Network Security 2018
Las Vegas | September 23-30

Protect Your Business | Advance Your Career
Over 40 hands-on, immersion-style courses taught by real-world practitioners

See inside for courses offered in:
- Cyber Defense
- Detection & Monitoring
- Optimizing SIEMs
- Penetration Testing
- Ethical Hacking
- Incident Response
- ICS/SCADA Security
- Digital Forensics
- Security Management
- Secure Development
- Audit
- Legal

“SANS training is the best in the industry and can’t be beat. What I learned at SANS I will continue to use throughout my career.”
Charles Chastain, Patagonia

SAVE $400
Register and pay by August 1st
Use code EarlyBird18

www.sans.org/network-security-2018
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.

“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)
The 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 65 unique courses are designed to align with dominant security team roles, duties, and disciplines. The courses 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, Penetration Testing, Industrial Control Systems Security, Secure Software Development, and more. Each curriculum area 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 most cutting-edge 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 designed for them to 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.

**SKILLS VALIDATION**
GIAC exams and certifications ensure that professionals have learned and can apply the real-world knowledge and skills taught in class. More than 30 certifications align with SANS training and ensure mastery in critical, specialized InfoSec domains and job-specific roles. See [www.giac.org](http://www.giac.org) for more information.

**SANS FORMATS**
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 around the world 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.

**THE SANS PROMISE**
At the heart of everything we do is the SANS Promise: Students will be able to use the new skills they’ve learned as soon as they return to work.

**HOW TO REGISTER FOR SANS TRAINING**
Students can learn more and register online by visiting [www.sans.org](http://www.sans.org).
Fewer than 100 individuals are currently qualified and designated to teach as SANS Instructors, globally. This select group of professionals includes recognized industry experts and real-world practitioners, all of whom have proven to be engaging teachers in the classroom. Their up-to-date examples and deep knowledge ensure that what you learn in class will be relevant to your job.

For instructor bios, visit: [www.sans.org/instructors](http://www.sans.org/instructors)

The lineup of SANS Instructors for SANS Network Security 2018 includes:

- **Heather Mahalik**
  - Senior Instructor
  - @HeatherMahalik
  - Teaching FOR585

- **Chris Christianson**
  - Certified Instructor
  - @cchristianson
  - Teaching SEC440

- **Aaron Cure**
  - Instructor
  - Teaching DEV544

- **Jason Fossen**
  - Faculty Fellow
  - @JasonFossen
  - Teaching SEC505

- **Philip Hagen**
  - Senior Instructor
  - @PhilHagen
  - Teaching FOR572

- **Moses Hernandez**
  - Certified Instructor
  - @moshesrenegade
  - Teaching SEC542

- **John Hubbard**
  - Instructor
  - @SecHubb
  - Teaching SEC455

- **Rob Lee**
  - Faculty Fellow
  - @roblee, @sansforensics
  - Teaching FOR500

- **Eric Conrad**
  - Faculty Fellow
  - @eric_conrad
  - Teaching SEC530

- **Adrien de Beaupre**
  - Certified Instructor
  - @adriendb
  - Teaching SEC642

- **Jeff Frisk**
  - Certified Instructor
  - Teaching MGT525

- **G. Mark Hardy**
  - Principal Instructor
  - @g_mark
  - Teaching MGT512

- **David Hoelzer**
  - Faculty Fellow
  - @it_audit
  - Teaching SEC503

- **Eric Johnson**
  - Certified Instructor
  - @emjohn20
  - Teaching DEV540

- **Frank Kim**
  - Senior Instructor
  - @fykim
  - Teaching MGT514

- **Micah Hoffman**
  - Certified Instructor
  - @WebBreacher
  - Teaching SEC487

- **Gregory Leonard**
  - Certified Instructor
  - @appsecgreg
  - Teaching DEV531

- **Mark Baggett**
  - Senior Instructor
  - @MarkBaggett
  - Teaching SEC573

- **Christopher Crowley**
  - Principal Instructor
  - @CCrowMontance
  - Teaching MGT517

- **Sarah Edwards**
  - Certified Instructor
  - @iamevltwin
  - Teaching FOR518

- **Bryce Galbraith**
  - Principal Instructor
  - @brycegalbraith
  - Teaching SEC501

- **Justin Henderson**
  - Certified Instructor
  - @SecurityMapper
  - Teaching SEC555

- **Eric Conrad**
  - Faculty Fellow
  - @eric_conrad
  - Teaching SEC530

- **Christopher Crowley**
  - Principal Instructor
  - @CCrowMontance
  - Teaching MGT517

- **Mark Baggett**
  - Senior Instructor
  - @MarkBaggett
  - Teaching SEC573
<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Social Media</th>
<th>Course Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeff McJunkin</td>
<td>Certified Instructor</td>
<td>@jeffmcjunkin</td>
<td>SEC580</td>
</tr>
<tr>
<td>Seth Misenar</td>
<td>Faculty Fellow</td>
<td>@sethmisenar</td>
<td>SEC511</td>
</tr>
<tr>
<td>Larry Pesce</td>
<td>Certified Instructor</td>
<td>@haxorthematrix</td>
<td>SEC617</td>
</tr>
<tr>
<td>Dave Shackleford</td>
<td>Senior Instructor</td>
<td>@daveshackleford</td>
<td>SEC545</td>
</tr>
<tr>
<td>Ed Skoudis</td>
<td>Faculty Fellow</td>
<td>@edskoudis</td>
<td>SEC560</td>
</tr>
<tr>
<td>Peter Szczepankiewicz</td>
<td>Certified Instructor</td>
<td>@_s14</td>
<td>FOR578</td>
</tr>
<tr>
<td>Alissa Torres</td>
<td>Certified Instructor</td>
<td>@sibertor</td>
<td>FOR526</td>
</tr>
<tr>
<td>Brian Ventura</td>
<td>Instructor</td>
<td>@brianwifaneye</td>
<td>MGT415</td>
</tr>
<tr>
<td>Jake Williams</td>
<td>Senior Instructor</td>
<td>@MalwareJake</td>
<td>SEC760</td>
</tr>
<tr>
<td>Tim Medin</td>
<td>Principal Instructor</td>
<td>@timmedin</td>
<td>SEC460</td>
</tr>
<tr>
<td>Jorge Orchilles</td>
<td>Certified Instructor</td>
<td>@jorgeorchilles</td>
<td>SEC524</td>
</tr>
<tr>
<td>Hal Pomeranz</td>
<td>Faculty Fellow</td>
<td>@hal_pomeranz</td>
<td>SEC506</td>
</tr>
<tr>
<td>Bryan Simon</td>
<td>Certified Instructor</td>
<td>@BryanOnSecurity</td>
<td>SEC401</td>
</tr>
<tr>
<td>Lance Spitzner</td>
<td>Certified Instructor</td>
<td>@lspitzner</td>
<td>MGT433</td>
</tr>
<tr>
<td>James Tarala</td>
<td>Senior Instructor</td>
<td>@isaudit</td>
<td>SEC566</td>
</tr>
<tr>
<td>Dr. Johannes Ullrich</td>
<td>Senior Instructor</td>
<td>@johullrich</td>
<td>DEV522</td>
</tr>
<tr>
<td>Joe Vest</td>
<td>Instructor</td>
<td>@joevest</td>
<td>SEC564</td>
</tr>
<tr>
<td>Joshua Wright</td>
<td>Senior Instructor</td>
<td>@joswr1ght</td>
<td>SEC575</td>
</tr>
<tr>
<td>Lenny Zeltser</td>
<td>Senior Instructor</td>
<td>@lennyzeltser</td>
<td>FOR610</td>
</tr>
<tr>
<td>Keith Palmgren</td>
<td>Senior Instructor</td>
<td>@kpalmgren</td>
<td>SEC301</td>
</tr>
<tr>
<td>Justin Searle</td>
<td>Senior Instructor</td>
<td>@meeas</td>
<td>ICS410</td>
</tr>
<tr>
<td>Stephen Sims</td>
<td>Faculty Fellow</td>
<td>@Steph3nSims</td>
<td>SEC660</td>
</tr>
<tr>
<td>John Strand</td>
<td>Senior Instructor</td>
<td>@strandjs</td>
<td>SEC504</td>
</tr>
<tr>
<td>Chad Tilbury</td>
<td>Senior Instructor</td>
<td>@chadtilbury</td>
<td>FOR508</td>
</tr>
<tr>
<td>Erik Van Buggenhout</td>
<td>Certified Instructor</td>
<td>@ErikVaBu</td>
<td>SEC599</td>
</tr>
<tr>
<td>Benjamin Wright</td>
<td>Senior Instructor</td>
<td>@benjaminwright</td>
<td>LEG523</td>
</tr>
<tr>
<td>Jeff McJunkin</td>
<td>Certified Instructor</td>
<td>@jeffmcjunkin</td>
<td>SEC460</td>
</tr>
<tr>
<td>David R. Miller</td>
<td>Certified Instructor</td>
<td>@DRM_CyberDude</td>
<td>MGT414</td>
</tr>
<tr>
<td>Larry Pesce</td>
<td>Certified Instructor</td>
<td>@haxorthematrix</td>
<td>SEC617</td>
</tr>
<tr>
<td>Hal Pomeranz</td>
<td>Faculty Fellow</td>
<td>@hal_pomeranz</td>
<td>SEC506</td>
</tr>
<tr>
<td>Bryan Simon</td>
<td>Certified Instructor</td>
<td>@BryanOnSecurity</td>
<td>SEC401</td>
</tr>
<tr>
<td>Lance Spitzner</td>
<td>Certified Instructor</td>
<td>@lspitzner</td>
<td>MGT433</td>
</tr>
<tr>
<td>James Tarala</td>
<td>Senior Instructor</td>
<td>@isaudit</td>
<td>SEC566</td>
</tr>
<tr>
<td>Dr. Johannes Ullrich</td>
<td>Senior Instructor</td>
<td>@johullrich</td>
<td>DEV522</td>
</tr>
<tr>
<td>Joe Vest</td>
<td>Instructor</td>
<td>@joevest</td>
<td>SEC564</td>
</tr>
<tr>
<td>Joshua Wright</td>
<td>Senior Instructor</td>
<td>@joswr1ght</td>
<td>SEC575</td>
</tr>
<tr>
<td>Lenny Zeltser</td>
<td>Senior Instructor</td>
<td>@lennyzeltser</td>
<td>FOR610</td>
</tr>
</tbody>
</table>
The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization’s training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher credits purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Credits must be used within 12 months, but the term can be extended with additional investments.

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 time as one week, your eligible team members can begin their training.

*Current exceptions from the SANS Voucher program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.

www.sans.org/vouchers
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.

The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization’s training needs.

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 time as one week, your eligible team members can begin their training.

As a SANS Voucher Program participant, you will be able to:

• Provide your cybersecurity team with the highest standard of skill training and certification available
• Give employees a simple way to select and procure the training they need, when they need it
• Easily approve and manage student enrollment
• Monitor employee training progress and exam scores to ensure satisfactory completion
• Track investments, debits, and account balance for optimal budgeting

Voucher credits purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Credits must be used within 12 months, but the term can be extended with additional investments.

* Current exceptions from the SANS Voucher program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.
**SEC401: Security Essentials Bootcamp Style**

**You Will Be Able To**

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMware and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools 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 that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark

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

Is SEC401: Security Essentials Bootcamp Style the right course for you?

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 that 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, then SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs. Learn to build a security roadmap that can scale today and into the future.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization’s critical information assets and business systems. 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.

Bryan Simon is an internationally recognized expert in cybersecurity who has been working in the information technology and security field since 1991. Over the course of his career, Bryan has held various technical and managerial positions in the education, environmental, accounting, and financial services sectors. Bryan speaks on a regular basis at international conferences and with the press on matters of cybersecurity. He has instructed individuals from the FBI, NATO, and the UN in matters of cybersecurity, on two continents. Bryan has specialized expertise in defensive and offensive capabilities. He has received recognition for his work in IT security and was most recently profiled by McAfee (part of Intel Security) as an IT Hero. Bryan holds 13 GIAC Certifications including GSEC, GCWN, GCID, GCFA, OPEN, GWAPT, GAWN, GISP GCIA, GCED, GCUX, GISF, and GMON. Bryan’s scholastic achievements have resulted in the honor of sitting as a current member of the SANS Institute Advisory Board and in his acceptance into the prestigious SANS Cyber Guardian program. Bryan teaches SEC401: Security Essentials Bootcamp Style, SEC501: Advanced Security Essentials – Enterprise Defender, SEC505: Securing Windows and Powershell Automaton, and SEC511: Continuous Monitoring and Security Operations. @BryanOnSecurity
Course Day Descriptions

DAY 1: Network Security Essentials
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 and ability to create and identify the goals of building a defensible network architecture are critical. It is just as important to know and understand the architecture of the system, types of designs, communication flow and how to protect against attacks using devices such as routers and firewalls. These essentials, and more, will be covered during 401.1 in order to provide a firm foundation for the consecutive days of training.


DAY 2: Defense-In-Depth and Attacks
To secure an enterprise network, you must understand the general principles of network security. In 401.2, we look at threats to our systems and take a “big picture” look at how to defend against them. You will learn that protections need to be layered – a principle called defense-in-depth. We explain some principles that will serve you well in protecting your systems. You will also learn about key areas of network security.

Topics: Defense-in-Depth; Access Control and Password Management; Security Policies; Critical Controls; Malicious Code and Exploit Mitigations; Advanced Persistent Threat (APT)

DAY 3: Threat Management
Whether targeting a specific system or just searching the Internet for an easy target, an attacker uses an arsenal of tools to automate finding new systems, mapping out networks, and probing for specific, exploitable vulnerabilities. This phase of an attack is called reconnaissance, and it can be launched by an attacker any amount of time before exploiting vulnerabilities and gaining access to systems and networks. In fact, evidence of reconnaissance activity can be a clue that a targeted attack is on the horizon.

Topics: Vulnerability Scanning and Penetration Testing; Network Security Devices; Endpoint Security; SIEM/Log Management; Active Defense

DAY 4: Cryptography, Risk Management, and Response
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. Sec401.4 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.

Topics: Cryptography; Cryptography Algorithms and Deployment; Applying Cryptography; Incident Handling and Response; Contingency Planning – BCP/DRP; IT Risk Management

DAY 5: Windows Security
Remember when Windows was simple? Windows XP desktops in a little workgroup... what could be easier? A lot has changed over time. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V; Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com, and other cloud giants for supremacy. The trick is to do it securely, of course. Windows is the most widely-used and targeted 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: Windows Security Infrastructure; Service Packs, Hot Fixes, and Backups; Windows Access Controls; Enforcing Security Policy; Securing Windows Network Services; Automation, Auditing, and Forensics

DAY 6: Linux Security
While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. This final course day provides step-by-step guidance to improve the security of any Linux system. The course combines practical “how to” instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise. This module discusses the foundational items that are needed to understand how to configure and secure a Linux system. It also provides an overview of the operating system and mobile markets. To lay a foundation, it provides an overview of the different operating systems that are based on Linux.

Topics: Linux Security: Structure, Permissions and Access, Hardening and Securing Linux Services, Monitoring and Attack Detection, Security Utilities

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

“SEC401 is a great intro and overview of network security. It covered just enough information to get a baseline level of knowledge without going too in-depth on any one topic.”

- Josh Winter, Washington County, MN

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

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 ls 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

John Strand | SANS Senior Instructor

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.

This course enables you to turn the tables on computer attackers by helping you 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.

“THE TRAINING OFFERED AT SANS IS THE BEST IN THE INDUSTRY, AND THE SEC504 COURSE IS A MUST FOR ANY IT SECURITY PROFESSIONAL – HIGHLY RECOMMENDED.”

- Michael Hoffman, Shell Oil Products US

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

@strandjs
## Course Day Descriptions

### DAY 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

### DAY 2: 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

### DAY 3: 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 day covers the third phase 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; Nettac: The Attacker’s Best Friend; Hands-on Exercises with a List of Tools

### DAY 4: Computer and Network Hacker Exploits – Part 3
This course day 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

### DAY 5: Computer and Network Hacker Exploits – Part 4
This course day covers the fourth and fifth phases 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

### DAY 6: 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

---

**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

“I will almost always recommend SEC504 as a baseline so that everyone is speaking the same language. I want my sys-admins to take it, my network admins to take it, even my devs to take it, regardless of whether they’re going to eventually move into an incident handling role. In my opinion it is the most critical, foundational class that SANS offers.”

-Kevin Wilcox, Information Security Specialist

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)
SEC503: Intrusion Detection In-Depth

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.

This course 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.

“SEC503 is fundamental for anyone performing blue team/defensive operations.”


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

@it_audit
For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses

**Course Day Descriptions**

**Day 1: 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

**Day 2: 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 on 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

**Day 3: Application Protocols and Traffic Analysis**

Day 3 introduces the versatile packet crafting tool Scapy. It is a very powerful Python-based tool that allows for 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, aiming to understand the true capabilities and limitations 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; HTTP2/TLS, SMTP, IDS/IPS Evasion Theory

**Day 4: 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

**Day 5: 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 by examining the third scenario, including Command and Control channels and managing analysis when very large packet capture files are involved.

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

**Day 6: 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 a real-world environment.

**Who Should Attend**

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

“I got a deeper understanding of key topics from SEC503. This training will help me get more data out of my investigations.”

- Alphonse Wichrowski, Allegiant Air
SEC511: Continuous Monitoring and Security Operations

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 a 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 SP 800-137 guidelines
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources 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, which is 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!

Seth Misenar is the founder of and lead consultant for Context Security, a Jackson, Mississippi-based company that provides information security thought leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both a physical and network security consultant for Fortune 100 companies, as well as the Health Insurance Portability and Accountability Act, and as information security officer for a state government agency. Prior to becoming a security geek, Seth received a bachelor’s degree in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is no stranger to certifications and thus far has achieved credentials that include the CISSP®, GPEN, GWAPT, GSEC, GCIA, GCHH, GCWN, GCFA, and MCSE. @sethmisenar
Course Day Descriptions

DAY 1: 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

DAY 2: 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

DAY 3: 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 emphasized baking visibility and detective capabilities into the design. Now we must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise.
Topics: Continuous Monitoring Overview; Network Security Monitoring (NSM), Practical NSM Issues; Cornerstone NSM

DAY 4: 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

DAY 5: 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 to 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

DAY 6: 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

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)

“SEC511 is a VERY worthwhile addition to the Cyber Defense curriculum for Blue Teamers.”
- Robert Peden, NextGear Capital
SEC301: Introduction to Cyber Security

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
- Understand computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings
- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, and intrusion detection systems, content filters, sniffers, etc.
- Build a simple but fully functional firewall configuration
- Secure your browser using a variety of security plug-ins
- Secure a wireless access point (also known as a wireless router)
- Scan for malware, clean malware from a system, and whitelist legitimate software identified by an anti-malware scanner as “potentially unwanted”
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.

To determine if SANS SEC301: Introduction to Cyber Security is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to cybersecurity 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 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 cybersecurity and need formal training and certification?

If you answer yes to any of these questions, then the SEC301: Introduction to Cyber Security training course is for you. Students with a basic knowledge of computers and technology but no prior cybersecurity experience can jump-start their security education with insight and instruction from real-world security experts in SEC301.

This completely revised and comprehensive five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, step-by-step learning format will enable you to grasp all the information presented even if some of the topics are new to you. You’ll learn fundamentals of cybersecurity that will serve as the foundation of your security 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 SANS course in this progression, 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.

“SEC301 provided a great foundation for the topic of security, since I deal with it on a daily basis on a high level.”

-Richard Pollich, Broadridge Financial Solutions Inc.

Keith Palmgren | SANS Senior Instructor

Keith Palmgren is an IT security professional with over 30 years of experience specializing in the field. He began his career with the U.S. Air Force working with cryptographic keys and codes management. He also worked in what was at the time the newly-formed Air Force computer security department. Following the Air Force, Keith worked as an MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the DoD and the National Security Agency. Later, as Security Consulting Practice Manager for both Sprint and Netigy, Keith built and ran the security consulting practice. He was responsible for all security consulting worldwide and for leading dozens of security professionals on many consulting engagements across all business spectrums. For the last several years, Keith has run his own company, NetIP, Inc. He divides his time between consulting, training, and freelance writing projects. In his career, Keith has trained over 10,000 IT professionals and authored more than 20 IT security training courses including the SANS SEC301 course. Keith currently holds 10 computer security certifications (CISSP®, GSEC, GCID, GCED, GISF, CEH, Security+, Network+, A+, CTT+).

@kpalmgren
**Course Day Descriptions**

**DAY 1: Security’s Foundation**
Every good security practitioner and every good 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 Confidentiality, Integrity, Availability (CIA), and you’ll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, and authentication/authorization/accountability.

**DAY 2: 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 the American Standard Code for Information Interchange (ASCII). 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. The networking discussion 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 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 but never quite understood, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS.

**DAY 3: An Introduction to Cryptography**
Cryptography is one of the most complex issues faced by security practitioners. 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. Instead, we learn 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?

**DAY 4: 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. 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 (VPN) technologies.

**DAY 4: Cyber Security Technologies – Part 2**
The final day of our SEC301 journey continues the discussion of cybersecurity technologies. The day begins by looking at several security technologies, including compartmentalization, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS), sniffers, content filters, etc. We then take a good look at browser and web security, and the difficulties of securing the web environment. For example, students will understand why and how their browser connects to anywhere from 5 to 100 different Internet locations each time they load a single web page. We end the day with a look at system security to include hardening operating systems, patching, virtual machines, cloud computing, and backup.

**Who Should Attend**
- Anyone new to cybersecurity and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don’t understand, but want to understand
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o’clock news
- Professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don’t need “deep in the weeds” detail
- Those who have decided to make a career change to take advantage of the job opportunities in cybersecurity and need formal training and certification

*“SEC301 is a great class for the individual who wants to learn an extensive amount of material in one week.”*  
-Steven Chovanec, Discover Financial Services
Micah Hoffman has been working in the information technology field since 1998 supporting federal government, commercial, and internal customers in their efforts to discover and quantify information security weaknesses in their organizations. He leverages years of hands-on, real-world OSINT, penetration testing, and incident response experience to provide excellent solutions to his customers. Micah is the author of SEC487: Open-Source Intelligence Gathering and Analysis, and holds GIAC’s GMON, GAWN, GWAPT, and GPEN certifications as well as the CISSP®. Micah is a highly active member in the cybersecurity and OSINT communities. When not working, teaching, or learning, Micah can be found hiking on Appalachian Trail or the many park trails in Maryland.

@WebBreacher

SEC487: Open-Source Intelligence Gathering and Analysis  NEW!

Immeasurable amounts of personal, potentially incriminating data is currently stored in the websites, apps, and social media platforms that people access and update via their devices daily. That data can become evidence for citizens, governments, and businesses to use in solving real financial, employment, and criminal issues with the help of a professional information gatherer.

SEC487 will teach students legitimate and effective ways to find, gather, and analyze this data from the Internet. You’ll learn about reliable places to harvest data using manual and automated methods and tools. Once you have the data, we’ll show you how to ensure that it is analyzed, sound, and useful to your investigations.

This is a foundational course in open-source intelligence (OSINT) gathering and, as such, will move quickly through many areas of the field. The course will teach you current, real-world skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour the massive amount of information across the Internet, analyze the results, and pivot on interesting pieces of data to find other areas for investigation. Our goal is to provide the OSINT knowledge base for students to be successful in their fields whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

Throughout the course week, students will participate in numerous hands-on labs using the tools and techniques that are the basis for gathering free data from the Internet. The 20 labs in this course use the live Internet and dark web to help students gain real-world confidence. You’ll leave the course knowing not just how to use search features on a website, but all of the scenario-based requirements and OSINT techniques needed to gather truly important OSINT data.

“Micah’s delivery was entertaining and engaging.”

-Paul Ryan, GDIT
DAY 1: Foundations of OSINT
We begin with the basics and answer the questions “what is OSINT” and “how do people use it.” This first day is about level-setting and ensuring that all students understand the background behind what we do in the OSINT field. We also establish the foundation for the rest of the week by learning how to document findings and set up an OSINT platform, and we discuss effective research habits for OSINT analysts. This day is a key component for the success of an OSINT analyst because without these concepts and processes in place, researchers can get themselves into serious trouble during assessments by inadvertently alerting their targets or improperly collecting data, making it less useful when delivered to the customer.

Topics: Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting Up an OSINT Platform; Effective Research Habits; Creating Sock Puppets

DAY 2: Gathering, Searching, and Analyzing OSINT
Open-Source Intelligence (OSINT) data collection begins on day two after we get a glimpse of some of the fallacies that could influence our conclusions and recommendations. From this point in the class forward, we examine distinct categories of data and think about what it could mean for our investigations. Retrieving data from the Internet could mean using a web browser to view a page or, as we learn in this section, command line tools, scripts, and helper applications can also be used.

Topics: Data Analysis Challenges; Creating Your OSINT Process; Harvesting Web Data; OSINT Frameworks; Basic Data: Street Addresses, Basic Data: Phone Numbers; Email Addresses; User Names; Avatars and Reverse Image Searches; Leveraging Search Engines

DAY 3: Social Media and File Analysis
Finding data on people, especially basic content such as email addresses, home address, and phone numbers, can be made easier using online people search engines. This is how day three kicks off, examining free and paid choices in this data aggregator area and understanding how to use the data we receive from them. Some of these engines provide social media content in their results. This makes a terrific transition for us to move into social media data. We finish the day examining document and image metadata to glean interesting data points from different document types.

Topics: People Search Engines; Facebook Analysis; LinkedIn Data; Twitter Data; Instagram; Dating and Adult Websites, Registries and Wish Lists; Web and Traffic Cameras; File Metadata Analysis

DAY 4: Geolocation, Networks, Government, and Business
Day four focuses on many different but related OSINT issues. We begin by looking at how various mapping sites can assist our assessments with aerial data, distance-measuring, and “street view” imagery. Moving beyond just using one vendor’s mapping system, students will learn about the breadth of free mapping resources available for OSINT.

Topics: Remote Location Recon; Geolocation, IP Address and Whois, IP Address Geolocation, Domain Name System (DNS); Wireless Networks; Recon Tool Suites and Frameworks; U.S. Government Data; Researching Companies

DAY 5: The Dark Web and International Issues
The entire morning of day five focuses on understanding and using three of the most popular dark web networks for OSINT purposes. Students will learn why people (good and bad) use Freenet, I2P, and Tor. The first module in the afternoon examines how we scrape content from paste sites. We then focus our attention to international issues by performing OSINT activities on websites outside of the United States. We leave some time at the end of the day for a massive lab (the “Grand Exercise”) that helps students put together all that they have learned in a semi-guided walk-through that touches on many of the concepts taught throughout the week.

Topics: The Surface, Deep, and Dark Web; The Dark Web; Freenet, I2P – Invisible Internet Project; Tor; Searching Data Dump Sites; International issues; Vehicle Searches

DAY 6: Capstone: Capture (and Present) the Flags
The capstone for the course is a group event that brings together everything that students learned throughout the week. This is not a “canned” Capture the Flag event where specific flags are planted and your team must find them. It is a competition where each team will collect specific OSINT data about a certain group of people. The output from this work will be turned in as a “deliverable” to the “client” (the instructor), and then the three teams with the most-complete work will present their research to the class for voting. This four-hour, hands-on event will reinforce what the students practiced in the Grand Exercise the day before and add the complexity of performing OSINT assessments under pressure and in a group.

Author Statement
“I have always been intrigued by the types and amount of data that are available on the Internet. From researching the best restaurants in a foreign town to watching people via video cameras, it all fascinates me. As the Internet evolved, more high-quality, real-time resources became available and every day was like a holiday, with new and wonderful tools and sites coming online and freely accessible. “At a certain point, I was no longer in awe of the great resources on the web and, instead, transitioned to surprise that people would post images of themselves in illegal or compromising positions or that a user profile contained such explicit, detailed content. My wonder shifted to concern for these people. Didn’t they know that their profiles, images, videos, comments, etc. were publicly accessible? Didn’t they care about it? What I found was that, if you looked in the right places, you could find almost anything about a person, a network, or a company. Piecing together seemingly random pieces of data into meaningful stories became my passion and, ultimately, the reason for this course. “I recognized that the barrier to performing excellent OSINT was not that there was no free data on the Internet. It was that there was too much data on the Internet. The challenge transitioned from ‘how do I find something’ to ‘how do I find only what I need?’ This course was born from this need to help others learn the tools and techniques to effectively gather and analyze OSINT data from the Internet.”

-Micah Hoffman

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

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

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

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

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

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

“SEC501 is a very valuable course to a Network/Security Administrator. The first chapter of Defensible Network Architecture is worth the price of admission in of itself.”

- Ryan Bast, Subzero Group, Inc.

Bryce Galbraith | SANS Principal Instructor

As a contributing author of the internationally bestselling book Hacking Exposed: Network Security Secrets & Solutions, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone’s renowned penetration testing team, and served as a senior instructor and co-author of Foundstone’s Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security, where he provides specialized vulnerability assessment and penetration testing services for clients. He teaches several of the SANS institute’s most popular courses and develops curriculum around current topics. He has taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who’s who of top companies, financial institutions, and government agencies around the globe. Bryce is an active member of several security-related organizations, holds several security certifications, and speaks at conferences around the world. @brycegalbraith
<table>
<thead>
<tr>
<th>Course Day Descriptions</th>
<th>Topics:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DAY 1: Defensive Network Architecture</strong></td>
<td>Security Benchmarks; Standards, and the Role of Audit in Defending Infrastructure; Defense Using Authentication and Authorization, and Defending Those Services; The Use of Logging and Security Information and Event Management (SIEM) in Defending an Organization from Attack; Attacking and Defending Critical Protocols; Several Man-in-the-Middle Attack Methods, and Defenses against Each; Infrastructure Defense Using IPS, Next-Generation Firewalls, and Web Application Firewalls; Defense of Critical Servers and Services; Active Defense; Defense of Private and Public Cloud Architectures</td>
</tr>
<tr>
<td><strong>DAY 2: Penetration Testing</strong></td>
<td>In this section, you will learn the core concepts of both “Digital Forensics” and “Incident Response.” We’ll explore some of the hundreds of artifacts that can give forensic investigators specific insight into what occurred during an incident. You will also learn how incident response currently operates, after years of evolving, in order to address the dynamic procedures used by attackers to conduct their operations. We’ll look at how to integrate DFIR practices into a continuous security operations program.</td>
</tr>
<tr>
<td><strong>DAY 3: Network Detection and Packet Analysis</strong></td>
<td>“Prevention is ideal, but detection is a must” is a critical motto for network security professionals. While organizations always want to prevent as many attacks as possible, some adversaries will still sneak into the network. In cases where an attack is not successfully prevented, network security professionals need to analyze network traffic to discover attacks in progress, ideally stopping them before significant damage is done. Packet analysis and intrusion detection are at the core of such timely detection. Organizations need to not only detect attacks but also to react in a way that ensures those attacks can be prevented in the future.</td>
</tr>
<tr>
<td><strong>DAY 4: Digital Forensics and Incident Response</strong></td>
<td>Topics: DFIR Core Concepts: Digital Forensics; DFIR Core Concepts: Incident Response; Modern DFIR: A Live and Continuous Process; Widening the Net: Scaling the DFIR Process and Scoping a Compromise</td>
</tr>
<tr>
<td><strong>DAY 5: Malware Analysis</strong></td>
<td>Malicious software is responsible for many incidents in almost every type of organization. Types of malware vary widely, from Ransomware and Rootkits to Crypto Currency Miners and worms. We will define each of the most popular types of malware and walk through multiple examples. The four primary phases of malware analysis will be covered: Fully Automated Analysis, Static Properties Analysis, Interactive Behavior Analysis, and Manual Code Reversing. You will complete various in-depth labs requiring you to fully dissect a live Ransomware specimen from static analysis through code analysis. You will get hands-on experience with tripping the malware through behavioral analysis techniques, as well as decrypting files encrypted by Ransomware by extracting the keys through reverse engineering. All steps are well defined and tested to ensure that the process to achieve these goals is actionable and digestible.</td>
</tr>
<tr>
<td><strong>DAY 6: Enterprise Defender Capstone</strong></td>
<td>The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, using the 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 techniques will be used 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 submit flags to score points. More difficult challenges will be worth more points. In this defensive exercise, challenges include packet analysis, routing protocols, scanning, malware analysis, and other challenges related to the course material.</td>
</tr>
</tbody>
</table>
SEC505: Securing Windows and PowerShell Automation

You Will Be Able To

- 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 other attacks discussed in SEC504 and other SANS hacking courses
- Execute PowerShell commands on remote systems and begin to write your own PowerShell scripts
- Harden PowerShell itself against abuse, and enable transcription logging for your SIEM
- Use Group Policy and PowerShell to grant administrative privileges in a way that reduces the harm if an attack succeeds (assume breach)
- Block hacker lateral movement and malware Command & Control channels using Windows Defender Firewall, IPsec, DNS sinkholes, admin credential protections, and more
- Prevent exploitation using AppLocker and other Windows OS hardening techniques in a scalable way with PowerShell
- Configure PowerShell remoting to use Just Enough Admin (JEA) policies to create a Windows version of Linux sudo and setuid root
- 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 must-have protocols against exploitation, such as SSL/TLS, RDP, DNS, DNSSEC, PowerShell Remoting, and SMB
- Use PowerShell to access the WMI service for remote command execution, searching event logs, reconnaissance, and more

Jason Fossen | SANS Faculty Fellow

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/DevOps 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 architecture: 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 disaster across the board. Managing administrative privileges and credentials is a tough problem, so this course devotes an entire day to just this one critical task. Perhaps you’ve taken a hacking course at SANS and you now want to learn Windows mitigations: SEC505 is that course. SEC505 is the defense-only mirror image of SEC504 with regard to Windows and Active Directory.

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. Many of the PowerShell scripts written by the course author are available to download from GitHub for free.

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.

SEC505 will also prepare you for the GIAC Certified Windows Security Administrator (GCWN) certification exam to prove your Windows security expertise. The GCWN certification counts towards a Master’s Degree in Information Security from the SANS Technology Institute (www.sans.edu) and satisfies the Department of Defense 8140 computing environment requirement. The GCWN is also a foundational certification for soldiers in the U.S. Army’s 255-S Information Protection Program. For DoD students, we will see how to apply the NSA/DISA Secure Host Baseline.

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 Windows security at the same time!

Jason Fossen is a principal security consultant at Enclave Consulting LLC, a published author, and a frequent public speaker on Microsoft security issues. He is the sole author of the SANS week-long Securing Windows course (SEC505), maintains the Windows day of Security Essentials (SEC401S), and has been involved in numerous other SANS projects since 1998. He graduated from the University of Virginia, received his master’s degree from the University of Texas at Austin, and holds a number of professional certifications. He currently lives in Dallas, Texas.

@JasonFossen
Course Day Descriptions

DAY 1: PowerShell Automation and Security
This course section covers what you need to know to get started using PowerShell. You don’t need to have any prior scripting or programming experience. We have PowerShell labs throughout the week, so today is not the only PowerShell material. We start with the essentials, then go more in depth as the week progresses. Don’t worry, you won’t be left behind, the PowerShell labs walk you through every step.
Topics: PowerShell Overview and Tips; What Can We Do With PowerShell?; Write Your Own Scripts

DAY 2: 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/DevOps.
Topics: Continuous Secure Configuration Enforcement; Group Policy Precision Targeting; Server Hardening for SecOps/DevOps; PowerShell Desired State Configuration (DSC)

DAY 3: Windows Public Key Infrastructure 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. And we don’t really have a choice anymore: running a PKI is pretty much mandatory for Microsoft security and cloud computing. This day of the course is basically one long hands-on lab to install and configure a full Windows Server PKI. This includes a Certificate Authority (CA), Group Policy certificate auto-enrollment on endpoints, Online Certificate Status Protocol (OCSP) revocation checking, private key roaming for users, smart card certificate deployment, and, of course, more PowerShell examples.
Topics: Why Is a PKI Necessary?; How to Install the Windows PKI; How to Manage Your PKI; Deploying Smart Cards

DAY 4: Administrative Compromise and Privilege Management
Why do submarines have pressure doors to seal off compartments? Because they are designed to assume a breach will occur. In a Windows environment, a security breach will occur, so we must design the architecture with an “assume breach” mindset as well. If we assume that some day the computers and credentials of our administrators will be compromised, then how do we build damage control into the network from the beginning? This is not about detection and incident response. The challenge here is how to design for damage control when we delegate administrative privileges. We need to proactively design damage control into the architecture, not wait until after there is a breach (when it’s too late).
Topics: Secure Architecture: Admin Privileges; Compromise of Administrative Powers; PowerShell Just Enough Admin (JEA); Active Directory Permissions and Delegation

DAY 5: Endpoint Protection and Pre-Forensics
You are already applying patches and updating anti-virus signatures. But endpoint protection is much more than that. Because most advanced malware infections start with a compromised endpoint, we want to proactively build defensibility and damage control into our systems using a “zero trust” or “assume breach” model. How? AppLocker is an application whitelisting tool built into Windows to control which executables, scripts, DLLs and installer packages users may run. If hackers or malware attempt to launch an unauthorized process post-exploitation, the aim is to block it and log it. In the lab, we’ll use PowerShell and Group Policy to manage AppLocker. Application whitelisting can be hard to manage if used too aggressively, so we’ll also talk about how to get started without making the help desk phone ring off the hook.
Topics: Anti-Exploitation; IPSec Port Permissions; Host-Based Firewalls, Pre-Forensics

DAY 6: Defensible Networking and Blue Team WMI
Hackers love the Windows Management Instrumentation (WMI) service, and so should we. We are the linebackers on the Blue Team and the WMI service was made to benefit us, not hackers. The WMI service is enabled by default and accessible over the network. Through WMI we can do remote command execution (without PowerShell being installed at the target), forcibly log off the user, reboot the machine, stop services, search for processes running as Administrator, kill any process, and much more. The WMI service is nearly all-powerful and it’s built for remote administration. PowerShell is tightly integrated into WMI, and we’ll look at several PowerShell examples.
Topics: PowerShell and WMI; Hardening DNS; Dangerous Protocols We Can’t Live Without

Who Should Attend
- Security Operations personnel
- Blue Team players who were terrified by SECS04
- 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
- DoD admins applying the NSA/DISA Secure Host Baseline
- Individuals deploying or managing a PKI or smart cards
- Anyone wanting a more rugged Windows architecture

“This class provided real-world examples and sample scripts to make a Windows-centric environment fundamentally more secure.”
-Nick Boardman, HRSD

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
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

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, and Apache
- Forensic Investigation of Linux Systems

“Linux security courses are a rare commodity and a valuable resource to the security professional.”

-Trevor Sellers, IDA Center for Communications Research
Course Day Descriptions

**DAY 1: Hardening Linux/Unix Systems – Part 1**
This course day tackles some of the most important techniques for protecting your Linux/Unix systems from external attacks, and 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

---

**DAY 2: Hardening Linux/Unix Systems – Part 2**
Continuing our exploration of Linux/Unix security issues, this course day focuses 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

---

**DAY 3: Hardening Linux/Unix Systems – Part 3**
Monitoring your systems is critical for maintaining a secure environment. This course day 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

---

**DAY 4: Application Security – Part 1**
This course day 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

---

**DAY 5: Application Security – Part 2**
This course section 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`

---

**DAY 6: Digital Forensics for Linux/Unix**
This hands-on course day is designed to be an information-rich introduction 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

---

**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 insight into Linux and Unix security tools, procedures, and best practices

---

“**This course gave me a better understanding of Linux internals and specific threat hunting ideas that I will use in my environment.**”

- Shelby Peterson, Adobe
SEC530: Defensible Security Architecture  NEW!

SEC530: Defensible Security Architecture is designed to help students build and maintain a truly defensible security architecture. “The perimeter is dead” is a favorite saying in this age of mobile, cloud, and the Internet of Things, and we are indeed living in a new world of “de-perimeterization” where the old boundaries of “inside” and “outside” or “trusted” and “untrusted” no longer apply.

This changing landscape requires a change in mindset, as well as a repurposing of many devices. Where does it leave our classic perimeter devices such as firewalls? What are the ramifications of the “encrypt everything” mindset for devices such as Network Intrusion Detection Systems?

In this course, students will learn the fundamentals of up-to-date defensible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better address the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

While this is not a monitoring course, this course will dovetail nicely with continuous security monitoring, ensuring that security architecture not only supports prevention, but also provides the critical logs that can be fed into a Security Information and Event Management (SIEM) system in a Security Operations Center.

Hands-on labs will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Determine appropriate security monitoring needs for organizations of all sizes
- Maximize existing investment in security architecture by reconfiguring existing assets
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Configure appropriate logging and monitoring to support a Security Operations Center and continuous monitoring program

“SANS training provides the most relevant security issues and practices that immediately increase my work capabilities.”

- Steven Launius, Discover Financial Services
Course Day Descriptions

**DAY 1: Defensible Security Architecture**

**Topics:**
Modern Attack Techniques; Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis

**DAY 2: Network Security Architecture**

**Topics:**
Layer 1; Layer 2: Switches; Layer 3: Routers; Layer 3/4 Stateful Firewalls

**DAY 3: Architecting Application Layer Security**

**Topics:**
Proxy; NGFW; NIDS/NIPS; Sandboxing; Encryption; Whole Disk Encryption; Secure Remote Access; Org Remotely Using/Accessing; Virtualized Infrastructure; Cloud Services; Mobile Devices/Applications; Mobile Applications

**DAY 4: Data and Application Security Architecture**

**Topics:**
Protecting Web/Mobile Applications; Protecting Endpoints from Malicious/Compromised Applications; Securing the Internet of Things (IoT)

**DAY 5: Zero Trust Architecture: Addressing the Adversaries Already in Our Networks**

**Topics:**
Rogue Devices; Compromised Internal Assets; Deceptive Security Ops; Building Tripwires for Breach Detection; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis

**DAY 6: Secure the Flag Challenge**

The course culminates in a team-based design-and-secure 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 throughout this course. Teams will assess, design, and secure a variety of computer systems and devices, leveraging all seven layers of the OSI model.

**Topics:**
Capstone – Design/Detect/Defend

**Who Should Attend**

- Security architects
- Network engineers
- Network architects
- Security analysts
- Senior security engineers
- System administrators
- Technical security managers
- CND analysts
- Security monitoring specialists
- Cyber threat investigators

“This training introduces very good tools and processes necessary for individuals and enterprises alike to be successful and stay on top of their security posture."

-Mark Vlcek, Cisco Systems, Inc.
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 Amazon Web Services and native tools
- Incorporate vulnerability management, scanning, and penetration testing into cloud environments

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.

SEC545: Cloud Security Architecture and Operations will tackle these issues one by one. We’ll start with a brief introduction to cloud security fundamentals, 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 the 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.

“"If an organization is starting its journey to the cloud, SEC545 is a must for security practitioners to take!”" —Troy Davidson, Suncor

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

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

@daveshackelford

Dave Shackleford | SANS Senior Instructor
DAY 1: Cloud Security Foundations
The first day of the course 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 course.

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

DAY 2: 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

DAY 3: 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 lock 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 there can form the backbone of your 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 disaster recovery 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

DAY 4: 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 significantly 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

DAY 5: 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 Offensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up
SEC555: SIEM with Tactical Analytics  NEW!

You Will Be Able To

- Deploy the SANS SOF-ELK VM in production environments
- Demonstrate ways most SIEMs commonly lag current open-source solutions (e.g., SOF-ELK)
- Get up to speed on SIEM use, architecture, and best practices
- Know what type of data sources to collect logs from
- Deploy a scalable logs solution with multiple ways to retrieve logs
- Operationalize ordinary logs into tactical data
- Develop methods to handle billions of logs from many disparate data sources
- Understand best practice methods for collecting logs
- Dig into log manipulation techniques challenging many SIEM solutions
- Build out graphs and tables that can be used to detect adversary activities and abnormalities
- Combine data into active dashboards that make analyst review more tactical
- Utilize adversary techniques against them by using frequency analysis in large data sets
- Develop baselines of network activity based on users and devices
- Develop baselines of Windows systems with the ability to detect changes from the baseline
- Apply multiple forms of analysis such as long tail analysis to find abnormalities
- Correlate and combine multiple data sources to achieve more complete understanding
- Provide context to standard alerts to help understand and prioritize them

Many organizations have logging capabilities but lack the people and processes to analyze them. 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 students with the training, methods, and processes to enhance 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 Information and Event 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 SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is 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, how to 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 can 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.

“The immediate value of the SEC555 course material is unlike any course or training I've received. A++.”

- David Savercool, Dart Container

Justin Henderson is a passionate and dedicated information technology professional who has been in the field since 2005. Justin focuses on providing comprehensive industry training and uses his knowledge and experience to mentor others. Justin is particularly proficient in working with technical platforms, including operating systems, networking, security, storage, and virtualization, but he has also worked in governance, project management, as well as service management. He has a BS degree in network design and administration from Western Governors University and has over 40 certifications, including the GPEN and GCWN. Justin has also taught network security at Lake Land College. Some of his other achievements include mentoring individuals in the information technology field as well as developing the virtual dojo, a fully automated cloud computing solution showcase environment.

@SecurityMapper
DAY 1: SIEM Architecture and SOF-ELK
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

DAY 2: Service Profiling with SIEM
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 will be 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 they are 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

DAY 3: Advanced Endpoint Analytics
The value in endpoint logs provides tremendous visibility in detecting attacks. In particular, 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 that 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

DAY 4: Baselining and User Behavior Monitoring
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

DAY 5: Tactical SIEM Detection and Post-Mortem Analysis
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, preventing compromise is the beginning, 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 the Enterprise
- Monitor Firewall Activity
- SIEM Tripwires
- Post Mortem Analysis

DAY 6: 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:**
- Define-the-Flag Challenge – Hands-on Experience

Who Should Attend
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and 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

“**This course is as practical and real-world as it gets. SEC555 provides numerous quick wins and really stimulates thinking about relative value of numerous ways to defend your organization.”**

-Mikhail Vitrebskiy, Lexington Partners
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.

**“SEC566 provides great tools, explanation, and insight!”**

- Ryan LeVan, Trex Company, Inc.
DAY 1: 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

DAY 2: 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

DAY 3: 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

DAY 4: 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

DAY 5: 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)

“The training helps me understand why the Controls are necessary for securing systems at my organization.”

- Brandon McWilliams, SRP
You just got hired to help our virtual organization “SyncTechLabs” build out a cybersecurity capability. On your first day, your manager tells you: “We looked at some recent cybersecurity trend reports and we feel like we’ve lost the plot. Advanced persistent threats, ransomware, denial of service...We’re not even sure where to start!”

Cyber threats are on the rise: ransomware is affecting small, medium and large enterprises alike, while state-sponsored adversaries are attempting to obtain access to your most precious crown jewels. SEC599: Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses will provide an in-depth understanding of how current adversaries operate and arm you with the knowledge and expertise you need to detect and respond to today’s threats.

SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

Course authors Erik Van Buggenhout and Stephen Sims (both certified as GIAC Security Experts) are hands-on practitioners who have achieved a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked “But how do I prevent this type of attack?” With more than 20 labs plus a full-day defend-the-flag exercise during which students attempt to defend our virtual organization from different waves of attacks against its environment, SEC599 gives students real-world examples of how to prevent attacks.

Our six-day journey will start with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce the Advanced Persistent Threat (APT) Attack Cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization “SyncTechLabs” in our Day 1 exercises.

Throughout days 2 through 5 we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. Some of the topics we will address include:

- How red and blue teams can improve collaboration, forming a true purple team
- How current advanced adversaries are breaching our defenses
- Security controls structured around the Kill Chain

In designing the course and its exercises, the authors went the extra mile to ensure that attendees “build” something that can be used later on. For this reason, the different technologies illustrated throughout the course (e.g., IDS systems, web proxies, sandboxes, visualization dashboards, etc.) will be provided as usable virtual machines on the course USB. SEC599 will finish with a bang. During the Defend-the-Flag challenge on the final course day, you will be pitted against advanced adversaries in an attempt to keep your network secure. Can you protect the environment against the different waves of attacks? The adversaries aren’t slowing down, so what are you waiting for?

**Erik Van Buggenhout**  
**SANS Certified Instructor**
**Course Day Descriptions**

**DAY 1: Knowing the Adversary, Knowing Yourself**

Our six-day journey will start with an introduction on the purple team concept. What is it all about? Should you form another dedicated cybersecurity team? We will focus on how red and blue teams can be encouraged to form a strong feedback loop for maximum effect. We will explain how recent attacks operate through in-depth case studies and introduce the APT attack cycle as a structured approach to describing attacks. In order to understand how attacks work, you will also compromise our virtual organization “SyncTechLabs” during the day’s exercises. Once we understand how adversaries are operating, we will flip over to the blue side and explain how defenders can better understand their own environments, set up a fundamental detection capability, and understand their own “soft spots.”

**Topics:** Course Outline and Lab Set-up; Current Threat and Attack Landscape; Introducing the APT Attack Cycle; A Defensible Architecture and Environment; Preparation – Knowing Yourself

**DAY 2: Averting Payload Delivery**

Day 2 will cover how attackers take their first steps. How do they deliver their initial payload and what can defenders do about it? We will cover the most frequently used payload delivery mechanisms:

- Delivery through (spear-)phishing
- Delivery through removable media
- Delivery through the network (e.g., Server Message Block relays, Responder, etc.)
- Delivery through HTTP or HTTPS

As always, students will first learn how the adversaries are operating by simulating the attacks in our lab environment, after which they will implement security controls to prevent and detect these attacks. The courseware will cover technical controls, but will also touch upon “soft topics” such as security awareness.

**Topics:** End-User Security Awareness; Leveraging Suricata IDS/IPS; Stopping Delivery Through Removable Media; Stopping Delivery Through the Network; Stopping Delivery Through Email; Stopping Delivery Through HTTP(S)

**DAY 3: Preventing Exploitation**

On Day 3 we will explain how exploitation can be prevented. Attendees will gain an in-depth understanding of current exploitation tactics. We will introduce effective security controls to stop exploitation attempts dead in their tracks. Discussions will include:

- Operating system hardening
- Payload execution control (including application whitelisting and script control)
- Securing applications from the ground up by doing threat modeling and implementing compile-time controls
- Securing vulnerable applications by implementing exploit mitigating techniques

**Topics:** Operating System Hardening; Preventing Execution of Payloads; Securing Applications

**DAY 4: Avoiding Installation, Foiling Command and Control, and Thwarting Lateral Movement**

On Day 4 we will continue our journey in the Kill Chain, with a key focus on how malicious adversary persistence can be avoided, how command and control channels can be detected, and how lateral movement can be stopped. Topics to be discussed include:

- Principle of least privilege to prevent malware persistence
- Detecting malware persistence in user land
- Network monitoring to detect command and control
- Hardening Windows to prevent lateral movement
- Analyzing Windows event logs to detect ongoing lateral movement

**Topics:** Avoiding Installation; Foiling Command and Control; Thwarting Lateral Movement

**DAY 5: Thwarting Exfiltration, Cyber Deception, and Incident Response**

Day 5 focuses on stopping the adversary during the final stages of the attack:

- How can data exfiltration be detected and stopped?
- How can cyber deception be used to slow down and stop advanced adversaries?
- How can threat intelligence aid defenders in the APT Attack Cycle?
- How can defenders perform effective incident response?

As always, theoretical concepts will be illustrated during the different exercises performed throughout the day.

**Topics:** Data Exfiltration; Cyber Deception Strategies; Patrolling Your Neighborhood; Leveraging Threat Intelligence; Incident Response

**DAY 6: Advanced Persistent Threat Defender Capstone**

The course culminates in a team-based Defend-the-Flag competition. 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 cybersecurity controls studied all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge.

**Topics:** Applying Previously Covered Security Controls in-depth; Reconnaissance; Weaponization; Delivery; Exploitation; Installation; Command and Control, Action on Objectives

---

**Who Should Attend**

- Security architects
- Security engineers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- IT administrators
- Penetration testers who want to better understand how defensive controls work
- IT administrators
- Individuals looking to better understand how persistent cyber adversaries operate and how the IT environment can be improved to better prevent, detect, and respond to incidents

---

“SEC599 gives really good background about adversary behavior and the steps needed to detect it.”

-Tarot Wake, Halkyn Consulting Ltd

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)
Hands-On Information Security Challenges

NetWars:

• Cyber Defense
• Penetration Testing
• Digital Forensics & Incident Response
• ICS

Develop skills in:
- Cyber Defense
- Penetration Testing
- Digital Forensics & Incident Response
- ICS

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

– Kyle McDaniel, Lenovo

Choose from:
Core NetWars | DFIR NetWars | Cyber Defense NetWars | ICS NetWars

Experience NetWars at Network Security 2018

Play solo or in a team of up to five players

Seating is limited, register for NetWars when you register for your course.

www.sans.org/netwars
To be the best, learn from the best.

Join the only graduate program designed and taught exclusively by world-renowned SANS faculty.

Find out why over 500 infosec professionals have chosen SANS graduate programs to advance their careers while remaining active in their jobs.

Attend an online information session or meet with current students and admissions staff in person at SANS Network Security 2018.

“As a SANS graduate student, I learn cutting-edge, hands-on skills that are immediately useful at work.”

– Susan Ramsey, MSISE Candidate, Senior Security Engineer, UCAR

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

Graduate Certificate Programs:
- Cyber Defense Operations
- Cybersecurity Engineering (Core)
- Incident Response
- Industrial Control Systems
- Penetration Testing & Ethical Hacking

Tuition Reimbursement
Regional accreditation and Title IV eligibility means tuition meets the requirements for most corporate tuition reimbursement plans.

Funding for Veterans
Master’s degree and graduate certificate programs are eligible for VA Education Benefits.

Interest-free Payment Plan
Qualified master’s candidates can finance the program in monthly installments through SANS’ Tuition Payment Program.

Learn more at www.sans.edu
SEC560: Network Penetration Testing and Ethical Hacking

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.

“SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective.”

-Steve Nolan, General Dynamics

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

@edskoudis
**Course Day Descriptions**

**DAY 1: 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 will 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

**DAY 2: 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 Nettac. 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; Nettac for the Pen Tester; Monitoring Services During a Scan

**DAY 3: 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

**DAY 4: Post-Exploitation and Merciless Pivoting**
This section of the course zooms in on pilaging 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 msfsconsole 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

**DAY 5: 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-compose John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack snifed 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 (CSRF), command injection, and SQL injection flaws in applications such as online banking, blog sites, and more.

**Topics:** Password Cracking with John the Ripper; Snifing 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

**DAY 6: 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

---

**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

---

“For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses

---

**Extended hours; hands-on labs**

---

“**The hacker perspective in SEC560 allows new penetration testers and cyber defenders to identify security posture gaps and holes by adapting to a diverse skillset.”**

-Ryan Guest, Southern Company

---

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
SEC542: Web App Penetration Testing and Ethical Hacking

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

Moses Hernandez
SANS Certified Instructor

Moses Hernandez is a seasoned security professional with over 15 years in the IT industry. He has held positions as a network engineer, network architect, security architect, platform engineer, site reliability engineer, and consulting sales engineer. He has a background in complex network systems, systems administration, forensics, penetration testing, and development. He has worked with some of the largest companies in the nation as well as fast-growing, bootstrap startups. Moses has developed information security regimens safeguarding some of the most sensitive personal data in the nation. He creates custom security software to find and mitigate unknown threats, and works on continually evolving his penetration testing skills. He enjoys building software, networks, systems, and working with business-minded individuals. Moses’s current passions include offensive forensics, building secure systems, finance, economics, history, and music.

@mosesrenegade

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.
Course Day Descriptions

**DAY 1: 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

**DAY 2: 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

**DAY 3: 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; Injection: 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

**DAY 4: XXE 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:** XML External Entity (XXE), Cross-Site Scripting (XSS), Browser Exploitation Framework (BeEF), AJAX, XML and JSON, Document Object Model (DOM), Logic Attacks, API Attacks, Data Attacks

**DAY 5: 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 Testing; 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

**DAY 6: 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.

**Who Should Attend**
- General security practitioners
- Penetration testers
- Ethical hackers
- Web application developers
- Website designers and architects

---

“SEC542 shows a hands-on way of doing web app penetration testing – not just how to use this tool, or that tool.”
-
Christopher J. Stover, Infogressive Inc.
Computer exploitation is on the rise. As advanced adversaries become more numerous, more capable, and much more destructive, organizations must become more effective at mitigating their information security risks at the enterprise scale. SEC460 is the premier course focused on building technical vulnerability assessment skills and techniques, while highlighting time-tested practical approaches to ensure true value across the enterprise.

The course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel from organizations charged with effectively and efficiently securing 10,000 or more systems.

SEC460 begins with an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

SEC460 will teach you how to use real industry-standard security tools for vulnerability assessment, management, and mitigation. It is the only course that teaches a holistic vulnerability assessment methodology while focusing on challenges faced in a large enterprise. You will learn on a full-scale enterprise range chock full of target machines representative of an enterprise environment, leveraging production-ready tools, and a proven testing methodology.

This course takes you beyond the checklist, giving you a tour of the attackers’ perspective that is crucial to discovering where they will strike. Operators are more than the scanner they employ. SEC460 emphasizes this personnel-centric approach by examining the shortfalls of many vulnerability assessment programs in order to provide you with the tactics and techniques required to secure networks against even the most advanced intrusions.

We wrap up the first five days of instruction with a discussion of triage, remediation, and reporting before putting your skills to the test on the final day against an enterprise-grade cyber range with numerous target systems for you to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises. By adopting an end-to-end approach to vulnerability assessment, you can be confident that your skills will provide much-needed value in securing your medium- or large-scale organization.

“SEC460 has provided me the knowledge to build a great Vulnerability Management/Vulnerability Assessment Program that vendor courses couldn’t provide.”

- Eric Osmus, ConocoPhillips Company
DAY 1: Methodology, Planning, and Threat Modeling
In this section of the course, students will develop the skills needed to conduct high-value vulnerability assessments with measurable impact. We will explore the elemental components of successful vulnerability assessment programs, deconstruct the logistical precursors to value-added operations, and integrate adversarial threat modeling and intelligence.

Topics: Maximizing Value from Vulnerability Assessments and Programs; Setting Up for Success at Scale: Enterprise Architecture and Strategy; Developing Transformational Vulnerability Assessment Strategies; Performing Enterprise Threat Modeling; Generating Compounding Interest from Threat Intelligence and Avoiding Information Overload; The Vulnerability Assessment Framework; Overview of Comprehensive Network Scanning; Compliance Standards and Information Security

DAY 2: Discovery
Having mastered the structural foundations of vulnerability management, we pivot to the realm of direct, tactical application. Comprehensive reconnaissance, enumeration, and discovery techniques are the prime elements of successful vulnerability assessment. While gaining additional familiarity with hands-on enterprise operations, you will systematically probe the environment in order to discover the relevant host, service, version, and configuration details that will drive the remainder of the assessment system.

Topics: Active and Passive Reconnaissance; Identification and Enumeration with DNS, DNS Zone Speculation and Dictionary-Enabled Discovery; Port Scanning with Nmap and Zenmap; Scanning Large-Scale Environments; Commonplace Services; Scanning the Network Perimeter and Engaging the DMZ; The Windows Domain: Exchange, SharePoint, and Active Directory; Recruiting Disparate Data Sources. Patches, Hotfixes, and Configurations: Trade-offs. Speed, Efficiency, Accuracy, and Thoroughness; Introduction to PowerShell

DAY 3: Enhanced Vulnerability Scanning and Automation
We begin day three by delving into the next phase of the Vulnerability Assessment Framework and charging into the most exciting topic in security testing: automation to handle scale. We start by breaking vulnerability scanning into its elemental components and gaining an understanding of vulnerability measurement that can be applied to task automation. This focus will direct us to the quantitative facets underlying cybersecurity vulnerabilities and drive our discussion of impact, risk, and triage. Each topic discussed will focus on identifying, observing, and assessing the entry points that threats leverage during network attacks. Later in the day, we will apply our understanding of the vulnerability concept to evolve our PowerShell skills and take action on an enterprise scale.

Topics: Enhanced Vulnerability Scanning; Risk Assessment Matrices and Rating Systems; Quantitative Analysis Techniques Applied to Vulnerability Scoring; Performing Tailored Risk Calculation to Drive Triage; General Purpose vs. Application Specific Vulnerability Scanning; Tuning the Scanner to the Task, the Enterprise, and Tremendous Scale; Scan Policies and Compliance Auditing; Performing Vulnerability Discovery with Open-Source and Commercial Appliances; Nmap Scripting Engine and OpenVAS; Testing and Insecure Cryptographic Implementations Including SSL; Assessing VOIP Environments; Discovering Vulnerabilities in the Enterprise Backbone: Active Directory, Exchange, and SharePoint; Evaluating Vulnerability Risk in Custom and Unique Systems including Web Applications; Minimizing Supplemental Risk While Conducting Authenticated Scanning through Purposeful Application of Least Privilege; Probing for Data Link Liability to Identify Hazards in Wireless Infrastructure, Switches, and VLANs; Manual Vulnerability Discovery Automated to Attain Maximal Efficacy

DAY 4: Vulnerability Validation, Triage, and Data Management
Over the course of this day we will tackle the next phase of our overarching testing methodology: vulnerability validation, while simultaneously confronting one of the biggest headaches common to a vulnerability assessment at scale. At large scale, vulnerability data can be overwhelming and possibly even contradictory. We will cover the specific techniques needed to wrangle through and better focus those data. Next, we will examine techniques for collaboration and data management with the Acheron tool for analyzing vulnerability data across an organization.

Topics: Assigning a Confidence Value and Validating Exploitable Potential of Vulnerabilities; Manual Vulnerability Validation Targeting Enterprise Infrastructure; Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base; Managing Large Repositories of Vulnerability Data; Querying the Vulnerability Knowledge Base; Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

DAY 5: Remediation and Reporting
Many well-intentioned vulnerability assessment programs begin with zeal and vitality, but after the discovery of vulnerabilities there is often a tendency to ignore the risk reality and shift back to the status quo. Over the previous course modules we focused on knowing the target environment and deconstructing the logistical precursors to value-added operations, and integrate adversarial threat modeling and intelligence. And that’s exactly what we cover in this section of the course. Developing this plan in conjunction with the Vulnerability Assessment Report is an opportunity to galvanize the team, while enhancing the vulnerability assessment value proposition.

Topics: Team Operations and Collaboration; Security Operations Project Management Essentials; Transforming Triage Listing into the Vulnerability Remediation Plan; Developing the Cybersecurity Risk Sight Picture; Connecting Related Datasets and Framing the Narrative; Developing a Web of Network and Host Affiliations; Modeling Account Relationships on Active Directory Forests; Creating Effective Vulnerability Assessment Reports; Curbing the Vulnerability Lifecycle and Aspiring to Zero Hour; Closure: Be a Positive Influence in the Context of the Global Information Security Crisis

DAY 6: Vulnerability Assessment Foundry
In celebration of your diligence, curiosity, and mad new vulnerability skills, we welcome you to your final hands-on challenge to hammer home your capabilities. The guided scenario on this final course day is designed to test your mettle through trial and detailed work in a fun capture-the-flag-style environment. The challenge is the canvas upon which you can hone your skills and measure your maturing talents. Armed for the fight, you will doubtless rise to the challenge...and triumph! The scenario: An organization called “The Foundry” has engaged you to perform a vulnerability assessment of its environment. The organization is very aware of your particular set of vulnerability assessment skills, and treasures the insights it is certain you will provide to help secure the organization against its formidable adversaries, including nefarious cybercrime cartels and jealous nation-state actors. Teams will work together to help squash issues that would lead to a compromise of The Foundry’s precious assets.

Topics: Tactical Employment of the Vulnerability Assessment Framework; Threat Modeling: Discovery, Vulnerability Scanning, Validation, Data Management and Triage

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
SEC573: Automating Information Security with Python

You Will Be Able To

- Develop forensics tools to carve artifacts from forensics evidence for which no other tool exists or use third-party modules for well-known artifacts that hide 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 the 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, and 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, and Exception handling
- Interact with websites using Requests, Packet Analysis, Packet reassembly techniques, and much more

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.

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.

Finally, what do you do when “off-the-shelf” tools and exploits fall short? As a penetration tester you need to evolve as quickly as the threats you are paid to emulate, so the answer is simple, if you have the skills: 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 self-paced style of the class will meet you where you are to let you get the most out of what is being taught. 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 in 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.

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from software developer to chief information security officer. He is the author of the SEC573: Automating Information Security with Python course. Mark has a master’s degree in information security engineering and many industry certifications, including being the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. He is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter, which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. Since January 2011, Mark has served as the SANS Technical Advisor to the DoD, where he assists various entities in the development of information security capabilities.

Mark Baggett | SANS Senior Instructor

Register at www.sans.org/network-security-2018 | 301-654-SANS (7267)
Course Day Descriptions

**DAY 1: 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

---

**DAY 2: 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 on how to debug your code.

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

---

**DAY 3: Defensive Python**
Day three includes in-depth coverage of 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 network defenders who need 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

---

**DAY 4: 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

---

**DAY 5: 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

---

**DAY 6: Capture the Flag**
In this final course 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 ciphers, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

---

“SEC573 is excellent. I went from having almost no Python coding ability to being able to write functional and useful programs.”

-Caleb Jaren, Microsoft
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.

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

@joswr1ght
Course Day Descriptions

**DAY 1: 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 11, 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, Application 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 Architecture; Mobile Device Analysis; Mobile Device Malware Threats

**DAY 2: 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 on 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

**DAY 3: 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 application report card project.

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

**DAY 4: 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

**DAY 5: 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

**DAY 6: 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 learned 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.

---

**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

---

“SEC575 provides an incredible amount of information, and the hands-on labs are awesome. It is a must-have for mobile penetration testers.”

-Richard Takacs, Integrity360

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)

---

This course is available via Simulcast. See page 100 for more information.
SEC617: Wireless Penetration Testing and Ethical Hacking NEW!

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 devices to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones
- Implement a WPA2 Enterprise penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize Scapy to force custom packets to manipulate wireless networks in new ways, quickly building custom attack tools to meet specific penetration test requirements
- Identify WiFi attacks using network packet captures traces and freely available analysis tools
- Identify and exploit shortcomings in the security of proximity key card systems
- Decode proprietary radio signals using Software-Defined Radio
- Mount a penetration test against numerous standards-based or proprietary wireless technologies

This course is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers.

The authors of SEC617, as penetration testers themselves, know that many organizations overlook wireless security as an attack surface, and therefore fail to establish required defenses and monitoring, even though wireless technologies are now commonplace in executive suites, financial departments, government offices, manufacturing production lines, retail networks, medical devices, and air traffic control systems. Given the known risks of insecure wireless technologies and the attacks used against them, SEC617 was designed to help people build the vital skills needed to identify, evaluate, assess, and defend against these threats. These skills are “must-haves” for any high-performing security organization.

For many analysts, “wireless” was once synonymous with “WiFi,” the ever-present networking technology, and many organizations deployed complex security systems to protect these networks. Today, wireless takes on a much broader meaning – not only encompassing the security of WiFi systems, but also the security of Bluetooth, ZigBee, Z-Wave, DECT, RFID, NFC, contactless smart cards, and even proprietary wireless systems. To effectively evaluate the security of wireless systems, your skillset needs to expand to include many different types of wireless technologies.

SEC617 will give you the skills you need to understand the security strengths and weaknesses of wireless systems. You will learn how to evaluate the ever-present cacophony of WiFi networks and identify the WiFi access points (APs) and client devices that threaten your organization. You will learn how to assess, attack, and exploit deficiencies in modern WiFi deployments using WPA2 technology, including sophisticated WPA2 Enterprise networks. You will gain a strong, practical understanding of the many weaknesses in WiFi protocols and how to apply that understanding to modern wireless systems. Along with identifying and attacking WiFi access points, you will learn to identify and exploit the behavioral differences in how client devices scan for, identify, and select APs, with deep insight into the behavior of the Windows 10, macOS, Apple iOS, and Android WiFi stacks.

A significant portion of the course focuses on Bluetooth and Bluetooth Low Energy (BLE) attacks, targeting a variety of devices, including wireless keyboards, smart light bulbs, mobile devices, audio streaming devices, and more. You will learn to assess a target Bluetooth device, identify the present (or absent) security controls, and apply a solid checklist to certify a device’s security for use within your organization.

Beyond analyzing WiFi and Bluetooth security threats, analysts must also understand many other wireless technologies that are widely utilized in complex systems. SEC617 provides insight and hands-on training to help analysts identify and assess the use of ZigBee and Z-Wave wireless systems used for automation, control, and home systems. The course also investigates the security of cordless telephony systems in the worldwide Digital Enhanced Cordless Telephony (DECT) standard, including audio eavesdropping and recording attacks.

Radio frequency identification (RFID), near field communication (NFC), and contactless smart card systems are more popular than ever in countless applications such as point of sale systems and data center access control systems. You will learn how to assess and evaluate these deployments using hands-on exercises to exploit the same kinds of flaws discovered in mass transit smart card systems, hotel guest room access systems, and more.

In addition to standards-based wireless systems, we also dig deeper into the radio spectrum using software-defined radio (SDR) systems to scour for signals. Using SDR, you will gain new insight into how widely pervasive wireless systems are deployed. With your skills in identifying, decoding, and evaluating the data these systems transmit, you will be able to spot vulnerabilities even in custom wireless infrastructures.

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

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

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

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

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

#### DAY 1: WiFi Data Collection and Analysis

The first section of the course quickly looks at wireless threats and attack surfaces and analyzes where you will likely see non-WiFi systems deployed in modern networks. We start off with a look at fundamental analysis techniques for evaluating WiFi networks, including the identification and analysis of rogue devices, and finish with a dive into remote penetration testing techniques using compromised Windows 10 and macOS devices to pivot.

**Topics:** Characterize the Wireless Threat; Sniffing WiFi; Rogue Access Point (AP) Analysis

---

#### DAY 2: WiFi Attack and Exploitation Techniques

After developing skills needed to capture and evaluate WiFi activity, we start our look at exploiting WiFi, targeting AP and client devices. We cover techniques that apply to any WiFi products, from consumer to enterprise-class devices, focusing on understanding protocol-level deficiencies that will continue to be applied throughout the course on non-WiFi wireless systems as well.

**Topics:** Exploiting WiFi Hotspots; WiFi Client Attacks; Exploiting WEP; Denial of Service (DoS) Attacks; WiFi Fuzzing for Bug Discovery

---

#### DAY 3: Enterprise WiFi, DECT, and ZigBee Attacks

We finish our look at WiFi attack techniques with a detailed look at assessing and exploiting WPA2 networks. Starting with WPA2 consumer networks, we investigate the flaws associated with pre-shared key networks and WiFi Protected Setup (WPS) deployments, continuing with a look at exploiting WPA2 Enterprise networks using various Extensible Authentication Protocol (EAP) methods. We continue to investigate the security of wireless networks on day 3, switching to non-WiFi analysis with a look at exploiting the worldwide Digital Enhanced Cordless Telephony (DECT) standard to capture and export audio conversations from cordless headsets and phones. We also investigate the security of ZigBee and IEEE 802.15.4 networks, looking at cryptographic flaws, key management failures, and hardware attacks.

**Topics:** Attacking WPA2 Pre-Shared Key Networks; Attacking WPA2 Enterprise Networks; Attacking Digital Enhanced Cordless Telephony Deployments; Attacking ZigBee Deployments

---

#### DAY 4: Bluetooth and Software Defined Radio Attacks

Bluetooth technology is nearly as pervasive as WiFi, with widespread adoption in smart phones, fitness trackers, wireless keyboard, smart watches, and more. In this module, we dig into the Bluetooth Classic, Enhanced Data Rate, and Low Energy protocols, including tools and techniques to evaluate target devices for vulnerabilities. Immediately following our look at Bluetooth technology, we jump into the practical application of Software Defined Radio (SDR) technology to identify, decode, and access proprietary wireless systems. We investigate the hardware and software available for SDR systems, and look at the tools and techniques to start exploring this exciting area of wireless security assessment.

**Topics:** Bluetooth Introduction and Attack Techniques; Bluetooth Low Energy Introduction and Attack Techniques; Practical Application of Software Defined Radio (SDR)

---

#### DAY 5: RFID, Smart Cards, and NFC Hacking

On day 5, we evaluate RFID technology in its multiple forms to identify the risks associated with privacy loss and tracking, while also building an understanding of both low-frequency and high-frequency RFID systems and NFC. We examine the security associated with contactless Point of Sale (PoS) terminals, including Apple Pay and Google Wallet, and proximity lock access systems from HID and other vendors. We also examine generalized techniques for attacking smart card systems, including critical data analysis skills needed to bypass the intended security of smart card systems used for mass transit systems, concert venues, bike rentals, and more.

**Topics:** RFID Overview; RFID Tracking and Privacy Attacks; Low-Frequency RFID Attacks; Exploiting Contactless RFID Smart Cards; Attacking NFC

---

#### DAY 6: Capture-the-Flag Event

On the last day of class, we will pull together all the concepts and technology we have covered during the week in a comprehensive Capture-the-Flag event. In this hands-on exercise, you will have the option to participate in multiple roles: identifying unauthorized/rogue WiFi access points, attacking live and recorded WiFi networks, decoding proprietary wireless signals, exploiting smart card deficiencies, and more. During this wireless security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers, simulating the realistic environment you will be prepared to protect when you get back to the office.

---

#### 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

---

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

-Garret Picchioni, Salesforce

---

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)
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 even 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?

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.

This course offers 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 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
Penetration Testing
Vulnerabilities; New HTTP/2 Protocol Issues and Web Services; WebSocket Protocol Issues and ActiveX, and Silverlight Vulnerabilities; SOAP and from Mobile Applications; Flash, Java, Intercepting Traffic to Web Services

Topics:
- Suite and other automated toolsets. We’ll use techniques will make use of tools such as Burp to test the applications and backend systems. These various techniques to discover flaws within 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 tools. We’ll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

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

DAY 1: 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

DAY 2: 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

DAY 3: 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

DAY 4: 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 tools. 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

DAY 5: 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 Firewall Rules 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

DAY 6: 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.
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.

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS’s only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP®, CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

@Steph3nSims
Course Day Descriptions

**DAY 1: 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

**DAY 2: Crypto and Post-Exploitation**
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

**DAY 3: 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 to 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

**DAY 4: 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

**DAY 5: Exploiting Windows for Penetration Testers**
On day five we start with covering the OS security features (ASLR, DEP, etc.) added to the Windows OS over the years, as well as Windows-specific constructs, such as the process environment block (PEB), structured exception handling (SEH), thread information block (TIB), and the Windows API. Differences between Linux and Windows will be covered. These topics are critical in assessing Windows-based applications. We then focus on stack-based attacks against programs running on the Windows OS.

**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

**DAY 6: 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 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

"SEC660 is the right balance between theory and practice; it’s hands-on, not too hard, but also not too easy."

- Anton Ebertzed, Siemens AG

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)
Jake Williams is a principal consultant at Rendition Infosec. He has more than a decade of experience in secure network design, penetration testing, incident response, forensics, and malware reverse engineering. Before founding Rendition Infosec, Jake worked with various cleared government agencies in information security roles. He is well-versed in cloud forensics and previously developed a cloud forensics course for a U.S. government client. Jake regularly responds to cyber intrusions by state-sponsored actors in the financial, defense, aerospace, and healthcare sectors using cutting-edge forensics and incident response techniques. He often develops custom tools to deal with specific incidents and malware-reversing challenges. Additionally, Jake performs exploit development and has privately disclosed a multitude of zero day exploits to vendors and clients. He found vulnerabilities in one of the state counterparts to healthcare.gov and recently exploited antivirus software to perform privilege escalation. Jake developed Dropsmack, a pentesting tool (okay, malware) that performs command and control and data exfiltration over cloud file-sharing services. Jake also developed an anti-forensics tool for memory forensics, Attention Deficit Disorder (ADD). This tool demonstrated weaknesses in memory forensics techniques.

@MalwareJake

SEC760: Advanced Exploit Development for Penetration Testers

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, the SANS Institute’s only 700-level course, 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.

Jake Williams
SANS Senior Instructor

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

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

“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
Course Day Descriptions

**DAY 1: Threat Modeling, Reversing and Debugging with IDA**

Many penetration testers, incident handlers, developers, and other related professionals lack reverse-engineering and debugging skills. These are different skills than reverse-engineering malicious software. As part of the Security Development Lifecycle (SDL) and Secure-SDL, 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; 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.**

**DAY 2: 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.**

**DAY 3: 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; patchdiffl, 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; UsingROPto Compiled Shellcode on the Fly (Return-Oriented Shellcode).**

**DAY 4: Windows Kernel Debugging and Exploitation**

The Windows Kernel is very complex and intimidating. This course day aims to help you understand the Windows Kernel and the various exploitation 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.**

**DAY 5: Windows Heap Overflows and Client-Side Exploitation**

The focus of this section is primarily on Windows browser and client-side exploitation. You will learn to analyze C++ vtable overflows, one of the most common mechanisms used to compromise a modern Windows system. Many of these vulnerabilities are discovered in the browser, so browser techniques will also be taught, including modern heap spraying to deal with Internet Explorer 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++ vtable/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.**

**DAY 6: Capture-the-Flag Challenge**

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

**Who Should Attend**

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

**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-SDL 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

“SEC760 is the challenge I am looking for. It will be overwhelming, but well worth it.”

-William Stott, Raytheon
Extend and Validate Your Training

Add an OnDemand Bundle or GIAC Certification Attempt

to your course within seven days of this event to get bundle pricing.*

Extend Your Training Experience with an OnDemand Bundle

• Four months of supplemental online review
• 24/7 online access to your course lectures, materials, quizzes, and labs
• Subject-matter-expert support to help you increase your retention of course material

OnDemand Bundle price – $729

Get Certified with GIAC Certifications

• Distinguish yourself as an information security leader
• 30+ GIAC cybersecurity certifications available
• Two practice exams included
• Four months of access to complete the attempt

GIAC bundle price – $729

“The course content and OnDemand delivery method have both exceeded my expectations.”

-ROBERT JONES, TEAM JONES, INC.

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

-CHRISTINA FORD, DEPARTMENT OF COMMERCE

More Information

www.sans.org/ondemand/bundles | www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.
Hire Cybersecurity Professionals Now!

When you need to fill cybersecurity positions, the SANS CyberTalent Academies can help. These immersive, accelerated training programs increase the number of qualified professionals entering the cybersecurity field, provide meaningful career opportunities for U.S. veterans, and increase gender diversity in the InfoSec industry.

The Academies quickly and cost-effectively meet the specific needs of organizations and employers seeking to discover, develop, and retain top cybersecurity talent.

“SANS CyberTalent Academy is a great program to provide industry-best training to a group of disciplined, trustworthy, and accomplished people. Having recently hired a Vet who came through the program, I can say it was perhaps the easiest ‘get up to speed’ period we’ve ever experienced here at Sage. We’d recommend other companies look to the program to find future talent!”

— John H. Rogers
Director of Advisory Services
Sage Data Security, LLC

Learn more at: www.sans.org/academy4employers

Academy Graduates are seeking opportunities! Contact immersionacademy@sans.org for more information.
### FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting

#### 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 utilityware 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.

#### FOR508: Advanced Digital Forensics, Incident Response, and Threat 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 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!

### Chad Tilbury | SANS Senior Instructor

Chad has nearly 20 years of experience working with government agencies, defense contractors, and Fortune 500 companies. He has served as a special agent with the Air Force Office of Special Investigations, where he conducted computer forensics examinations for a variety of crimes and ushered counter-espionage techniques into the digital age. Chad has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. In addition, Chad has worked as a computer security engineer and forensic lead for a major defense contractor and served as the vice president of worldwide Internet enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries. Today, Chad brings his wealth of experience to his role as technical director at CrowdStrike, where he specializes in incident response, corporate espionage, and computer forensics. In addition to being a graduate of the U.S. Air Force Academy, Chad holds B.S. and M.S. degrees in computer science, as well as the GCFA, GCIH, GREM, and ENCE certifications.

@chadtilbury

---

<table>
<thead>
<tr>
<th>6 Day Program</th>
<th>36 CPEs</th>
<th>Laptop Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FOR508 analyzes Advanced Persistent Threat samples that are affecting our industry today. This training can’t get any better!"  
- Neel Mehta, Chevron
Course Day Descriptions

Day 1: 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.

Day 2: Memory Forensics in Incident Response and 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 forensics 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.

Day 3: 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.

Day 4: 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 and Analysis.

Day 5: 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.

Day 6: 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 activist groups.
Topics: Identification and Scoping; Containment and Threat Intelligence Gathering; Remediation and Recovery.

Who Should Attend
- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Information security professionals
- Federal agents and law enforcement personnel
- Red team members, penetration testers, and exploit developers
- SANS FOR500 and SEC504 graduates

“This was an amazing class that showed, from beginning to end, how to investigate a possible breach and the ways to identify and prevent it.”

-Jimmy Hwang, Wyndham Worldwide Corp

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing for follow-on malware analysis or definitive data loss determination
- Use historical NetFlow data to identify relevant past network occurrences, allowing for 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

Philip Hagen
SANS Senior Instructor

This course will enable you to 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 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: Threat Hunting, Analysis, and Incident Response was built from the ground up to cover the most critical skills needed to mount efficient and effective post-intrusion 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 ndump, tcpextract, 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.
Course Day Descriptions

**DAY 1: 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

**DAY 2: Core Protocols & Log Aggregation/Analysis**
Understanding log data and how it can guide the investigative process is an important network forensics 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 andLogs; Firewall, Intrusion Detection System, and Network Security Monitoring Logs; Logging Protocol and Aggregation; ELK Stack and the SOF-ELK Platform

**DAY 3: 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

**DAY 4: 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

**DAY 5: 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

**DAY 6: 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

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

---

“**I love how this course is very well organized and the step-by-step walk-through of the lab allows even someone new to network forensics to get started right away.”**

-Paul Kim, PWC
FOR500: Windows Forensic Analysis

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

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 detailed step-by-step workbook meticulously outlines 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

Rob Lee | SANS Faculty Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC area and currently the Curriculum Lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years’ experience in computer forensics, vulnerability and exploit development, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and earned his MBA from Georgetown University. He served in the U.S. Air Force as a member of the 609th Information Warfare Squadron (IWS), the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI), where he led crime investigations and an incident response team. Over the next seven years, he worked directly with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for vulnerability discovery and exploit development teams, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team.

Most recently, Rob was a Director for MANDIANT, a commercial firm focusing on responding to advanced adversaries such as the APT. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob is also co-author of the MANDIANT threat intelligence report “M-Trends: The Advanced Persistent Threat.”

@roblee & @sansforensics

Register at www.sans.org/network-security-2018 | 301-654-SANS (7267)
DAY 2: 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

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

"Anyone involved in digital investigations needs to take this class! It covers or touches upon almost every aspect of Windows forensic investigations in a very short period of time."

-Cy Bleistine, NJSP
FOR518: **Mac and iOS Forensic Analysis and Incident Response**

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.

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.

This course will teach you:

- **Mac and iOS 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.
- **Apple Technologies:** How to understand and analyze many Mac and iOS specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac and iOS forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac-specific data files, tracking of 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 or iOS forensics case.

**FORENSICATE DIFFERENTLY!**

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

**“We have a primarily Mac OS environment and I don’t think I could find a tenth of this information through my own research.”**

- Kevin Neely, Pure Storage

A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today’s digital forensic investigations. Sarah has worked with federal law enforcement agencies on a variety of high-profile investigations in such areas as computer intrusions, criminal cases, counter-intelligence, counter-narcotics, and counter-terrorism. Her research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering.

@iamevltwin

Sarah Edwards | SANS Certified Instructor
For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)

**Course Day Descriptions**

**DAY 1: Mac and iOS Essentials**
This section introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure. Acquisition fundamentals are the same with Mac and iOS devices, but there are a few tips and tricks that can be used to successfully and easily collect Mac and iOS systems for analysis. 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:** Apple Essentials; Mac Essentials and Acquisition; Disks & Partitions; iOS Essentials; iOS Acquisition; iOS Backups

**DAY 2: HFS+ File System & System Triage**
The building blocks of Mac and iOS forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, students will learn the basic principles of the primary file system implemented on Mac OS X systems. The students will then use that information to look at a variety of great artifacts that use the file system and that are different from other operating systems. Students will review Mac and iOS triage data.

**Topics:** HFS+ File System; Extended Attributes; File System Events Store Database; Spotlight; Portable Artifacts; Mac and iOS Triage; Most Recently Used (MRU)

**DAY 3: User Data, System Configuration, and Log Analysis**
This section contains a wide array of information that can be used to profile and understand how individuals use their computers. 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. 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:** User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

**DAY 4: Application Data Analysis**
In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, etc. These data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.

**Topics:** Application Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Photos; Maps; Location Data; Random Apps; Apple Watch; Third-Party Apps

**DAY 5: Advanced Analysis Topics**
Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud, and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.

**Topics:** Live Response; Time Machine; OS X Malware and Intrusion Analysis; Cloud; Versions; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

**DAY 6: Mac Forensics Challenge**
Students will put their new Mac forensics skills to the test by running through a real-life scenario with team members.

**Topics:** 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

---

**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, and 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, FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

---

Sun, Sep 23 - Fri, Sep 28
9:00am - 5:00pm
Hands-on labs

67
FOR526: *Memory Forensics In-Depth*

**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

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 OS X 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.

FOR526: Memory Forensics In-Depth will teach you:
- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming 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

MALWARE CAN HIDE, BUT IT MUST RUN

Alissa Torres | SANS Certified Instructor

Alissa has more than 15 years of experience in computer and network security spanning government, academic, and corporate environments. She has the deep experience and technical savvy to take on even the most difficult computer forensics challenges that come her way. Her current role as an incident response advisor at Cargill provides daily challenges “in the trenches” and demands constant technical growth. Alissa is also founder of her own firm, Sibertor Forensics, and has taught internationally in more than 10 countries. Alissa has a B.S from the University of Virginia and a M.S in information technology from the University of Maryland. She is a GIAC Certified Forensic Analyst (GCFA), and holds the GCSE, GCH, GSEC, CISSP®, and EnCE certifications. Alissa has served as a member of the GIAC Advisory Board since 2013 and was recognized by SC Magazine as one of its “2016 Women to Watch.”

@sibertor
Other than Windows

www.sans.org/event/network-security-2018/courses

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses

**Course Day Descriptions**

**DAY 1: 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 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

---

**DAY 2: 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

---

**DAY 3: 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

---

**DAY 4: 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 Suspicous 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

---

**DAY 5: 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

---

**DAY 6: Memory Analysis Challenge**

This final course 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)

---

**Who Should Attend**

- Incident response team members
- Experienced digital forensic analysts
- Red team members, penetration testers, and exploit developers
- Law enforcement officers, federal agents, and detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

---

“The training opened my eyes to the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations.”

-Greg Caouette, Kroll
In his past work with the military, Peter responded to network attacks and worked with both defensive and offensive red teams. Currently, Peter is a Senior Security Engineer with IBM. Peter believes that people lead technology, not the other way around, and he works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. As Peter explains, “Putting together networks only to tear them apart is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place.”

Peter Szczepankiewicz
SANS Certified Instructor

Security practitioners should attend FOR578: Cyber Threat Intelligence because it is unlike any other technical training. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. The course will help practitioners from across the security spectrum to:

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn about the different sources from which to collect adversary data and how to exploit and pivot off of those data
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- Establish structured analytical techniques to be successful in any security role

It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques that will complement their existing knowledge as well as establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary’s intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated 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.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries’ methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats. In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578: Cyber Threat Intelligence will equip you, your security team, and your organization with the tactical, operational, and strategic-level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats.

Who Should Attend
- Security practitioners
- Incident response team members
- Threat hunters
- Security Operations Center personnel and information security practitioners
- Digital forensic analysts and malware analysts
- Federal agents and law enforcement officials
- Technical managers
- SANS alumni looking to take their analytical skills to the next level

Register at www.sans.org/network-security-2018 | 301-654-SANS (7267)
**Course Day Descriptions**

**DAY 1: Cyber Threat Intelligence and Requirements**
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. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. 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; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

**DAY 2: The Fundamental Skillset: Intrusion Analysis**
Intrusion analysis is at the heart of threat intelligence. It is a fundamental skillset for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the “kill chain” and the “Diamond Model.” These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section, students will participate in and be walked 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 in terms of structuring and defining adversary campaigns.

**Topics:** Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains; Collection Source: Malware

**DAY 3: Collection Sources**
Cyber Threat Intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers as an example but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this course section, students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

**Topics:** Case Study: Axiom; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots; Exploitation: Storing and Structuring Data

**DAY 4: Analysis and Dissemination of Intelligence**
Many organizations seek to share intelligence but often fail to understand its value, its limitations, and the right formats to choose for each audience. Additionally, indicators and information shared without analysis are not intelligence. Structured analytical techniques such as the Analysis of Competing Hypotheses can help add considerable value to intelligence before it is disseminated. This section will focus on identifying both open-source and professional tools that are available for students as well as on 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. Students 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 building the singular intrusions into campaigns and being able to communicate about those campaigns.

**Topics:** Analysis: Exploring Hypotheses; Analysis: Building Campaigns; Dissemination: Tactical; Case Study: Sony Attack; Dissemination: Operational

**DAY 5: Higher-Order Analysis and Attribution**
A core component of intelligence analysis at any level is the ability to defeat biases and analyze information. The skills required to think critically are exceptionally important and can have an organization-wide or national-level impact. In this course 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, including 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 once they complete the course.

**Topics:** Logical Fallacies and Cognitive Biases; Dissemination Strategies; Case Study: Stuxnet; Fine-Tuning Analysis, Case Study: Sofacy; Attribution

“This course gives a very smart and structured approach to Cyber Threat Intelligence, something that the global community has been lacking to date.”

- John Geary, Citigroup
FOR585: Advanced Smartphone Forensics

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

SMARTPHONES HAVE MINDS OF THEIR OWN. DON’T MAKE THE MISTAKE OF REPORTING SYSTEM EVIDENCE AS USER ACTIVITY. IT’S TIME TO GET SMARTER!

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, 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. Examination and interpretation of 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 forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, 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 on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you’re working on the day you complete the course.

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

Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden’s media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics—there’s hardly a device or platform she hasn’t researched or examined or a commercial tool she hasn’t used. These days Heather is the Director of Forensic Engineering at ManTech CARD. Heather previously led the mobile device team for Bassi Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Struz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she handled a number of high-profile cases. She has also developed and implemented forensic training programs and standard operating procedures.

@HeatherMahalik

Heather Mahalik
SANS Senior Instructor
### DAY 1: Malware Forensics, Smartphone Overview, and SQLite Introduction

Although smartphone forensic concepts are similar to those of digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. On this first course day, students will apply what they know to smartphone forensic handling, device capabilities, acquisition methods, and SQLite database examination and query development. Students will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. Malware affects a plethora of smartphone devices. This course section will examine various types of malware, how it exists on smartphones, and how to identify and analyze it. Most commercial smartphone 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 Concepts of Smartphones; Smartphone Forensics Tool Overview; JTAG Forensics; Smartphone Components; Introduction to SQLite

### DAY 2: 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

### DAY 3: Android Backups and iOS Device Forensics

Android backups can be created for forensic analysis or by a user. Smartphone examiners need to understand the file structures and how to parse these data. 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:** Android Backup Files; iOS Forensics Overview and Acquisition; iOS File System Structures; iOS Evidentiary Locations; Handling Locked iOS Devices; Traces of User Activity on iOS Devices

### DAY 4: iOS Backups, Windows, and BlackBerry 10 Forensics

iOS backups are extremely common and are found in the cloud and on hard drives. Not only do users create backups, we often find that our best data can be derived from creating an iOS backup for forensic investigation. We realize that not everyone examines BlackBerry and Windows Phone devices, which is why we are focusing primarily on BlackBerry 10, Windows Phone 8 and 10 and application usage. Both the Windows Phone and BlackBerry 10 sections highlight pieces of evidence that can be found on multiple smartphones. BlackBerry smartphones are designed to protect user privacy, but techniques taught on this course day will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of BlackBerry device file systems. 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 before embarking on a BlackBerry 10 lab that covers tying SIM cards and application usage to a device.

**Topics:** iOS Backup File Forensics; Windows Phone/Mobile Forensics; BlackBerry 10 Forensic Overview; BlackBerry 10 File System, Evidentiary Locations, and Forensic Analysis

### DAY 5: Third-Party Application and Knock-Off 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. The rest of the day focuses heavily on secure chat applications, recovering deleted application data and attachments, mobile browser artifacts, and knock-off phone forensics. The skills learned in this section will provide you with advanced methods for decoding data stored in third-party applications across all smartphones. We will show you what the commercial tools miss and teach you how to recover these artifacts yourself.

**Topics:** Third-Party Applications Overview; Third-Party Application Artifacts; Messaging Applications and Recovering Attachments; Secure Chat Applications; Mobile Browsers; Knock-off Phone Forensics

### DAY 6: 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.

---

**Who Should Attend**

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, and detectives
- Accident reconstruction investigators
- IT auditors
- Graduates of SANS SEC575, SEC563, FOR500, FOR508, FOR526, FOR610, or FOR518 who want to take their skills to the next level

---

“The best part about advanced smartphone forensics is that it provides real-world technologies for forensically investigating devices without the typical point and click approaches.”

- Brad Wardman, PayPal
FOR610: **Reverse-Engineering Malware:** Malware Analysis Tools and Techniques

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
- Derive Indicators of Compromise (IOCs) from malicious executables to strengthen incident response and threat intelligence efforts

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.

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

Lenny Zeltser | SANS Senior Instructor

Aptly called the “Yoda” of malware analysis by his students, Lenny Zeltser keeps his eye on the big picture and focuses on the sum of events rather than individual occurrences. He lives by that philosophy and brings it to his job and classroom. A seasoned business and technology leader with extensive information security expertise, Lenny started his professional journey in a variety of technical InfoSec roles before serving as the national lead of the U.S. security consulting practice at a major cloud services provider. Later in his career he oversaw a portfolio of security services at a Fortune 500 technology company. Today, as VP of Products at Minerva Labs, Lenny designs and builds creative anti-malware products. Lenny also developed the Linux toolkit REMnux to make it easier to use a variety of freely available malware analysis tools, many of which run well on Linux but can be difficult to find and install. Lenny earned the prestigious GIAC Security Expert professional designation, and he currently serves on the Board of Directors of the SANS Technology Institute. Lenny holds a bachelor’s degree in computer science from the University of Pennsylvania and a master’s in business administration from MIT Sloan. He is the co-author of four books on malware, network security, and digital forensics.

@lennyzeltser

DAY 1: 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 (REnux) 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

DAY 2: 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 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

DAY 3: 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

DAY 4: 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

DAY 5: 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

DAY 6: 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

“An excellent course to enable the student to master malware analysis and have the tools to carry out analysis in a safe environment.”

- G. Conway, NCA

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
SANS Training Formats

After selecting your training path or course, compare SANS multiple live and online training formats for the structure and schedule that works best for you. SANS is committed to ensuring your training experience always exceeds expectations.

Live Classroom Instruction

Training Events

Our most recommended format, live SANS training events, deliver SANS top instructors teaching multiple courses at a single time and location. The events feature:

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

Our 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 99 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 Training delivers the same world-renowned instructors, content, and learning results as SANS live training options, with several unique and valuable benefits. Students who train online enjoy subject-matter-expert support throughout the course, online access to all course labs, and the ability to revisit content without limits. No matter where you are or when you can train, SANS has courses that will fit around your life.

Top Reasons to Take SANS Training Online:

• Rewind your training, so you can review complex details or topics
• Revisit content to ensure you master key concepts
• Reinforce your learning with subject-matter experts and labs
• Retain your knowledge of course content with four or months of access

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.

“I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses.”

—Nick Sewell, IIT

“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
Security awareness is hard. We make it easy.

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 that 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. The 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
G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events worldwide. He provides consulting services as a virtual CISO, expert witness testimony, and domain expertise in blockchain and cryptocurrency. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation. He is a retired U.S. Navy captain who was entrusted with nine command assignments, including responsibility for leadership training for 70,000 sailors. A graduate of Northwestern University, he holds a B.S. in computer science, a B.A. in mathematics, a master’s degree in business administration, and a master’s degree in strategic studies, and holds the GSLC, CISSP®, CISM and CISA certifications.

@g_mark

### MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™

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!

**“The information is very comprehensive and relevant for cybersecurity management professionals.”**

- Gerard Trotta, Citi

---

Course Day Descriptions

**DAY 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

**DAY 2: IP Concepts, Attacks Against the Enterprise, and Defense-in-Depth**
On this course day 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 the attack surface.

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

**DAY 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

**DAY 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

**DAY 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

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

**Course Author Statement**
“SANS designed the Security Leadership Essentials for Managers course to emulate the format utilized by many executive MBA programs. While core source material is derived from our highly regarded SANS Security Essentials program, we decided to focus this course on the big picture of securing the enterprise: network fundamentals, security technologies, using cryptography, defense-in-depth, policy development, and management practicum. This course includes executive briefings designed to present a distilled summary of vitally important information security topics like operating system security and security threat forecasts. Ultimately, the goal of this program is to ensure that managers charged with the responsibility for information security can make informed choices and decisions that will improve their organization’s security.”

-Stephen Northcutt

**“SANS prepared me for the certification and provided valuable information that I can use on the job immediately. Networking with peers and SANS@Nght provided extra value that’s not normally available at other training sessions.”**

-Rick Derks, FCS Financial
David R. Miller has been a technical instructor since the early 1980s and has specialized in consulting, auditing, and lecturing on information systems security, legal and regulatory compliance, and network engineering. David has helped many enterprises develop their overall compliance and security programs through policy writing; network architecture design including security zones; development of incident response teams and programs; design and implementation of public key infrastructures; security awareness training programs; specific security solution designs like secure remote access and strong authentication architectures; disaster recovery planning and business continuity planning; and pre-audit compliance gap analysis and remediation. He serves as a security lead and forensic investigator on numerous enterprise-wide IT design and implementation projects for Fortune 500 companies, providing compliance, security, technology, and architectural recommendations and guidance. Projects David has worked on include Microsoft Windows Active Directory enterprise designs, security information and event management systems, intrusion detection and protection systems, endpoint protection systems, patch management systems, configuration monitoring systems, and enterprise data encryption for data at rest, in transit, in use, and within email systems. David is an author, lecturer and technical editor of books, curriculum, certification exams, and computer-based training videos.

"This training was a comprehensive overview of all topics covered in the CISSP® exam. All in attendance were there for a common goal, including the instructor. It was easy to follow, and the real-world examples given were priceless."

-Ron Pinnock, Navy Exchange Service Command

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.

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

After completing the course students will have:
- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:
The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

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
Course Day Descriptions

**DAY 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

**DAY 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 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 2018 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)

**DAY 3: Security Engineering – Part 2; Communication and Network Security**
This course 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

**DAY 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

**DAY 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 discovery, logging and monitoring, and provisioning. We will discuss cutting-edge technologies such as the cloud, and we’ll wrap up day five with a deep dive into disaster recovery.

**Topics:** Domain 6: Security Assessment, Domain 7: Security Operations

**DAY 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

---

**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

---

“Great discussions and examples that provide a clear understanding and relate material to examples.”
-Kelley O’Neil, Wells Fargo

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
Frank is the founder of ThinkSec, a security consulting and CISO advisory firm. Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world. Frank continues to lead the management and software security curricula at SANS, helping to develop the next generation of security leaders. Frank was also executive director of cybersecurity at Kaiser Permanente, where he built an innovative security program to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $60 billion, 10 million members, and 175,000 employees. Frank holds degrees from the University of California at Berkeley and is the author and instructor of popular courses on strategic planning, leadership, application security, and DevOps.

@fykim

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.

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.
**Course Day Descriptions**

**DAY 1: Strategic Planning Foundations**
On this first day we will introduce the key elements of strategic security plans and lay the groundwork for the rest of the course. Creating strategic plans for security requires a fundamental understanding of the business and a deep understanding of the threat landscape.

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

**DAY 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

**DAY 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

**DAY 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

**DAY 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

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

“**This course provides invaluable info with specific guidance on how to perform leadership tasks as well as providing links to useful info...Outstanding.”**

-Jeff Haynes, NELO
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 so that it can be adjusted to work within the context and 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 and provide them with guidance and training. 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.

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 Security Operations Center (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

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

Christopher Crowley
SANS Principal Instructor

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. He is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP® certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration, and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities.

@CCrowMontance

"Insanely valuable content. This course is validating and filling in the gaps for my SOC."

-Robert Wysor, Duke Energy

Register at www.sans.org/network-security-2018 | 301-654-SANS (7267)
Course Day Descriptions

**DAY 1: 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

**DAY 2: 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

**DAY 3: 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

**DAY 4: 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

**DAY 5: 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 tabletop 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 compromises 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

“*This course touches on the art and science of cybersecurity operations management.*”

- Joanne Lim, Citibank

For course updates, prerequisites, special notes, or laptop requirements, visit [www.sans.org/event/network-security-2018/courses](http://www.sans.org/event/network-security-2018/courses)
MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep

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 life cycle
- 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

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 life cycle
- 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.Ps 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 recently been updated to fully prepare you for changes in the 2018 PMP® exam. 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 – Sixth 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 – Sixth 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 updated 2018 Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

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

PMP®, PMBOK®, and the PMI Registered Education Provider® logo are registered trademarks of the Project Management Institute, Inc.

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

**DAY 1: Project Management Structure and Framework**
This course day 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

**DAY 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

**DAY 3: Schedule and Cost Management**
Our third day details the schedule 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 milestone 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

**DAY 4: Communications and Project Resources**
During day four, we move into project and 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

**DAY 5: Quality and Risk Management**
On day five you will become familiar with quality planning, assurance, and control methodologies, as well as learn 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

**DAY 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

**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

“MGT525 offers tools and techniques that will directly improve the planning, execution, and closing of your projects.”

- Michael Long, ARCYBER

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
LEG523: Law of Data Security and Investigations

Day Program 30 CPES  Laptop Not Needed
Sun, Sep 23 - Thu, Sep 27 | 9:00am - 5:00pm

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 software, service 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)

LEG523 is constantly updated to address changing trends and current events. Here’s a sampling of what’s 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.
- How a breach involving EU data can lead to cascade of investigations into not just your security, but all aspects of your General Data Protection Regulation compliance, even if you have no physical presence in the European Union.
- Lessons from lost FBI text messages.
- How to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event

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

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

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security.

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.

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement personnel
- Privacy officers
- Penetration testers
- Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, civil defense and the like)

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

@benjaminwright
ICS410: ICS/SCADA Security Essentials

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 (ICS) 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.

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.

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

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

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/2018-network-security/courses

89
DEV522: Defending Web Applications Security Essentials

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.

Who Should Attend

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

Dr. Johannes Ullrich
SANS Senior Instructor

Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format. Listen to Johannes discuss “HTML5: Risky Business or Hidden Security Tool Chest for Mobile Web App Authentication” in this SANS webinar. @johullrich

“Brilliant! The combination of hands-on exercises and Q&A streamlines learning like nothing else.”
-McKell Gomm, Henry Schein
Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, and continuous integration pipelines. He serves on the advisory board for the SANS Securing the Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA.

Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, IA and outside the office enjoys spending time with his family, attending Iowa State athletic events, and playing golf.

@emjohn20

**DEV540: Secure DevOps and Cloud Application Security  NEW!**

This course covers how developers and security professionals can build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). It explains how principles, practices, and tools in DevOps and AWS can be leveraged to improve the reliability, integrity, and security of applications.

The first two days of the course cover how Secure DevOps can be implemented using lessons from successful DevOps security programs. Students build a secure DevOps CI/CD toolchain and understand how code is automatically built, tested, and deployed using popular open-source tools such as git, Puppet, Jenkins, and Docker. In a series of labs you learn to inject security into your CI/CD toolchain using various security tools, patterns, and techniques.

The final three days of the course cover how developers and security professionals can utilize AWS services to build secure software in the cloud. Students leverage the CI/CD toolchain to push application code directly to the cloud instead of to local servers on their class virtual machines. Students analyze and fix applications hosted in the cloud using AWS services and features such as API Gateway, IAM, signed cookies, Security Token Service, autoscaling, KMS, encryption, WAF, and Lambda for Serverless computing.

The course makes extensive use of open-source materials and tooling for automated configuration management ("Infrastructure as Code"), Continuous Integration, Continuous Delivery, Continuous Deployment, containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring.

This course also makes extensive use of AWS and associated developer tools such as CloudFormation, CodeCommit, CodeBuild, CodePipeline, and other cloud application services so students can experience how these services can be utilized in their applications.

**You Will Be Able To**
- Understand the core principles and patterns behind DevOps
- Map out and implement a Continuous Delivery/Deployment pipeline
- Map out where security controls and checks can be added in Continuous Delivery and Continuous Deployment
- Integrate security into production operations
- Create a plan for introducing – or improving – security in a a DevOps environment
- Move your DevOps workflows to the cloud
- Consume cloud services to secure cloud applications

**Who Should Attend**
- Anyone working in the DevOps environment or transitioning to a DevOps environment
- Anyone who wants to understand where to add security checks, testing, and other controls to DevOps and Continuous Delivery
- Anyone interested in learning how to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in learning how to leverage cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

*“Extremely relevant to our DevOps/CICD journey.”* - Devon D., USAA

**Eric Johnson | SANS Certified Instructor**

Eric Johnson is a Principal Security Consultant at Cypress Data Defense, where he leads secure software development lifecycle consulting, web and mobile application penetration testing, secure code review assessments, static source code analysis, security research, and security tools development. He also founded the Puma Scan static analysis open-source project, which allows software engineers to run security-focused .NET static analysis rules during development and in continuous integration pipelines. At the SANS Institute, Eric authors application security courses on DevOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Securing the Human Developer awareness training program, delivers security training around the world, and has presented his security research at conferences including BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA.

Eric completed a bachelor of science degree in computer engineering and a master of science degree in information assurance at Iowa State University, and currently holds the CISSP®, GWAPT, GSSP-.NET, and GSSP-Java certifications. He is based in West Des Moines, IA and outside the office enjoys spending time with his family, attending Iowa State athletic events, and playing golf.

@emjohn20

For course updates, prerequisites, special notes, or laptop requirements, visit www.sans.org/event/network-security-2018/courses
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.

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

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

Aaron Cure | SANS Instructor
Aaron is a senior security consultant at Cypress Data Defense and an instructor and contributing author for the DEV544 Secure Coding in .NET course. After 10 years in the U.S. Army as a Russian linguist and a satellite repair technician he worked as a database administrator and programmer on the Iridium project, with subsequent positions as a telecommunications consultant, senior programmer, and security consultant. He also has experience developing security tools, performing secure code reviews, vulnerability assessments, and penetration testing, as well as risk assessments, static source code analysis, and security research. Aaron holds the GIAC GSSP-.NET, GWAPT, GMOB, and CISSP® certifications and is based in Arvada, CO. Outside the office Aaron enjoys boating, travel, and playing hockey.
Cyber Defense | Short Courses

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

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 agencies (including NSA, DHS, GAO, and many others) and private organizations 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 find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented. SEC440 does not contain any labs. Students looking for hands-on labs involving the Critical Controls should take SEC566.

“Gives specific direction for understanding risks and building a program to address them.”
- Eric Pierce, Mindbody

**SEC455: SIEM Design and Implementation NEW!**

Security Information and Event Management (SIEM) can be an extraordinary benefit to an organization’s security posture, but understanding and maintaining it can be difficult. Many solutions require complex infrastructure and software that necessitate professional services for installation. The use of professional services can leave security teams feeling as if they do not truly own or understand how their SIEM operates. Combine this situation of complicated solutions with a shortage of available skills, a lack of simple documentation, and the high costs of software and labor, and it is not surprising that deployments often fail to meet expectations. A SIEM can be the most powerful tool a cyber defense team can wield, but only when it is used to its fullest potential. This course is designed to address this problem by demystifying SIEMs and simplifying the process of implementing a solution that is usable, scalable, and simple to maintain.

The goal of this course is to teach students how to build a SIEM from the ground up using the Elastic Stack. Throughout the course, students will learn about the required stages of log collection. We will cover endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, and we will combine these components to make a flexible, high-performance SIEM solution. Using this approach empowers SIEM engineers and analysts to understand the complete system, make the best use of technology purchases, and supplement current underperforming deployments. This process allows organizations to save money on professional services, increase the efficiency of internal labor, and develop a nimbler solution than many existing deployments. For example, many organizations pay thousands of dollars in consulting fees when a unique log source needs a custom parser. This course will train students how to easily parse any log source without requiring consulting services, saving their organizations both time and money, and facilitating faster collection and use of new log sources.

“SANS training is relevant, concise and laser-focused on the exact topics relevant to my daily routine.”
- Alex Rifman, Anomali

**SEC524: Cloud Security Fundamentals**

SEC524: Cloud Security Fundamentals teaches you how to properly evaluate cloud providers, and perform risk assessment and review, with a focus on risk assessment versus technical implementation and operations. This course will discuss 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.
Penetration Testing | Short Courses

SEC564: Red Team Operations and Threat Emulation

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization’s overall security to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization’s security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security test and relies heavily on well-defined TTPs, which are critical to successfully emulating a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist.

Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate them. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing. This two-day course will explore Red Team concepts in-depth, provide the fundamentals of threat emulation, and help you reinforce your organization’s security posture.

“The content from SEC564 is great and I will be able to implement it in my organization right away!”

- Kirk Hayes, Rapid 7

SEC580: Metasploit Kung Fu for Enterprise Pen Testing

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 confirm vulnerabilities using an open-source and easy-to-use framework. This course will help students get the most out of this free tool.

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

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

“SEC580 definitely covers what I need to have for my metasploit skills.”

- Vincent Bartsch, Cubic Transportation Systems
MGT415: A Practical Introduction to Cyber Security Risk Management

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and 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 to best defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

“Our company is creating a formal cyber risk and controls assessment program. This class was a perfect introduction to the topic.”
- Jim Schleske, Ball Aerospace

MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their workforce. As a result, people, not technology, have become the most common target for cyber attackers. The most effective way to secure the human element is to establish a mature security awareness program that goes beyond just compliance, changes peoples’ behaviors and ultimately creates a secure culture. This intense two-day course will teach you the key concepts and skills needed to do just that, and is designed for those establishing a new program or wanting to improve an existing one. Course content is based on lessons learned from hundreds of security awareness programs from around the world. In addition, you will learn not only from your instructor, but from extensive interaction with your peers. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

“It will help me build a first-rate, top-notch awareness program.”
- Geoff Parker, Cheniere Energy Inc.

DEV531: Defending Mobile Applications Security Essentials

Mobile application development is growing exponentially year over year. As of late 2015, over 3 million apps were deployed in the Apple and Google app stores. These apps are consumed by over 700 million users world-wide and account for 33% of the traffic on the Internet. Average users have over 100 mobile apps installed on their device, many of which provide business critical services to customers and employees.

Unfortunately, these apps are often rushed to market to gain a competitive advantage with little regard for security. As seen in web applications for the past 20 years, software vulnerabilities always exist where code is being written, and mobile apps are no different. Mobile apps are vulnerable to a whole new class of vulnerabilities, as well as most traditional issues that have long plagued web and desktop applications. This problem will only continue to grow unless managers, architects, developers, and QA teams learn how to test and defend their mobile apps.

DEV531: Defending Mobile Applications Security Essentials 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.
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.

During Days One and Two of this course, 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 in order to assess their own company’s security posture or to augment their career as a penetration tester.

On Days Three and Four, students will learn to evaluate physical barriers, defensive lighting, doors, external and internal physical intrusion detection systems, camera placement, access controls, and standard operating procedures. They will also be exposed to best practice standards and a robust variety of adversarial methodologies used to compromise weak targets such as social engineering and the exploitation of a weak employee culture. Numerous in-depth case studies and practical hands-on demonstrations will be utilized to solidify the acquisition of knowledge.

The training concludes on Days Five and Six with an intense specialization focus: electronic access control systems and badge readers. Students will be immersed in the world of 125KHz (low frequency) credentials, vehicle transponders, 13.56MHz (high frequency) credentials, and smart cards. Whether an enterprise is using HID Prox cards, NXP Hitag chips, Mifare credentials, or even iCLASS technology, students who have taken this course will be well-versed in the functionality, weaknesses, and attack vectors of such systems. From how to perform practical card cloning attacks in the field to advanced format downgrade attacks, students will be prepared for real-world red team scenarios and learn how to exploit access control technology with the latest attack hardware. There are also modules detailing the backend of such systems, which opens the door to Man in the Middle and Denial of Service attacks.

By the end of this course, students will be very prepared to make educated and fiscally responsible security decisions not only for their respective organizations but also for themselves. Participants will be able to approach any target, sight-unseen, and then either conduct a walk through assessment highlighting attack vectors, or proceed directly with an attack, gaining physical access to critical areas and infrastructure. Additionally, these newly-minted professionals in our training will also be able to provide sound documentation while making recommendations to management or to their insurance providers, saving money for their companies.
Bonass Sessions

Enrich your SANS training experience! Evening talks led by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

**KEYNOTE:** **WMI Attacks: What You Don’t Know CAN Hurt You**

Chad Tilbury

In the spectrum of things that keep enterprise security teams up at night, Windows Management Instrumentation (WMI) should be heading to the forefront. Advanced adversaries are increasingly adding WMI-based attacks to their repertoires, and most teams are woefully unprepared to face this new threat. You need to understand what you are up against, and attendees will leave this presentation with a comprehensive overview of the state of WMI hacking, including real-world examples of nation-state and criminal actor tradecraft. Once you have a strong understanding of the threat, Chad will pivot to defense and discuss detection tools and analysis techniques. While parts of this presentation will necessarily be technical, even less technically oriented attendees will leave with a greater understanding of the threat and a checklist of actionable steps to better increase their organization’s security posture.

**Traveling Paranoid (But Not Too Paranoid)**

Philip Hagen and Chris Crowley

As every security professional knows, travel can be even more stressful when you’re carrying multiple laptops, evidence drives, mobile devices, connection cables, and the like. Whether traveling domestically or internationally, your private data and those of your clients are arguably at the greatest risk when transiting customs or other airport screening points. You must realistically consider whether you would give up encryption passwords or forfeit your hardware at a border crossing, for example. Now, consider how people within your organization would deal with the same challenges. How should you equip them for international and domestic travel without creating an imposition on their busy schedules? How can you keep up with delivering information to traveling staff? What advice do you give them regarding foreign (or domestic) customs agents demanding passwords and data access? What sort of knowledge do you want to develop about attempts to access your information assets while your staff travels? This talk will cover various practical ways we can protect electronic interests in various common situations for you and your organization. We’ll cover both preventive measures as well as mechanisms to detect whether your gear has been fiddled with while outside your immediate control. Measures for various operating systems will be addressed, while considering how to maintain practical paranoia without drawing attention to yourself.

**Blockchain: The New Digital Swiss Army Knife?**

G. Mark Hardy

Blockchain as a technology has been proposed as a solution to everything from frictionless currency transfer to tracking cargo on ships. With over $1 billion in venture funds invested and several hundred patents filed, every security professional must know the impact on organizations in terms of risk, volatility, and competitiveness. This talk will explore alternative uses for blockchain technology other than cryptocurrency, and provide a framework for utilizing and securing a technology considered as disruptive as the Internet was in the 1990s.

**“Could We Have Stopped This?” Attack Simulations for Blue Team Hardening**

Alissa Torres

A post-compromise, post-remediation security team is made up of steely-eyed veterans, tempered by the fire of system ownage and soul-wrenching defense and detection failures. Their experience is invaluable, but arrived at with significant cost to the organization. How can we grow such a hardened blue team of this meddle without the cost and pain of time on the battlefield? Start by going beyond the tabletop walk-throughs and testing the “load bearing” capacity of your threat detection and response (TDR) people, process and technology. Throw your team into simulations of the hard stuff; real-world challenges that model complex multi-pronged attacks. Join Alissa Torres for this one-hour session walk-through of stress-test techniques that develop your blue team, and stop checking annual compliance boxes.

**So, You Wanna Be a Pen Tester?**

Adrien de Beaupre

This presentation will discuss the things that you will actually need to become a penetration tester. Be prepared for a no-fluff honest discussion. You will need attitude, aptitude, initiative, desire, dedication, discipline, integrity, ethics, experience, knowledge, and tools.

**Continuous Security: Monitoring and Active Defense in the Cloud**

Eric Johnson

Monitoring and feedback loops from production are a critical tenant in DevOps for measuring performance, runtime errors, statistics, and changes. In the SecDevOps world, security teams can take advantage of DevOps monitoring tools to increase security visibility, identify anomalies, and respond swiftly to real-time attacks. Cloud providers are offering powerful infrastructure, development, and application continuous monitoring services that generate a wealth of data. But building continuous security monitoring on top of the data can be challenging. Where are the log files? What is the log file format? What security events are captured? How do we display meaningful metrics? Can we detect and defend in real time? This talk will introduce attendees to a realistic Amazon Web Service environment’s monitoring and active defense system and discuss real data collected during a war game exercise. Afterwards, we will walk through the postmortem, review the alerts raised during the incident, determine if there were any surprises, and identify opportunities to improve the system. Attendees will walk away with actionable techniques for building an active defense framework to help protect their organization’s cloud resources.

**Hacking Dumberly, Just Like the Bad Guys**

Tim Medin

Tim Medin will discuss the dumbest red team tricks and hacks he’s encountered over the years. He is going to take the A out of APT, because so few attackers really need to use advanced techniques. He’ll also discuss the simple defenses that make an attacker’s life much more difficult.
How to Write Presentation Proposals That Get Selected for Cybersecurity Conferences

Women’s Connect Workshop – Sponsored by SANS Summits
Alissa Torres, Heather Mahalik, My-Ngoc Nguyen, Phil Hagen, Rebekah Brown, and Sarah Edwards

Just in case no one has said this to you yet, you have an interesting, unique, and important perspective on cybersecurity that is worth sharing. Yes, YOU. The agenda at many cybersecurity events looks like a line-up of the usual suspects. But the community needs to hear diverse viewpoints. While it may feel intimidating to throw your hat into the ring, and no one likes rejection, we need your voice. SANS is committed to identifying and developing talented cybersecurity professionals. In this workshop, some of the top SANS instructors and seasoned industry speakers will arm you with the tools to draft presentation proposals that make it onto the agenda. Join Alissa Torres, Heather Mahalik, My-Ngoc Nguyen, Phil Hagen, Rebekah Brown, and Sarah Edwards, who will share their experience and advice. This is your chance to work through the ideas you’ve been percolating and get answers to all the questions you haven’t been able to ask until now. This workshop is open to anyone interested in building the skills and confidence to deliver presentations at cybersecurity events.

Responding to the European Union’s New General Data Protection Regulation
Ben Wright

The European Union has long been a leader in privacy law. It has now advanced the law with a sweeping new regulation that applies to a broad range of companies around the world, even those that do not have a physical presence in Europe. We will discuss how to manage risk under this new regulation.

Nation-State-Level Honeypotting: Emulating Vulnerable Applications at Scale
Dr. Johannes Ullrich

Honeypots have been used for a long time to learn more about how attackers are targeting and exploiting vulnerable systems. Web applications in particular have been one of the primary targets of attackers and honeypots have been used to understand these attacks better. However, applications are very diverse. Hundreds if not thousands of different vulnerable applications can easily be exploited, and new ones are regularly added to the list. In this talk, you will learn how you can participate in our large-scale agile honeypot network that can easily be tuned to detect and collect metrics for the attack of the day, and that is large enough to rival the size of some nations’ infrastructure.

Coffee and Donuts with the Graduate Students
Get the inside scoop on what it’s like to pursue a graduate degree in cybersecurity from SANS from like-minded information security professionals currently enrolled in the SANS graduate programs. SANS regionally accredited graduate program, the SANS Technology Institute, combines SANS technical training and certifications with leadership and management curriculum specifically designed for the unique needs of aspiring leaders. Find out how the class you’re taking this week may be applied towards a master’s degree or graduate certificate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.

Let’s Go Hunting Bad Guys
John Strand

In this presentation, John will share with you custom free tools on hunting bad guys inside and outside of your network...with awesomeness and math. But mostly math.

Defense Is Doable: Breaking the Cyber Kill Chain
Erik Van Buggenhout & Stephen Sims

Recent security incidents and breaches often make it look like there’s no way of preventing adversaries from compromising your environment. During this fast-paced presentation, Erik Van Buggenhout (SANS Certified Instructor) and Stephen Sims (SANS Fellow) will discuss how advanced adversaries are attempting to penetrate your environment and what you can do to stop or detect them. The talk will focus on principles and techniques that are readily available to all (or most) organizations, WITHOUT breaking the bank to purchase a myriad of commercial tools. The material covered is a sample of the content in our new course, SANS SEC599: Defeating Advanced Adversaries – Implementing Kill Chain Defenses. One example that will be covered is how to use Windows Credential Guard to stop tools such as Mimikatz from being used to compromise credentials.

Stuck in the Box, a SIEM’s Tale
Justin Henderson

Organizations often spend excessive amounts of money on Security Information and Event Management (SIEM) products only to end up with a log collection box when they thought they purchased a tactical detection system. Most organizations find themselves with a SIEM but unsure how to use its capabilities. Point solutions are quick to defend deficiencies by stating each environment is different so you, the customer, must tell them what you want the SIEM to do and then they’ll help with professional services or by replacing your current SIEM with something “better and more advanced.” This is complete hogwash. Organizations tend to have a lot of overlap such as the use of Windows systems or network protocols such as DNS. As such there are high-fidelity detects that can be implemented in every organization. Enough is enough. If you are looking for techniques and methods to get value out of your current SIEM or are interested in seeing how a new open-source big data solution such as the Elastic Stack, formerly ELK, most likely can beat what you have today, then this talk is for you. Fact is that it is time to think outside the box. Come find out how one organization spent 14 months deploying a top magic quadrant SIEM solution to have it beaten by ELK in two weeks.

An Evening of Hacking the Internet of Things (IoT)
Stephen Sims, James Lyne, Tim Medin, & Jim Shewmaker

Somewhere along the line product developers thought it would be a good idea to connect things like pet food dispensers, BBQ grills, refrigerators, and many other “items” to the Internet. What could possibly go wrong? We will have a collection of “things” for you to try and find vulnerabilities in, as well as some guided exercises... If you find something interesting you may even be able to take the item home! We’ll walk through an introduction of how to extract and analyze firmware, and the types of bugs that are most commonly found, along with some examples. What do you need to bring? A laptop with VMware Player, Workstation, or Fusion, and a copy of Kali Linux. We will have some USB sticks on it with Kali if you forget to bring a copy.

Register at www.sans.org/network-security-2018 | 301-654-SANS (7267)
Future Training Events

**SANSFIRE**

<table>
<thead>
<tr>
<th>City</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washington, DC</td>
<td>Jul 14-21</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>City</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pittsburgh</td>
<td>Pittsburgh, PA</td>
<td>Jun 25-30</td>
</tr>
<tr>
<td>Boston Summer</td>
<td>Boston, MA</td>
<td>Aug 6-11</td>
</tr>
<tr>
<td>San Antonio</td>
<td>San Antonio, TX</td>
<td>Aug 6-11</td>
</tr>
<tr>
<td>New York City Summer</td>
<td>New York City, NY</td>
<td>Aug 13-18</td>
</tr>
<tr>
<td>Northern Virginia – Alexandria</td>
<td>Alexandria, VA</td>
<td>Aug 13-18</td>
</tr>
<tr>
<td>Virginia Beach</td>
<td>Virginia Beach, VA</td>
<td>Aug 20-31</td>
</tr>
<tr>
<td>Chicago</td>
<td>Chicago, IL</td>
<td>Aug 20-25</td>
</tr>
<tr>
<td>San Francisco Summer</td>
<td>San Francisco, CA</td>
<td>Aug 26-31</td>
</tr>
<tr>
<td>Tampa-Clearwater</td>
<td>Tampa, FL</td>
<td>Sep 4-9</td>
</tr>
<tr>
<td>Baltimore Fall</td>
<td>Baltimore, MD</td>
<td>Sep 8-15</td>
</tr>
</tbody>
</table>

Future Summit Events

<table>
<thead>
<tr>
<th>City</th>
<th>Location</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Orleans, LA</td>
<td>New Orleans, LA</td>
<td>Jun 25-30</td>
</tr>
<tr>
<td>Charleston, SC</td>
<td>Charleston, SC</td>
<td>Aug 6-15</td>
</tr>
<tr>
<td>New York City, NY</td>
<td>New York City, NY</td>
<td>Aug 20-27</td>
</tr>
<tr>
<td>New Orleans, LA</td>
<td>New Orleans, LA</td>
<td>Sep 6-13</td>
</tr>
<tr>
<td>Anchorage, AK</td>
<td>Anchorage, AK</td>
<td>Sep 10-15</td>
</tr>
</tbody>
</table>

Future Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit [www.sans.org/community](http://www.sans.org/community) for up-to-date Community course information.

Take SANS Training Anytime, Anywhere with OnDemand

More than 30 of the most popular SANS courses are available in our online training format OnDemand, and all include:

- Four months of online access to your course
- Subject-matter-expert support
- Training with SANS top instructors
- All printed books and materials
- Labs and quizzes to reinforce your learning
- No travel required

Visit [www.sans.org/ondemand](http://www.sans.org/ondemand) to learn more about your OnDemand training options.
Cancellation & Access Policy

If an attendee must cancel, a substitute may attend instead. Substitution requests can be made at any time prior to the event start date. Processing fees will apply. All substitution requests must be submitted by email to registration@sans.org.

If an attendee must cancel and no substitute is available, a refund can be issued for any payments received by August 29, 2018. A credit memo can be requested up to the event start date. All cancellation requests must be submitted in writing by mail or fax and received by the stated deadlines. Payments will be refunded by the method that they were submitted. Processing fees will apply.

SANS Voucher Program

Expand your training budget!

For organizations with multiple employees taking SANS training courses, the SANS Voucher Program is an easy-to-use, flexible training management solution. Based on the number of anticipated students and investment, you may be eligible to receive bonus funds from SANS. Your investment and bonus funds can be used for classroom and online training, and can also be used to purchase GIAC certifications. See page 8 or contact SANS for more detailed information about our Voucher Program. www.sans.org/vouchers

Caesars Palace

3570 Las Vegas Blvd. South | Las Vegas, NV  89109
877-427-7243
www.sans.org/event/network-security-2018/location

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

Top three reasons to stay at the Caesars Palace

1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Caesars Palace, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
3. SANS schedules morning and evening events at the Caesars Palace that you won’t want to miss!

Special Hotel Rates Available

A special discounted rate of $195.00 S/D will be honored based on space availability.

These rates include high-speed Internet in your room (2-device connections per day). All reservations must be guaranteed with a deposit for the first night’s guestroom and tax charge. If guaranteed by a credit card, the first night’s guestroom and tax charge, per room, will be billed immediately to the cardholder’s account. Government per diem rooms are available at the prevailing rate, with proper ID.

An optional, discounted resort fee of $35.00/day plus taxes includes unlimited local phone calls and two guest passes to the fitness center (does not include spa). The resort fee can be added to your reservation but is not required. You do have the option to utilize and pay for the above services per use as needed at the prevailing rates.

Register online at www.sans.org/network-security-2018

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

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

An email confirmation will be sent to you when once the registration form has been completed. If you have not received this email confirmation within two business days of registering, please call 301-654-7267 or contact registration@sans.org for assistance.

Pay Early and Save*

<table>
<thead>
<tr>
<th>DATE</th>
<th>DISCOUNT</th>
<th>DATE</th>
<th>DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay &amp; enter code by</td>
<td>8-1-18</td>
<td>$400.00</td>
<td>8-22-18</td>
</tr>
</tbody>
</table>

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS SIMULCAST

Nothing beats the SANS live training experience, but if you are unable to attend, learn how you can register for a SANS Network Security 2018 Simulcast course. Visit www.sans.org/event/network-security-2018/attend-remotely
<table>
<thead>
<tr>
<th>Courses</th>
<th>Paid before 8-1-18</th>
<th>Paid before 8-22-18</th>
<th>Paid after 8-22-18</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC201 Introduction to Cyber Security</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC401 Security Essentials Bootcamp Style</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>SEC460 Enterprise Threat and Vulnerability Assessment</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC487 Open-Source Intelligence Gathering and Analysis</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC501 Advanced Security Essentials – Enterprise Defender</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC503 Intrusion Detection In-Depth</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC505 Securing Windows and PowerShell Automation</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC506 Securing Linux/Unix</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>SEC510 Continuous Monitoring and Security Operations</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC542 Web App Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC545 Cloud Security Architecture and Operations</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC555 SIEM with Tactical Analytics</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>SEC560 Network Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC566 Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC573 Automating Information Security with Python</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC575 Mobile Device Security and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC599 Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC617 Wireless Penetration Testing and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC642 Adv. Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>SEC760 Advanced Exploit Development for Penetration Testers</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR500 Windows Forensic Analysis</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR518 Mac and iOS Forensic Analysis and Incident Response</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR526 Memory Forensics In-Depth</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>FOR578 Cyber Threat Intelligence</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>FOR585 Advanced Smartphone Forensics</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT443 SANS Training Program for CISSP® Certification</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™</td>
<td>$5,420</td>
<td>$5,620</td>
<td>$5,820</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT576 Security Strategic Planning, Policy, and Leadership</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT577 Managing Security Operations: Detection, Response, and Intelligence</td>
<td>$5,420</td>
<td>$5,620</td>
<td>$5,820</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>LEG523 Law of Data Security and Investigations</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td></td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>ICS410 ICS/SCADA Security Essentials</td>
<td>$5,310</td>
<td>$5,510</td>
<td>$5,710</td>
<td>$1,260</td>
<td>$729</td>
<td></td>
</tr>
<tr>
<td>DEV522 Defending Web Applications Security Essentials</td>
<td>$5,810</td>
<td>$6,010</td>
<td>$6,210</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>DEV540 Secure DevOps and Cloud Application Security</td>
<td>$4,980</td>
<td>$5,180</td>
<td>$5,380</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>DEV544 Secure Coding in .NET: Developing Defensible Applications</td>
<td>$4,470</td>
<td>$4,670</td>
<td>$4,870</td>
<td>$1,260</td>
<td>$729</td>
<td>$1,260</td>
</tr>
<tr>
<td>HOSTED Physical Security Specialist – Full Comprehensive Edition</td>
<td>$6,910</td>
<td>$6,910</td>
<td>$6,910</td>
<td></td>
<td>$729</td>
<td>$1,260</td>
</tr>
</tbody>
</table>

### Skill-Based Short Courses

<table>
<thead>
<tr>
<th>Courses</th>
<th>Course fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC440 Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$1,860</td>
</tr>
<tr>
<td>SEC455 SIEM Design &amp; Implementation</td>
<td>$1,860</td>
</tr>
<tr>
<td>SEC434 Cloud Security Fundamentals</td>
<td>$1,860</td>
</tr>
<tr>
<td>SEC564 Red Team Operations and Threat Emulation</td>
<td>$1,860</td>
</tr>
<tr>
<td>SEC580 Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$1,860</td>
</tr>
<tr>
<td>MGT415 A Practical Introduction to Cyber Security Risk Management</td>
<td>$1,860</td>
</tr>
<tr>
<td>MGT433 SANS Security Awareness: How to Build, Maintain, and Measure a Mature Security Awareness Program</td>
<td>$1,860</td>
</tr>
<tr>
<td>DEV531 Defending Mobile Applications Security Essentials</td>
<td>$1,860</td>
</tr>
<tr>
<td>SPECIAL Core NetWars Experience – Tournament Entrance Fee</td>
<td>FREE</td>
</tr>
<tr>
<td>SPECIAL DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
</tr>
<tr>
<td>SPECIAL Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
</tr>
<tr>
<td>SPECIAL ICS NetWars – Tournament Entrance Fee</td>
<td>FREE</td>
</tr>
</tbody>
</table>

### Early Bird Discounts

Pay for any long course using the code EarlyBird18 at checkout by August 1st to get $400 OFF or by August 22nd to get $200 OFF*  
*Some restrictions apply. Early bird discounts do not apply to Hosted courses.
As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

Join the SANS.org community today to enjoy these free resources at www.sans.org/account

Newsletters
NewsBites
Twice-weekly, high-level executive summary of the most important news relevant to cybersecurity professionals.

OUCH!
The world’s leading monthly free security awareness newsletter designed for the common computer user.

Webcasts
Ask the Experts 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.

@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.

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.

Other Free Resources (No SANS account is necessary)
- 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/network-security-2018

SAVE $400
Register and pay by August 1st
Use code EarlyBird18

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

NALT-BRO-NS2018