SANS

The Most Trusted Name in Information and Software Security Training

2015

Orlando, FL

April 11-18, 2015

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

NEW! Continuous Monitoring and Security Operations

NEW! Advanced Exploit Development for Penetration Testers

Security Essentials Bootcamp Style

Hacker Tools, Techniques, Exploits, and Incident Handling

Network Penetration Testing and Ethical Hacking

Windows Forensic Analysis

Web App Penetration Testing and Ethical Hacking

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

SANS 2015 will be held at the

Walt Disney World Swan and Dolphin Resort

"You're getting training from instructors who do this stuff for a living and not from someone who just teaches."

-Scott Avvento, Alpine Cyber Solutions, LCC

Save $400 by registering early!

See page 80 for more details.

GIAC Approved Training

Register at

sans.org/sans-2015

We invite you to our much-anticipated **SANS 2015** Information Security Training at the **Walt Disney World Swan and Dolphin Resort** in Orlando, Florida from April 11-18. SANS' intensive hands-on courses taught by top industry experts will provide you with all the tools and techniques you need for a technical cybersecurity career and help you master the skills to protect your enterprise's most important asset – its information.

This brochure describes more than 38 courses and a variety of training disciplines available at SANS 2015, including IT security, pen testing, mobile device security, hacker techniques, forensics, intrusion detection, security management, and IT auditing. SANS 2015 will also feature two new courses:

- **SEC511: Continuous Monitoring and Security Operations**
- **SEC760: Advanced Exploit Development for Penetration Testers**

In addition, SANS 2015 will feature our always-popular **CORE NetWars** and **DFIR NetWars Tournaments** on the evenings of April 16 and 17. **CORE NetWars Tournament** is a computer and network security challenge that represents real-world security issues, flaws, and resolutions. Participants work through various challenges and levels, with a focus on mastering critical skills. **DFIR NetWars Tournament** is an incident simulator that allows players to progress through multiple skill levels of increasing difficulty. You'll learn first-hand how to solve key challenges you might encounter during a serious incident. **CORE NetWars** and **DFIR NetWars Tournaments** are free with the purchase of a long course, but you must register to participate.

Our **SANS@Night** sessions will enhance your training through bonus presentations and keynote talks by some of the most dynamic speakers in the industry on current and cutting-edge information security topics.

There is a shortage of technical cybersecurity talent and employers are looking for certified information security personnel. **GIAC** certification holders are recognized as experts in the IT industry who demonstrate they have the hands-on skills to protect vital systems and data. Do you need to meet **DoD Directive 8570** requirements? SANS 2015 offers several GIAC certifications that align with those requirements. Complete your training experience and register for a GIAC certification attempt at www.giac.org.

Many of the courses offered at SANS 2015 can be applied toward an accredited Master of Science in Information Security degree at **SANS Technology Institute**. Visit www.sans.edu to learn more about how to start earning your master's degree or graduate certificate.

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

At SANS 2015, you'll learn more than you can imagine and discover countless opportunities to expand your network of security experts and friends. Start making your training and travel plans early and meet us at Disney this April.
Register today for SANS 2015!

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

"A fantastic instructor and now I will need a week to rest my brain!"
-Lorretta Filiault, Dynamac Corporation

"One of the best SANS courses I've taken. Extremely knowledgeable instructor with a great way of relating topics to students so they understand!"
-Ryan Gurr, NuScale Power

"The instructor is very experienced and is very good at communicating his experiences and skills."
-James Medley, Hyperion Technologies, Inc.

"There's a level of knowledge in the field and real-world examples have a great deal of value."
-Jim Gainor, Edmonton Police Service

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

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. These security professionals will dig into technical protocols and specifications for a greater understanding of security threats than most of their 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 Tools, Techniques, Exploits, and Incident Handling **GCIH**

ENTERPRISE	WEB	LAB-CENTERED	MOBILE/WIRELESS
SEC560 Network Penetration Testing and Ethical Hacking **GPEN**	**SEC542** Web App Penetration Testing and Ethical Hacking **GWAPT**	**SEC561** Intense Hands-on Pen Testing Skill Development (with SANS NetWars)	**SEC575** Mobile Device Security and Ethical Hacking **GMOB**
SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**	**SEC642** Advanced Web App Penetration Testing and Ethical Hacking	**SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise	**SEC617** Wireless Ethical Hacking, Penetration Testing & Defenses **GAWN**
SEC760 Advanced Exploit Development for Penetration Testers			

SPECIALIZATION

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 those vulnerabilities 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

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 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 where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC analysts work 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 Tools, Techniques, Exploits, and Incident Handling **GCIH**

The Security Operations Center (SOC) is the focal point for safeguarding against cyber-related incidents, security monitoring, and safeguarding assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous surveillance, 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 Digital Forensics 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 **GSSP-JAVA**
- **DEV544** Secure Coding in .NET: Developing Defensible Applications **GSSP-.NET**

The security-savvy software developer leads all developers in creating secure software and 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

NETWARS

In-Depth, Hands-On InfoSec Skills

sans.org/netwars

NetWars is designed to help participants develop skills in several critical areas:
- Vulnerability Assessment
- 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 Training Program for CISSP Certification®
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: How to Build, Maintain & Measure a High-Impact 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 responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to and mitigate a security incident.

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

CORE COURSES
SEC301 (GISF) ▸ SEC401 (GSEC)

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

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 Digital Forensics 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 Digital Forensics and Incident Response
GCFA

FOR585
Advanced Smartphone Forensics

FOR518
Mac Forensic 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 skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

SANS 2015 ORLANDO BROCHURE CHALLENGE

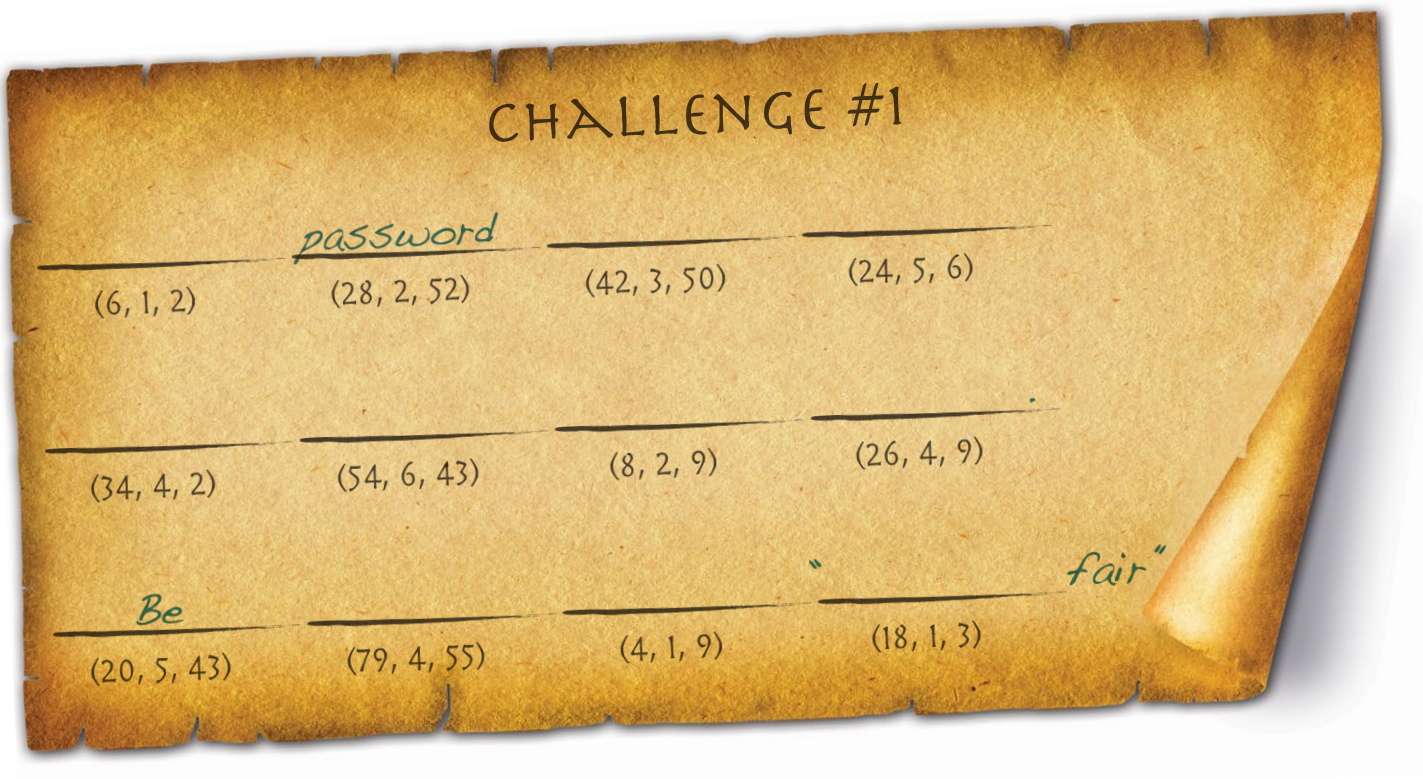
Are you ready for a new SANS challenge – a puzzle that will test your skills in Historical Ciphers, Packet Analysis & Cryptography? This new challenge unfolds from the pages of this brochure, then continues online.

All you need to play is a copy of the SANS 2015 brochure and the Internet (and if you are reading this, you already have the first one)! Please note that the online version of the SANS 2015 – Orlando Challenge works as well. The challenge includes three puzzles (one located below, and the other two online).

So, how can you win? Answer all three puzzle questions correctly to enter a drawing to **win four months of NetWars Continuous, valued at over $2,000!** Make sure to get all your answers in by April 20, 2015 to be eligible for the prize!

How to play:

- Solve Challenge #1 (below)
- Find details for Challenges #2 and #3 online at sans.org/event/sans-2015/brochurechallenge
- Solve all three challenges and submit your answers by April 20, 2015



Rules of Engagement:

- No sharing of challenge links, hints, or write-ups before the contest deadline has passed.
- When a person answers all three challenges correctly they will have their name included in the drawing for NetWars Continuous.
- Contest ends on Monday, April 20, 2015. Responses must be submitted by that evening at 9pm EST.
- Each time a person answers all three challenges correctly they will have their name included in the drawing for NetWars Continuous.
- SANS will choose only one winner, and the odds of winning the contest depend upon the total number of all eligible entries received.
- SANS is not responsible for lost, late, or unintelligible entries, lost connections, miscommunications, failed transmissions, other technical difficulties or failures.

Courses-at-a-Glance

For an up-to-date course list please check the website at sans.org/event/sans-2015/schedule

			SAT 4/11	SUN 4/12	MON 4/13	TUE 4/14	WED 4/15	THU 4/16	FRI 4/17	SAT 4/18
SEC301	Intro to Information Security	SIMULCAST			PAGE 4					
SEC401	Security Essentials Bootcamp Style	SIMULCAST			PAGE 6					
SEC440	Critical Security Controls: Planning, Implementing and Auditing		PAGE 65							
SEC501	Advanced Security Essentials – Enterprise Defender	SIMULCAST			PAGE 8					
SEC503	Intrusion Detection In-Depth	SIMULCAST			PAGE 10					
SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling				PAGE 12					
SEC505	Securing Windows with the Critical Security Controls				PAGE 14					
SEC511	Continuous Monitoring and Security Operations **NEW!**	SIMULCAST			PAGE 16					
SEC524	Cloud Security Fundamentals		PAGE 65							
SEC542	Web App Penetration Testing and Ethical Hacking				PAGE 18					
SEC560	Network Penetration Testing and Ethical Hacking				PAGE 20					
SEC561	Intense Hands-on Pen Testing Skill Development (with SANS NetWars)				PAGE 22					
SEC566	Implementing and Auditing the Critical Security Controls – In-Depth				PAGE 24					
SEC573	Python for Penetration Testers				PAGE 26					
SEC575	Mobile Device Security and Ethical Hacking				PAGE 28					
SEC579	Virtualization and Private Cloud Security				PAGE 30					
SEC580	Metasploit Kung Fu for Enterprise Pen Testing		PAGE 65							
SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses				PAGE 32					
SEC642	Advanced Web App Penetration Testing and Ethical Hacking				PAGE 34					
SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking				PAGE 36					
SEC760	Advanced Exploit Development for Penetration Testers **NEW!**				PAGE 38					
FOR408	Windows Forensic Analysis	SIMULCAST			PAGE 40					
FOR508	Advanced Digital Forensics and Incident Response				PAGE 42					
FOR572	Advanced Network Forensics and Analysis				PAGE 44					
FOR585	Advanced Smartphone Forensics				PAGE 46					
FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques				PAGE 48					
MGT305	Technical Communication and Presentation Skills for Security Professionals			P 66						
MGT414	SANS Training Program for CISSP Certification®				PAGE 50					
MGT415	A Practical Introduction to Risk Assessment			P 66						
MGT433	Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program	SIMULCAST	PAGE 67							
MGT512	SANS Security Leadership Essentials for Managers with Knowledge Compression™				PAGE 52					
MGT514	IT Security Strategic Planning, Policy, and Leadership				PAGE 54					
MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep				PAGE 56					
MGT535	Incident Response Team Management			P 67						
AUD507	Auditing & Monitoring Networks, Perimeters, and Systems				PAGE 58					
DEV522	Defending Web Applications Security Essentials				PAGE 60					
DEV544	Secure Coding in .NET: Developing Defensible Applications				PAGE 61					
LEG523	Law of Data Security and Investigations				PAGE 62					
HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program				PAGE 64					
HOSTED	Offensive Countermeasures: The Art of Active Defenses		PAGE 64							
HOSTED	Physical Penetration Testing – Introduction		PAGE 64							
HOSTED	Health Care Security Essentials **NEW!**		PAGE 64							
	NetWars Tournaments (CORE & DFIR)							PAGE 2		

CONTENTS

SECURITY 301

Intro to Information Security

SANS

Five-Day Program
Mon, April 13 - Fri, April 17
9:00am - 5:00pm
Laptop Required
30 CPEs
Instructor: Keith Palmgren
- GIAC Cert: GISF

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

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

"Mr. Palmgren is amazing! So much knowledge and excellent delivery on all levels. This course really brought to light how much I didn't know about security. I feel better prepared now."
-Valerie Moore, 391OS

"The material presented in SEC301 was very insightful and filled with wonderful information."
-Donte Leggette, MECU

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.

ATTEND REMOTELY

SIMULCAST

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

More info on page 70

Keith Palmgren *SANS Certified Instructor*

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

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, Authentication Methods, 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 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 (Observe, Orient, 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; Incident Handling; Measuring Progress

giac.org

SECURITY 401

Security Essentials Bootcamp Style

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
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
- STI Master's Program
- DoDD 8570

"Really good foundational stuff so far. I have been working with TCP/IP for many years, but felt like today really clarified my understanding of what happens behind the scenes."
-John Hanes, Apparatus

"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 organization's critical information assets and business systems. This course will show you how to prevent your organization's 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 organization's network depends on the effectiveness of the organization's 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 you'll 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 70

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 company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine 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 services, 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 company's 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 including 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: Unix/Linux Security

While organizations do not have as many Unix/Linux systems, for those that they do have them, these systems are often among the most critical systems that need to be protected. Day 6 provides step-by-step guidance to improve the security of any Linux system by combining practical how-to instructions with background information for Linux beginners, as well as security advice and best practices for administrators with 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 REQUIRED FOR DoD 8570 sans.org/8570

SECURITY 501

Advanced Security Essentials – Enterprise Defender

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

- GIAC Cert: GCED
- STI Master's Program
- DoDD 8570

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

ATTEND REMOTELY

SIMULCAST

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

More info on page 70

"I enjoyed real-life business cases that were discussed in SEC501 to make the material relevant."
-Lorelei Duff, Lockheed Martin

"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

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. **SEC501: Advanced Security Essentials Enterprise Defender** builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

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

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Paul A. Henry *SANS Senior Instructor*

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project (USA), and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, to which 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

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: Pentest

An organization must understand the changing threat landscape and compare that against its own vulnerabilities. On day three students will understand the variety of tests that can be run and how to perform penetration testing in an effective manner. Students will learn about external and internal 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 investigations and find indications of an attack. This information will be fed into the incident response process to ensure that 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

REQUIRED FOR DoD 8570

sans.org/8570

SECURITY 503

Intrusion Detection In-Depth

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Mike Poor

- GIAC Cert: GCIA
- Cyber Guardian
- STI Master's Program
- DoDD 8570

Reports of prominent organizations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Who Should Attend

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

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to configure and master different open-source tools like tcpdump, Wireshark, Snort, Bro, and many more. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material. In addition, most exercises include an "extra credit" stumper question intended to challenge even the most advanced student.

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

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and often vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in **SEC503: Intrusion Detection In-Depth** is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

"SEC503 provides real-world content perspectives, data and tools. The instructor is very knowledgeable and is a great educator."
-George Diolamou, Jacob's Engineering

"SEC503 covers the best processes for intrusion analysis and how to cut out most of the network noise and identify the important traffic. Mike Poor is a rock-star, and I look forward to learning more from him in the future."
-Mike Boya, Warner Bros.

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

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

You Will Be Able To

- Configure and run open-source Snort and write Snort signatures
- Configure and run open-source Bro to provide a hybrid traffic analysis framework
- Understand TCP/IP component layers to identify normal and abnormal traffic
- Use open-source traffic analysis tools to identify signs of an intrusion
- Comprehend the need to employ network forensics to investigate traffic to identify and investigate a possible intrusion
- Use Wireshark to carve out suspicious file attachments
- Write tcpdump filters to selectively examine a particular traffic trait
- Synthesize disparate log files to widen and augment analysis
- Use the open-source network flow tool SiLK to find network behavior anomalies
- Use your knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire

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

REQUIRED FOR DoD 8570

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 70

SECURITY 504

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: John Strand

- GIAC Cert: GCIH
- Cyber Guardian
- STI Master's Program
- DoDD 8570

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), 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. As defenders, it is essential we understand these hacking tools and techniques .

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, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

"SEC504 is awesome! Everything included in this course is very useful in my job as a security professional!"
-Vereleo Bateo, KCG Holdings, Inc.

"John is very good at including real-life examples in all of the lessons."
-Douglas Mitchell, BB&T

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

Who Should Attend

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

The first part of this section looks at the invaluable Incident Handling Step-by-Step model, which was created through a consensus process involving experienced incident handlers from corporations, government agencies, and educational institutes, and has been proven effective in hundreds of organizations. This section is designed to provide students a complete introduction to the incident handling process, using the six steps (preparation, identification, containment, eradication, recovery, and lessons learned) one needs to follow to prepare for and deal with a computer incident. The second part of this section examines from-the-trenches case studies to understand what does and does not work in identifying computer attackers. This section provides valuable information on the steps a systems administrator can take to improve the chances of catching and prosecuting attackers.

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

Seemingly innocuous data leaking from your network could provide the clue needed by an attacker to blow your systems wide open. This day-long course covers the details associated with reconnaissance and scanning, the first two phases of many computer attacks.

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. Attackers employ a variety of strategies to take over systems from the network level up to the application level. This section covers the attacks in depth, from the details of buffer overflow and format string attack techniques to the latest in session hijacking of supposedly secure protocols

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

This course starts out by covering one of the attackers' favorite techniques for compromising systems: worms. We will analyze worm developments over the last two years and project these trends into the future to get a feel for the coming Super Worms we will face. Then the course turns to another vital area often exploited by attackers: web applications. Because most organizations' homegrown web applications do not get the security scrutiny of commercial software, attackers exploit these targets using SQL injection, cross-site scripting, session cloning, and a variety of other mechanisms discussed in detail.

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

This day-long course covers the fourth and fifth steps of many hacker attacks: maintaining access and covering their tracks. Computer attackers install backdoors, apply Rootkits, and sometimes even manipulate the underlying kernel itself to hide their nefarious deeds. Each of these categories of tools requires specialized defenses to protect the underlying system. In this course, we will analyze the most commonly used malicious code specimens, as well as explore future trends in malware, including BIOS-level and combo malware possibilities.

Topics: Maintaining Access; Covering the Tracks; Putting It All Together; Hands-on Exercises with a List of Tools

504.6 HANDS ON: Hacker Tools Workshop

Over the years, the security industry has become smarter and more effective in stopping hackers. Unfortunately, hacker tools are becoming smarter and more complex. One of the most effective methods to stop the enemy is to actually test the environment with the same tools and tactics an attacker might use against you. This workshop lets you put what you have learned over the past week into practice.

Topics: Hands-on Analysis

giac.org

sans.org/cyber-guardian

sans.edu

REQUIRED FOR DoD 8570

sans.org/8570

You Will Be Able To

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

SECURITY 505

Securing Windows with the Critical Security Controls

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Jason Fossen

- GIAC Cert: GCWN
- Cyber Guardian
- STI Master's Program

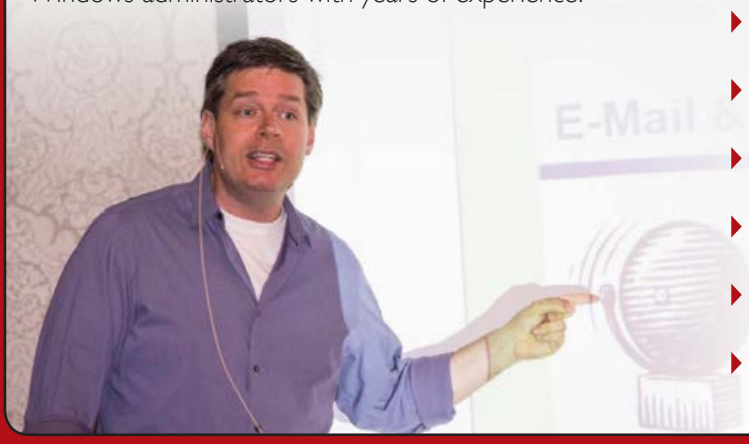
How can we deal with pass-the-hash attacks, token abuse, administrator account compromise, and lateral movement of hackers inside our networks? How do we actually implement the Critical Security Controls on Windows in a large environment? How can we significantly reduce the client-side exploits that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

Understanding how penetration testers and hackers break into networks is not the same as knowing how to design defenses against them, especially when you work in a large and complex Active Directory environment. Knowing about tools like Metasploit, Cain, Netcat, and Poison Ivy is useful, but there is no simple patch against their abuse. The goal of this course is to show you ways to defend against both current Windows attack techniques and the likely types of attacks we can expect in the future. This requires more than just reactive patch management - we need to proactively design security into our systems and networks. That is what SEC505 is about.

Your adversaries want to elevate their privileges to win control over your servers and domain controllers, so a major theme of this course is controlling administrative powers through Group Policy hardening and PowerShell scripting. Learning PowerShell is probably the single best new skill for Windows users, especially with the trend toward cloud computing. Most of your competition in the job market lacks scripting skills, so knowing PowerShell is a great way to make your resume stand out. This course devotes an entire day to PowerShell, but we start with the basics so you do not need any prior scripting experience.

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.



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

"The course content is excellent. The in-class activities were very valuable and the instructor had very good teaching skills and knowledge."
-Jesus Perez, Texas A&M University

"A great way to have an experienced guide take you through the latest and greatest from Microsoft Windows. There were tips and strategies for administrators of all skill levels."
-Eric Hamilton, Agrium

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 can authenticate users in Active Directory to implement share permissions for TCP and UDP ports based on the user's global group memberships. IPSec can also encrypt packet payloads to keep data secure. Imagine configuring the Windows Firewall on your servers and tablets to only permit access to RPC or SMB ports if 1) the client has a local IP address, 2) the client is authenticated by IPSec to be a member of the domain, and 3) the packets are all encrypted with AES. This is not only possible, but is actually relatively easy to deploy with Group Policy. On this course day we will see exactly how to do this.

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 them? 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 now be managed from the command line and scripts. 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 in order 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 511

Continuous Monitoring and Security Operations

NEW

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Eric Conrad

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

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

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

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day (Day 6) features a capture-the-flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the capture-the-flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

With your training journey now complete and your skills enhanced and honed, it is time to go back to work and deliver on the SANS promise that you will be able to apply what you learn in this course the day you return to the office.

Who Should Attend

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

ATTEND REMOTELY

SIMULCAST

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

More info on page 70

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

511.1 HANDS ON: Current State Assessment, SOCs & Security Architecture

We begin with the end in mind by defining the key techniques and principles that will allow us to get there. An effective modern SOC or Security Architecture must enable an organization's ability to rapidly find intrusions to facilitate containment and response. Both significant knowledge and a commitment and continuous monitoring are required to achieve this goal.

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

511.2 HANDS ON: Network Security Architecture

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

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

You Will Be Able To

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

511.3 HANDS ON: Endpoint Security Architecture

One of the hallmarks of modern attacks is an emphasis on client-side exploitation. The days of breaking into networks via direct frontal assaults on unpatched mail, web, or DNS servers are largely behind us. We must focus on mitigating the risk of compromise of clients. Day 3 details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities. These endpoints are increasingly portable devices that frequently stray beyond the traditional perimeter. This day ends with discussion about current modern security architecture and SOC design challenges and offers ways to accommodate rapidly changing business environments. Security architecture and virtualization, cloud services, mobile devices/applications, and web applications will be considered as the course moves from the design elements to the monitoring aspects.

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

511.4 HANDS ON: Network Security Monitoring

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

Topics: Continuous Monitoring Overview; Network Security Monitoring (NSM); Practical NSM Issues; Cornerstone NSM

511.5 HANDS ON: Automation and Continuous Security Monitoring

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

Topics: CSM Overview; Industry Best Practices; Winning CSM Techniques; Maintaining Situational Awareness; Host, Port and Service Discovery; Vulnerability Scanning; Monitoring Patching; Monitoring Applications; Monitoring Service Logs; Monitoring Change to Devices and Appliances; Leveraging Proxy and Firewall Data; Configuring Centralized Windows Event Log Collection; Monitoring Critical Windows Events; Scripting and Automation

511.6 HANDS ON: Capstone: Design, Detect, and Defend

The course culminates in a team-based "Capture-the-Flag" challenge that is a full day of hands-on work applying the principles taught throughout the week.

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

SECURITY 542

Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Seth Misenar

- GIAC Cert: GWAPT
- Cyber Guardian
- STI Master's Program

Web applications play a vital role in every modern organization. This becomes apparent when adversaries compromise these applications, damage business functionality and steal data.

Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. SEC542 helps students move beyond push-button penetration testing to professional web application penetration testing that finds flaws before the adversaries discover and abuse them.

Who Should Attend

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

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so, not surprisingly, every major industry study finds that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but web application penetration testing requires something deeper. SEC542 will enable students to capably assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organizations.

Even technically gifted security geeks often struggle with helping organizations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

Beyond high-quality course content, SEC542 focuses heavily on hands-on exercises to ensure that students can immediately apply all they learn. The world-class team of seasoned security professionals who serve as SEC542 instructors ensures that you will be taught by someone who is both a gifted instructor and a skilled practitioner. In addition to more than 30 formal hands-on labs throughout the course, there is also a Capture the Flag event on the final day during which students work in teams to perform a web application penetration test from start to finish.

"I enjoyed learning more about the depth of HTTP, especially in terms of authentication."
-Daniel Breakiron, DoD

"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

Seth Misenar *SANS Principal Instructor*

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth's background includes network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include, but are not limited to, the following: CISSP, GPEN, GWAPT, GSEC, GCIA, GCIH, GCWN, GCFA, and MCSE. @sethmisenar

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

Understanding the attacker's perspective is key to successful web application penetration testing. The course begins by thoroughly examining web technology, including protocols, languages, clients and server architectures, from the attacker's perspective. We will also examine different authentication systems, including Basic, Digest, Forms and Windows Integrated authentication, and discuss how servers use them and attackers abuse them.

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

542.2 HANDS ON: Reconnaissance and Mapping

The second day starts the actual penetration testing process, beginning with the reconnaissance and mapping phases. Reconnaissance includes gathering publicly available information regarding the target application and organization, identifying the machines that support our target application and building a profile of each server, including the operating system, specific software and configuration. Our discussion will be augmented by practical, hands-on exercises in which we conduct reconnaissance against an in-class target.

Topics: Discovering the Infrastructure Within the Application; Identifying the Machines and Operating Systems; Secure Sockets Layer (SSL) Configurations and Weaknesses; Exploring Virtual Hosting and Its Impact on Testing; Learning Methods to Identify Load Balancers; Software Configuration Discovery; Exploring External Information Sources; Google Hacking; Learning 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: Discovery

This section continues to explore our methodology with the discovery phase. We will build on the information started the previous day, exploring methods to find and verify vulnerabilities within the application. Students will also begin to explore the interactions between the various vulnerabilities.

Topics: Vulnerability Discovery Overview; Creating Custom Scripts for Penetration Testing; Python for Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Interception Proxies; Fiddler; Zed Attack Proxy (ZAP); Burp Suite; Information Leakage, and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection; Blind SQL Injection

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

542.4 HANDS ON: Discovery (CONTINUED)

On day four, students will continue exploring the discovery phase of the methodology. We will cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting and Cross-Site Request Forgery. Manual discovery methods will be employed during hands-on exercises.

Topics: Cross-Site Scripting (XSS); Cross-Site Scripting Discovery; Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; API Attacks; Data Binding Attacks; patproxy; Automated Web Application Scanners; skipfish; w3af

542.5 HANDS ON: Exploitation

On the fifth day we will launch actual exploits against real-world applications, building on the previous three steps, expanding our foothold within the application, and extending it to the network on which it resides. As penetration testers, we will specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

Topics: Exploring Methods to Zombify Browsers; Discussing Using Zombies to Port Scan or Attack Internal Networks; Exploring Attack Frameworks; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; Exploiting the Various Vulnerabilities Discovered; Leveraging Attacks to Gain Access to the System; How to Pivot our Attacks Through a Web Application; Understanding Methods of Interacting with a Server Through SQL Injection; Exploiting Applications to Steal Cookies; Executing Commands Through Web Application Vulnerabilities

542.6 HANDS ON: Capture the Flag

On day six of the course students will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this Capture the Flag event is for students to explore the techniques, tools and methodology they have learned over the last five days. They will be able to use these ideas and methods against a realistic intranet application. At the end of the day, students will provide a verbal report of the findings and methodology they followed to complete the test.

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 560

Network Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Ed Skoudis

- GIAC Cert: GPEN
- Cyber Guardian
- STI Master's Program
- DoDD 8570

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

SEC560 is the must-have course for every well-rounded security professional.

This course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks and wireless and web apps, with over 30 detailed hands-on labs throughout.

Who Should Attend

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

Learn the best ways to test your own systems before the bad guys attack.

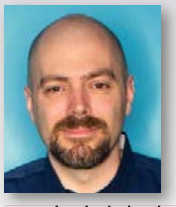
Chock full of practical, real-world tips from some of the world's best penetration testers, SEC560 prepares you to perform detailed reconnaissance by examining a target's infrastructure and mining blogs, search engines, social networking sites and other Internet and intranet infrastructure. You will be equipped to scan target networks using best-of-breed tools. We will not just cover run-of-the-mill options and configurations, we will also go over the less-known but highly useful capabilities of the best pen test toolsets available today. After scanning, you will learn dozens of methods for exploiting target systems to gain access and measure real business risk, then examine post-exploitation, password attacks, wireless and web apps, pivoting through the target environment to model the attacks of real-world bad guys.

"Ed is one of the best instructors I have ever had. It's no secret why he is such a world-class pen tester!"
-Patrick McCoy, KEYW Corporation

"I really enjoyed having real-world stories, not just technical "how-to", but also the logistical items such as cleaning up after the pen test."
-Matt Armstrong, Stroz Friedberg, LLC

You will bring comprehensive penetration testing and ethical hacking know-how back to your organization.

After building your skills in challenging labs over five days, the course culminates with a full-day, real-world network penetration test scenario. You will conduct an end-to-end penetration test, applying the knowledge, tools and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization.



Ed Skoudis *SANS Faculty Fellow*

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

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

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

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

560.2 HANDS ON: In-Depth Scanning

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

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

560.3 HANDS ON: Exploitation and Post-Exploitation

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

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

560.4 HANDS ON: Password Attacks and Merciless Pivoting

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

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

560.5 HANDS ON: Wireless and Web Apps Penetration Testing

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

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

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

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

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

You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 561

Intense Hands-on Pen Testing Skill Development (with SANS NetWars)

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

To be a top penetration testing professional, you need fantastic hands-on skills for finding, exploiting and resolving vulnerabilities. Top instructors at SANS engineered **SEC561: Intense Hands-on Pen Testing Skill Development** from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises, maximizing keyboard time on in-class labs and making this SANS' most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical skills needed to handle today's pen test and vulnerability assessment projects in enterprise environments. Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios using skills that they will be able to apply the day they get back to their jobs.

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

Who Should Attend

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

"SEC561 really forces you to think, and the format rewards your hard work and dedication to finding the solutions."
-Michael Nutbrown, Solers, Inc

"Great challenge – it forces you to use skills you might not otherwise use."
-Brian Thompson, Avista

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

561.1 HANDS ON: Security Platform Analysis

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

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

561.2 HANDS ON: Enterprise Security Assessment

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

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

561.3 HANDS ON: Web Application Assessment

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

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

561.4 HANDS ON: Mobile Device and Application Analysis

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

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

561.5 HANDS ON: Advanced Penetration Testing

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

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

561.6 HANDS ON: Capture the Flag Challenge

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

Topics: VoIP Supporting Infrastructure; VoIP Environment Awareness

You Will Be Able To

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

SECURITY 566

Implementing and Auditing the Critical Security Controls – In-Depth

NEW GIAC CERTIFICATION AVAILABLE – GCCC

SANS

Five-Day Program
Mon, April 13 - Fri, April 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: James Tarala
- GIAC Cert: GCCC
- STI Master's Program

"The 20 controls presented in the course are requirements found in most regulated industries. I found the format and layout of each control well explained and easy to follow."
-Josh Ellis, Iberdrola USA

"SEC566 is a very comprehensive course, and the collections of lists are useful, informative tools that can be moved into the real day-to-day job."
-Henry Jiang

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

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 introduce you to all 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 573

Python for Penetration Testers

SANS

Five-Day Program
Mon, April 13 - Fri, April 17
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Mark Baggett

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

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

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

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

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

Who Should Attend

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

"SEC573 is vital for anyone who considers themselves to be a pen tester."
-Jeff Turner, Lexis Nexis Risk Solutions

"Mark has a very effective and thorough teaching style – great for learning new material."
-Roswitha MacLean, SELF

"SEC573 is a great course. Advanced thinking is required and the challenges are excellent!"
-Kevin Nicholson, Motorola Solutions

You Will Receive

- A virtual machine with sample code and working examples
- A copy of "Violent Python"

573.1 HANDS ON: Essentials Workshop – PART 1

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

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

573.2 HANDS ON: Essentials Workshop – PART 2

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

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

573.3 HANDS ON: Pen Testing Applications – PART 1

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

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

573.4 HANDS ON: Pen Testing Applications – PART 2

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

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

573.5 HANDS ON: Capture the Flag

Working in teams, students apply the skills they have mastered in a series of penetration testing challenges. Participants will exercise the skills and code they have developed over the previous four days as they exploit vulnerable systems, break encryption cyphers, and remotely execute code on target systems. Test your skills! Prove your might!

You Will Be Able To

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

"SEC573 gave me exposure to tools and techniques I wouldn't have normally considered, but now are part of my arsenal."
-Allen Cox, DoD

Mark Baggett *SANS Certified Instructor*

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

SECURITY 575

Mobile Device Security and Ethical Hacking

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Joshua Wright

- GIAC Cert: GMOB
- STI Master's Program

"Excellent overview and a detailed explanations of difficult mobile device technology, OS, and apps."
-Paul Bresnowitz, U.S. Army ARDEC

"Awesome material was presented in SEC575. Day 3 really picked up the pace and the instructor demonstrated interesting techniques."
-Ted Moskalenko, University of Pennsylvania

Mobile phones and tablets have become essential to enterprise and government networks ranging from small organizations to Fortune 500 companies and large agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access, as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning (ERP) to project management.

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

For all of its convenience, however, the ubiquitous use of mobile devices in the work place and beyond has brought new security risks. As reliance on these devices has grown exponentially, organizations have quickly recognized that mobile phones and tablets need greater security implementations than a simple screen protector and clever password. Whether an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, these devices have become hugely attractive and vulnerable targets for nefarious attackers. The use of such devices poses an 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, and 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.

Joshua Wright *SANS Senior Instructor*

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethically disclosing significant product and protocol security weaknesses to well-known organizations. As an open-source software advocate, Josh has conducted cutting-edge research resulting in several software tools that are commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and ZigBee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyber warriors in the U.S. military, government agencies, and critical infrastructure providers. @joshwr1ght

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.

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 effect 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

You Will Be Able To

- Use jailbreak tools for Apple iOS and Android systems
- Conduct an analysis of iOS and Android filesystem data to plunder compromised devices and extract sensitive mobile device use information
- Analyze Apple iOS and Android applications with reverse-engineering tools
- Conduct an automated security assessment of mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks used by mobile devices
- Intercept and manipulate mobile device network activity
- Leverage mobile-device-specific exploit frameworks to gain unauthorized access to target devices
- Manipulate the behavior of mobile applications to bypass security restrictions

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

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 deliver 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) challenge. During 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
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dave Shackleford

"Overall, it's a great course! The exploits and PoC are cutting edge!! This is the future of IT and security knowledge is power!"
-Joe Marshall, Exelon

"Great course! Anyone involved with managing virtual system environments will benefit from taking SEC579."
-Randall Riley,
Defense Security Services

"Dave is an excellent teacher and communicator. He made a highly technical course interesting and the overall experience was thoroughly enjoyable!!"
-Wayne Rosen, Adnet Systems, Inc.

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

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

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

Who Should Attend

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

Dave 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: Auditing and Compliance for 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 617

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Larry Pesce

- GIAC Cert: GAWN
- Cyber Guardian
- STI Master's Program

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

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

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

Who Should Attend

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

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

"SEC617 is an excellent course to prepare you for wireless lecturing space."
Gary Pecht,
Dept. of National Defense

Larry Pesce *SANS Certified Instructor*

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

617.1 HANDS ON: Wireless Data Collection & WiFi MAC Analysis

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

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

617.2 HANDS ON: Wireless Tools and Information Analysis

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

Topics: Wireless LAN Assessment Techniques

617.3 HANDS ON: Client, Crypto, and Enterprise Attacks

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

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

617.4 HANDS ON: Advanced WiFi Attack Techniques

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

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

617.5 HANDS ON: Bluetooth, DECT, and ZigBee Attacks

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

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

617.6 HANDS ON: Wireless Security Strategies and Implementation

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

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

You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 642

Advanced Web App Penetration Testing and Ethical Hacking

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Justin Searle

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications.

Who Should Attend

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

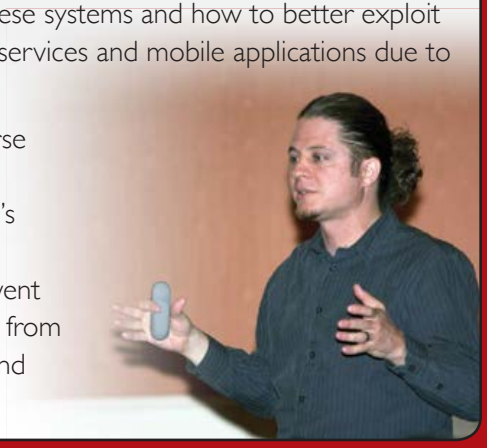
We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real-world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full day Capture the Flag (CtF) event. This CtF will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.



"SEC642 is the perfect course for someone who has a background in web app pen testing, but wants to really gain advanced skills."
-Matthew Sullivan, Webfilings

"Outstanding course!! It is great to have an opportunity to learn the material from someone who is extremely relevant in the field and is able to impart the value of his experiences."
-Bobby Bryant, DoD

Justin Searle *SANS Certified Instructor*

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

642.1 HANDS ON: Advanced Discovery and Exploitation

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle these targets. We will begin the class by exploring how Burp Suite works and more advanced ways to use it within your penetration-testing processes. The exploration of Burp Suite will focus on its ability to work within the traditional web penetration testing methodology and assist in manually discovering the flaws within the target applications.

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

642.2 HANDS ON: Discovery and Exploitation for Specific Applications

We will continue the exploration of advanced discovery and exploitation techniques. We'll start by exploring client-side flaws such as cross-site scripting (XSS) and cross-site request forgery (XSRF). We will explore some of the more advanced methods for discovering these issues. After finding the flaws, you will learn some of the more advanced methods of exploitation, such as scriptless attacks and building web-based worms using XSRF and XSS flaws within an application.

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

You Will Be Able To

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

642.3 HANDS ON: Web Application Encryption

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

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

642.4 HANDS ON: Mobile Applications and Web Services

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

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

642.5 HANDS ON: Web Application Firewall and Filter Bypass

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

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

642.6 HANDS ON: Capture the Flag

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

SECURITY 660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: James Lyne

- GIAC Cert: GXPN
- Cyber Guardian
- STI Master's 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, you need 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 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.

"The SEC660 course was hands-on, packed with content, and current to today's technology!"
-Michael Horken, Rockwell Automation

"James Lyne demostrates a great mastery knowledge and has a great personality."
-Brian Anderson, Northrop Grumman Corporation

James Lyne *SANS Certified Instructor*

James Lyne is the Director of EMEA at SANS and the Director of Technology Strategy at the security firm Sophos. James comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. James spent many years as a hands-on analyst dealing with deep technical issues and is a self-professed "massive geek". Eventually James escaped dark rooms and learned some social skills, and today is a keen presenter at conferences and industry events. With a wide range of experience working in a technical and strategic capacity from incident response to forensics with some of the world's largest organizations, James participates in industry panels, policy groups, and is a frequently-called-upon expert advisor all over the world. James is a frequent guest lecturer and often appears on national TV and other media outlets. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify and develop new talent. @jameslyne

660.1 HANDS ON: Network Attacks for Penetration Testers

Day one serves as an advanced network attack module, building on knowledge gained from SEC560. 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.

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

660.5 HANDS ON: Exploiting Windows for Penetration Testers

On day five we start off with covering the OS security features (ALSR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS. We look at fuzzing skills, which are required to test remote services, such as TFTP and FTP, for faults.

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 learned throughout the course, think outside the box, and solve simple-to-complex problems. In this offensive exercise, challenges range from local privilege escalation to remote exploitation on both Linux and Windows systems, as well as networking attacks and other challenges related to the course material.

You Will Be Able To

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

giac.org

sans.org/cyber-guardian

sans.edu

SECURITY 760

Advanced Exploit Development for Penetration Testers

NEW

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
Laptop Required
46 CPEs
Instructor: Stephen Sims

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

Who Should Attend

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

Not sure if you are ready for SEC760?
Take this 10 question quiz. **sans.org/sec760/quiz**

"SEC760 is the kind of training we couldn't get anywhere else. It's not all theory, we got to implement and to exploit everything we learned."
-Jenny Kitaichit, Intel

"Looking at everything I have learned from Stephen, I definitely feel I have gained an edge when it come to the augmentation of my pentest skills. He made the impossible understandable."
-Alexander Cobblah, Booz Allen Hamilton

You Will Learn:

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

What You Will Receive

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

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 performing reverse-engineering, exploit development, threat modeling, and penetration testing. Stephen has an MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music. @Steph3nSims

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

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

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

760.2 HANDS ON: Advanced Linux Exploitaiton

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

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

You Will Be Able To

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

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

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

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

760.4 HANDS ON: Windows Kernel Debugging and Exploitation

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

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

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

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

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

760.6 HANDS ON: Capture the Flag

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

FORENSICS 408

Windows Forensic Analysis

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Rob Lee
- GIAC Cert: GCFE
- STI Master's 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

"Rob Lee takes Windows forensics to the highest level. It's not just about forensics, it's about forensic methodology."
-Thomas Cook, Army Cyber Institute

"FOR408 is the best course ever! I can't wait to go back to my cases and apply this stuff."
-Rick Kiper, U.S. Dept. of Justice

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.

This course utilizes a brand-new Windows 8.1-based realistic case exercise for which it took over 6 months to create the data. 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 new case workbook will detail step-by-step what each investigator needs to know to examine the latest Windows 8.1.

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

Rob Lee *SANS Faculty Fellow*

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

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 – E-mail Forensics

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

Topics: Evidence of User Communication; How E-mail Works; Determining Sender's Geographic Locations; Examination of E-mail; 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 Challenge

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

Topics: Digital Forensic Case; Mock Trial

You Will Be Able To

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

giac.org sans.edu digital-forensics.sans.org

ATTEND REMOTELY

SIMULCAST

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

More info on page 70

FORENSICS 508

Advanced Digital Forensics and Incident Response

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

- GIAC Cert: GCFA
- Cyber Guardian
- STI Master's Program
- DoDD 8570

DAY 0: A 3-letter government agency contacts you to say critical information was stolen through a targeted attack on your organization. They won't tell how they know, but they identify several breached systems within your enterprise. An Advanced Persistent Threat adversary, aka an APT, is likely involved - the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years.

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

"Excellent course and delivery. I have learned a great deal and look forward to using the skills I've learned in my job."
-Helen Barnard, Royal Navy

"FOR508 is an extremely valuable course overall. It brings essential topics into one class and covers extensive amount of topics along with excellent reference material."
-Edgar Zayas, U.S. Securities and Exchange Commission

Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds. Your team can no longer afford antiquated incident response techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident.

FOR508: Advanced Digital Forensics Analysis and Incident Response will help you determine:

- **How did the breach occur?**
- **What systems were compromised and affected?**
- **What did attackers take? What did they change?**
- **How do we contain and remediate the incident?**

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism. Constantly updated, the incident response course (FOR508) addresses today's incidents by providing hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases.

A hands-on enterprise intrusion lab – developed from a real-world targeted APT attack on an enterprise network and based on how an APT group will target your network – leads you through the challenges and solutions via extensive use of the SANS SIFT Workstation collection of tools.

During the intrusion lab exercises, you will identify where the initial targeted attack occurred and lateral movement through multiple compromised systems. You will extract and create crucial cyber threat intelligence that can help you properly scope the compromise and detect future breaches.

During a targeted attack, an organization needs the best incident response team in the field. FOR508: Advanced Digital Forensics and Incident Response will train you and your team to respond, detect, scope, and stop intrusions and data breaches.

GATHER YOUR INCIDENT RESPONSE TEAM - IT'S TIME TO GO HUNTING

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 U.S. 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 in Incident Response

Timeline analysis will change the way you approach digital forensics and incident response...forever. 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. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response and forensic cases.

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

508.3 HANDS ON: Timeline Analysis

In digital forensics, many tools simply require a few mouse clicks to automatically recover data, and it is very difficult to identify a skilled attacker solely using antiquated and slow commercial toolsets. This section will free you from relying on "push button" forensic techniques by showing you how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to do it by hand and then show how automated tools should be able to recover the same data.

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

In digital forensics, many tools simply require a few mouse clicks to automatically recover data. However, this "push button" mentality has led to many inaccurate results in the past few years. It is also very difficult to identify a skilled attacker solely using antiquated and slow commercial toolsets. This section will free you from relying on "push button" forensic techniques by showing you how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to do it by hand and then 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: Adversary and Malware Hunting

Over the years, we have observed that many incident responders have a challenging time finding malware without pre-built indicators of compromise or threat intelligence gathered prior to a breach. This advanced session will demonstrate techniques used by first responders to identify 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 APT Incident Response Challenge

This incredibly rich and realistic enterprise intrusion exercise is based on a real-world advanced persistent threat (APT) group. 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 attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hactivist groups.

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

giac.org

sans.org/cyber-guardian

sans.edu

REQUIRED FOR DoD 8570


sans.org/8570

digital-forensics.sans.org

FORENSICS 572

Advanced Network Forensics and Analysis

NEW GIAC CERTIFICATION AVAILABLE – GNFA

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Philip Hagen

- GIAC Cert: GNFA
- STI Master's Program

"The instructor was very knowledgeable with relevant and interesting examples to illustrate key points."
-Everett Sherlock, Kapstone Paper

"SEC572 was an excellent course that kept my attention and it will be immediately useful when I get back to work."
-John Ives, UC Berkeley

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

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

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

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

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

Who Should Attend

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

Philip Hagen *SANS Certified Instructor*

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where he engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil became a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is the course lead and co-author of FOR572: Advanced Network Forensics and Analysis. @PhilHagen

572.1 HANDS ON: Off the Disk and Onto the Wire

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

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

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

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

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

572.3 HANDS ON: Network Protocols and Investigations

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

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

572.4 HANDS ON: Logging, OPSEC, and Footprint

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

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

You Will Be Able To

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

572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

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

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

572.6 HANDS ON: Network Forensics Capstone Challenge

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

Topics: Network Forensic Case

giac.org

sans.edu

digital-forensics.sans.org

FORENSICS 585

Advanced Smartphone Forensics

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Cindy Murphy

"FOR585 provides a comprehensive overview of advanced smartphone forensics for iOS, Android, Blackberry, Windows mobile, and other smart devices."
-Dave White, District Attorneys Office

"It was an incredibly valuable week of training. I would recommend this course to anyone looking to expand their mobile forensic skills."
-Manny Ortiz, AT&T

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

The course focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation and security breach cases.

The hands-on exercises in this course cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data that tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones.

This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensics professionals. It is time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

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

Who Should Attend

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

Cindy Murphy *SANS Certified Instructor*

Detective Cindy Murphy works for the City of Madison, WI Police Department and has been a law enforcement officer since 1985. She is a certified forensic examiner (EnCE, CCFT, DFCP), and has been involved in computer forensics since 1999. She earned her MSc in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part-time digital forensics instructor at Madison College, and a part-time mobile device forensics instructor for the SANS Institute. @cindymurph

585.1 HANDS ON: Smartphone Overview and Malware Forensics

Although smartphone forensics concepts are similar to those of digital forensics, smartphone file system structures require specialized decoding skills to correctly interpret the data acquired from the device. On the first course day students will apply what they already know to smartphone forensics handling, device capabilities, acquisition methods and data encoding concepts of smartphone components. Students will also become familiar with the forensics tools required to complete comprehensive examinations of smartphone data structures. Malware affects a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones and how to identify it.

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

585.2 HANDS ON: Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on them, you will be unprepared for the rapidly evolving world of smartphone forensics.

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

585.3 HANDS ON: iOS Forensics

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

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

585.4 HANDS ON: Backup File and BlackBerry Forensics

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

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

You Will Be Able To

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

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

Given the prevalence of other types of smartphones around the world, it is critical for examiners to develop a foundation of understanding about data storage on multiple devices. Nokia smartphones running the Symbian operating system may no longer be manufactured, but they still exist in the wild. You must acquire skills for handling and parsing data from uncommon smartphone devices. This day of instruction will prepare you to deal with "misfit" smartphone devices and provide you with advanced methods for decoding data stored in third-party applications across all smartphones.

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

585.6 HANDS ON: Smartphone Forensics Capstone Exercise

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

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Lenny Zeltser

- GIAC Cert: GREM
- STI Master's Program

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.

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 are 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

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 provide additional opportunities to learn 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.

Lenny Zeltser *SANS Senior Instructor*

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

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

digital-forensics.sans.org

MANAGEMENT 414

SANS Training Program for CISSP Certification®

Six-Day Program
Mon, April 13 - Sat, April 18
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: Jonathan Ham
- GIAC Cert: GISP
- DoDD 8570

"I think the course material and the instructor are very relevant for the task of getting a CISSP. The overall academic exercise is solid."
-Aaron Lewter, Availity

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experimental knowledge in examples and explanations."
Sean Hoar,
Davis Wright Tremaine

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: Operations Security
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.

***NOTICE:** Over the past 4 years, 98% of all surveyed students who took SANS MGT414 and then took the exam passed, compared to a national average of around 70% for other prep courses.*

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

Jonathan Ham *SANS Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues from policy and procedure to staffing and training, scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.

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

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

414.4 Cryptography and Security Architecture and Design

Cryptography plays a critical role in the protection of information. Examples showing the correct and incorrect ways to deploy cryptography, and common mistakes made, will be presented. The three types of crypto systems are examined to show how they work together to accomplish the goals of crypto. Understanding the components of the computer, 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 focus 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

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

giac.org

REQUIRED FOR DoD 8570

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
Mon, April 13 - Fri, April 17
9:00am - 6:00pm (Days 1-4)
9:00am - 4:00pm (Day 5)
33 CPEs
Laptop NOT Needed
Instructor: David Hoelzer

- GIAC Cert: GSLC
- STI Master's 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.

"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

"MGT512 has great info for newly assigned managers to cybersecurity."
Kerry Taylor,
U.S. Army Corps of Engineer

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!

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 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow for the Center for Cybermedia Research and for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for 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. He 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

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

This course section examines 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

REQUIRED FOR DoD 8570

sans.org/8570

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/event/sans-2015/courses

MANAGEMENT 514

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
Mon, April 13 - Fri, April 17
9:00am - 5:00pm
30 CPEs
Laptop Recommended
Instructor: G. Mark Hardy
- STI Master's Program

"The instructor is very knowledgeable and his stories are credible to the curriculum. Having the ability to benefit from his experience has been an added bonus."
-Pamela Livingston-Spruill, NNSA

"As I progress in my career within cybersecurity I find that courses such as MGT514 will allow me to plan and lead my organization forward."
-Eric Burgan, Idaho National Labs

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

Who Should Attend

- Existing, recently appointed, and aspiring IT and IT security managers and supervisors who desire to enhance their leadership and governance skills to develop their staff into a more productive and cohesive team.

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

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

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

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

Leadership tends to be a bit "squishy" and courses covering the topic are often based upon the opinions of people who were successful in the marketplace. However, success can be as much a factor of luck as skill, so we base this part of the course on five decades of the research of social scientists and their experiments going as far back as Maslow and on research as current as Sunstein and Thaler. We discuss leadership skills that apply to commercial business, non-profit, for-profit, or other organizations. This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization's climate and team-building skills to support the organization's mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

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. He 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.

514.1 An Approach to Strategic Planning

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

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

514.2 Planning to Ensure Institutional Effectiveness

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

514.3 Security Policy Development

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

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

You Will Be Able To

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

514.4 Comprehensive Security Policy Assessment

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

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

514.5 Leadership and Management Competencies

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

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

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

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

sans.edu

MANAGEMENT 525

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

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop NOT Needed
Instructor: Jeff Frisk

- GIAC Cert: GCPM
- STI Master's Program

Who Should Attend

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

"I am in a role where I need to manage and contribute to a number of projects. The things I learned in MGT525 will have exponential benefits."
-Sandy Dunn, Hewlett Packard

"MGT525 is solid project-management training with real-world examples taught by an instructor with significant project-management and technical knowledge."
-Rich Graves, Carleton College

Recently updated to fully prepare you for the 2015 PMP® Exam. **SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep** is a PMI Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP®) and other professional credentials. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide* (Fifth Edition) and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management – from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide* (Fifth Edition) is provided to all participants. You can reference the guide and use your course material along with the knowledge you gain in class to prepare for the 2014 updated PMP® Exam and the GIAC Certified Project Manager Exam.

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

Jeff Frisk *SANS Certified Instructor*

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

525.1 Project Management Structure and Framework

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

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

525.2 Project Charter and Scope Management

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

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

525.3 Time and Cost Management

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

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

525.4 Communications and Human Resources

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

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

You Will Be Able To

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

525.5 Quality and Risk Management

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

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

525.6 Procurement, Stakeholder Management, and Project Integration

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

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

giac.org

sans.edu

AUDIT 507

Auditing & Monitoring Networks, Perimeters, and Systems

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tanya Baccam

- GIAC Cert: GSNA
- STI Master's Program
- DoDD 8570

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

This course is 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

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

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.

Tanya Baccam *SANS Senior Instructor*

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

507.1 Effective Auditing, Risk Assessment, and Reporting

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 giving you the knowledge to be able to recommend additional compensating controls to address the risk. Nearly a third of the day is spent covering important audit considerations and questions dealing with virtualization and 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 Effective Network and Perimeter Auditing/Monitoring

The focus in this section is 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 attain, thus allowing for the implementation of controls that can be audited. Overall, this course will teach the student everything needed to audit routers, switches, and firewalls in the real world.

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

507.3 Web Application Auditing

Web applications have consistently been rated as 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: Identifying Controls Against Information Gathering Attacks; Processing 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, constituting a standard against which one can conduct audits
- Perform a network and perimeter audit using a seven-step process
- Audit firewalls to validate that rules/settings are working as designed, blocking traffic as required
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources.
- Audit web applications configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system to baseline and automatically audit Active Directory and all systems in a Windows domain

507.4 Advanced Windows Auditing and Monitoring

Microsoft's business class system makes 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 Advanced Unix Auditing and Monitoring

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

REQUIRED FOR DoD 8570


sans.org/8570

DEVELOPER 522

Defending Web Applications Security Essentials

SANS

Six-Day Program
Mon, April 13 - Sat, April 18
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dr. Johannes Ullrich
- GIAC Cert: GWEB
- STI Master's Program

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

"I have taken multiple SANS courses and the virtual image for this course seemed most polished and everything just worked. Good course test apps as well."
Feliz Simmons, AIG

giac.org sans.edu

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

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

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

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

Who Should Attend

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

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

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

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

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

Dr. Johannes Ullrich *SANS Senior Instructor*

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

DEVELOPER 544

Secure Coding in .NET: Developing Defensible Applications

SANS

Four-Day Program
Mon, April 13 - Thu, April 16
9:00am - 5:00pm
24 CPEs
Laptop Required
Instructor: Eric Johnson

- GIAC Cert: GSSP-.NET
- STI Master's Program

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

Have you ever wondered if the built-in ASP.NET validation is effective? Have you been concerned that Windows Communication Foundation (WCF) services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework?

DEV544: Secure Coding in .NET: Developing Defensible Applications will help students leverage built-in and custom defensive technologies to integrate security into their applications. This comprehensive course covers a huge set of skills and knowledge. It is not a high-level theory course. It is about real programming. Students examine actual code, work with real tools, build applications, and gain confidence in the resources they need to improve the security of .NET applications.

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

The class culminates with a security review of a real-world open-source application. Students will conduct a code review, review a penetration test report, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that they have learned in class, implement fixes for these issues.

PCI Compliance

Section 6.5 of the Payment Card Industry (PCI) Data Security Standard (DSS) instructs auditors to verify processes that require training in secure coding techniques for developers. This is the course for you if your application processes cardholder data and you are required to meet PCI compliance.

Who Should Attend

- ASP.NET developers who want to build more secure web applications
- .NET framework developers
- Software engineers
- Software architects
- Developers who need to be trained in secure coding techniques to meet PCI compliance
- Application security auditors
- Technical project managers
- Senior software QA specialists
- Penetration testers

"DEV544 has useful information on static and dynamic analysis as well as code reviews."
-Daryl Webb, HSMV

"DEV544 has material that can be applied in my job as a developer."
Erick Cacers, VyStar CU

"This course will help us write better code!"
-David Morgan, Satcom Direct

giac.org sans.edu

Eric Johnson *SANS Instructor*

Eric Johnson is a security consultant at Cypress Data Defense and an instructor and contributing author for the SANS DEV544 Secure Coding in.NET course. He previously spent six years performing web application security assessments for a large financial institution and another four years focusing on ASP .NET web development. Other experience includes developing security tools, secure code review, vulnerability assessment, penetration testing, risk assessment, static source code analysis, and security research. Eric completed a bachelor of science in computer engineering and a master of science in information assurance at Iowa State University. Eric currently holds the GSSP-.NET, GWAPT, and CISSP certifications and is located in West Des Moines, IA. Outside the office, Eric enjoys spending time with his wife and daughter, attending Iowa State athletic events, and golfing on the weekends. @emjohn20

LEGAL 523

Law of Data Security and Investigations

SANS

Five-Day Program
Mon, April 13 - Fri, April 17
9:00am - 5:00pm
30 CPE/CMU Credits
Laptop NOT Needed
Instructor: Benjamin Wright
- GIAC Cert: GLEG
- STI Master's Program

"Coming from an intense IT operations background, it was extremely valuable to receive an understanding of my security role from a legal point of view."
-John Ochman, BD

"LEG523 was an excellent use of time. Benjamin Wright knows material very well. He has excellent flow and is right on target with course description."
-Sharon O'Bryan, DeVry Inc

"LEG523 provides a great foundation and introduction into the legal issues involving cybersecurity."
-Tracey Kinslow,
TN Air National Guard

- **New for live delivery as of October 2014: Home Depot's legal and public statements about payment card breach.**
- **New legal tips on confiscating and interrogating mobile devices.**
- **New for live delivery as of April 2014: Course covers lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.**
- **New for live delivery as of January 2014: The public response by retailer Target to a major payment card security incident.**

Who Should Attend

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

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

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

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security. We will cover breaking stories ranging from Home Depot's legal and public statements about payment card breach to the lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

Benjamin Wright *SANS Senior Instructor*

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

523.1 Fundamentals of IT Security Law and Policy

Course day number 1 is an introduction to Law and IT, serving as the foundation for the discussion in later course days. Students survey the general legal issues that must be addressed in establishing best InfoSec practices. This course day canvasses the many new laws on data security, and evaluates InfoSec as a field of growing legal liability. It covers computer crime and intellectual property laws when a network is compromised, as well as emerging topics like honeypots, and active defenses, i.e., enterprises hacking back against hackers. It also considers the impact of future technologies on law and investigations. A key goal is to help professionals factor in legal concerns when they draft enterprise IT security policies.

Day 1 includes a lab on the drafting of IT security policies from a legal perspective. Students will debate what the words of an enterprise policy would mean in a courtroom. It also includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI).

523.2 E-Records, E-Discovery and Business Law

IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in this course day number 2. It emphasizes the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), how to manage implementation of a "legal hold" over some records to prevent their destruction and how to coordinate with legal counsel to develop workable strategies to legal challenges.

Day 2 is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

523.3 Contracting for Data Security & Other Technology

Course day number 3 is focused on the essentials of contract law sensitive to the current legislative requirements for security. Compliance with many of the new data security laws requires contracts. Because IT pulls together the products and services of many vendors, consultants and outsourcers, enterprises need appropriate contracts to comply with Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, EU Data Directive, California Senate Bill 1386 and others.

When appropriate, course day 3 leaves the student with practical steps and tools to be applied in his or her enterprise. It includes a lab at the end of the day to help students learn about writing contract-related documents relevant to their professional responsibility. Students will learn the language of common IT contract clauses. They will learn the meaning of and issues surrounding those clauses and become familiar with specific legal cases to show how different disputes have resolved in litigation.

523.4 The Law of IT Compliance: How to Conduct Investigations

InfoSec professionals and cyber investigators operate in a world of ambiguity, rapid change and legal uncertainty. To address these challenges, course day number 4 presents methods for analyzing a situation and then acting in a way that is ethical and defensible and that reduces risk.

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

Day 4 surveys white collar fraud, with an emphasis on the role of technology in the commission and prevention of that fraud. It teaches IT managers practical, case-study-driven, lessons about the monitoring of employees and employee privacy.

523.5 Applying Law to Emerging Dangers: Cyber Defense

Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. Day 5 is organized around extended case studies in security law – break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage, and defamation. The studies lay out the chronology of events and critiques what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills for addressing incidents in your day-to-day work.
In addition to case studies, the core material will include tutorials on relevant legislation and judicial decisions in such areas as privacy, negligence, contracts, e-investigations and computer crime.

giac.org

sans.edu

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

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

Five-Day Program | Mon, April 13 - Fri, April 17 | 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.

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

HOSTED Offensive Countermeasures: The Art of Active Defenses

Two-Day Course | Sat, April 11 - Sun, April 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Mick Douglas

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

In this class you will learn how to force attackers to take more moves to attack your network – moves that can increase your ability to detect them. You will learn how to gain more knowledge about 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.

The current threat landscape is shifting. Traditional defenses are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. Some of the things we talk about you may implement immediately, others may take you a while to implement. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, determine who is attacking you and, finally, attack the attackers.

This class is based on the DARPA funded Active Defense Harbinger Distribution live Linux environment. This VM is built from the ground up for defenders to quickly implement Active Defenses in their environments. This class is also very heavy with hands-on labs. We won't just talk about Active Defenses. We will be doing hands-on labs in a way that will enable you to quickly and easily implement what you learn in your working environment.

HOSTED Physical Penetration Testing – Introduction

Two-Day Course | Sat, April 11 - Sun, April 12 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: The CORE Group

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

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

HOSTED Health Care Security Essentials

NEW

Two-Day Course | Sat, April 11 - Sun, April 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Greg Porter

Health Care Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in health care information security and regulatory compliance. The class provides a foundational set of skills and knowledge for health care security professionals by integrating case studies, hands-on labs, and tips for securing and monitoring electronic Protected Health Information ("ePHI"). Administrative insights for those managing the many aspects of health care security operations will also be discussed. The goal of the course is to present a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on the U.S. health care system.

SECURITY 440

Critical Security Controls: Planning, Implementing and Auditing

Two-Day Course | Sat, April 11 - Sun, April 12 | 9:00am - 5:00pm | 12 CPEs | Laptop NOT Needed | Instructor: Randy Marchany

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

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

SECURITY 524

Cloud Security Fundamentals

Two-Day Course | Sat, April 11 - Sun, April 12 | 9:00am - 5:00pm | 12 CPEs | Laptop Required | Instructor: Dave Shackleford

SEC524 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 represent 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 an in-depth discussion of the risks involved. The course will go in-depth on architecture and infrastructure fundamentals for private, public and hybrid clouds, including a wide range of topics such as patch and configuration management, virtualization security, application security and change management. Policy, risk assessment and governance within cloud environments will also be covered, with recommendations for both internal policies and contract provisions. 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.

The second day will start with coverage of audits and assessments for cloud environments. The session will include hands-on exercises for students to learn about new models and approaches for performing assessments, as well as for evaluating audit and monitoring controls. Next, the class will turn to protecting the actual data. New approaches for data encryption, network encryption, key management and data lifecycle concerns will be covered in detail, as will be the challenges of identifying and accessing management in cloud environments. 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 also be covered, along with how best to manage these critical security processes and the technologies that support them given that most controls are managed by the CSP.

SECURITY 580

Metasploit Kung Fu for Enterprise Pen Testing

Two-Day Course | Sat, April 11 - Sun, April 12 | 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.

MANAGEMENT 305

Technical Communication and Presentation Skills for Security Professionals

One-Day Course | Sun, April 12 | 9:00am - 5:00pm | 6 CPEs | Laptop Required | Instructor: David Hoelzer

sans.edu

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

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

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

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

Who Should Attend

- All SANS Master's Degree students
- Auditors
- Security Architects
- Managers
- Incident Handlers
- Forensic Examiners
- Individuals seeking to improve their technical writing, presentation and reporting skills
- Individuals who write reports or make presentations to management
- Awareness trainers, local mentors
- Management should strongly consider sending individuals who must write and present reports and project plans to this course.

MANAGEMENT 415

A Practical Introduction to Risk Assessment

One-Day Course | Sun, April 12 | 9:00am - 5:00pm | 6 CPEs | Laptop Required | Instructor: G. Mark Hardy

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.

Who Should Attend

- Security engineers, compliance directors, managers, auditors
- Auditors
- Directors of security compliance
- Information assurance management
- System administrators

MANAGEMENT 433

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

Two-Day Course | Sat, April 11 - Sun, April 12 | 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 its 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 the 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 70

MANAGEMENT 535

Incident Response Team Management

One-Day Course | Sun, April 12 | 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

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: Understanding the Offense to Build a Better Defense *Dr. Eric Cole*

Many organizations do not perform proper threat modeling and understand what the adversary is capable of. The only way to be good at the defense is to understand the offense. Understanding how the threat targets and attacks a system can provide insight in to implementing a proper security program. In this talk, the attacker killer chain will be examined as will specific steps organizations can take to properly defend themselves.

Using an Open-Source Threat Model for Prioritized Defense *James Tarala*

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors. So why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization's defenses - without all the confusion. James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk it faces. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements facing organizations today. Whether you are in the Department of Defense or work for a small mom and pop retailer, you will be able to use this model to specifically devise a prioritized defense for your organization.

Preparing for PowerShellmageddon – Investigating Windows Command Line Activity *Chad Tilbury*

There is a reason hackers use the command line, and it isn't to impress you with their prowess. Throughout the history of Windows, the command line has left far fewer forensic artifacts than equivalent operations via the GUI. To make matters worse, the transition to Windows 7 and 8 has spread PowerShell throughout the enterprise. While it makes our lives easier as defenders, it does the same for our adversaries. Every time you marvel at the capabilities of PowerShell, you should fear how your adversaries may use that power against you. This talk will demonstrate how incident responders are countering the command line threat with real-world examples. Learn to identify when it is in play, extract command history, and see what is new on the horizon from Microsoft to make tracking command line and PowerShell activity easier.

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

iOS Game Hacking: How I Ruled the Worl^Hd and Built Skills For AWESOME Mobile App Pen Tests *Josh Wright*

I am a terrible video game player. I lack the skills to competitively arrange words with colleagues, crush jelly beans, or achieve a high score arranging numbers by threes. However, what I lack in video game competition, I make up for in iOS app hacking. In this talk, we'll explore the profitable market of iOS games, looking at several techniques that are used to cheat, hack, or even steal from iOS game developers. You'll be able to apply these techniques to give yourself a leg up on your next gaming experience. Most importantly, each and every technique we'll discuss is also directly applicable to penetration testing and assessing the security of the iOS apps your organization uses each and every day. Learn to pwn games while becoming a better app pen tester! What's not to like?

Enterprise PowerShell for Remote Security Assessment *James Tarala*

As organizations assess the security of their information systems, the need for automation has become more and more apparent. Not only are organizations attempting to automate their assessments, the need is becoming more pressing to perform assessments centrally against large numbers of enterprise systems. Forensic analysts, incident handlers, penetration testers, and auditors all regularly find themselves in situations where they need to remotely assess a large number of systems through an automated set of tools. Microsoft's PowerShell scripting language has become the de facto standard for many organizations looking to perform this level of distributed automation. In this presentation James Tarala of Enclave Security will describe to students the enterprise capabilities PowerShell offers and show practical examples of how PowerShell can be used to perform large-scale Windows security assessments.

Debunking the Complex Password Myth *Keith Palmgren*

Perhaps the worst advice you can give a user is "choose a complex password". The result is the impossible-to-remember password requiring the infamous sticky note on the monitor. In addition, that password gets used at a dozen sites at home, AND the very same password gets used at work. The final result ends up being the devastating password compromise. In this one-hour talk, we will look at the technical and non-technical (human nature) issues behind passwords. Attendees will gain a more complete understanding of passwords and receive solid advice on creating more easily remembered AND significantly stronger passwords at work and at home, for their users, for themselves and even for their children.

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

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

BONUS SESSIONS

Securing The Kids *Lance Spitzner*

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

Gone In 60 Minutes

60 minutes from discovery through exploitation – how fast is your patching process?

David Hoelzer

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

The 13 Absolute Truths of Security

Keith Palmgren

Keith Palmgren has identified thirteen "Absolute Truths" of security - things that remain true regardless of circumstance, network topology, organizational type, or any other variable. Recognizing these thirteen absolute truths and how they affect a security program can lead to the success of that program. Failing to recognize these truths will spell almost certain doom. Here we will take a non-technical look at each of the thirteen absolute truths in turn, examine what they mean to the security manager, what they mean to the security posture, and how understanding them will lead to a successful security program.

Find complete details at

sans.org/event/sans-2015/bonus-sessions

Malware Analysis for Incident Responders: Getting Started *Lenny Zeltser*

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. A good way to get started with such efforts involves examining how malicious software behaves in a controlled laboratory environment. In this two-hour seminar briefing, Lenny Zeltser demonstrates key aspects of this process, walking you through behavioral analysis of a malware specimen by using several free tools and even peeking into the world of code analysis. You will see practical techniques in action and understand how malware analysis will help you to triage the incident to assess key capabilities of the malicious software. You will also learn how to determine ways of identifying this malware on systems in your environment by establishing indicators of compromise (IOCs). This seminar will help you start learning how to turn malware inside out.

Self-Education: Using the Pull Method for Security Awareness Training *Lance Spitzner*

Traditionally security awareness training has used a push method, from pushing out CBT training to mandatory workshops. Organizations are now trying a different approach, the pull method. This is when employees are encouraged to actively seek out training on their own. Learn how organizations are effectively building and promoting pull training and the successes they are seeing.

GIAC Program Overview *Jeff Frisk*

GIAC is the leading provider and developer of Information Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military, and industry to protect the cyber environment.

SANS Technology Institute Open House

Bill Lockhart

SANS Technology Institute Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers: management skills and technical mastery.

Vendor Expo

Wednesday, April 15

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

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

Vendor-Sponsored Lunch Sessions

Wednesday, April 15 | 12:00pm - 1:30pm

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

Vendor-Sponsored Lunch & Learn Presentations

Throughout SANS 2015, vendors will provide sponsored lunch presentations where attendees can interact with peers and receive education on vendor solutions. Take a break and get up-to-date on security technologies!

Vendor Welcome Reception

Wednesday, April 15 | 5:00pm - 7:30pm

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 real time and includes four months of online access.

Can't travel to SANS 2015?

The following courses will be Simulcast live from the event:

SEC301 | SEC401 | SEC501 | SEC503 | SEC511 | FOR408 | 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

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, and IT security law.

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

-Christina Ford, Department of Commerce

Get Certified at **giac.org**

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

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

Master's Degree Programs:

- M.S. in Information Security Engineering
- M.S. in Information Security Management

Specialized Graduate Certificates:

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

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

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

Fund Your SANS Training: How to Persuade Your Employer

EXPLORE

- Read this brochure and note the courses that will enhance your role at your organization.
- Use the *Career Roadmap* (sans.org/media/security-training/roadmap.pdf) to arm yourself with all the necessary materials to make a good case for attending a SANS training event.

RELATE

- Show how recent problems or issues will be solved with the knowledge you gain from the SANS course.
- Describe how your knowledge will allow you to become an expert resource for the rest of your team.

VALIDATE

- Earn a GIAC certification, proving to your employer that you gained the expertise they paid for!
- Hone your skills at NetWars and report your competitive score (available free with 5- or 6-day courses at live training events).

SAVE

- The earlier you sign up and pay, the more you save, so explain the benefit of paying up early.
- Save even more with group discounts, or bundled course packages! See inside for details.

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.

ALTERNATIVES

- If time out of the office is limited, pitch *SANS OnDemand*, *Event Simulcast*, or *Live Online Training*.
- Highlight that students in our online courses earn the same GIAC scores as those who take training live!

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!"

The CORE NetWars and DFIR NetWars Tournaments will be held simultaneously at SANS 2015!

NETWARS

CORE NETWARS TOURNAMENT

SANS CORE NetWars Tournament is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars OnSites to help identify skilled personnel and as part of extensive hands-on training. With CORE NetWars Tournament, you'll build a wide variety of skills while having a great time.

Who Should Attend

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff

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

DFIR NETWARS TOURNAMENT

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges covering host forensics, network forensics, and malware and memory analysis. It is developed by incident responders and analysts who use these skills daily to stop data breaches and solve crimes. Sharpen your team's skills prior to being involved in a real incident.

Who Should Attend

- Digital forensic analysts
- Forensic examiners
- Reverse-engineering and malware analysts
- Incident responders
- Law enforcement officers, federal agents, and detectives
- Security Operations Center analysts
- Cyber crime investigators
- Media exploitation analysts

Challenge Yourself Before the Enemy Does – DFIR NetWars

Both NetWars competitions will be played over two evenings: April 16-17, 2015

Prizes will be awarded at the conclusion of the tournaments.

REGISTRATION IS FREE BUT LIMITED

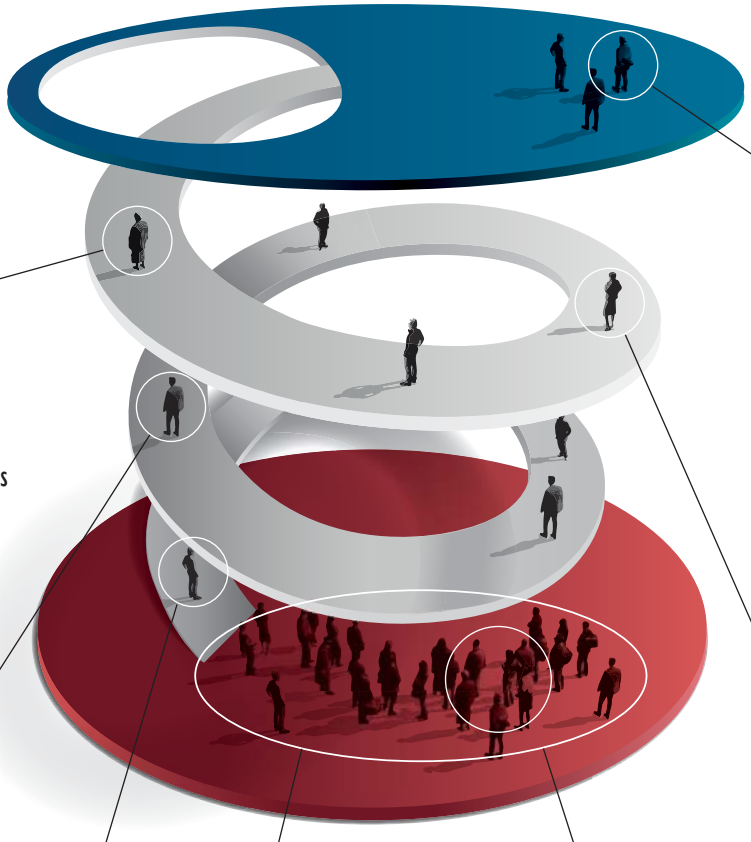
for students attending any long course at SANS 2015 *(NON-STUDENT'S ENTRANCE FEE IS $1,249).*

Register at sans.org/event/sans-2015/courses

EDUCATING THE WORLD IN CYBERSECURITY

Protecting data has never been more important. As attackers become more sophisticated and determined, preventing a breach requires information security professionals to own a honed skillset with real-world knowledge and capabilities. SANS is a one-stop education provider for information security, including security awareness program, hands-on training, GIAC certification and graduate programs. SANS world-class instructors and proven curricula will empower you with the ability to protect and defend your vital systems and data.

The SANS family of products includes:



Cyber Guardian

Designed for the elite teams of technical security professionals whose role includes securing systems, reconnaissance, counterterrorism and counter hacks

sans.org/cyber-guardian

SANS NetWars

Testing hands-on technical skills in a safe environment so security professionals are prepared when a real incident occurs

sans.org/netwars

SANS Training

Hands-on security training for professionals just starting in security up to seasoned professionals

Training courses are delivered at live events and online

sans.org

SANS Security Awareness

Everything your organization needs for an effective security awareness program

securingthehuman.org

SANS Technology Institute

A regionally accredited postgraduate institution focused solely on information security education for working professionals

sans.edu

GIAC Certification

Validate the technical skills and knowledge of your security professionals

giac.org

SANS CyberTalent

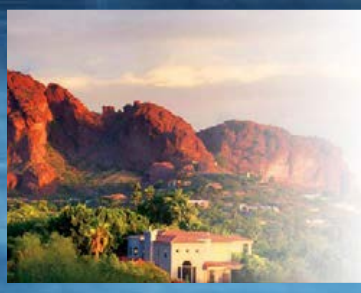
Assess the skills and aptitude of security professionals so you can feel confident in your hiring decisions

sans.org/cybertalent

Learn more at **www.sans.org**

FUTURE SANS TRAINING EVENTS

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



SANS
Scottsdale
Scottsdale, AZ
Feb 16-21, 2015

SANS 2015
Orlando, FL
Apr 11-18, 2015

10TH ANNUAL
ICS Security
SUMMIT & TRAINING
Orlando, FL
Feb 23 - Mar 2, 2015

SANS
Security West
San Diego, CA
May 4-12 2015

DFIR MONTEREY 2015
a REDFIRE Event
Monterey, CA Feb 23-28, 2015

SANS
Pen Test Austin
Austin, TX
May 18-23, 2015

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

SANSFIRE
Baltimore, MD
Jun 11-22, 2015

SANS
Northern Virginia
Reston, VA
Mar 9-14, 2015

SANS
Rocky Mountain
Denver, CO
Jun 22-27, 2015

SANS
Houston
Houston, TX
March 23-28, 2015

SANS
Capital City
Washington, DC
Jul 6-11

SANS Security Operations Training

SANS CYBER DEFENSE

SOC Diagram:
Specific task assigned to a SOC

SOC Background Description

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

SOC Education + Training

SANS + Formal Training = Qualified SOC Personnel Capable of:

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

SANS offers SOC Training in the following areas:

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

Check out the SOC Career Paths to the right:

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

SANS will put you on a
Path To Success!

SANS Security Operations Training is flexible and offers:

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

Security Operations Center (SOC) Career Roadmap

Security Analyst

SEC401 Security Essentials Bootcamp Style — **GSEC**

↓

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

↓

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

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

SAMPLE JOB TITLES

- Security Engineers
- Security Analysts
- Data Center Operators
- Help Desk/Technicians

Security Engineer

SEC401 Security Essentials Bootcamp Style — **GSEC**

↓

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

↓

SEC502 Perimeter Protection In-Depth — **GCFW**

SEC503 Intrusion Detection In-Depth — **GCIA**

SAMPLE JOB TITLES

- Security Analysts
- Security Auditors
- Security Architects
- Security Engineers

Intrusion Analyst

SEC401 Security Essentials Bootcamp Style — **GSEC**

↓

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

↓

SEC503 Intrusion Detection In-Depth — **GCIA**

SEC504 Hacker Tools, Techniques, Exploits & Incident Handling — **GCIH**

↓

FOR508 Advanced Digital Forensics and Incident Response — **GCFA**

SAMPLE JOB TITLES

- Chief Information Officers
- Security Managers
- Chief Information Security Officers
- Business Unit Managers
- Director/Security Consultants

Security Operations Center (SOC) Analyst

The core courses in the Career Roadmap focus on building, running, and deploying a SOC. Security has become critical for the success of an organization constantly under attack. Defense against the vast array of attacks requires continuous monitoring of the network and assessment of the security infrastructure. Properly trained people who can detect and respond to attacks are critical to the overall success and security of an organization.

SAMPLE JOB TITLES

- Security Consultants
- SOC Managers
- Security Operations Supervisors
- Security Operations Directors

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

↓

New! **SEC511** Continuous Monitoring and Security Operations

↓

SEC503 Intrusion Detection In-Depth — **GCIA**

↓

FOR572 Advanced Network Forensics and Analysis — **GNFA**

SANS 2015

Hotel Information

Training Campus

Walt Disney World Swan & Dolphin

1500 Epcot Resorts Blvd.
Lake Buena Vista, FL 32830

www.sans.org/event/sans-2015/location

Special Hotel Rates Available

A special discounted rate of $218.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through March 23, 2015.

The award-winning Walt Disney World Swan and Dolphin Resort is a deluxe hotel and your gateway to Central Florida's illustrious theme parks and attractions.

The resort is located in between Epcot® and Disney's Hollywood Studios™ and close to Disney's Animal Kingdom® Theme Park and Magic Kingdom® Park. Discover our magical surroundings, superior service, luxurious facilities and redesigned guest rooms featuring the Heavenly Bed®. Enjoy the new Mandara Spa, 17 spectacular restaurants and lounges, five pools, a white sand beach, two health clubs, tennis, nearby golf and many special Disney benefits.

Staying on-site at our resort allows you to enjoy many special Disney benefits including:

- Disney Fastpass+ Benefit
- Extra Magic Hours Benefit at the Theme Parks
- Complimentary Scheduled Transportation Throughout Walt Disney World® Resort
- On-Site Disney Ticket Desks
- Character Dining
- Advance Tee Times on Championship Walt Disney World® Golf Courses
- Complimentary Delivery of Purchases Made in Walt Disney World® Theme Parks
- Complimentary Parking at Walt Disney World® Theme Parks

Designed by award-winning architect Michael Graves, the duo of hotels share similar design elements but each has its own distinct appearance. The two waterfront resorts sit across from one another on Crescent Lake in Lake Buena Vista, Florida.

The posh guest rooms at both resorts have been redesigned to include sophisticated décor and popular Heavenly Beds® to comfortably whisk guests away to a good night's rest after a full day of exploring Orlando's premier attractions.

Top 5 reasons to stay at the Walt Disney World Swan and Dolphin

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

Weather

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

COME TO ORLANDO!

Dear Colleagues and Friends,

What a perfect time to visit sunny Orlando, right at the start of spring. Come and experience the best cybersecurity training in the industry! SANS 2015 will be offering more classes, night sessions, and vendor events than ever before including both Core NetWars and DFIR NetWars tournaments.

We are back at the **Walt Disney World Swan and Dolphin Hotel** (swandolphin.com), right next door to the Boardwalk with Epcot® and Disney's Hollywood Studios™. You can order Magic Bands and make FastPass+ reservations before you leave home.

The Walt Disney World® property is twice the size of Manhattan, so we recommend staying at the hotel complex. Benefits include complimentary transportation around Walt Disney World® and Orlando Premium Outlets as an extra treat to SANS attendees, plus complimentary high-speed Internet, access to fitness facilities, and bottled water in the guest room. Be sure to book under the SANS special rate as these amenities are not available to the general public.

This year SANS 2015 coincides with The Epcot® Flower and Garden Festival, which features special flower and garden displays, presentations and demonstrations, and concerts throughout the festival. The Magic Kingdom® Park has just doubled the size of Fantasyland with some brand new attractions including themes based on the Little Mermaid, Beauty and the Beast, and a new coaster based on Snow White and the Seven Dwarfs.

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

For tips on the Walt Disney World® parks and Orlando attractions, check out my personal favorite site at www.allearsnet.com where you will find reviews, restaurant menus with prices, and park updates. You will also want to check out the SANS2015 program guide for all of the action-packed presentations, receptions, and events as well as the social board for student gatherings. Please feel free to send me an e-mail at Brian@sans.org if I can be of any assistance.

See you real soon at SANS 2015!

Brian Correia

Brian Correia
Director, Business Development & Venue Planning

Five Reasons to Register

1. The best career move you will ever make!
That's how one SANS alumnus described the IT security education and networking opportunities offered by SANS. Attending SANS 2015 is a way of investing in your career. To reap the maximum benefit, read the course descriptions carefully. Check out the long courses plus a wide variety of one- to three-day skill-based short courses.

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

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

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

5. Don't miss out on a good opportunity!
This is your chance to make a great career move, be taught by the cream of the crop, challenge yourself, and become part of an elite group during a full week of IT security education and networking opportunities. Come prepared to learn; we will come prepared to teach.

REGISTRATION INFORMATION

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

How to Register

1. To register, go to sans.org/event/sans-2015/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 e-mail confirmation will arrive soon after you register.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	2/18/15	$400.00	3/18/15	$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 SANS 2015 Simulcast course, please visit sans.org/event/sans-2015/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 $629 when combined with SANS 2015 training
- Deadline to register at this price is the last day of SANS 2015
- Price goes to $949 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 e-mail 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 March 18, 2015. 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 or have payments refunded.

SANS 2015 REGISTRATION FEES

Register online at sans.org/event/sans-2015/courses

If you don't wish to register online, please call 301-654-SANS (7267) 9:00am-8:00pm (Mon-Fri) EST and we will fax or mail you an order form.

Job-Based Long Courses		Paid by 2/18/15	Paid by 3/18/15	Paid after 3/18/15	Add GIAC Cert	Add OnDemand	Add NetWars Continuous
☐ SEC301	Intro to Information Security	$4,215	$4,415	$4,615	☐ $629	☐ $629	☐ $1,099
☐ SEC401	Security Essentials Bootcamp Style	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC501	Advanced Security Essentials – Enterprise Defender	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC503	Intrusion Detection In-Depth	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC504	Hacker Tools, Techniques, Exploits, and Incident Handling	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC505	Securing Windows with the Critical Security Controls	$4,875	$5,075	$5,275	☐ $629	☐ $629	☐ $1,099
☐ SEC511	Continuous Monitoring and Security Operations NEW!	$4,950	$5,150	$5,350			☐ $1,099
☐ SEC542	Web Application Penetration Testing and Ethical Hacking	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC560	Network Penetration Testing and Ethical Hacking	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC561	Intense Hands-on Pen Testing Skill Development (with SANS NetWars)	$4,950	$5,150	$5,350			☐ $1,099
☐ SEC566	Implementing and Auditing the Critical Security Controls – In-Depth	$4,370	$4,570	$4,770	☐ $629	☐ $629	☐ $1,099
☐ SEC573	Python for Penetration Testers	$4,215	$4,415	$4,615			☐ $1,099
☐ SEC575	Mobile Device Security and Ethical Hacking	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC579	Virtualization and Private Cloud Security	$4,950	$5,150	$5,350		☐ $629	☐ $1,099
☐ SEC617	Wireless Ethical Hacking, Penetration Testing, and Defenses	$4,740	$4,940	$5,140	☐ $629	☐ $629	☐ $1,099
☐ SEC642	Advanced Web App Penetration Testing and Ethical Hacking	$4,740	$4,940	$5,140		☐ $629	☐ $1,099
☐ SEC660	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ SEC760	Advanced Exploit Development for Penetration Testers NEW!	$4,950	$5,150	$5,350			☐ $1,099
☐ AUD507	Auditing & Monitoring Networks, Perimeters, and Systems	$4,740	$4,940	$5,140	☐ $629	☐ $629	☐ $1,099
☐ DEV522	Defending Web Applications Security Essentials	$4,740	$4,940	$5,140	☐ $629	☐ $629	☐ $1,099
☐ DEV544	Secure Coding in .NET: Developing Defensible Applications	$3,750	$3,950	$4,150	☐ $629	☐ $629	☐ $1,099
☐ FOR408	Windows Forensic Analysis	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ FOR508	Advanced Digital Forensics and Incident Response	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ FOR572	Advanced Network Forensics and Analysis	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ FOR585	Advanced Smartphone Forensics	$4,950	$5,150	$5,350		☐ $629	☐ $1,099
☐ FOR610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	$4,950	$5,150	$5,350	☐ $629	☐ $629	☐ $1,099
☐ LEG523	Law of Data Security and Investigations	$4,215	$4,415	$4,615	☐ $629	☐ $629	☐ $1,099
☐ MGT414	SANS® +S™ Training Program for the CISSP® Certification Exam	$4,215	$4,415	$4,615	☐ $629	☐ $629	☐ $1,099
☐ MGT512	SANS Security Leadership Essentials For Managers with Knowledge Compression™	$4,595	$4,795	$4,995	☐ $629	☐ $629	☐ $1,099
☐ MGT514	IT Security Strategic Planning, Policy and Leadership	$4,215	$4,415	$4,615		☐ $629	☐ $1,099
☐ MGT525	IT Project Management, Effective Communication, and PMP® Exam Prep	$4,215	$4,415	$4,615	☐ $629	☐ $629	☐ $1,099
☐ HOSTED	(ISC)²® Certified Secure Software Lifecycle Professional (CSSLP®) CBK® Education Program	$3,145	$3,145	$3,145			☐ $1,099

Skill-Based Short Courses		If taking a 5-6 day course					
☐ SEC440	Critical Security Controls: Planning, Implementing and Auditing	$1,350	$2,100	$2,100	$2,100		
☐ 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 & Measure a High-Impact Awareness Program	$1350	$1,980	$1,980	$1,980		
☐ MGT535	Incident Response Team Management	$750	$1,150	$1,150	$1,150		
☐ HOSTED	Physical Penetration Testing – Introduction		$2,000	$2,000	$2,000		
☐ HOSTED	Offensive Countermeasures: The Art of Active Defenses		$1,900	$1,900	$1,900		
☐ HOSTED	Health Care Security Essentials NEW!		$1,995	$1,995	$1,995		☐ $1,099
☐ SPECIAL	CORE NetWars Tournament – Tournament Entrance Fee	FREE	$1,299	$1,299	$1,299		
☐ SPECIAL	DFIR NetWars Tournament – Tournament Entrance Fee	FREE	$1,299	$1,299	$1,299		

Individual Courses Available

	MON 4/13	TUE 4/14	WED 4/15	THU 4/16	FRI 4/17	SAT 4/18
AUD507	☐ 507.1	☐ 507.2	☐ 507.3	☐ 507.4	☐ 507.5	☐ 507.6
SEC301	☐ 301.1	☐ 301.2	☐ 301.3	☐ 301.4	☐ 301.5	
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 . . . $1,420
- ☐ Two Full Days . . . $2,255
- ☐ Three Full Days . . . $3,180
- ☐ Four Full Days . . . $4,150
- ☐ Five Full Days . . . $4,615
- ☐ Six Full Days . . . $5,355

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

SANS NewsBites

Join over 200,000 professionals who subscribe to this high-level, executive summary of the most important news and issues relevant to cybersecurity professionals. Delivered twice weekly. Read insightful commentary from expert SANS instructors.

InfoSec Reading Room

Computer security research and whitepapers

Security Policies

Templates for rapid information security policy development

Top 25 Software Errors

The most widespread and critical errors leading to serious vulnerabilities

OUCH!

OUCH! is the world's leading, free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the SANS Securing The Human team, SANS instructor subject-matter experts and team members of the community. Each issue focuses on a specific topic and actionable steps people can take to protect themselves, their family and their organization.

Open a SANS Portal Account

Sign up for a **SANS Portal Account** and receive free webcasts, newsletters, the latest news and updates, and many other free resources.

sans.org/portal

Webcasts

SANS Information Security Webcasts are live broadcasts by knowledgeable speakers addressing key issues in cybersecurity, often in response to breaking news about risks. Gain valuable information on topics you tell us are most interesting!

Critical Security Controls

Consensus guidelines for effective cyber defense

Industry Thought Leadership

In-depth interviews with the thought leaders in information security and IT

Intrusion Detection FAQ

The Internet's most trusted site for vendor-neutral intrusion detection information

@RISK: The Consensus Security Alert

@RISK provides a reliable weekly summary of:

1. Newly discovered attack vectors
2. Vulnerabilities with active new exploits
3. Insightful explanations of how recent attacks worked and other valuable data

A key purpose of @RISK is to provide data that will ensure that the Critical Controls continue to be the most effective defenses for all known attack vectors.

SAVE $400

Scan the QR code and register and pay by Feb 18th to SAVE $400 on SANS 2015 courses.

sans.org/info/168567