# SANS

## Washington, DC | December 10-19, 2014

CYBER DEFENSE INITIATIVE

POWERED BY NETWARS

*Includes 3rd Annual Tournament of Champions*

*Choose from these popular courses:*

### SECURITY

Security Essentials Bootcamp Style

Hacker Techniques, Exploits, and Incident Handling

Web App Penetration Testing and Ethical Hacking

Intrusion Detection In-Depth

### FORENSICS

Memory Forensics In-Depth NEW!

Windows Forensic Analysis

REM: Malware Analysis Tools and Techniques

### MANAGEMENT

SANS Security Leadership Essentials For Managers with Knowledge Compression™

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

### INDUSTRIAL CONTROL SYSTEMS

ICS/SCADA Security Essentials NEW!

*And more!*

GIAC Approved Training

**Register at**

sans.org/event/cyber-defense-initiative-2014

# NETWARS

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

**For more information, look for the NetWars insert located in the center of this brochure!**

## There will be three simultaneous NetWars Tournament events held at SANS CDI 2014.

Each event will be held on the evenings of December 15-16 from 6:30-9:30pm

**1** CORE NETWARS TOURNAMENT

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

**2** DFIR NETWARS TOURNAMENT

***Challenge Yourself Before the Enemy Does***

**3** NETWARS TOURNAMENT of CHAMPIONS

***3rd Annual NetWars Tournament of Champions (Invite Only)***

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

**REGISTRATION IS LIMITED AND IS FREE**

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

**Register at sans.org/event/cyber-defense-initiative-2014**

SANS

# IT SECURITY TRAINING AND YOUR CAREER ROADMAP

## Information Security

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

**SAMPLE JOB TITLES**
- Cybersecurity analyst
- Cybersecurity engineer
- Cybersecurity architect

**CORE COURSES**

| TECHNICAL INTRODUCTORY | CORE | IN-DEPTH |
|---|---|---|
| **SEC301** Intro to Information Security **GISF** | **SEC401** Security Essentials Bootcamp Style **GSEC** | **SEC501** Advanced Security Essentials – Enterprise Defender **GCED** |

## Penetration Testing/Vulnerability Assessment

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

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

| ENTERPRISE | WEB | MOBILE/WIRELESS |
|---|---|---|
| **SEC560** Network Penetration Testing and Ethical Hacking **GPEN** | **SEC542** Web App Penetration Testing and Ethical Hacking **GWAPT** | **SEC575** Mobile Device Security and Ethical Hacking **GMOB** |
| **SEC561** Intense Hands-On Pen Testing Skill Development | **SEC642** Advanced Web App Penetration Testing and Ethical Hacking | **SEC617** Wireless Ethical Hacking, Penetration Testing & Defenses **GAWN** |
| **SEC660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN** | | |
| **SEC760** Advanced Exploit Development for Penetration Testers | | |

**SPECIALIZATION**

**SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise

**SEC573** Python for Penetration Testers

**SEC580** Metasploit Kung Fu for Enterprise Pen Testing

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

**SAMPLE JOB TITLES**
- Penetration tester
- Vulnerability assessor
- Ethical hacker
- Red/Blue team member
- Cyberspace engineer

## Risk and Compliance/Auditing/Governance Titles

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

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

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

**SAMPLE JOB TITLES**
- Auditor
- Compliance officer

## Network Operations Center, System Admin, Security Architecture

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

**SAMPLE JOB TITLES**
- System/IT administrator
- Security administrator
- Security architect/engineer

**CORE COURSES**
SEC301 (GISF) ▸ SEC401 (GSEC) ▸ SEC501 (GCED)

- **SEC505** Securing Windows with the Critical Security Controls **GCWN**
- **SEC506** Securing Linux/Unix **GCUX**
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth **GCCC**
- **SEC579** Virtualization and Private Cloud Security

## Security Operations Center/Intrusion Detection

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

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

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

**ENDPOINT MONITORING**
- **SEC501** Advanced Security Essentials – Enterprise Defender **GCED**
- **FOR508** Advanced Computer Forensic Analysis and Incident Response **GCFA**

**NETWORK MONITORING**
- **SEC502** Perimeter Protection In-Depth **GPPA**
- **SEC503** Intrusion Detection In-Depth **GCIA**
- **FOR572** Advanced Network Forensics and Analysis **GNFA**
- **SEC511** Continuous Monitoring and Security Operations

**SAMPLE JOB TITLES**
- Intrusion detection analyst
- Security operations center analyst/engineer
- CERT member
- Cyber threat analyst

## Development – Secure Development

- **Securing the Human for Developers – STH.Developer** Application Security Awareness Modules
- **DEV522** Defending Web Applications Security Essentials **GWEB**
  - **DEV541** Secure Coding in Java/JEE: Developing Defensible Applications
  - **DEV544** Secure Coding in .NET: Developing Defensible Applications

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

**SAMPLE JOB TITLES**
- Developer
- Software architect
- QA tester
- Development manager

**SPECIALIZATION**
- **SEC542** Web App Penetration Testing and Ethical Hacking **GWAPT** → **SEC642** Advanced Web App Penetration Testing and Ethical Hacking


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

sans.org/netwars

NetWars is designed to help participants develop skills in several critical areas:
- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing
- Intrusion Detection

## Cyber or IT Security Management

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

**SAMPLE JOB TITLES**
- CISO
- Cybersecurity manager/officer
- Security director

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

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

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

**MGT535**
Incident Response Team Management

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

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

**SEC440**
Critical Security Controls: Planning, Implementing, and Auditing

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

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

## Incident Response

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

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

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

**SAMPLE JOB TITLES**
- Security analyst/engineer
- SOC analyst
- Cyber threat analyst
- CERT member
- Malware analyst

**SPECIALIZATION**

**FOR526**
Memory Forensics In-Depth

**MGT535**
Incident Response Team Management

**NETWORK ANALYSIS**

**SEC503**
Intrusion Detection In-Depth
GCIA

**FOR572**
Advanced Network Forensics and Analysis
GNFA

**ENDPOINT ANALYSIS**

**FOR408**
Windows Forensic Analysis
GCFE

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

**MALWARE ANALYSIS**

**FOR610**
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

## Digital Forensic Investigations and Media Exploitation

**FOR408**
Windows Forensic Analysis
GCFE

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

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

**FOR585**
Advanced Smartphone Forensics

**FOR518**
Mac Forensics Analysis

**FOR526**
Memory Forensics In-Depth

**FOR610**
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

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

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. Government organizations also need the skills to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

Dear Colleague,

**SANS Cyber Defense Initiative (CDI)** is coming to Washington DC on December 10-19. We are bringing more than 25 courses of SANS' most comprehensive and challenging educational programs to meet the needs of the sophisticated cybersecurity community in the nation. SANS is known for providing intensive, immersion training designed to develop security skills that are practical, and taught by many of the nation's most accomplished security practitioners. You already know there are a growing number of attacks on our networks that are testing your skills. Learn and understand about the most current hacking methods and the types of tools so that you can proactively and effectively protect internal systems against intrusions. Hands-on training is the hallmark of SANS' events along with the promise that you will be able to put what you acquire in SANS courses to work as soon as you get back to the office

SANS CDI 2014 is offering these new leading-edge courses: **FOR526: Memory Forensics In-Depth** with Alissa Torres, and **ICS410: ICS/SCADA Security Essentials** (GICSP) with Justin Searle. An additional opportunity is **SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise** with Tim Medin. This new hands-on course teaches the practical skills cyber warriors need to analyze, control, and defend the kinetic infrastructures they will increasingly face in the future.

SANS CDI 2014 is powered by **NetWars – Tournament**. We'll be running **Core NetWars** and **DFIR NetWars** competitions, available FREE to CDI attendees taking a five- or six-day class, while seats last. To add extra excitement, SANS CDI 2014 will include our **Third Annual NetWars Tournament of Champions**, where the best-of-the-best NetWars participants from the past year will face off to see who comes out on top.

NetWars Tournaments are a two-evening simulation featuring real-world computer and network security challenges. Participants have fun conquering these challenges as they build skills and demonstrate their abilities in this safe, informal, and engaging event. Whether you are a first-time NetWars participant looking to have fun and build your skills, or a seasoned champion, please make sure you sign up for NetWars when you register for a CDI long course. Space is limited, so please register early.

Our campus for the main event this year is the Grand Hyatt Washington, centrally located in the trendy Penn Quarter near popular local attractions. In December the nation's capital is awash in twinkling lights and holiday cheer. From the National Christmas Tree near The White House to holiday markets throughout the city – see more at: http://washington.org/topics/winter#sthash. This is your opportunity to get unmatched training. We look forward to seeing you in Washington DC in December.

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

**"The course content is extremely valuable for use in real-world application and directly pertinent to analysis conducted. It's great to go to a class and be able to utilize nearly everything that was taught."**
-H. Polend, VA Department of Forensic Science

**"The current security landscape is rapidly changing so the course content is relevant and important to software security and compliance software."**
-Scott Hoof, Tripwire Inc.

**"I find this training very valuable because its comprehensive and the instructor are very knowledgeable."**
-George Diolamou, Jacob's Engineering

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

# Courses-at-a-Glance

For an up-to-date course list please check the website at sans.org/event/cyber-defense-initiative-2014/schedule

| | | WED 12/10 | THU 12/11 | FRI 12/12 | SAT 12/13 | SUN 12/14 | MON 12/15 | TUE 12/16 | WED 12/17 | THU 12/18 | FRI 12/19 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SEC301 | Intro to Information Security | | | PAGE 4 | | | | | | | |
| SEC401 | Security Essentials Bootcamp Style SIMULCAST | | | PAGE 6 | | | | | | | |
| SEC434 | Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting | PAGE 44 | | | | | | | | | |
| SEC501 | Advanced Security Essentials – Enterprise Defender | | | PAGE 8 | | | | | | | |
| SEC503 | Intrusion Detection In-Depth | | | PAGE 10 | | | | | | | |
| SEC504 | Hacker Techniques, Exploits, and Incident Handling SIMULCAST | | | PAGE 12 | | | | | | | |
| SEC505 | Securing Windows with the Critical Security Controls SIMULCAST | | | PAGE 14 | | | | | | | |
| SEC524 | Cloud Security Fundamentals | PAGE 44 | | | | | | | | | |
| SEC542 | Web App Penetration Testing and Ethical Hacking | | | PAGE 16 | | | | | | | |
| SEC562 | CyberCity Hands-on Kinetic Cyber Range Exercise NEW! | | | PAGE 18 | | | | | | | |
| SEC566 | Implementing and Auditing the Critical Security Controls – In-Depth | | | PAGE 20 | | | | | | | |
| SEC575 | Mobile Device Security and Ethical Hacking | | | PAGE 22 | | | | | | | |
| SEC579 | Virtualization and Private Cloud Security | | | PAGE 24 | | | | | | | |
| SEC580 | Metasploit Kung Fu for Enterprise Pen Testing | | | | | | | | | PAGE 45 | |
| SEC660 | Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | | | PAGE 26 | | | | | | | |
| FOR408 | Windows Forensic Analysis | | | PAGE 28 | | | | | | | |
| FOR508 | Advanced Computer Forensic Analysis & Incident Response SIMULCAST | | | PAGE 30 | | | | | | | |
| FOR526 | Memory Forensics In-Depth NEW! | | | PAGE 32 | | | | | | | |
| FOR610 | Reverse-Engineering Malware: Malware Analysis Tools and Techniques SIMULCAST | | | PAGE 34 | | | | | | | |
| MGT305 | Technical Communication & Presentation Skills for Security Professionals | | P 45 | | | | | | | | |
| MGT414 | SANS® +S™ Training Program for the CISSP® Certification Exam | | | PAGE 36 | | | | | | | |
| MGT415 | A Practical Introduction to Risk Assessment | | P 45 | | | | | | | | |
| MGT433 | Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program SIMULCAST | | | PAGE 38 | | | | | | | |
| MGT512 | SANS Security Leadership Essentials for Managers with Knowledge Compression™ | PAGE 46 | | | | | | | | | |
| MGT535 | Incident Response Team Management | | P 46 | | | | | | | | |
| AUD507 | Auditing & Monitoring Networks, Perimeters, and Systems | | | PAGE 40 | | | | | | | |
| ICS410 | ICS/SCADA Security Essentials NEW! SIMULCAST | | | PAGE 42 | | | | | | | |
| HOSTED | (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program | | | PAGE 43 | | | | | | | |
| HOSTED | Physical Penetration Testing – Introduction | PAGE 47 | | | | | | | | | |
| HOSTED | Embedded Device Security Assessments for the Rest of Us NEW! | PAGE 47 | | | | | | | | | |
| HOSTED | Offensive Countermeasures: The Art of Active Defenses | | | | | | | | | PAGE 47 | |
| | NetWars Tournaments (Core & DFIR) | | | | | | PAGE 2 | | | | |

# CONTENTS

SECURITY 301

# Intro to Information Security

COURSE NOW INCLUDES HANDS-ON LABS

SANS

Five-Day Program
Fri, Dec 12 - Tue, Dec 16
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Fred Kerby
- GIAC Cert: GISF

This introductory certification course is the fastest way to get up to speed in information security. Written and taught by battle-scarred security veterans, this entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security and the basics of risk management.

Organizations often tap someone who has no information security training and say, "Congratulations, you are now a security officer." If you need to get up to speed fast, Security 301 is the course for you!

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

**"I enjoyed the connection between real-life scenarios and training material."**
-Stephanie Westbrook, Offensive Logic-LLC

**"Fred is an excellent instructor who blends theory with practical examples."**
-Kwabby Gyasi IMF

**"SEC301 does an excellent job of giving you an idea of how well your security policy is written."**
-Terry Benes, University of Nebraska Foundation

**Fred Kerby** *SANS Senior Instructor*

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

## 301.1 HANDS ON: A Framework for Information Security

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

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

## 301.2 HANDS ON: Securing the Infrastructure

To appreciate the risks associated with being connected to the Internet one must have a basic understanding of how networks function. Day two covers the basics of networking (including a review of some sample network designs), including encapsulation, hardware and network addresses, name resolution, and address translation. We explore some of the various types of malware and associated delivery mechanisms. We conclude with a review of some typical attacks against the networking and computing infrastructure as well as discussing human-based attacks.

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

### 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

## 301.3 HANDS ON: Cryptography and Security in the Enterprise

Cryptography can be used to solve a number of security problems. Cryptography and Security in the Enterprise provides an in-depth introduction to a complex tool (cryptography) using easy-to-understand examples and avoiding complicated mathematics. Attendees will gain meaningful insights into the benefits of cryptography (along with the pitfalls of poor implementation of good tools). The day continues with an overview of Operational Security (OPSEC) as well as Safety and Physical Security. We conclude the day with a whirlwind overview of wireless networking technology benefits and risks, including a roadmap for reducing risks in a wireless environment.

**Topics:** Cryptography (Cryptosystem Components, Cryptographic Services, Algorithms, Keys, Cryptographic Applications, Implementation); Operations Security (OPSEC), Physical Security, Safety: Wireless Network Technology (Wireless Use and Deployments, Wireless Architecture and Protocols, Common Misconceptions, Top 4 Security Risks, Steps to Planning a Secure WLAN)

## 301.4 HANDS ON: Information Security Policy

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

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

## 301.5 HANDS ON: Defense In-Depth: Lessons Learned

The goal of day five is to enable managers, administrators, and those in the middle to strike a balance between "security" and "getting the job done." We'll explore how risk management deals with more than just security. We discuss the six phases of incident handling as well as some techniques that organizations can use to develop meaningful metrics.

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


giac.org

SECURITY 401

# Security Essentials Bootcamp Style

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
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 lets me go back and improve my organization's security. It has given me tools, more insights, and an overall refreshment of my knowledge. Excellent trainer in every aspect!!!"**
-Jerry Robels de Medina Godo

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

***Learn to build a security roadmap that can scale today and into the future.***

**SEC401: Security Essentials Bootcamp Style** is focused on teaching you the essential information security skills and techniques you need to protect and secure your organizations critical information assets and business systems. Our course will show you how to prevent your organizations security problems from being headline news in the *Wall Street Journal*!

## PREVENTION IS IDEAL BUT DETECTION IS A MUST.

With the advanced persistent threat, it is almost inevitable that organizations will be targeted. Whether the attacker is successful in penetrating an organizations network depends on the effectiveness of the organizations defense. 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 really 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:

- **What is the risk?**
- **Is it the highest priority risk?**
- **What is the most cost-effective way to reduce the risk?**

Security is all about making sure you focus on the right areas of defense. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge youll need 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 learn up-to-the-minute skills 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

**ATTEND REMOTELY**

**SIMULCAST**

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

*More info on page 52*

## 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. @drericcole

## 401.1 HANDS ON: Networking Concepts

A key way that attackers gain access to a companys 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 what is hostile. 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 during this course day in order to provide a firm foundation for the consecutive days of training.

**Topics:** Network Fundamentals; IP Concepts; IP Behavior; Virtual Machines

## 401.2 HANDS ON: Defense In-Depth

To secure an enterprise network, you must have an understanding of the general principles of network security. In this course, you will learn about six key areas of network security. The day starts with information assurance foundations. Students look at both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. The first half of the day also covers creating sound security policies and password management, including tools for password strength on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at what can be done to test and protect a web server in your company.

**Topics:** Information Assurance Foundations; Computer Security Policies; Contingency and Continuity Planning; Access Control; Password Management; Incident Response; Offensive and Defensive Information Warfare; Web Security

## 401.3 HANDS ON: Internet Security Technologies

Military agencies, banks, and retailers offering electronic commerce programs, as well as dozens of other types of organizations, are striving to understand the threats they are facing and what they can do to address those threats. On day 3, you will be provided with a roadmap to help you understand the paths available to organizations that are considering deploying or planning to deploy various security devices and tools such as intrusion detection systems and firewalls. When it comes to securing your enterprise, there is no single technology that is going to solve all your security issues. However, by implementing an in-depth defense strategy that includes multiple risk-reducing measures, you can go a long way toward securing your enterprise.

**Topics:** Attack Methods; Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention; 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 deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day 4 looks at various aspects of encryption and how it can be used to secure a companys assets. A related area called steganography, or information hiding, is also covered. Wireless is becoming a part of most modern networks, but is often implemented in a non-secure manner. Security issues associated with wireless, and what can be done to protect these networks, will also be discussed. This section finishes by tying all of the other pieces together by looking at operations security.

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

### You Will Be Able To

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

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

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

## 401.6 HANDS ON: Linux Security

While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. Day 6 provides step-by-step guidance to improve the security of any Linux system. The course combines practical how to instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise.

**Topics:** Linux Landscape; Permissions and User Accounts; Linux OS Security; Maintenance, Monitoring, and Auditing Linux; Linux Security Tools

giac.org

sans.org/
cyber-guardian

sans.edu


DoDD 8570 Required
sans.org/8570

SECURITY 501

# Advanced Security Essentials – Enterprise Defender

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required
Instructor: Bryce Galbraith

- GIAC Cert: GCED
- Masters Program
- DoDD 8570

## Who Should Attend

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

**"I learned how to manage the risks, how to protect data, and how to prevent the loss of data that my institution owns."**
-Puiu Lucian, CHITU ANCOM

**"After taking SEC401 and GSEC, this course is the perfect follow up. Going deep into attacking techniques while understanding the most-used vulnerabilities and how to defend your network against those attacks."**
-Fawaz AlHomoud, Saudi Aramco

Cybersecurity continues to be a critical area for organizations and will increase in importance as attacks become stealthier, have a greater financial impact on organization,'s and cause reputational damage. Security Essentials lays a solid foundation for the security practitioner to engage the battle.

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

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

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

**"SEC501 is helping me expand my security knowledge by putting the history and the information in an explanation of real-world technologies."**
-Gerald Servidio, General Electric

**Bryce Galbraith** *SANS Principal Instructor*

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

## 501.1 HANDS ON: Defensive Network Infrastructure

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

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

## 501.2 HANDS ON: Packet Analysis

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

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

### You Will Be Able To

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

## 501.3 HANDS ON: Penetration Test

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

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

## 501.4 HANDS ON: First Responder

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

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

## 501.5 HANDS ON: Malware

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

**Topics:** Malware; Microsoft Malware; External Tools and Analysis

## 501.6 HANDS ON: Data Loss Prevention

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

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


giac.org


sans.edu

DoDD 8570 Required
sans.org/8570

SECURITY 503

# Intrusion Detection In-Depth

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
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

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

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

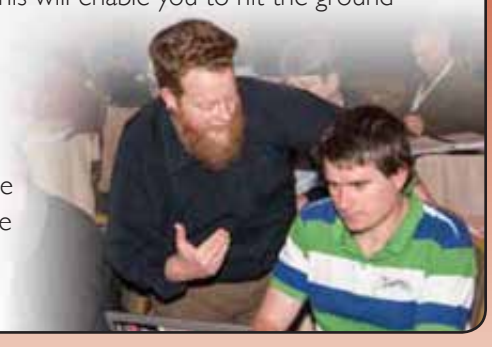
Industry expert and instructor Mike Poor has created a VMware distribution, Packetrix, specifically for this course. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis. Packetrix is supplemented with demonstration "pcaps" –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

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

Exercises have two different approaches. The first is a more basic one that assists you by giving hints for answering the questions. Students who feel that they would like more guidance can use this approach. The second approach provides no hints, permitting a more challenging experience for a student who may already know the material or who has quickly mastered new material. Additionally, there is an "extra credit" stumper question for exercises intended to challenge the most advanced student.

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

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



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

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

**"Mike does an excellent job balancing dry technical info with enough personal anecdotes to keep it lively."**
-Benjamin Jones, U.S. Navy

## Mike Poor *SANS Senior Instructor*

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

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

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

**Topics:** Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3, IPv4, and IPv6

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

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

**Topics:** Wireshark Display Filters; Writing tcpdump Filters; TCP; UDP; ICMP

### 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

## 503.3 HANDS ON: Application Protocols and Traffic Analysis

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

**Topics:** Advanced Wireshark; Detection Methods for Application Protocols; Microsoft Protocols; HTTP; SMTP; DNS; Packet Crafting and nmap OS Identification; IDS/IPS Evasion Theory; Real-World Traffic Analysis

## 503.4 HANDS ON: Open-Source IDS: Snort and Bro

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

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

## 503.5 HANDS ON: Network Traffic Forensics and Monitoring

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

**Topics:** Analyst Toolkit; SiLK; Network Forensics; Network Architecture for Monitoring; Correlation of Indicators

## 503.6 HANDS ON: IDS Challenge

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

giac.org

sans.org/cyber-guardian

sans.edu

DoDD 8570 Required
sans.org/8570

**ATTEND REMOTELY**

**SIMULCAST**

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

*More info on page 52*

SECURITY 504

# Hacker Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 6:30pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

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

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

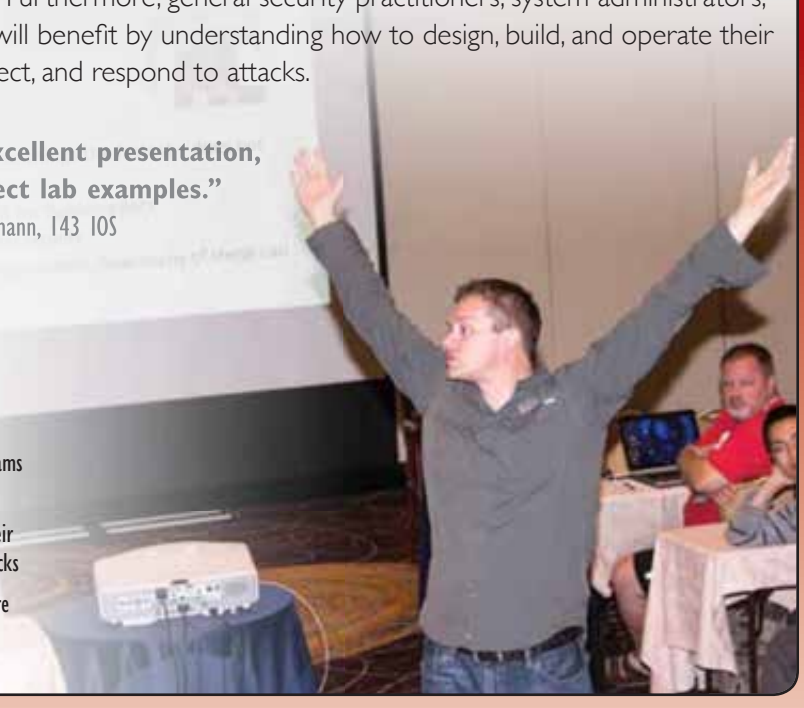
By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers.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

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

**"John Strand is clear, energetic, and has a great depth of knowledge."**
-Jason MacDonald, DOD Canada

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

**"Excellent training, excellent presentation, and applicable direct lab examples."**
-Rodney Lindemann, 143 IOS



## Who Should Attend

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

**John Strand** *SANS Senior Instructor*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 504.6 HANDS ON: Hacker Tools Workshop

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

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

### You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

DoDD 8570 Required
sans.org/8570

**ATTEND REMOTELY**

**SIMULCAST**

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

*More info on page 52*

SECURITY 505

# Securing Windows with the Critical Security Controls

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Cyber Guardian
- Masters Program

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

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

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

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

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

**"SEC505 should be required for anyone administering windows domains."**
-Tom Gonzales,
Credit Union of Colorado

**"Jason's way of explaining objects in Powershell is both unique and was easy to understand. The best explanation I've heard since Powershell came out."**
-Mark Lucas, Caltech

**ATTEND REMOTELY**

**SIMULCAST**

If you are unable to attend this event, this course is also available via SANS Simulcast.
*More info on page 52*

## Who Should Attend

- Windows security engineers and system administrators
- Anyone who wants to learn PowerShell
- Anyone who wants to implement the 20 Critical Security Controls
- Those who must enforce security policies on Windows hosts
- Anyone who needs a whole drive encryption solution
- Those deploying or managing a PKI or smart cards
- Anyone who needs to prevent malware infections
- Anyone implementing the Australian Directorate's Four Controls

## Jason Fossen *SANS Faculty Fellow*

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

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

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

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

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

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

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

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

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

**Topics:** Why Have a PKI?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards, BitLocker Drive Encryption and Secure Boot

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

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

**Topics:** Why IPSec?; Creating IPSec Policies; Windows Firewall; Securing Wireless Networks; RADIUS for Wireless and Ethernet

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

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

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

## 505.6 HANDS ON: Windows PowerShell Scripting

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

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

### You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 542

# Web App Penetration Testing and Ethical Hacking

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

- GIAC Cert: GWAPT
- Cyber Guardian
- Masters Program

## Who Should Attend

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

**"The SEC542 tools and course presentation are top-notch. I'll be using this material extensively."**
-Jeremy Pierson, Academy Mortgage

**"Web app assessment is currently what I do. SEC542 really fills in the gaps in on-the-job training."**
-James Kelly, Blue Canopy LLP

**"With the infinite tools used for web app penetration, SEC542 helps you understand/use the best tools for your environment."**
-Linh Sithihao, UT Southwestern Medical Center

**"SEC542 is an essential course for application security professionals."**
-John Yamich, Exact Target

### *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.

**Eric Conrad** *SANS Principal Instructor*

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

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

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

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

## 542.2 HANDS ON: Reconnaissance and Mapping

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

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

## 542.3 HANDS ON: Server-Side Discovery

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

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

## 542.4 HANDS ON: Client-Side Discovery

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

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

## 542.5 HANDS ON: Exploitation

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

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

## 542.6 HANDS ON: Capture the Flag

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

### You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 562

# CyberCity Hands-on Kinetic Cyber Range Exercise

NEW

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend these important infrastructures. In this innovative and cutting-edge course, you'll learn how to analyze and assess the security of kinetic control systems, finding vulnerabilities that could result in significant kinetic impact.

## Who Should Attend

- Red and blue team members
- Cyber warriors
- Incident handlers
- Penetration testers
- Ethical hackers
- Other security personnel who are first responders when systems come under attack

SEC562 includes over 80% of course time devoted directly to hands-on labs to help participants build real keyboard skills quickly, powered by the SANS NetWars engine. Participants will conduct thorough exercises as a series of missions, all with the goal of achieving specific objectives in preventing attackers from causing physical damage. In each mission, participants gain access to different critical systems including electrical distribution systems, water filtration systems, traffic light controllers, and medical patient data management systems, exploiting the same flaws that are used by advanced adversaries, all with the goal of finding and mitigating flaws before an adversary does.

Using the innovative SANS CyberCity project as a target environment, participants analyze and exploit actual critical infrastructure systems, building skills in attacking general-purpose servers and specialized control protocols including DNP3, Common Industrial Protocol (CIP), Modbus/TCP, Profinet, and more. Combined with 20% classroom lecture, 80% hands-on exercises, and individualized guidance from an expert instructor, participants will build the skills needed to scan, evaluate, exploit, and assess real-world systems representing a critical infrastructure component for many organizations today.

## Topics addressed in the course include:

- Understanding how cyber infrastructures control and impact kinetic infrastructures
- Analyzing a variety of industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols.
- Rapidly prototyping computer attack tools against specific vulnerabilities
- Analyzing security flaws in a variety of SCADA and Industrial Control Systems (ICSs)
- Penetration testing experience with kinetic infrastructures

**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. @timmedin

## 562.1 HANDS ON: Team Building, Visualizing the Battlespace, and Protocol Manipulation

MISSION 1: **Team-building mission:** Recon, social networking, intel gathering, and controlling billboards

MISSION 2: **Camera mission:** Visualizing the battlespace

MISSION 3: **Traffic light mission:** Manipulating modbus for system control

## 562.2 HANDS ON: Network Recon, Data Integrity, and Operator Interface Terminals

MISSION 4: **Network reconnaissance:** Surveying the infrastructure

MISSION 5: **Hospital mission:** Ensure the integrity of medical record information

MISSION 6: **Streetlight mission:** Restore streetlights through manipulating an operator interface terminal

## 562.3 HANDS ON: Alarms, Data Historians, and SCADA Switching

MISSION 7: **Bank alarm mission:** Control a bank alarm system

MISSION 8: **Water reservoir mission:** Ensure the water reservoir human machine interface and data historian properly reflect water records to prevent contamination

MISSION 9: **Train derailment mission:** Interact with SCADA-controlled train switching junctions to prevent a disaster

### You Will Be Able To

- Scan for and discover the details associated computer, network, and ICS assets.
- Analyze and manipulate commonly used, very powerful, but often less-well-understood protocols such as Profinet, DNP3, Modbus, and more.
- Work as part of a team analyzing attacker actions and preventing kinetic impacts against industrial control systems.
- Look for vulnerabilities in systems associated with electrical power distribution, water systems, traffic systems, and other infrastructures.
- Use a variety of hands-on tools for analyzing and interacting with target systems, including Wireshark, tcpdump, Nmap, Metasploit, and much more.
- Control various Human Machine Interfaces and Operator Interface Terminals widely used by SCADA and other Industrial Control Systems (ICSs)
- Prevent attackers from wreaking havoc by manipulating computers that control physical infrastructures

## 562.4 HANDS ON: Wifi and Thwarting Denial of Service

MISSION 10: **Coffee shop WiFi mission:** Analyze and thwart attackers from attacking wireless client machines in the coffee shop

MISSION 11: **Landing strip mission:** Neutralize a denial of service attack to restore lighting to an airfield landing strip

MISSION 12: **ISP HVAC mission:** Prevent attackers from manipulating the HVAC systems of CyberCity's ISP

## 562.5 HANDS ON: Power Grid and Weapons Systems

MISSION 13: **Residential power grid mission:** Regain control of power grid systems to restore the residential infrastructure after a blackout

MISSION 14: **City-wide power grid mission:** Gain control of SCADA systems to restore power on a city-wide basis

MISSION 15: **Rocket-launcher mission:** Retake control of a rocket launcher and discharge its weapons safely

## 562.6 HANDS ON: Force-On-Force Attack and Defend

**Capture the Flag:** Defend your systems and attack other parts of CyberCity

SECURITY 566

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

SANS

Five-Day Program
Fri, Dec 12 - Thu, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala
- GIAC Cert: GCCC
- Masters Program

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

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

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

## 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 goes into great detail in his explanations and examples. At first I thought this might become tedious, but I soon realized that some things I knew well, I didn't know as well as I thought. His breadth of knowledge is impressive."**
-Kenneth Eichman,
Chemical Abstracts Service

**"SEC566 is very valuable. This course allows me to understand the importance of managing risk as it relates to these control categories."**
-Ian Perry-Okpara,
Federal Reserve Bank of Atlanta

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.

**James Tarala** *SANS Senior Instructor*

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

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

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

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

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

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

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

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

## 566.3 HANDS ON: Critical Controls 7, 8, 9, 10, and 11

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

## 566.4 HANDS ON: Critical Controls 12, 13, 14, and 15

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

## 566.5 HANDS ON: Critical Controls 16, 17, 18, 19, and 20

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

### You Will Be Able To

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

**"Topics addressed real-world and current threats – gives great suggestions to assist an organization to better protect their IP space."**
-Bill Coffey, Shaw AFB

giac.org

sans.edu

SECURITY 575

# Mobile Device Security and Ethical Hacking

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Christopher Crowley

- GIAC Cert: GMOB
- Masters Program

**"In the fast-paced world of BYOD and mobile device management, SEC575 is a must course for InfoSec managers."**
-Jude Meche, DSCC

**"The content of SEC575 is simply eye-opening. Organizations are so busy trying to roll out their BYOD projects without any understanding of the risks. This course is a must for security professionals rolling out BYOD projects."**
-Vijay Kora,
Open Solutions Consulting Inc.

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

## 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

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 evaluating the network activity generated by mobile applications to mobile code analysis, from exploiting the weaknesses in common mobile applications to conducting a full-scale mobile penetration test, 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.

## Christopher Crowley *SANS Certified Instructor*

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

## 575.1 HANDS ON: Architecture and Management

The first part of the course looks at the significant threats affecting mobile phone deployments and how organizations are being attacked through these systems. As a critical component of a secure deployment, we'll examine the architectural and implementation differences between Android, Apple, BlackBerry, and Windows Phone systems including platform software defenses, and application permission management. We'll also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification and more. We'll apply hands-on exercises to interact with mobile device emulator features including low-level access to installed application services. We'll also examine the critical considerations for platform management systems and how attackers evade or manipulate platform management controls. While we look at the positive side of mobile device management (MDM) systems, we'll also look at the evil side of malicious policies and how attackers can use MDM tools to manipulate victim mobile devices. Finally we'll address the threats of mobile malware including emerging malware threats and the increasingly complex and advanced trends in mobile device malware.

**Topics:** Mobile Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Device Security Models; Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

## 575.2 HANDS ON: Security Controls and Platform Access

With an understanding of the threats, architectural components and desired security methods, we can design incident response processes to mitigate the effective of common threat scenarios including device loss. We'll look at building such a program, while building our own skills at analyzing mobile device data and applications through rooting and jailbreaking, filesystem data analysis, and network activity analysis techniques.

**Topics:** Mitigating Stolen Devices; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

## 575.3 HANDS ON: Application Analysis

One of the critical decisions you will need to make in supporting a mobile device deployment is to approve or disapprove of unique application requests from end-users in a corporate device deployment. With some analysis skills, we can evaluate applications to determine the type of access and information disclosure threats they represent. We'll examine the techniques for reverse-engineering iOS and Android applications, obtaining source code for applications from public app stores. For Android applications we'll look at opportunities to change the behavior of applications as part of our analysis process by decompiling, manipulating, and recompiling code, and adding new code to existing applications without prior source code access. For iOS we'll extract critical app definition information available in all apps to examine and manipulate app behavior through the Cycript tool

**Topics:** Static Application Analysis; Automated Application Analysis Systems; Manipulating App Behavior

### 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, dextranslator, and apktool to identify malware and information leakage threats in mobile applications
- Conduct an automated security assessment of mobile applications using iAuditor, Cycript, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks, crack WEP and WPA/ WPA2 access points, bypass enterprise wireless network authentication requirements, and harvest user credentials
- Intercept and manipulate mobile device network activity using Burp to manipulate the actions taken by a user in an application and to deliver mobile device exploits to vulnerable devices

## 575.4 HANDS ON: Penetration Testing Mobile – PART 1

An essential component of developing a secure mobile phone deployment is to perform an ethical hacking assessment. Through ethical hacking or penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that delivery unauthorized access to data or supporting networks. Through the identification of these flaws we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

**Topics:** Fingerprinting Mobile Devices; Wireless Network Probe Mapping; Weak Wireless Attacks; Enterprise Wireless Security Attacks

## 575.5 HANDS ON: Penetration Testing Mobile – PART 2

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

**Topics:** Network Manipulation Attacks; Mobile Application Attacks; Web Framework Attacks; Back-end Application Support Attacks

## 575.6 HANDS ON: Mobile Security Event

On the last day of class we'll pull in all the concepts and technology we've covered in the week for a comprehensive Capture the Flag (CTF) event. In the CTF event, you'll have the option to participate in multiple roles, designing a secure infrastructure for the deployment of mobile phones, monitoring network activity to identify attacks against mobile devices, extracting sensitive data from a compromised iPad and attacking a variety of mobile phones and related network infrastructure components. In the CTF you'll use the skills you've built to practically evaluate systems and defend against attackers, simulating the realistic environment you'll be prepared to protect when you get back to the office.

giac.org

sans.edu

SECURITY 579

# Virtualization and Private Cloud Security

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dave Shackleford

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

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

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

## Who Should Attend

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

**"The rush for virtualization is difficult for security sensitive environments. SEC579 helps demonstrate which risks are valid."**
-Paul Mayers, Lloyds Banking Group

**"SEC579 actually provides pertinent information outside what is freely available and is applicable to securing my organization's virtual infrastructure."**
-David Richardson, ManTech

**"Dave is one of the best instructors on the face of the planet! SEC579 is the absolute best virtualization security information available! And it's immediately usable."**
-Leonard Lyons, Northrop Grumman

## Dave Shackleford *SANS Senior Instructor*

Dave Shackleford 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. @daveshackleford

## 579.1 HANDS ON: Virtualization Security Architecture and Design

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

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

### You Will Be Able To

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

## 579.2 HANDS ON: Virtualization and Private Cloud Infrastructure Security

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

## 579.3 HANDS ON: Virtualization Offense and Defense – PART 1

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

## 579.4 HANDS ON: Virtualization Offense and Defense – PART 2

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

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

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

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

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

SECURITY 660

# Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Stephen Sims

- GIAC Cert: GXPN
- Cyber Guardian
- Masters Program

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

### Who Should Attend

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

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

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

**"Looking at everything I have learned from SANS, I definitely feel I have gained an edge when it comes to the augmentation of my pentest skills."**
-Alexander Cobblah, Booz Allen Hamilton

**"Awesome teaching style. Great character. Steve uses his real world scenarios to drive home the different topics."**
-Brian Anderson, Northrop Grumman Corporation

## Stephen Sims *SANS Senior Instructor*

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant. He has spent many years performing security architecture, exploit development, reverse engineering, and penetration testing. Stephen has an MS in information assurance from Norwich University. He is the author of SANS' only 700-level course, SEC710: Advanced Exploit Development, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. @Steph3nSims

## 660.1 HANDS ON: Network Attacks for Penetration Testers

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

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

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

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

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

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

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

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

## 660.4 HANDS ON: Exploiting Linux for Penetration Testers

Day four begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. 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

### 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

## 660.5 HANDS ON: Exploiting Windows for Penetration Testers

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

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

## 660.6 HANDS ON: Capture the Flag

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

giac.org

sans.org/cyber-guardian

sans.edu

FORENSICS 408

# Windows Forensic Analysis

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Pilkington

- GIAC Cert: GCFE
- Masters Program

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

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

## Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

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

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

**"FOR408 is going to help me obtain my GCFE certification, and will help me in my day-to-day job as a digital forensic associate."**
-Christine Casey, Stroz Friedberg

**"FOR408 provides in-depth knowledge of the best forensic practices that can be applied directly to investigations."**
-Nathan Lewis, KPMG

## FOR408 Windows Forensic Analysis will teach you to:

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

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

DFIR
digital-forensics.sans.org

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

**Mike Pilkington** *SANS Instructor*

Mike Pilkington is a senior security consultant for a Fortune 500 company in the oil & gas industry. He has been an IT professional since graduating in 1996 from the University of Texas with a B.S. in Mechanical Engineering. Since joining his company in 1997, he has been involved in software quality assurance, systems administration, network administration, and information security. Outside of his normal work schedule, Mike has also been involved with the SANS Institute as a mentor and instructor in the digital forensics program. @mikepilkington

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

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

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

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

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

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

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

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

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

## 408.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 – Windows Artifact and Log File Analysis

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

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

## 408.5 HANDS ON: CORE WINDOWS FORENSICS PART 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome

This section looks at Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what individuals did while surfing via their web browser. The results will give you pause the next time you use the web.

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

## 408.6 HANDS ON: Windows Forensic Challenges

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

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

giac.org

sans.edu

### You Will Be Able To

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

FORENSICS 508

# Advanced Computer Forensic Analysis and Incident Response

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee

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

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.*

## 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

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?

**ATTEND REMOTELY**

**SIMULCAST**

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

*More info on page 52*

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

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

**"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."**
-Naveel Koya,
A C-DAC - Trivandrum

**"FOR508 has an interesting curriculum delivered flawlessly, with hands-on labs that reinforce the material covered."**
-Everett Sherlock, Kapstone Paper

DFIR
digital-forensics.sans.org

**Chad Tilbury** *SANS Senior Instructor*

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a Special Agent with the Air Force Office of Special Investigations, he investigated and conducted computer forensics for a variety of crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and as the Vice President of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Chad is a graduate of the U.S. Air Force Academy and holds a B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. @chadtilbury

## 508.1 HANDS ON: Enterprise Incident Response

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

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

## 508.2 HANDS ON: Memory Forensics

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

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

## 508.3 HANDS ON: Timeline Analysis

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

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

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

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

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

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

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

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

## 508.6 HANDS ON: The Incident Response & Intrusion Forensic Challenge

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

giac.org

sans.org/cyber-guardian

sans.edu


DoDD 8570 Required
sans.org/8570

### You Will Be Able To

- Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hackivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- Use the SIFT Workstation's capabilities, and perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- Use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data the attacker has collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS $I30 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, and recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistent mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autorunsc, psexec, jobparser, group policy, triage-ir, and IOCFinder

FORENSICS 526

# Memory Forensics In-Depth

NEW

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Alissa Torres

"Very valuable for what my group is doing at JPL. With the acquisition of MIR and RAM in first response, this is exactly the skill set we need to master."
-Rick Smith, Jet Propulsion Lab

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

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

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

## 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

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

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

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

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

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

DFIR
digital-forensics.sans.org

## Alissa Torres *SANS Certified Instructor*

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

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

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

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

## 526.2 HANDS ON: Unstructured Analysis and Process Exploration

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

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

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

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

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

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

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

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

### 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

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

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

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

## 526.6 HANDS ON: Final Day Memory Analysis Challenge

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

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

FORENSICS 610

# Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jake Williams

- GIAC Cert: GREM
- Masters Program

## Who Should Attend

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

**"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats."**
-Paul Gunnerson, U.S. Army

**"The training is very well documented with lots of hands-on labs, in addition, all topics are discussed thoroughly and reinforced."**
-Chaz Hobson, Deutsche Bank

ATTEND REMOTELY

SIMULCAST

If you are unable to attend this event, this course is also available via SANS Simulcast.
*More info on page 52*

DFIR
digital-forensics.sans.org

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

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

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

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

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

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

**Jake Williams** *SANS Certified Instructor*

Jake Williams is the chief scientist at CSRgroup computer security consultants and has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before joining CSRgroup, he worked with various government agencies in information security roles. Jake is a two-time victor at the annual DC3 Digital Forensics Challenge. @MalwareJake

## 610.1 HANDS ON: Malware Analysis Fundamentals

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

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

## 610.2 HANDS ON: Malicious Code Analysis

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

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

## 610.3 HANDS ON: In-Depth Malware Analysis

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

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

### You Will Be Able To

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

## 610.4 HANDS ON: Self-Defending Malware

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

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

## 610.5 HANDS ON: Malicious Documents and Memory Forensics

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

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

## 610.6 HANDS ON: Malware Reverse-Engineering Tournament

Section six assigns students to the role of a malware reverse engineer working as a member of an incident response and malware analysis team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a student's ability to respond to typical malware-reversing tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, the challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice. The students who score the highest in the malware reverse-engineering challenge will be awarded the coveted SANS' Digital Forensics Lethal Forensicator coin. Game on!

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

giac.org

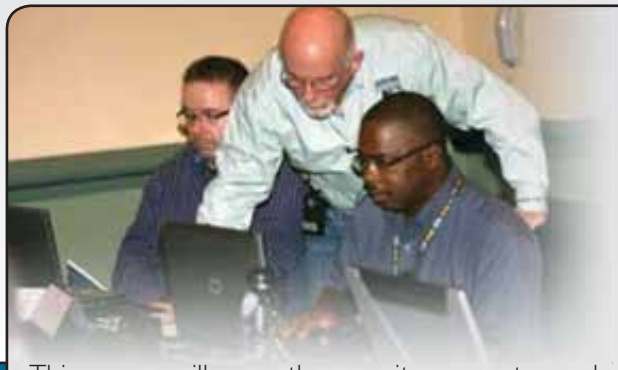
sans.edu

MANAGEMENT 414

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

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 7:00pm (Day 1)
8:00am - 7:00pm (Days 2-5)
8:00am - 5:00pm (Day 6)
46 CPEs
Laptop NOT Needed
Instructor: Paul A. Henry

- GIAC Cert: GISP
- DoDD 8570



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

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

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

## Who Should Attend

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

## You Will Receive With This Course:

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

## Obtaining Your CISSP® Certification Consists of:

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

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

**"MGT414 offers a good top-level look at the information – it helps to know what to focus on."**
-Paul Gunnerson, U.S. Army

**"Great course and well worth it if you are considering taking the CISSP exam."**
-David Raymond, U.S. Army

## 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. @phenrycissp

## 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

### You Will Be Able To

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

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

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

## 414.4 Cryptography and Security Architecture and Design

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

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

## 414.5 Security Operations and Business Continuity and Disaster Recovery Planning

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

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

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

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

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

giac.org


DoDD 8570 Required
sans.org/8570

**Take advantage of SANS CISSP® Get Certified Program currently being offered.**
sans.org/special/cissp-get-certified-program

MANAGEMENT 512

# SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
Fri, Dec 12 - Tue, Dec 16
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: G. Mark Hardy

- GIAC Cert: GSLC
- Masters Program
- DoDD 8570

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

## Who Should Attend

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

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.

**"Excellent instruction. I will be sending more managers to MGT512, and requesting Hardy."**
-Jason Payne, Alert Logic

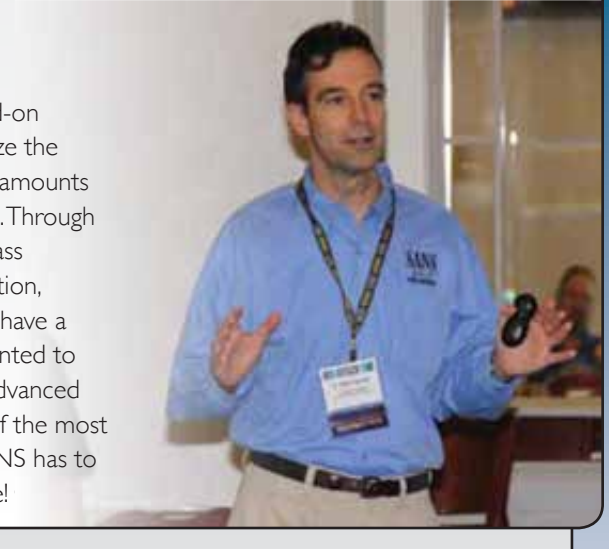
**"MGT512 is awesome! Lots of material covered, so I will need to go back and read the notes and study more. The course was very structured, relevant, and concise."**
-Juan Canino, SWIFT

**"G. Mark Hardy was very knowledgeable on the subject matter and delivered the course material clearly."**
-Carl Ford, Burke & Herbert Bank

## Knowledge Compression™

***Maximize your learning potential!***

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



**G. Mark Hardy** *SANS Certified Instructor*

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

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

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

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

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

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

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

## 512.3 Secure Communications

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

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

### 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.

## 512.4 The Value of Information

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

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

## 512.5 Management Practicum

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

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

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

giac.org

sans.edu


DoDD 8570 Required
sans.org/8570

AUDIT 507

# Auditing & Monitoring Networks, Perimeters, and Systems

SANS

Six-Day Program
Fri, Dec 12 - Wed, Dec 17
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: David Hoelzer

- GIAC Cert: GSNA
- Masters Program
- DoDD 8570

**"AUD507 provided me additional insight to the technical side of security auditing. Great course and a super instructor!"**
-Carlos Everfield, U.S. Army

**"Providing value to businesses is an important part of my company's work. AUD507 is showing me ways to provide value. David's professional experience is evident and his lecture style is entertaining and interactive."**
-Michael Decker, CNS Security

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

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

## Who Should Attend

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

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

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

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

## David Hoelzer *SANS Faculty Fellow*

David Hoelzer is the author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow in the Center for Cybermedia Research and also a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate of the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @david_hoelzer

## 507.1 Advanced System and Network Auditing

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 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. These diagrams will allow the auditor to identify what objectives the routers and firewalls are seeking to meet, thus allowing controls to be implemented which 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 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

### 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 risk assessment of network to identify vulnerabilities and prioritize what will be audited
- Establish a well-secured baseline for computers and networks, a standard to conduct 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 deci- sions about risk and resources.
- Audit web applications configuration, authentication, and session management 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

## 507.4 Microsoft Windows: Auditing & Continuous Monitoring

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

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

## 507.5 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 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:** Network Devices; Servers; Applications; Workstations

giac.org

sans.edu

DoDD 8570 Required
sans.org/8570

INDUSTRIAL CONTROL SYSTEMS 410

# ICS/SCADA Security Essentials

NEW

SANS

Five-Day Program
Fri, Dec 12 - Tue, Dec 16
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Justin Searle
- GIAC Cert: GICSP

"Excellent content and very informative."
-Khalid Alsomaly, Saudi Aramco

ATTEND REMOTELY

SIMULCAST

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

More info on page 52

## Who Should Attend

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

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

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

*The course will provide you with:*

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

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

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

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

GICSP
giac.org

## Justin Searle *SANS Certified Instructor*

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

HOSTED

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

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

Five-Day Program
Fri, Dec 12 - Tue, Dec 16
9:00am - 5:00pm
35 CPEs
Laptop NOT Needed
Instructor: 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** – knowing what constitutes secure software and what design aspects to take into consideration to architect hack-resilient software
- **Secure Software Requirements** – capturing all of the security requirements from various stakeholders and understanding the sources and processes needed to ensure a more effective design
- **Secure Software Design** – securing design elements, software architecture, securing design review, and conducting threat modeling
- **Secure Software Implementation/Coding** – securing coding practices, vulnerabilities to look for, and how to review the code to ensure that there are no errors in the code or security controls
- **Secure Software Testing** – integrating software testing for security functionality, reliability, resiliency to attack, and recoverability
- **Software Acceptance** – security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria and methods of independent testing
- **Software Deployment, Operations, Maintenance and Disposal** – security issues around steady state operations and management of software – security measures that must be taken when a product reaches its end of life
- **Supply Chain and Software Acquisition** – providing a holistic outline of the knowledge and tasks required in managing risk for outsourced development, acquisition, and procurement of software and related services

## 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.

SECURITY 434

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

Two-Day Course | Wed, Dec 10 - Thu, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Jake Williams

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

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

SECURITY 524

## Cloud Security Fundamentals

Two-Day Course | Wed, Dec 10 - Thu, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Dave Shackleford

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

The SANS Cloud Security Fundamentals course starts out with a detailed introduction to the various delivery models of cloud computing ranging from Software as a Service (SaaS) to Infrastructure as a Service (IaaS) and everything in between. Each of these delivery models represents an entirely separate set of security conditions to consider, especially when coupled with various cloud types including: public, private, and hybrid. An overview of security issues within each of these models will be covered with in-depth discussions of risks to consider. Attendees will go in-depth on architecture and infrastructure fundamentals for private, public, and hybrid clouds. A wide range of topics will be covered including: patch and configuration management, virtualization security, application security, and change management. Policy, risk assessment, and governance within cloud environments will be covered with recommendations for both internal policies and contract provisions to consider. This path leads to a discussion of compliance and legal concerns. The first day will wrap-up with several fundamental scenarios for students to evaluate.

Attendees will start off the second day with coverage of audits and assessments for cloud environments. The day will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as evaluating audit and monitoring controls. Next the class will turn to protecting the data itself! New approaches for data encryption, network encryption, key management, and data lifecycle concerns will be covered in-depth. The challenges of identity and access management in cloud environments will be covered. The course will move into disaster recovery and business continuity planning using cloud models and architecture. Intrusion detection and incident response in cloud environments will be covered along with how best to manage these critical security processes and technologies that support them given that most controls are managed by the CSP.

## SECURITY SKILL-BASED COURSE

SECURITY 580

### Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Thu, Dec 18 - Fri, Dec 19 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Eric Conrad

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

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

## MANAGEMENT SKILL-BASED COURSES

MANAGEMENT 305

### Technical Communication and Presentation Skills for Security Professionals

One-Day Course | Thu, Dec 11 | 9:00am - 5:00pm
6 CPEs | Laptop Required | Instructor: David Hoelzer

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

sans.edu

MANAGEMENT 415

### A Practical Introduction to Risk Assessment

One-Day Course | Sun, Oct 19 | 9:00am - 5:00pm | 6 CPEs
Laptop Required | Instructor: James Tarala

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

MANAGEMENT 433

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

Two-Day Course | Wed, Dec 10 - Thu, Dec 11 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Lance Spitzner

Organizations have invested a tremendous amount of money and resources into securing technology, but little, if anything, into securing the human element. As a result, people are now the weakest link; the simplest way for cyber attackers to hack into any organization is to target your employees. One of the most effective ways to secure the human element is to build an active awareness and education program that goes beyond just compliance and changes behaviors. In this challenging course you will learn how to do just that. You will learn the key concepts and skills needed to build, maintain and measure a high-impact security awareness program. All course content is based on lessons learned from hundreds of organizations around the world. In addition, you will learn not only from extensive interaction with the instructor, but from working with your peers, as well. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so that you can immediately implement your own customized awareness program upon returning to your organization.

sans.edu

### Who Should Attend

- Security awareness training officers
- Chief Security Officers (CSO's) and security management
- Security auditors, governance, and compliance officers
- Training, human resources and communications staff
- Organizations regulated by 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

ATTEND REMOTELY

SIMULCAST

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

More info on page 52

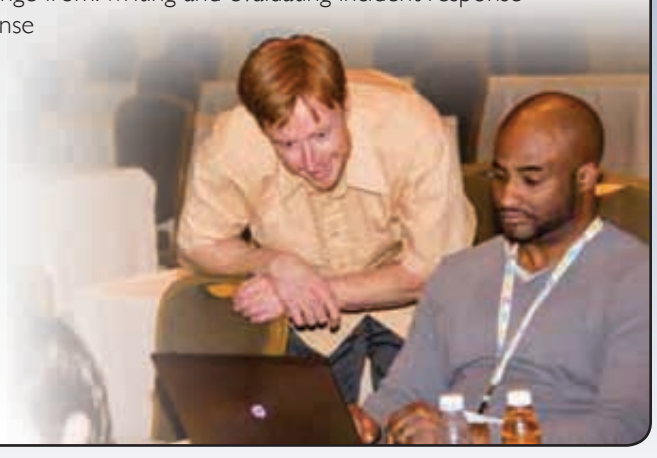
MANAGEMENT 535

## Incident Response Team Management

One-Day Course | Thu, Dec 11 | 9:00am - 5:00pm | 6 CPEs | Laptop NOT Needed | Instructor: Christopher Crowley

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

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



### 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


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

HOSTED

## Physical Penetration Testing – Introduction

Two-Day Program
Wed, Dec 10 - Thu, Dec 11
9:00am - 5:00pm
12 CPEs
Laptop NOT Needed
Instructor: Deviant Ollam

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

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

### Who Should Attend

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

HOSTED

NEW

## Embedded Device Security Assessments For The Rest Of Us

Two-Day Program
Wed, Dec 10 - Thu, Dec 11
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: Paul Asadoorian

The Internet of Things has grown large enough to affect us all in a variety of ways (both positively and negatively!). Whether you are a penetration tester or working in IT security for your organization, you've encountered an embedded device (or 10) that likely contains vulnerabilities. The challenges we all face is how to assess the security of these devices accurately, efficiently, and thoroughly. If you've wondered how much damage attackers can do with devices such as printers, wireless routers, thermostats, TVs, and even Wi-Fi-enabled treadmills, look no further than this course. If you've wondered just how to test "The Internet of Things" for security without crashing the device and uncover its hidden secrets, this course will satisfy your curiosity. The goal of this course is to enable you to uncover embedded system's vulnerabilities as part of your duties as a security professional.

### Who Should Attend

- Individuals responsible for securing systems in an organizations
- Consultants performing penetration testing for clients
- Systems administrators who are responsible for maintaining embedded systems

HOSTED

## Offensive Countermeasures: The Art of Active Defenses

Two-Day Program
Thu, Dec 18 - Fri, Dec 19
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructors Mick Douglas

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

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

### Who Should Attend

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

# 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:

### Continuous Ownage: Why You Need Continuous Monitoring

*Eric Conrad*

Repeat after me, I will be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring. The talk will also give you a hint at the value you and your organization will gain from attending Seth Misenar and Eric Conrad's new course: **SEC511: Continuous Monitoring and Security Operations**.

### Securing The Kids

*Lance Spitzner*

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

### 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.

### Gone in 60 Minutes: Have You Patched Your System Today?

*David Hoelzer*

In our industry we hear about new vulnerabilities every day, but there can be a perception that moving from the discovery of a flaw to a workable exploit is very difficult. The result is that most organizations are perfectly happy operating with a 30 day patch rollout cycle. Is this really fast enough? How hard is it really to exploit a vulnerability? How hard is it to scale a proof of concept into a working tool that can compromise thousands of hosts? This presentation demonstrates the entire process, walking through the process that a security researcher or hacker follows from research through proof of concept and working exploit... al in less than 60 minutes. While aspects of this presentation can be somewhat technical, the emphasis isn't on the technical but on the process and speed with which a working exploit can be developed. There's something for everyone to take away from this presentation!

### Security Awareness Metrics: Measuring Human Behavior

*Lance Spitzner*

Security awareness is nothing more than another control designed to reduce risk, specifically human risk. This session will discuss the different ways organizations are effectively measuring human risk, which methods are proving to be the most successful, and steps you can take to have successful metrics for your awareness program.

# BONUS SESSIONS

## A Night of Crypto

*G. Mark Hardy*

Want to learn a bit more about cryptography but not get wrapped up in the math? G. Mark Hardy has been writing crypto contests for major hacker conferences for years (DEFCON, Toorcon, Shmoocon, THOTCON, SkyDogCon, etc.), and is going to share insights into the reasons behind cryptography, why some algorithms work and some fail, and a look at what's in use in business today. We'll even cover the cryptographic principles behind Bitcoin. Plus, you'll get a chance to see how crypto puzzles are designed, which might give you some ideas for your own.

## 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

## IT Security Meets Research: Lessons from NASA's Science Labs

*Joel Offenberg*

IWith a complicated web of partnerships, customized equipment, always-changing configurations, and arbitrary deadlines, securing a science lab's computer systems can seem to be a daunting task. The solutions to securing the lab can be elegant or expensive, complicated or cheap or anywhere in-between...and can be used in other challenging environments. The author discusses solutions for research lab cybersecurity based on his experiences working with scientists and engineers as a NASA contractor.

## Everything They Told Me About Security Was Wrong

*John Strand*

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

**Find complete details at sans.org/event/cyber-defense-initiative-2014/bonus-sessions**

## Vendor Expo

**Monday, December 15, 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

**Monday, December 15, 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 CDI 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

**Monday, December 15, 2014 | 5:00pm - 7:00pm**

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

# SANS LIVE ONLINE TRAINING

*Train Day or Night from Any Location*

## DAYTIME ONLINE TRAINING

SIMULCAST

**SANS Simulcast training allows you to complete live SANS courses in five or six full days, and includes four months of online access.**

## *Can't travel to CDI 2014?*

***The following courses will be Simulcast live from the event:***

SEC401 | SEC504 | SEC505 | FOR508 | FOR610 | ICS410 | MGT433

sans.org/simulcast

## EVENING ONLINE TRAINING

VLIVE

SANS vLive training allows you to complete live SANS courses in five or six weeks, meeting two evenings per week.

**vLive courses also include 6 months of online access**

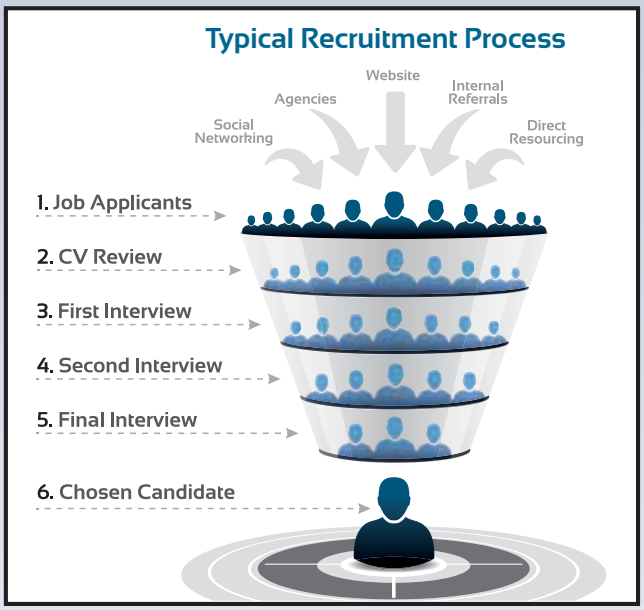
To see a list of upcoming live evening courses, visit

sans.org/vlive

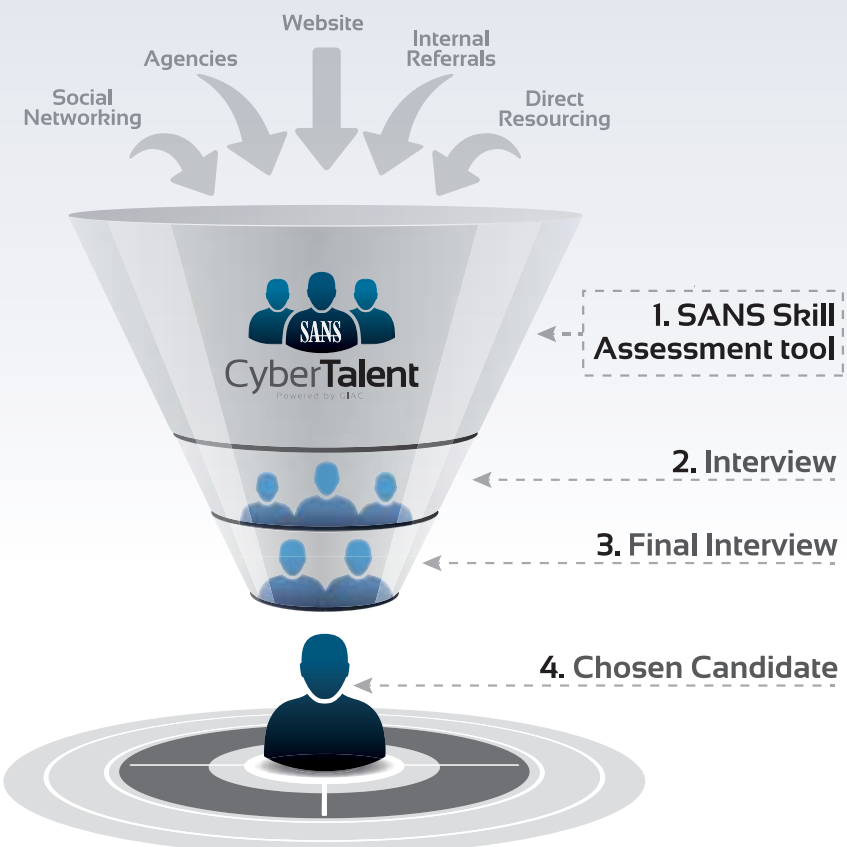
SANS CyberTalent
Powered by GIAC

## How SANS CyberTalent Assessments Work

SANS CyberTalent is a web-based skills evaluation tool that enables hiring managers and recruiters to accurately gauge the skillset of information security job applicants and current staff. 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.




## Future Recruitment Process




SANS CyberTalent
Powered by GIAC

**Using the SANS Skills Assessment tool will have the following results:**

1. Greatly increase the candidate pool
2. Reduce in interview and admin time by cutting out two stages of the recruitment process
3. Provide clear knowledge that the people you are interviewing can do what they say they can (and sometimes more!)

# 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 26 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, IT security law, and industrial control systems.

*"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**

# The SANS Technology Institute

## *Graduate Programs in Information Security*

### Master of Science Degrees
### Example: Information Security Engineering (MSISE)

#### REQUIRED COURSES

| | | | *SANS & GIAC Elements* |
|---|---|---|---|
| **FIRST YEAR** 13.5 CREDITS | ISE 5100 | Engineering Enterprise Information Security | SEC401 \| GSEC & Gold Paper |
| | ISE 5000 | Research & Communications | MGT305 |
| | ISE 5200 | Hacking Techniques & Incident Response | SEC504 \| GCIA \| NetWars |
| | ISE 5300 | Building Security Awareness | MGT433 |
| | ISE 5400 | Advanced Network Intrusion Detection | SEC503 \| GCIA & Gold Paper |
| **SECOND YEAR** 13 CREDITS | ISE 5500 | Research Presentation I | |
| | ISE 6000 | Standards-based Enterprise Controls | SEC566 \| GCCC & Gold Paper |
| | ISE 6xxx | Technical Elective I | *See below* |
| | ISE 5600 | IT Security Leadership Competencies | MGT514.5 |
| | ISE 5800 | IT Security Project Management | MGT525 \| GCPM |
| | ISE 5700 | Incident Response Practicum (24-hour group project) | |
| **THIRD YEAR** 9.5 CREDITS | ISE 5900 | Research Presentation II | |
| | ISE 6xxx | Technical Elective II | *See below* |
| | ISE 6100 | Security Project Practicum (30-day group project) | |
| | ISE 6xxx | Technical Elective III | *See below* |
| | ISE 6900 | Information Security Fieldwork | |
| | Capstone | GIAC Security Expert Exam | GSE |

#### ELECTIVE COURSE OPTIONS

**Cyber Defense**

ISE 6215: Advanced Security Essentials
ISE 6220: Network Perimeter Protection
ISE 6230: Securing Windows with the Critical Security Controls
ISE 6235: Securing Linux/Unix

**Digital Forensics & Incident Response**

ISE 6420: Computer Forensics – Windows
ISE 6425: Advanced Computer Forensics – Windows
ISE 6440: Advanced Network Forensic Analysis
ISE 6460: Malware Analysis and Reverse Engineering

**Penetration Testing & Ethical Hacking**

ISE 6315: Web App PenTesting
ISE 6320: Network PenTesting
ISE 6325: Mobile Device Security
ISE 6330: Wireless Pen Testing
ISE 6360: Advanced Network PenTesting

**Software Development, Audit, Legal**

ISE 6615: Defending Web Application Security Essentials
ISE 6715: Auditing & Monitoring Networks, Perimeters, and Systems
ISE 6720: Legal Issues In Data Security and Investigations



### Focused Graduate Certificate Programs

Penetration Testing & Ethical Hacking | Incident Response | Cybersecurity Engineering (Core)

The SANS Technology Institute makes shorter groups of courses available to students who are unable to commit to a full master's degree program. These certificate programs will augment your skills, provide specialized training, and impart a credential that will help advance your career. Because these course progressions are from an accredited school, they likely qualify for tuition reimbursement plans.

The SANS Technology Institute offers three of its most popular graduate course progressions as certificate programs for credit. You can choose from:

| **Penetration Testing & Ethical Hacking Certificate** - 13 credit hours | | | |
|---|---|---|---|
| ISE 5200 | Hacking Techniques and Incident Response | SEC504 | GCIH, NetWars |
| ISE 6315 | Web Application Penetration Testing and Ethical Hacking | SEC542 | GWAPT |
| ISE 6320 | Network Penetration Testing & Ethical Hacking | SEC560 | GPEN |
| *Select one of the following:* | | | |
| ISE 6325 | Mobile Device Security | SEC575 | GMOB |
| ISE 6330 | Wireless Networks Penetration Testing | SEC617 | GAWN |
| ISE 6360 | Advanced Network Penetration Testing | SEC660 | GXPN |

| **Incident Response Certificate** - 13 credit hours | | | |
|---|---|---|---|
| ISE 5200 | Hacking Techniques and Incident Response | SEC504 | GCIH, NetWars |
| ISE 6425 | Advanced Computer Forensic Analysis and Incident Response | FOR508 | GCFA |
| ISE 6440 | Advanced Network Forensics Analysis | FOR572 | GNFA |
| ISE 6460 | Malware Analysis and Reverse Engineering | FOR610 | GREM |

| **Cybersecurity Engineering (Core) Certificate** - 12 credit hours | | | |
|---|---|---|---|
| ISE 5100 | Engineering Enterprise Information Security | SEC401 | GSEC & Gold Paper |
| ISE 5200 | Hacking Techniques and Incident Response | SEC504 | GCIH, NetWars |
| ISE 5400 | Advanced Network Intrusion Detection and Analysis | SEC503 | GCIA & Gold Paper |

**Apply now at www.sans.edu**


# SANS CYBER GUARDIAN PROGRAM

www.sans.org/
cyber-guardian

**Stay ahead of cyber threats!**

**Join the SANS Cyber Guardian Program today.**

## How the Program Works

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

# 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<br>Network+CE<br>SSCP | **GSEC**<br>Security+CE<br>SSCP | **GCED**<br>**GCIH**<br>**CISSP**<br>(or Associate)<br>CISA, CASP | **GSLC**<br>CAP<br>Security+CE | **GSLC**<br>**CISSP**<br>(or Associate)<br>CAP, CASP<br>CISM | **GSLC**<br>**CISSP**<br>(or Associate)<br>CISM |

### Computer Network Defense (CND) Certifications

| CND Analyst | CND Infrastructure Support | CND Incident Responder | CND Auditor | CND Service Provider Manager |
|---|---|---|---|---|
| **GCIA**<br>**GCIH**<br>CEH | SSCP<br>CEH | **GCIH**<br>**GCFA**<br>CSIH, CEH | **GSNA**<br>CISA<br>CEH | CISSP - ISSMP<br>CISM |

### Information Assurance System Architecture & Engineering (IASAE) Certifications

| IASAE I | IASAE II | IASAE III |
|---|---|---|
| **CISSP**<br>(or Associate)<br>CASP, CSSCP | **CISSP**<br>(or Associate)<br>CASP, CSSLP | CISSP - ISSEP<br>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

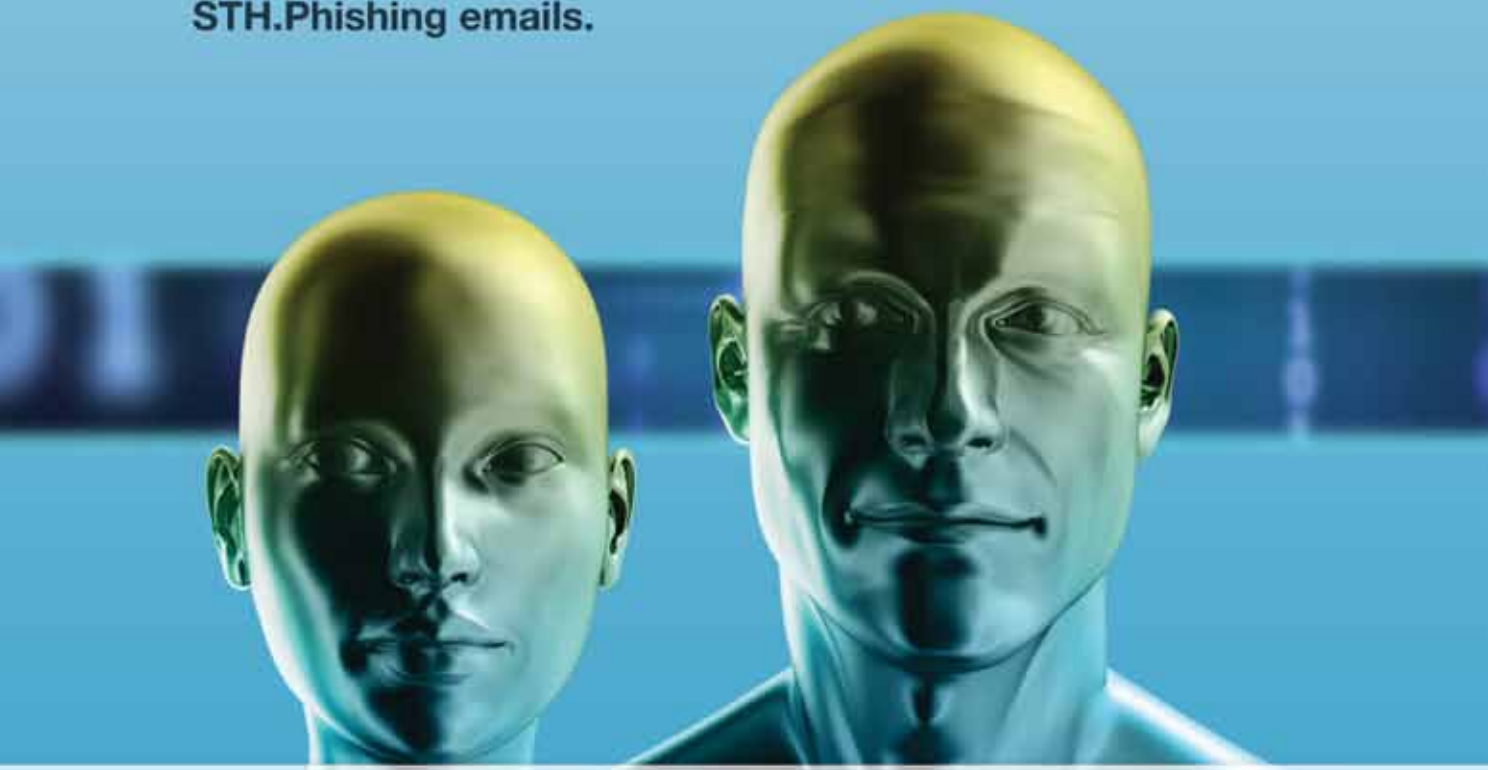
| SANS TRAINING COURSE | | DoDD APPROVED CERT |
|---|---|---|
| SEC401 | **Security Essentials Bootcamp Style** | **GSEC** |
| SEC501 | **Advanced Security Essentials – Enterprise Defender** | **GCED** |
| SEC503 | **Intrusion Detection In-Depth** | **GCIA** |
| SEC504 | **Hacker Techniques, Exploits, and Incident Handling** | **GCIH** |
| AUD507 | **Auditing & Monitoring 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** |

# SECURITY AWARENESS

## FOR THE 21ST CENTURY

### End User - Utility - Engineer - Developer - Phishing

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



SANS SECURING THE HUMAN

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

# FUTURE SANS TRAINING EVENTS

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

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


SANS
## Security East
New Orleans, LA
Jan 16-21, 2015

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

SANS
## Scottsdale
Scottsdale, AZ
Feb 16-21, 2015


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

SANS DFIRCON WEST
Monterey, CA Feb 23-28, 2015

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


SANS
## Cyber Guardian
Baltimore, MD
Mar 2-7, 2015

SANS DFIRCON EAST
Fort Lauderdale, FL Nov 3-8, 2014

SANS
## Northern Virginia
Reston, VA
Mar 19-25, 2015

CYBER DEFENSE INITIATIVE

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

SANS
## Houston
Houston, TX
March 2015

# FUTURE SANS TRAINING EVENTS

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

## SANS 2015

Orlando, FL
Apr 11-20, 2015

SANS
## Austin Pen Test

Austin, TX
May 18-23, 2015

SANS
## Security West

San Diego, CA
May 5-10, 2015

## SANSFIRE

Baltimore, MD
June 11-22, 2015

# SANS TRAINING FORMATS

## LIVE CLASSROOM TRAINING

### Training Events
***Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers***
sans.org/security-training/by-location/all

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

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

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

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

## ONLINE TRAINING

### OnDemand
***E-learning Available Anytime, Anywhere, at Your Own Pace***
sans.org/ondemand

### vLive
***Online Evening Courses with SANS' Top Instructors***
sans.org/vlive

### Simulcast
***Attend a SANS Training Event without Leaving Home***
sans.org/simulcast

### OnDemand Bundles
***Extend Your Training with an OnDemand Bundle Including Four Months of E-learning***
sans.org/ondemand/bundles

# FUTURE SUMMIT EVENTS

*Summits provide a unique experience where people, ideas, and solutions connect.*

## Pen Test Hackfest
SUMMIT & TRAINING

**Washington, DC | Nov 13-20, 2014**

*Courses offered:*

| | | |
|---|---|---|
| SEC542 | SEC561 | SEC573 |
| SEC560 | | SEC642 |

## Healthcare Cyber Security
SUMMIT & TRAINING

**San Francisco, CA | Dec 3-10, 2014**

*Courses offered:*

| | | |
|---|---|---|
| SEC301 | SEC542 | FOR508 |
| SEC504 | | ICS410 |

## Cyber Threat Intelligence
SUMMIT & TRAINING

**Washington, DC | Feb 2-9, 2015**

*Courses offered:*

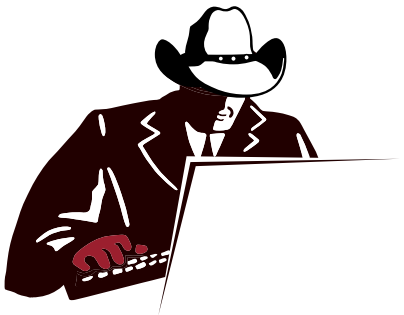
| | | |
|---|---|---|
| FOR572 | SEC401 | SEC511 |
| | SEC504 | |

## ICS Security
SUMMIT & TRAINING

**Orlando, FL | Feb 23 - Mar 1, 2014**

*Courses offered:*

| | | |
|---|---|---|
| ICS410 | MGT405 | 2 Hosted |
| SEC562 | MGT433 | Courses |



## Digital Forensics Incident Response
SUMMIT & TRAINING

**Austin, TX | Jul 7-14, 2014**

*Courses offered:*

| | | |
|---|---|---|
| FOR408 | FOR572 | FOR610 |
| FOR508 | | DFIR NetWars |

# HOTEL INFORMATION

*Training Campus*

## Grand Hyatt Washington

1000 H Street NW

Washington, DC 20001

sans.org/event/cyber-defense-initiative-2014/location

Experience the upscale elegance of Grand Hyatt Washington, a full-service Washington, DC hotel. Centrally located in the trendy Penn Quarter near popular local attractions, Grand Hyatt Washington is ideally situated, a welcoming destination with a host of world-class services and amenities, and convenient Metro Center access directly from the lobby.

### Special Hotel Rates Available

**A special discounted rate of $209.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through November 18, 2014. To make reservations, please use the following links:**

**For rooms at the SANS group rate:**
https://resweb.passkey.com/go/SansInstitute2014

**For rooms at the Government rate:**
https://resweb.passkey.com/go/SansGovernmentRooms

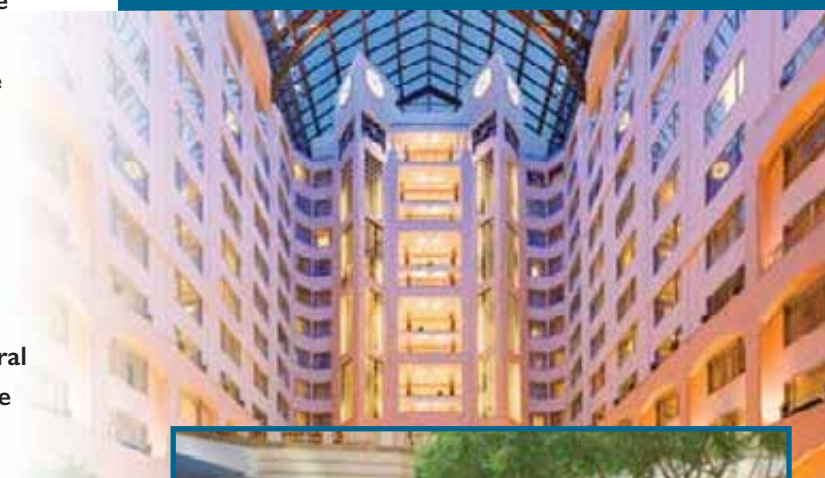
**You can also make reservations by calling Central Reservations at 888-421-1442 and asking for the SANS group rate.**

### Weather Conditions

December in Washington, DC is mild with highs around 48° and lows near 28°. For the latest weather conditions and forecast, please consult weather.com.

### Top 5 reasons to stay at the Grand Hyatt Washington

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 Grand Hyatt Washington, 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 Grand Hyatt Washington that you won't want to miss!
5. Everything is in one convenient location!




# REGISTRATION INFORMATION

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

## How to Register

**1. To register, go to sans.org/event/cyber-defense-initiative-2014/courses.**

Select your course or courses and indicate whether you plan to test for GIAC certification. If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. We do not take registrations by phone.

**2. Provide payment information.**

**3. Print your invoice.**

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

## Register Early and Save

| | DATE | DISCOUNT | DATE | DISCOUNT |
|---|---|---|---|---|
| Register & pay by | 10/22/14 | $400.00 | 11/12/14 | $200.00 |

Some restrictions apply.

## Group Savings (Applies to tuition only)

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

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

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

**To register for a CDI 2014 Simulcast course, please visit sans.org/event/cyber-defense-initiative-2014/attend-remotely**


## Group Discounts for SANS Security Training

sans.org/vouchers

### SANS Universal Voucher Credit Program

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


## Get GIAC Certified!

- Only $599 when combined with SANS training
- Deadline to register at this price is the last day of SANS CDI 2014
- Price goes to $899 after deadline
- Register today at registration@sans.org

## Frequently Asked Questions

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

## Cancellation Policy

If an attendee must cancel, a substitution request may be made at any time. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org.

If an attendee must cancel without substitution, a refund can be issued for any received payments. All cancellation requests must be submitted in writing by mail or fax and postmarked by Oct 1, 2014. Payments will be refunded by the method that they were submitted. Processing fees will apply. No refunds will be given after the stated deadline. Accessed online materials cannot be transferred to a substitute nor have payments refunded.

# CDI 2014 REGISTRATION FEES

Register online at sans.org/event/cyber-defense-initiative-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 10/22/14 | Paid by 11/12/14 | Paid after 11/12/14 | Add GIAC Cert | Add OnDemand |
|---|---|---|---|---|---|---|
| ☐ SEC301 | Intro to Information Security | $4,215 | $4,415 | $4,615 | ☐ $599 | ☐ $599 |
| ☐ SEC401 | Security Essentials Bootcamp Style | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC501 | Advanced Security Essentials – Enterprise Defender | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC503 | Intrusion Detection In-Depth | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC504 | Hacker Techniques, Exploits, and Incident Handling | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC505 | Securing Windows with the Critical Security Controls | $4,875 | $5,075 | $5,275 | ☐ $599 | ☐ $599 |
| ☐ SEC542 | Web Application Penetration Testing and Ethical Hacking | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC562 | CyberCity Hands-on Kinetic Cyber Range Exercise NEW! | $5,895 | $6,095 | $6,295 | | |
| ☐ SEC566 | Implementing and Auditing the Critical Security Controls – In-Depth | $4,370 | $4,570 | $4,770 | ☐ $599 | ☐ $599 |
| ☐ SEC575 | Mobile Device Security and Ethical Hacking | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ SEC579 | Virtualization and Private Cloud Security | $4,950 | $5,150 | $5,350 | | ☐ $599 |
| ☐ SEC660 | Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ FOR408 | Windows Forensic Analysis | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ FOR508 | Advanced Computer Forensic Analysis and Incident Response | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ FOR526 | Memory Forensics In-Depth NEW! | $4,950 | $5,150 | $5,350 | | ☐ $599 |
| ☐ FOR610 | Reverse-Engineering Malware: Malware Analysis Tools and Techniques | $4,950 | $5,150 | $5,350 | ☐ $599 | ☐ $599 |
| ☐ MGT414 | SANS® +S™ Training Program for the CISSP® Certification Exam | $4,215 | $4,415 | $4,615 | ☐ $599 | ☐ $599 |
| ☐ MGT512 | SANS Security Leadership Essentials For Managers with Knowledge Compression™ | $4,595 | $4,795 | $4,995 | ☐ $599 | ☐ $599 |
| ☐ AUD507 | Auditing & Monitoring Networks, Perimeters, and Systems | $4,740 | $4,940 | $5,140 | ☐ $599 | ☐ $599 |
| ☐ ICS410 | ICS/SCADA Security Essentials NEW! | $4,215 | $4,415 | $4,615 | ☐ $599 | ☐ $599 |
| ☐ HOSTED | (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program | $3,145 | $3,145 | $3,145 | | |

## Skill-Based Short Courses

| | | If taking a 5-6 day course | | | | |
|---|---|---|---|---|---|---|
| ☐ SEC434 | Log Management In-Depth: Compliance, Security, Forensics, and Troubleshooting | $1,450 | $2,255 | $2,255 | $2,255 | |
| ☐ SEC524 | Cloud Security Fundamentals | $1,250 | $1,980 | $1,980 | $1,980 | |
| ☐ SEC580 | Metasploit Kung Fu for Enterprise Pen Testing | $1,250 | $1,980 | $1,980 | $1,980 | |
| ☐ MGT305 | Technical Communication and Presentation Skills for Security Professionals | $750 | $1,150 | $1,150 | $1,150 | |
| ☐ MGT415 | A Practical Introduction to Risk Assessment | $750 | $1,150 | $1,150 | $1,150 | |
| ☐ MGT433 | Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program | $1,350 | $1,980 | $1,980 | $1,980 | |
| ☐ MGT535 | Incident Response Team Management | $750 | $1,150 | $1,150 | $1,150 | |
| ☐ HOSTED | Physical Penetration Testing – Introduction | | $1,900 | $1,900 | $1,900 | |
| ☐ HOSTED | Embedded Device Security Assessments for the Rest of Us | | $1,900 | $1,900 | $1,900 | |
| ☐ HOSTED | Offensive Countermeasures: The Art of Active Defenses | | $1,700 | $1,700 | $1,700 | |
| ☐ SPECIAL | Core NetWars – Tournament Entrance Fee | FREE | $1,299 | $1,299 | $1,299 | |
| ☐ SPECIAL | DFIR NetWars – Tournament Entrance Fee | FREE | $1,299 | $1,299 | $1,299 | |

## Individual Courses Available

| | FRI 12/12 | SAT 12/13 | SUN 12/14 | MON 12/15 | TUE 12/16 | WED 12/17 |
|---|---|---|---|---|---|---|
| AUD507 | ☐ 507.1 | ☐ 507.2 | ☐ 507.3 | ☐ 507.4 | ☐ 507.5 | ☐ 507.6 |
| SEC301 | ☐ 301.1 | ☐ 301.2 | ☐ 301.3 | ☐ 301.4 | ☐ 301.5 | |
| SEC401 | ☐ 401.1 | ☐ 401.2 | ☐ 401.3 | ☐ 401.4 | ☐ 401.5 | ☐ 401.6 |
| SEC501 | ☐ 501.1 | ☐ 501.2 | ☐ 501.3 | ☐ 501.4 | ☐ 501.5 | ☐ 501.6 |
| SEC503 | ☐ 503.1 | | | | | |
| SEC504 | ☐ 504.1 | | | | | |
| SEC505 | ☐ 505.1 | ☐ 505.2 | ☐ 505.3 | ☐ 505.4 | ☐ 505.5 | ☐ 505.6 |

## Individual Course Day Rates If Not Taking a Full Course

| | |
|---|---|
| ☐ One Full Day | $1,350 |
| ☐ Two Full Days | $2,145 |
| ☐ Three Full Days | $3,025 |
| ☐ Four Full Days | $3,952 |
| ☐ Five Full Days | $4,395 |
| ☐ Six Full Days | $5,100 |
| ☐ Seven Full Days | $5,475 |
| ☐ Eight Full Days | $5,995 |

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

Setting the Standard for Security Training

SANS

SANS is the most trusted and by far the largest source for information security training, certification, and research in the world.

# Five Tips to Get Approval for SANS Training

## 1. EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (inside cover) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.
- Note that the core, job-based courses can be complemented by short, skill-based courses of one or two days. We also offer deep discounts for bundled course packages. Consider a *GIAC Certification*, which will show the world that you have achieved proven expertise in your chosen field.

## 2. RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Promise to share what you've learned with your colleagues.

## 3. SAVE

- The earlier you sign up, the more you save, so explain the benefit of signing up early.
- Save even more with group discounts! See inside for details.

Scan the QR code and register by October 22nd to **SAVE $400** on SANS CDI 2014 courses.

**sans.org/info/162787**

## 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!"*