Forensics and Incident Response (DFIR) professionals as critical to the success of an investigation, whether it be a criminal case, employee policy violation, or enterprise intrusion. Investigators who are not looking 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.

Just as it is crucial to understand disk and registry structures in order 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 current case. 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 takes the DFIR professional through acquisition, validation, and memory analysis with hands-on, real-world, and malware-laden memory images. The course draws on best practices and recommendations from top experts in the DFIR field.

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.

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: Acquisition and Unstructured Memory Analysis

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

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

526.2 HANDS ON: Windows Memory Internals

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

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

526.3 HANDS ON: User Visible Structures

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

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

526.4 HANDS ON: Internal Structures in Memory

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

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

526.5 HANDS ON: Memory Forensics in the Real World Workbook – Windows Memory Forensics In-Depth – Hands-on Exercises

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

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

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructors: George Bakos &
Philip Hagen

You Will Receive

- ▶ Linux version of the SIFT Workstation Virtual Machine with over 500 digital forensics and incident response tools prebuilt into the environment, including network forensic tools added just for this course
- ▶ Windows Virtual Machine with preinstalled network forensic tools
- ▶ Windows 8 Standard Full Version License and Key for the Windows VMware Image
- ▶ Realistic case data to examine during class, from multiple sources including:
 - Network captures in pcap format
 - NetFlow data
 - Web proxy, firewall, and intrusion detection system logs
 - Network service logs
- ▶ 64GB USB disk loaded with case examples, tools, and documentation


<http://computer-forensics.sans.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 Forensic alumni from 408 and 508 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, tcpxtract, 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



George Bakos SANS Certified Instructor

George Bakos has been interested in computer security since the early 1980s when he discovered the joys of BBSs and corporate databases. These days he is Technical Director of Intelligence & Response and a Tech Fellow at Northrop Grumman, a global leader in Cybersecurity, Aerospace & Defense. While at the Institute for Security Technology Studies, George was the developer of Tiny Honeypot and the IDABench intrusion analysis system and led the Dartmouth Distributed Honeynet System, fielding deception systems and studying the actions of attackers worldwide. He developed and taught the U.S. Army National Guard's CERT technical curriculum and ran the NGB's Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams throughout the United States. A recognized authority in computer security, he has contributed to numerous books and open source software projects; been interviewed on radio, television, and online publications; briefed the highest levels of government; and been a member of the SANS Institute teaching faculty since 2001. Outside the lab, George enjoys the beauties of his home state, Vermont, through skiing, ice and rock climbing, and mountain biking.

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: Network Protocols and Commercial Network Forensics

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)

572.3 HANDS ON: Netflow Analysis and Wireless Network Forensics

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

572.4 HANDS ON: Logging, OPSEC, and Footprint

In this section, you will learn 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 attacker's 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

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop Required

Instructor: Lenny Zeltser

► GIAC Cert: GREM

► Masters Program

"Lenny Zeltser is an outstanding instructor who cares about his students. His expertise combined with his teaching skills makes for an outstanding class."

-Ryan Kelley, Diebold, Inc.

"This class gave me essential tools that I can immediately apply to protect my organization."

-Don Lopez, Valley National Bank



<http://computer-forensics.sans.org>

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

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

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

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

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss malware analysis tools and techniques of intermediate complexity. Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops, and functions. The course spends some time discussing essential aspects of x86 assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

Who Should Attend

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



Lenny Zeltser SANS Senior Instructor

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



610.1 HANDS ON: Malware Analysis Fundamentals

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

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

610.2 HANDS ON: Additional Malware Analysis Approaches

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

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

610.3 HANDS ON: Malicious Code Analysis

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

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

610.4 HANDS ON: Self-Defending Malware

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

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

610.5 HANDS ON: Malicious Documents and Memory Forensics

Day five starts by exploring common patterns of assembly instructions often used to gain initial access to the victim's computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner, and explore steps for analyzing malicious PDF documents with utilities such as Origami and PDF Tools. Another major topic covered in this section is the reversing of malicious Windows executables using memory forensics techniques. We will explore this topic with the help of tools such 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 reverse-engineer malware more efficiently.

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

610.6 HANDS ON: Malware Reverse-Engineering Tournament

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

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

You Will Be Able To

- ▶ Build an isolated 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 on Microsoft Windows
- ▶ Uncover and analyze malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- ▶ Control some aspect of the malicious program's behavior through network traffic interception and code patching
- ▶ Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- ▶ Bypass a variety of 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
- ▶ 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 contain and recover from the incident
- ▶ Utilize practical memory forensics techniques to examine capabilities of rootkits



www.giac.org



www.sans.edu

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

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 7:00pm (Day 1)

8:00am - 7:00pm (Days 2-5)

8:00am - 5:00pm (Day 6)

46 CPE/CMU Credits

Laptop NOT Needed

Instructor: Eric Conrad

▶ GIAC Cert: GISP

▶ DoDD 8570

“This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor’s knowledge and teaching skills are excellent.”

-Jeff Jones,
Constellation Energy Group

“This class focuses like a laser on the key concepts you’ll need to understand the CISSP exam. Don’t struggle with thousand page textbooks – let this course be your guide!”

-Carl Williams, Harris Corporation



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

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

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

Who Should Attend

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

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 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.



Eric Conrad SANS Certified Instructor

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

414.1 Introduction and Access Control

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

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

414.2 Telecommunications and Network Security

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

Topics: Domain 2: Telecommunications and Network Security

414.3 Information Security Governance & Risk Management and Software Development Security

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

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

414.4 Cryptography and Security Architecture & Design

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

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

414.5 Security Operations and Business Continuity & Disaster Recovery Planning

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

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

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

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

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



www.giac.org



DoDD 8570 Required
www.sans.org/8570

You Will Be Able To

- ▶ Understand the 10 domains of knowledge that are covered on the CISSP® exam
- ▶ Analyze questions on the exam and be able 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 back to work
- ▶ Understand and explain all of the concepts covered in the 10 domains of knowledge



SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program

Mon, Apr 7 - Fri, Apr 11

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

“Every IT security professional should attend no matter what their position. This information is important to everyone.”

-John Flood, NASA

“Gives a good understanding of what knowledge our employees need to have to be successful.”

-Teddie Steele,

State Department of FCU

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

Who Should Attend

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



G. Mark Hardy SANS Certified Instructor

G. Mark Hardy is founder and President of 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 GSEC, 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 & the Procurement Process

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

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

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

512.3 Secure Communications

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

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

512.4 The Value of Information

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

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

512.5 Management Practicum

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

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

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.

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.



www.giac.org



www.sans.edu



DoDD 8570 Required
www.sans.org/8570

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

Six-Day Program

Mon, Apr 7 - Sat, Apr 12

9:00am - 5:00pm

36 CPE/CMU Credits

Laptop NOT Needed

Instructor: Jeff Frisk

▶ GIAC Cert: GCPM

▶ Masters Program

“Within the first five minutes I knew this would be a very different (and welcomed) experience than prior training with other vendors. SANS’ attention to detail is evident in every slide.”

-Jayme Jordan, Raytheon

“I think this is an awesome course that provides the knowledge and tools that I can use right when I get back to work.”

-Johnny Matamoros Jr., Freeman



Updated course contents to help you prepare 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. This course has been recently updated to fully prepare you for the 2014 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical 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* 5th 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 *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the 2014 updated Project Management Professional (PMP®) Exam and the GIAC Certified Project Manager Exam.

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is 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



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 a certified SANS instructor and course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from The Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, 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 Base Lining; 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 management, 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 request 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 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 Projects 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 which 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, assign triggers and risk response responsibilities
- ▶ Create project earned value baselines and project schedule and cost forecasts



www.giac.org



www.sans.edu

Auditing Networks, Perimeters, and Systems

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 9:00am - 5:00pm
 36 CPE/CMU Credits
 Laptop Required
 Instructor: David Hoelzer
 ▶ GIAC Cert: GSNA
 ▶ Masters Program
 ▶ DoDD 8570

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

-Jay Russell, U.S. Navy

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

-Brooks Adams,
 Georgia Southern University



David Hoelzer SANS Faculty Fellow

David Hoelzer is a high-scoring SANS Fellow instructor and author of more than twenty sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA

Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. 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.

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

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

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

You'll be able to use what you learn immediately. Five of the six days in the course will either produce or provide you directly with a general checklist that can be customized for your audit practice. Each of these days includes hands-on exercises with a variety of tools discussed during the lecture sections so that you will leave knowing how to verify each and every control described in the class. Each of the five hands-on days gives you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theoretical, hands-on, and practical knowledge.

Who Should Attend

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

507.1 Effective Auditing, Risk Assessment, Reporting & Cloud Computing

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

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

507.2 HANDS ON: Auditing the Perimeter

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

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

507.3 HANDS ON: Web Application Auditing

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

Topics: Identify controls against information gathering attacks; Process controls to prevent hidden information disclosures; Control validation of the user sign-on process; Examining controls against user name harvesting; Validating protections against password harvesting; Best practices for OS and web-server configuration; How to verify session tracking and management controls; Identification of controls to handle unexpected user input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

507.4 HANDS ON: Advanced Windows Auditing

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

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

507.5 HANDS ON: Auditing Unix Systems

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will have the opportunity to explore, assess and audit Unix systems hands-on. Lectures describe the different audit controls that are available on standard Unix systems, as well as, access controls and security models.

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

507.6 HANDS ON: Audit the Flag: A NetWars Experience

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

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

You Will Be Able To

- ▶ Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- ▶ Conduct a proper network risk assessment to identify vulnerabilities and prioritize what will be audited
- ▶ Establish a well-secured baseline for computers and networks — a standard to conduct an audit against
- ▶ Perform a network and perimeter audit using a seven-step process
- ▶ Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- ▶ Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- ▶ Audit web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- ▶ Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain



www.giac.org



www.sans.edu



DoDD 8570 Required
www.sans.org/8570

Defending Web Applications Security Essentials

SANS

Six-Day Program
 Mon, Apr 7 - Sat, Apr 12
 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

ATTEND
REMOTELY



SIMULCAST

If you are unable to attend this event, this course is also available in SANS Simulcast.
 More info on page 61.

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



www.giac.org



www.sans.edu



Dr. Johannes Ullrich SANS Senior Instructor

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

Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program

Mon, Apr 7 - Thu, Apr 10

9:00am - 5:00pm

24 CPE/CMU Credits

Laptop Required

Instructor: Gregory Leonard

▶ GIAC Cert: GSSP-JAVA

▶ 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

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.



www.giac.org



www.sans.edu

Secure Coding in .NET: Developing Defensible Applications

Four-Day Program

Mon, Apr 7 - Thu, Apr 10

9:00am - 5:00pm

24 CPE/CMU Credits

Laptop Required

Instructor: Eric Johnson

▶ GIAC Cert: GSSP-.NET

▶ 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:

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

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 on the security controls built into the ASP.NET framework? **Secure Coding in ASP.NET** will answer these questions and far more.



www.giac.org



www.sans.edu

Law of Data Security and Investigations

Five-Day Program

Mon, Apr 7 - Fri, Apr 11

9:00am - 5:00pm

30 CPE/CMU Credits

Laptop NOT Needed

Instructor: Benjamin Wright

▶ GIAC Cert: GLEG

▶ Masters Program

“This course was an eye-opener to the various legal issues in data security. Practices I will use when back in office.”

-Albertus Wilson, Saudi Aramco

“Legal 523 is a great course to help the IT professional become aware of various laws, and the implications of the changing trends in cyber defense.”

-Betty Lambuth,

Info Tech Solutions & Security

“Its applicability to real-life cases depicts the practicality of the course.”

-Samson Okocha, National Identity Management Commission



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. Wright maintains a popular blog at <http://legal-beagle.typepad.com>.

New laws on privacy, e-discovery, and data security are creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. The needed professional training is uniquely available in SANS' 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 legal and security issues become even more interlocked.

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.

Day 1: Fundamentals of IT Security Law and Policy

Day 2: E-Records, E-Discovery and Business Law

Day 3: Contracting for Data Security & Other Technology

Day 4: The Law of IT Compliance: How to Conduct Investigations

- ▶ Lessons from day 4 will be invaluable to the effective and credible execution of any kind of investigation — internal, government, consultant, security incidents and the like. These lessons integrate with other tips on investigations introduced in other days of the LEGAL 523 course series.

Day 5: Applying Law to Emerging Dangers: Cyber Defense

- ▶ In-depth review of legal response to the major security breach at TJX.
- ▶ Learn how to incorporate effective public communications into your cybersecurity program.

These five days of integrated education—where each successive day builds upon lessons from the earlier day(s)—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 and bad publicity connected with IT security.

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

This course adopts an increasingly global perspective. Non-US professionals attend the 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 these help the instructor, US attorney Benjamin Wright, improve the course and include more non-US content as he constantly revises it.

This course is complementary to SANS' rigorous digital forensics program. Together, LEG523 and the SANS' digital forensics program provide professional investigators an unparalleled suite of training resources.

Who Should Attend

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



www.giac.org



www.sans.edu

HOSTED COURSES

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

HOSTED

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

Five-Day Program

Mon, Apr 7 - Fri, Apr 11
9:00am - 5:00pm
35 CPE/CMU Credits
Laptop NOT Needed
Instructor: ISC² 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.

The comprehensive (ISC)² CSSLP® CBK® Education program covers the following domains:

- **Secure Software Concepts** – security implications in software development
- **Secure Software Requirements** – capturing security requirements in the requirements gathering phase
- **Secure Software Design** – translating security requirements into application design elements
- **Secure Software Implementation/Coding** – unit testing for security functionality and resiliency to attack, and developing secure code and exploit mitigation
- **Secure Software Testing** – integrated QA testing for security functionality and resiliency to attack
- **Software Acceptance** – security implication in the software acceptance phase
- **Software Deployment, Operations, Maintenance and Disposal** - security issues around steady state operations and management of software

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

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

HOSTED

Physical Penetration Testing - Introduction

Two-Day Course

Sun, Apr 13 - Mon, Apr 14
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.

Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company's security posture or to augment their career as a penetration tester.

Who Should Attend

- ▶ Penetration testers, security auditors, IT professionals responsible for infrastructure oversight

SEC434

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

Two-Day Course

Sat, Apr 5 - Sun, Apr 6

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop Required

Instructor: Jake Williams

This first-ever dedicated log management class teaches system, network, and security logs and their analysis and management, and covers the complete lifecycle of dealing with logs: the whys, how's and whats.

You will learn how to enable logging and then how to deal with the resulting data deluge by managing data retention, analyzing data using search, filtering and correlation, and how to apply what you learned to key business and security problems. The class also teaches applications of logging to forensics, incident response and regulatory compliance.

In the beginning, you will learn what to do with various log types and provide brief configuration guidance for common information systems. Next, you will learn a phased approach to implementing a company-wide log management program, and go into specific log-related tasks that need to be done on a daily, weekly, and monthly basis in regards to log review and monitoring.

Everyone is looking for a path through the PCI DSS and other regulatory compliance maze and that is what you will learn in the next section of the course. Logs are essential for resolving compliance challenges; this class will teach you what you need to concentrate on and how to make your log management compliance-friendly. And people who are already using log management for compliance will learn how to expand the benefits of your log management tools beyond compliance.

You will learn to leverage logs for critical tasks related to incident response, forensics, and operational monitoring. Logs provide one of the key information sources while responding to an incident and this class will teach you how to utilize various log types in the frenzy of an incident investigation.

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

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

SEC546

IPv6 Essentials

Two-Day Course

Sat, Apr 5 - Sun, Apr 6

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop Required

Instructor:

Dr. Johannes Ullrich

(Bio is on page 52)

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the next years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

The Security Impact of IPv6

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.

What You Will Learn

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

“IPv6 is here and it's enabled. If you don't know how to control it on your network the rest of the world is going to do it for you.”

-Adam Jasionowski,
Holyoke Gas and Electric

SEC580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course

Sun, Apr 13 - Mon, Apr 14

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop Required

Instructor: Eric Conrad

(Bio is on page 42)

Many enterprises today face regulatory or compliance requirements that mandate regular penetration testing and vulnerability assessments. Commercial tools and services for performing such tests can be expensive. While really solid free tools such as Metasploit are available, many testers do not understand the comprehensive feature sets of such tools and how to apply them in a professional-grade testing methodology. Metasploit was designed to help testers with confirming vulnerabilities using an Open Source and easy-to-use framework. This course will help students get the most out of this free tool.

This class will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, according to a thorough methodology for performing effective tests. Students who complete the course will have a firm understanding of how Metasploit can fit into their penetration testing and day-to-day assessment activities. The course will provide an in-depth understanding of the Metasploit Framework far beyond simply showing attendees how to exploit a remote system. The class will cover exploitation, post-exploitation reconnaissance, token manipulation, spear-phishing attacks, and the rich feature set of the Meterpreter, a customized shell environment specially created for exploiting and analyzing security flaws.

The course will also cover many of the pitfalls that a tester may encounter when using the Metasploit Framework and how to avoid or work around them, making tests more efficient and safe.

“Wow!**Take this class!”**

-Todd Hick, BIMA

IT AUDIT SKILL-BASED COURSE

AUD521

Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant

Two-Day Course

Sun, Apr 13 - Mon, Apr 14

9:00am - 5:00pm

12 CPE/CMU Credits

Laptop Required

Instructor: David Hoelzer

(Bio is on page 50)

The payment card industry has been working over the past several years to formalize a standard for security practices that are required for organizations that process or handle payment card transactions. The fruit of this labor is the Payment Card Industry Data Security Standard (currently at version 2.0).

This standard, which started life as the Visa Digital Dozen, is a set of focused comprehensive controls for managing the risks surrounding payment card transactions, particularly over the Internet. Of course, compliance validation is one of the requirements. This course was created to allow organizations to exercise due care by performing internal validations through a repeatable, objective process. While the course will cover all of the requirements of the standard, the primary focus is on the technical controls and how they can be measured. Every student will leave the class with a toolkit that can be used to validate any PCI/DSS environment technically and the knowledge of how to use it.

“AUD521 was amazing.

Very informative and the instructor made the material interesting. Looking forward to my next SANS course!”

-Nancy Johnsen, Fortis Properties



- Outline how you are proving, discussing
- Provide at least five that could be with
- Instructor will be
- Kind suggestions

AUDIT444

Auditing Security and Controls of Active Directory and Windows

Three-Day Program
 Mon, April 7 - Wed, April 9
 9:00am - 5:00pm
 18 CPE/CMU Credits
 Laptop Required
 Instructors: Tanya Baccam &
 Bryan Simon

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

“AUD444 offers relevant theory backed by experience and great hands-on practice.”

-Bryan Camereno, Charles Schwab

Who Should Attend

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

AUDIT445

Auditing Security and Controls of Oracle Databases

Three-Day Program
 Thu, April 10 - Sat, April 12
 9:00am - 5:00pm
 18 CPE/CMU Credits
 Laptop Required
 Instructors: Tanya Baccam &
 Bryan Simon

“AUD445 covers the important knowledge needed to perform an effective Oracle database audit.”

-Gary Johnson,
 Colorado PERA

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

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

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

Who Should Attend

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



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, she 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 GCIF, 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.

Bryan Simon SANS Instructor

Bryan Simon is a cybersecurity professional with 23 years of experience in operational IT, and has specialized in IT security for the past 13 years. He has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks at national conferences and with the press on matters of cybersecurity. He has specialized expertise in vulnerability assessments, penetration testing, and auditing. He has received recognition for his work in IT security and was most recently profiled by McAfee as an IT Hero. Bryan's scholastic achievements have resulted in the honour of sitting as a current member of the Advisory Board for the SANS Institute, and his acceptance into the prestigious SANS Cyber Guardian program.

MGT305

Technical Communication and Presentation Skills for Security Professionals

One-Day Course
Sun, Apr 6
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Required
Instructor: G. Mark Hardy
(Bio is on page 44)

"Tips for impactful presentations and avoiding common errors were extremely valuable."

-Mark Allen, Scott and White



www.sans.edu

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

Writing reports is a task that many IT professionals struggle with, sometimes from the perspective of writing the report and other times from the perspective of having to read someone else's report! In the morning material we cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this material.

After writing a meaningful report, it is not uncommon to find that we must present the key findings from that report before an audience, whether that audience is our department, upper management, or perhaps even the entire organization. How do you transform an excellent report into a powerful presentation? We will work through a process that works to either condense a report into a presentation or can even be used to write a presentation from scratch that communicates your important thoughts in a meaningful and interesting way.

Writing the presentation is only half of the battle, though. How do you stand up in front of a group of five or even five thousand and speak? We will share tips and techniques of top presenters that you can apply to give the best presentation of your career. Additionally, students will have the opportunity to work up and deliver a short presentation to the class followed by some personal feedback from one of SANS' top speakers.

Who Should Attend

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

MGT415

A Practical Introduction to Risk Assessment

NEW

One-Day Course
Sun, Apr 6
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Required
Instructor: James Tarala
(Bio is on page 20)

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 all organizations, whether they do so in an organized manner or not, will make priority decisions on how best to defend their valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Who Should Attend

- ▶ Security engineers, compliance directors, managers, auditors — basically any SANS alumni
- ▶ Auditors
- ▶ Directors of security compliance
- ▶ Information assurance management
- ▶ System administrators

Topics

- ▶ Understanding Risk
- ▶ How to Perform a Simple Risk Assessment
- ▶ Risk Assessment Case Study
- ▶ Formal Risk Management Models and Tools



MGT433

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

Two-Day Course
Sat, Apr 5 - Sun, Apr 6
9:00am - 5:00pm
12 CPE/CMU Credits
Laptop NOT Needed
Instructor: Lance Spitzner



www.sans.edu

Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and changes to behaviors. In this challenging course you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant. In addition, you will develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.



Who Should Attend

- ▶ Security awareness training officers
- ▶ Chief Security Officers (CSOs) and security management
- ▶ Security auditors, governance, and compliance officers
- ▶ Training, human resources, and communications staff
- ▶ Organizations regulated by Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Family Educational Rights and Privacy Act (FERPA), Payment Card Industry-Data Security Standards (PCI-DSS), ISO/IEC 27001, Family Educational Rights and Privacy Act (FERPA), Sarbanes-Oxley Act (SOX), or any other compliance-driven standards
- ▶ Anyone responsible for planning, deploying, or maintaining an awareness program

MGT535

Incident Response Team Management

One-Day Course
Sun, Apr 6
9:00am - 5:00pm
6 CPE/CMU Credits
Laptop Recommended
Instructor: Alissa Torres

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

Who Should Attend

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

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

"Very useful information for existing or new IR teams."

-Dave Stock, The Mosaic Company





**You don't have to miss out on
SANS' top-rated training.
Attend your choice of five 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
SANS 2014
courses will be
available via
SANS Simulcast:**

LONG COURSES

**SEC401
SEC503
SEC560
DEV522**

SHORT COURSE

MGT433

**To register for a SANS 2014 Simulcast course, please visit
www.sans.org/event/sans-2014/attend-remotely**

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 Attacks Exposed: Network, Host, Memory, and Malware Analysis

Rob Lee, Ovie Carroll, Alissa Torres, Phil Hagen, and Lenny Zeltser

For many years, professionals have been asking to see real APT data in a way that shows them how the adversaries compromise and maintain presence on our networks. Now you can experience it first hand - using real data. The SANS Digital Forensics and Incident Response team will take you through an end-to-end investigation similar to briefs that are supplied to C-level executives who want to understand how their network was compromised and how these adversaries think, act, and move around their enterprise.

Starting with core steps in digital forensics, incident response, network forensics, memory analysis, and RE malware, instructors Ovie Carroll (FOR408: Digital Forensics), Rob Lee (FOR508: Incident Response), Alissa Torres (FOR526: Windows Memory Forensics), Phil Hagen (FOR572: Network Forensics), and Lenny Zeltser (FOR610: RE Malware) will walk through how key skills are used to solve a single intrusion for 20 minutes each. The tag team approach will detail how response teams can be leveraged in your environment to effectively respond to incidents in your enterprise.

This talk is perfect for those in the trenches or for those in management who really want to understand how a response team identifies and responds to these adversaries. What is it they are after? How did they get in? How did our systems fail to detect them? These questions and more will be answered in this one-of-a-kind keynote.

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>

How the West was Pwned

G. Mark Hardy

Can you hear it? The giant sucking sound to the East? With it are going more than just manufacturing jobs — it's our manufacturing know-how, intellectual property, military secrets, and just about anything you can think of. If we're so technologically advanced, how are the People's Republic of China (PRC) and others able to continue to pull this off? Why do we keep getting pwned at our own game?

There has been much talk about "cyberwar," but there may not be a war. If a victor can extract tribute from the vanquished, war isn't necessary. Today, intellectual capital is a proxy for tribute. We'll look at some specifics, including documents that outline the plan of attack, details about what operations have been run against us, and progress in efforts to create an international legal framework for when the bits start flying.

Effective Phishing that Employees Like

Lance Spitzner

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

Evolving VoIP Threats

Paul A. Henry

VoIP is thriving in an otherwise down economy. VoIP implementations are growing, driven by cost savings. Cost is typically the only consideration in the implementation of VoIP - it is all about saving money. Security, if considered at all, is clearly an afterthought. Too many still dismiss VoIP threats as theoretical. VoIP can afford significant costs savings while not sacrificing an organizations security. Recognizing the threats and implementing the compensating and technical controls can make all the difference in a successful VoIP implementation.

There's *GOLD* in Them Thar Package Management Databases!

Phil Hagen

There is a lot of useful file metadata stored in package management databases for popular Linux distributions. The RedHat Package Manager (RPM) and Debian's dpkg are two examples. We'll focus on how to leverage RPM in forensic investigations, as it can provide a quick and effective way to find changed files that warrant more in-depth analysis. We'll also discuss potential shortfalls to consider in using this method.

Passing the Hack: Raising Kids to Understand Security and the Hacker Mindset

Kevin and Brenna Johnson

In this presentation, Kevin Johnson of Secure Ideas, and his daughter Brenna will discuss how we need to build the next generation of hackers. Kevin and Brenna will explain how they have learned together and provide some tricks and ideas on teaching your kids how to be safe online while still encouraging the exploration necessary to build critical thinking and security knowledge.

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.

BONUS SESSIONS

Introduction to IDA Pro and Debugging

Stephen Sims

In this presentation, Stephen will discuss the most commonly used features and plugins for IDA Pro and WinDbg from an exploitation perspective. You will learn about IDA navigation, IDAPython and IDC scripting, remote debugging, and Kernel debugging. The presentation will be 50% lecture and 50% demonstration. Feel free to bring a demo or licensed version of IDA and WinDbg to play along.

Securing The Kids *Lance Spitzner*

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

Key takeaways include:

- Why securing kids online is harder than securing kids in the physical world
- Top three risks they face; strangers, friends and themselves
- Use of education to inform and secure them
- Use of a dedicated computer just for kids
- Kids Acceptable Use Policy
- Filtering and monitoring tools
- Additional lessons learned and resources to learn more.

Pillage the Village! *Mike Poor*

Many Penetration testers worry so much about pwn'ing this and getting domain admin on that, that they forget to pillage the boxes and networks they compromise. From hacking in-flight entertainment systems, web applications and hardware, we will go through examples from penetration tests where the hidden tidbits we found made the test.

Hacking Back, Active Defense and Internet Tough Guys *John Strand*

In this presentation John Strand will demonstrate the Active Defense Harbinger Distribution, a DARPA funded, free Active Defense virtual machine. He will debunk many of the myths, outright lies, and subtle confusions surrounding taking active actions against attackers. From this presentation, you will not only know how to take action against attackers, you will learn how to do it legally.

An Introduction to PowerShell for Security Assessments *James Tarala*

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

Vendor Expo

Wednesday, April 9, 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, April 9, 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 SANS 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, April 9, 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 using to address security threats in their organization. Attendees can visit sponsors to receive raffle tickets and enter to win exciting prizes. Prize drawings occur throughout the expo.



The NetWars Tournament and the DFIR NetWars Tournament will be held simultaneously at SANS 2014!

NETWARS TOURNAMENT

**A True Hands-On
Interactive Security
Challenge!**

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

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

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

Register at
www.sans.org/event/sans-2014/courses

NETWARS



DFIR NetWars is packed with challenges covering host forensics, network forensics, and malware and memory analysis. Each NetWars level is designed to not only exercise an individual's capabilities to solve a particular problem, but teach them proper analysis techniques regardless of the toolset they use. SANS DFIR NetWars is unique as it truly tests a blue team's capabilities to perform in real-world situations by solving a series of unique challenges commonly found during major incidents. DFIR NetWars also helps organizations evaluate performance and identify areas where their response teams might need to obtain additional knowledge.

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

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

**Challenge yourself
before the enemy does –
SANS DFIR NetWars**

**The NetWars
competitions
will be played
over two evenings:
April 10-11, 2014**

**Prizes will be awarded at the
conclusion of the games.
REGISTRATION IS LIMITED
AND IS FREE
for students attending any
long course at SANS 2014
(NON-STUDENTS ENTRANCE FEE IS \$1,249).**



Security Operations Center (SOC) Career Roadmap

SOC Background Description

Cybersecurity entity of an organization that is responsible for situational awareness and continuous monitoring of all assets in the enterprise's information infrastructure

SOC Education + Training

SANS + Formal Training = Qualified SOC Personnel Capable of:

- Timely and Proactive Detection of Attacks
- Proactive Prevention of Attacks
- Successfully Responding to and Remediating Incidents

SANS offers SOC Training in the following areas:

- Intrusion Detection/Cyber Defense
- Incident Response
- Penetration Testing/Vulnerability Assessment
- Digital Forensics Investigations and Media Exploitation

Check out the SOC Career Paths on the next page to:

- Select a Career Roadmap
- Maximize Career Opportunities
- Accelerate and Advance Career

SANS will put you on a Path To Success!

SANS Security Operations Training is flexible and offers:

- Single Courses that Enhance Skillset
- Multiple Courses Based on Logical Progression
- Across Specialized Areas:
 - Incident Response
 - Penetration Testing
 - Digital Forensics

SOC Diagram:
Specific task assigned to a SOC



Reasons to attend SANS 2014:

- ▶ **Expert Training** — SANS instructors are the industry leaders
- ▶ **Networking** — SOC reception
- ▶ **Thought Leadership** — SANS@Night talks
- ▶ **SAVE \$400** — Register and pay by Feb 12th and save \$400 on any 5- or 6-day course

Security Analyst

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials -
Enterprise Defender
GCED

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

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

SAMPLE JOB TITLES:

- Security Analyst
- Security Auditor
- Security Architect
- Security Engineer

Security Engineer

SEC401
Security Essentials Bootcamp Style
GSEC

SEC501
Advanced Security Essentials -
Enterprise Defender
GCED

SEC502
Perimeter
Protection
In-Depth
GCFW

SEC503
Intrusion
Detection
In-Depth
GCIA

SAMPLE JOB TITLES:

- Security Analyst
- Security Auditor
- Security Architect
- Security Engineer

Intrusion Analyst

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

SAMPLE JOB TITLES:

- System Administrators
- IDS Specialists
- Security Analysts/Specialists
- SOC Engineer
- Intrusion Detection Analysts

The Security Operations Center (SOC) is the focal point of cyber related incidents, security monitoring, and safe-guarding assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous monitoring, including monitoring traffic, blocking unwanted traffic from and to 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

NETWORK MONITORING

SEC503
Intrusion
Detection
In-Depth
GCIA

SEC502
Perimeter
Protection
In-Depth
GPPA

FOR572
Advanced
Network
Forensics and
Analysis

FOR578
Cyber-Threat
Intelligence

ENDPOINT MONITORING

SEC501
Advanced
Security
Essentials –
Enterprise
Defender
GCED

FOR508
Advanced
Computer
Forensic Analysis
and Incident
Response
GCFA

VULNERABILITY ASSESSMENT & PEN TESTING (VAPT)

SEC560
Network
Penetration Testing
and Ethical Hacking
GPPN

SEC660
Advanced
Penetration Testing,
Exploits, and
Ethical Hacking
GXPN

It is no longer news that targeted attacks are on the rise, organizations are being compromised, and attacks can go undetected for months. Smart organizations know that risk management is a key part of all security decisions, but many don't know where to start. The five-step Cyber Defense process outlined below will enable you to identify risk, determine the highest priorities, focus in on the areas that really matter, and measure progress against established baselines to improve your overall security posture.

STEP 1: Identify Critical Data

Align critical assets with threats and vulnerabilities to focus on risk

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

STEP 2: Align the Defense with the Offense

- 1 Reconnaissance
- 2 Scanning
- 3 Exploitation
- 4 Creating backdoors
- 5 Covering tracks

STEP 3: Know Thy Organization

If the offense knows more than the defense you will lose

Requirements:

- 1 Accurate up-to-date network diagram
- 2 Network visibility map
- 3 Configuration management and change control

STEP 4: Defense in Depth

There is no such thing as an unstoppable adversary

Requirements:

- 1 Inbound prevention
- 2 Outbound Detection
- 3 Log correlation
- 4 Anomaly detection

STEP 5: Common Metrics

Requirements:

Utilize the Critical Controls:

- 1 Offense informing the defense
- 2 Automation and continuous monitoring of security
- 3 Metrics to drive measurement and compliance

Five Key Steps to Cyber Defense

Providing curriculum options by job role in the areas of:

- ▶ Cybersecurity manager/officer
- ▶ Intrusion analyst/security operations center monitoring
- ▶ Operations management
- ▶ Security analyst
- ▶ Security engineer
- ▶ System/security administrator

Download your free roadmap brochure at cyber-defense.sans.org/training/roadmap

SANS2014 Cyber Defense Classes:

- ▶ SEC301 ▶ SEC401 ▶ SEC501
- ▶ SEC503 ▶ SEC566 ▶ MGT414

**SAVE
\$400**

Register and pay for a Cyber Defense course before Feb 12th and receive a \$400 discount!

For more information, contact:
cyber-defense@sans.org

SECURITY AWARENESS

FOR THE 21ST CENTURY

End User - Utility - Developer - Phishing

- Go beyond compliance and focus on changing behaviors.
- Create your own training program by choosing from a variety of modules:
 - STH.End User is mapped against the Critical Security Controls.
 - STH.Developer uses the OWASP Top 10 web vulnerabilities as a framework.
 - STH.Utility fully addresses NERC-CIP compliance.
 - 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.



For a free trial visit us at:
www.securingthehuman.org

How Are You Protecting Your

➤ **Data?**

➤ **Network?**

➤ **Systems?**

➤ **Critical
Infrastructure?**



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

Get GIAC certified!

GIAC offers over 27 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

"GIAC Certification demonstrates an applied knowledge versus studying a book."

-ALAN C, USMC

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





Contact Us to Learn More
www.sans.org/cybertalent

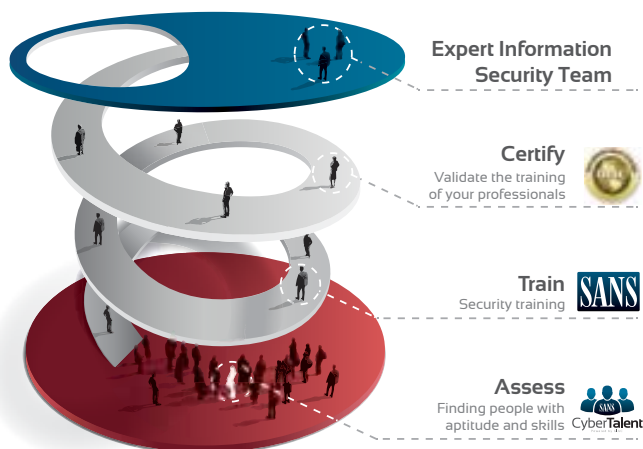
CyberTalent

Powered by GIAC



A Web-Based Recruitment and Talent Management Tool

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



Benefits of SANS CyberTalent Assessments

For Recruiting

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

For Talent Management

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

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

Department of Defense Directive 8570

(DoDD 8570)

www.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.

DoD Baseline IA Certifications

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

Computer Network Defense (CND) Certifications

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

Information Assurance System Architecture & Engineering (IASAE) Certifications

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

Computer Environment (CE) Certifications

GCWN	GCUX
-------------	-------------

Compliance/Recertification:

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

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

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 or visit www.sans.org/8570

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

WHAT'S YOUR NEXT CAREER MOVE?

SANS Technology Institute, an independent subsidiary of SANS,
is now 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.

*"It's great to learn
from an organization
at the forefront
of both academics,
and in the field."*

-JOSEPH FAUST,
MSISE PROGRAM

Two unique, respected master's degree programs:

**MASTER OF SCIENCE IN
INFORMATION SECURITY ENGINEERING**

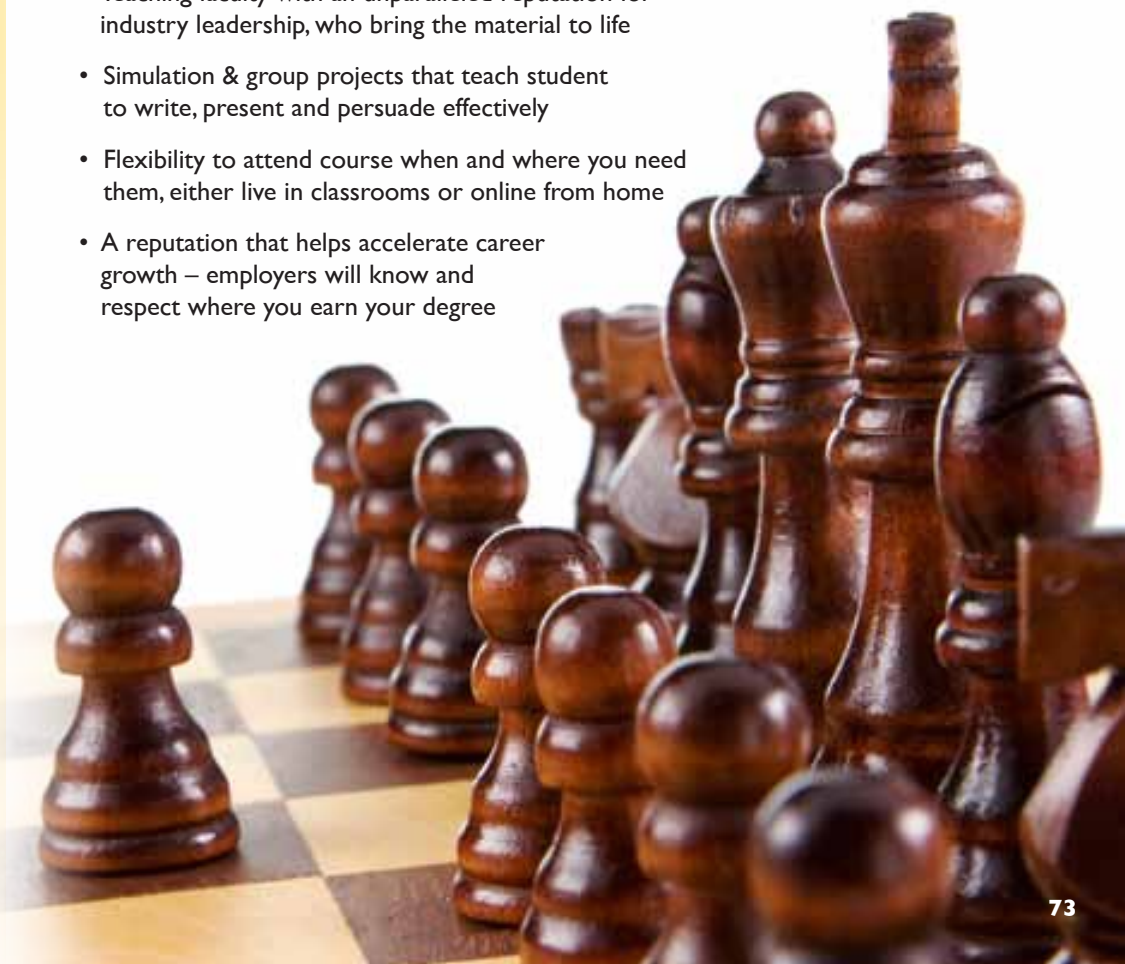
**MASTER OF SCIENCE IN
INFORMATION SECURITY MANAGEMENT**

*SANS Technology Institute offers key qualities
students seek in a cyber master's program:*

- World-class, cutting-edge technical courses that establish and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership, who bring the material to life
- Simulation & group projects that teach student to write, present and persuade effectively
- Flexibility to attend course when and where you need them, either live in classrooms or online from home
- A reputation that helps accelerate career growth – employers will know and respect where you earn your degree



Learn more at
www.sans.edu
info@sans.edu





How the SANS Cyber Guardian Program Works

This program begins with hands-on core courses that will build and increase your knowledge and skills. These skills will be reinforced by taking and passing the associated GIAC certification exam. After completing the core courses, you will choose a course and certification from either the Red or Blue Team. The program concludes with participants taking and passing the GIAC Security Expert (GSE) certification.

Contact us at onsite@sans.org to get started!

Program Prerequisites

- Five years of industry-related experience
- A GSEC certification (with a score of 80 or above) or CISSP certification

Core Courses

- SEC503** Intrusion Detection In-Depth (GCIA)
- SEC504** Hacker Techniques, Exploits, and Incident Handling (GCIH)
- SEC560** Network Penetration Testing and Ethical Hacking (GPEN)
- FOR508** Advanced Computer Forensic Analysis & Incident Response (GCFA)

After completing the core courses, students must choose one course and certification from either the Blue or Red Team

Blue Team Courses

- SEC502** Perimeter Protection In-Depth (GPPA)
- SEC505** Securing Windows & Resisting Malware (GCWN)
- SEC506** Securing Linux/Unix (GCUX)

Red Team Courses

- SEC542** Web App Penetration Testing & Ethical Hacking (GWAPT)
- SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses (GAWN)
- SEC660** Advanced Penetration Testing, Exploits, and Ethical Hacking (GXPN)

The SANS Cyber Guardian program is a unique opportunity for information security individuals or organizational teams to develop specialized skills in incident handling, perimeter protection, forensics, and penetration testing.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING



Multi-Course Training Events

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



Community SANS

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



OnSite

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



Mentor

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



Summit

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

ONLINE TRAINING



OnDemand

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



vLive

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



Simulcast

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



CyberCon

Live online training event
www.sans.org/cybercon



SelfStudy

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

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all



SANS
Security East
New Orleans, LA
Jan 20-25, 2014



SANS
ICS Security
SUMMIT - ORLANDO
Lake Buena Vista, FL
March 12-18, 2014



SANS
AppSec
Austin, TX
Feb 3-8, 2014




SANS
Northern Virginia
Reston, VA
March 17-22, 2014



SANS
CyberCon Spring
Online
Feb 10-15, 2014




SANS
Austin
Austin, TX
April 28-May 3, 2014




SANS
Scottsdale
Scottsdale, AZ
Feb 17-22, 2014



SANS
Security West
San Diego, CA
May 10-15, 2014



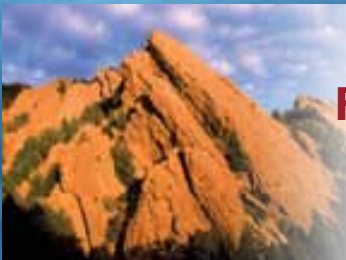
SANS
Cyber Guardian
Baltimore, MD
March 3-8, 2014



SANS
Digital Forensics & Incident Response
SUMMIT
Austin, TX
June 3-10, 2014



SANS
DFIRCON
Monterey, CA
March 5-10, 2014



SANS
Rocky Mountain
Denver, CO
June 7-14, 2014

FUTURE SANS TRAINING EVENTS

Information on all events can be found at www.sans.org/security-training/by-location/all



SANSFIRE

Baltimore, MD
June 19-30, 2014



SANS Baltimore

Baltimore, MD
Sept 22-27, 2014



DC

Washington, DC
July 7-12, 2014



SANS Seattle

Seattle, WA
Sept 29-Oct 4, 2014



SANS San Francisco

San Francisco, CA
July 14-19, 2014



SANS Network Security

Las Vegas, NV
Oct 20-27, 2014



SANS Boston

Boston, MA
July 28-August 2, 2014



SANS San Diego

San Diego, CA
Nov 3-8, 2014



SANS Virginia Beach

Virginia Beach, VA
August 18-29, 2014



SANS South Florida

Fort Lauderdale
Nov 14-19, 2014



SANS Albuquerque

Albuquerque, NM
Sept 15-20, 2014



SANS Cyber Defense Initiative

Washington, DC
Dec 9-19, 2014

Hotel Information

Training Campus

Walt Disney World Dolphin

1500 Epcot Resorts Blvd.

Lake Buena Vista, FL 32830

www.sans.org/event/sans-2014/location

Special Hotel Rates Available

A special discounted rate of \$218.00 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 March 17, 2014.

Leave the every-day world behind and enter a world of wonder and enchantment at the Walt Disney World® Resort. Located in the heart of the most magical place on earth, the Walt Disney World Swan and Dolphin Resort provides a truly extraordinary backdrop for your Orlando vacation or meeting. Beautiful tropical landscaping, tranquil waterways and classic art and architecture work together to create a stunning landmark in the midst of one of the most spectacular places on earth.

Inside the magnificent Disney resort, an environment of elegance and sophistication awaits. Newly refurbished throughout, from the spectacular lobbies and the unique new restaurants, to the exotic Mandara Spa and the incredibly comfortable guest rooms, the resort offers the ultimate escape just moments away from the thrill and excitement of the Walt Disney World® Resort.

The stylishly redesigned lobbies provide guests with a warm and inviting welcome and a distinct sense of arrival. Swan and Dolphin guest rooms have been enhanced with new earth tones and warm hues, including custom draperies, upgraded technology and of course, all rooms feature the incredibly comfortable Heavenly Bed®.

Walt Disney World® Resort Transportation

A comfortable water taxi offers access from the Disney resorts' dock, running approximately every 15 – 20 minutes to and from Epcot® and Disney's Hollywood Studios™. Or you can take a leisurely stroll along a series of walkways that will also lead you to the entrance of these two theme parks.

Disney resort shuttle buses arrive at the main entrance of the Disney hotels approximately every 15 - 20 minutes to transport guests to Magic Kingdom® Park, Disney's Animal Kingdom® Theme Park, Downtown Disney® area, and Disney's Blizzard Beach Water Park and Disney's Typhoon Lagoon Water Park.

As an additional benefit taxi, town car and limousine transportation is available 24-hours through the Mears Transportation desk, located in the guest services area of the Dolphin. Reservations are required.

Top 5 reasons to stay at the Walt Disney World® Dolphin

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

Weather

Temperature range in Orlando during April is 60°-83°.



COME TO ORLANDO!

Dear Colleagues and Friends,

We are back in sunny Orlando at the **Walt Disney World® Resort** for **SANS 2014!** What a perfect time to visit sunny Orlando in early spring while enjoying the best cybersecurity training in the industry! SANS 2014 will be offering more courses, night sessions, and vendor events than ever before, including NetWars, our cyber range challenge.

SANS 2014 is located at the award-winning **Walt Disney World Swan and Dolphin Resort** (www.swandolphin.com) where there are many dining options in the hotel or right outside at the Boardwalk. **Epcot®** and **Disney's Hollywood Studios™** are within walking distance. The Disney property is twice the size of Manhattan, so we recommend staying at the hotel complex. Benefits include complimentary transportation around **Walt Disney World® Resort** and, as an extra treat to SANS attendees, complimentary high-speed Internet, access to fitness facilities, and bottled water in the guest room. Be sure to book under the SANS special rate as these amenities are not available to the general public.

This year SANS 2014 coincides with the **Epcot® Flower and Garden Festival**, which features special flower and garden displays, presentations and demonstrations, and concerts throughout the festival. The **Magic Kingdom®** has just doubled the size of Fantasyland with some brand new attractions including attractions based on the Little Mermaid and Beauty and the Beast. The **Disney's Hollywood Studios™** has a new 3-D version of StarTours featuring multiple versions of the ride based on the Star Wars series.

Since the course days are so intense, take advantage of the SANS hotel rate and enjoy a day or two before or after your training so you can experience everything that Orlando offers. Your family members are invited to all of our SANS receptions. We have special pricing if you would like to go to the parks after class or spend a full day in the parks.

For tips on the Disney parks and Orlando attractions, check out my personal favorite site at www.allearsnet.com where you will find reviews, restaurant menus with prices, and park updates. You will also want to check out the SANS 2014 program guide for all of the action-packed presentations, receptions, and events as well as the social board for student gatherings. Please feel free to send me an e-mail at Brian@sans.org for more recommendations on things to do in Orlando.

See you real soon at SANS 2014!

Brian Correia

Brian Correia

SANS, Director, Business Development & Venue Planning

Five Reasons to Register

1. The best career move you will ever make!

That's how one SANS alumnus described the IT security education and networking opportunities offered by SANS. Attending SANS 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



Register online at
www.sans.org/event/sans-2014/courses

How to Register

1. To register, go to www.sans.org/event/sans-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.

Even if you do not want to submit your payment information online, still complete the online form! There is an option to submit credit card information for payment by fax or phone once the online form is completed and you have your invoice number.

SANS ACCEPTS ONLY U.S. and CANADIAN FEDERAL GOVERNMENT PURCHASE ORDERS

If you normally use a PO and are not part of the federal government, please see our additional PO information on the tuition information page:
www.sans.org/event/sans-2014/attendee-info

3. Print your invoice.

If you need one, you must print YOUR OWN INVOICE at the end of the online registration process. The invoice will pop up automatically when the registration is successfully submitted. You may also access your invoice at <https://portal.sans.org/history>.

4. E-mail confirmation will arrive soon after you register.



To register for a SANS 2014 Simulcast course, please visit
<http://www.sans.org/event/sans-2014/attend-remotely>

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	2/12/14	\$400.00	2/26/14	\$250.00

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
www.sans.org/security-training/discounts prior to registering.



Get GIAC Certified!

- Only \$599 when combined with SANS training
- Deadline to register at this price is the last day of SANS 2014
- Price goes to \$799 after deadline
- Register today at
registration@sans.org

Frequently Asked Questions

Frequently asked questions about SANS Training and GIAC Certification are posted at
www.giac.org/overview/faq.php.

Cancellation

You may substitute another person in your place at any time by sending an e-mail request to registration@sans.org or a fax request to 301-951-0140. Processing fees may apply. No refunds will be given after the stated deadline. Cancellation requests must be received by Wednesday, March 19, 2014, by fax or mail-in order to receive a refund.

SANS 2014 REGISTRATION FEES

Register online at www.sans.org/event/sans-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 2/12/14	Paid by 2/26/14	Paid after 2/26/14	Add GIAC Cert	Add OnDemand
<input type="checkbox"/> SEC301	Intro to Information Security	\$3,995	\$4,145	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC401	Security Essentials Bootcamp Style.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC501	Advanced Security Essentials – Enterprise Defender.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC502	Perimeter Protection In-Depth.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	
<input type="checkbox"/> SEC503	Intrusion Detection In-Depth NEW!	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC504	Hacker Techniques, Exploits, and Incident Handling.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC505	Securing Windows and Resisting Malware.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC542	Web Application Penetration Testing and Ethical Hacking.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC560	Network Penetration Testing and Ethical Hacking.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC561	Intense Hands-on Pen Testing Skill Development NEW!	\$4,695	\$4,845	\$5,095		
<input type="checkbox"/> SEC566	Implementing & Auditing the Twenty Critical Security Controls – In-Depth.	\$3,995	\$4,145	\$4,395		<input type="checkbox"/> \$449
<input type="checkbox"/> SEC575	Mobile Device Security and Ethical Hacking.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC579	Virtualization and Private Cloud Security.	\$4,695	\$4,845	\$5,095		<input type="checkbox"/> \$449
<input type="checkbox"/> SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> SEC642	Advanced Web App Penetration Testing and Ethical Hacking.	\$4,495	\$4,645	\$4,895		<input type="checkbox"/> \$449
<input type="checkbox"/> SEC660	Advanced Penetration Testing, Exploits, and Ethical Hacking.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> FOR408	Computer Forensic Investigations – Windows In-Depth.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> FOR508	Advanced Computer Forensic Analysis and Incident Response.	\$4,695	\$4,845	\$5,095	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> FOR526	Windows Memory Forensics In-Depth	\$3,995	\$4,145	\$4,395		<input type="checkbox"/> \$449
<input type="checkbox"/> FOR572	Advanced Network Forensics and Analysis NEW!	\$4,695	\$4,845	\$5,095		
<input type="checkbox"/> FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam.	\$3,795	\$3,945	\$4,195	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™.	\$4,495	\$4,645	\$4,895	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep.	\$3,795	\$3,945	\$4,195	<input type="checkbox"/> \$599	
<input type="checkbox"/> AUD507	Auditing Networks, Perimeters, and Systems.	\$4,270	\$4,420	\$4,670	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> DEV522	Defending Web Applications Security Essentials.	\$4,270	\$4,420	\$4,670	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> LEG523	Law of Data Security and Investigations.	\$3,995	\$4,145	\$4,395	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449
<input type="checkbox"/> HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program.	\$3,145	\$3,145	\$3,145		

Skill-Based Short Courses

<input type="checkbox"/> SEC434	Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting.	\$1,350	\$2,145	\$2,145	\$2,145				
<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 NEW!	\$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"/> MGT535	Incident Response Team Management.	\$575	\$1,095	\$1,095	\$1,095				
<input type="checkbox"/> AUD444	Auditing Security and Controls of Active Directory and Windows.	N/A	\$2,525	\$2,525	\$2,525				
<input type="checkbox"/> AUD445	Auditing Security and Controls of Oracle Databases.	N/A	\$2,525	\$2,525	\$2,525				
<input type="checkbox"/> AUD521	Meeting the Minimum: PCI/DSS 2.0: Becoming and Staying Compliant.	\$1,250	\$1,885	\$1,885	\$1,885				
<input type="checkbox"/> DEV541	Secure Coding in Java/JEE: Developing Defensible Applications.	N/A	\$3,550	\$3,700	\$3,950	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449		
<input type="checkbox"/> DEV544	Secure Coding in .NET: Developing Defensible Applications.	N/A	\$3,550	\$3,700	\$3,950	<input type="checkbox"/> \$599	<input type="checkbox"/> \$449		
<input type="checkbox"/> HOSTED	Physical Penetration Testing - Introduction.	N/A	\$1,900	\$1,900	\$1,900				
<input type="checkbox"/> SPECIAL	NetWars – Tournament Entrance Fee.	FREE	\$1,249	\$1,249	\$1,249				

Individual Courses Available

	MON 4/7	TUE 4/8	WED 4/9	THU 4/10	FRI 4/11	SAT 4/12
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
FOR610						<input type="checkbox"/> 610.6

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.



5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this **Promo Code** and
receive a special invitation to the
**SANS Executive
Reception**

To be removed from future mailings please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.



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.

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!”



Scan the QR code and
register by February 12th to
SAVE \$400
on SANS 2014 courses.

www.sans.org/info/142992

Setting the Standard for Security Training