SANS

The most trusted source for information security training, certification, and research

INFORMATION SECURITY TRAINING

Fall **2017** Course Catalog

80+
Extraordinary SANS certified instructors

200+
Live events globally, plus multiple online options

Curricula

Cyber Defense
Detection and Monitoring
Penetration Testing
Incident Response
Digital Forensics

Ethical Hacking
Management, Audit, Legal
Secure Development
ICS/SCADA Security

"You cannot beat the quality of SANS classes and instructors. I came back to work and was able to implement my skills learned in class on day one. Invaluable."

- Melissa Sokolowski, Xerox

www.sans.org

Table of Contents

"SANS courses give you real-world skills that have an immediate value on the security environment."

– Eric Kaithula, Symetra

SANS Institute

The most trusted source for information security training, certification, and research

SANS Institute's mission is to deliver cutting-edge information security knowledge and skills to companies, military organizations, and governments in order to protect people and assets.

CUTTING-EDGE TRAINING

More than 55 unique courses are designed to align with dominant security team roles, duties, and disciplines. They prepare students to meet today's threats and tomorrow's challenges.

The SANS curriculum spans Cyber Defense, Digital Forensics & Incident Response, Threat Hunting, Audit, Management, Pen Testing, Industrial Control Systems Security, Secure Software Development, and more. Each curriculum offers a progression of courses that can take professionals from a subject's foundations right up to top-flight specialization.

We constantly update and rewrite these courses to teach the tools and techniques that are proven to keep networks safe.

Our training is designed to be practical. Students are immersed in hands-on lab exercises built to let them practice, hone, and perfect what they've learned.

LEARN FROM EXPERTS

SANS courses are taught by an unmatched faculty of active security practitioners. Each instructor brings a wealth of real-world experience to every classroom – both live and online. SANS instructors work for high-profile organizations as red team leaders, CISOs, technical directors, and research fellows.

Along with their respected technical credentials, SANS instructors are also expert teachers. Their passion for the topics they teach shines through, making the SANS classroom dynamic and effective.

WHY SANS IS THE BEST TRAINING AND EDUCATIONAL INVESTMENT

SANS immersion training is intensive and hands-on, and our courseware is unrivaled in the industry.

SANS instructors and course authors are leading industry experts and practitioners. Their real-world experience informs their teaching and training content. SANS training strengthens a student's ability to achieve a GIAC certification.

THE SANS PROMISE

At the heart of everything we do is the SANS Promise: Students will be able to deploy the new skills they've learned as soon as they return to work.

HOW TO REGISTER FOR SANS TRAINING

The most popular option to take SANS training is to attend a 5- or 6-day technical course taught live in a classroom at one of our 200+ training events held globally throughout the year. SANS training events provide an ideal learning environment and offer the chance to network with other security professionals as well as SANS instructors and staff.

SANS training can also be delivered online, with several convenient options to suit your learning style. All SANS online courses include at least four months of access to the course material anytime and anywhere, enabling students to revisit and rewind content.

Students can learn more and register online by visiting www.sans.org/online

SANS LIVE & ONLINE TRAINING

GIAC CERTIFICATIONS

SANS Technology Institute

SANS SECURITY AWARENESS

CyberTalent

INTERNET STORM CENTER

NETWARS

SANS Training Formats

Whether you choose to attend a training class live or online, the entire SANS team is dedicated to ensuring your training experience exceeds expectations.

Live Classroom Instruction

Premier Training Events

Our most recommended format, live SANS training events deliver SANS's top instructors teaching multiple courses at a single time and location, allowing

- Focused, immersive learning without the distractions of your office environment
- Direct access to SANS Certified Instructors
- Interactions and learning from other professionals
- @Night events, NetWars, Vendor presentations, industry receptions, and many other benefits

Our premier live training events in North America, serving thousands of students, are held in Orlando, Washington DC, Las Vegas, New Orleans, and San Diego. Regional events with hundreds of students are held in most major metropolitan areas during the year. See page 97 for upcoming Training Events in North America.

Summits

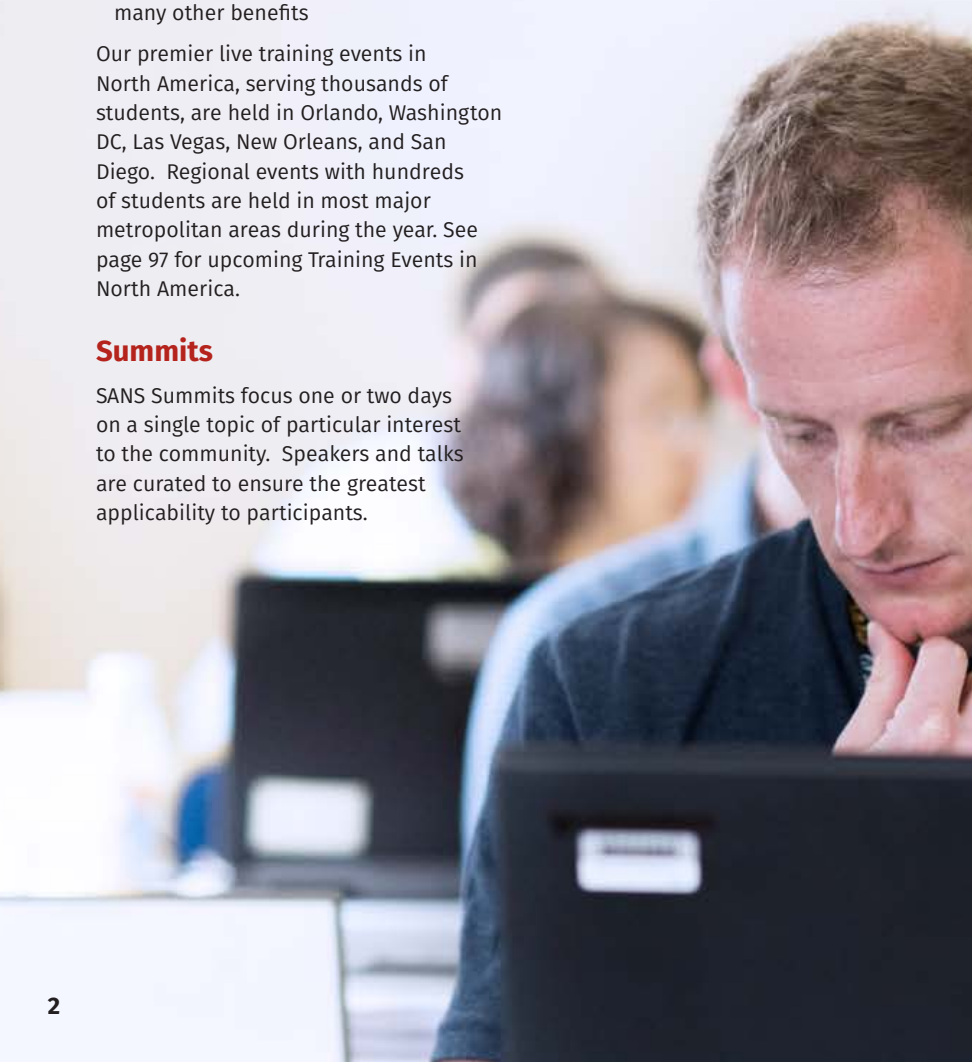
SANS Summits focus one or two days on a single topic of particular interest to the community. Speakers and talks are curated to ensure the greatest applicability to participants.

Community SANS Courses

Same SANS courses, courseware, and labs, taught by up-and-coming instructors in a regional area. Smaller classes allow for more extensive instructor interaction. No need to travel; commute each day to a nearby location.

Private Classes

Bring a SANS Certified Instructor to your location to train a group of your employees in your own environment. Save on travel and address sensitive issues or security concerns in your own environment.



Online Training

SANS Online successfully delivers the same measured learning outcomes to students at a distance that we deliver live in classrooms. More than 30 courses are available for you to take whenever or wherever you want. Thousands of students take our courses online each year and frequently achieve certification.

Top reasons to take SANS courses online:

- Learn at your own pace, over four months
- Spend extra time on complex topics
- Repeat labs to ensure proficiency with skills
- Save on travel costs
- Study at home or in your office

Our SANS OnDemand, vLive, Simulcast, and SelfStudy formats are backed by nearly 100 professionals who ensure we deliver the same quality instruction online (including support) as we do at live training events.

"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."

-Dan Trueman, Novae PLC

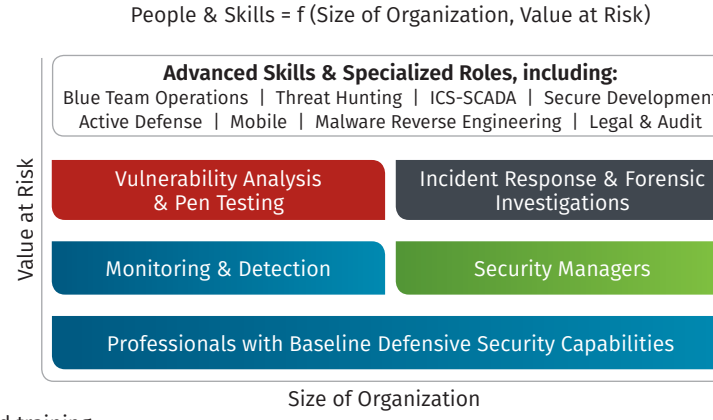
Build a High-Performing Security Organization

SANS recommends three strategies for building an information security group, based on our research and observations globally:

1 - Use practical organizing principles to design your plan and efforts. Nearly all of the more complex frameworks may be reduced to four or five simpler constructs, such as "Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents."

2 - Prioritize your efforts within these areas using the **CIS Critical Controls** as you mature your own organization.

3 - Determine the number and type of professionals you require to perform the hands-on work. **Engage in a persistent campaign** to develop professionals with the appropriate skills and capabilities. Cybersecurity is a specialized practice area within IT and demands specialized training.



- Every professional entrusted with hands-on work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents when they occur. Set a high bar for the baseline set of skills in your security organization.
- Four job roles typically emerge as organizations grow in size and risk/complexity:
  - **Security Monitoring & Detection Professionals** – The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Vendor training all too often teaches to the tool, and not how or why the tool works, or how best it can be deployed. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and interpret their output.
  - **Pen Testers & Vulnerability Analysts** – The professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different way of thinking and different tools, but is essential for defense specialists to improve defenses.
  - **Forensic Investigators & Incident Responders** – Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.
  - **Security Managers** – With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.
- Within (or beyond) these four areas, high-performing security organizations will develop individual professionals to either utilize advanced skills generally, or to meet specialized needs. Along the entire spectrum, from Active Defense to Cloud Defense to Python for Pen Testers to Malware Re-engineering, SANS offers more than 30 courses for specialized roles or more advanced topics, meeting the needs of nearly all security professionals at every level.

VIEW THE SANS TRAINING ROADMAP to match courses to associated training paths, job roles, and skills. p.4

SANS Training Roadmap | Choose Your Path

Baseline Skills

1 **You are** experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the "offense informs defense" preparation that teaches defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

- SEC**401** Security Essentials Bootcamp Style — **GSEC** Certification Security Essentials (p. 8)
- SEC**504** Hacker Tools, Techniques, Exploits, and Incident Handling — **GCIH** Certification Certified Incident Handler (p. 10)

1b **You** will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management

- MGT**512** SANS Security Leadership Essentials for Managers with Knowledge Compression™ — **GSLC** Certification Security Leadership (p. 12)
- SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth — **GCCC** Certification Critical Security Controls (p. 14)

New to Cybersecurity?

- SEC**301** Intro to Information Security — **GISF** Certification Information Security Fundamentals (p. 22)

Focus Job Roles

2 **You are** experienced in security, preparing for a specialized job role or focus

Security Monitoring & Detection

- SEC**503** Intrusion Detection In-Depth — **GCIA** Certification Certified Intrusion Analyst (p. 18)
- SEC**511** Continuous Monitoring and Security Operations — **GMON** Certification Continuous Monitoring (p. 20)

Penetration Testing & Vulnerability Analysis

- SEC**560** Network Penetration Testing and Ethical Hacking — **GPEN** Certification Penetration Tester (p. 38)
- SEC**542** Web App Penetration Testing and Ethical Hacking — **GWAPT** Certification Web Application Penetration Tester (p. 40)

Incident Response and Enterprise Forensics

- FOR**508** Advanced Digital Forensics, Incident Response, and Threat Hunting — **GCFA** Certification Forensic Analyst (p. 60)
- FOR**572** Advanced Network Forensics and Analysis — **GNFA** Certification Network Forensic Analyst (p. 62)

- MGT**414** SANS Training Program for CISSP® Certification — **GISP** Certification Information Security Professional (p. 78)

Crucial Skills, Specialized Roles

SANS's comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 **You are** a candidate for specialized or advanced training

Cyber Defense Operations

- SEC**501** Advanced Security Essentials – Enterprise Defender **GCED** (p. 24)
- SEC**505** Securing Windows and PowerShell Automation **GCWN** (p. 26)
- SEC**506** Securing Linux/Unix | **GCUX** (p. 28)
- SEC**545** Cloud Security Architecture and Operations (p. 30)
- SEC**555** SIEM with Tactical Analytics (p. 32)
- SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC** (p. 14)
- SEC**579** Virtualization and Software-Defined Security (p. 34)

Industrial Control Systems Security

- ICS**410** ICS/SCADA Security Essentials | **GICSP** (p. 92)
- ICS**456** Essentials for NERC Critical Infrastructure Protection (p. 96)
- ICS**515** ICS Active Defense and Incident Response | **GRID** (p. 94)

Penetration Testing & Ethical Hacking

- SEC**550** Active Defense, Offensive Countermeasures and Cyber Deception (p. 43)
- SEC**561** Immersive Hands-On Hacking Techniques (p. 44)
- SEC**573** Automating Information Security with Python **GPYC** (p. 46)
- SEC**575** Mobile Device Security and Ethical Hacking **GMOB** (p. 48)
- SEC**617** Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN** (p. 50)
- SEC**642** Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques (p. 52)
- SEC**660** Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN** (p. 54)
- SEC**760** Advanced Exploit Development for Penetration Testers (p. 56)

Digital Forensics and Incident Response

- FOR**500** **(formerly FOR408)** Windows Forensic Analysis **GCFE** (p. 64)
- FOR**518** Mac Forensic Analysis (p. 66)
- FOR**526** Memory Forensics In-Depth (p. 68)
- FOR**578** Cyber Threat Intelligence **(Certification Coming Soon)** (p. 70)
- FOR**585** Advanced Smartphone Forensics | **GASF** (p. 72)
- FOR**610** Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM** (p. 74)

Software Security

- DEV**522** Defending Web Applications Security Essentials **GWEB** (p. 88)
- DEV**541** Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA** (p. 90)
- DEV**544** Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET** (p. 91)

Management

- MGT**514** IT Security Strategic Planning, Policy, and Leadership | **GSTRT** (p. 80)
- MGT**517** Managing Security Operations: Detection, Response, and Intelligence (p. 82)
- MGT**525** IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM** (p. 84)

Audit | Legal

- AUD**507** Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA** (p. 86)
- SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC** (p. 14)
- LEG**523** Law of Data Security and Investigations | **GLEG** (p. 87)

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few Powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled "You Will Be Able To." Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of skills and knowledge that a GIAC Certification provides. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

SANS Baseline Skills

Core Security Techniques | Security Management

The foundation of a successful career in information security – whether technical or managerial – should be comprehensive and rooted in real-world expertise. Learn more about the SANS courses and certifications recommended for baseline skills below and on the following pages.

Core Security Techniques
Defend & Maintain

SEC**401** Security Essentials Bootcamp Style	**GSEC** Certification Security Essentials
SEC**504** Hacker Tools, Techniques, Exploits and, Incident Handling	**GCIH** Certification Certified Incident Handler

Summary: Every hands-on technical professional should possess the baseline set of knowledge and skills taught in **SEC401** and **SEC504**. These courses cover the essentials of defense-in-depth, the mental model for how attacks work, and the proven methods for handling incidents when they occur.

Who This Path is For: Hands-on technical professionals such as Network Administrators and Engineers, Security Analysts, and Consultants who need well-rounded and effective baseline security skills.

Why This Training is Important: This training gives you an essential knowledge and understanding about how a variety of attacks occur and how to respond to them.

Security Management

MGT**512** SANS Security Leadership Essentials for Managers with Knowledge Compression™	**GSLC** Certification Security Leadership
SEC**566** Implementing and Auditing the Critical Security Controls – In-Depth	**GCCC** Certification Critical Security Controls

Summary: Those who are expected to lead security policy development, security projects or teams of information security technicians should be versed in the content of **MGT512** and **SEC566**. These courses provide the knowledge and tools required to execute information security activities effectively.

Who This Path is For: Managers, auditors, or security tasks supervisors, such as: Security Architects and Engineers, Managers of IT, or Risk Consultants

Why This Training is Important: These courses help you understand terminology, learn cutting-edge security practices, and prepare you to supervise the security component of any technology project.

SEC401

GSEC Certification
Security Essentials

www.giac.org/gsec

Security Essentials Bootcamp Style

Six-Day Program
46 CPEs
Laptop Required
This course has evening Bootcamp Sessions

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

You Will Be Able To

- Design and build a network architecture using VLANs, NAC and 802.1x based on an 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 the 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
- 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
- Apply what you learned directly to your job when you go back to work

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

STOP and ask yourself the following questions:

- **Do you fully understand why some organizations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident that you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

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. Our 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 rise in advanced persistent threats, 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 will 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.

"This training builds the foundation for a security professional."

-M. D. Arifuzzaman, CSIRO

SANS Technology Institute
www.sans.edu

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

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: Setting Up a Lab with Virtual Machines; 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 attack strategies and how the offense operates.

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

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: Firewalls and Perimeters; Honeypots; Host-based Protection; Network-based Intrusion Detection and Prevention; Vulnerability Scanning and Remediation; Web Security

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. The day finishes by looking at using the Critical Security Controls for metrics-based dashboards and performing risk assessment across an organization.

Topics: Cryptography; Steganography; Critical Security Controls; Risk Assessment and Auditing

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 by looking at automation, auditing, and forensics.

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 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

***SEC401** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach	Long Beach, CA	Jul 10-15
SANSFIRE	Washington, DC	Jul 24-29
San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21-26
Tampa-Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Jul 24-29
Virtual/Online	Aug 21-26
Virtual/Online	Sep 25-30
Virtual/Online	Oct 30 - Nov 4
Virtual/Online	Dec 14-19

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online	Oct 30 - Dec 6
Virtual/Online	Dec 11 - Jan 24

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Minneapolis, MN	Jul 10-15
Phoenix, AZ	Jul 10-15
Colorado Springs, CO	Jul 17-22
Charleston, SC	Jul 24-29
Fort Lauderdale, FL	Jul 31-Aug 5
Omaha, NE	Aug 14-19
San Diego, CA	Aug 21-26
Trenton, NJ	Aug 21-26
Albany, NY	Sep 11-16
Columbia, MD	Sep 18-23
Dallas, TX	Sep 18-23
Boise, ID	Sep 25-30
New York, NY	Sep 25-30
Sacramento, CA	Oct 2-7

Mentor Classes

Ventura, CA	Jul 12 - Sep 13
Macon, GA	Jul 12 - Aug 23
Arlington, VA	Sep 20 - Nov 1

Private Training

All SANS courses are available through Private Training.

SEC504

GCIH Certification
Incident Handler

www.giac.org/gcih

Hacker Tools, Techniques, Exploits, and Incident Handling

Six-Day Program
37 CPEs
Laptop Required
This course has extended hours

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

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

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection and 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.**

"The hands-on labs and the technical background on how attacks work are very insightful and shows us how hackers operate."

-Christopher Miller, Global Payments Inc.

This course enables you to turn the tables on computer attackers by helping you to understand their 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. 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 for, 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, exploiting, and defending systems. **This course will enable you to discover the holes in your system before the bad guys do!**

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

"As someone who works in information security but has never had to do a full incident report, SEC504 taught me all the proper processes and steps."

-Todd Choryan, Motorola Solutions

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

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) necessary 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 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**

***SEC504** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach Long Beach, CA . . . . . Jul 10-15
SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
San Antonio. . . . . San Antonio, TX . . . . . Aug 6-11
Boston . . . . . Boston, MA . . . . . Aug 7-12
New York City . . . . . New York, NY. . . . . Aug 14-19
Salt Lake City . . . . . Salt Lake City, UT . . . . Aug 14-19
Chicago . . . . . Chicago, IL . . . . . Aug 21-26
Virginia Beach. . . . . Virginia Beach, VA Aug 27 - Sep 1
Tampa-Clearwater. . . . . Clearwater, FL. . . . . Sep 5-10
San Francisco Fall . . . . . San Francisco, CA . . . . Sep 5-10
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15
Baltimore Fall . . . . . Baltimore, MD . . . . . Sep 25-30
Rocky Mountain Fall . . . Denver, CO . . . . . Sep 25-30
Phoenix-Mesa . . . . . Mesa, AZ . . . . . Oct 9-14
San Diego . . . . . San Diego, CA . . . Oct 30 - Nov 4
Seattle . . . . . Seattle, WA . . . . . Oct 30 - Nov 4
Miami . . . . . Miami, FL . . . . . Nov 6-11
San Francisco Winter . . . San Francisco, CA Nov 27 - Dec 2
Austin Winter. . . . . Austin, TX . . . . . Dec 4-9
CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

Summit Events

ICS & Energy – Houston, TX . . . . . Jul 10-15
Security Awareness – Nashville, TN . . . . . Aug 4-9
Pen Test Hackfest – Bethesda, MD. . . . . Nov 15-20

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online . . . . . Dec 14-19

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online . . . . . Sep 5 - Oct 12

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Seattle, WA . . . . . Jul 10-15
Sacramento, CA. . . . . Jul 17-22
Phoenix, AZ. . . . . Jul 24-29
Des Moines, IA . . . . . Jul 24-29
Annapolis, MD. . . . . Jul 24-29
Raleigh, NC. . . . . Aug 7-12
Memphis, TN. . . . . Aug 21-26
Columbia, MD . . . . . Sep 25-30
New York, NY . . . . . Nov 6-11

Mentor Classes

Denver, CO . . . . . Aug 29 - Oct 10
Arlington, VA. . . . . Sep 20 - Nov 1
Boston, MA . . . . . Sep 26 - Nov 7

Private Training

All SANS courses are available through Private Training.

MGT512

GSLC Certification
Security Leadership

www.giac.org/gslc

SANS Security Leadership Essentials For Managers with Knowledge Compression™

Five-Day Program
33 CPEs
Laptop Recommended
This course has extended hours

Who Should Attend

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

You Will Be Able 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

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

Essential security topics covered in this management track include network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, web application security, and offensive and defensive information warfare, culminating with our management practicum. The material uses Knowledge Compression,™ special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

Knowledge Compression™

Maximize your learning potential!

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

SANS Technology Institute
www.sans.edu

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

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**

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; 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.

"This was a great course that I feel all management should take. It helps managers understand not only security but also technical and business concepts and issues."-David Stewart, ADM

***MGT512** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach	Long Beach, CA	Jul 10-14
SANSFIRE	Washington, DC	Jul 24-28
San Antonio	San Antonio, TX	Aug 6-10
Chicago	Chicago, IL	Aug 21-25
Virginia Beach	Virginia Beach, VA	Aug 21-25
Tampa-Clearwater	Clearwater, FL	Sep 5-9
NETWORK SECURITY	Las Vegas, NV	Sep 11-15
Tysons Corner Fall	McLean, VA	Oct 16-20
San Diego	San Diego, CA	Oct 30 - Nov 3
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-18

OnDemand

E-learning available anytime, anywhere, at your pace

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Seattle, WA	Aug 14-18
New Orleans, LA	Aug 21-25
New York, NY	Aug 28 - Sep 1
Columbus, OH	Sep 25-29

Private Training

All SANS courses are available through Private Training.

"MGT512 is one of the most valuable courses I've taken with SANS. It really did help bridge the gap from security practitioner to security orchestrator. Truly a gift!"

-John Madick, Epiq Systems, Inc.

SEC566

GCCC Certification
Critical Controls

www.giac.org/gccc

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel or contractors
- Staff and clients of federal agencies
- 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

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

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? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

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

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

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS's 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.

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.

SANS Technology Institute

www.sans.edu

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: Controlled Use of Administrative Privileges
Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

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

Topics: **Critical Control 7: Email and Web Browser Protections**
Critical Control 8: Malware Defenses
Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 10: Data Recovery Capability (validated manually)
Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

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

Topics: **Critical Control 12: Boundary Defense**
Critical Control 13: Data Protection
Critical Control 14: Controlled Access Based on the Need to Know
Critical Control 15: Wireless Device Control

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

Topics: **Critical Control 16: Account Monitoring and Control**
Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
Critical Control 18: Application Software Security
Critical Control 19: Incident Response and Management (validated manually)
Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

"This course provides direction and metrics for evaluating an organization's system."

-Anthony Clarke, Marion County Public Schools

***SEC566** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-28
Chicago ..... Chicago, IL ..... Aug 21-25
San Francisco Fall ..... San Francisco, CA ..... Sep 5-9
NETWORK SECURITY ..... Las Vegas, NV ..... Sep 11-15
Rocky Mountain Fall ..... Denver, CO ..... Sep 25-29
Phoenix-Mesa ..... Mesa, AZ ..... Oct 9-13
Tysons Corner Fall ..... McLean, VA ..... Oct 16-20
San Diego ..... San Diego, CA ..... Oct 30 - Nov 3
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-18

Summit Events

Security Awareness – Nashville, TN ..... Aug 4-8

OnDemand

E-learning available anytime, anywhere, at your pace

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Scottsdale, AZ ..... Aug 14-18

Private Training

All SANS courses are available through Private Training.

"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

"I think the exam was both fair and practical. These are the kind of real world problems I expect to see in the field."

– Carl Hallberg, Wells Fargo,
GIAC Reverse Engineering Malware (GREM)

"GIAC made the testing process much better than other organizations. The material is spot on with what I do at work, daily."

– Jason Pfister, EWEB,
GIAC Continuous Monitoring (GMON)

"It feels like SANS and GIAC are working with the candidates to help them to meet the required standards, which are achievable with hard work."

– Thomas Gurney,
GIAC Certified Intrusion Analyst (GCIA)

"It's an awesome effort; great questions, excellent material and presentation throughout the (training event) week. I've really enjoyed it and will recommend it to many. Thank you GIAC/SANS!"

– Nicolas B., Intrasys,
GIAC Certified Incident Handler (GCIH)

GIAC
The Highest Standard in Cybersecurity Certification

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

SANS | GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

WWW.GIAC.ORG

Focus Job Roles and Specialized Skills

Monitoring and Detection

Security Monitoring and Detection

SEC503 Intrusion Detection In-Depth

GCIA Certification Certified Intrusion Analyst

SEC511 Continuous Monitoring and Security Operations

GMON Certification Continuous Monitoring

Summary: Effective monitoring and detection of threats in your network environment requires focused training and techniques. The core skills required are taught in **SEC503: Intrusion Detection In-depth**, and **SEC511: Continuous Monitoring and Security Operations**.

Specialized and advanced cyber defense skills are taught in SANS courses **SEC501**, **SEC505**, **SEC506** and **SEC579**. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path is For: Security and Network Analysts, Engineers, Operations Professionals, and SOC Managers.

Why This Training is Important: Practicing proactive monitoring, continuous diagnostics and mitigation, and knowing the underlying theory of TCP/IP so that you can configure and master open-source tools to analyze traffic on your network, are keys to being an effective cyber defender. The payoff to using these tools and techniques is the early detection of an intrusion, or successfully thwarting the efforts of attackers altogether.

"The focus on methodologies was superb because the techniques taught are applicable to every environment regardless of the tools utilized."

-Conrad Bovell, DSS

"This is great training that shows you potential indicators of compromise and the tools and techniques to look for and identify potentialy compromised systems."

-Stephen Larkin, Exekib Corporation

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst

www.giac.org/gcia

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

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
- Craft packets with Scapy
- 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

"This course gives rookie and experienced professionals great tools and techniques to go with the knowledge."

-Brian Nichols, County of Midland, MI

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?

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 sometimes 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 with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasizes the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

"The concepts learned in SEC503 helped me bridge a gap in knowledge of what we need to better protect our organization."

-Greg Thys, Mary Greeley Medical Center

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 DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. 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.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS


www.sans.org/8140

503.1 HANDS ON: Fundamentals of Traffic Analysis – PART 1

Day 1 provides a refresher or introduction, depending on your background, to TCP/IP. It describes the need to understand packet structure and content. It covers the essential foundations such as the TCP/IP communication model, and the theory of bits, bytes, binary and hexadecimal. We introduce the use of open-source Wireshark and tcpdump for analysis. We begin our exploration of the TCP/IP communication model with the study of the link layer, the IP layer, both IPv4 and IPv6 and packet fragmentation in both. We describe the layers and analyze traffic not just in theory and function, but from the perspective of an attacker and defender. All traffic is discussed and displayed using the two open-source tools, Wireshark and tcpdump.

Topics: Concepts of TCP/IP; Introduction to Wireshark; Network Access/Link Layer: Layer 2; IP Layer: Layer 3

503.2 HANDS ON: Fundamentals of Traffic Analysis – PART 2

Day 2 continues where the previous day ended in understanding the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using their advanced features 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 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows the manipulation, creation, reading, and writing of packets. Scapy can be used to craft packets to test the detection capability of an IDS/IPS, especially important when a new user-created IDS rule is added, for instance for a recently announced vulnerability. The examination of TCP/IP culminates with an exploration of the application protocol layer. The concentration is on some of the most widely used, and sometimes vulnerable, crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications. Our focus is on protocol analysis, a key skill in intrusion detection. IDS/IPS evasions are the bane of the analyst, so the theory and possible implications of evasions at different protocol layers are examined.

Topics: Scapy; Advanced Wireshark; Detection Methods for Application Protocols; DNS; Microsoft Protocols; HTTP(2)/TLS; SMTP; IDS/IPS Evasion Theory

503.4 HANDS ON: Network Monitoring: Snort and Bro

The fundamental knowledge gained from the first three days provides a fluid progression into one of the most popular days of SEC503. Snort and Bro are widely deployed open-source IDS/IPS solutions that have been industry standards for many years. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a look at options and requirements of devices that can sniff and capture the traffic for inspection. Next, the topic of the analyst's role in the detection process is examined. Before Snort and Bro are discussed, the capabilities and limitations are considered. Snort detection flow, running Snort, and rules are explored with an emphasis on writing efficient rules. It is likely that false positives and negatives will occur and tips for dealing with them are presented. Bro's unique capability to use its own scripting language to write code to analyze patterns of event-driven behavior is one of the most powerful detection tools available to the analyst. We discuss how this enables monitoring and correlating activity and demonstrate with examples.

Topics: Network Architecture; Introduction to IDS/IPS Analysis; Snort; Bro

503.5 HANDS ON: Network Traffic Forensics

The penultimate day continues the format of less instruction and more hands-on training using three separate incidents that must be analyzed. The three incident scenarios are introduced with some new material to be used in the related hands-on analysis. This material includes an introduction to network forensics analysis for the first scenario. It continues with using network flow records to assist in analysis of the traffic from the second scenario. It concludes with the third scenario where Command and Control channels are discussed and managing analysis when very large packet capture files are involved is examined.

Topics: Introduction to Network Forensics Analysis; Using Network Flow Records; Examining Command and Control Traffic; Analysis of Large pcaps

503.6 HANDS ON: NetWars: IDS Version

The week culminates with a fun hands-on NetWars: IDS Version challenge. Students compete on teams to answer many questions that require using tools and theory covered in the first five days. This is a great way to end the week because it reinforces what was learned by challenging the student to think analytically and strengthens confidence to employ what was learned in in a real-world environment.

***SEC503** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
Virginia Beach	Virginia Beach, VA	Aug 21-26
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Jul 24-29
Virtual/Online	Sep 25-30
Virtual/Online	Oct 30 - Nov 4

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online . . . . . Sep 11 - Oct 18

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Scottsdale, AZ . . . . . Oct 2-7

Private Training

All SANS courses are available through Private Training.

SEC511

GMON Certification
Continuous Monitoring

www.giac.org/gmon

Continuous Monitoring and Security Operations

Six-Day Program
46 CPEs
Laptop Required
This course has evening Bootcamp Sessions

Who Should Attend

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

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 Center (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)
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP800-137
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

"This course has been awesome at teaching me how to use tools and existing architecture in ways I haven't thought of before!"

-John Hubbard, GlaxoSmithKline

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant 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 will 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 this course 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!

SANS Technology Institute

www.sans.edu

511.1 HANDS ON: Current State Assessment, SOCs, and 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 Security Operations Center (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 to 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 Operations Center

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 make up a modern defensible security architecture.

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

511.3 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 network security architecture presented in days one and two emphasize 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

511.4 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 four details ways in which endpoint systems can be both more resilient to attack and also enhance detective capabilities.

Topics: Security Architecture – Endpoint Protection; Dangerous Endpoint Applications; Patching

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 to 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 proactively and repeatedly assesses and reassesses 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, Defend

The course culminates in a team-based design, detect, and defend the flag competition that is a full day of hands-on work applying the principles taught throughout the week.

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

***SEC511** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
Boston	Boston, MA	Aug 7-12
Virginia Beach	Virginia Beach, VA	Aug 21-26
Chicago	Chicago, IL	Aug 21-26
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
San Diego	San Diego, CA	Oct 30 - Nov 4
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Aug 21 - 26
Virtual/Online	Oct 30 - Nov 4

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online	Sep 6 - Oct 12

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

New York, NY	Jul 10-15
Tampa, FL	Jul 17-22
Minneapolis, MN	Aug 21-26

Private Training

All SANS courses are available through Private Training.

SEC301

GISF Certification
Information Security Fundamentals

www.giac.org/gisf

Intro to Information Security

Five-Day Program
30 CPEs
Laptop Required

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Gain an understanding of computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and discuss various security technologies including anti-malware, firewalls, and intrusion detection systems
- Determine your "Phishing IQ" to more easily identify SPAM email messages
- Understand physical security issues and how they support cybersecurity
- Understand incident response, business continuity, and disaster recovery planning at an introductory level
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

"SEC301 is the perfect blend of technical and practical information for someone new to the field, and I would recommend it to a friend."

-Steve Mecco, Draper

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- **Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?**
- **Are you bombarded with complex technical security terms that you don't understand?**
- **Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?**
- **Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?**
- **Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?**

If you answer yes to any of these questions, the SEC301: Intro to Information Security training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised, five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

"I very much appreciate the passion of the instructors. Their knowledge is incredible and the presentation of their knowledge is down-to-earth and helpful. SANS training is far better than privacy-related certification."

-Ron Hoffman, Mutual of Omaha

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Written by a security professional with over 30 years of experience in both the public and private sectors, SEC301 provides uncompromising real-world insight from start to finish. The course prepares you for the Global Information Security Fundamentals (GISF) certification test, as well as for the next course up the line, **SEC401: Security Essentials Bootcamp Style**. It also delivers on the SANS promise: ***You will be able to use the knowledge and skills you learn in SEC301 as soon as you return to work.***

301.1 HANDS ON: Security's Foundation

Every good security practitioner and security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and the Confidentiality, Integrity, and Availability (CIA) Triad, and you'll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, authentication/authorization/accountability.

301.2 HANDS ON: Computer Functions and Networking

This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using ASCII (American Standard Code for Information Interchange). We then spend the remainder of the day on networking. All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. Day two begins with a non-technical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You'll learn about common network hardware such as switches and routers, and you'll finally grasp what is meant by terms like "protocol" and "encapsulation." We'll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you'll have a fundamental grasp of any number of critical technical networking acronyms that you've often heard and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

301.3 HANDS ON: An Introduction to Cryptography

Cryptography is one of the most complex issues faced by security practitioners and cannot be explained in passing, so we will spend some time on it. It is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won't take you through the math behind cryptography, but we'll look at basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a "work factor" in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and "cryptographic hash," and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?

301.4 HANDS ON: Cyber Security Technologies – PART 1

Our fourth day in the classroom begins our exploration of cybersecurity technologies. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. From there, we move into a discussion of network security technologies and methods including compartmentalization, firewalls, intrusion detection and prevention systems, sniffers, content filters, and so on. We end the day with an examination of several data protection protocols used for email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network technologies.

301.5 HANDS ON: Cyber Security Technologies – PART 2

The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at the system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup. We move to application security to learn about browser security and web security, as well as email and instant messaging concerns. We discuss competitive intelligence gathering methods and how you can defend against them. We close the course with an explanation of awareness training and social engineering so that students understand what it is and why it's so difficult to defend against.

***SEC301** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach	Long Beach, CA	Jul 10-14
SANSFIRE	Washington, DC	Jul 24-28
San Antonio	San Antonio, TX	Aug 6-10
New York City	New York, NY	Aug 14-18
Chicago	Chicago, IL	Aug 21-25
NETWORK SECURITY	Las Vegas, NV	Sep 11-15
Baltimore Fall	Baltimore, MD	Sep 25-29
Phoenix-Mesa	Mesa, AZ	Oct 9-13
Tysons Corner Fall	McLean, VA	Oct 16-20
Miami	Miami, FL	Nov 6-10
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-18

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Sep 11-15

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Toronto, ON	Jul 10-14
Boston, MA	Jul 24-28
Portland, OR	Sep 18-22

Private Training

All SANS courses are available through Private Training.

SEC501

GCED Certification
Certified Enterprise Defender

www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Six-Day Program
36 CPEs
Laptop Required

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

You Will Be Able To

- Identify the threats against network infrastructures and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks 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
- Apply the six-step incident handling process
- 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

"SEC501 is the perfect course to immerse enterprise security staff into essential skills. Failing to attend this course is done at the peril of your organization."

-John N. Johnson,
Houston Police Department

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.

"The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion."

-Rachel Weiss, UPS Inc.

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.

"It's great to hear about the instructor's past experiences and real-world cases. This content will greatly enhance my effectiveness upon returning to work."

-Andrew D'Albor, CB&I

SANS Technology Institute
www.sans.edu

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

501.1 HANDS ON: Defensive Network Infrastructure

Making your network secure from attack starts with designing, building, and implementing a robust network infrastructure. There are many aspects to implementing a defense-in-depth network that are often overlooked when companies focus only on functionality. Achieving the proper balance between business drivers and core information security requires that an organization build a secure network that is mission-resilient to a variety of potential attacks. 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 more stealthy and more difficult to find. Only by understanding the core principles of traffic analysis can one become a skilled analyst and distinguish normal traffic from attack traffic. Security professionals must be able to detect new, advanced zero-day attacks before they compromise a network. Prevention, detection, and reaction must all be closely knit so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can continue to operate.

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

501.3 HANDS ON: Pentest

An organization must understand the changing threat landscape and compare that against its own vulnerabilities. On day three students will be shown 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)

***SEC501** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
Boston ..... Boston, MA ..... Aug 7-12
Virginia Beach ..... Virginia Beach, VA ... Aug 21-26
San Francisco Fall ..... San Francisco, CA .... Sep 5-10
NETWORK SECURITY ..... Las Vegas, NV ..... Sep 11-16
Baltimore Fall ..... Baltimore, MD ..... Sep 25-30
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

Summit Events

Secure DevOps – Denver, CO ..... Oct 12-17
Pen Test Hackfest – Bethesda, MD ..... Nov 15-20

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online ..... Aug 21-26
Virtual/Online ..... Sep 25-30

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online ..... Nov 21 - Dec 28

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Portland, OR ..... Jul 17-22
New York, NY ..... Aug 7-12
Columbia, MD ..... Sep 18-23

Private Training

All SANS courses are available through Private Training.

SEC505

GCWN Certification
Windows Security Administrator

www.giac.org/gcwn

Securing Windows and PowerShell Automation

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Security Operations engineers
- Windows endpoint and server administrators
- Anyone who wants to learn PowerShell automation
- Anyone implementing the NSA Top 10 Mitigations
- Anyone implementing the CIS Critical Security Controls
- Those deploying or managing a Public Key Infrastructure or smart cards
- Anyone who needs to reduce malware infections

You Will Be Able To

- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts
- Harden PowerShell itself against abuse, and enable transcription logging
- Use Group Policy to execute PowerShell scripts on an almost unlimited number of hosts, while using Group Policy Object permissions, organizational units, and Windows Management Instrumentation (WMI) to target just the systems that need the scripts run
- Use PowerShell Desired State Configuration (DSC) and Server Manager scripting for the sake of SecOps/DevOps automation of server hardening
- Assuming a breach will occur, use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux *sudo* and *setuid root*
- Configure mitigations against attacks such as pass-the-hash, Kerberos golden tickets, Remote Desktop Protocol (RDP) man-in-the-middle, Security Access Token abuse, and others
- Use PowerShell and Group Policy to manage the Microsoft Enhanced Mitigation Experience Toolkit (EMET), AppLocker whitelisting rules, INF security templates, Windows Firewall rules, IPSec rules, and many other security-related settings
- Install and manage a full Windows Public Key Infrastructure (PKI), including smart cards, certificate auto-enrollment, Online Certificate Status Protocol (OCSP) web responders, and detection of spoofed root Certification Authorities (CAs)
- Harden SSL/TLS, RDP, DNS, and SMB against attacks. This includes deploying DNSSEC, DNS sinkholes for malware, SMB encryption, and TLS cipher suite optimization
- Use PowerShell with the WMI service, such as remote command execution, searching event logs, and doing a remote inventory of user applications

Hackers know how to use PowerShell for evil. Do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – *now what?* A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, IT'S TOO LATE.

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course; we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open source on GitHub for Linux and Mac OS, too.

This course is not a vendor show to convince you to buy another security appliance or to install yet another endpoint agent. The idea is to use built-in or free Windows and Active Directory security tools when we can (especially PowerShell and Group Policy) and then purchase commercial products only when absolutely necessary.

If you are an IT manager or CIO, the aim for this course is to have it pay for itself 10 times over within two years, because automation isn't just good for SecOps/DevOps, it can save money, too.

This course is designed for systems engineers, security architects, and the Security Operations (SecOps) team. The focus of the course is on how to automate the NSA Top 10 Mitigations and the CIS Critical Security Controls related to Windows, especially the ones that are difficult to implement in large environments.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. We don't cover patch management, share permissions, or other such basics – the aim is to go far beyond that. Come have fun learning PowerShell and agile Windows security at the same time!

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

MEETS DoDD 8140
(8570) REQUIREMENTS


www.sans.org/8140

505.1 HANDS ON: PowerShell Automation and Security

PowerShell is made for Security Operations (SecOps) automation on Windows. Today's course covers what you need to know to get started using PowerShell. You don't need to have any prior scripting experience. We will do PowerShell labs throughout the week, so today is not the only PowerShell content. Don't worry, you won't be left behind, the PowerShell labs will walk you through every step. Learning PowerShell is not only good for network security, it's also good for *job* security.

Topics: PowerShell Overview and Tips; What Can We Do With PowerShell?; Write Your Own Scripts

505.2 HANDS ON: Continuous Secure Configuration Enforcement

Running a vulnerability scanner is easy, but remediating vulnerabilities in a large enterprise is hard. Most vulnerabilities are fixed by applying patches, but this course does not talk about patch management, you're doing that already. What about the other vulnerabilities, the ones not fixed by applying patches? These vulnerabilities are, by definition, remediated by configuration changes. That's the hard part. We need a secure architecture designed for SecOps.

Topics: Continuous Secure Configuration Enforcement; Group Policy Precision Targeting; Server Hardening for SecOps/DevOps; PowerShell Desired State Configuration (DSC)

505.3 HANDS ON: Windows PKI and Smart Cards

Don't believe what you hear on the street: Public Key Infrastructure (PKI) is not that hard to manage on Windows! You'll be pleasantly surprised at how much Group Policy, Active Directory, and PowerShell can help you manage your PKI. We don't really have a choice anymore; having a PKI is pretty much mandatory for Microsoft security. The labs in this course mostly use graphical PKI tools, but there are also PowerShell labs to delete unwanted certificates installed by malware, audit our lists of trusted CAs, perform file hashing, compare thousands of recorded file hashes at two different times (similar to Tripwire), and encrypt secret data in our own PowerShell applications, such as for encrypting admin passwords.

Topics: Why Is A PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

505.4 HANDS ON: Administrative Compromise and Privilege Management

Is there a Windows version of *sudo*, like on Linux? Yes, it's called Just Enough Admin (JEA) for PowerShell. JEA allows non-admin users to remotely execute commands with administrative privileges, but without exposing any administrative credentials to them (kind of like setuid root on Linux). With JEA, all PowerShell commands are blocked by default except those you explicitly allow, and you can even use regular expression patterns to limit the arguments to those commands. And for less-technical users who'd prefer a graphical interface, don't forget that graphical applications can be built on top of PowerShell JEA too. In this course, we will see how to set up JEA and PowerShell Remoting.

Topics: You Don't Know The Power!; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

505.5 HANDS ON: Endpoint Protection and Pre-Forensics

Despite our best efforts, we must still assume breach. Pre-forensics describes what we should configure on Windows to prepare for a security incident. It's not about the response itself, it's about the preparations, such as enabling centralized logging. Preparation is half the battle. Pre-forensics also means gathering ongoing operational data to give to the Hunt Team and incident responders while they look for indicators of compromise. When the Hunt Team has a baseline of what is "normal" on a server to compare against, identifying what is new and out of place is vastly easier. PowerShell makes creating these scheduled baseline snapshots easy.

Topics: Anti-Exploitation; IPSec Port Permissions; Host-Based Firewalls; Pre-Forensics

505.6 HANDS ON: Defensible Networking and Blue Team WMI

Hackers love Windows Management Instrumentation (WMI), and so should we. We are the linebackers on the Blue Team and the WMI service was made to benefit us, not hackers. Beyond WMI, there are several other network services or protocols that we cannot live without, but which are targeted by hackers. To move laterally inside the LAN, hackers go after SSL/TLS, DNS, Kerberos, Remote Desktop Protocol (RDP), PowerShell Remoting, or the File and Print Sharing protocol (SMB/CIFS). We must assume there will be a breach, so we will learn how to harden, eliminate, or encrypt these protocols, and we will do it with little or no user disruption. We can't keep hackers and malware out entirely, but with PKI, IPSec encryption, and proper hardening, RDP can be made safe enough to use, even for administrators.

Topics: PowerShell and WMI; Hardening DNS; Dangerous Protocols We Can't Live Without

***SEC505** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
Virginia Beach ..... Virginia Beach, VA Aug 27 - Sep 1
NETWORK SECURITY .... Las Vegas, NV ..... Sep 10-15
San Francisco Winter ... San Francisco, CA Nov 27 - Dec 2
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online ..... Nov 27 - Dec 2

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online ..... Sep 18 - Nov 6

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

"Really great course for anyone involved in the administration or securing of Windows environments."
-David Hazar, Oracle

"I loved the course! When I return to the office, I am recommending it to the rest of my team."
-Alex Fox, Federal Home Loan Bank Chicago

SEC506

Securing Linux/Unix

GCUX Certification
UNIX Security Administrator

www.giac.org/gcux

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

You Will Be Able To

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

SEC506: Securing Linux/Unix provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix.

The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS's practical approach uses hand-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

Topics

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

Course Author Statement

A wise man once said, "How are you going to learn anything if you know everything already?" And yet there seems to be a quiet arrogance in the Unix community that we have figured out all of our security problems, as if to say, "Been there, done that." All I can say is that what keeps me going in the Unix field, and the security industry in particular, is that there is always something new to learn, discover, or invent. In 20 plus years on the job, what I have learned is how much more there is that I can learn. I think this is also true for the students in my courses. I regularly get comments back from students who say things like, "I have been using Unix for 20 years, and I still learned a lot in this class." That is really rewarding.

- Hal Pomeranz

"Best of any course I've ever taken. I love the idea of being able to bring the material home to review."

-Eric Koebelen, Incident Response US

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

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

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

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

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

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

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

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

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

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

506.4 HANDS ON: Application Security – PART 1

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

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

506.5 HANDS ON: Application Security – PART 2

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

Topics: BIND; DNSSec; Apache; Web Application Firewalls with mod_security

506.6 HANDS ON: Digital Forensics for Linux/Unix

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

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

***SEC506** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15

OnDemand

E-learning available anytime, anywhere, at your pace

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

"This course is painting a big picture of how various system tools can be used together to support security, and I like how the labs are continuing to build upon each other."

-Chris H., U.S. Naval Academy

SEC545

Cloud Security Architecture and Operations *NEW!*

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security monitoring analysts
- Cloud security architects
- DevOps and DevSecOps engineers
- System administrators
- Cloud administrators

You Will Be Able To

- Revise and build internal policies to ensure cloud security is properly addressed
- Understand all major facets of cloud risk, including threats, vulnerabilities, and impact
- Articulate the key security topics and risks associated with SaaS, PaaS, and IaaS cloud deployment models
- Evaluate Cloud Access Security Brokers (CASBs) to better protect and monitor SaaS deployments
- Build security for all layers of a hybrid cloud environment, starting with hypervisors and working to application layer controls
- Evaluate basic virtualization hypervisor security controls
- Design and implement network security access controls and monitoring capabilities in a public cloud environment
- Design a hybrid cloud network architecture that includes IPSec tunnels
- Integrate cloud identity and access management (IAM) into security architecture
- Evaluate and implement various cloud encryption types and formats
- Develop multi-tier cloud architectures in a Virtual Private Cloud (VPC), using subnets, availability zones, gateways, and NAT
- Integrate security into DevOps teams, effectively creating a DevSecOps team structure
- Build automated deployment workflows using AWS and native tools
- Incorporate vulnerability management, scanning, and penetration testing into cloud environments
- Build automated and flexible detection and response programs using tools like AWS-IR, CloudWatch, CloudTrail, and AWS Lambda
- Leverage the AWS CLI to automate and easily execute operational tasks
- Set up and use an enterprise automation platform, Ansible, to automate configuration and orchestration tasks
- Use CloudWatch, CloudFormation, and other automation tools to integrate automated security controls into your cloud security program

As more organizations move data and infrastructure to the cloud, security is becoming a major priority. Operations and development teams are finding new uses for cloud services, and executives are eager to save money and gain new capabilities and operational efficiency by using these services. But, will information security prove to be an Achilles' heel? Many cloud providers do not provide detailed control information about their internal environments, and quite a few common security controls used internally may not translate directly to the public cloud.

The SEC545 course, Cloud Security Architecture and Operations, will tackle these issues one by one. We'll start with a brief introduction to cloud security fundamentals, and then cover the critical concepts of cloud policy and governance for security professionals. For the rest of day one and all of day two, we'll move into technical security principles and controls for all major cloud types (SaaS, PaaS, and IaaS). We'll learn about the Cloud Security Alliance framework for cloud control areas, then delve into assessing risk for cloud services, looking specifically at technical areas that need to be addressed.

The course then moves into cloud architecture and security design, both for building new architectures and for adapting tried-and-true security tools and processes to the cloud. This will be a comprehensive discussion that encompasses network security (firewalls and network access controls, intrusion detection, and more), as well as all the other layers of the cloud security stack. We'll visit each layer and the components therein, including building secure instances, data security, identity and account security, and much more. We'll devote an entire day to adapting our offense and defense focal areas to cloud. This will involve looking at vulnerability management and pen testing, as well as covering the latest and greatest cloud security research. On the defense side, we'll delve into incident handling, forensics, event management, and application security.

We wrap up the course by taking a deep dive into SecDevOps and automation, investigating methods of embedding security into orchestration and every facet of the cloud life cycle. We'll explore tools and tactics that work, and even walk through several cutting-edge use cases where security can be automated entirely in both deployment and incident detection-and-response scenarios using APIs and scripting.

545.1 HANDS ON: Cloud Security Foundations

The first day of the class starts out with an introduction to the cloud, including terminology, taxonomy, and basic technical premises. We also examine what is happening in the cloud today, and cover the spectrum of guidance available from the Cloud Security Alliance, including the Cloud Controls Matrix, the 14 major themes of cloud security, and other research available. Next we spend time on cloud policy and planning, delving into the changes an organization needs to make for security and IT policy to properly embrace the cloud. After all the legwork is done, we'll start talking about some of the main technical considerations for the different cloud models. We'll start by breaking down Software-as-a-Service (SaaS) and some of the main types of security controls available. A specialized type of Security-as-a-Service (SecaaS) known as Cloud Access Security Brokers (CASBs) will also be explained, with examples of what to look for in such a service. We'll wrap up with an introduction to Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) controls, which will set the stage for the rest of the class.

Topics: **Introduction to the Cloud and Cloud Security Basics; Cloud Security Alliance Guidance; Cloud Policy and Planning; SaaS Security; Cloud Access Security Brokers (CASBs); Intro to PaaS and IaaS Security Controls**

545.2 HANDS ON: Core Security Controls for Cloud Computing

The second day of SEC545 compares traditional in-house controls with those in the cloud today. Some controls are similar and mostly compatible, but not all of them. Since most cloud environments are built on virtualization technology, we walk through a short virtualization security primer, which can help teams building hybrid clouds that integrate with internal virtualized assets, and also help teams properly evaluate the controls cloud providers offer in this area. We'll then break down cloud network security controls and tradeoffs, since this is an area that is very different from what we've traditionally run in-house. For PaaS and IaaS environments, it's critical to secure virtual machines (instances) and the images we deploy them from, so we cover this next. At a high level, we'll also touch on identity and access management for cloud environments to help control and monitor who is accessing the cloud infrastructure, as well as what they're doing there. We also cover data security controls and types, including encryption, tokenization, and more. Specific things to look for in application security are laid out as the final category of overall controls. We then pull it all together to demonstrate how you can properly evaluate a cloud provider's controls and security posture.

Topics: **Cloud Security: In-House versus Cloud; A Virtualization Security Primer; Cloud Network Security; Instance and Image Security; Identity and Access Management; Data Security for the Cloud; Application Security for the Cloud; Provider Security: Cloud Risk Assessment**

545.3 HANDS ON: Cloud Security Architecture and Design

Instead of focusing on individual layers of our cloud stack, we start day three by building the core security components. We'll break down cloud security architecture best practices and principles that most high-performing teams prioritize when building or adding cloud security controls and processes to their environments. We start with infrastructure and core component security - in other words, we need to look at properly locking down all the pieces and parts we covered on day two! This then leads to a focus on major areas of architecture and security design. The first is building various models of access control and compartmentalization. This involves breaking things down into two categories: identity and access management (IAM) and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider's DR and continuity, and so this is covered as well.

Topics: **Cloud Security Architecture Overview; Cloud Architecture and Security Principles; Infrastructure and Core Component Security; Access Controls and Compartmentalization; Confidentiality and Data Protection; Availability**

545.4 HANDS ON: Cloud Security – Offense and Defense

There are many threats to our cloud assets, so the fourth day of the course begins with an in-depth breakdown of the types of threats out there. We'll look at numerous examples. The class also shows students how to design a proper threat model focused on the cloud by using several well-known methods such as STRIDE and attack trees and libraries. Scanning and pen testing the cloud used to be challenging due to restrictions put in place by the cloud providers themselves. But today it is easier than ever. There are some important points to consider when planning a vulnerability management strategy in the cloud, and this class touches on how to best scan your cloud assets and which tools are available to get the job done. Pen testing naturally follows this discussion, and we talk about how to work with the cloud providers to coordinate tests, as well as how to perform testing yourself. On the defensive side, we start with network-based and host-based intrusion detection, and how to monitor and automate our processes to better carry out this detection. This is an area that has definitely changed from what we're used to in-house, so security professionals need to know what their best options are and how to get this done. Our final topics on day four include incident response and forensics (also topics that have changed significantly in the cloud). The tools and processes are different, so we need to focus on automation and event-driven defenses more than ever.

Topics: **Threats to Cloud Computing; Vulnerability Management in the Cloud; Cloud Pen Testing; Intrusion Detection in the Cloud; Cloud IR and Event Management; Cloud Forensics**

545.5 HANDS ON: Cloud Security Automation and Orchestration

On our final day, we'll focus explicitly on how to automate security in the cloud, both with and without scripting techniques. We will use tools like the AWS CLI and AWS Lambda to illustrate the premises of automation, then turn our attention toward SecDevOps principles. We begin by explaining what that really means, and how security teams can best integrate into DevOps and cloud development and deployment practices. We'll cover automation and orchestration tools like Ansible and Chef, as well as how we can develop better and more efficient workflows with AWS CloudFormation and other tools. Continuing some of the topics from day four, we will look at event-driven detection and event management, as well as response and defense strategies that work. While we won't automate everything, some actions and scenarios really lend themselves to monitoring tools like CloudWatch, tagging assets for identification in security processes, and initiating automated response and remediation to varying degrees. We wrap up the class with a few more tools and tactics, followed by a sampling of real-world use cases.

Topics: **Scripting and Automation in the Cloud; SecDevOps Principles; Creating Secure Cloud Workflows; Building Automated Event Management; Building Automated Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up**

***SEC555** is available via (subject to change):*

Featured Training Events

San Francisco Fall . . . . . San Francisco, CA . . . . . Sep 5-9

SEC555

SIEM with Tactical Analytics *NEW!*

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- SOC analysts
- SOC engineers
- SOC managers
- CND analysts
- Security monitoring specialists
- System administrators
- Cyber threat investigators
- Individuals working to implement Continuous Security Monitoring
- Individuals working in a hunt team capacity

Author Statement

"Today, security operations do not suffer from a 'big data' problem but rather a 'data analysis' problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs and it is easy to get lost in the perils of data saturation. This class is the switch from the typical churn and burn log systems to achieving actionable intelligence and developing a tactical Security Operations Center (SOC)."
-Justin Henderson

Many organizations have logging capabilities but lack the people and processes to analyze it. In addition, logging systems collect vast amounts of data from a variety of data sources that require an understanding of the sources for proper analysis. This class is designed to provide individuals training, methods, and processes for enhancing existing logging solutions. This class will also help you understand the when, what, and why behind the logs. This is a lab-heavy course that utilizes SOF-ELK, a SANS-sponsored free Security Incident and Events Management (SIEM) solution, to provide hands-on experience and the mindset for large-scale data analysis.

Today, security operations do not suffer from a "big data" problem but rather a "data analysis" problem. Let's face it, there are multiple ways to store and process large amounts of data without any real emphasis on gaining insight into the information collected. Added to that is the daunting idea of an infinite list of systems from which one could collect logs. It is easy to get lost in the perils of data saturation. This class moves away from the typical churn-and-burn log systems and moves instead towards achieving actionable intelligence and developing a tactical Security Operations Center (SOC).

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the "appropriate" use of a SEIM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyze key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students may employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualizations.

555.1 HANDS ON: SIEM Architecture and SOF-ELK

Logging and analysis is a critical component in cyber network defense and allows for both reactive and proactive detection of adversarial activities. When properly utilized it becomes the backbone for agile detection and provides understanding to the overall environment. Logging and analysis products and techniques have been around for many years and are quickly gaining more and more functionality. This section will introduce free logging and analysis tools and focus on techniques to make sense of and augment traditional logs. It also covers how to handle the big data problem of handling billions of logs and how advances in free tools are starting to give commercial solutions a run for their money. Day one is designed to bring all students up to speed on SIEM concepts and to bring all students to a base level to carry them through the rest of the class. It is designed to also cover SIEM best practices. During day one we will be introducing Elasticsearch, Logstash, and Kibana within SOF-ELK and immediately go into labs to get students comfortable with ingesting, manipulating, and reporting on log data.

Topics: **State of the SOC/SIEM; Log Monitoring; Logging Architecture; SIEM Platforms; Planning a SIEM; SIEM Architecture; Ingestion Techniques and Nodes; Data Queuing and Resiliency; Storage and Speed; Analytical Reporting**

555.2 HANDS ON: Service Profiling with SIEM

A vast majority of network communication occurs over key network protocols, yet it is uncommon for organizations to use or collect this data. The sheer volume can be overwhelming. However, these common data sources provide an opportunity in identifying modern day attacks. This section covers how to collect and handle this massive amount of data. Methods for collecting these logs through service logs such as from DNS servers will be covered as well as passive ways of pulling the same data from the network itself. Techniques will be demonstrated to augment and add valuable context to the data as it is collected. Finally, analytical principles will be covered for finding the needles in the stack of needles. We will cover how, even if we have the problem of searching through billions of logs, we can surface only meaningful items of interest. Active dashboards will be designed to quickly find the logs of interest and to provide analysts with additional context for what to do next.

Topics: **Detection Methods and Relevance to Log Analysis; Analyzing Common Application Logs that Generate Tremendous Amounts of Data; Apply Threat Intelligence to Generic Network Logs; Active Dashboards and Visualizations**

555.3 HANDS ON: Advanced Endpoint Analytics

The value in endpoint logs provides tremendous visibility in detecting attacks. Especially, in with regard to finding post-compromise activity, endpoint logs can quickly become second to none. However, logs even on a single desktop can range in the tens if not hundreds of thousands of events per day. Multiply this by the number of systems in your environment and it is no surprise why organizations get overwhelmed. This section will cover the how and more importantly the why behind collecting system logs. Various collection strategies and tools will be used to gain hands-on experience and to provide simplification with handling and filtering the seemingly infinite amount of data generated by both servers and workstations. Workstation log strategies will be covered in depth due to their value in today's modern attack vectors. After all, modern-day attacks typically start and then spread from workstations.

Topics: **Endpoint Logs**

555.4 HANDS ON: Baselining and User Behavior Monitoring

Know thyself is often quoted to defenders as a key defense strategy, and yet this is one of the most difficult things to accomplish. Take something such as having a list of all assets in an organization and knowing if any non-company assets are on the network. The task sounds simple but ends up being incredibly difficult to maintain in today's ever-evolving networks. This section focuses on applying techniques to automatically maintain a list of assets and their configurations as well as methods to distinguish if they are authorized or unauthorized. Key locations to provide high-fidelity data will be covered and techniques to correlate and combine multiple sources of data together will be demonstrated to build a master inventory list. Other forms of knowing thyself will be introduced such as gaining hands-on experience in applying network and system baselining techniques. We will monitor network flows and identify abnormal activity such as C2 beaconing as well as look for unusual user activity. Finally, we will apply large data analysis techniques to sift through massive amounts of endpoint data. This will be used to find things such as unwanted persistence mechanisms, dual-homed devices, and more.

Topics: **Identify Authorized and Unauthorized Assets; Identify Authorized and Unauthorized Software; Baseline Data**

555.5 HANDS ON: Tactical SIEM Detection and Post-Mortem Analysis

Multiple security devices exist but often are designed to be independent. Analysts are commonly divided into specialty areas and focus on their respective area such as a network intrusion detection system. However, alerts from a single security device lack context and are akin to the common analogy of "looking up from the bottom of a well." This section focuses on combining multiple security logs for central analysis. More importantly, we will cover methods for combining multiple sources to provide improved context to analysts. We will also show how providing context with asset data can help prioritize analyst time, saving money and addressing risks that matter. After covering ways to optimize traditional security alerts, we will jump into new methods to utilize logging technology to implement virtual tripwires. While it would be ideal to prevent attackers from gaining access to your network, it is a given that at some point you will be compromised. However, compromise is just the beginning and not the end goal. Adversaries will crawl your systems and network to achieve their own ends. Knowing this, we will implement logging-based tripwires—and if a single one is stepped on, we can quickly detect it and respond to the adversary.

Topics: **Centralize NIDS and HIDS Alerts; Analyze Endpoint Security Logs; Augment Intrusion Detection Alerts; Analyze Vulnerability Information; Correlate Malware Sandbox Logs with Other Systems to Identify Victims Across Enterprise; Monitor Firewall Activity; SIEM Tripwires; Post Mortem Analysis**

555.6 HANDS ON: Capstone: Design, Detect, Defend

The course culminates in a team-based design, detect, and defend the flag competition. Powered by NetWars, day six provides a full day of hands-on work applying the principles taught throughout the week. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cyber defense techniques promoted all week long. From building a logging architecture to augmenting logs, analyzing network logs, analyzing system logs, and developing dashboards to find attacks, this challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

Topics: **Defend-the-Flag Challenge – Hands-on Experience**

SEC555 *is available via (subject to change):*

Featured Training Events

Virginia Beach . . . . . Virginia Beach, VA . . . Aug 21-26
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15
San Diego . . . . . San Diego, CA . . . Oct 30 - Nov 4

Private Training

All SANS courses are available through Private Training.

SEC579

Virtualization and Software-Defined Security *NEW!*

Five-Day Program
30 CPEs
Laptop Required

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

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 converged and software-defined 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

"SEC579 was one of the best-produced SANS courses I have taken. The blend of ops and security was extremely valuable."

-Scott Towery, Visions

One of today's most rapidly evolving and widely deployed technologies is server virtualization. **SEC579: Virtualization and Software-Defined Security** is intended to help security, IT operations, and audit and compliance professionals build, defend, and properly assess both virtual and converged infrastructures, as well as understand software-defined networking and infrastructure security risks.

Many organizations are already realizing cost savings from implementing virtualized servers, and systems administrators love the ease of deployment and management of virtualized systems. More and more organizations are deploying desktop, application, and network virtualization as well. 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 infrastructure.

With these benefits comes a dark side, however. Virtualization technology is the focus of many new potential threats and exploits, and it presents new vulnerabilities that must be managed. There are also 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 using converged infrastructure that employs software-defined tools and programmable stack layers to control large, complex data centers. Security architecture, policies, and processes will need to be adapted to work within a converged infrastructure, and there are many changes that security and operations teams will need to accommodate to ensure that assets are protected.

This course will cover core operational functions like secure network design and segmentation, building secure systems, and secure virtualization implementation and controls. Cutting-edge topics like software-defined networking and container technology will also be covered in detail with an emphasis on security techniques and controls. Security-focused virtualization, integration, and monitoring will be covered at length. Attacks and threats to virtual environments will be discussed, and students will learn how to perform vulnerability assessments and penetration tests in their virtual environments. We'll also look at how to implement network intrusion detection and access controls, implement log and event management, and perform forensics and incident handling in virtual and converged data centers. Finally, students will learn how to perform technical audits and assessments of their in-house and public cloud environments, creating reports and documenting technical controls. This instruction will heavily emphasize automation and scripting techniques.

579.1 HANDS ON: Core Concepts of Virtualization Security

The first day of class will cover the foundations of virtualization infrastructure and different types of technology. We will define and clarify the differences between server, desktop, application, and storage virtualization, and dissect the various virtualization elements that make up the architecture one by one, with a focus on the security configurations that will help you create or revise your virtualization design to be as secure as possible.

Topics: **Virtualization Components and Architecture Designs; Different Types of Virtualization, Ranging from Desktops to Servers and Applications; Hypervisor Lockdown Controls for VMware, Microsoft Hyper-V, and Citrix Xen; Virtual Machine Security Configuration Options, with a Focus on VMware VMX Files; Storage Security and Design Considerations; Locking Down Management Servers and Clients for vCenter, XenServer, and Microsoft SCVMM; Security Design Considerations for VDI**

579.2 HANDS ON: Virtualization and Software-Defined Security Architecture and Design

Day 2 starts with several topics that round out our discussions on virtualization and infrastructure components, delving into container technology and converged infrastructure platforms and tools (along with security considerations for both). We'll then begin our discussion of virtualization and software-defined architecture and networking. We'll cover design concepts and models, network capabilities and models in virtual environments, with time devoted to virtual switches and other platforms, and look at how network security adapts to fit into a virtual infrastructure.

Topics: **Container Technology Security Considerations; Converged Infrastructure Security Considerations; Defining "Software Defined" Components and Architectural Models; Designing Security for Software-Defined Environments; Virtual Network Design Cases with Pros and Cons of Each; Virtual Switches and Port Groups, with Security Options Available; Commercial and Open-Source Virtual Switches Available, with Configuration Options; Segmentation Techniques, Including VLANs and PVLANs; Software-Defined Networking and Architecture; Network Isolation and Access Control; Adapting Firewalls, IPS, Proxies, and More to Virtual Environments; Products and Capabilities Available Today**

***SEC579** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-28

NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 11-15

Private Training

All SANS courses are available through Private Training.

"This is the future of IT and security. Knowledge is power!"

-Joe Marshall, Exelon

579.3 HANDS ON: Virtualization Threats, Vulnerabilities, and Attacks

This session will delve into the offensive side of security specific to virtualization and cloud technologies. We will first examine a number of specific attack scenarios, then we will go through the entire penetration testing and vulnerability assessment lifecycle, with an emphasis on virtualization tools and technologies. We'll progress through scanners and how to use them to assess virtual systems, then turn to virtualization exploits and attack toolkits that can be easily added into existing penetration test regimens. We will also cover some specific techniques that may help in cloud environments, providing examples of scenarios where certain tools and exploits are less effective or more risky to use than others.

Topics: **Threats and Attack Research Related to Virtualization Infrastructure; Attack Models That Pertain to Virtualization and Cloud Environments; Threat Modeling for Virtualization and Software-Defined Technology; Specific Virtualization Platform Attacks and Exploits; Pen Testing Cycles with a Focus on Virtualization Attack Types; Password Attacks Against Virtualization and Software-Defined Platforms; How to Modify Vulnerability Management Processes and Scanning Configuration to Get the Best Results in Virtualized Environments; How to Use Attack Frameworks Like VASTO to Exploit Virtualization Systems**

579.4 HANDS ON: Defending Virtualization and Software-Defined Technologies

We will start off with an analysis of anti-malware techniques, looking at traditional antivirus, whitelisting, and other tools and techniques to combat malware, with a specific eye toward virtualization and converged environments. Then we will turn to intrusion detection, monitoring traffic and learning about logs and log management in virtual environments. The second half of this session will focus on incident response and forensics in a virtualized or converged infrastructure and how students can adapt forensics processes and tools to work in virtual environments.

Topics: **Data Protection in Virtual and Converged Environments; Identity and Access Management in Virtual and Software-Defined Environments; How to Implement Intrusion Detection Tools and Processes in a Virtual Environment; What Kinds of Logs and Logging are Most Critical for Identifying Attacks and Live Incidents in Virtual Environments?; How Anti-Malware Tools Function in Virtual Environments; How the Six-Step Incident Response Process Can be Modified and Adapted to Work with Virtual Infrastructure; What Kinds of Incidents to Look for Within Virtual Environments, and What the Warning Signs Are; Processes and Procedures to Build and Grow Incident Response Capabilities for Virtual Environments; How Forensics Processes and Tools Should Be Used and Adapted for Virtual Systems; What Tools Are Best to Get the Most Accurate Results From Virtual Machine System Analysis?; How to Most Effectively Capture Virtual Machines for Forensic Evidence Analysis; What Can Be Done to Analyze Hypervisor Platforms, and What Does the Future Hold for VM Forensics?**

579.5 HANDS ON: Virtualization Operations, Auditing, and Monitoring

Today's session will start off with a lively discussion on virtualization assessment and auditing. We will cover the top virtualization configuration and hardening guides from DISA, CIS, Microsoft, and VMware, and talk about the most critical information to take away from these guides and implement. Students will learn to implement audit and assessment techniques by scripting with the VI CLI, as well as some general shell scripting! We will look at automation and orchestration tools and techniques that can help to streamline and manage configuration and auditing (examples include Chef, Puppet, and more), as well as monitoring techniques that provide a feedback loop.

Topics: **Key Configuration Controls from the Leading DISA, CIS, VMware, and Microsoft Hardening Guides; Sound Configuration Management and Patching in Virtual Infrastructure; Scripting Techniques in VI CLI and PowerShell for Automating Audit and Assessment Processes; Sample Scripts That Help Implement Key Audit Functions; Automation and Orchestration with Puppet, Chef, ManageEngine, etc.; Full Hardening-Guide-Scripted Audit**

Employers need good talent. Veterans need good jobs. SANS VetSuccess Immersion Academy delivers both.

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

For employers, the academy is a faster, more reliable, and less expensive way to find, train, certify, and employ highly qualified cybersecurity talent.

For transitioning veterans, the academy provides free accelerated training and certifications to quickly and effectively launch careers in cybersecurity.

Find out how your organization can benefit from hiring graduates or launching an academy to meet your specific talent needs.

sans.org/cybertalent/immersion-academy
Email: immersionacademy@sans.org

SANS CyberTalent IMMERSION ACADEMY

Read the Pilot Program Results Report
Visit sans.org/vetsuccess

Women's Academy Pilot
1st cohort graduation Summer 2016

VetSuccess

Focus Job Roles and Specialized Skills

Penetration Testing & Vulnerability Analysis

Penetration Testing & Vulnerability Analysis

SEC560 Network Penetration Testing and Ethical Hacking	**GPEN** Certification Penetration Tester
SEC542 Web App Penetration Testing and Ethical Hacking	**GWAPT** Certification Web Application Penetration Tester

Summary: High-performing security organizations need specially trained professionals who can continuously challenge the defenses and monitoring systems set up by the cyber defense operating teams and discover vulnerabilities to be addressed that might otherwise be exploited by attackers. Professionals focusing on this career path must be able to test both network and wireless vulnerabilities and understand these environments before advancing to additional areas.

SEC560 and **SEC542** teach you the skills that are core to this type of role. An additional nine SANS penetration testing courses, in advanced and specialized topics, allow you to mold your career into a particular practice area or task. Review the following pages for detailed information about all of these courses and the certifications that validate your acquired skills.

Who This Path is For: Information Security Engineers, Analysts, and Risk Consultants master this coursework in particular to hone their penetration testing, ethical hacker, and vulnerability analysis skills.

Why This Training is Important: These courses teach proper planning, scoping, and recon, while diving deep into scanning, target exploitation, password attacks, web app configuration, identity, authentication, custom scripting, and interception proxies. Together with dozens of detailed, hands-on labs, this training allows you to go back to work with the practical, real-world examples and practice needed to do your job efficiently and masterfully.

"I was pleasantly humbled, challenged, encouraged and trained. I feel 100% more qualified to defend my company's network after taking this training."

-Ivan Dominguez, NWCU.com

SEC560

GPEN Certification
Penetration Tester

www.giac.org/gpen

Network Penetration Testing and Ethical Hacking

Six-Day Program
37 CPEs
Laptop Required
This course has extended hours

Who Should Attend

- Security personnel whose job involves assessing networks and systems to find and remediate vulnerabilities
- Penetration testers
- Ethical hackers
- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Red and blue team members
- Forensics specialists who want to better understand offensive tactics

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 safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy
- Utilize the Windows PowerShell and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further 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
- Launch web application vulnerability scanners and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection to understand the business risk faced by an organization

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.

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

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

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

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

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

SANS Technology Institute
www.sans.edu

www.sans.org/cyber-guardian

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

In this section of the course, you will develop the skills needed to conduct a best-of-breed, high-value penetration test. We will go in-depth on how to build penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We will then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll 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, as well as a lab using Recon-ng to plunder a target's DNS infrastructure for information such as the anti-virus tools the organization relies on.

Topics: **The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Effective Pen Test Reporting to Maximize Impact; 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 target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We will 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 will 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. And we will examine the best ways to conduct your scans safely and efficiently.

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

560.3 HANDS ON: 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. We'll also analyze the topic of anti-virus evasion to bypass the target organization's security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

Topics: **Comprehensive Metasploit Coverage with Exploits/Stagers/Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage Shell Access of a Target Environment**

560.4 HANDS ON: Post-Exploitation and Merciless Pivoting

Once you've successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This section of the course zooms in on pillaging target environments and building formidable hands-on command line skills. We'll cover Windows command line skills in-depth, including PowerShell's awesome abilities for post-exploitation. We'll see how we can leverage malicious services and the incredible WMIC toolset to access and pivot through a target organization. We'll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we'll look at Metasploit's fantastic features for pivoting, including the msfconsole route command.

Topics: **Windows Command Line Kung Fu for Penetration Testers; PowerShell's Amazing Post-Exploitation Capabilities; 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; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi**

560.5 HANDS ON: In-Depth Password Attacks and Web App Pen Testing

In this section of the course, we'll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You'll 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. We'll see how Rainbow Tables really work to make password cracking much more efficient, all hands-on. And we'll cover powerful "pass-the-hash" attacks, leveraging Metasploit, the Meterpreter, and more. We then turn our attention to web application pen testing, covering the most powerful and common web app attack techniques with hands-on labs for every topic we address. We'll cover 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: **Password Cracking with John the Ripper; Sniffing and Cracking Windows Authentication Exchanges Using Cain; Using Rainbow Tables to Maximum Effectiveness; Pass-the-Hash Attacks with Metasploit and More; 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 Test and Capture-the-Flag Workshop

This lively session represents the culmination of the network penetration testing and ethical hacking course. You'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop during which 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. 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; Merciless Pivoting; Analyzing Results**

***SEC560** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
San Antonio	San Antonio, TX	Aug 6-11
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Virginia Beach	Virginia Beach, VA	Aug 21-26
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

Summit Events

Pen Test Hackfest – Bethesda, MD . . . . . Nov 15-20

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online . . . . . Aug 21-26

Virtual/Online . . . . . Dec 14-19

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online . . . . . Nov 13 - Dec 20

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Columbia, MD . . . . . Jul 17-22

Columbus, OH . . . . . Jul 17-22

Columbia, MD . . . . . Sep 11-16

New York, NY . . . . . Dec 11-16

Mentor Classes

Augusta, GA. . . . . Jul 12 - Aug 23

Dallas, TX . . . . . Sep 13 - Nov 15

Private Training

All SANS courses are available through Private Training.

SEC542

GWAPT Certification
Web Application Penetration Tester

www.giac.org/gwapt

Web App Penetration Testing and Ethical Hacking

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture the Flag exercise to bring techniques and tools together into a comprehensive test

Web applications play a vital role in every modern organization. However, if your organization doesn't properly test and secure its web apps, adversaries can 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 scanning to professional, thorough, and high-value web application penetration testing.

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 business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, and major industry studies find 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 effective web application penetration testing requires something deeper.

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

In this course, students will come to understand major web application flaws and their exploitation. Most importantly, they'll 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. This course will help you demonstrate the true impact of web application flaws through exploitation.

In addition to high-quality course content, SEC542 focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn.

In addition to having more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned.

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

542.1 HANDS ON: Introduction and Information Gathering

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; Heartbleed Exploitation; Utilizing the Burp Suite in Web App Penetration Testing

542.2 HANDS ON: Configuration, Identity, and Authentication Testing

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. The discussion is underscored through several practical, hands-on labs in which we conduct reconnaissance against in-class targets.

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; Learning Tools to Spider a Website; Scripting to Automate Web Requests and Spidering; Brute Forcing Unlinked Files and Directories; Discovering and Exploiting Shellshock

542.3 HANDS ON: Injection

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: Python for Web App Penetration Testing; Web App Vulnerabilities and Manual Verification Techniques; Interception Proxies; Zed Attack Proxy (ZAP); Burp Suite; Information Leakage, and Directory Browsing; Username Harvesting; Command Injection; Directory Traversal; SQL Injection; Blind SQL Injection; Local File Inclusion (LFI); Remote-File Inclusion (RFI); JavaScript for the Attacker

542.4 HANDS ON: JavaScript and XSS

On day four, students continue exploring the discovery phase of the methodology. We cover methods to discover key vulnerabilities within web applications, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF/XSRF). Manual discovery methods are employed during hands-on labs.

Topics: Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Session Flaws; Session Fixation; AJAX; Logic Attacks; Data Binding Attacks; Automated Web Application Scanners; w3af; XML and JSON

542.5 HANDS ON: CSRF, Logic Flaws, and Advanced Tools

On the fifth day, we 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 specifically focus on ways to leverage previously discovered vulnerabilities to gain further access, highlighting the cyclical nature of the four-step attack methodology.

Topics: Metasploit for Web Penetration Testers; The sqlmap Tool; Exploring Methods to Zombify Browsers; Browser Exploitation Framework (BeEF); Walking Through an Entire Attack Scenario; 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, students form teams and compete in a web application penetration testing tournament. This NetWars-powered Capture-the-Flag exercise provides students an opportunity to wield their newly developed or further-honed skills to answer questions, complete missions, and exfiltrate data, applying skills gained throughout the course. The style of challenge and integrated-hint system allows students of various skill levels to both enjoy a game environment and solidify the skills learned in class.

***SEC542** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
Boston ..... Boston, MA ..... Aug 7-12
Virginia Beach ..... Virginia Beach, VA Aug 27 - Sep 1
NETWORK SECURITY ..... Las Vegas, NV ..... Sep 10-15
Tysons Corner Fall ..... McLean, VA ..... Oct 16-21
San Francisco Winter ..... San Francisco, CA Nov 27 - Dec 2
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online ..... Dec 14-19

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

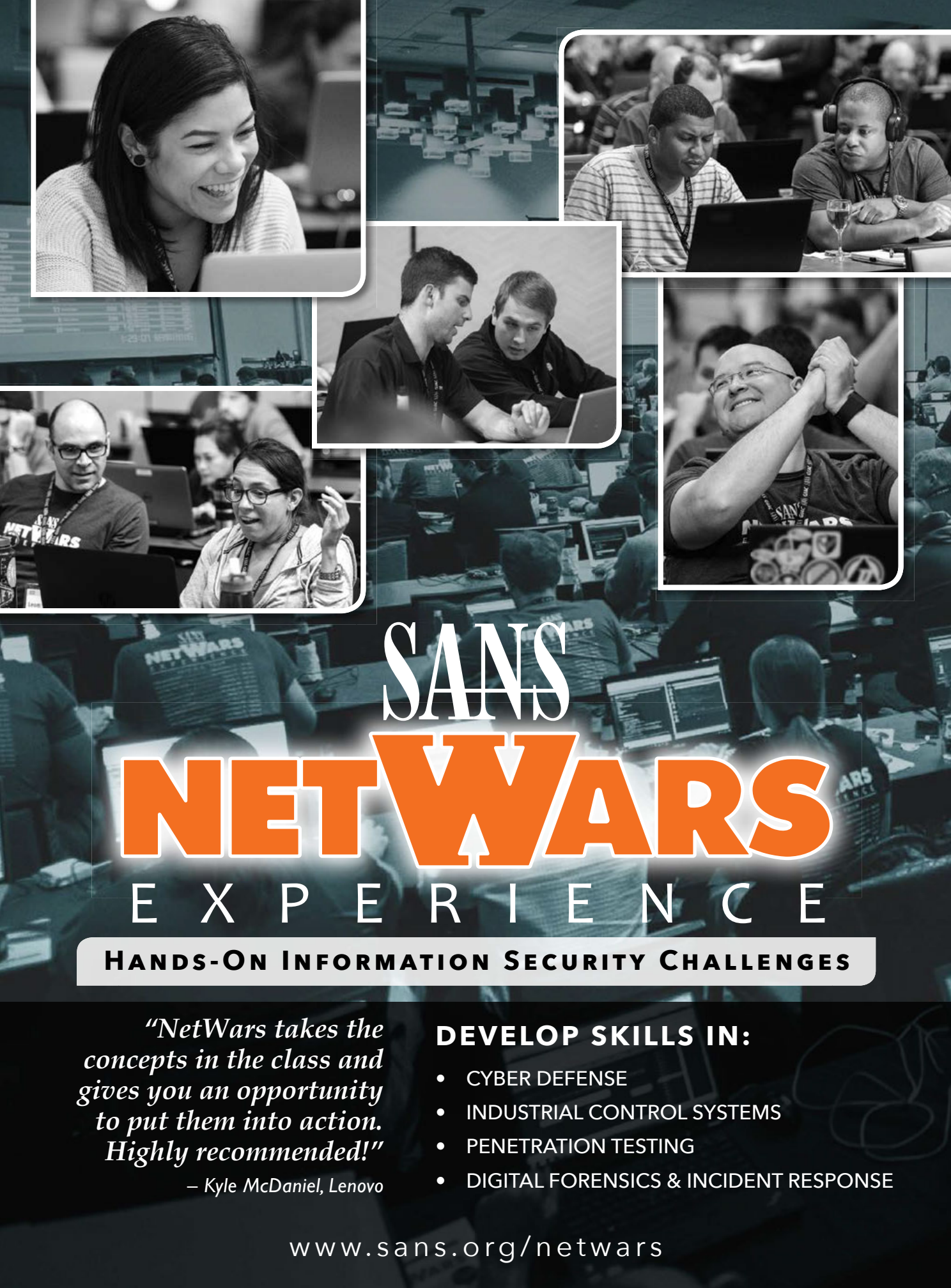
Detroit, MI ..... Aug 7-12
Tampa, FL ..... Nov 13-18

Private Training

All SANS courses are available through Private Training.

"SEC542 is a step-by-step introduction to testing and penetrating web applications – a must for anyone who builds, maintains, or audits web systems."
-Brad Milhorn, i2P LLC

"As a web application developer this course gives great insight into what I can do better."
-Joshua Barone, Geocent



SANS NETWARS EXPERIENCE

HANDS-ON INFORMATION SECURITY CHALLENGES

"NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!"

– Kyle McDaniel, Lenovo

DEVELOP SKILLS IN:

- CYBER DEFENSE
- INDUSTRIAL CONTROL SYSTEMS
- PENETRATION TESTING
- DIGITAL FORENSICS & INCIDENT RESPONSE

www.sans.org/netwars

SEC550

Active Defense, Offensive Countermeasures, and Cyber Deception

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

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

You Will Be Able To

- Track bad guys with callback Word documents
- Use Honeybadger to track web attackers
- Block attackers from successfully attacking servers with honeyports
- Block web attackers from automatically discovering pages and input fields
- Understand the legal limits and restrictions of Active Defense
- Obfuscate DNS entries
- Create non-attributable Active Defense Servers
- Combine geolocation with existing Java applications
- Create online social media profiles for cyber deception
- Easily create and deploy honeypots

***SEC550** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-28
NETWORK SECURITY .... Las Vegas, NV ..... Sep 11-15
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-18

Private Training

All SANS courses are available through Private Training.

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. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Learn:

- **How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker**
- **How to gain better attribution as to who is attacking you and why**
- **How to gain access to a bad guy's system**
- **Most importantly, you will find out how to do the above legally**

What You Will Receive

- **A fully functioning Active Defense Harbinger Distribution ready to deploy**
- **Class books and a DVD with the necessary tools and the OCM virtual machine, which is a fully functional Linux system with the OCM tools installed and ready to go for the class and for the students' work environments**

Course Day Descriptions

550.1 HANDS ON: Setup and Baseline

Topics: **Setup; Mourning Our Destiny, Leaving Youth and Childhood Behind; Bad Guy Defenses; Basics and Fundamentals (Or, Don't Get Owned Doing This); Playing With Advanced Backdoors; Software Restriction Policies; Legal Issues; Venom and Poison**

550.2 HANDS ON: Annoyance

Topics: **How to Connect to Evil Servers (Without Getting Shot); Remux.py; Recon on Bad Servers and Bad People; Honeypots; Honeyports; Kippo; Deny Hosts; Artillery; More Evil Web Servers; Cryptolocked**

542.3 HANDS ON: Attribution

Topics: **Dealing with TOR; Decloak; Word Web Bugs (Or Honeydocs); More Evil Web Servers; Cryptolocked**

550.4 HANDS ON: More Attribution and Attack

Topics: **Nova; Infinitely Recursive Windows Directories; Web Application Street Fighting with BeEF!; Wireless and Brotherly Love; Evil Java Applications with SET; AV Bypass (for the Good Guys!); Arming Word Documents; Python Injection; Ghostwriting; HoneyBadger; Let's Try to Trojan Some Java Applications**

550.5 HANDS ON: Capture the Flag

The Capture-the-Flag challenge draws on what you have learned over the previous four days of the course.

SEC561

Immersive Hands-on Hacking Techniques

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

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

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: Immersive Hands-On Hacking Techniques** 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 during in-class labs and making this SANS's 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.

"This training changed my perspective of IT and taught me how to think outside of the box."
-Timothy McKenzie, DELL/Secureworks

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.

Topics addressed in the course include:

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

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

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. Students will participate in a larger version of the exercises presented in the class to independently reinforce skills learned throughout the course. They will then 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.

***SEC561** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29

NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15

Private Training

All SANS courses are available through Private Training.

Course Author Statement

In creating this course, we focused on getting as much practical, hands-on skill building into the classroom as possible. Each day begins with a short briefing on the technical topics students will work on throughout the day. Then, students build their skills analyzing real-world target systems in the classroom. When students walk out of the class, they will have mastered over 100 new techniques for finding, exploiting and then fixing security flaws. Just as aircraft pilots need more 'stick' time learning how to fly, this course provides penetration testers and other security professionals with the real-world experience they need to excel in their work. - Josh Wright

"The course really forces you to think and the format rewards your hard work and dedication to finding the solutions."

-Michael Nutbrown, Solers, Inc

SEC573

GPYC Certification
Python Coder

www.giac.org/gpyc

Automating Information Security with Python *NEW!*

Six-Day Program
36 CPEs
Laptop Required

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

You Will Be Able To

- Develop forensics tool to carve artifacts from forensics evidence for which no other tool exists or use third-party modules for well-known artifacts to hidden evidence relevant to your investigations
- Create defensive tools to automate the analysis of log file and network packets using hunt team techniques to track down attackers in your network. Implement custom whitelisting, blacklisting, signature detection, long tail and short tail analysis, and other data analysis techniques to find attacks overlooked by conventional methods.
- Write penetration testing tools including several backdoors with features like process execution, upload and download payloads, port scanning and more. Build essential tools that evade antivirus software and allow you to establish that required foothold inside your target.
- Understand Python coding fundamentals required to automate common information security tasks. Language essentials like variables, loops, if then else, logic, file operations, command line arguments, debugging are all covered assuming no prerequisite knowledge.
- Tap into the wealth of existing Python modules to complete tasks using Regular Expressions, Database interactions with SQL, IP Networking, Exception handling, Interact with websites using Requests, Packet Analysis, Packet reassembly techniques and much more.

SANS Technology Institute

www.sans.edu

All security professionals, including Penetration Testers, Forensics Analysts, Network Defenders, Security Administrators, and Incident Responders, have one thing in common: CHANGE. Change is constant. Technology, threats, and tools are constantly evolving. If we don't evolve with them, we'll become ineffective and irrelevant, unable to provide the vital defenses our organizations increasingly require.

Maybe your chosen Operating System has a new feature that creates interesting forensics artifacts that would be invaluable for your investigation, if only you had a tool to access it. Often for new features and forensics artifacts, no such tool has yet been released. You could try moving your case forward without that evidence or hope that someone creates a tool before the case goes cold... or you can write a tool yourself.

Or, perhaps an attacker bypassed your defenses and owned your network months ago. If existing tools were able to find the attack, you wouldn't be in this situation. You are bleeding sensitive data and the time-consuming manual process of finding and eradicating the attacker is costing you money and hurting your organization big time. The answer is simple if you have the skills: Write a tool to automate your defenses.

Or, as a Penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when "off-the-shelf" tools and exploits fall short? If you're good, you write your own tool.

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, **SEC573: Automating Information Security with Python** will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object-oriented coding and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today's information security professional, and achieving more value in less time. 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. Join us and learn Python in-depth and fully weaponized.

573.1 HANDS ON: Essentials Workshop with pyWars

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

Topics: Python Syntax; Variables; Math Operators; Strings; Functions; Modules; Control Statements; Introspection

573.2 HANDS ON: Essentials Workshop with MORE pyWars

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 covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and how to debug your code.

Topics: Lists; Loops; Tuples; Dictionaries; The Python Debugger; Coding Tips, Tricks, and Shortcuts; System Arguments; ArgParser Module

573.3 HANDS ON: Defensive Python

Day three includes in-depth coverage about how defenders can use Python automation as we cover Python modules and techniques that everyone can use. Forensicators and offensive security professionals will also learn essential skills they will apply to their craft. We will play the role of a network defender who needs to find the attackers on their network. We will discuss how to analyze network logs and packets to discover where the attackers are coming from and what they are doing. We will build scripts to empower continuous monitoring and disrupt the attackers before they exfiltrate your data.

Topics: File Operations; Python Sets; Regular Expressions; Log Parsing; Data Analysis tools and techniques; Long Tail/Short Tail Analysis; Geolocation Acquisition; Blacklists and Whitelists; Packet Analysis; Packet Reassembly; Payload Extraction

573.4 HANDS ON: Forensics Python

On day four we will play the role of a forensics analyst who has to carve evidence from artifacts when no tool exists to do so. Even if you don't do forensics you will find that these skills covered on day four are foundational to every security role. We will discuss the process required to carve binary images, find appropriate data of interest in them, and extract that data. Once you have the artifact isolated, there is more analysis to be done. You will learn how to extract metadata from image files. Then we will discuss techniques for finding artifacts in other locations such as SQL databases and interacting with web pages.

Topics: Acquiring Images from Disk, Memory, and the Network; File Carving; The STRUCT Module; Raw Network Sockets and Protocols; Image Forensics and PIL; SQL Queries; HTTP Communications with Python Built-In Libraries; Web Communications with the Requests Module

573.5 HANDS ON: Offensive Python

On day five we play the role of penetration testers whose normal tricks have failed. Their attempts to establish a foothold have been stopped by modern defenses. To bypass these defenses, you will build an agent to give you access to a remote system. Similar agents can be used for Incident response or systems administration, but our focus will be on offensive operations.

Topics: Network Socket Operations; Exception Handling; Process Execution; Blocking and Non-blocking Sockets; Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

573.6 HANDS ON: Capture the Flag

In this final section you will be placed on a team with other students. Working as a team, you will apply the skills you have mastered in a series of programming challenges. Participants will exercise the skills and code they have developed over the previous five days as they exploit vulnerable systems, break encryption cyphers, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

"Highly recommended. This course truly gives you the power to forensicate at scale – or hunt adversaries." -Mark Osborn, SecureWorks

***SEC573** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
NETWORK SECURITY .... Las Vegas, NV ..... Sep 10-15

Summit Events

Pen Test Hackfest – Bethesda, MD ..... Nov 15-20

Community SANS Events

Redwood City, CA ..... Nov 12-17

Private Training

All SANS courses are available through Private Training.

Course Author Statement

Good scripting skills are essential to professionals in all aspects of information security. Understanding how to develop your own applications means you can automate tasks and do more, with fewer resources, in less time. As penetration testers, knowing how to use canned information security tools is a basic skill that you must have. But knowing how to build your own tools when the tools someone else wrote fail is what separates the great penetration testers from the good ones. This course is designed for security professionals who want to learn how to apply basic coding skills to do their job more efficiently. The course will help take your career to the next level by teaching you the essential skills needed to develop applications that interact with networks, websites, databases, and file systems. We will cover these essential skills as we build practical applications that you can immediately put into use in your penetration tests.
- Mark Baggett

"This is a course every cyber analyst needs! The instruction and course materials are the best I've seen from the over 500 hours of training I have received."
-Jonathan C., DoD

SEC575

GMOB Certification
Mobile Device Security Analyst

www.giac.org/gmob

Mobile Device Security and Ethical Hacking

Six-Day Program
36 CPEs
Laptop Required

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

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
- Change the functionality of Android and iOS apps to defeat anti-jailbreaking or circumvent in-app purchase requirements
- 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

SANS Technology Institute

www.sans.edu

Imagine an attack surface spread throughout your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. You don't need to imagine any further because this already exists today: **mobile devices**. These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterize threats for management and decision-makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

You'll then use your new skills to apply a mobile device deployment penetration test in a step-by-step fashion. Starting with gaining access to wireless networks to implement man-in-the-middle attacks and finishing with mobile device exploits and data harvesting, you'll examine each step in conducting such a test with hands-on exercises, detailed instructions, and tips and tricks learned from hundreds of successful penetration tests. By building these skills, you'll return to work prepared to conduct your own test, and you'll be better informed about what to look for and how to review an outsourced penetration test.

Mobile device deployments introduce new threats to organizations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

575.1 HANDS ON: Device Architecture and Common Mobile Threats

The first section of the course quickly looks at the significant threats affecting mobile device deployments, highlighted with a hands-on exercise evaluating network traffic from a vulnerable mobile banking application. As a critical component of a secure deployment, we will examine the architectural and implementation differences and similarities in Android (including Android Marshmallow), Apple iOS 10, and the Apple Watch and Google Wear platforms. We will also look at the specific implementation details of popular platform features such as iBeacon, AirDrop, App Verification, and more. Hands-on exercises will be used to interact with mobile devices running in a virtualized environment, including low-level access to installed application services and application data.

Topics: Mobile Problems and Opportunities; Mobile Device Platform Analysis; Wearable Platforms: Mobile Device Lab Analysis Tools; Mobile Device Malware Threats

575.2 HANDS ON: Mobile Platform Access and Application Analysis

With an understanding of the threats, architectural components and desired security methods, we dig deeper into iOS and Android mobile platforms focusing on sandboxing and data isolation models, and the evaluation of mobile applications. This section is designed to help build skills in analyzing mobile device data and applications through rooting and jailbreaking Android and iOS devices and using that access to evaluate file system artifacts.

Topics: Static Application Analysis; Unlocking, Rooting, Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Network Activity Monitoring

575.3 HANDS ON: Mobile Application Reverse Engineering

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. In this section we will use automated and manual application assessment tools to evaluate iOS and Android apps. We'll build upon the static application analysis skills covered in day 2 to manipulate application components including Android intents and iOS URL extensions. We'll also learn and practice techniques for manipulating iOS and Android applications: method swizzling on iOS, and disassembly, modification, and reassembly of iOS apps. The day ends with a look at a standard system for evaluating and grading the security of mobile applications in a consistent method through the application report card project.

Topics: Application Report Cards; Automated Application Analysis Systems; Manipulating App Behavior

575.4 HANDS ON: Penetration Testing Mobile Devices – 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; Network Manipulation Attacks; Sidejacking Attacks

575.5 HANDS ON: Penetration Testing Mobile Devices – PART 2

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on iOS and Android devices. We will also examine platform-specific application weaknesses and look at the growing use of web framework attacks in mobile application exploitation.

Topics: SSL/TLS Attacks; Client Side Injection (CSI) Attacks; Web Framework Attacks; Back-end Application Support Attacks

575.6 HANDS ON: Capture the Flag

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.

***SEC575** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15
Tysons Corner Fall . . . . . McLean, VA . . . . . Oct 16-21
CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online . . . . . Sep 10-15

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

"Outstanding course material and instructor presentation. It truly drills in the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L, U.S. Air Force

SEC617

GAWN Certification

Assessing and Auditing Wireless Networks

www.giac.org/gawn

Wireless Ethical Hacking, Penetration Testing, and Defenses

Six-Day Program
36 CPEs
Laptop Required

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

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

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 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.

"SEC617 is great for someone looking for a top-to-bottom rundown in wireless attacks."

-Garret Picchioni, Salesforce

To be a wireless security expert, you need to have a comprehensive understanding of the technology, threats, exploits, and defensive 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.

"Clear and clean presentation of wireless security.
Easy to understand with real-life stories to back them up."

-Erich Winkler, Costco Wholesale

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

617.1 HANDS ON: Wireless Data Collection and 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; Rogue AP Analysis; Wireless Hotspot Networks; Attacking WEP**

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.

Topics: **Cisco LEAP Attacks; Wireless Client Attacks; Attacking WPA2-PSK Networks; Assessing Enterprise WPA2**

617.4 HANDS ON: Advanced WiFi Attack Techniques

Topics: **Deficiencies in TKIP Networks; Leveraging WiFi DoS Attacks; Wireless Fuzzing for Bug Discovery; Bridging the Airgap: Remote WiFi Pentesting; Framework and Post-Exploitation Modules**

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 their impact on organizations.

Topics: **DECT Attacks; Exploiting ZigBee; Enterprise Bluetooth Threats; Advanced Bluetooth Threats**

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. 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 Analyst Techniques; Evaluating Proprietary Wireless Technology; Deploying a Secure Wireless Infrastructure; Configuring and Securing Wireless Clients**

"This class gave me a greater appreciation for the risks associated with wireless technologies – well worth my time."

-Thomas W., USMC

***SEC617** is available via (subject to change):*

Featured Training Events

NETWORK SECURITY. . . . Las Vegas, NV . . . . . .Sep 10-15

Summit Events

Pen Test Hackfest – Bethesda, MD. . . . . Nov 15-20

Private Training

All SANS courses are available through Private Training.

Course Author Statement

It's been amazing to watch the progression of wireless technology over the past several years. WiFi has grown in maturity and offers strong authentication and encryption options to protect networks, and many organizations have migrated to this technology. At the same time, attackers are becoming more sophisticated, and we've seen significant system breaches netting millions of payment cards that start with a wireless exploit. This pattern has me very concerned, as many organizations, even after deploying WPA2 and related technology, remain vulnerable to a number of attacks that expose their systems and internal networks.

With the tremendous success of WiFi, other wireless protocols have also emerged to satisfy the needs of longer-distance wireless systems (WiMAX), lightweight embedded device connectivity (ZigBee and IEEE 802.15.4), and specialty interference-resilient connectivity (Bluetooth and DECT). Today, it's not enough to be a WiFi expert; you also need to be able to evaluate the threat of other standards-based and proprietary wireless technologies as well.

When putting this class together, I wanted to help organizations recognize the multi-faceted wireless threat landscape and evaluate their exposure through ethical hacking techniques. Moreover, I wanted my students to learn critical security analysis skills so that, while we focus on evaluating wireless systems, the vulnerabilities and attacks we leverage to exploit these systems can be applied to future technologies as well. In this manner, the skills you build in this class remain valuable for today's wireless technology, tomorrow's technology advancements, and for other complex systems you have to evaluate in the future as well.

- Joshua Wright

SEC642

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Web penetration testers
- Red team members
- Vulnerability assessment personnel
- Network penetration testers
- Security consultants
- Developers
- QA testers
- System administrators
- IT managers
- System architects

You Will Be Able To

- Perform advanced Local File Include (LFI)/ Remote File Include (RFI), Blind SQL injection (SQLi), and Cross-Site Scripting (XSS) combined with Cross-Site Request Forger (XSRF) discovery and exploitation
- Exploit advanced vulnerabilities common to most backend language like Mass Assignments, Type Juggling, and Object Serialization
- Perform JavaScript-based injection against ExpressJS, Node.js, and NoSQL
- Understand the special testing methods for content management systems such as SharePoint and WordPress
- Identify and exploit encryption implementations within web applications and frameworks
- Discover XML Entity and XPath vulnerabilities in SOAP or REST web services and other datastores
- Use tools and techniques to work with and exploit HTTP/2 and Web Sockets
- Identify and bypass Web Application Firewalls and application filtering techniques to exploit the system

Can Your Web Apps Withstand the Onslaught of Modern Advanced Attack Techniques?

Modern web applications are growing more sophisticated and complex as they utilize exciting new technologies and support ever more critical operations. Long gone are the days of basic HTML requests and responses. Even in the age of Web 2.0 and AJAX, the complexity of HTTP and modern web applications is progressing at breathtaking speed. With the demands of highly available web clusters and cloud deployments, web applications are looking to deliver more functionality in smaller packets, with a decreased strain on backend infrastructure. Welcome to an era that includes tricked-out cryptography, WebSockets, HTTP/2, and a whole lot more. Are your web application assessment and penetration testing skills ready to evaluate these impressive new technologies and make them more secure?

"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

Are You Ready to Put Your Web Apps to the Test with Cutting-Edge Skills?

This pen testing course is designed to teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. The course uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The final course day culminates in a Capture-the-Flag competition, where you will apply the knowledge you acquired during the previous five days in a fun environment based on real-world technologies.

Hands-on Learning of Advanced Web App Exploitation Skills

We begin by exploring advanced techniques and attacks to which all modern-day complex applications may be vulnerable. We'll learn about new web frameworks and web backends, then explore encryption as it relates to web applications, digging deep into practical cryptography used by the web, including techniques to identify the type of encryption in use within the application and methods for exploiting or abusing it. We'll look at alternative front ends to web applications and web services such as mobile applications, and examine new protocols such as HTTP/2 and WebSockets. The final portion of the class will focus on how to identify and bypass web application firewalls, filtering, and other protection techniques.

"SEC642 helps sharpen the pen testing mindset and to be more creative when performing pen tests."

-Jesper Pettersson, Klarna

642.1 HANDS ON: Advanced Attacks

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle advanced targets. We'll start the course with a warm-up pen test of a small application. After our review of this exercise, we will explore some of the more advanced techniques for LFI/RFI and SQLi server-based flaws. We will then take a stab at combined XSS and XSRF attacks, where we leverage the two vulnerabilities together for even greater effect. After discovering the flaws, we will then work through various ways to exploit these flaws beyond the typical means exhibited today. These advanced techniques will help penetration testers find ways to demonstrate these vulnerabilities to their organization through advanced and custom exploitation.

Topics: Review of the Testing Methodology; Using Burp Suite in a Web Penetration Test; Exploiting Local and Remote File Inclusions; Exploring Advanced Discovery Techniques for SQL Injection and Other Server-Based Flaws; Exploring Advanced Exploitation of XSS and XSRF in a Combined Attack; Learning Advanced Exploitation Techniques

642.2 HANDS ON: Web Frameworks

We'll continue exploring advanced discovery and exploitation techniques for today's complex web applications. We'll look at vulnerabilities that could affect web applications written in any backend language, then examine how logic flaws in applications, especially in Mass Object Assignments, can have devastating effects on security. We'll also dig into assumptions made by core development teams of backend programming languages and learn how even something as simple as handling the data types in variables can be leveraged through the web with Type Juggling and Object Serialization. Next we'll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. Part of this discussion will lead us to cutting-edge technologies like the MEAN stack, where JavaScript is leveraged from the browser, web server, and backend NoSQL storage. The final section of the class examines applications in content management systems such as SharePoint and WordPress, which have unique needs and features that make testing them both more complex and more fruitful for the tester.

Topics: Web Architectures; Web Design Patterns; Languages and Frameworks; Java and Struts; PHP-Type Juggling; Logic Flaws; Attacking Object Serialization; The MEAN Stack; Content Management Systems; SharePoint; WordPress

642.3 HANDS ON: Web Cryptography

Cryptographic weaknesses are common, 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 only 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 ranging from identifying what the encryption technique is to exploiting various flaws within the encryption or hashing.

Topics: Identifying the Cryptography Used in the Web Application; Analyzing and Attacking the Encryption Keys; Exploiting Stream Cipher IV Sollisions; Exploiting Electronic Codebook (ECB) Mode Ciphers with Block Shuffling; Exploiting Cipher Block Chaining (CBC) Mode with Bit Flipping; Vulnerabilities in PKCS#7 Padding Implementations

642.4 HANDS ON: Alternative Web Interfaces

Web applications are no longer limited to the traditional HTML-based interfaces. 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. We will examine Flash, Java, Active X, and Silverlight flaws. We will 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. We'll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

Topics: Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing of Web Services; WebSocket Protocol Issues and Vulnerabilities; New HTTP/2 Protocol Issues and Penetration Testing

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. The controls block many of the automated tools and simple techniques used to discover flaws. On this day we'll explore techniques used to map the control and how that control is configured to block attacks. You'll be able to map out the rule sets and determine the specifics of how the Web Application Firewall detects attacks. This mapping will then be used to determine attacks that will bypass the control. You'll use HTML5, UNICODE, and other encodings that will enable your discovery techniques to work within the protected application.

Topics: Understanding of Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall's Best-Defended Vulnerabilities, XSS and SQLi

642.6 HANDS ON: Capture the Flag

On this final course day you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this exercise 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 skills 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). You will be able to use this both in the class and after leaving and returning to your jobs.

***SEC642** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15
CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

Summit Events

Pen Test Hackfest – Bethesda, MD . . . . . Nov 15-20

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

SEC660

GXPN Certification

Exploit Researcher and Advanced Penetration Tester

www.giac.org/gxpn

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Six-Day Program
46 CPEs
Laptop Required
This course has evening Bootcamp Sessions

Who Should Attend

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

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

SANS Technology Institute

www.sans.edu

sapere aude

www.sans.org/cyber-guardian

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

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. **SEC660 provides 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.**

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; 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; IPv6 for Penetration Testers**

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: **Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; Delivering Malicious Operating Systems to Devices Using Network Booting and PXE; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Using PXE, Network Attacks, and Local Privilege Escalation**

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; 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**

***SEC660** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
NETWORK SECURITY .... Las Vegas, NV ..... Sep 11-16
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

Summit Events

Pen Test Hackfest – Bethesda, MD ..... Nov 15-20

OnDemand

E-learning available anytime, anywhere, at your pace

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online ..... Oct 17 - Nov22

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

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

"This material puts me at that next level."
-Adam Logue, Spectrum Health

660.5 HANDS ON: Exploiting Windows for Penetration Testers

On day five we start 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.

Topics: **The State of Windows OS Protections on Windows 7, 8, 10, Server 2008 and 2012; Understanding Common Windows Constructs; Stack Exploitation on Windows; Defeating OS Protections Added to Windows; Creating a Metasploit Module; Advanced Stack-Smashing on Windows; Using ROP; Building ROP Chains to Defeat DEP and Bypass ASLR; Windows 7 and 8; Porting Metasploit Modules; Client-side Exploitation; Windows Shellcode**

660.6 HANDS ON: Capture the Flag Challenge

This day will serve as a real-world challenge for students by requiring them to utilize skills they have learned throughout the course, think outside the box, and solve a range of problems from simple to complex. A web server scoring system and Capture-the-Flag engine will be provided to score students as they capture flags. More difficult challenges will be worth more points. 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.

SEC760

Advanced Exploit Development for Penetration Testers

Six-Day Program
46 CPEs
Laptop Required
This course has evening Bootcamp Sessions

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

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

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- 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.

"SEC760 is a kind of training we could not get anywhere else. It is not a theory, we got to implement and to exploit everything we learned."

-Jenny Kitaichit, Intel

Some of the skills you will learn in SEC760 include:

- **How to write modern exploits against the Windows 7/8/10 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**

"As always, I think SANS training is extremely valuable for any security professional. This course sits on top of the mountain of great SANS material." -Doug Rodgers, Wells Fargo

Not sure if you are ready for SEC760?

Take this 10 question quiz: **www.sans.org/sec760/quiz**

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 Exploitation

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

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

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

Attackers often download patches as soon as they are distributed by vendors such as Microsoft in order to find newly patched vulnerabilities. Vulnerabilities are usually 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. You will use the material covered in this day to identify bugs patched by vendors and take them through to exploitation.

Topics: **The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff, patchdiff2, turbodiff, and DarunGrim4; 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; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)**

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 7/8 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and HAL Dispatch Table Overwrites**

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; Understanding the Low Fragmentation Heap (LFH); 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; Using Custom Flash Objects to Bypass ASLR; Defeating ASLR, DEP, and Other Common Exploit Mitigation Controls**

760.6 HANDS ON: Capture the Flag Challenge

Day 6 will feature a Capture the Flag event with different types of challenges taken from material taught throughout the week.

***SEC760** is available via (subject to change):*

Featured Training Events

NETWORK SECURITY. . . . Las Vegas, NV . . . . . .Sep 10-15

Summit Events

Pen Test Hackfest – Bethesda, MD. . . . . Nov 15-20

Private Training

All SANS courses are available through Private Training.

Course Author Statement

As a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic as of late and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 7 and 8, the number of experts with the skills to produce working exploits is highly limited. More and more companies are looking to hire professionals with the ability to conduct a Secure-SDLC process, perform threat modeling, determine if vulnerabilities are exploitable, and carry out security research. This course was written to help you get into these highly sought-after positions and to teach you cutting-edge tricks to thoroughly evaluate a target, providing you with the skills to improve your exploit development.
- Stephen Sims

SANS Technology Institute

Join the only graduate degree program designed and taught by the world-class faculty at SANS.

"I chose the SANS graduate program because the technical content and faculty are unparalleled, and the mix of live and online instruction fit into my work life."

- Joshua Lewis, EY, MSISE candidate

GIAC CERTIFICATIONS

Students earn GIAC certifications during most technical courses.

GI Bill.

The SANS Technology Institute is approved to accept and/or certify Veterans for education benefits.

Built on proven SANS courses and GIAC certification exams, and accessible through live classes around the country and online from work or home, our graduate programs transform the best of SANS training and faculty into an unparalleled educational experience that is custom designed for a working professional.

Master of Science Degrees

The master's programs of the SANS Technology Institute provide the foremost education for cyber professionals.

- Master of Science in Information Security Engineering (MSISE)
- Master of Science in Information Security Management (MSISM)

Graduate Certificates

The certificate programs offer individuals the opportunity to earn a post-baccalaureate, graduate-level credential by completing a series of three to four related technical courses.

- Cybersecurity Engineering (Core)
- Cyber Defense Operations
- Penetration Testing and Ethical Hacking
- Incident Response

Accreditation

The SANS Technology Institute is accredited by the Middle States Commission on Higher Education, 3624 Market Street, Philadelphia, PA 19104 (267-284-5000). The Middle States Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Visit sans.edu for complete information on courses, admissions, and tuition.

Focus Job Roles and Specialized Skills

Incident Response and Enterprise Forensics

Incident Response and Enterprise Forensics

FOR**508** Advanced Digital Forensics, Incident Response, and Threat Hunting	**GCFA** Certification Forensic Analyst
FOR**572** Advanced Network Forensics and Analysis	**GNFA** Certification Network Forensic Analyst

Summary: Properly trained Incident Responders can hunt for and identify compromised systems, provide effective containment during a breach, and rapidly remediate an incident. They must have in-depth digital forensics knowledge of both host and network systems within the enterprise as well as knowing how to apply proactive threat intelligence – skills taught by SANS in **FOR508**, **FOR572**, and **FOR578**.

Specialized incident response and forensics skills are taught in six additional SANS courses, covering everything from Windows forensics to reverse engineering malware. Review the following pages for detailed information about all of these courses.

Who This Path is For: Incident Responders, Cyber Threat Analysts, Forensic Examiners, Security Analysts and Engineers all utilize this training path to advance their threat hunting and responding skills.

Why This Training is Important: This training will teach you to detect compromised and affected systems, how and when a breach occurred, what attackers took or changed, and how to contain and remediate incidents. Upon completing your focus path in incident response and enterprise forensics, you will be able to incorporate evidence from different sources such as networks, mobile devices, and more into your investigations, provide better findings and get the job done faster.

"This material is directly relevant to what our analysts are doing daily. Highly useful."

-Tom L., USAF

"This training gave me immediately applicable skills from active professionals in the field."

-Abe Jones, Spectrum Health

FOR508

GCFA Certification
Forensic Analyst

www.giac.org/gcfa

Advanced Digital Forensics, Incident Response, and Threat Hunting

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Detect and hunt unknown live, dormant, and custom malware in memory across multiple Windows systems in an enterprise environment
- Hunt through and perform incident response across hundreds of unique systems simultaneously using F-Response Enterprise and the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via memory forensics, registry analysis, and network connection residue
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Target advanced adversary anti-forensics techniques like hidden and time-stomped malware, along with utility-ware used to move in the network and maintain an attacker's presence
- Use memory analysis, incident response, and threat hunting tools in the SIFT Workstation to detect hidden processes, malware, attacker command lines, rootkits, network connections, and more
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Recover data cleared using anti-forensics techniques via Volume Shadow Copy and Restore Point analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection
- Understand how the attacker can acquire legitimate credentials – including domain administrator rights – even in a locked-down environment
- Track data movement as the attackers collect critical data and shift them to exfiltration collection points
- Recover and analyze archives and .rar files used by APT-like attackers to exfiltrate sensitive data from the enterprise network
- Use collected data to perform effective remediation across the entire enterprise

FOR508: Advanced Digital Forensics, Incident Response, and Theat Hunting will help you to:

- **Detect how and when a breach occurred**
- **Identify compromised and affected systems**
- **Determine what attackers took or changed**
- **Contain and remediate incidents**
- **Develop key sources of threat intelligence**
- **Hunt down additional breaches using knowledge of the adversary**

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organizations like yours, and that your organization is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organization's networks. Organizations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

"This is, by far, the best training I have ever had. My forensic knowledge increased more in the last five days than in the last year." -Vito Rocco, UNLV

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

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

SANS Technology Institute
www.sans.edu

sapere aude
www.sans.org/cyber-guardian

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

508.1 HANDS ON: Advanced Incident Response and Threat Hunting

Incident responders and threat hunters should be armed with the latest tools, memory analysis techniques, and enterprise methodologies to identify, track, and contain advanced adversaries and to remediate incidents. Incident response and threat hunting analysts must be able to scale their analysis across thousands of systems in their enterprise. This section examines the six-step incident response methodology as it applies to an enterprise's response to a targeted attack.

Topics: Real Incident Response Tactics; Threat Hunting; Cyber Threat Intelligence; Threat Hunting in the Enterprise; Malware Persistence Identification; Remote and Enterprise Incident Response

508.2 HANDS ON: Memory Forensics in Incident Response & Threat Hunting

Now a critical component of many incident response and threat hunting teams that detect advanced threats in their organization, memory forensics has come a long way in just a few years. Memory forensics can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. This extremely popular section will introduce some of the most capable tools available and give you a solid foundation to add core and advanced memory forensic skills to your incident response and forensics capabilities.

Topics: Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

508.3 HANDS ON: Intrusion Forensics

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker's action leaves a corresponding artifact, and understanding what is left behind as footprints can be critical to both red and blue team members. Attacks follow a predictable pattern, and we focus our detective efforts on immutable portions of that pattern. In this section, we cover common attacker tradecraft and discuss the various data sources and forensic tools you can use to identify malicious activity in the enterprise.

Topics: Advanced Evidence of Execution Detection; Window Shadow Volume Copy Analysis; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Event Log Analysis for Incident Responders and Hunters

508.4 HANDS ON: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. This section will step you through the two primary methods of building and analyzing timelines created during advanced incident response, threat hunting, and forensic cases. Exercises will show analysts how to create a timeline and also how to introduce the key methods to help you use those timelines effectively in your cases.

Topics: Timeline Analysis Overview; Memory Analysis Timeline Creation; Filesystem Timeline Creation & Analysis; Super Timeline Creation & Analysis

508.5 HANDS ON: Incident Response and Hunting Across the Enterprise | Advanced Adversary and Anti-Forensics Detection

Over the years, we have observed that many incident responders and threat hunters have a challenging time finding threats without pre-built indicators of compromise or threat intelligence gathered before a breach. This is especially true in APT adversary intrusions. 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: Evolution of Incident Response Scripting; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

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. It brings together techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge brings it all together using a real intrusion into a complete Windows enterprise environment. 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.

Topics: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery

***FOR508** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach Long Beach, CA . . . . . Jul 10-15
SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
Virginia Beach . . . . . Virginia Beach, VA Aug 27 - Sep 1
NETWORK SECURITY . . . . Las Vegas, NV . . . . . Sep 10-15
Tysons Corner Fall . . . . . McLean, VA . . . . . Oct 16-21
Seattle . . . . . Seattle, WA . . . . . Oct 30 - Nov 4
Austin Winter . . . . . Austin, TX . . . . . Dec 4-9
CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

Summit Events

Data Breach – Chicago, IL . . . . . Sep 27 - Oct 2

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online . . . . . Jul 24-29
Virtual/Online . . . . . Sep 10-15

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online . . . . . Oct 16 - Nov 22

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Columbia, MD . . . . . Aug 21-26

Private Training

All SANS courses are available through Private Training.

FOR572

GNFA Certification
Network Forensic Analyst

www.giac.org/gnfa

Advanced Network Forensics and Analysis *NEW!*

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- Anyone interested in computer network intrusions and investigations
- Security Operations Center personnel and information security practitioners

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determination
- 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
- 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

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or even prove useful in definitively proving 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, an on-staff forensic practitioner, or a member of the growing ranks of "threat hunters", this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC 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 FOR500 (formerly 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 the use of disk or memory images.

The hands-on labs in this class cover a wide range of tools and platforms, including the venerable tcpdump and Wireshark for packet capture and analysis; NetworkMiner for artifact extraction; and open-source tools including nfdump, tcpxtract, tcpflow, and more. Newly added tools in the course include the SOF-ELK platform – a VMware appliance pre-configured with the ELK stack. This "big data" platform includes the Elasticsearch storage and search database, the Logstash ingest and parse utility, and the Kibana graphical dashboard interface. Together with the custom SOF-ELK configuration files, the platform gives forensicators a ready-to-use platform for log and NetFlow analysis. For full-packet analysis and hunting at scale, the Moloch platform is also used. Through all of the in-class labs, your shell scripting abilities will also be used to make easy work of ripping through hundreds and thousands of data records.

SANS Technology Institute

www.sans.edu

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 you'll 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: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

572.2 HANDS ON: Core Protocols & Log Aggregation/Analysis

Understanding log data and how it can guide the investigative process is an important network forensicator skill. Examining network-centric logs can also fill gaps left by an incomplete or nonexistent network capture. In this section, you will learn various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You'll use the SOF-ELK platform for post-incident log aggregation and analysis, bringing quick and decisive insight to a compromise investigation.

Topics: Hypertext Transfer Protocol (HTTP): Protocol and Logs; Domain Name Service (DNS): Protocol and Logs; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

572.3 HANDS ON: NetFlow and File Access Protocols

In this section, you will learn the contents of typical NetFlow protocols, as well as common collection architectures and analysis methods. You'll also learn how to distill full-packet collections to NetFlow records for quick initial analysis before diving into more cumbersome pcap files. In addition, you'll examine the File Transfer Protocol, including how to reconstruct specific files from an FTP session. While FTP is commonly used for data exfiltration, it is also an opportunity to refine protocol analysis techniques, due to its multiple-stream nature. Lastly, you'll explore a variety of the network protocols unique to a Microsoft Windows or Windows-compatible environment. Attackers frequently use these protocols to "live off the land" within the victim's environment. By using existing and expected protocols, adversaries can hide in plain sight and avoid deploying malware that could tip off the investigators to their presence and actions.

Topics: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol (FTP); Microsoft Protocols

572.4 HANDS ON: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools hold clear advantages in some situations a forensicator may typically encounter. Most commonly, this centers on scalability. Many open-source tools are designed for tactical or small-scale use. Whether they are used for large-scale deployments or for specific niche functionalities, these tools can immediately address many investigative needs. You'll look at the typical areas where commercial tools in the network forensic realm tend to focus, and discuss the value each may provide for your organizational requirements or those of your clients. Additionally, we will address the forensic aspects of wireless networking.

Topics: Simple Mail Transfer Protocol (SMTP); Commercial Network Forensics; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

572.5 HANDS ON: Encryption, Protocol Reversing, OPSEC, and Intel

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: Encoding, Encryption, and SSL; Man in the Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

572.6 HANDS ON: Network Forensics Capstone Challenge

Students will test their understanding of network evidence and their ability to articulate and support hypotheses through presentations made to the instructor and class. The audience will include senior-level decision-makers, so all presentations must include executive summaries as well as technical details. Time permitting, students should also include recommended steps that could help to prevent, detect, or mitigate a repeat compromise.

Topics: Network Forensic Case

***FOR572** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29
Virginia Beach . . . . . Virginia Beach, VA Aug 27 - Sep 1
NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15
Seattle . . . . . Seattle, WA . . . . . Oct 30 - Nov 4
CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online . . . . . Jul 24-29
Virtual/Online . . . . . Dec 14-19

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

FOR500 (Formerly FOR408)

Windows Forensic Analysis

GCFE Certification
Forensic Examiner

www.giac.org/gcfe

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

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

You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7/8/10
- 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
- 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

All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR500 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR500 is continually updated. This course utilizes a brand-new intellectual property theft and corporate espionage case that took over six months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The incredibly detailed step-by-step workbook details the tools and techniques that each investigator should follow to solve a forensic case.

MASTER WINDOWS FORENSICS –
YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

500.1 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; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

500.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 – Windows Registry Forensics and Analysis

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. Each examiner will learn how to navigate and examine the Registry to obtain user-profile data and system data. The course teaches forensic investigators how to prove that a specific user performed key word searches, ran specific programs, opened and saved files, perused folders, and used removable devices.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; Tools Utilized

500.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 – USB Devices, Shell Items, and Key Word Searching

Being able to show the first and last time a file was opened is a critical analysis skill. Utilizing shortcut (LNK) and jumplist databases, we are able to easily pinpoint which file was opened and when. We will demonstrate how to examine the pagefile, system memory, and unallocated space – all difficult-to-access locations that can offer the critical data for your case.

Topics: Shell Item Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations; Key Word Searching and Forensics Suites (AccessData's FTK, Guidance Software's EnCase)

500.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 – Email, Key Additional Artifacts, and Event Logs

This section discusses what types of information can be relevant to an investigation, where to find email files, and how to use forensic tools to facilitate the analysis process. We will find that the analysis process is similar across different types of email stores, but the real work takes place in the preparation – finding and extracting the email files from a variety of different sources. The last part of the section will arm each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

Topics: Email Forensics; Forensicating Additional Windows OS Artifacts; Windows Event Log Analysis

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

Throughout the section, investigators will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, and Internet Explorer along with Windows Operating System artifacts.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox; Chrome; Examination of Browser Artifacts; Tools Used

500.6 HANDS ON: Windows Forensic Challenge

This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

Topics: Digital Forensic Case; Windows 7 Forensic Challenge

SANS Technology Institute

www.sans.edu

***FOR500** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Virginia Beach	Virginia Beach, VA	Aug 21-26
Tampa-Clearwater	Clearwater, FL	Sep 5-10
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Jul 24-29
Virtual/Online	Sep 10-15
Virtual/Online	Nov 27 - Dec 2

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Columbia, MD	Jul 24-29
Columbia, MD	Aug 14-19
Ottawa, ON	Nov 20-25

Private Training

All SANS courses are available through Private Training.

"If you need to track down what happened in your environments, this is a must have course!"

-Fran Moniz, American National Insurance

FOR518

Mac Forensic Analysis

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, or detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents/intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR500 (formerly FOR408), FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

You Will Be Able To

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals' usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

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

Times and trends change and forensic investigators and analysts need to change with them. The new **FOR518: Mac Forensic Analysis** course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FOR518: Mac Forensic Analysis will teach you:

- **Mac Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) by hand and recognize the specific domains of the logical file system and Mac-specific file types.**
- **User Activity: How to understand and profile users through their data files and preference configurations.**
- **Advanced Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.**
- **Mac Technologies: How to understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.**

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

FORENSICATE DIFFERENTLY!

"Best of any course I've ever taken.
I love the idea of being able to bring the material home to review."
-Eric Koebelen, Incident Response US

"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."
-Kevin J. Ripa, Computer Evidence Recovery, Inc.

518.1 HANDS ON: Mac Essentials and the HFS+ File System

This section introduces the student to Mac system fundamentals such as acquisition, the Hierarchical File System (HFS+), timestamps, and logical file system structure. Acquisition fundamentals are the same with Mac systems, but there are a few Mac-specific tips and tricks that can be used to successfully and easily collect Mac systems for analysis. The building blocks of Mac Forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, the student will learn the basic principles of the primary file system implemented on Mac OS X systems. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system: the data are the same, only the format differs.

Topics: Mac Fundamentals; Mac Acquisition; Incident Response; HFS+ File System; Volumes; Mac Basics

518.2 HANDS ON: User Domain File Analysis

The logical Mac file system is made up of four domains; User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations, e-mail, Internet history, and user-specific application data. This section contains a wide array of information that can be used to profile and understand how individuals use their computers.

Topics: User Home Directory; User Account Information; User Data Analysis; Internet & E-mail; Instant Messaging; Native Mac Applications

518.3 HANDS ON: System and Local Domain File Analysis

The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

Topics: System Information; System Applications; Log Analysis; Timeline Analysis & Correlation

518.4 HANDS ON: Advanced Analysis Topics

Mac systems implement some technologies that are available only to those with Mac devices. These include data backup with Time Machine, Versions, and iCloud; extensive file metadata with Extended Attributes and Spotlight; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, Mac intrusion and malware analysis, Mac Server, and Mac memory analysis.

Topics: Extended Attributes; Time Machine; Spotlight; Cracking Passwords & Encrypted Containers; iCloud; Document Versions; Malware & Antivirus; Memory Acquisition & Analysis; Portable OS X Artifacts; Mac OS X Server

518.5 HANDS ON: iOS Forensics

From iPods to iPhones to iPads, it seems everyone has at least one of these devices. Apple iDevices are seen in the hands of millions of people. Much of what goes on in our lives is often stored on them. Forensic analysis of these iOS devices can provide an investigator with an incredible amount of information. Data on these iOS devices will be explored to teach the student what key files exist on them and what advanced analysis techniques can be used to exploit them for investigations.

Topics: History of iOS Devices; iOS Acquisition; iOS Analytical Tool Overview; iOS Artifacts Recovered from OS X Systems; iOS File System; iOS Artifacts & Areas of Evidentiary Value; Third-Party Applications

518.6 HANDS ON: The Mac Forensics Challenge

Students will put their new Mac forensics skills to the test by completing the following tasks:

- **In-Depth HFS+ File System Examination**
- **File System Timeline Analysis**
- **Advanced Computer Forensics Methodology**
- **Mac Memory Analysis**
- **File System Data Analysis**
- **Metadata Analysis**
- **Recovering Key Mac Files**
- **Volume and Disk Image Analysis**
- **Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault**
- **Advanced Log Analysis and Correlation**
- **iDevice Analysis and iOS Artifacts**

***FOR518** is available via (subject to change):*

Featured Training Events

NETWORK SECURITY. . . . Las Vegas, NV . . . . . .Sep 10-15

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

Course Author Statement

This course is designed to allow an analyst comfortable in Windows-based forensics to perform just as well on the Mac. The Mac market share is an ever increasing and popular platform for many companies and government entities.

I believe a well-rounded forensic analyst is an extremely well-prepared and employable individual in a Windows forensics world. Windows analysis is the base education in the competitive field of digital forensics. Any additional skills you can acquire can set you apart from the crowd, whether it is Mac, mobile, memory, or malware analysis.

Mac forensics is truly a passion of mine that I genuinely want to share with the forensics community. While you may not work on a Mac investigation every day, the tools and techniques you learn in this course will help you with other investigations including Windows, Linux, and mobile.
-Sarah Edwards

FOR526

Memory Forensics In-Depth

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Incident response team members who regularly respond to complex security incidents/intrusions and would like to know how memory forensics will expand their reach
- Experienced digital forensic analysts who want to consolidate and expand their understanding of memory forensics
- Red team members, penetration testers, and exploit developers who want to learn how their opponents can identify their actions. Discover how common mistakes can compromise operations on remote systems, and how to avoid them. This course covers remote system forensics and data collection techniques that can be easily integrated into post-exploit operating procedures and exploit testing batteries.
- Law enforcement officers, federal agents, or detectives who want to become a deep subject-matter expert on memory forensics
- SANS FOR508 and SEC504 graduates looking to take their memory forensics skills to the next level.
- Forensics investigators working in organizations where memory is regularly obtained by first responders, and who want to raise the bar by analyzing the images

Course Author Statement

Having the skills to conquer memory forensics pushes you into the top tier of forensics professionals out there today. File system forensics is now taught in community colleges, and as a result, new grads with entry level forensics skills are flooding the job market. Experienced professionals now need deeper technical expertise to set themselves apart from the pack. FOR526 class delivers this expertise. We have written this class with the specific goals of creating experts by making a specialist out of a generalist. My co-authors and I, forensics practitioners ourselves, understand the types of cases and challenges examiners are up against today. As firm believers in 'exposure therapy,' we provide our students with the tools to get the job done and then throw them right into some of the most complex yet exceedingly more common memory forensics scenarios.
- Alissa Torres

"This course is totally awesome, relevant, and eye opening. I want to learn more every day."

-Matthew Britton,

Blue Cross Blue Shield of Louisiana

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

MALWARE CAN HIDE, BUT IT MUST RUN

FOR526: Memory Forensics In-Depth will teach you:

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

526.1 HANDS ON: Foundations in Memory Analysis and Acquisition

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

Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

526.2 HANDS ON: Unstructured Analysis and Process Exploration

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

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

526.3 HANDS ON: Investigating the User via Memory Artifacts

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

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

526.4 HANDS ON: Internal Memory Structures

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

Topics: Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

526.5 HANDS ON: Memory Analysis on Platforms Other than Windows

Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac – that is, platforms other than Windows.

Topics: Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

526.6 HANDS ON: Memory Analysis Challenges

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

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

***FOR526** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV ..... Sep 10-15
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

Event Simulcast

Virtual/Online ..... Sep 10-15

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

What You Will Receive

- SIFT Workstation 3
  - This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.
  - Ubuntu LTS Base
  - 64-bit based system
  - Better memory utilization
  - Auto-DFIR package update and customizations
  - Latest forensic tools and techniques
  - VMware Appliance ready to tackle forensics
  - Cross-compatibility between Linux and Windows
  - Expanded Filesystem Support (NTFS, HFS, EXFAT, and more)
- Windows 8.1 Workstation with license
  - 64-bit based system
  - A licensed virtual machine loaded with the latest forensic tools
  - VMware Appliance ready to tackle forensics
- 32 GB Course USB 3.0
  - USB loaded with memory captures, SIFT workstation 3, tools, and documentation
- SANS Memory Forensics Exercise Workbook
  - Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder
- SANS DFIR Cheat sheets to Help Use the Tools
- MP3 audio files of the complete course lecture

FOR578

Cyber Threat Intelligence

GIAC Certification Available Late 2017

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Security Operations Center personnel and information security practitioners
- Federal agents and law enforcement officials
- SANS FOR500 (formerly FOR408), FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

Course Author Statement

"Before threat intelligence was a buzzword, it was something we all used to just do as part of incident response. But I'll admit that most of us used to do it badly. Or more accurately, ad hoc at best. We simply lacked structured models for intrusion analysis, campaign tracking, and consistent reporting of threats. Today, we need analysts trained in intelligence analysis techniques ready to perform proper campaign modeling, attribution, and threat analysis. The Cyber Threat Intelligence course teaches students all of that, as well as how to avoid cognitive biases in reporting and the use of alternative competing hypothesis in intelligence analysis. These are critical skills that most in industry today absolutely lack."
-Jake Williams

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- **Understand and develop skills in tactical, operational, and strategic-level threat intelligence**
- **Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)**
- **Validate information received from other organizations to minimize resource expenditures on bad intelligence**
- **Leverage open-source intelligence to complement a security team of any size**
- **Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX**

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. **FOR578: Cyber Threat Intelligence** will train you and your team in the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

THERE IS NO TEACHER BUT THE ENEMY!

"Outstanding course material and instructor presentation! It truly drills into the analytic process, while remaining technical. I highly recommend this course to anyone performing any level of intelligence support to defensive cyber operations."

-Thomas L., USAF

578.1 HANDS ON: Cyber Threat Intelligence

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

Topics: **Case-Study: Carbanak, "The Great Bank Robbery"; Understanding Intelligence; Understanding Cyber Threat Intelligence; Tactical Threat Intelligence Introduction; Operational Threat Intelligence Introduction; Strategic Threat Intelligence Introduction**

578.2 HANDS ON: Tactical Threat Intelligence: Kill Chain for Intrusion Analysis

Tactical cyber threat intelligence requires that analysts extract and categorize indicators and adversary tradecraft from intrusions. These actions enable all other levels of threat intelligence by basing intelligence on observations and facts that are relevant to the organization. One of the most commonly used models for assessing adversary intrusions is the "kill chain." This model is a framework to understand the steps an adversary must accomplish to be successful. This section will help tactical threat intelligence develop the skills required to be successful by using the kill chain as a guide. Students will then pivot into open-source intelligence-gathering tradecraft to enrich their understanding of the analyzed intrusion. The section walks students through multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process to structuring and defining adversary campaigns.

Topics: **Kill Chain Courses of Action; Tactical Threat Intelligence Requirements; Kill Chain Deep Dive; Handling Multiple Kill Chains; Pivoting to Open-Source Intelligence**

578.3 HANDS ON: Tactical/Operational Threat Intelligence: Campaigns and Open-Source Intelligence

Developing an understanding of adversary campaigns and tradecraft requires piecing together individual intrusions and data points. Organizations of any size will need to complement what they know from internal analysis with open-source intelligence (OSINT) to enrich and validate the information. This allows security personnel to understand dedicated adversaries more fully and consistently defend their environments. In this section, students learn what campaigns are, why they are important, and how to define them. From this baseline intelligence, gaps and collection opportunities are identified for fulfillment via open-source resources and methods. Common types and implementations of open-source data repositories, as well as their use, are explored in-depth through classroom discussion and exercises. These resources can produce an enormous volume of intelligence about intrusions, which may contain obscure patterns that further elucidate campaigns or actors. Tools and techniques to expose these patterns within the data through higher-order analysis will be demonstrated in narrative and exercise form. The application of the resulting intelligence will be articulated for correlation, courses of action, campaign assembly, and more.

Topics: **Case Study: Axiom; OSINT Pivoting, Link Analysis, and Domains; OSINT From Malware; Case Study: GlassRAT; Intelligence Aggregation and Data Visualization; Defining Campaigns; Communicating About Campaigns**

578.4 HANDS ON: Operational Threat Intelligence: Sharing Intelligence

Many organizations seek to share intelligence but often falter in understanding the value of shared intelligence, its limitations, and the right formats to choose for each audience. This section will focus on identifying both open-source and professional tools that are available for students as well as sharing standards for each level of cyber threat intelligence both internally and externally. Students will learn about YARA and generate YARA rules to help incident responders, security operations personnel, and malware analysts. They will gain hands-on experience with STIX and understand the CybOX and TAXII frameworks for sharing information between organizations. Finally, the section will focus on sharing intelligence at the strategic level in the form of reports, briefings, and analytical assessments in order to help organizations make required changes to counter persistent threats and safeguard business operations.

Topics: **Storing Threat Intelligence; Sharing: Tactical; Case Study: Sony Attack; Sharing: Operational; Sharing: Strategic**

578.5 HANDS ON: Strategic Threat Intelligence: Higher-Order Analysis

A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. At the strategic level of cyber threat intelligence, the skills required to think critically are exceptionally important and can have organization-wide or national-level impact. In this section, students will learn about logical fallacies and cognitive biases as well as how to defeat them. They will also learn about nation-state attribution, when it can be of value, and when it is merely a distraction. Students will also learn about nation-state-level attribution from previously identified campaigns and take away a more holistic view of the cyber threat intelligence industry to date. The class will finish with a discussion on consuming threat intelligence and actionable takeaways for students to make significant changes in their organizations after class.

Topics: **Logical Fallacies and Cognitive Biases; Analysis of Competing Hypotheses; Case Study: Stuxnet; Human Elements of Attribution; Nation-State Attribution; Case Study: Sofacy; A Look Backward; Case Study: Cyber Attack on the Ukrainian Power Grid; Active Defense**

***FOR578** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-28
San Antonio	San Antonio, TX	Aug 6-10
Boston	Boston, MA	Aug 7-11
Virginia Beach	Virginia Beach, VA	Aug 28 - Sep 1
NETWORK SECURITY	Las Vegas, NV	Sep 11-15
Rocky Mountain Fall	Denver, CO	Sep 25-29
Tysons Corner Fall	McLean, VA	Oct 16-20
Miami	Miami, FL	Nov 6-10
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 1
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-18

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Jul 24-28
Virtual/Online	Nov 27 - Dec 1

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

FOR585

GASF Certification
Advanced Smartphone Forensics

www.giac.org/gasf

Advanced Smartphone Forensics

Six-Day Program
36 CPEs
Laptop Required

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- IT auditors
- SANS SEC575, FOR500 (formerly FOR408), FOR508, FOR518, and FOR572 graduates looking to take their skills to the next level

You Will Be Able To

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users
- Identify how the evidence got onto the mobile device – we'll teach you how to know if the user created the data, which will help you avoid the critical mistake of reporting false evidence obtained from tools
- Incorporate manual decoding techniques to recover deleted data stored on smartphones and mobile devices
- Tie a user to a smartphone at a specific date/time and at various locations
- Recover hidden or obfuscated communication from applications on smartphones
- Decrypt or decode application data that are not parsed by your forensic tools
- Detect smartphones compromised by malware and spyware using forensic methods
- Decompile and analyze mobile malware using open-source tools
- Handle encryption on smartphones and bypass, crack, and/or decode lock codes manually recovered from smartphones, including cracking iOS backup files that were encrypted with iTunes
- Understand how data is stored on smartphone components (SD cards) and how encrypted data can be examined by leveraging the smartphone
- Extract and use information from smartphones and their components, including Android, iOS, BlackBerry, Windows Phone, Nokia (Symbian), Chinese knock-offs, SIM cards, and SD cards
- 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
- 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

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. **FOR585: Advanced Smartphone Forensics** will teach you those skills.

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's 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!

SMARTPHONE DATA CAN'T HIDE FOREVER –
IT'S TIME TO OUTSMART THE MOBILE DEVICE!

SANS Technology Institute

www.sans.edu

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. Most commercial tools help you identify malware, but none of them will allow you to tear down the malware to the level we cover in class. Up to five labs will be conducted on this first day alone!

Topics: **The SIFT Workstation; Malware and Spyware Forensics; Introduction to Smartphones; Smartphone Handling; Forensic Acquisition of Smartphones; Smartphone Forensics Tool Overview; JTAG Forensics; 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; Handling Locked Android Devices; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices**

585.3 HANDS ON: iOS Forensics

Apple 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 forensic investigation.

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

585.4 HANDS ON: Backup File and BlackBerry Forensics

We realize that not everyone examines BlackBerry devices. However, this section highlights pieces of evidence that can be found on multiple smartphones. Most importantly, we cover encrypted data on SD cards and how those data need to be acquired and examined. 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 smartphone images are commonly found on external media and the cloud, and may be the only forensic acquisition method for newer iOS devices that are locked. Learning how to access and parse data from encrypted backup files may be the only lead to smartphone data relating to your investigation.

Topics: **Backup File Forensics Overview; Common File Formats For Smartphone Backups; Creating and Parsing Backup Files; Evidentiary Locations on Backup Files; Locked Backup Files; Blackberry Forensics Overview; BlackBerry File System, Evidentiary Locations and Forensic Analysis**

***FOR585** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
Chicago ..... Chicago, IL ..... Aug 21-26
San Francisco Fall ..... San Francisco, CA .... Sep 5-10
NETWORK SECURITY. ... Las Vegas, NV ..... Sep 10-15
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online ..... Sep 10-15

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online ..... Jul 10 - Aug 16

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

"This class exceeded my expectations. The material is cutting edge."

-Kevin McNamara, San Diego Police Department

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

This day starts with third-party applications across all smartphones and is designed to teach students how to leverage third-party application data and preference files to support an investigation. Next, other smartphones not afforded a full day of instruction are discussed and labs for each are provided. 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. You must acquire skills for handling and parsing data from uncommon smartphone devices. This course day 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. The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped Windows Phone.

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 final course day 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 forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

FOR610

GREM Certification
Reverse Engineering Malware

www.giac.org/grem

Reverse-Engineering Malware: Malware Analysis Tools and Techniques *NEW!*

Six-Day Program
36 CPEs
Laptop Required

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

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, registry, 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 the 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

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

The course begins by establishing the foundation for analyzing malware in a way that dramatically expands upon the findings of automated analysis tools. You will learn how to set up a flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. You will also learn how to redirect and intercept network traffic in the lab to explore the specimen's capabilities by interacting with the malicious program.

Malware is often obfuscated to hinder analysis efforts, so the course will equip you with the skills to unpack executable files. You will learn how to dump such programs from memory with the help of a debugger and additional specialized tools, and how to rebuild the files' structure to bypass the packer's protection. You will also learn how to examine malware that exhibits rootkit functionality to conceal its presence on the system, employing code analysis and memory forensics approaches to examining these characteristics.

FOR610 malware analysis training also teaches how to handle malicious software that attempts to safeguard itself from analysis. You will learn how to recognize and bypass common self-defensive measures, including code injection, sandbox evasion, flow misdirection, and other measures.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systematic manner. 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.

"FOR610 is the best course in the industry for performing malware analysis."

-David Bernal, Alstom

SANS Technology Institute

www.sans.edu

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; Interacting with Malware in a Lab to Derive Additional Behavioral Characteristics

610.2 HANDS ON: Reversing Malicious Code

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 material will then build on this foundation and expand your understanding to incorporate 64-bit malware, given its growing popularity. Throughout the discussion, you will learn to recognize common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

Topics: Understanding Core x86 Assembly Concepts to Perform Malicious Code analysis; Identifying Key Assembly Logic Structures with a Disassembler; Following Program Control Flow to Understand Decision Points During Execution; Recognizing Common Malware Characteristics at the Windows API level (Registry Manipulation, Keylogging, HTTP Communications, Droppers); Extending Assembly Knowledge to Include x64 Code Analysis

610.3 HANDS ON: Malicious Web and Document Files

Section three focuses on examining malicious web pages and documents, which adversaries can use to directly perform malicious actions on the infected system and launch attacks that lead to the installation of malicious executable files. The section begins by discussing how to examine suspicious websites that might host client-side exploits. Next, you will learn how to de-obfuscate malicious scripts with the help of script debuggers and interpreters, examine Microsoft Office macros, and assess the threats associated with PDF and RTF files using several techniques.

Topics: Interacting with Malicious Websites to Assess the Nature of their Threats; De-obfuscating Malicious JavaScript Using Debuggers and Interpreters; Analyzing Suspicious PDF Files; Examining Malicious Microsoft Office Documents, Including Files with Macros; Analyzing Malicious RTF Document Files

610.4 HANDS ON: In-Depth Malware Analysis

Section four builds on the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. The section begins by discussing how to handle packed malware. We will examine ways to identify packers and strip away their protection with the help of a debugger and other utilities. We will also walk through the analysis of malware that employs multiple technologies to conceal its true nature, including the use of registry, obfuscated JavaScript and PowerShell scripts, and shellcode. Finally, we will learn how malware implements Usermode rootkit functionality to perform code injection and API hooking, examining this functionality from both code and memory forensics perspectives.

Topics: Recognizing Packed Malware; Getting Started with Unpacking; Using Debuggers for Dumping Packed Malware from Memory; Analyzing Multi-Technology and Fileless Malware; Code Injection and API Hooking; Using Memory Forensics for Malware Analysis

610.5 HANDS ON: Examining Self-Defending Malware

Section five takes a close look at the techniques malware authors commonly employ to protect malicious software from being examined. You will learn how to recognize and bypass anti-analysis measures designed to slow you down or misdirect you. In the process, you will gain more experience performing static and dynamic analysis of malware that is able to unpack or inject itself into other processes. You will also expand your understanding of how malware authors safeguard the data that they embed inside malicious executables. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

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 Analysis Tournament

Section six assigns students to the role of a malware analyst working as a member of an incident response or forensics 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. Students who score the highest in the malware analysis challenge will be awarded the coveted SANS Lethal Forensicator coin.

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

***FOR610** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
New York City	New York, NY	Aug 14-19
Virginia Beach	Virginia Beach, VA	Aug 27 - Sep 1
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online	Sep 25-30

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Ottawa, ON	Sep 18-23
New York, NY	Oct 16-21

Private Training

All SANS courses are available through Private Training.

Security awareness is hard.
We make it easy.

SANS SECURITY AWARENESS

Expert

SANS security awareness training content is built by the world's leading cybersecurity practitioners. Our team of PhD instructional designers and cybersecurity experts ensures learners engage with the content in a way that actually changes behavior.

Easy

The Advanced Cybersecurity Learning Platform (ACLP) makes it easy to manage and deliver your awareness program by reducing the administrative burden through intuitive design. The ACLP helps you avoid training fatigue by using role and rule-based training audiences.

Efficient

SANS delivers the platforms, products, resources and support security awareness professionals need to do more with less. SANS support is second to none because we know what it takes to be successful.

SANS Securing The Human Named Leader in Gartner 2016 Magic Quadrant

SANS content is designed, built and delivered by world-class instructors and cybersecurity practitioners. These are the experts called in to analyze and fix high profile, high stakes cybersecurity incidents. SANS Institute was named a Leader in the 2016 Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors.

Download the Report
securingthehuman.sans.org/gartner

Phishing Training ■ Knowledge Assessments ■ Culture & Behavior Change ■ Managed Services

Focus Job Roles and Specialized Skills

Management | Audit | Legal

Summary: Professional security managers require a broad and proven knowledge of policy, standards and practices in order to provide the greatest level of security to their organizations. They also need to speak their technician's language, and design security plans that withstand attack from all angles. SANS's specialized management, audit, and legal courses deliver the tools and techniques required to lead with confidence.

More than 10 advanced and specialized training options in this practice area are detailed on the following pages.

Who This Path is For: CISOs, IT directors, or others with responsibility for managing their organization's security operations benefit from the experience-rich instruction in SANS management, audit, and legal courses. Security, system, and network administrators who are pursuing a CISSP or a new management role should also prepare themselves for this type of training.

Why This Training is Important: Professionals who train and certify in these skills are the leaders of cyber security. They master the specific techniques and tools needed to implement and audit the Critical Security Controls, they have a firm understanding of the eight domains of knowledge covered in the CISSP, they can communicate information security best practices to executives and technical teams, and they are designing the security operation centers of the future.

Software Security | Industrial Control System Security

For specialists in software security or industrial control system security, find detailed information about six additional SANS courses available in the spring and summer of 2017 on pages 85 – 90.

MGT414

GISP Certification
Information Security Professional

www.giac.org/gisp

SANS Training Program for CISSP® Certification

Six-Day Program
46 CPEs
Laptop Not Needed
This course has evening and morning Bootcamp Sessions

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

You Will Be Able To

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

MEETS DoDD 8140 (8570) REQUIREMENTS

www.sans.org/8140

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the CISSP® exam.

MGT414 focuses solely on the eight domains of knowledge as determined by $(ISC)^2$ that form a critical part of the CISSP® exam. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

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**

"Best security training I have ever received and just the right amount of detail for each domain."

-Tony Barnes, United States Sugar Corp

"It was extremely valuable to have an experienced information security professional teaching the course as he was able to use experiential knowledge in examples and explanations."

-Sean Hoar, Davis Wright Tremaine

"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

414.1 Introduction; Security and Risk Management

On the first day of training for the CISSP® exam, MGT414 introduces the specific requirements needed to obtain certification. The exam update will be discussed in detail. We will cover the general security principles needed to understand the eight domains of knowledge, with specific examples for each domain. The first of the eight domains, Security and Risk Management, is discussed using real-world scenarios to illustrate the critical points.

Topics: Overview of CISSP® Certification; Introductory Material; Overview of the Eight Domains; Domain 1: Security and Risk Management

414.2 Asset Security and Security Engineering – PART 1

Understanding asset security is critical to building a solid information security program. The Asset Security domain, the initial focus of today's course section, describes data classification programs, including those used by both governments and the military as well as the private sector. We will also discuss ownership, covering owners ranging from business/mission owners to data and system owners. We will examine data retention and destruction in detail, including secure methods for purging data from electronic media. We then turn to the first part of the Security Engineering domain, including new topics for the 2016 exam such as the Internet of Things, Trusted Platform Modules, Cloud Security, and much more.

Topics: Domain 2: Asset Security; Domain 3: Security Engineering (Part 1)

414.3 Security Engineering – PART 2; Communication and Network Security

This section continues the discussion of the Security Engineering domain, including a deep dive into cryptography. The focus is on real-world implementation of core cryptographic concepts, including the three types of cryptography: symmetric, asymmetric, and hashing. Salts are discussed, as well as rainbow tables. We will round out Domain 3 with a look at physical security before turning to Domain 4, Communication and Network Security. The discussion will cover a range of protocols and technologies, from the Open Systems Interconnection (OSI) model to storage area networks.

Topics: Domain 3: Security Engineering (Part 2); Domain 4: Communication and Network Security

414.4 Identity and Access Management

Controlling access to data and systems is one of the primary objectives of information security. Domain 5, Identity and Access Management, strikes at the heart of access control by focusing on identification, authentication, and authorization of accounts. Password-based authentication represents a continued weakness, so Domain 5 stresses multi-factor authentication, biometrics, and secure credential management. The CISSP® exam underscores the increased role of external users and service providers, and mastery of Domain 5 requires an understanding of federated identity, SSO, SAML, and third-party identity and authorization services like Oauth and OpenID.

Topics: Domain 5: Identity and Access Management

414.5 Security Assessment and Testing; Security Operations

This course section covers Domain 6 (Security Assessment) and Domain 7 (Security Operations). Security Assessment covers types of security tests, testing strategies, and security processes. Security Operations covers investigatory issues, including eDiscovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as cloud, and we'll wrap up day five with a deep dive into disaster recovery.

Topics: Domain 6: Security Assessment; Domain 7: Security Operations

414.6 Software Development Security

Domain 8 (Software Development Security) describes the requirements for secure software. Security should be "baked in" as part of network design from day one, since it is always less effective when it is added later to a poor design. We will discuss classic development models, including waterfall and spiral methodologies. We will then turn to more modern models, including agile software development methodologies. New content for the CISSP® exam update will be discussed, including DevOps. We will wrap up this course section by discussing security vulnerabilities, secure coding strategies, and testing methodologies.

Topics: Domain 8: Software Development Security

***MGT414** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-29
Boston	Boston, MA	Aug 7-12
Salt Lake City	Salt Lake City, UT	Aug 14-19
Tampa-Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10
NETWORK SECURITY	Las Vegas, NV	Sep 10-15
Baltimore Fall	Baltimore, MD	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Seattle	Seattle, WA	Oct 30 - Nov 4
San Diego	San Diego, CA	Oct 30 - Nov 4
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-19

OnDemand

E-learning available anytime, anywhere, at your pace

Custom Simulcast

Customized training for distributed workforces

vLive Events

Virtual/Online	Jul 17 - Aug 23
Virtual/Online	Sep 19 - Oct 26
Virtual/Online	Nov 7 - Dec 14

SelfStudy

Individual study with course books and lecture MP3s.

Mentor Classes

Atlanta, GA	Sep 13 - Nov 15

Private Training

All SANS courses are available through Private Training.

MGT514

GSTRT Certification

Strategic Policy, Planning, and Leadership

www.giac.org/gstrt

IT Security Strategic Planning, Policy, and Leadership

Five-Day Program
30 CPEs
Laptop Not Needed

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams

"This course is the Rosetta Stone between an MBA and a career in cyber."

-Livingston, Deloitte

"I have been in IT 25 years. This is what I should have begun with!"

-Brian Bounds, Tx Biomedical

SANS Technology Institute

www.sans.edu

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to do three things:

Develop Strategic Plans

Strategic planning is hard for people in IT and IT security because we spend so much time responding and reacting. 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. Learn how to develop strategic plans that resonate with other IT and business leaders.

Create Effective Information Security Policy

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and your response was, "No way, I am not going to do that?" Policy must be aligned with an organization's culture. We will break down the steps to policy development so that you have the ability to develop and assess policy to successfully guide your organization.

Develop Management and Leadership Skills

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. 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. Learn to utilize management tools and frameworks to better lead, inspire, and motivate your teams.

How the Course Works

Using case studies from Harvard Business School, team-based exercises, and discussions that put students in real-world scenarios, students will participate in activities that they can then carry out with their own team members when they return to work.

The next generation of security leadership must bridge the gap between security staff and senior leadership by strategically planning how to build and run effective security programs. After taking this course you will have the fundamental skills to create strategic plans that protect your company, enable key innovations, and work effectively with your business partners.

514.1 Strategic Planning Foundations

Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

Topics: **Vision & Mission Statements; Stakeholder Management; PEST Analysis; Porter's Five Forces; Threat Actors; Asset Analysis; Threat Analysis**

514.2 Strategic Roadmap Development

With a firm understanding of business drivers as well as the threats facing the organization, you will develop a plan to analyze the current situation, identify the target situation, perform gap analysis, and develop a prioritized roadmap. In other words, you will be able to determine (1) what you do today, (2) what you should be doing in the future, (3) what you don't do, and (4) what you should do first. With this plan in place you will learn how to build and execute your plan by developing a business case, defining metrics for success, and effectively marketing your security program.

Topics: **Historical Analysis; Values and Culture; SWOT Analysis; Vision and Innovation; Security Framework; Gap Analysis; Roadmap Development; Business Case Development; Metrics and Dashboards; Marketing and Executive Communications**

514.3 Security Policy Development and Assessment

Policy is one of the key tools that security leaders have to influence and guide the organization. Security managers must understand how to review, write, assess, and support security policy and procedure. Using an instructional delivery methodology that balances lecture, exercises, and in-class discussion, this course section will teach techniques to create successful policy that users will read and follow and business leaders will accept. Learn key elements of policy, including 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.

Topics: **Purpose of Policy; Policy Gap Analysis; Policy Development; Policy Review; Awareness and Training**

514.4 Leadership and Management Competencies

Learn the critical skills you need to lead, motivate, and inspire your teams to achieve the goal. By establishing a minimum standard for the knowledge, skills, and abilities required to develop leadership you will understand how to motivate employees and develop from a manager into a leader.

Topics: **Leadership Building Blocks; Creating and Developing Teams; Coaching and Mentoring; Customer Service Focus; Conflict Resolution; Effective Communication; Leading Through Change; Relationship Building; Motivation and Self-Direction; Teamwork; Leadership Development**

514.5 Strategic Planning Workshop

Using the case study method, students will work through real-world scenarios by applying the skills and knowledge learned throughout the course. Case studies are taken directly from Harvard Business School, the pioneer of the case-study method, and focus specifically on information security management and leadership competencies. The Strategic Planning Workshop serves as a capstone exercise for the course, allowing students to synthesize and apply concepts, management tools, and methodologies learned in class.

Topics: **Creating a Security Plan for the CEO; Understanding Business Priorities; Enabling Business Innovation; Working with BYOD; Effective Communication; Stakeholder Management**

***MGT514** is available via (subject to change):*

Featured Training Events

SANSFIRE	Washington, DC	Jul 24-28
Boston	Boston, MA	Aug 7-11
Salt Lake City	Salt Lake City, UT	Aug 14-18
NETWORK SECURITY	Las Vegas, NV	Sep 11-15
Baltimore Fall	Baltimore, MD	Sep 25-29
Phoenix-Mesa	Mesa, AZ	Oct 9-13
San Francisco Winter	San Francisco, CA	Nov 27-Dec 1
Austin Winter	Austin, TX	Dec 4-8
CYBER DEFENSE INITIATIVE	Washington, DC	Dec 14-18

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- Information security managers
- SOC managers, analysts, and engineers
- Information security architects
- IT managers
- Operations managers
- Risk management professionals
- IT/System administration/Network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

You Will Be Able To

- Design security operations to address all needed functions for the organization
- Select technologies needed to implement the functions for a SOC
- Maintain appropriate business alignment with the security capability and the organization
- Develop and streamline security operations processes
- Strengthen and deepen capabilities
- Collect data for metrics, report meaningful metrics to the business, and maintain internal SOC performance metrics
- Hire appropriate SOC staff and keep existing SOC staff up to date

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organization. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the constraints of the organization. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- **Business alignment and ongoing adjustment of capabilities and objectives**
- **Designing the SOC and the associated objectives of functional areas**
- **Software and hardware technology required for performance of functions**
- **Knowledge, skills, and abilities of staff as well as staff hiring and training**
- **Execution of ongoing operations**

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organization.

Course Author Statement

The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for a specialist to look only at her piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a security operations center as a tool, and not the unification of people, processes, and technologies.

This course provides a comprehensive picture of what a Cyber Security Operations Center (CSOC or SOC) is. Discussion on the technology needed to run a SOC are handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. Staff roles needed are enumerated. Informing and training staff through internal training and information sharing is addressed. The interaction between functional areas and data exchanged is detailed.

After attending this class, the participant will have a roadmap for what needs to be done in the organization seeking to implement security operations.

-Christopher Crowley

517.1 HANDS ON: Design the Security Operations Center

We will focus on how to align and deploy a Security Operations Center (SOC). This day lays the foundational aspects of the SOC by discussing the functional areas that form the basis of the build and operate days that follow. The first issue to address is how the SOC will serve the business. To understand what is to be built, we explore the business drivers for SOCs. Each company has its own circumstances and needs, but there are common drivers for setting out to build a SOC. From business alignment, systems analysis performed shows all the things that need to be done. This is an elaborate and substantial effort to undertake. Knowing what components are available and how the pieces fit together is critical. This analysis will be followed with design and build on day 2.

Topics: SOC Fundamentals; SOC Components; Sizing and Scoping; SOC Program

517.2 HANDS ON: Build the Security Operations Center

Once a clear picture of what should be done to secure the organization is produced from analysis of what the needs are, and what resources are available, we set out to build the SOC. The build-out starts with an operating plan decided on by the key stakeholders from the organization. The interactions, inputs, outputs, and actions within each of the process components are identified. Each functional area needs specific hardware and software to accomplish each process, so alternatives are discussed for all of these. Open-source, inexpensive, and enterprise-level solutions are presented for each need. We will discuss the available solutions in-depth, and help focus the budget available on the necessary tools. The output of this day is on all the procurement necessary for building out a SOC.

Topics: Governance Structure; Process Engineering; Technical Components

517.3 HANDS ON: Operate and Mature the Security Operations Center

Designing and building-out a SOC are considered projects. Operation is an ongoing and perpetual effort. If the design of the system is insufficient or short-sighted, then operating the system will be difficult and inefficient. The overriding challenge of management is discussed in terms of organizational dimensions. The analytical processes of competing hypotheses, the kill chain, and the diamond model are discussed to provide a context for the analytical currency of the SOC. We will evaluate the staffing structure, how to hire, and how to keep those staff continually trained and updated. A schedule of meetings, specific metrics to report, and specific metrics to use to measure the relationship within the functional areas of the SOC are shown. Specific processes and the data relationships when performing the processes are discussed to depict the standard operating procedures that the SOC must carry out.

Topics: People and Processes; Measurements and Metrics; Process Development

517.4 HANDS ON: Incident Response Management – PART 1

Further detail on incident response is developed to show the operation of the SOC. Since the response component is the action of defense, the operation of the incident response team is addressed in great detail. An examination of cloud-based systems shows a special case of incident response. The preparation of response capability in the cloud is insufficient because the contractual negotiations of the service rarely address incident response adequately. We discuss appropriate preparation and response action within cloud services. User training and awareness is developed as a basis for corrective action when incident response is required.

Topics: The Cloud; Incident Response Process; Creating Incident Requirements; Training, Education, and Awareness

517.5 HANDS ON: Incident Response Management – PART 2

Continuing the operation of incident response, we discuss the staffing requirements in detail. Common caveats of incidence response operations are discussed, and table top exercises are developed to mitigate those caveats. Communication requirements are laid out and incident tracking methods are discussed. We also look at how to make the most out of a response and damage control task. Tools for estimating and tracking costs associated with incidents are demonstrated, and overall recommendations are presented on how to interface with law enforcement. The final topic addressed is the development of appropriate response techniques for APT-style actors, including strategies for quickly differentiating APT-style compromise using threat intelligence, sufficient scope identification, and eradication of the current wave of compromise.

Topics: Staffing Considerations; Setting Up Operations; Managing Daily Operations; Cost Considerations; Legal and Regulatory Issues; Advanced Threat Response

***MGT517** is available via (subject to change):*

Featured Training Events

Los Angeles – Long Beach	Long Beach, CA	Jul 10-14
SANSFIRE	Washington, DC	Jul 24-28
Chicago	Chicago, IL	Aug 21-25
Virginia Beach	Virginia Beach, VA	Aug 28 - Sep 1
NETWORK SECURITY	Las Vegas, NV	Sep 11-15
Rocky Mountain Fall	Denver, CO	Sep 25-29
San Diego	San Diego, CA	Oct 30-Nov 3
San Francisco Winter	San Francisco, CA	Nov 27-Dec 1
Austin Winter	Austin, TX	Dec 4-8

"SANS coursework is the most thorough learning available anywhere. What you learn is not only conceptual, but also hands-on, showing you what to do, why you do it, and how you can apply solutions that you learn to real-world problems."

-Duane Tucker, Barmark Partners

MGT525

GCPM Certification
Project Manager

www.giac.org/gcpm

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

Six-Day Program
36 CPEs
Laptop Not Needed

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

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

This course is offered by the SANS Institute as 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. PMP® is a registered trademark of Project Management Institute, Inc.

This course has been recently updated to fully prepare you for the 2016 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide – 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, and to completing, closing, and documenting as your project finishes. A copy of the *PMBOK® Guide – Fifth Edition* is provided to all participants. You can reference the *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the 2016 updated Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

"Honestly, this is one of the best courses I have had to date. I feel like I have thousands of things to take back to my job."

-Ryan Spencer, Reed Elsevier Inc.

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.

SANS Technology Institute

www.sans.edu

PMI Registered Education Provider — Project Management Institute

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 your project is well defined from the outset. 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**

525.5 Quality and Risk Management

On day five you will become familiar with quality planning, assurance, and 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 how to understand and use 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**

***MGT525** is available via (subject to change):*

Featured Training Events

SANSFIRE . . . . . Washington, DC . . . . . Jul 24-29

NETWORK SECURITY. . . . Las Vegas, NV . . . . . Sep 10-15

Private Training

All SANS courses are available through Private Training.

Course Author Statement

Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service-based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential.
-Jeff Frisk

"SANS offers relevant, practical and highly informative courses that are taught by instructors who truly understand the content."

-Tyler Leet, Computer Services, Inc.

AUD507

GSNA Certification
Systems and Network Auditor

www.giac.org/gsna

Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program
36 CPEs
Laptop Required

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

You Will Be Able To

- Understand the different types of controls (e.g., technical vs. non-technical) essential to perform a successful audit
- Conduct a proper risk assessment of a 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 application 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

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? How do we turn this into a continuous monitoring process? 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 are taken from real-world examples.

"The entire course has been fantastic – it far exceeded my expectations. I think SANS training is far superior to other training programs."
-Paul Petrasko, Bemis Company

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that these controls address. In this course these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and 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 her own Windows 7 Professional 64 bit or higher laptop for use during class. The ideal laptop will have at least 4 gigabytes of RAM.

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 gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

SANS Technology Institute
www.sans.edu

MEETS DoDD 8140 (8570) REQUIREMENTS
www.sans.org/8140

***AUD507** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV ..... Sep 10-15

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

LEG523

GLEG Certification
Law of Data Security & Investigations

www.giac.org/gleg

Law of Data Security and Investigations

Five-Day Program
30 CPEs
Laptop Not Needed

Who Should Attend

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

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate technology law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)

NEW!

- **Form contract for inviting outside incident responders - including police, contractors, National Guard, or civil defense agency anywhere in the world - to help with a cyber crisis**
- **EU's new General Data Protection Regulation and its impact around the world**
- **The impact of Trump presidency and Brexit on data security law and regulatory enforcement**
- **The EU's adoption of "Privacy Shield" to replace "Privacy Safe Harbor" for transferring data to the United States**
- **Cyber insurer's lawsuit against hospital to deny coverage after data breach and $4.1 million legal settlement with patients**

New laws on privacy, e-discovery and data security are creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. 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 laws 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.

"Outstanding instructor! Keep doing what you are doing."
-Paul Mobley, FIS Global

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.

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.

SANS Technology Institute
www.sans.edu

***LEG523** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-28
NETWORK SECURITY. . . . Las Vegas, NV ..... Sep 11-15

Summit Events

Data Breach – Chicago, IL ..... Sep 27 - Oct 1

OnDemand

E-learning available anytime, anywhere, at your pace

vLive Events

Virtual/Online ..... Oct 10 - Nov 9

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

DEV522

GWEB Certification
Web Application Defender

www.giac.org/gweb

Defending Web Applications Security Essentials

Six-Day Program
36 CPEs
Laptop Required

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

You Will Be Able To

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfill the training requirement as stated in PCI DSS 6.5
- Deploy and consume web services (SOAP and REST) in a more secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program in a large environment
- Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- Develop strategies to assess the security posture of multiple web applications

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

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you 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 applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

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

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

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. 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 and conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

"DEV522 goes over security issues that every web developer and appsec employee needs."

-Allen Ott, Boeing

SANS Technology Institute

www.sans.edu

522.1 HANDS ON: Web Basics and Authentication Security

We begin day one with an overview of recent web application attack and security trends, then follow up by examining the essential technologies that are at play in web applications. You cannot win the battle if you do not understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

522.2 HANDS ON: Web Application Common Vulnerabilities & Mitigations

Since the Internet does not guarantee the secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. This course day covers the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

Topics: SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-site Request Forgery; Business Logic Flaws; Concurrency; Input-related Flaws and Related Defenses; SQL Injection Vulnerabilities, Testing, and Defense

522.3 HANDS ON: Proactive Defense and Operation Security

Day three begins with a detailed discussion on cross-site scripting and related mitigation and testing strategies, as well as HTTP response splitting. The code in an application may be totally locked down, but if the server setting is insecure, the server running the application can be easily compromised. Locking down the web environment is essential, so we cover this basic concept of defending the platform and host. To enable any detection of intrusion, logging and error handling must be done correctly. We will discuss the correct approach to handling incidents and logs, then dive even further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

Topics: Cross-site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Applications; Incident Handling; Honeytoken

522.4 HANDS ON: AJAX and Web Services Security

Day four is dedicated to the security of asynchronous JavaScript and XML (AJAX) and web services, which are currently the most active areas in web application development. Security issues continue to arise as organizations dive head first into insecurely implementing new web technologies without first understanding them. We will cover security issues, mitigation strategies, and general best practices for implementing AJAX and web services. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. Discussion focuses on the web services in the morning and AJAX technologies in the afternoon.

Topics: Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

522.5 HANDS ON: Cutting-Edge Web Security

Day five focuses on cutting-edge web application technologies and current research areas. Topics such as clickjacking and DNS rebinding are covered. These vulnerabilities are difficult to defend and multiple defense strategies are needed for their defense to be successful. Another topic of discussion is the new generation of single-sign-on solutions such as OpenID. We cover the implications of using these authentication systems and the common "gotchas" to avoid. With the Web2.0 adoption, the use of Java applet, Flash, ActiveX, and Silverlight are on the increase. The security strategies of defending these technologies are discussed so that these client-side technologies can be locked down properly.

Topics: Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single-Sign-On Solution and Security; IPv6 Impact on Web Security

522.6 HANDS ON: Capture and Defend the Flag Exercise

Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the focus is a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, and then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. Students will learn through these hands-on exercises how to secure the web application, starting with the operating system, the web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.

Topics: Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation

***DEV522** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-29
NETWORK SECURITY. . . . Las Vegas, NV ..... Sep 10-15
Seattle ..... Seattle, WA ..... Oct 30 - Nov 4
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

Summit Events

Secure DevOps – Denver, CO ..... Oct 12-17

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

Course Author Statement

Too many websites are getting compromised these days. The goal of DEV522 is to arm students with defensive strategies that can work for all web applications. We all know it is very difficult to defend a web application because there are so many different types of vulnerabilities and attack channels. Overlook one thing and your web app is owned. The defensive perimeter needs to extend far beyond just the coding aspects of web application. This course covers the security vulnerabilities so that students have a good understanding of the problems at hand. We then provide the defensive strategies and tricks, as well as the overall architecture, that have been proven to help secure sites. I have also included some case studies throughout the course so we can learn from the mistakes of others and make our own defense stronger. The exercises in class are designed to help you further your understanding and help you retain this knowledge through hands-on practice. By the end of the course, you will have the practical skills and understanding of the defensive strategies to lock down existing applications and build more secure applications in the future.

- Jason Lam

DEV541

GSSP-JAVA Certification
Secure Software Programmer – Java

www.giac.org/gssp-java

Secure Coding in Java/JEE: Developing Defensible Applications

Four-Day Program
24 CPEs
Laptop Required

Who Should Attend

- Developers who want to build more secure applications
- Java Enterprise Edition (JEE) programmers
- 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 who want a deeper understanding of target applications or who want to provide more detailed vulnerability remediation options

You Will Be Able To

- Use a web application proxy to view and manipulate HTTP requests and responses
- Review and perform basic exploits of common web application vulnerabilities, such as those found among the SANS/CWE Top 25 Most Dangerous Software Errors and the OWASP Top 10
- Mitigate common web application vulnerabilities using secure coding practices and Java libraries
- Build applications using:
  - Java Enterprise Edition authentication
  - Basic and form-based authentication
  - Client certificates
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
  - Java Secure Sockets Extension
  - Secure password storage techniques
  - Java Cryptography Architecture
  - Security Manager
- Implement a secure software development lifecycle, including code review, static analysis and dynamic analysis techniques

This secure coding course will teach students how to build secure Java applications and gain the knowledge and skills to keep a website from getting hacked, counter a wide range of application attacks, prevent critical security vulnerabilities that can lead to data loss, and understand the mindset of attackers.

The course teaches you the art of modern web defense for Java applications by focusing on foundational defensive techniques, cutting-edge protection, and Java EE security features you can use in your applications as soon as you return to work. This includes learning how to:

- **Identify security defects in your code**
- **Fix security bugs using secure coding techniques**
- **Utilize secure HTTP headers to prevent attacks**
- **Secure your sensitive representational state transfer (REST) services**
- **Incorporate security into your development process**
- **Use freely available security tools to test your applications**

Great developers have traditionally distinguished themselves by the elegance, effectiveness and reliability of their code. That is still true, but the security of the code now needs to be added to those other qualities. This unique SANS course allows you to hone the skills and knowledge required to prevent your applications from getting hacked.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications is a comprehensive course covering a wide set of skills and knowledge. It is not a high-level theory course – it is about real-world, hands-on programming. You will examine actual code, work with real tools, build applications and gain confidence in the resources you need to improve the security of Java applications.

Rather than teaching students to use a given set of tools, the course covers 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 course culminates in a Secure Development Challenge in which students perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and implement fixes for these issues using the secure coding techniques that you have learned in course.

***DEV541** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-27
NETWORK SECURITY .... Las Vegas, NV ..... Sep 11-14

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

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.

DEV544

GSSP-.NET Certification
Secure Software Programmer – .NET

www.giac.org/gssp-net

Secure Coding in .NET: Developing Defensible Applications

Four-Day Program
24 CPEs
Laptop Required

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

You Will Be Able To

- Use a web application proxy to view HTTP requests and responses
- Review and perform basic exploits of common .NET web application vulnerabilities, such as those found in the SANS/CWE Top 25 and the OWASP Top 10
- Mitigate common web application vulnerabilities using industry best practices in the .NET framework
- Understand built-in ASP .NET security mechanisms
- Apply industry best practices (NIST, PCI) for cryptography and hashing in the .NET framework
- Implement a secure software development lifecycle (SDLC) to include threat modeling, static analysis and dynamic analysis

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?

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.

"It is shocking to see how much we are missing in our code. I am going back to change the code immediately."

-Ruojie Wang,
New Jersey Hospital Association

***DEV544** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-27
NETWORK SECURITY .... Las Vegas, NV ..... Sep 11-14

OnDemand

E-learning available anytime, anywhere, at your pace

SelfStudy

Individual study with course books and lecture MP3s.

Private Training

All SANS courses are available through Private Training.

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.

ICS410

ICS/SCADA Security Essentials

GICSP Certification
Industrial Cyber Security Professional

www.giac.org/gicsp

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

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

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

You Will Be Able To

- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems' lifecycles
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

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

The course will provide you with:

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

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

"Best training course I've taken in 25+ years."
-Curt Imanse, Accenture

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

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

SANS Technology Institute

www.sans.edu

410.1 ICS Overview

Students will develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Field Components; Programming Controllers; Supervisory Components; Types of ICS Systems; IT & ICS Differences; Physical Security; ICS Network Architecture

410.2 ICS Attack Surface

If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Day 2, defenders will develop a better understanding of where these specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them. Each student will use a vulnerable target virtual machine to further understand attacks targeting the types of web servers used on many ICS devices for management purposes. Simulators will be configured to allow students to conduct attacks against unauthenticated ICS protocols. A variety of data samples are used to examine additional attack vectors on remote devices.

Topics: ICS Attack Surface; Attacks on HMIs and UIs; Attacks on Control Servers; Attacks on Network Communications; Attacks on Remote Devices

410.3 Defending ICS Servers and Workstations

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. We'll examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.

Topics: Windows in ICS; Linux/Unix in ICS; Updates and Patching; Processes and Services; Configuration Hardening; Endpoint Defenses; Automation and Auditing; Log Management; Databases and Historians

410.4 Defending ICS Networks and Devices

With an understanding of the ICS environment, the attack vectors that exist, and the defender-specific capabilities available on servers, workstations, and applications, students will now learn network-specific defense approaches. We'll first examine common IT protocols and network components used within ICS environments, then discuss ICS-specific protocols and devices. Technologies used to defend ICS networks will be reviewed along with implementation approaches. Students will interact with ICS traffic and develop skills to analyze it, then work through a number of tools to further explore a series of staged adversary actions conducted in a lab environment.

Topics: Network Fundamentals; Ethernet; TCP/IP Protocol Suite; ICS Protocols over TCP/IP; Enforcement Zone Devices; Honeypots; Wireless in Control Systems; Network Capture Forensics; Field and Plant Floor Equipment; Cryptography Fundamentals

410.5 ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Topics: Information Assurance Foundations; Security Policies; Contingency and Continuity Planning; Risk Assessment and Auditing; Attack Tree Analysis; Password Management; Incident Handling; Incident Response

***ICS410** is available via (subject to change):*

Featured Training Events

SANSFIRE ..... Washington, DC ..... Jul 24-28
Salt Lake City ..... Salt Lake City, UT ..... Aug 14-18
NETWORK SECURITY ..... Las Vegas, NV ..... Sep 11-15
San Diego ..... San Diego, CA ..... Oct 30-Nov 3
CYBER DEFENSE INITIATIVE Washington, DC ..... Dec 14-19

Summit Events

ICS & Energy – Houston, TX ..... Jul 10-14

OnDemand

E-learning available anytime, anywhere, at your pace

Event Simulcast

Virtual/Online ..... Oct 30 - Nov 3

Custom Simulcast

Customized training for distributed workforces

SelfStudy

Individual study with course books and lecture MP3s.

Community SANS Events

Philadelphia, PA ..... Jul 17-21
Ottawa, ON ..... Sep 11-15

Private Training

All SANS courses are available through Private Training.

"Great introduction into ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company."

-Mike Poulos, Coca-Cola Enterprises

ICS515

GRID Certification
Response and Industrial Defense

www.giac.org/grid

ICS Active Defense and Incident Response

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center (SOC) team leads and analysts
- ICS red team and penetration testers
- Active defenders

You Will Be Able To

- How to perform ICS incident response focusing on security operations and prioritizing the safety and reliability of operations.
- How ICS threat intelligence is generated and how to use what is available in the community to support ICS environments. The analysis skills you learn will enable you to critically analyze and apply information from ICS threat intelligence reports on a regular basis.
- How to identify ICS assets and their network topologies and how to monitor ICS hotspots for abnormalities and threats. Methodologies such as ICS network security monitoring and approaches to reducing the control system threat landscape will be introduced and reinforced.
- How to analyze ICS malware and extract the most important information needed to quickly scope the environment and understand the nature of the threat.
- How to operate through an attack and gain the information necessary to instruct teams and decision-makers on when operations must shut down, or if it is safe to respond to the threat and continue operations.
- How to use multiple security disciplines in conjunction with each other to leverage an active defense and safeguard the ICS, all reinforced with hands-on labs and technical concepts.

ICS515: ICS Active Defense and Incident Response will help you deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations.

This course will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

This course will prepare you to:

- **Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats**
- **Use active defense concepts such as threat intelligence consumption, network security monitoring, malware analysis, and incident response to safeguard the ICS**
- **Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends**
- **Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others**
- **Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more**
- **Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII**
- **Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security**

"The course was like a catalyst. It boosted my knowledge about the threats facing ICS environments and provided me with a framework to actively defend these threats. Additionally, it inspired me to learn more."

-Srinath Kannan, Accenture

515.1 HANDS ON: Threat Intelligence

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), and guide security teams to find threats in the environment. Today you will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This day features four hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

Topics: Case Study: Havex; Introduction to ICS Active Defense and Incident Response; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; External ICS Threat Intelligence; Internal ICS Threat Intelligence; Sharing and Consuming ICS Threat Intelligence

515.2 HANDS ON: Asset Identification and Network Security Monitoring

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach students to use tools such as Wireshark, TCPdump, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and analyze the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

Topics: Case Study: BlackEnergy2; ICS Asset and Network Visibility; Identifying and Reducing the Threat Landscape; ICS Network Security Monitoring – Collection; ICS Network Security Monitoring – Detection; ICS Network Security Monitoring – Analysis

515.3 HANDS ON: Incident Response

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept in an ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but students in this section will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use this data to perform timely forensic analysis and create IOCs. In the previous section's labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

Topics: Case Study: Stuxnet; Incident Response and Digital Forensics Overview; Preparing an ICS Incident Response Team; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Time-Critical Analysis; Maintaining and Restoring Operations

515.4 HANDS ON: Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section's labs identified the infected HMI and gathered a sample of the APT malware. In this section's labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

Topics: Case Study: German Steelworks; ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Analyzing Acquired Evidence; Memory Forensics; Malware Analysis Methodologies; Case Study: BlackEnergy2 Automated Analysis; Indicators of Compromise; Environment Manipulation

515.5 HANDS ON: Active Defense and Incident Response Challenge

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

Topics:

Scenario One: Identify the Assets and Map the ICS Networks; Perform ICS Network Security Monitoring to Identify the Abnormalities; Execute ICS Incident Response Procedures Into the SANS Cyber City Data Files; Analyze the Malicious Capability and Determine if the Threat is an Insider Threat or a Targeted External Threat

Scenario Two: Identify the Software and Information Present on the DCS; Leverage ICS Active Defense Concepts to Identify the Real-World Malware; Determine the Impact on Operations and Remediation Needs

***ICS515** is available via (subject to change):*

Featured Training Events

CYBER DEFENSE INITIATIVE Washington, DC . . . . . Dec 14-19

Summit Events

ICS & Energy – Houston, TX . . . . . Jul 10-14

Private Training

All SANS courses are available through Private Training.

Course Author Statement

This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is do-able.
- Robert M. Lee

"Awesome!! This course was my sixth SANS course, and Robert M. Lee demonstrated and reiterated the fact that SANS has the world's best instructors."
-Srinath Kannan, Accenture

"Very powerful tools and concepts!"
-Randy Wagner, Basin Electric

ICS456

Essentials for NERC Critical Infrastructure Protection

Five-Day Program
30 CPEs
Laptop Required

Who Should Attend

Individuals with CIP responsibilities in the following areas:

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations
- Incident response
- Compliance staff
- Team leaders
- Governance
- Vendors/Integrators
- Auditors

***ICS456** is available via (subject to change):*

Featured Training Events

Chicago ..... Chicago, IL ..... Aug 21-25
San Diego ..... San Diego, CA ... Oct 30 - Nov 3
Austin Winter..... Austin, TX ..... Dec 4-8

Summit Events

ICS & Energy – Houston, TX ..... Jul 10-14

The Essentials for NERC Critical Infrastructure Protection 5-day course empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance. Our 25 hands-on labs range from securing workstations to digital forensics and lock picking.

Course Day Descriptions

456.1 HANDS ON: Asset Identification and Governance

A transition is underway from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. In day 1 students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. The day will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario based competition that helps bring the concepts to life and highlights the important role we play in defending 'the grid.

456.2 HANDS ON: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During day 2 we move beyond the "what" of CIP compliance to understanding the "why" and the "how." Firewalls, proxies, gateways, IDS and more - learn where and when they help and learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you'll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will re-inforce the learnings throughout the day and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

456.3 HANDS ON: System Management

CIP-007 has consistently been one of the most violated Standards going back to CIP version 1. With the CIP Standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout day 3, students will dive into CIP-007. We'll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This day will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We'll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

456.4 HANDS ON: Information Protection and Response

Education is key to every organization's success with NERC CIP and the students in ICS 456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, each student can be a valued resource to their organization's CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. In day 4 we'll examine CIP-008 and CIP-009 covering identification, classification communication of incidents as well as the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs in day 4 will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

456.5 HANDS ON: CIP Process

On the final day students will learn the key components for running an effective CIP Compliance program. We will review the NERC processes for standards development, violation penalty determination, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally we'll identify recurring and audit related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFE's, and self-reporting. We'll also look at the challenge of preparing for NERC audits and provide tips to be prepare to demonstrate the awesome work your team is doing. Finally, we'll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of day 5 students will have a strong call to action to participate in the on-going development of CIP within their organization and in the industry overall as well as a sense that CIP is doable! Labs in day 5 will cover DOE C2M2, audit tools, and an audit focused take on 'blue team - red team' exercise.

ADDITIONAL TRAINING COURSES

Cyber Defense SHORT COURSES

SEC440: Critical Security Controls: Planning, Implementing, and Auditing (2 DAYS)

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These 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 known attacks and help find and mitigate damage from the attacks that get through.

SEC440 Training Events

SANSFIRE ..... Washington, DC. ... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE INITIATIVE ..... Washington, DC. ... Dec 12-13

SEC440 Summit Events

Data Breach – Chicago, IL ..... Sep 27-28

SEC440 Community SANS Events

Fullerton, CA ..... Jul 20-21
Denver, CO ..... Aug 3-4
Atlanta, GA ..... Aug 7-8
Las Vegas, NV ..... Aug 17-18
Pittsburgh, PA ..... Aug 30-31

SEC440 Mentor Classes

Riverside, CA ..... Aug 23 - Sep 6

SEC524: Cloud Security Fundamentals (2 DAYS)

This course will go in-depth into 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.

SEC524 Training Events

SANSFIRE ..... Washington, DC. ... Jul 22-23
CYBER DEFENSE INITIATIVE ..... Washington, DC. ... Dec 12-13

SEC546: IPv6 Essentials (2 DAYS)

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

SEC546 Training Events

SANSFIRE ..... Washington, DC. ... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE INITIATIVE ..... Washington, DC. ... Dec 12-13

Penetration Testing SHORT COURSES

SEC567: Social Engineering for Penetration Testers (2 DAYS)

This course covers the principles of persuasion and the psychological foundations required to craft effective attacks and bolsters this with many examples of what works, drawing on cyber criminal cases and on the experiences of the authors in combating cyber crime. On top of these principles we provide a number of tools and labs centered around the key technical skills required to measure your social engineering success and report it to your company or client.

SEC567 Training Events

SANSFIRE ..... Washington, DC. ... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE INITIATIVE ..... Washington, DC. ... Dec 12-13

SEC567 Summit Events

Security Awareness – Nashville, TN .. Jul 31 - Aug 1

SEC580: Metasploit Kung Fu for Enterprise Pen Testing (2 DAYS)

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.

SEC580 Training Events

SANSFIRE ..... Washington, DC. ... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE INITIATIVE ..... Washington, DC. ... Dec 12-13

SEC580 Community SANS Events

Columbia, MD ..... Mar 20-21

ADDITIONAL TRAINING COURSES

Management & Audit SHORT COURSES

MGT305: Technical Communication and Presentation Skills for Security Professionals (1 DAY)

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

MGT305 Training Events

SANSFIRE ..... Washington, DC..... Jul 23

MGT305 Summit Events

Security Awareness – Nashville, TN . . Jul 31 - Aug 1

MGT415: A Practical Introduction to Cybersecurity Risk Management (2 DAYS)

There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore all organizations, whether they do so in an organized manner or not, will make priority decisions on how best to defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

MGT415 Training Events

SANSFIRE ..... Washington, DC.... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE
INITIATIVE ..... Washington, DC.... Dec 12-13

MGT415 Summit Events

Data Breach – Chicago, IL ..... Sep 27-28

MGT433: Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program (2 DAYS)

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world.

MGT433 Training Events

SANSFIRE ..... Washington, DC.... Jul 22-23
NETWORK SECURITY Las Vegas, NV ..... Sep 16-17
CYBER DEFENSE
INITIATIVE ..... Washington, DC.... Dec 12-13

MGT433 Summit Events

Security Awareness – Nashville, TN . . Jul 31 - Aug 1
Data Breach – Chicago, IL ..... Sep 27-28

MGT535: Incident Response Team Management (2 DAYS)

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense. Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge.

Software Security SHORT COURSES

DEV531: Defending Mobile Apps Security Essentials *NEW!* (2 DAYS)

This course covers the most prevalent mobile app risks, including those from the OWASP Mobile Top 10. Students will participate in numerous hands-on exercises available in both the Android and iOS platforms. Each exercise is designed to reinforce the lessons learned throughout the course, ensuring that you understand how to properly defend your organization's mobile applications.

DEV531 & DEV534 Training Events

SANSFIRE .....Washington, DC . . Jul 22-23
NETWORK SECURITY . .Las Vegas, NV . . . Sep 16-17
CYBER DEFENSE
INITIATIVE (DEV534) . .Washington, DC . . Dec 12-13

DEV531 & DEV534 Summit Events

Secure DevOps – Denver, CO .....Oct 12-13

DEV534: Secure DevOps: A Practical Introduction *NEW!* (2 DAYS)

This course explains the fundamentals of DevOps, and how DevOps teams can build and deliver secure software. It will explain the principles and practices and tools in DevOps and how they can be leveraged to improve the reliability, integrity and security of systems.

DEV543: Secure Coding in C & C++ (2 DAYS)

The C and C++ programming languages are the bedrock for most operating systems, major network services, embedded systems and system utilities. Even though C and, to a lesser extent, C++, are well understood languages, the flexibility of the language and inconsistencies in the standard C libraries have led to an enormous number of discovered vulnerabilities over the years. The unfortunate truth is that there are probably more undiscovered vulnerabilities than there are known vulnerabilities! This course will cover all of the most common programming flaws that affect C and C++ code.

SANS Hosted **TRAINING COURSES**

SANS Hosted is a series of courses presented by other educational providers to complement your needs for training outside of our current course offerings. A complete list of Hosted courses and descriptions is available at at www.sans.org/courses/hosted.

Assessing and Exploiting Control Systems

Six Days | 36 CPEs | Laptop Required

This is not your traditional SCADA/ICS/IoT security course! How many courses send you home with your own PLC and a set of hardware/RF hacking tools?!? This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. This course is structured around the formal penetration testing methodology created by UtiliSec for the United States Department of Energy. Using this methodology and Control Things Pentest Platform (previously SamuraiSTFU), an open source Linux distribution for pentesting energy sector systems and other critical infrastructure, we will perform hands-on penetration testing tasks on user interfaces (on master servers and field device maintenance interfaces), control system protocols (modbus, DNP3, IEC 60870-5-104), RF communications (433MHz, 869MHz, 915MHz), and embedded circuit attacks (memory dumping, bus snooping, JTAG, and firmware analysis).

Critical Infrastructure and Control System Cybersecurity

Five Days | 30 CPEs | Laptop Provided

This is an intermediate to advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. This course will provide hands-on analysis of control system environments allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls.

Topics:

- Attendee Laboratory Training Kit Details
- Hands-on Critical Infrastructure Control System Cybersecurity 5-Day Course
- Roadmap and Overview
- Course Ethics and General Security Awareness
- Critical Infrastructure Control System Cybersecurity Background
- Control System Cyber Architecture and Device Programming
- Cyber Asset Vulnerability Assessments
- Automation Technologies Attack Surface and Mitigations
- Communications Attack Surface and Mitigations
- OLE for Process Control / Human Machine Interface Attack Surface and Mitigations
- Integrated Defense in Depth Security Controls

Physical Security Specialist – Full Comprehensive Edition

Six Days | 36 CPEs | Laptop Required

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.

The CORE Group is a firm with divisions that focus on penetration testing, physical defense, personal protection details, and law enforcement training. Those who attend this course 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. Our subject matter experts will immerse you in all the necessary components of a well-layered physical defense system and then teach you how to conduct a thorough site analysis of a facility.

This training is ideal for any individual who is tasked with making physical security decisions for existing or new facilities.

Health Care Security Essentials

Two Days | 12 CPEs | Laptop Required

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.

Physical Penetration Testing

Two Days | 12 CPEs

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.

Voucher Program

The SANS Voucher Program allows organizations to:

- Centrally administer their employee training and budget
- Potentially receive bonus funds based on their investment

Training Investment & Bonus Funds

To open a Voucher Account, an organization pays an agreed-upon training investment. Based on the amount of the training investment, that organization could be eligible to receive bonus funds.

Investment and bonus funds:

- Can be applied to any live or online SANS training course, SANS Summit, GIAC certification, or certification renewal*
- Can be increased at any time by making additional investments
- Need to be utilized within 12 months; however, the term can be extended by investing additional funds before the end of the 12-month term

*Current exceptions are the Partnership Program, Security Awareness Training, and SANS workshops hosted at events run by other companies.

Flexibility & Control

The online SANS Admin Tool allows organizations to manage their training at any time and from anywhere.

With the SANS Admin Tool, the Administrator can:

- Approve and manage student enrollment
- View fund usage in real time
- View students' certification status and test results
- Obtain OnDemand course progress by student per course

Get Started

Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little as one week, your employees can begin their training.

www.sans.org/vouchers

Future Training Events

Los Angeles – Long Beach	Long Beach, CA	Jul 10-15
SANSFIRE	**Washington, DC**	**Jul 22-29**
San Antonio	San Antonio, TX	Aug 6-11
Boston	Boston, MA	Aug 7-12
New York City	New York, NY	Aug 14-19
Salt Lake City	Salt Lake City, UT	Aug 14-19
Chicago	Chicago, IL	Aug 21-26
Virginia Beach	Virginia Beach, VA	Aug 21 - Sep 1
Tampa-Clearwater	Clearwater, FL	Sep 5-10
San Francisco Fall	San Francisco, CA	Sep 5-10
Network Security	**Las Vegas, NV**	**Sep 10-17**
Baltimore Fall	Baltimore, MD	Sep 25-30
Rocky Mountain Fall	Denver, CO	Sep 25-30
Phoenix-Mesa	Mesa, AZ	Oct 9-14
Tysons Corner Fall	McLean, VA	Oct 16-21
San Diego	San Diego, CA	Oct 30 - Nov 4
Seattle	Seattle, WA	Oct 30 - Nov 4
Miami	Miami, FL	Nov 6-11
San Francisco Winter	San Francisco, CA	Nov 27 - Dec 2
Austin Winter	Austin, TX	Dec 4-9
Cyber Defense Initiative	**Washington, DC**	**Dec 12-19**

Future Summit Events

ICS & Energy	Houston, TX	Jul 10-15
Security Awareness	Nashville, TN	Jul 31 - Aug 9
Data Breach	Chicago, IL	Sep 25 - Oct 2
Secure DevOps	Denver, CO	Oct 10-17
Pen Test Hackfest	Bethesda, MD	Nov 13-20

Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit **www.sans.org/community** for up-to-date Community course information.

Private Training

SANS Institute's private information security training options allow your organization to build custom training programs for any group of 25 students or more, anywhere in the world. We can deliver our world-class courses and certified instructors live onsite, online, or via a combination of live and online using our Simulcast technology. Visit **www.sans.org/private-training** to learn more.

SANS OnDemand

Take SANS Training Anytime, Anywhere with OnDemand

More than 30 of SANS most popular courses are available in our online training format OnDemand, and all include:

- Four months of online access to your course
- Subject-matter-expert support
- Train with SANS top instructors
- All printed books and materials
- Labs and quizzes to reinforce your learning
- No travel required

Visit www.sans.org/ondemand to learn more about your OnDemand training options.

Create a **SANS Account** today to enjoy these FREE resources:

WEBCASTS

Ask The Expert Webcasts – SANS experts bring current and timely information on relevant topics in IT Security.

Analyst Webcasts – A follow-on to the SANS Analyst Program, Analyst Webcasts provide key information from our whitepapers and surveys.

WhatWorks Webcasts – The SANS WhatWorks webcasts bring powerful customer experiences showing how end users resolved specific IT Security issues.

Tool Talks – Tool Talks are designed to give you a solid understanding of a problem, and how a vendor's commercial tool can be used to solve or mitigate that problem.

NEWSLETTERS

NewsBites – Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals

OUCH! – The world's leading free monthly security awareness newsletter designed for the common computer user

@RISK: The Consensus Security Alert – A reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) how recent attacks worked, and (4) other valuable data

OTHER FREE RESOURCES

- InfoSec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Intrusion Detection FAQs
- Tip of the Day
- Security Posters
- Thought Leaders
- 20 Coolest Careers
- Security Glossary
- SCORE (Security Consensus Operational Readiness Evaluation)

www.sans.org/account