SANSFIRE 2020
Washington, DC | June 13-20 | netWARS

No matter what cybersecurity skills you need to learn or which certifications you’re hoping to obtain, SANS and GIAC have you covered. Choose from 45+ hands-on courses taught by the industry’s top practitioners, giving you the knowledge and skills you need to validate your expertise with a GIAC certification.

“SANS is the best information security training you’ll find anywhere. World-class instructors, hands-on instruction, actionable information you can really use, and NetWars!”

— Jeff Stebelton, Netjets, Inc.
For more than 30 years and counting, the SANS Institute has been committed to supporting its growing community of cybersecurity professionals. SANS offers a variety of ways for professionals working in global enterprises and government organizations to increase their knowledge and skills, as well as share knowledge across their peer network.

You can get to know SANS by looking at the numbers below, and you can see these programs in action by visiting sans.org

**THE SANS PROMISE**

You will be able to use the skills you’ve learned in our training and programs immediately.

- **120+** Certified Instructors
- **65+** Cybersecurity Courses
- **35+** GIAC Certifications
- **40,000** SANS Students per Year
- **3,000** Subject-Matter Expert Whitepapers
- **137,000+** Certifications Issued
- **30** Countries Featuring SANS Courses
- Security Awareness and Phishing Training
- Weekly Educational Webcasts, Podcasts, Newsletters, the Internet Storm Center, and much more.
- Graduate and Undergraduate Programs, and Academies
At SANS, our course authors and instructors are renowned cybersecurity experts who share their knowledge by drawing on their own real-world experiences and top-shelf curriculum. Industry professionals choose SANS training again and again, year after year, for access to these highly regarded experts.

There are only about 120 individuals in the world currently qualified as SANS Certified Instructors. Each is selected after proving his or her technical and teaching expertise through years of work and success. The instructors are the founders of international cybersecurity organizations, authors of best-selling books, and developers of the world’s most advanced cyber ranges and Capture-the-Flag challenges. Many are regularly called upon to share their expertise with government and commercial organizations around the world.

In addition to their impressive résumés, every member of the SANS faculty is fully committed to providing the most comprehensive training possible. Our instructors do more than just stand in front of a classroom—they’re present for their students every step of the way, with follow-ups, webcasts, mentoring, and more. Their goal is your success, and that dedication is what truly sets SANS training apart from all the rest.

Whether you train with SANS online or at one of our live events, we promise you’ll be able to apply what you learn from these top-tier instructors as soon as you return to work.

Meet the SANS faculty: sans.org/sansfire/instructors
Securing Approval and Budget for Training

As a cybersecurity professional, you already know that SANS is the most trusted resource for the training you need. But getting buy-in from your manager or the C-Suite can be a challenge—especially if they don’t yet understand the benefits that SANS training can bring. By following some simple guidelines, you can show them what they need to know, and get them to support your training.

Packaging matters

Submit a formal request

- Most successful training requests are made via a written document—a short memo or a few slides—justifying the need for training. Training request templates are available for popular SANS courses. They can be found in the “Justify Your Training” section of the course page. Most managers will respect and value the effort you put in to provide written justification.
- A formal request is a chance for you to provide all the necessary information in one place. If you include additional SANS resources, you can give your manager context and present your request as a complete package. Some helpful additions include the “Why SANS?” web page, the Training Roadmap, an instructor bio, and a course description.

Clearly state the benefits

Be specific

- How does the course relate to your job? Will it help you establish baseline skills? Transition to a more focused role? Decision-makers need to understand the plan.
- Highlight specific tasks you’ll be able to take on as a result of the training. Each SANS course description includes a section titled “You Will Be Able To.” Include this section in your request to make the benefits clear. Match the training to your job tasks and goals.

Set the context

Establish long-term expectations

- Cybersecurity is a specialized career path within IT. Its practices evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of team salaries to keep skills current. Training for such a dynamic field is an annual, per-person expense—not a once-and-done item.
- Sign up for the related GIAC certification in order to validate that you learned the skills taught in the class. Your employer can be confident you learned what they paid for, since GIAC exams are psychometrically designed to confirm competency in job-related tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expenses into their employment agreements when they’re hired; some offer to stay for a year after they complete the training.
Build a High-Performing Security Organization

Based on our global research, SANS has identified effective strategies for building an information security group:

Use practical organizing principles to design your plan. Nearly all of the more complex frameworks may be reduced to a few simpler constructs, such as “Build and Maintain Defenses – Monitor and Detect Intrusion – Proactively Self-Assess – Respond to Incidents.”

Prioritize your efforts within these areas using the Center for Internet Security Critical Controls as you mature your own organization.

Determine the number and types of professionals you need to perform the hands-on work, then launch an ongoing campaign to develop a team with the appropriate skills in mind. Cybersecurity is a specialized practice area within IT, and demands specialized training.

The job roles and skills required in information security grow and change as the organization scales. While every professional needs a baseline of knowledge and capabilities in cyber defense and incident response, over time you will develop specialized members of your team to work together in particular areas.

Four critical job roles typically emerge:

• Security Monitoring & Detection Professionals – Identifying security anomalies within your environment requires an increasingly sophisticated set of skills. All too often, vendor training teaches to the tool, without explaining how the tool works or how it can be best used. To deploy detection and monitoring tools and interpret their output, you need a more robust understanding of tools, techniques, and analysis.

• Pen Testers & Vulnerability Analysts – A professional who can find weaknesses is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires a different set of tools and a different way of thinking, but it’s still essential in improving defenses.

• Forensic Investigators & Incident Responders – Large organizations need specialized professionals who can move beyond first-level incident response. Whether you’re maintaining a trail of evidence or hunting for threats, you need the skills to analyze attacks and develop appropriate remediation and recovery plans.

• Security Managers – As their staffs of talented technologists grow, organizations require effective leaders to manage them. These managers won’t necessarily perform hands-on work, but they must understand enough about underlying technologies and frameworks to help set security strategy, develop appropriate policies, interact with their skilled practitioners, and measure outcomes.

Within (or beyond) these four areas, a high-performing security organization will develop its professional staff even further, with some individuals covering more areas while others go deeper into just one specialty. Along the entire spectrum from active defense to cloud defense, and from Python for InfoSec professionals to malware reengineering, SANS and GIAC offer more than 65 courses and 35 certifications for professionals at every level.
Cybersecurity Training Roadmap

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

Focus Job Roles

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

Security essentials
- Essentials 301: Introduction to Cyber Security | GSF

Core techniques
- Prevention, Defense, and Monitoring

Security management
- Managing Technical Security Operations

Monitoring & Detection
- Intrusion Detection, Monitoring Over Time
- Scan Packets & Networks

Penetration Testing
- Vulnerability Analysis, Ethical Hacking
- Every Pen Tester Should Know
- Networks: SEC696 Network Penetration Testing and Ethical Hacking | GPN
- Web Apps: SEC493 Web App Penetration Testing and Ethical Hacking | GWAPT

Incident Response & Threat Hunting
- Host & Network Forensics
- Every Forensic and IR Professional Should Know
- Endpoint Forensics: FOR501 Windows Forensic Analysis | GCFI
- FOR505 Advanced Incident Response, Threat Hunting, Analysis, and Incident Response | GBAR

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A bare minimum of team/blue team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Penetration testing skills are essential for defense specialists to improve their defenses.

Whether you’re seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

Baseline Skills

How to Cyber Security
- Concepts, Tools, & Skills

New to Cyber Security
- SEC301 Introduction to Cyber Security | GSF

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

Penetration Testing
- SEC493 Web App Penetration Testing and Ethical Hacking | GWAPT
- SEC501 Advanced Incident Response, Threat Hunting, Analysis, and Incident Response | GBAR
- SEC505 Windows Forensic Analysis | GCFI

Incident Response & Threat Hunting
- Host & Network Forensics
- SEC493 Web App Penetration Testing and Ethical Hacking | GWAPT

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations
- Handle Specific Defenses

Specialized Defensive Area
- Blue Team | SEC450 Blue Team Fundamentals: Security Operations and Analysis
- GSWT | SEC440 Open-Source Intelligence (OSINT) Gathering and Analysis
- Cloud Security | SEC496 Cloud Security Architecture and Operations
- Windows/PowerShell | SEC496 Securing Windows and PowerShell Automation | GWAPT
- Linux/Unix Defense | SEC596 Securing Linux/Unix | GCEO
- CDRM | SEC555 CDRM with Tactical Analysis | GCDA

Other Advanced Defense Courses
- Security Architecture: SEC520 Defensible Security Architecture and Engineering | GCEO
- Adversary Emulation: SEC595 Defending Advanced Adversaries – Purple Team Tactics and Red Team Defenses | GCD

Specialized Penetration Testing
- Focused Techniques & Areas
- In-Depth Coverage

Vulnerability Assessment: SEC448 Enterprise Threat and Vulnerability Assessment | GCDA
- Networks: SEC496 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GCPM
- SEC596 Advanced Pragmatic Defense for Penetration Testers
- SEC424 Advanced Web App Ethical Testing, Ethical Hacking, and Exploitation Techniques
- Mobile: SEC455 Mobile Device Security and Ethical Hacking | GCEO
- Wireless: SEC497 Wireless Penetration Testing and Ethical Hacking | GWAPT
- Python Coding: SEC597 Automating Information Security with Python | GPYC

Digital Forensics, Malware Analysis, & Threat Intel
- Specialized Investigative Skills

- Malware Analysis
- FOR110 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GCE
- Threat Intelligence
- FOR999 Cyber Threat Intelligence | GCTI
- Digital Forensics & Media Exploitation
- FieldSight & Data Acquisition
- FOR990 Battlefield Forensics & Data Acquisition
- Smartphones: FOR991 Smartphone Forensic Analysis in Depth | GSF
- Memory Forensics: FOR992 Advanced Memory Forensics & Threat Detection
- MAC Forensics: FOR993 MAC and ICS Forensics: Analysis and Incident Response

Advanced Management
- Advanced Leadership, Audit, Legal

Management SANS
- Planning, Policy, Leadership
- SEC503 Security Strategic Planning, Policy, and Leadership | GSTR
- Managing Vulnerabilities: SEC505 Managing Security Vulnerabilities: Enterprise and Cloud
- Project Management: SEC502 IT Project Management, Effective Communication, and PMI® Exam Prep | GCDA
- Audit & Legal
- Audit & Monitor: AUD430 Auditing and Monitoring Networks, Perimeters, and Systems | GCEO
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 – $799*

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

-Robert Jones, Team Jones, Inc.

---

**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
- Save over $1,100 when added to your SANS training

*GIAC bundle price – $799*

“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](http://www.sans.org/ondemand/bundles)  |  [www.giac.org](http://www.giac.org)

*GIAC and OnDemand Bundles are only available for certain courses.*
Benefits of Attending a Live SANS Training Event

This live SANS training event is just one of many held throughout North America each year. Every SANS event provides hands-on, skills-based training that can be applied immediately to your work, and you'll learn from the best practitioners in the industry.

Our live training events take place in many popular and convenient locations and host thousands of cybersecurity professionals. SANS also schedules local events throughout the year in most major metropolitan areas, bringing our top cybersecurity courses to the professionals who need them.

SANS live training events provide you with:

• Immersion training without home or office distractions
• Access to top SANS cybersecurity instructors who are renowned experts in the field
• A variety of networking opportunities
• Hands-on experience through NetWars challenges
• Content-loaded SANS@Night bonus sessions
• Exposure to leading solution providers at Solutions Expos, lunch and learns, industry receptions, and more

Visit sans.org/live-training to view the 2020 live training calendar and register for your courses.

“Attending live training events puts you in the same location with a large number of security professionals. It is a fantastic opportunity to network and socialize with so many people, and not just those in your same training class.”
— Scott Meyer, Fortive

“Nothing beats interacting with peers and subject-matter experts on a one-on-one basis for rapid assimilation of information in a manner that is retainable. SANS live training facilitates that superbly.”
— Tom Stogdale, Honeywell
SEC301: Introduction to Cyber Security

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Communicate with confidence regarding information security topics, terms, and concepts
- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- 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 is an extremely valuable course, even for someone with 12 years of IT experience!”
— Brian Pfau, Banfield Pet Hospital

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 a MIS director for a small company before joining AT&T/Lucent as a Senior Security Architect working on engagements with the Department of Defense 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, GCIC, GCED, GISF, CEH, Security+, Network+, A+, CTT+).

Keith Palmgren
SANS Senior Instructor
### 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 work our way up the OSI stack 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 5: 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, including 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

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/sansfire/courses](https://sans.org/sansfire/courses)
SEC401: Security Essentials Bootcamp Style

You Will Be Able To

- 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 becoming 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
SANS Principal Instructor

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 the GSEC, GCWN, GCICH, GCFIA, GPEN, GWAPT, GAWN, GISF, GCIA, GCED, GCUX, GSF, 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. In addition to teaching SEC401, Bryan teaches SEC501: Advanced Security Essentials – Enterprise Defender; SEC505: Securing Windows and Powershell Automation; and SEC511: Continuous Monitoring and Security Operations.

@BryanOnSecurity

Register at sans.org/sansfire | 301-654-SANS (7267)
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 this first day in order to provide a firm foundation for the following days of training.

Topics: Defensible Network Architecture; Virtualization and Cloud Security; Network Device Security; Networking and Protocols; Securing Wireless Networks; Securing Web Communications

Day 2: Defense-In-Depth and Attacks
To secure an enterprise network, you must understand the general principles of network security. On this second course day, 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. This course section 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 provided a vast library of information on developing a strong security posture, and in the course of the training my brain shifted into a security-first gear thanks to the intense and deep exposure to the multitudinous recommendations for securing an organization’s network and data.”
— Laura Farvour, University of Minnesota
NEW! SEC450: Blue Team Fundamentals: Security Operations and Analysis

Is your organization looking for a quick and effective way to onboard new security analysts, engineers, and architects? Do your Security Operations Center (SOC) managers need additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC?

SEC450 is an accelerated on-ramp for new cyber defense team members and SOC managers. This course introduces students to the tools common to a defender’s work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know.

Students will learn the stages of security operations: how data are collected, where they are collected, and how threats are identified within those data. The class dives deep into tactics for triage and investigation of events that are identified as malicious, as well as how to avoid common mistakes and perform continual high-quality analysis. Students will learn the inner workings of the most popular protocols, and how to identify weaponized files as well as attacks within the hosts and data on their network.

The course employs practical, hands-on instruction using a simulated SOC environment with a real, fully-integrated toolset that includes:

- Security Information and Event Management (SIEM)
- An incident tracking and management system
- A threat intelligence platform
- Packet capture and analysis
- Automation tools

While cyber defense can be a challenging and engaging career, many SOCs are negatively affected by turnover. To preemptively tackle this problem, this course also presents research-backed information on preventing burnout and how to keep engagement high through continuous growth, automation, and false positive reduction. Students will finish the course with a full-scope view of how collection and detection work, how SOC tools are used and fit together, and how to keep their SOC up and running over the long term.

“Very valuable for learning how organizations should set up a SOC and how to evaluate your own. Walk-throughs of the tools helps tremendously.”

— Troy Dinkel, Aires

John is a dedicated blue-teamer and is driven to help develop defensive talent around the world. Through his years of experience as the SOC Lead for GlaxoSmithKline, he has real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks and is eager to share these lessons with his students. As a SANS Cyber Defense curriculum instructor and course author of SEC455, John specializes in threat hunting, network security monitoring, SIEM design and optimization, and constructing defensive postures that allow organizations to protect their most sensitive data. Throughout class, he works with students to explain difficult concepts in relatable and clear language, illustrates important ideas with stories and demonstrations, and encourages students to push themselves beyond the limit of what they thought possible. John holds degrees in electrical and computer engineering and his past research ranges from malware reverse-engineering to car hacking, mobile app security, and IoT devices. In his free time, John enjoys catching every InfoSec conference he can attend, FPV drone racing, coffee roasting, and slowly turning his home into a data center.

@SecHubb
### DAY 1: Blue Team Tools and Operations

This day starts with an introduction to the blue team, the mission of a Security Operations Center (SOC), and how to understand an organization’s threat model and risk appetite. It is focused on top-down learning to explain the mindset of an analyst, the workflow, and monitoring tools used in the battle against attackers. Throughout this course day students will learn how SOC information management tools fit together, including incident management systems, threat intelligence platforms, SIEMs, and SOAR tools. We end the day describing the various groups of attackers, how their methods differ, and their motivations.

**Topics:** Introduction to the Blue Team Mission; SOC Overview; Defensible Network Concepts; Events, Alerts, Anomalies, and Incidents; Incident Management Systems; Threat Intelligence Platforms; SIEM; Automation and Orchestration; Who Are Your Enemies?

### DAY 2: Understanding Your Network

Day 2 begins the technical journey of understanding the environment. To defend a network, you must thoroughly understand its architecture and the impact that it will have on analysis. This day introduces the concepts of a modern organization’s network traffic flow by dissecting a basic home Internet connection and describing the features necessary for segmentation and monitoring. These modules ensure that students have a firm grasp on how network design affects their “view of the world” as an analyst. We then go in-depth on common network services. Day 2 provides thorough working explanations of the current and upcoming features of DNS, HTTP(S), SMTP, and more, with a focus on the most important points for analysts to understand. These sections explain what normal data look like, as well as the common fields and areas that are used to spot anomalous behavior. The focus will be on quickly recognizing the common tricks used by attackers to turn these everyday services against us.

**Topics:** Corporate Network Architecture; Traffic Capture and Visibility; Understanding DNS; DNS Analysis and Attacks; Understanding HTTP and HTTPS; Analyzing HTTP for Suspicious Activity; How SMTP and Email Attacks Work; Additional Important Protocols

### DAY 3: Understanding Endpoints, Logs, and Files

It is extremely difficult to succeed at cyber defense without knowing where and how your data are produced, so day 3 takes us down to the host, logging, and file level. Starting with an overview of common endpoint-based attack tactics, we orient students to the array of techniques that are used against their hosts. These first sections, followed by a section on defense in-depth, will give students an idea of how each step of the attack lifecycle aligns with its defensive tools, and what students can use to prevent and detect adversary attack advancement on their endpoints. The course day then turns to the parsing and enrichment of logs, as well as how the SIEM normalization and categorization processes work. These topics give a complete view of what happens from the moment a log is generated to when it shows up in our security tools. The final part of day 3 provides students with the concepts needed to reason through the answer, diving into files at the byte level. Students will finish this day understanding how different common file formats work, how they get types of files weaponized, and how to quickly decide whether or not a given sample is likely to be malicious.

**Topics:** Endpoint Attack Tactics; Endpoint Defense In-Depth; How Windows Logging Works; How Linux Logging Works; Interpreting Important Events; Kerberos and Active Directory Events; Log Collection, Parsing, and Normalization; File Contents and Identification; Identifying and Handling Suspicious Files

### DAY 4: Triage and Analysis

Now that the course has covered the ground required to understand the tools and data most frequently encountered by analysts, it’s time to focus on analysis itself. This day will focus on how the analysis process works and explain how to avoid the common mistakes new analysts can slip into. We can combat the tendency to overlook the obvious by examining how our memory perception affects analysis and how cognitive biases cause us to fail to see what is right in front of us. The goal is to teach students not only how to think clearly, but also how to explain and leave a trail of how they reached their conclusions that can support future analysis and act as an audit trail. In addition, we will cover many of the mental models and concepts used in information security from both the offensive and defensive perspectives. Students will then use these models to look at an alert queue and get a quick and intuitive understanding of which alerts may pose the biggest threat, and thus must be attended to first. Safe analysis techniques and operational security concerns are covered to ensure that we do not give up our tactical advantage during the investigation process. We’ll discuss specifics on alert triage methods and prioritization, as well as investigation techniques, so that students will leave this day better prepared to understand their alert queues and perform error-free investigation.

**Topics:** Alert Triage and Prioritization; Perception and Investigation; Memory and Investigation; Mental Models for Information Security; Structured Analysis Techniques; Analysis Tactics and OPSEC; Network, File, and Event Alerts; Intrusion Discovery; Incident Closing and Quality Review

### DAY 5: Continuous Improvement, Analytics, and Automation

This day focuses squarely on improving the efficiency and enthusiasm of working in SOCs by tackling the most common problems head on. Through process optimization, careful analytic design and tuning, and workflow efficiency improvements, we can eliminate many of these common pain points. This frees us from the repetitive work we loathe and allows us to focus on what we do best – analysis! Having the time for challenging and novel work leads to a virtuous cycle of growth and engagement throughout the SOC – while improving everyone’s life in the process. This day will focus on tuning your tools using clever analysis techniques and process automation to remove the monotonous and non-value-added activities from your day. We also cover containment activities, including the tools you can use and how to decide how to halt a developing incident or infection from the host or network angle. We’ll wrap up the day with recommendations on skill growth, long-term career development, and how to get more involved in the cyber defense community.

**Topics:** Improving Life in the SOC; Analytic Features and Enrichment; New Analytic Design, Testing, and Sharing; Tuning and False Positive Reduction, Automation and Orchestration; Improving Operational Efficiency and Workflow, Containing Identified Intrusions; Skill and Career Development

### DAY 6: Capstone: Defend the Flag

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 be challenged to progress through multiple levels and missions designed to ensure mastery of the concepts and data covered during the course.

**Who Should Attend**
- Security analysts
- Incident investigators
- Security engineers and architects
- Technical security managers
- SOC managers looking to gain additional technical perspective on how to improve analysis quality, reduce turnover, and run an efficient SOC
- Anyone looking to start their career on the blue team

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/sansfire/courses](http://sans.org/sansfire/courses)
Immeasurable amounts of personal, potentially incriminating data are currently stored in the websites, apps, and social media platforms that people access and update via their devices daily. Those 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 teaches students legitimate and effective ways to find, gather, and analyze these 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 those data are 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.

You Will Be Able To

- Create an OSINT process
- Conduct OSINT investigations in support of a wide range of customers
- Understand the data collection life cycle
- Create a secure platform for data collection
- Analyze customer collection requirements
- Capture and record data
- Create sock puppet accounts
- Create your own OSINT process
- Harvest web data
- Perform searches for people
- Access social media data
- Assess a remote location using online cameras and maps
- Examine geolocated social media
- Research businesses
- Use government-provided data
- Collect data from the dark web
- Leverage international sites and tools

“Fantastic introduction to a wide spectrum of OSINT techniques and practices, with great interactive labs and lots of deep dives!”

— Dave Huffman, Rockwell Automation

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 the Appalachian Trail or the many park trails in Maryland.

@WebBreacher
**Course Day Descriptions**

**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 course by learning how to document findings and set up an OSINT platform. The information taught in this section 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.

**Topics:** Course Introduction; Understanding OSINT; Goals of OSINT Collection; Diving into Collecting; Taking Excellent Notes; Determining Your Threat Profile; Setting up an OSINT Platform; Effective Habits and Process; Leveraging Search Engines

---

**DAY 2: Gathering, Searching, and Analyzing OSINT**
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 they 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, using command line tools, scripts, and helper applications.

**Topics:** Data Analysis Challenges; Harvesting Web Data; File Metadata Analysis; OSINT Frameworks; Basic Data: Addresses and Phone Numbers; Basic Data: Email Addresses; User Names; Avatars and Reverse Image Searches; Additional Public Data; Creating Sock Puppets

---

**DAY 3: Social Media, Geolocation, and Imagery**
Day three kicks off by examining free and paid choices in people search engines 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, geolocation, and eventually mapping and imagery.

**Topics:** People Search Engines; Exercise in People Searching; Facebook Analysis; LinkedIn Data; Instagram; Twitter Data; Geolocation; Imagery and Maps

---

**DAY 4: Networks, Government, and Business**
Day four focuses on many different but related OSINT issues. This is our blue team day, as we dive into OSINT for IP addresses, domain names, DNS, and Whois. We then move into how to use wireless network information for OSINT. We end the section with two huge modules on searching international government websites for OSINT data and supporting business processes with OSINT.

**Topics:** Whois; IP Addresses; DNS; Finding Online Devices; Wireless Networks; Recon Tool Suites and Frameworks; 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 use Freenet, I2P, and Tor. The first module in the afternoon examines how blue teamers (cyber defenders) can use monitoring to receive alerts when data of interest appear on the Internet. We then shift our focus to data found on “paste” sites. Considering that a big barrier to using non-English websites can be the language, students learn how to use techniques to translate content and search locally for relevant information in our international OSINT section. We leave some time at the end of the day for a massive lab, the “Solo Capture-the-Flag” event, which 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 Webs; The Dark Web; Freenet; I2P - Invisible Internet Project; Tor; Monitoring and Alerting; International Issues; Vehicle Searches; Solo CTF Challenge

---

**DAY 6: Capstone: Capture (and Present) the Flag**
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 multi-hour, hands-on event will reinforce what the students practiced in the Solo CTF the day before and add the complexity of performing OSINT assessments under pressure and in a group.

**Topics:** Capstone Capture-the-Flag Event

---

**Who Should Attend**
- Cyber incident responders
- Digital Forensics and Incident Response (DFIR) analysts
- Penetration testers
- Social engineers
- Law enforcement personnel
- Intelligence personnel
- Recruiters
- Private investigators
- Insurance investigators
- Human resources personnel
- Researchers

---

“*This course sets up the student with a whole range of OSINT tools that are essential for investigation!*”
— Selvi Krishnan, Blue Voyant
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 was a member of Foundstone’s world-renowned penetration testing team and served as a co-author and senior instructor of Foundstone’s groundbreaking, *Ultimate Hacking: Hands-On* course series. Bryce continues to provide highly specialized ethical hacking and cybersecurity consulting services to clients around the world and teaches thousands of cybersecurity professionals, from a who’s who of top organizations, how to defend against advanced adversaries.

@brycegalbraith
**DAY 1: Defensive Network Architecture**

This course day will focus on security in the design and configuration of various enterprise infrastructures. From a security perspective, proper design and configuration protects both the components being configured, as well as the rest of the organization that depends on that gear to defend other components from attacks. In other words, a good house needs a good foundation.

**Topics:** 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

**DAY 2: Penetration Testing**

Security is all about understanding, mitigating, and controlling the risk to an organization’s critical assets. An organization must understand the changing threat landscape and have the capacity to compare it against its own vulnerabilities that could be exploited to compromise the environment. On day two, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration tests to better understand the security posture for network services, operating systems, and applications. In addition, we’ll talk about social engineering and reconnaissance activities to better emulate increasingly prevalent threats to users.

**Topics:** Introduction to Penetration Testing Concepts; Penetration Testing Scoping and Rules of Engagement; Online Reconnaissance and Offensive Counterintelligence; Social Engineering; Network Mapping and Scanning Techniques; Enterprise Vulnerability Scanning; Network Exploitation Tools and Techniques; Web Application Exploitation Tools and Techniques; Post-Exploitation and Pivoting; OS and Application Exploit Mitigations; Reporting and Debriefing

**DAY 3: Security Operations Foundations**

“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.

**Topics:** Network Security Monitoring; IP, TCP, and UDP Refresher; Advanced Packet Analysis; Introduction to Network Forensics with Security Onion; Identifying Malicious Content and Streams; Extracting and Repairing Content from PCAP files; Traffic Visualization Tools; Intrusion Detection and Intrusion Prevention; Handling Encrypted Network Traffic

**DAY 4: Digital Forensics and Incident Response**

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.

**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

**DAY 5: Malware Analysis**

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 tricking 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.

**Topics:** Introduction to Malware Analysis; The Many Types of Malware; ATM/Cash Machine Malware; Building a Lab Environment for Malware Analysis; Malware Locations and Footprints; Fully Automated Malware; Cuckoo Sandbox; Static Properties Analysis; Interactive Behavior Analysis; Manual Code Reversing; Tools such as IDA, PeStudio, ILSpy, Process Hacker, Process Monitor, NoFuserEx, etc.

**DAY 6: Enterprise Defender Capstone**

The concluding section of the course will serve as a real-world challenge for students by requiring them to work in teams, use 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 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.
SEC503: Intrusion Detection In-Depth

You Will Be Able To

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

SEC503 is one of the most important courses that you will take in your information security career. While past students describe it as the most difficult class they have ever taken, they also tell us it was the most rewarding. This course isn’t for people who are simply looking to understand alerts generated by an out-of-the-box Intrusion Detection System (IDS). It’s for people who want to deeply understand what is happening on their network today, and who suspect that there are very serious things happening right now that none of their tools are telling them about. If you want to be able to find zero-day activities on your network before disclosure, this is definitely the class for you.

What sets this course apart from any other training is that we take a bottom-up approach to teaching network intrusion detection and network forensics. Rather than starting with a tool and teaching you how to use that tool in different situations, this course teaches you how and why TCP/IP protocols work the way they do. After spending the first two days examining what we call “Packets as a Second Language,” we add in common application protocols and a general approach to researching and understanding new protocols. With this deep understanding of how network protocols work, we turn our attention to the most widely used tools in the industry to apply this deep knowledge. The result is that you will leave this class with a clear understanding of how to instrument your network and the ability to perform detailed incident analysis and reconstruction.

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

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

“The course has equipped me with super powers. I can see everything! I don’t know how I was able to do my job without this knowledge. This course is a must for any cyber defense analyst.”

— Joe Morrissey, Nationwide

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.

@it_audit
**Course Descriptions**

**Day 1: Fundamentals of Traffic Analysis – Part 1**

Day 1 begins our bottom-up coverage of the TCP/IP protocol stack, providing a refresher or introduction, depending on your background, to TCP/IP. This is the first step in what we think of as a “Packets as a Second Language” course. Students begin to be introduced to the importance of collecting the actual packets involved in attacks and are immediately immersed in low-level packet analysis. We will cover the essential foundations such as the TCP/IP communication model, theory of bits, bytes, binary and hexadecimal, and the meaning and expected behavior of every field in the IP header. Students are introduced to the use of open-source Wireshark and tcpdump tools for traffic analysis.

**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 first section ended. Students will gain a deep understanding of the primary transport layer protocols used in the TCP/IP model. Two essential tools, Wireshark and tcpdump, are further explored, using advanced features to give you the skills to analyze your own traffic. The focus of these tools is to filter large-scale data down to traffic of interest using Wireshark display filters and tcpdump Berkeley Packet Filters. These are used in the context of our exploration of the TCP/IP transport layers covering TCP, UDP, and ICMP. Once again, we discuss the meaning and expected function of every header field, covering a number of modern innovations that have very serious implications for modern network monitoring, and we 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, Real-World Analysis – Command Line Tools

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

Day 3 builds on the foundation of the first two sections of the course, moving into the world of application layer protocols. Students are introduced to the versatile packet crafting tool Scapy. This 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. Various practical scenarios and uses for Scapy are provided throughout this section.

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

**Day 4: Network Monitoring: Signatures vs. Behaviors**

The fundamental knowledge gained from the first three sections provides the foundation for deep discussions of modern network intrusion detection systems during section 4. Everything that students have learned so far is now synthesized and applied to designing optimized detection rules for Snort/Firepower, and this is extended even further with behavioral detection using Zeek. The day begins with a discussion on network architecture, including the features of intrusion detection and prevention devices, along with a discussion about options and requirements for devices that can sniff and capture the traffic for inspection. This section provides an overview of deployment options and considerations, and allows students to explore specific deployment considerations that might apply to their respective organizations.

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

**Day 5: Network Traffic Forensics**

Day 5 continues the trend of less formal instruction and more practical application using hands-on exercises. It consists of three major topics, beginning with practical network forensics and an exploration of data-driven monitoring vs. alert-driven monitoring, followed by a hands-on scenario that requires students to use all of the skills developed so far. The second topic continues the theme of data-driven analysis by introducing large-scale analysis and collection using NetFlow and IPFIX data.

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

**Day 6: Advanced IDS Capstone Event**

The course culminates with a fun, hands-on, score-server-based IDS challenge. Students compete as solo players or on teams to answer many questions that require using tools and theory covered in the first five sections. The challenge presented is based on hours of live-fire, real-world data in the context of a time-sensitive incident investigation. The challenge is designed as a "ride-along” event, where students are answering questions based on the analysis that a team of professional analysts performed of these same data.
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.

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.

“SEC504 is the essential cert course needed to trust if a candidate is valuable enough to do incident response.”
— Troy Merritt, Blueshield of CA

Joshua Wright
SANS Senior Instructor
**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 (IDS) Evasion; Enumerating Windows Active Directory Targets

**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:** Physical-layer Attacks; Gathering and Parsing Packets; Operating System and Application-level Attacks; Netcat: The Attacker’s Best Friend; Endpoint Security Bypass

**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

**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 disguising 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 and explore future trends in malware designed to obscure an attacker’s presence and disguise attribution.

**Topics:** Maintaining Access; Covering the Tracks; Putting It All Together

**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
- General security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks

“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
NEW! SEC505: Securing Windows and PowerShell Automation

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

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

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

In the SEC505 course you will learn how to:
- Write PowerShell scripts for Windows and Active Directory security automation
- Safely run PowerShell scripts on thousands of hosts over the network
- Defend against PowerShell malware, such as ransomware
- Harden Windows Server and Windows 10 against skilled attackers

In particular, we will use PowerShell to secure Windows against many of the attacks described in the MITRE ATT&CK matrix, especially against stolen administrative credentials, ransomware, hacker lateral movement inside the LAN, and insecure Windows protocols such as RDP and SMB.

You will leave this course ready to start writing your own PowerShell scripts to help secure your Windows environment. It’s easy to find Windows security checklists, but how do you automate those changes across thousands of machines? How do you safely run scripts on many remote boxes? In this course you will learn not just Windows and Active Directory security, but how to manage security using PowerShell.

DON'T JUST LEARN POWERSHELL SYNTAX, LEARN HOW TO LEVERAGE POWERSHELL AS A FORCE MULTIPLIER FOR WINDOWS SECURITY

There is another reason PowerShell has become popular: PowerShell is just plain fun! You will be surprised at how much you can accomplish with PowerShell in a short period of time, it’s much more than just a scripting language, and you don’t have to be a coding guru to get going.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for IT people with PowerShell skills. In response, even though SEC505 has had at least one day of PowerShell instruction for more than 10 years, today PowerShell is the centerpiece of the course. You don’t have to know any PowerShell to attend this course, we will learn it together during the labs.

You can learn basic PowerShell syntax on YouTube for free, but this week goes far beyond syntax. In this course we will learn how to use PowerShell as a platform for managing security, as a “force multiplier” for the Blue Team, and as a rocket booster for your Windows IT career.

WE WILL WRITE A POWERSHELL RANSOMWARE SCRIPT AND DEFEND AGAINST IT

Unfortunately, PowerShell is being abused by hackers and malware authors. On the last day of the course, we will write our own ransomware script to see how to defend against scripts like it.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security at the same time.
DAY 1: Learn PowerShell Scripting for Security

The first day of the course 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 course progresses. Don’t worry, you won’t be left behind, the PowerShell labs walk you through every step. If you already have PowerShell experience, then there will also be intermediate topics for you.

Topics: Write Your Own PowerShell Scripts and Functions; Flow Control; PowerShell Core vs. Windows PowerShell; Privileged Objects, Not Text; Classes, Objects, Properties, Methods; Importing Modules; Exporting Sata to CSV and XML Files

DAY 2: You Don’t Know the POWER!

How can we run PowerShell scripts on thousands of systems with just a few lines of code? This day is about remote command execution using PowerShell Remoting, the Secure Shell (SSH) service on Windows, the Task Scheduler service, and boot-up scripts assigned through Group Policy. SSH is not just for Linux. Windows now has built-in support for it as both a client and server. We can use Just Enough Admin (JEA) policies to block all remoting commands by default, then only allow the commands and arguments we want. And with JEA, PowerShell Remoting commands are magically (and safely?) elevated to administrator status, similar to setuid root on Linux.

Topics: PowerShell Remote Command Execution of Scripts; SSH for Windows; Smart Card Authentication for PowerShell Remoting; SSL/TLS Encryption vs. SSH; Key-based Authentication for SSH; Just Enough Admin Remoting; Running PowerShell Scripts as SYSTEM with the Task Scheduler; Group Policy-assigned Startup Scripts

DAY 3: PowerShell for WMI and Active Directory

PowerShell is deeply integrated into the Windows Management Instrumentation (WMI) service. Hackers love the WMI service too, but for the wrong reasons. The WMI service is enabled by default and accessible over the network. Active Directory (AD) is also manageable through PowerShell: we can find abandoned user accounts and disable them, enforce desired group memberships, reset passwords, and more. What about local admin accounts? Don’t use Microsoft LAPS! There are better ways to protect admin passwords, including a PowerShell solution we will implement in a lab. With proper AD permissions and auditing, combined with PowerShell JEA on jump servers, we can delegate IT authority in AD much more safely.

Topics: PowerShell for WMI; PowerShell for Active Directory; WMI Namespaces and Classes; Remote Command Execution with WMI; WMI and AD Reconnaissance; AD Permissions and Auditing; A Better (and Free) Alternative to Microsoft LAPS

DAY 4: Hardening Network Services with PowerShell

On day four we will use PowerShell and Group Policy to automate the hardening of many exploitable services and protocols, such as DNS, RDP, and SMB. We will see how to use PowerShell to install roles, manage services, and accomplish other security tasks for DevOps. For example, firewall rules and IPSec policies can be applied through PowerShell. The trick is to be able to apply different sets of firewall and IPSec rules to different sets of machines in a scalable, repeatable, and automated way, hence the need for PowerShell. IPSec is not just for Virtual Private Networks (VPNs)! In fact, we won’t discuss VPNs at all in this section. The built-in Windows IPSec driver can authenticate users in Active Directory in order to implement share permissions for our TCP/UDP listening ports based on our users’ global group memberships in Active Directory. If you move to Server Core or Server Nano, knowing PowerShell becomes a job requirement.

Topics: PowerShell for Server and Workstation Automation, DevOps Style; PowerShell for Firewall Rules and IPSec Policies; IPSec is Built in and Not Just for VPNs; Automate the Hardening of Server Core, Server Nano, and Other Stand-alone Machines; PowerShell Management of Networking Settings

DAY 5: Multi-Factor Authentication with Smart Cards and Smart Tokens

Smart cards and smart tokens, like YubiKeys, are the gold standard for multi-factor authentication (MFA). On day five, we will use PowerShell to install a certificate server that can be used to deploy smart cards and smart USB tokens. Smart cards and tokens can be used for PowerShell Remoting, signing PowerShell scripts, Remote Desktop Protocol (RDP) logons, Virtual Private Networks, and more. Everything you need to roll out a full smart card/token solution for your administrators is included with Windows. If you have a Trusted Platform Module (TPM) chip in your laptop or tablet, the TPM can also be used as a built-in smart card. TPMs also protect biometric data, encrypt BitLocker keys, and help enhance Windows 10 Credential Guard. PowerShell Remoting network traffic can be encrypted with SSL/TLS. The target server is authenticated with its certificate, just like a web server using HTTPS, but how do you install SSL/TLS certificates on thousands of workstations and servers? We will show you how to do that.

Topics: Smart Cards and Smart Tokens Such as YubiKeys; Smart Cards for PowerShell Remoting; SSL/TLS Encryption for PowerShell Remoting and Other Web Services; TPM Virtual Smart Cards; TPM for Biometrics and Credential Guard; Certificate Auto-enrollment; Online Certificate Status Protocol Revocation Checking

DAY 6: Capstone: PowerShell Security, Ransomware, and DevOps

On day six we will write a PowerShell ransomware script and unleash it inside our training Virtual Machine (don’t release it into the wild, you’ll go to federal prison). The purpose of this ethical hacking is to discuss defenses: how can we secure PowerShell itself? PowerShell is not a single tool, so we must deploy several defenses in-depth. Most importantly, we must prevent the compromise of Domain Admin credentials. PowerShell hacking tools and ransomware with Domain Admin credentials are nearly unstoppable! As a capstone to pull together the week’s material, we will also create a DevOps-style script to reconfigure nearly all the security features discussed during the week. The goal is to have an all-in-one script that can ideally reconfigure everything. Soon, we will all need to be “full stack engineers” for automation (and job security).

Topics: PowerShell Ransomware; PowerShell Security; PowerShell Encryption; DevOps-Style Script; Running PowerShell Scripts; SSL/TLS Encryption; Domain Admin Credentials; Windows 10 Credential Guard; Privileged Access Workstations (PAWS) and Jump Servers; Capstone DevOps Script for Automation

Who Should Attend
- Security Operations personnel
- Blue Team players who were terrified by SEC504
- 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

“In SEC505, real-life solutions are offered by someone who understands the roadblocks in the way. This is information I could implement tomorrow and make my network more secure.”

— Mary Becken, Egan Company
This course provides in-depth coverage of Linux and Unix security issues that includes specific configuration guidance and practical, real-world examples, tips, and tricks. We examine how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. The course will teach you the skills to use freely available tools to handle security issues, including SSH, AIDE, sudo, lsof, and many others. SANS’ practical approach uses hands-on exercises every day to ensure that you will be able to use these tools as soon as you return to work. We will also put these tools to work in a special section that covers simple forensic techniques for investigating compromised systems.

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

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe and with global corporations. Equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS Lethal Forensicator, and is the creator of the SANS Linux/Unix Security track (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS Forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS Computer Forensics blog and co-author of the Command Line Kung Fu blog.

@hal_pomeranz
## Course Day Descriptions

**Mon, Jun 15 – Sat, Jun 20**

<table>
<thead>
<tr>
<th>Day</th>
<th>Course Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1: Hardening Linux/Unix Systems – Part 1</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: Memory Attacks and Overflows; Vulnerability Minimization; Boot-Time Configuration; Encrypted Access; Host-Based Firewalls</td>
<td></td>
</tr>
<tr>
<td>Day 2: Hardening Linux/Unix Systems – Part 2</td>
<td></td>
</tr>
<tr>
<td>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?</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: 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</td>
<td></td>
</tr>
<tr>
<td>Day 3: Hardening Linux/Unix Systems – Part 3</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: Automating Tasks With SSH; AIDE via SSH; Linux/Unix Logging Overview; SSH Tunneling; Centralized Logging with Syslog-NG</td>
<td></td>
</tr>
<tr>
<td>Day 4: Linux Application Security – Part 1</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: chroot() for Application Security; The SCP-Only Shell; SELinux Basics; SELinux and the Reference Policy</td>
<td></td>
</tr>
<tr>
<td>Day 5: Linux Application Security – Part 2</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: BIND; DNSSec; Apache; Web Application Firewalls with mod_security</td>
<td></td>
</tr>
<tr>
<td>Day 6: Digital Forensics for Linux/Unix</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Topics</strong>: Tools Throughout; Forensic Preparation and Best Practices; Incident Response and Evidence Acquisition; Media Analysis; Incident Reporting</td>
<td></td>
</tr>
</tbody>
</table>

### 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
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!

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

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

@eric_conrad

Eric Conrad
SANS Faculty Fellow
**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

---

**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 detection 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 detection 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 detection 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 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 provides a high-level view all the way down to packets. It’s a great, great course on detecting/preventing threats. This course is hands-down worth every dollar. I learned more actionable things in a week than in four semesters of school!”

— Matt McCullough, MN IT

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/sansfire/courses](sans.org/sansfire/courses)
SEC530: Defensible Security Architecture and Engineering

SEC530: Defensible Security Architecture and Engineering 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 to aid in building a robust security infrastructure.

While this is not a monitoring course, it 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

**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

"As a systems programmer working on the development of security tools, the architectural content provided has been highly informative and extremely valuable.”

— Merv Hammer, Workday Inc.

"SEC530 provided an excellent understanding of application attacks and how to protect against them.”

— Shayne Douglass, AMEWAS Inc.

Ismael Valenzuela founded one of the first IT security consultancies in Spain and has participated as a security professional in numerous projects across the globe over the past 17 years. As a top cybersecurity expert with a strong technical background and deep knowledge of penetration testing, security architectures, intrusion detection and computer forensics, Ismael has provided security consultancy, advice and guidance to large government and private organizations, including major EU Institutions and U.S. government agencies. Prior to his current role as Principal Engineer at McAfee, where he leads research on threat hunting using machine-learning and expert-system-driven investigations, Ismael led the delivery of Security Operations Center, incident response and forensics services for the Foundstone Services team within Intel globally. Previously, Ismael worked as Global IT Security Manager for iSOFT Group Ltd, one of the world’s largest providers of healthcare IT solutions, managing its security operations in more than 40 countries. He holds a bachelor’s degree in computer science from the University of Malaga (Spain), has a certificate in business administration, and holds many professional certifications, including the highly regarded GIAC Security Expert (GSE #132) in addition to the GREM, GCFA, GCIA, GCIH, GPEN, GCUX, GWAPT, GSNA, GMON, CISSP®, ITIL, CISM, and IRCA 27001 Lead Auditor from Bureau Veritas UK.
DAY 1: Defensible Security Architecture and Engineering

Day 1 of the course describes hardening systems and networks at every layer, from layer one (physical) to layer seven (applications and data). To quote Richard Bejtlich’s *The Tao of Network Security Monitoring*, defensible networks “encourage, rather than frustrate, digital self-defense.” The section begins with an overview of traditional network and security architectures and their common weaknesses. The defensible security mindset is “build it once, build it right.” All networks must perform their operational functions effectively, and security can be complementary to this goal. It is much more efficient to bake security in at the outset than to retrofit it later. The discussion will then turn to layer one (physical) and layer two (data link) best practices, including many “ripped from the headlines” tips the course authors have successfully deployed in the trenches to harden infrastructure in order to prevent and detect modern attacks. Examples include the use of private VLANs, which effectively kills the malicious client-to-client pivot, and 802.1X and NAC, which mitigate rogue devices. Specific Cisco IOS syntax examples are provided to harden switches.

**Topics:** Traditional Security Architecture Deficiencies; Defensible Security Architecture; Threat, Vulnerability, and Data Flow Analysis; Layer 1 Best Practices; Layer 2 Best Practices; Netflow.

DAY 2: Network Security Architecture and Engineering

Day 2 continues hardening the infrastructure and moves on to layer three routing. Actionable examples are provided for hardening routers, with specific Cisco IOS commands to perform each step. The section then continues with a deep dive on IPv6, which currently accounts for 23% of Internet backbone traffic, according to Google, while simultaneously being used and ignored by most organizations. This section will provide deep background on IPv6, discuss common mistakes (such as applying an IPv4 mindset to IPv6), and provide actionable solutions for securing the protocol. The section wraps up with a discussion of VPN and stateful layer three/four firewalls.

**Topics:** Layer 3: Router Best Practices; Layer 3 Attacks and Mitigation; Layer 2 and 3 Benchmarks and Auditing Tools; Securing SNMP; Securing NTP; Bogon Filtering, Blackholes, and Darknets; IPv6, Securing IPv6, VPN, Layer 3/4 Stateful Firewalls; Proxy.

DAY 3: Network-Centric Security

Organizations own or have access to many network-based security technologies ranging from next-generation firewalls to web proxies and malware sandboxes. Yet the effectiveness of these technologies is directly affected by their implementation. Too much reliance on built-in capabilities like application control, antivirus, intrusion prevention, data loss prevention, or other automatic evil-finding deep packet inspection engines leads to a highly preventative-focused implementation, with huge gaps in both prevention and detection. Day 3 focuses on using application layer security practices that an organization already owns with a modern mindset. By thinking outside the box, even old controls like a spam appliance can be used to catch modern attacks such as phishing via cousin domains and other spoofing techniques. And again, by engineering defenses for modern attacks, both prevention and detection capabilities gain significantly.

**Topics:** NGFW; NIDS/NIPS; Network Security Monitoring; Sandboxing; Encryption; Secure Remote Access; Distributed Denial-of-Service (DDOS).

DAY 4: Data-Centric Security

Organizations cannot protect something they do not know exists. The problem is that critical and sensitive data exist all over. Complicating this even more is that data are often controlled by a full application stack involving multiple services that may be hosted on-premise or in the cloud. Day 4 focuses on identifying core data where they reside and how to protect those data. Protection includes the use of data governance solutions and full application stack security measures such as web application firewalls and database activity monitoring, as well as keeping a sharp focus on securing the systems hosting core services such as on-premise hypervisors, cloud computing platforms, and container services such as Docker. The data-centric security approach focuses on what is core to an organization and prioritizes security controls around it. Why spend copious amounts of time and money securing everything when controls can be optimized and focused on securing what matters? Let’s face it: Some systems are more critical than others.

**Topics:** Application (Reverse) Proxies; Full Stack Security Design; Web Application Firewalls; Database Firewalls; Database Activity Monitoring; File Classification; Data Loss Prevention (DLP); Data Governance; Mobile Device Management (MDM) and Mobile Application Management (MAM); Private Cloud Security; Public Cloud Security; Container Security.

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

Today, a common security mantra is “trust but verify.” But this is a broken concept. Computers are capable of calculating trust on the fly, so rather than thinking in terms of “trust but verify” organizations should be implementing “verify then trust.” By doing so, access can be constrained to appropriate levels at the same time that access can become more fluid. This section focuses on implementing a zero-trust architecture where trust is no longer implied but must be proven. By doing so, a model of variable trust can be used to change access levels dynamically. This, in turn, allows for implementing fewer or more security controls as necessary given a user’s and a device’s trust maintained over time. The focus is on implementing zero trust with existing security technologies to maximize their value and impact for an organization’s security posture. During this section encryption and authentication will be used to create a hardened network, whether external or internal. Also, advanced defensive techniques will be implemented to stop modern attack tools in their tracks while leaving services fully functional for authorized assets.

**Topics:** Zero-Trust Architecture; Credential Rotation; Compromised Internal Assets; Securing the Network; Tripwire and Red Herring Defenses; Patching; Deputizing Endpoints as Hardened Security Sensors; Scaling Endpoint Log Collection/Storage/Analysis.

DAY 6: Hands-On 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.
SEC545: Cloud Security Architecture and Operations

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.

“SEC545 is excellent for cloud security understanding and overviews. I would definitely recommend this course for people looking at building a cloud security program.”

— Justin Pyle, Chan Zuckerberg Initiative

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.

@daveshackleford
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; 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 look at properly locking down all the pieces and parts we covered on day two! This then leads to a focus on major areas of architecture and security design. The first is building various models of access control and compartmentalization. This involves breaking things down into two categories: identity and access management and network security. We delve into these in significant depth, as they can form the backbone of a sound cloud security strategy. We then look at architecture and design for data security, touching on encryption technologies, key management, and what the different options are today. We wrap up our third day with another crucial topic: availability. Redundant and available design is as important as ever, but we need to use cloud provider tools and geography to our advantage. At the same time, we need to make sure we evaluate the cloud provider’s 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 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 Defensive Strategies; Tools and Tactics; Real-World Use Cases; Class Wrap-Up
SEC555: **SIEM with Tactical Analytics**

**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 those 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.

“**This course uses real-world events and hands-on training to allow me to immediately improve my organization’s security stance. Day one back in the office I was implementing what I learned.**”

— Frank Giachino, Bechtel

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, and 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
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 get students up to speed on SIEM concepts and to bring them all 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; Applying 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 activity 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: Identifying Authorized and Unauthorized Assets; Identifying 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 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: Centralizing NIDS and HIDS Alerts; Analyzing Endpoint Security Logs; Augmenting Intrusion Detection Alerts; Analyzing Vulnerability Information; Correlating Malware Sandbox Logs with Other Systems to Identify Victims Across the Enterprise; Monitoring 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: Defend-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 the relative value of numerous ways to defend your organization.”
— Mikhale Vitebskiy, 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’ 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.

James Tarala
SANS Senior Instructor

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

@isaudit
Course Day Descriptions

**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)

“This course is providing me with the necessary context to understand the Critical Security Controls in depth, and further helping me understand how to present recommendations to our business owners.”

— Chris Harper, Centrus Energy

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses
You Will Be Able To

- Understand how recent high-profile attacks were delivered and how they could have been stopped
- Implement security controls throughout the different phases of the Cyber Kill Chain and the MITRE ATT&CK framework to prevent, detect, and respond to attacks

Topics To Be Addressed

- Leverage MITRE ATT&CK as a "common language" in the organization
- Building your own Cuckoo sandbox solution to analyze payloads
- Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
- Highlighting key bypass strategies for script controls (unmanaged Powershell, AMSI bypasses, etc.)
- Stopping 0-day exploits using ExploitGuard and application whitelisting
- Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
- Detecting and preventing malware persistence
- Leveraging the Elastic stack as a central log analysis solution
- Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
- Blocking and detecting command and control through network traffic analysis
- Leveraging threat intelligence to improve your security posture

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 tactics are affecting small, mid-size, 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 & Kill Chain Defenses will arm you with the knowledge and expertise you need to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, we will introduce security controls aimed at stopping, detecting, and responding to your adversaries.

Course authors Stephen Sims and Erik Van Buggenhout (both certified as GIAC Security Experts) are hands-on practitioners who have built a deep understanding of how cyber attacks work through penetration testing and incident response. While teaching penetration testing courses, they were often asked the question: "How do I prevent or detect this type of attack?" Well, this is it! SEC599 gives students real-world examples of how to prevent attacks. The course features 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.

Our six-part journey will start off with an analysis of recent attacks through in-depth case studies. We will explain what types of attacks are occurring and introduce formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, you will also compromise our virtual organization "SYNCTECHLABS" in section one exercises.

In sections two through five, we will discuss how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. 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 against its environment. The adversaries aren’t slowing down, so what are you waiting for?

"SEC599 handles a lot of important aspects [of the entire Kill Chain]. It gives good insight into potential attacks and mitigation."
— Kevin Giesekam, Dutch Police

Erik Van Buggenhout is the lead author of SEC599: Defeating Advanced Adversaries. In addition, Erik teaches SEC560: Network Penetration Testing and Ethical Hacking and SEC562: Web Application Penetration Testing and Ethical Hacking. He has been involved with SANS since 2009, starting as a Mentor, working his way to Community Instructor in 2012, and finally becoming a Certified Instructor in 2016. Erik loves explaining deeply technical concepts by using war stories, adding a few funny anecdotes here and there. As testimony to his technical expertise, he has obtained the GSE, GCIA, GNFA, GPEN, GWAPT, GCIH, and GSEC certifications. Erik is the co-founder of the Belgian firm NVISO, which focuses on high-end cybersecurity services, specializing in government, defense and the financial sector. Together with his team of 20+ technical experts, Erik delivers a wide array of technical security services, including penetration testing, security monitoring and incident response. Prior to NVISO, Erik spent five years at a Big 4 firm, starting as a junior penetration tester and evolving into a subject-matter expert for the EMEA region. Erik is a self-confessed speed walker, so if you see him rushing around at a conference, feel free to stop him and say "Hi!" @ErikVaBu
**Course Day Descriptions**

**DAY 1: Introduction and Reconnaissance**
Our six-part journey starts with an analysis of recent attacks through in-depth case studies. We will explain what’s happening in real situations and introduce the Cyber Kill Chain and MITRE ATT&CK framework as a structured approach to describing adversary tactics and techniques. We will also explain what purple teaming is, typical tools associated with it, and how it can be best organized in your organization. In order to understand how attacks work, students will also compromise our virtual organization “SYNCTECHLABS” during section one exercises.

**Topics:** Course Outline and Lab Setup; Adversary Emulation and the Purple Team, Reconnaissance

**DAY 2: Payload Delivery and Execution**
Section 2 will cover how the attacker attempts to deliver and execute payloads in the organization. We will first cover adversary techniques (e.g., creation of malicious executables and scripts), then focus on how both payload delivery (e.g., phishing mails) and execution (e.g., double-clicking of the attachment) can be hindered. We will also introduce YARA as a common payload description language and SigMA as a vendor-agnostic use-case description language.

**Topics:** Common Delivery Mechanisms, Hindering Payload Delivery, Preventing Payload Execution

**DAY 3: Exploitation, Persistence, and Command and Control**
Section 3 will first explain how exploitation can be prevented or detected. We will show how security should be an integral part of the software development lifecycle and how this can help prevent the creation of vulnerable software. We will also explain how patch management fits in the overall picture. Next, we will zoom in on exploit mitigation techniques, both at compile-time (e.g., ControlFlowGuard) and at run-time (ExploitGuard). We will provide an in-depth explanation of what the different exploit mitigation techniques (attempt to) cover and how effective they are. We’ll then turn to a discussion of typical persistence strategies and how they can be detected using Autoruns and OSQuery. Finally, we will illustrate how command and control channels are being set up and what controls are available to the defender for detection and prevention.

**Topics:** Protecting Applications from Exploitation; Avoiding Installation; Foiling Command and Control

**DAY 4: Lateral Movement**
Section 4 will focus on how adversaries move laterally throughout an environment. A key focus will be on Active Directory (AD) structures and protocols (local credential stealing, NTLMv2, Kerberos, etc.). We will discuss common attack strategies, including Windows privilege escalation, UAC bypasses, (Over-) Pass-the-Hash, Kerberoasting, Silver Tickets, and others. We’ll also cover how BloodHound can be used to develop attack paths through the AD environment. Finally, we will discuss how lateral movement can be identified in the environment and how cyber deception can be used to catch intruders red-handed!

**Topics:** Protecting Administrative Access; Key Attack Strategies against AD; How Can We Detect Lateral Movement?

**DAY 5: Action on Objectives, Threat Hunting, and Incident Response**
Section 5 focuses on stopping the adversary during the final stages of the attack:

- How does the adversary obtain “domain dominance” status? This includes the use of Golden Tickets, Skeleton Keys, and directory replication attacks such as DCSync and DCShadow.
- How can data exfiltration be detected and stopped?
- How can threat intelligence aid defenders in the Cyber Kill Chain?
- How can defenders perform effective incident response?

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

**Topics:** Domain Dominance; Data Exfiltration; Leveraging Threat Intelligence; Threat Hunting and Incident Response

**DAY 6: APT Defender Capstone**
The course culminates in a team-based Defend-the-Flag competition. Section six is a full day of hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure mastery of the modern cybersecurity controls promoted all week long. This challenging exercise will reinforce key principles in a fun, hands-on, team-based challenge. Note that OnDemand students will enjoy this exercise on an individual basis. As always, SANS subject-matter experts are available to support every OnDemand student’s experience.

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

---

**Who Should Attend**
- Security architects and security engineers
- Red teamers and penetration testers
- Technical security managers
- Security Operations Center analysts, engineers, and managers
- 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.

---

“*The different topics covered in this course can bring eye-opening layers of defense to any organization.*”

— Mike Marx, Carbon Black
TBT570: Team-Based Training – Blue Team and Red Team Dynamic Workshop is a unique course during which student teams of three to five participants work together as a Blue Team to battle an adversary in real time. The technical terrain, the SANS Red/Blue Cyber Range, is a realistic enterprise environment.

This interactive exercise is designed for people who learn by actually doing. You will not be spoon-fed through lectures or follow-along labs in this session. Instead, you will participate in a dynamic exercise defending an environment under attack in real time as you build your skills working alongside your team. The course is designed to help students build team skills, leadership abilities, communication techniques, and technical expertise, all while under fire in a series of increasingly complex scenarios.

Student Blue Teams use a variety of enterprise tools to analyze and respond to advanced persistent threats (APTs) deeply embedded in the environment, defending against a series of offensive campaigns. In addition to learning from the instructors throughout the exercise, students are encouraged to share their own skills and techniques to cross-pollinate good ideas between the different Blue Teams represented in the room.

A SANS instructor will direct the Blue Teams as they uncover the attacker’s command-and-control channels and work to eradicate the adversary from compromised systems. SANS will provide skilled Red Team operators who will utilize the Tactics, Techniques, and Procedures to present various Indicators of Compromise from real-world APT cases throughout the workshop in order to challenge students to build their Blue Team skills.

The SANS White Cell oversees the exercise and ensures that it runs smoothly, while the SANS Ops team runs the underlying cyber range infrastructure. Each day finishes with a live hot-wash discussion during which the Red and Blue Teams review the activities from the day with the White Cell and each other to level-set and ensure that specific learning objectives have been met. These afternoon discussions will also allow Blue Team members from different organizations (including commercial companies, government agencies, military agencies, and more) to share their insights for dealing with such attacks.

The live, interactive battle will occur over five days, with a sixth and final day focused on the Blue and Red Teams presenting their After Action Reviews describing lessons learned. These reports make up a deliverable that students can bring back to their organization to improve its security stance.

**Author’s Statement**

“The SANS Blue Team/Red Team Dynamic Workshop course can really take an organization’s skills to the next level. Whenever we’ve run this session, the take-aways have been INCREDIBLE, with participants’ skills and capabilities increasing and improving significantly as they learn to function as an efficient team. In addition, the level-setting that we do at the end of each day helps ensure that the operations tempo remains vivid and exciting while learning occurs. This course is really an incredible opportunity for people who already have three or more years’ experience and are looking to ramp up their skills to be game changers in their organizations.”

— Ed Skoudis, SANS Fellow and Director of SANS Cyber Ranges

**You Will Be Able To**

- Analyze network traffic for malfeasance
- Identify attacker artifacts and activities on a variety of different enterprise systems
- Collect and analyze intel associated with the attack
- Analyze the malware used by attackers
- Eradicate the attacker’s presence from the environment
- Thwart the attacker’s plot to disrupt the enterprise mission

“TBT570 provides an immersive cyber range experience that is extremely applicable to real-world cybersecurity incidents.”

— Andy Scally, Secure-24

“TBT570 provided the best Red Team type engagement I’ve been a part of.”

— John Moran, Rackspace
Highly Custom Malware
Stealthy Nation-State Actor with Our Most Advanced Adversary – A

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

conduct the daily shot validation meeting.
abilities as they defeat this adversary and then Team instructor, students will further build out their skills and knowledge they've gained throughout goals. All along the way, students use the hands-on through the environment to achieve a series of stealthily and uses numerous techniques to pivot plunder, this subtle attacker undermines systems nation-state techniques to pillage, pilfer, and engage in Campaign C. Using a whole host of Team. Our most skilled and powerful adversary the now much more experienced student Blue On day 5, we really throw everything we've got at the adversary in the environment. By day 4, TBT570 students are working together very effectively as a team of teams. And that's a very good thing, because we up the capabilities of the adversary in Campaign B. For this campaign, students will face a nation-state-level adversary, presenting Indicators of Compromise (IOCs) and TTPs of a specific APT. After an initial intel in-briefing, students hunt for this adversary, supported with the coaching and encouragement of the Blue Team instructor and TA. By analyzing the IOCs presented by the attacker, students will do research to attempt to attribute these actions to a specific adversary. They can then use this intelligence to anticipate the adversary's next moves and to identify other IOCs left by this actor. With this information, students can disrupt various components of the attacker’s multiple command-and-control channels to thwart the adversary in the environment.

“TBT570 is the best course I've seen to give someone an understanding of what battling an advanced attacker is really like, and that shows the coordination that must occur between numerous teams to effectively eliminate the compromise.”

— Matthew Bainter, Caterpillar

“TBT570 is 90% hands-on, which makes it unique among course offerings. The cyber labs were realistic and hearing from the red team each day was valuable.”

— Edward Tanner, Booz Allen Hamilton

Day 1: In-Depth Tool Orientation and Team Dynamics
On this first day we discuss the Tactics, Techniques, and Procedures (TTPs) of today’s most dangerous adversaries. We then cover how organizations can utilize a team-based approach to effectively detect and eradicate such actors in their networks. We’ll cover effective small team dynamics, along with inter-team communication techniques that are essential to handling attacks on a larger-scale environment. With a series of team-based exercises, students learn how to work together more effectively as members and leaders of a team, while mastering incredibly useful tips, tricks, and skills that they can utilize right away to better defend their environments.

Day 2: Range Orientation and Campaign 0: Building Effective Team Skills to Detect and Eradicate an Adversary
On day 2, students get direct access to the TBT570 cyber range, along with a guided hands-on tour to orient them to the environment they’ll be working in to engage adversaries through the rest of the course. The range represents the IT infrastructure of a realistic town, with several enclaves that host different components of that town, including computer servers, clients, network equipment, and industrial control system devices. Using credentials and a network map, students explore the Windows Domain and its associated initial Group Policy, the SIM/SEM solution included in the range, the vulnerability scanning service, the trouble ticketing systems, and the management infrastructure.

Day 3: Campaign A: Engaging an Advanced Persistent Threat, Hardening the Environment, and Enhanced Team Communication
On day 3, we up the ante by introducing a more advanced adversary into the environment, played by the Red Team instructor. The session starts with an intel in-briefing, describing the situation and what is currently known about the new advanced persistent threat (APT) adversary and its goals. Students apply the tools and techniques learned in days 1 and 2, along with any additional optional tools that they brought with them, to find and battle the adversary in real time. The Blue Team instructor and TA act as coaches and advisors, as students build their skills in a realistic scenario.

Day 4: Campaign B: Identifying IOCs and TTPs, Disrupting an Adversary, and Cross-Pollination of Great Ideas Between Teams
By day 4, TBT570 students are working together very effectively as a team of teams. And that's a very good thing, because we up the capabilities of the adversary in Campaign B. For this campaign, students will face a nation-state-level adversary, presenting Indicators of Compromise (IOCs) and TTPs of a specific APT. After an initial intel in-briefing, students hunt for this adversary, supported with the coaching and encouragement of the Blue Team instructor and TA. By analyzing the IOCs presented by the attacker, students will do research to attempt to attribute these actions to a specific adversary. They can then use this intelligence to anticipate the adversary’s next moves and to identify other IOCs left by this actor. With this information, students can disrupt various components of the attacker’s multiple command-and-control channels to thwart the adversary in the environment.

Day 5: Campaign C: Tangling with Our Most Advanced Adversary – A Stealthy Nation-State Actor with Highly Custom Malware
On day 5, we really throw everything we’ve got at the now much more experienced student Blue Team. Our most skilled and powerful adversary utilizes custom malware created just for this course to engage in Campaign C. Using a whole host of nation-state techniques to pillage, pilfer, and plunder, this subtle attacker undermines systems stealthily and uses numerous techniques to pivot through the environment to achieve a series of goals. All along the way, students use the hands-on skills and knowledge they’ve gained throughout the course to find and dispel this attacker. It’s a fearsome battle, but armed with their skills and some tips, hints, and encouragement from the Blue Team instructor, students will further build out their abilities as they defeat this adversary and then conduct the daily shot validation meeting.

Day 6: After-Action Reviews/Post Mortem and a Plan for Action Upon Return
Throughout the previous five days of the course, instructors and TAs encouraged students to maintain a daily log of useful lessons they learned in class and will be able to apply when they get back to the office. On day 6, student teams work to create an After-Action Review/Post Mortem presentation. Using a presentation template we provide, students write up the lessons they learned in each campaign and reflect on how they’ll apply those lessons when they get back to the office. The Blue Team instructor will provide useful tips for developing and presenting the review. Students will then present their results to the rest of the class, so everyone benefits from the lessons learned by each student.
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.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight.”

– Jason Sevilla, Cyber Intelligence Analyst

“Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my résumé more appealing to recruiters.”

— Kim Ngoc, GuardSight, Inc.
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.

“Attackers are always evolving, and having a GIAC cert prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight.”

– Jason Sevilla, Cyber Intelligence Analyst

“Earning 3 GIAC certifications after I graduated from college has enabled me to enter the InfoSec field. Not only did they set me apart from my peers, GIAC certs also made my résumé more appealing to recruiters.”

– Kim Ngoc, GuardSight, Inc.

SANS NetWars Tournament is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world skills they need to excel in their field.

• Play solo or on a team
• Earn six Continuing Professional Education credits
• Experience cutting-edge cyber range training

Don’t miss out, add NetWars Tournament when you register for SANSFIRE 2020.

Participation is free for students taking a 5- or 6-day course.

“NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommend!”

– Kyle McDaniel, Lenovo

sans.org/netwars | @SANSNetWars
SEC460: Enterprise Threat and Vulnerability Assessment

You Will Be Able To

- Perform end-to-end vulnerability assessments
- Develop customized vulnerability discovery, management, and remediation plans
- Conduct threat intelligence gathering and analysis to create a tailored cybersecurity plan that integrates various attack and vulnerability modeling frameworks
- Implement a proven testing methodology using industry-leading tactics and techniques
- Adapt information security approaches to target real-world enterprise challenges
- Configure and manage vulnerability assessment tools to limit risk added to the environment by the tester
- Operate enumeration tools like Nmap, Masscan, Recon-ng, and WMI to identify network nodes, services, configurations, and vulnerabilities that an attacker could use as an opportunity for exploitation
- Conduct infrastructure vulnerability enumeration at scale across numerous network segments, in spite of divergent network infrastructure and nonstandard configurations
- Conduct web application vulnerability enumeration in enterprise environments while solving complex challenges resulting from scale
- Perform manual discovery and validation of cybersecurity vulnerabilities that can be extended to custom and unique applications and systems
- Manage large vulnerability datasets and perform risk calculation and scoring against organization-specific risks
- Implement vulnerability triage and prioritize mitigation

Adrien de Beaupre
SANS Principal Instructor

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 mid-sized to large 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.

SEC460 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 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

Adrien de Beaupre works as an independent consultant in beautiful Ottawa, Ontario. His work experience includes technical instruction, vulnerability assessment, penetration testing, intrusion detection, incident response and forensic analysis. He is a member of the SANS Internet Storm Center (isc.sans.edu). He is the lead course author of SANS SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques and SEC660: Enterprise Threat and Vulnerability Assessment. He is actively involved with the information security community, and has been working with SANS since 2000. Adrien holds a variety of certifications including the GXPN, GPE, GWAPT, GCH, GCIA, GSEC, CISSP®, OPST, and OQSA. When not geeking out he can be found with his family, or at the dojo.

@adriendb
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 Directory-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, inciting, or 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 for Insecure Cryptographic Implementations Including SSL; Assessing VQP 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 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 wade 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: Recruiting Disparate Data Sources: Patches, Hotfixes, and Configurations; 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; Evaluating Vulnerability Risk in Custom and Unique Systems, including Web Applications; 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 uncovering its weak points. Now it’s time for decision and action based on an understanding of the risks the organization faces. Developing an actionable remediation plan with time-based success targets sets the stage for continuous improvement, 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: Domain Password Auditing; Creating and Navigating Vulnerability Prioritization Schemes in Acheron; Developing a Web of Network and Host Affiliations; Modeling Account Relationships on Active Directory Forests; Creating Effective Vulnerability Assessment Reports; Transforming Triage Listing into the Vulnerability Remediation Plan; Closure: Be a Positive Influence in the Context of the Global Information Security Crisis

DAY 6: Vulnerability Assessment Foundry Hands-on Challenge
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

Who Should Attend
- Vulnerability assessors
- IT System administrators
- Security auditors
- Compliance professionals
- Penetration testers
- Vulnerability program managers
- Security analysts
- Security architects
- Senior security engineers
- Technical security managers

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses
SEC560: Network Penetration Testing and Ethical Hacking

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Configure and launch a vulnerability scanner such as Nessus so that it safely discovers vulnerabilities through both authenticated and unauthenticated scans, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy
- Utilize the Windows PowerShel and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- Analyze the output of scanning tools to eliminate false positive reduction with tools including Netcat and Scapy
- Utilize the Windows PowerShel and Linux bash command lines during post-exploitation to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment

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 over 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 with great skill.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

You’ll 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.

Finally, we focus deep on the technological heart of most organizations, the Windows Domain. We’ll cover the technical details of Kerberos and Active Directory and use that for Domain Dominance!

EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test and on the final day of the course you’ll do just that. After building your skills in comprehensive and challenging labs, the course culminates with a final 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 skills you’ve gained in this course.

“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

Tim Medin is the founder and Principal Consultant at Red Siege, a company focused on adversary emulation and penetration testing. Tim is also the Director of the SANS Masters Degree in Information Security Engineering Program, as well as a course author. Throughout the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim is an experienced international speaker, having presented at organizations around the world. Tim is also the creator of Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. Tim earned his MBA at the University of Texas.

@timmedin
Course Day Descriptions

DAY 1: Comprehensive Pen Test Planning, Scoping, and Recon
In this course section, you'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll also dig deep into the reconnaissance portion of a 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 which anti-virus tools the target organization uses.

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; Interrogating DNS for Juicy Information

DAY 2: In-Depth Scanning
This course section focuses on the vital task of mapping the target environment’s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We 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 also conduct a deep dive into some of the most useful tools available to pen testers today for formulating packets: Scapy and Netcat. We finish the module 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 examine the best ways to conduct your scans safely and efficiently.

Topics: Tips for Awesome Scanning; Tcpdump for the Pen Tester; Nmap In-Depth. The Nmap Scripting Engine, Version Scanning with Nmap, Vulnerability Scanning with Nessus; False-Positive Reduction; Packet Manipulation with Scapy; Enumerating Users; Netcat 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, and Stages; Strategies and Tactics for Anti-Virus Evasion; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding for Mercyless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment

DAY 4: Password Attacks and Merciless Pivoting
Once you’ve successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. This course section zooms in on pillaging target environments and building formidable hands-on command line skills. We’ll cover Windows command line skills in-depth, including PowerShell’s awesome abilities for post-exploitation. We’ll see how we can leverage malicious services and the incredible WMI toolset to access and pivot through a target organization. We’ll then turn our attention to password guessing attacks, discussing how to avoid account lockout, as well as numerous options for plundering password hashes from target machines including the great Mimikatz Kiwi tool. Finally, we’ll look at Metasploit’s fantastic features for pivoting, including the msfconsole route command.

Topics: Windows Command Line Kung Fu for Penetration Testers; PowerShell’s Amazing Post-Exploitation Capabilities; Password Attack Tips; Account Lockout and Strategies for Avoiding It; Automated Password Guessing with THC-Hydra; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

DAY 5: Domain Domination and Web App Pen Testing
In this course section, we’ll go even deeper in exploiting one of the weakest aspects of most computing environments: passwords. You’ll custom-compile John the Ripper to optimize its performance in cracking passwords. You’ll look at the amazingly full-featured Cain tool, running it to crack snipped Windows authentication messages. We’ll use the incredible Hashcat tool for increased speed in cracking passwords, 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 cover analysis to pull sensitive information: Kerberos Authentication Protocol; Poisoning Multicast Name Resolution withResponder, Domain Mapping and Exploitation with Bloodhound, Effective Domain Privilege Escalation; Persisting Administrative Domain Access; Using the ZAP Proxy to Manipulate Custom Web Applications; Maximizing Effectiveness of Command Injection Testing; Data Plundering with SQL Injection; Leveraging SQL Injection to Perform Command Injection

DAY 6: Penetration Testing 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 in a comprehensive, 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 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; Detailed Scanning to Find Vulnerabilities and Avenues to Entry; Exploitation to Gain Control of Target Systems; Post-Exploitation to Determine Business Risk; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise Corrective Actions

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 sans.org/sansfire/courses

This course is available via Simulcast. See page 92 for more information.

47
SEC573: Automating Information Security with Python

You Will Be Able To

- Modify existing open-source tools to customize them to meet the needs of your organization.
- Manipulate log file formats to make them compatible with various log collectors.
- Write new tools to analyze log files and network packets to identify attackers in your environment.
- Develop tools that extract otherwise inaccessible forensic artifacts from computer systems of all types.
- Automate the collection of intelligence information to augment your security from online resources.
- Automate the extraction of signs of compromise and other forensic data from the Windows Registry and other databases.
- Write a backdoor that uses exception handling, sockets, process execution, and encryption to provide you with your initial foothold in a target environment.

All security professionals, including penetration testers, forensic analysts, network defenders, security administrators, and incident responders, have one experience in common: CHANGE. Tools, technologies, and threats change constantly, but Python is a simple, user-friendly language that can help you keep pace with change, allowing you to write custom tools and automate tasks to effectively manage and respond to your unique threats.

Whether you are new to coding or have been coding for years, SEC573: Automating Information Security with Python will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience with or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the course.

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

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

Or, as a penetration tester, you need to evolve as quickly as the threats you are paid to emulate. What do you do when “off-the-shelf” tools and exploits fall short? If you’re good, you write your own tool or modify existing capabilities to make them perform as you need them to.

SEC573 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 to better automate the daily routine of today’s information security professional and to achieve 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. Learn Python in-depth with us to become 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.

@MarkBaggett

Mark Baggett
SANS Senior Instructor

Mark Baggett
SANS Senior Instructor
DAY 1: Essentials Workshop with pyWars
The course begins with a brief introduction to Python and the pyWars Capture-the-Flag challenge. We set the stage for students to learn at their own pace in the pyWars lab environment, which is 100 percent hands-on. 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: 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. This section continues the hands-on, lab-centric approach established at the beginning of the course. It covers data structures and more detailed programming concepts. Next, we focus on invaluable tips and tricks to make you a better Python programmer and to show you 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
In this section, we take on the role of a network defender with more logs to examine than there is time in the day. Attackers have penetrated the network and you will have to analyze the logs and packet captures to find them. 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. Forensicators and offensive security professionals won’t be left out because reading and writing files and parsing data are also essential skills they will apply to their craft.

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
In our forensics-themed section, we will assume the role of a forensic 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 the skills covered in this section 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 those 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
During our offensive-themed section, 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; Using the Select Module for Asynchronous Operations; The Select Module; Python Objects; Argument Packing and Unpacking

DAY 6: Capture-the-Flag Challenge
In this final section you will be placed on a team with other students to apply the skills you have mastered in a series of programming challenges. Participants will exercise the new skills and the code they have developed throughout the course in a series of challenges. You will solve programming challenges, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills! Prove your might!

Who Should Attend
- Security professionals who benefit from automating routine tasks so they can focus on what’s most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

You Will Receive
- A USB containing a virtual machine filled with sample code and working examples
- A copy of The Python Pocket Reference published by O’Reilly Press
- MP3 audio files of the complete course lecture

“Excellent class for learning how to construct automated and advanced discovery analytics for information systems.”
— Mary Gutierrez, Booz Allen Hamilton
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 skill set 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 APs, 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 smart 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.

James Leyte-Vidal is a team lead in a Fortune 100 company, currently focused on remediation efforts and control monitoring. In his 12 years in information security, James has performed various InfoSec functions including penetration testing, security assessments, remediation, vulnerability management, security program development and management, and incident response. Prior to his work in security, James worked several years as a Windows sysadmin and in an application support role. James has spoken publicly and taught for over 20 years, in college classrooms as well as at functions within his own company and elsewhere. James holds the GCIH, GPEN, GWAPT, GAWN, GXPN, GCLA, GCFA, GMOB, GSEC, CISSP®, MCSE, and CISA certifications as well as degrees in IT and psychology. When not teaching or helping to secure his own company, James can usually be found running or taking something apart.

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

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 techniques, and other protection techniques.

You Will Be Able To

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

Who Should Attend

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

Moses Frost

SANS Certified Instructor

Moses Frost (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
**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 Collisions; 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 toolsets. We’ll use lab exercises to explore the newer protocols of HTTP/2 and WebSockets, exploiting flaws exposed within each of them.

**Topics:** Intercepting Traffic to Web Services and from Mobile Applications; Flash, Java, ActiveX, and Silverlight Vulnerabilities; SOAP and REST Web Services; Penetration Testing 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 rulesets 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 Web Application Firewalling and Filtering Techniques; Determining the Rule Sets Protecting the Application; Fingerprinting the Defense Techniques Used; Learning How HTML5 Injections Work; Using UNICODE, CTYPEs, and Data URIs to Bypass Restrictions; Bypassing a Web Application Firewall’s Best-Defended Vulnerabilities; XSS and SQLi

---

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

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.
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

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

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

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. He is the author of SANS’ only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author 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 Access/Admission Control (NAC); Impersonating Devices with Admission Control Policy Exceptions; Exploiting EAP-MD Authentication; Custom Network Protocol Manipulation with Ettercap and Custom Filters; Multiple Techniques for Gaining Man-in-the-Middle Network Access; IPv6 for Penetration Testers; 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

---

**DAY 2: Crypto, Network Booting Attacks, and Escaping Restricted Environments**
Day two starts by taking a tactical look at techniques penetration testers can use to investigate and exploit common cryptography mistakes. We finish the module with lab exercises that allow you to practice your new-found crypto attack skill set against reproduced real-world application vulnerabilities.

**Topics:** Pen Testing Cryptographic Implementations; Exploiting CBC Bit Flipping Vulnerabilities; Exploiting Hash Length Extension Vulnerabilities; PowerShell Essentials; Enterprise PowerShell; Post-Exploitation with PowerShell and Metasploit; Escaping Software Restrictions; Two-hour Evening Capture-the-Flag Exercise Against a Modern Network with Hardened Servers, Desktops and vApp Targets

---

**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; Identifying and Analyzing Stack-Based Overflows on the Linux OS; Performing Return-to-libc (ret2libc) Attacks on the Stack; Return-Oriented Programming; 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 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 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 difficult challenges will be worth more points. The evening bootcamp sessions, which will focus on how to think outside the box, and solve a range of problems from simple to complex.

---

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

— Anton Ebertzeder, Siemens AG

---

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses
SEC760: Advanced Exploit Development for Penetration Testers

Vulnerabilities in modern operating systems such as Microsoft Windows 10 and the latest Linux distributions are often very complex and subtle. When exploited by very skilled attackers, these vulnerabilities can undermine an organization’s defenses and expose it to significant damage. Few security professionals have the skillset to discover why a complex vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity.

SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse-engineer 32-bit and 64-bit applications to find vulnerabilities, 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.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, kernel and driver exploitation, one-day exploitation through patch analysis, and other advanced attacks
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success

“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

Jaime Geiger is an experienced forward and reverse engineer with a passion for teaching. He currently works in the Washington, DC area for Grimm, where he enjoys the freedom to do work on software design and implementation, reverse engineering, exploit development, and network administration. Jaime also helps run an internal tech talk program for employee skill development and a college sponsorship program that helps create a competitive but friendly environment for college students to learn various computing security skills. Jaime holds a BS in information security and forensics from the Rochester Institute of Technology and currently holds the GIAC GXPN certification. In his free time, Jaime enjoys bouldering, snowboarding, and participating on red teams for events such as the Collegiate Cyber Defense Competition (CCDC).
For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses

Course Day Descriptions

### DAY 1: Exploit Mitigations and Reversing with IDA

The course starts with a deep dive into both mature and modern exploit mitigations. It is rare today to come across an operating system or application that doesn’t use a combination of mitigations to thwart the exploitation of a vulnerability. Outdated operating systems and applications do exist, such as in the industrial control system and Internet of Things space, but that is not the focus of this course. We address the effectiveness and technical details behind each control, such as those implemented in Windows Defender Exploit Guard. We then spend the remainder of day one using IDA Pro, which comes bundled with the course. We quickly ramp up on the basics of IDA Pro as a disassembler and then move into reverse engineering with the tool. We finish up day one utilizing IDA FLIRT and FLAIR and writing IDAPython scripts to help with bug hunting and analysis.

**Topics:** Exploit Mitigations; Windows Defender Exploit Guard; Introduction to IDA Pro; Debugging with IDA Pro; FLIRT & FLAIR; Scripting with IDAPython and Python 3

### DAY 2: Linux Application 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 SANS’ SEC660 course. 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, which is necessary to continue further with the course. Linux can sometimes be an easier operating system to learn these techniques, serving as a productive gateway into Windows. Most courses on exploit development focus purely on the Windows OS, and it’s important to have an understanding of vulnerability research on the Linux OS as well.

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

### DAY 3: Patch Diffing, One-Day Exploits, and Return-Oriented Shellcode

Attacker 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 aware of this and quickly work to find the patched vulnerability in order to take control of unpatched systems, as many organizations struggle with getting patches out quickly. Binary diffing and patch diffing 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 on this day to identify bugs patched by Microsoft, taking some of them through to exploitation. We will also focus on using Return Oriented Programming (ROP) to string together gadgets that emulate shellcode.

**Topics:** The Microsoft Patch Management Process and Patch Tuesday; Obtaining Patches and Patch Extraction; Binary Diffing with BinDiff; Visualizing Code Changes and Identifying Fixes; Reversing 32-bit and 64-bit Applications and Modules, Triggering Patched Vulnerabilities; Writing One-Day Exploits; Using ROP to Compiled Shellcode on the Fly (Return-Oriented Shellcode)

### DAY 4: Windows Kernel Debugging and Exploitation

The Windows kernel is complex and intimidating, so this day aims to help you understand the Windows kernel and the various exploit mitigations added into recent versions. You will learn how the kernel works with drivers to talk to devices and how some functionality can be exposed to user-mode, sometimes insecurely! You will perform kernel debugging on Windows 10 and learn to deal with its inherent complexities. Exercises will be performed to analyze Ring 0 driver vulnerabilities, look at exploitation techniques, and get working exploits.

**Topics:** Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel Protections; Debugging the Windows 10 Kernels and Drivers; WinDbg; Analyzing Kernel Vulnerabilities and Kernel Vulnerability Types; Kernel Exploitation Techniques; Token Stealing and Information Disclosure Vulnerabilities

### DAY 5: Advanced Windows Exploitation

The focus of this day is on the advanced exploitation of applications running on the Windows OS. For many years now memory corruption bugs have been the de facto standard regarding exploiting Windows applications. Examples include Use After Free (UAF) and Type Confusion bugs. Many of these vulnerabilities exist due to complexities with large C++ applications such as object tracking and dynamic memory management. In this section, we focus on these types of application vulnerabilities on the Windows 7, 8, and 10 operating systems.

**Topics:** Windows Heap Management, Constructs, and Environment; Understanding the Low Fragmentation Heap; Browser-Based and Client-Side Exploitation; Understanding C++ vtable/etable Behavior; Use-After-Free Attacks and Dangling Pointers; Avoiding Protections such as MemGC and Isolated Heap; Dealing with ASLR, DEP, and Other Common Exploit Mitigation Controls

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

Day six will feature a Capture-the-Flag event employing different types of challenges from material taught throughout the week. Test your reverse engineering, bug discovery, and exploit-writing skills in a full day of Capture-the-Flag exercises!

### Who Should Attend

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

### Course Authors’ Statements

“Siege is a perpetual student of information security, I am excited to offer SEC760: Advanced Exploit Writing for Penetration Testers. Exploit development is a hot topic and will continue to increase in importance moving forward. With all of the modern exploit mitigation controls offered by operating systems such as Windows 10, 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 discover vulnerabilities, determine if those vulnerabilities are exploitable, and carry out general 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

“Teaching and helping author SEC760: Advanced Exploit Writing for Penetration Testers has given me the opportunity to distill my past experiences in exploit writing and technical systems knowledge into a format worth sharing. This course is meant to give you a look into a number of different exploitation techniques and serves as an amazing jumping-off point for exploitation of any modern application or system. Even if you don’t plan on having a career in exploit writing or vulnerability research, this course will be valuable in understanding the thought process that goes into constructing an exploit and what technologies exist to stop an exploit writer from being successful.”

— Jaime Geiger

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

— William Stott, Raytheon
You Will Be Able To

- Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where they are stored
- Handle and process a scene properly to maintain evidentiary integrity
- Perform data acquisition from at-rest storage, including both spinning media and solid-state storage
- Identify the numerous places that data for an investigation might exist
- Perform Battlefield Forensics by going from evidence seizure to actionable intelligence in 90 minutes or less
- Assist in preparing the documentation necessary to communicate with online entities such as Google, Facebook, Microsoft, etc.
- Understand the concepts and usage of large-volume storage technologies, including JBOD, RAID storage, NAS devices, and other large-scale, network-addressable storage
- Identify and collect user data within large corporate environments where they are accessed using SMB
- Gather volatile data such as a computer system’s RAM
- Recover and properly preserve digital evidence on cellular and other portable devices
- Address the proper collection and preservation of data on devices such as Microsoft Surface/Surface Pro, where hard-drive removal is not an option
- Address the proper collection and preservation of data on Apple devices such as MacBook, MacBook Air, and MacBook Pro, where hard-drive removal is not an option
- Properly collect and effectively target email from Exchange servers, avoiding the old-school method of full acquisition and subsequent onerous data culling
- Properly collect data from SharePoint repositories
- Access and acquire online mail stores such as Gmail, Hotmail, and Yahoo Mail accounts

Kevin Ripa
SANS Certified Instructor

The FOR498: Battlefield Forensics & Data Acquisition course will help you to:

- Acquire data effectively from:
  - PCs, Microsoft Surface, and Tablet PCs
  - Apple Devices, Mac, and Macbooks
  - RAM and memory
  - Smartphones and portable mobile devices
  - Cloud storage and services
  - Network storage repositories
- Produce actionable intelligence in 90 minutes or less

The first step in any investigation is the gathering of evidence. Digital forensic investigations are no different. The evidence used in this type of investigation is data, and these data can live in many varied formats and locations. You must be able to first identify the data that you might need, determine where those data reside, and, finally, formulate a plan and procedures for collecting those data. With digital forensic acquisitions, you will typically have only one chance to collect data properly. If you manage the acquisition incorrectly, you run the risk of not only damaging the investigation, but more importantly, destroying the very data that could have been used as evidence.

With the wide range of storage media in the marketplace today, any kind of standardized methodology for all media is simply untenable. Many mistakes are being made in digital evidence collection, and this can cause the guilty to go free and, more importantly, the innocent to be incarcerated. The disposition of millions and millions of dollars can rest within the bits and bytes that you are tasked with properly collecting and interpreting. An examiner can no longer rely on “dead box” imaging of a single hard drive. In today’s cyber sphere, many people utilize a desktop, laptop, tablet, and cellular phone within the course of a normal day. Compound this issue with the expanding use of cloud storage and providers, and the proper collection of data from all these domains can become quite overwhelming.

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly identify, collect, respond to, and preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. Constantly updated, FOR498 addresses today’s need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Numerous hands-on labs throughout the course will give first responders, investigators, and digital forensics teams the practical experience needed when performing digital acquisition from hard drives, memory sticks, cellular phones, network storage areas, and everything in between. During a digital forensics response and investigation, an organization needs the most skilled responders possible, lest the investigation end before it has begun.

Kevin serves as president of The Grayson Group of Companies, which consists of Computer Evidence Recovery, Pro Data Recovery Inc., and J.S. Kramer & Associates, Inc. He provides investigative services to various levels of law enforcement, Fortune 500 companies, and the legal community. As a 25-year veteran of the digital investigations field, Kevin has designed, produced, hosted, and taught numerous industry-related courses, and has had over 100 speaking and training engagements with industry and law enforcement entities around the world. He holds a number of industry certifications, including the GCFE, GCFA, GSEC, GISF, EnCase Certified Examiner, Certified Data Recovery Professional, and more.

@kevinripa
and Online Attribution

sans.org/sansfire/courses

is pervasive. It is controlling our fridges, thermostats, security cameras, and door locks. From proper collection to legal documentation. Not to be left out, the Internet of Things devices, working at the command line. You have traced an artifact back to an IP, email, you’ll learn how to access and forensically image iPads, MacBooks, and other HFS+

remove the hard drive, as it is soldered directly to the motherboard. The uniqueness posed by APFS. Many of the Apple systems are closed systems, in that you simply cannot acquire data from Apple devices. We will acquire memory and identify systems that are as compared to Windows. The tools that exist can be quite expensive, and free There are very few tools and techniques available when it comes to acquisition of Apple products, as compared to Windows. The tools that exist can be quite expensive, and free tools are simply few and far between. In this section, we will explore the fundamentals of data acquisition, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, “live” acquisition will be your only hope.

Given that 99% of the necessary evidence typically will exist in 1-2% of the data acquired, it is easy to see how a great deal of time can be wasted following the normal procedures in today’s digital forensics world. Instead, let’s focus on this 1-2% and perform a very rapid triage collection that can be used to start our investigation sooner. Far too often, computers are seized in an “on” state, and immediately powered down because “that is how we’ve always done it.” With today’s computers this means you are throwing away (essentially destroying) many gigabytes of data. The RAM in a computer holds an incredibly important treasure trove of data, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, “live” acquisition will be your only hope.

When we think about acquisition, it usually involves opening the side of the computer, removing the hard drive, connecting to a write blocker or imaging equipment, and completing the task. While this is not an inaccurate assessment, it does not address a great deal of the access and acquisition questions surrounding so much data today. If full disk imaging is necessary, then it is certainly easier and quicker to do it directly from the storage itself. But what happens with devices such as iPads, Surface Books, and other such equipment, where it is glue and not screws that hold them together? Volume Shadow Copies also contain a wealth of historic data that are of great use to investigators. Knowing how to access and collect data from these shadow copies is critical in cases involving the Windows operating system. Battlefield forensics is considered the bleeding edge of digital forensics. It requires in-depth knowledge of where the most valuable data reside on the computer and how to get to that data as fast as possible. An effective battlefield forensicator needs to be extracting actionable intelligence in 90 minutes or less, but the clock does not start when the forensic imaging is done. Rather, it starts from the moment you lay your hands on the device. Learn how to identify and access data in non-traditional storage areas. In today’s world so much data live off site, and there are very few methods in place to access and properly acquire those data. In this section, we will identify these locations, including SharePoint, Exchange, webcam, network locations, cloud storage, and social media, not to mention Dropbox, Google Drive, and the Internet of Things. This also includes RAID storage and how to best collect these devices regardless of configuration.

There are very few tools and techniques available when it comes to acquisition of Apple products, as compared to Windows. The tools that exist can be quite expensive, and free tools are simply few and far between. In this section, we will explore the fundamentals of data acquisition, from keystrokes to network connections, running services, and, quite importantly, passwords and decryption keys. With the vastly increasing spread of file-less malware, in many cases the only place that evidence will exist is in memory. Another often-overlooked factor is full disk encryption. In cases like this, “live” acquisition will be your only hope.

The usefulness of file and stream carving cannot be overstated. Some data simply do not live in the defined file space that can be readily accessed by a viewer. From partially overwritten to deleted data, we will explore techniques you can employ when traditional tools fail. Data carving is a skill that is increasingly important. Once the reference to a file is destroyed, how can the data still be recovered? File carving tools will assist in this, but examiners must understand the limitations of their tools. Without the proper pieces of the original file, a carver is useless. At some point, you will be faced with non-functioning media. You’ll learn about the inner workings of hard drives, and what you can (and cannot) do to revive them to a point where you can then create your forensic image. We will also be looking at the “best of breed” data recovery tools, from those that are free to those that cost many thousands of dollars.

Course Day Descriptions

**DAY 1: Evidence File Quick Wins and Dealing with Smartphones**

Investigators will often be responding in high-stress environments where many different entities are critically scrutinizing the collection process. Personnel need to be properly trained and equipped to work in less than optimal surroundings, and be confident that they have managed the scene, identified all necessary data, collected the data in a properly defensible manner, and maintained its integrity. One of the most common scenarios that can cause headaches is receiving an evidence file (usually an E01), and being expected to provide answers immediately. The common approach is to mount the image and then start running carving and other tools against it. These automated tasks can take many hours (and sometimes days) just by themselves! Portable devices bring their own set of challenges, data collection, legal documentation, and proper preservation of systems. Without the proper tools, from those that are free to those that cost many thousands of dollars.

**DAY 2: Evidence Acquisition and Collection**

Investigators and first responders should be armed with the latest tools, digital container access techniques, and enterprise methodologies to identify, access, and preserve evidence across a vast range of devices and repositories. Personnel must also be able to scale their identification and collection across thousands of systems in their enterprise. Enterprise and cloud storage collection techniques are now a requirement to track activity that has been intentionally and unintentionally spread across many devices. Responding to these many systems cannot be accomplished using the standard “pull the hard drive” forensic examination methodology. Such an approach will cause frustration and result in lost opportunities due to the time it takes to forensically image entire hard drives. Furthermore, investigators need actionable intelligence as quickly and responsibly as possible. This section lays the foundation for evidence collection, from initial arrival on a scene to the fundamentals of understanding data at rest and properly identifying devices, interfaces, and tools that will be necessary to affect successful collection. This course section will explore the myriad of acquisition hardware and software, not to mention adapters and identification, so we can make the best decisions about the data.

**DAY 3: Quick Win Forensics**

Hand-on labs

Mon, Jun 15 – Sat, Jun 20
9:00am – 5:00pm
Hands-on labs

**DAY 4: Non-Traditional and Cloud Acquisition**

**DAY 5: Apple Acquisition, Internet of Things, and Online Attribution**

Who Should Attend

Federal agents and law enforcement personnel
First responders
Digital forensic analysts
Information security professionals
Incident response team members
Media exploitation analysts
Department of Defense and intelligence community professionals
Anyone interested in an understanding of the proper preservation of systems

“This course showed some useful info that I wasn’t aware of previously, i.e., RAID acquisition, tool usage, and data recovery.”

— Nina Turner, Travelers

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

59
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

Ovie Carroll
SANS Principal Instructor

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

FOR500: Windows Forensic Analysis will teach you to:

- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

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 such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital 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 experts 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 Microsoft Windows operating systems. You can’t protect what you don’t know about, and understanding forensic capabilities and artifacts is a core component of information security. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track particular user activity on your network, and organize findings for use in incident response, internal investigations, and civil/criminal litigation. You will 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 unbelievable 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, Windows 8/8.1, Windows 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 7 systems to just-discovered Windows 10 artifacts.

Ovie Carroll has 31 years of law enforcement experience and over 20 years of cyber investigative experience. He is the Director of the Cybercrime Lab of the Computer Crime and Intellectual Property Section (CCIPS) at the Department of Justice (DOJ). The lab provides advanced computer forensics, cybercrime investigation, and other technical assistance to DOJ prosecutors to support implementation of the department’s national strategies for digital evidence and to combat electronic penetration, data theft, and cyberattacks on critical information systems. At SANS Ovie teaches FOR500: Windows Forensic Analysis, a course he also co-authored. Prior to joining the DOJ, Ovie was a special agent in charge of overseeing the Technical Crimes Unit of the Postal Inspector General’s Office, where he was responsible for all computer intrusion investigations within the postal service network infrastructure and for providing all digital forensic analysis in support of criminal investigations and audits. He also served as a special agent in the U.S. Air Force Office of Special Investigations, investigating computer intrusions and working both general crimes and counterintelligence as well as conducting investigations into offenses including murder, rape, fraud, bribery, theft, and gangs and narcotics.

@ovie
**Course Day Descriptions**

**DAY 1: Windows Digital Forensics and Advanced Data Triage**
The Windows forensics course starts with an examination of digital forensics in today’s interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

**Topics:** Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File Carving; Custom Carving Signatures; Memory, Pagefile, and Unallocated Space Analysis

**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. Throughout the section, investigators will use their skills in a real hands-on case, exploring the evidence and analyzing evidence.

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

**DAY 3: Core Windows Forensics Part 2 – USB Devices and Shell Items**
Being able to show the first and last time a file or folder was opened is a critical analysis skill. Utilizing shortcut (LNK), jump list, and Shellbag databases through the examination of SHELL ITEMS, we can quickly pinpoint which file or folder was opened and when. The knowledge obtained by examining SHELL ITEMS is crucial in tracking user activity in intellectual property theft cases internally or in tracking hackers. Removable storage device investigations are often an essential part of performing digital forensics. We will show you how to perform in-depth USB device examinations on Windows 7, 8/8.1, and 10. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, and even the unique serial number of the device used.

**Topics:** SHELL ITEM Forensics; USB and Bring Your Own Device (BYOD) Forensic Examinations

**DAY 4: Core Windows Forensics Part 3 – Email, Key Additional Artifacts, and Event Logs**
Depending on the type of investigation and authorization, a wealth of evidence can be unearthed through the analysis of email files. Recovered email can bring excellent corroborating information to an investigation, and its informality often provides very incriminating evidence. It is common for users to have an email address that exists locally on their workstation, on their company email server, in a private cloud, and in multiple webmail accounts. Windows event log analysis has solved more cases than possibly any other type of analysis. Understanding the locations and content of these files is crucial to the success of any investigator. Many researchers overlook these records because they do not have adequate knowledge or tools to get the job done efficiently. This section arms each investigator with the core knowledge and capability to maintain this crucial skill for many years to come.

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

**DAY 5: Core Windows Forensics Part 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome**
With the increasing use of the web and the shift toward web-based applications and cloud computing, browser forensic analysis has become a critical skill. During this section, the investigator will comprehensively explore web browser evidence created during the use of Internet Explorer, Edge, Firefox, and Google Chrome. The analyst will learn how to examine every significant artifact stored by the browser and how to analyze some of the more obscure (and powerful) browser artifacts, such as session restore, tracking cookies, zoom levels, predictive site prefetching, and private browsing remnants.

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

**DAY 6: Windows Forensic Challenge**
This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections.

**Topics:** Digital Forensic Case, Windows 10 Forensic Challenge

---

**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

---

*“The hands-on [labs] are excellent – best I have had in 15 years of forensics classes – and the books are the best as well.”*

— Shawn Bostick, AR AG

*“It’s great to hear real-world examples that apply to the concepts that are being taught. It helps answer the ‘why’ behind the process.”*

— Bradley Chapple, Virustream
FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

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 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-stamped 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 Incident Response, Threat Hunting, and Digital Forensics will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Perform damage assessments and determine what was stolen 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. They won’t tell you 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.

The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done significant damage to the organization. For the incident responder, this process is known as “threat hunting.” Threat hunting uses known adversary behaviors to proactively examine the network and endpoints in order to identify new data breaches.

Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. Your team can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems, provide ineffective containment of the breach, and ultimately fail to rapidly remediate the incident. Incident response and threat hunting teams are the keys to identifying and observing malware indicators and patterns of activity in order to generate accurate threat intelligence that can be used to detect current and future intrusions.

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 hacktivists. Constantly updated, FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics 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.

ADVANCED THREATS ARE IN YOUR NETWORK – 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 U.S. 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 a consultant, 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
## 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 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 incident response for advanced threat groups. We will show the importance of developing cyber threat intelligence to impact the adversary’s “kill chain” and demonstrate live response techniques and tactics that can be applied to a single system and across the entire enterprise.

**Topics:**
- Real Incident Response Tactics; Threat Hunting; Threat Hunting in the Enterprise; Incident Response and Hunting across Endpoints; Malware Defense Evasion and Identification; Malware Persistence Identification; Investigating WMI-Based Attacks

## Day 2: Intrusion Analysis

Cyber defenders have a wide variety of tools and artifacts available to identify, hunt, and track adversary activity in a network. Each attacker 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 detection efforts on immutable portions of that pattern. As an example, at some point attackers will need to run code to accomplish their objectives. We can identify this activity via application execution artifacts. Attackers will also need one or more accounts to run code. Consequently, account auditing is a powerful means of identifying malicious actions. Attackers also need a means to move throughout the network, so we look for artifacts left by the relatively small number of ways there are to accomplish this part of their mission. 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:**
- Theft and Utilization of Legitimate Credentials; Advanced Evidence of Execution Detection; Lateral Movement Adversary Tactics, Techniques, and Procedures (TTPs); Log Analysis for Incident Responders and Hunters

## Day 3: Memory Forensics in Incident Response and Threat Hunting

Now a critical component of many incident response and threat hunting teams that regularly detect advanced adversaries 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, PowerShell, and advanced malware used by APT attackers. In fact, some attacks may be nearly impossible to unravel without memory analysis. Memory analysis was traditionally the domain of Windows internals experts, but the recent development of new tools and techniques makes it accessible today to all investigators, incident responders, and threat hunters. Better tools, interfaces and detection heuristics have greatly leveled the playing field. Understanding attack patterns in memory is a core analyst skill applicable across a wide range of endpoint detection and response products. This extremely popular section will cover many of the most powerful memory analysis capabilities available and give you a solid foundation of advanced memory forensic skills to super-charge investigations, regardless of the toolset employed.

**Topics:**
- Remote and Enterprise Incident Response; Triage and Endpoint Detection and Response; Memory Acquisition; Memory Forensics Analysis Process for Response and Hunting; Memory Forensics Examinations; Memory Analysis Tools

## Day 4: Timeline Analysis

Learn advanced incident response and hunting techniques uncovered via timeline analysis directly from the authors who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. Pioneered by Rob Lee in 2001, timeline analysis has become a critical incident response, hunting, and forensics technique. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. The analysis that once took days now takes minutes. 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 and Analysis; Super Timeline Creation and Analysis

## Day 5: Incident Response & 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:**
- Cyber Threat Intelligence; Malware and Anti-Forensic Detection; Anti-Forensic Detection Methodologies; Identifying Compromised Hosts without Active Malware

## Day 6: The APT Threat Group 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
- Security Operations Center analysts
- 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

---

**Favorite SANS class so far. Really excellent material. Really excellent delivery.”**

— Joshua Sitta, Center State Bank

---

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/sansfire/courses](https://sans.org/sansfire/courses)
FOR526: **Advanced Memory Forensics & Threat Detection**

**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

**Alissa Torres**

*SANS Principal Instructor*

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

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

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

FOR526: Advanced Memory Forensics & Threat Detection 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 timeline, high-low 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 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. In her current role as a Senior Cyber Defense Operator at SimSpace, she architects and investigates the latest adversary tactics, which requires 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 (GCFCA), and holds the GCFE, GCIH, 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
Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu IFT and Windows 10 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 Suspicious Binaries,” it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

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

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 Challenges
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)
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

Phil Hagen
SANS Senior Instructor

This course will help you take your system-based forensic knowledge onto the wire, enabling you to 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 a perpetrator’s 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, or 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 is designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today’s investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting that uses existing evidence along with newly acquired threat intelligence to uncover evidence of previously unidentified incidents. Other teams focus on post-incident investigations and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim’s environment. In these situations and more, the artifacts left behind from attackers’ communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have 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-based dissection, 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 under way.

FOR572 is truly an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stake networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course as you hone your skills to fight crime.

UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME.

Phil Hagen began his studies at the U.S. Air Force Academy’s Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. Today, Phil’s career has spanned the full attack life cycle – tool development, deployment, operations, and the investigative aftermath – giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He has supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. All of that brings Phil to his role today as the DFIR strategist at Red Canary, where he supports the firm’s managed threat detection service. Phil also spends time developing and maintaining the SOF-ELK distribution, a virtual appliance free for the DFIR Community.

@PhilHagen
### Course Day Descriptions

**DAY 1: Off the Disk and Onto the Wire**

Although many fundamental network forensic concepts align with those of any other digital forensic investigation, the network presents many nuances that require special attention. Today you will learn how to apply what you already know about digital forensics and incident response to network-based evidence. You will also become acclimated to the basic tools of the trade.

**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**

There are countless network protocols that may be in use in a production network environment. We will cover those that are most likely to benefit the forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the “typical” behaviors of these protocols, we can more readily identify anomalies that may suggest misuse of the protocol for nefarious purposes. These protocol artifacts and anomalies can be profiled through direct traffic analysis as well as through the log evidence created by systems that have control or visibility of that traffic. While this affords the investigator with vast opportunities to analyze the network traffic, efficient analysis of large quantities of source data generally requires tools and methods designed to scale.

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

---

**DAY 3: NetFlow and File Access Protocols**

Network connection logging, commonly called NetFlow, may be the single most valuable source of evidence in network investigations. Many organizations have extensive archives of flow data due to its minimal storage requirements. Since NetFlow does not capture any content of the transmission, many legal issues with long-term retention are mitigated. Even without content, NetFlow provides an excellent means of guiding an investigation and characterizing an adversary’s activities from pre-attack through operations. Whether within a victim’s environment or for data exfiltration, adversaries must move their quarry around through the use of various file access protocols. By knowing some of the more common file access and transfer protocols, a forensicator can quickly identify an attacker’s theft 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 are a mainstay in the network forensicator’s toolkit. We’ll explore the various roles that commercial tools generally fill, as well as how they can be best integrated into an investigative workflow. With the runaway adoption of wireless networking, investigators must also be prepared to address the unique challenges this technology brings to the table. However, regardless of the protocol being examined or budget used to perform the analysis, having a means of exploring full-packet capture is a necessity, and having a toolkit to perform this at scale is critical.

**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**

Advances in common technology have made it easier to be a bad guy and harder for us to track them. Strong encryption methods are readily available and custom protocols are easy to develop and employ. Despite this, there are still weaknesses even in the most advanced adversaries’ methods. As we learn what the attackers have deliberately hidden from us, we must operate carefully to avoid tipping our hats regarding the investigative progress – otherwise the attacker can quickly pivot, nullifying our progress.

**Topics:** Encoding, Encryption, and SSL/TLS; Meddler-in-the-Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

---

**DAY 6: Network Forensics Capstone Challenge**

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

**Topics:** Network Forensic Case

---

### Who Should Attend

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

---

“This course is fantastic. It has prepared me with new ideas to take back to work.”

— Ryan Fletcher, Fulton Financial Corp

“First course I’ve taken that gives insight into the forensic mindset required for investigating incidents.”

— Tyler Whittington, PWC

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/sansfire/courses](https://sans.org/sansfire/courses)
FOR578: Cyber Threat Intelligence

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

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 skill set 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.

“I could take this course five times more and get something new each time! So much valuable info to take back to my organization.”
— Charity Willhoite, Armor Defense, Inc.

Robert M. Lee
SANS Senior Instructor

Robert is the CEO and founder of his own company, Dragos, Inc., which provides cybersecurity solutions for industrial control system (ICS) networks. Robert got his start in information security making small control systems for humanitarian missions. He joined the U.S. Air Force and became a cyberspace warfare operations officer in the U.S. Intelligence community. In that role, he created and led a mission examining nation-states targeting ICS, the first mission of its kind in the U.S. intelligence community. When the Ukraine power grid went down due to a cyber attack in 2015, Robert helped form a specialized team to analyze the event, then passed the information on to the impacted parties as well as the U.S. government and private sector. He and his team also analyzed the malware from the 2016 cyber-attack on Ukraine’s Kiev substation and dubbed it CRASHOVERRIDE as the first ever malware tailored to specifically disrupt electricity grid operations. Robert has a master’s degree in cybersecurity and computer forensics from Utica College as well as cyber and warfare training through the U.S. Air Force, and he’s pursuing his doctorate in war studies from King’s College London. He was named one of Forbes’ 30 under 30 in Enterprise Technology in 2016, awarded EnergySec’s 2015 Cyber Security Professional of the Year, and named one of Passcode’s “Influencers.”

@RobertMLee
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, as well as 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 Skill Set: Intrusion Analysis

Intrusion analysis is at the heart of threat intelligence. It is a fundamental skill set 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, Threat Intelligence Consumption, Positioning the Team to Generate Intelligence, Planning and Direction 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: Sopacy; Attribution

“This course is terrific! Class discussion and relevant case studies are extremely helpful for better understanding the content.”
— Larci Robertson, Epsilon

“Great information on TLS cert pivoting. I will be using this as soon as I get back to work.”
— Rich Ferguson, Refinitiv
FOR585: Smartphone Forensic Analysis In-Depth

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 manual timeline development and link analysis (e.g., who communicated with whom, where, and when) without relying on a tool
- 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, suggestions, or application associations 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: Smartphone Forensic Analysis In-Depth 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 31 hands-on labs, a forensic challenge, and a bonus take-home case 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.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it’s time for the good guys to get smarter and for the bad guys to know that their smartphone activity can and will be used against them!

Smartphone data can’t hide forever — it’s time to outsmart the mobile device!

Heather Mahalik
SANS Senior Instructor

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 Senior Director of Digital Intelligence at Cellebrite. Heather previously led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the federal government. She also worked as a forensic examiner at Stroz 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

FOR585: Smartphone Forensic Analysis In-Depth will help you understand:
- Where key evidence is located on a smartphone
- How the data got onto the smartphone
- How to recover deleted mobile device data that forensic tools miss
- How to decode evidence stored in third-party applications
- How to detect, decompile, and analyze mobile malware and spyware
- Advanced acquisition terminology and free techniques to gain access to data on smartphones
- How to handle locked or encrypted devices, applications, and containers

Register at sans.org/sansfire | 301-654-SANS (7267)
Course Day Descriptions

Mon, Jun 15 – Sat, Jun 20

9:00am – 5:00pm

Hands-on labs

DAY 1: Smartphone Overview, Misfit Devices, SQLite Introduction, and Android Forensics Overview

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, misfit devices, SQLite database examination, and query development. They’ll also gain an overview of Android devices and manually crack locked Androids. Students will become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures. We realize that not every examines Blackberry and knock-off devices, which is why we offer “choose your own adventure” labs, meaning that students can select the labs most relevant to them. BlackBerry 10 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 10 device file systems. Knock-off devices are another outlier than can be parsed and decoded once you become familiar with the file system structures.

Topics: The SIFT Workstation, Forensic Acquisition Concepts of Smartphones, Smartphone Components, Introduction to SQLite, Android Forensic Overview, Handling Locked Android Devices

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. Unfortunately, gaining access to these devices isn’t as easy as it used to be. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. However, without honing the appropriate skills to bypass locked Androids and correctly interpret the data stored on them, you will be unprepared for the rapidly evolving world of smartphone 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. Additionally, Android and Google cloud data store tons of valuable information. You will find Google artifacts from iOS users as well.

Topics: Android Acquisition Considerations; Android File System Structures; Android Evidentiary Locations; Traces of User Activity on Android Devices; Android Backup Files; Google Cloud Data and Extractions

DAY 3: iOS Device Forensics

Apple iOS devices contain substantial amounts of data (including deleted records) that can be decoded and interpreted into useful information. Proper handling and parsing skills are needed for bypassing locked iOS devices and correctly interpreting the data. Without iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

Topics: iOS Forensic 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, Malware and Spyware Forensics, and Detecting Evidence Destruction

iOS backups are extremely common and are found in the cloud and on hard drives. Users create backups, and we often find that our best data can be derived from creating an iOS backup for forensic investigation. This section will cover methodologies to extract backups and cloud data and analyze the artifacts for each. Malware affects a plethora of smartphone devices. We 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 day alone! The day ends with the students challenging themselves using tools and methods learned throughout the week to recover user data from a wiped smartphone.

Topics: iOS Backup File Forensics; Locked iOS Backup Files; iCloud Data Extraction and Analysis; Malware and Spyware Forensics; Detecting Evidence Destruction

DAY 5: Third-Party Application Analysis

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, recovery of 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; Mobile Browsers; Secure Chat Applications

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.

Topics: Identification and Scoping; Forensic Examination; Forensic Reconstruction

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, FOR572, FOR526, FOR610, or FOR518 who want to take their skills to the next level

“Absolutely, it is the best course for mobile forensics.”

— Mantautas Neniskis, PWC

“Mobile phones have become increasingly prevalent in digital investigations, and this course equips examiners with the latest techniques to perform a holistic examination.”

— Bilal Malik, Stroz Friedberg
Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training helps 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.

The course culminates with a series of Capture-the-Flag challenges designed to reinforce the techniques learned in class and provide additional opportunities to learn practical, hands-on malware analysis skills in a fun setting.

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.

Aply 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 for examining and interacting with malware.

Aply 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, Lenny leads the cybersecurity program as the Chief Information Security Officer (CISO) at Axonius. 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 certification, 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 (REMnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab—with guidance and explanations from the instructor—to reinforce the concepts discussed throughout the day.

**Topics:**
- Assembling a Toolkit for Effective Malware Analysis
- Examining Static Properties of Suspicious Programs
- Performing Behavioral Analysis of Malicious Windows Executables
- Performing Static and Dynamic Code Analysis of Malicious Windows Executables
- Interacting with Malware in a Lab to Derive Additional Behavioral Characteristics

---

### 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 intel assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The material will then build on this foundation and expand your understanding to incorporate 64-bit malware, given its growing popularity. Throughout the discussion, you will learn to recognize common characteristics at a code level, including HTTP command and control, keylogging, and command execution.

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

---

### 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 executables. 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:**
- How Malware Detects Debuggers and Protects Embedded Data
- Unpacking Malicious Software that Employs Process Hollowing
- Bypassing the Attempts by Malware to Detect and Evade the Analysis Toolkit
- Handling Code Misdirection Techniques, Including SEH and TLS Callbacks
- Unpacking Malicious Executable by Anticipating the Packer’s Actions

---

### 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

---

“For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses

“**This is a truly a step-by-step mentorship course. The content is immediately applicable to DFIR job roles.”**

— Chad Reams, Parsons Inc.”
SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the Certified Information Systems Security Professional (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 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.

“**This course really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back.**”

— Merewyn Boak, Apple

**Seth Misenar**
SANS Faculty Fellow

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, GCIH, GCWN, GCFA, and MCSE. @sethmisenar
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 latest 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 2020 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 sans.org/sansfire/courses
## MGT512: Security Leadership Essentials for Managers

Security managers need both technical knowledge and management skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics.

This course empowers you to become an effective security manager and 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.

To accomplish this goal, MGT512 covers a wide range of security topics across the entire security stack. Data, network, host, application, and user controls are covered in conjunction with key management topics that address the overall security lifecycle. This also includes governance and technical controls focused on protecting, detecting, and responding to security issues.

This approach prepares you to:

- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

MGT512 uses case studies, group discussions, team-based exercises, and in-class games to help students absorb both technical and management topics.

### You Will Be Able To
- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals
- Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage technical personnel
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud

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

— Rick Derks, FCS Financial

**G. Mark Hardy**  
SANS Principal Instructor

G. Mark Hardy is founder and president of National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 35 years, and is an internationally recognized expert and keynote speaker who has presented at over 250 events world-wide. 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
Course Day Descriptions

**DAY 1: Building Your Program**
The course starts with a tour of the information and topics that effective security managers and leaders must know to function in the modern security environment. This includes an understanding of the different types of cybersecurity frameworks available to structure your security team and program. Risk is central to effective information security management, and key risk concepts are discussed to lay the foundation for effective risk assessment and management. Security policy is a key tool that security managers use to manage risk. We'll cover approaches to policy to help you plan and manage your policy process. Finally, security functions, reporting relationships, and roles and responsibilities are discussed to give the advancing manager a view into effective security team and program structure.

**Topics:** Security Frameworks, Understanding Risk, Security Policy, Program Structure

---

**DAY 2: Protecting Data and Networks**
Day 2 provides foundational knowledge to protect data and networks. This includes building an understanding of cryptography concepts, encryption algorithms, and applications of cryptography. Since encrypting data alone is not sufficient, the distinction between privacy and security is discussed to give managers a primer on key privacy concepts. Finally, a thorough discussion of network security is modeled around the various layers of the network stack. This allows managers to gain a deeper understanding of what their teams are talking about, what vendors are selling, and where various issues and protections lay within the seven layers of the network model.

**Topics:** Data Protection, Privacy Primer, Network Security

---

**DAY 3: Protecting and Patching Systems**
Day 3 is focused on protecting and patching systems. This includes coverage of host security that encompasses endpoint and server security along with malware and attack examples. Modern infrastructure as code approaches and tools are also discussed as ways to automate consistent deployment of standard configurations. Managers must also be knowledgeable about software development processes, issues, and application vulnerabilities. Coverage includes an overview of the secure SDLC, OWASP Top Ten, and leading-edge development processes built on DevOps. Managers must also understand physical security controls that, when not implemented appropriately, can cause technical security controls to fail or be bypassed. All of these issues and corresponding vulnerabilities must be appropriately managed. This leads to a discussion on building a vulnerability management program and the associated process for successfully finding and fixing vulnerabilities.

**Topics:** Host Security, Application Security, Physical Security, Vulnerability Management

---

**DAY 4: Leading Modern Security Initiatives**
Day 4 covers what managers need to know about leading modern security initiatives. Security awareness is a huge component of any security program that is focused on driving activities that lead to changes in human behavior and creating a more risk-aware and security-aware culture. For any project or initiative, security leaders must also be able to drive effective project execution. Having a well-grounded understanding of the project management process makes it easier to move these projects forward. The cloud is a major initiative that many organizations are either tackling now or planning to undertake. To get ready for these initiatives, an overview of Amazon Web Services (AWS) is provided to serve as a reference, along with a discussion of key cloud security issues based on the Cloud Security Alliance guidance. The cloud, the rise of mobile devices, and other factors are highlighting weaknesses in traditional, perimeter-oriented security architectures. This leads to a discussion of the Zero Trust Model. To execute such new initiatives security leaders must also develop negotiation skills and the ability to manage highly technical team members.

**Topics:** Security Awareness, Project Management, Cloud Security, Modern Security Architecture, Management Methods

---

**DAY 5: Detecting and Responding to Attacks**
Day 5 is focused on detection and response capabilities. This includes gaining appropriate visibility via logging and monitoring, and thinking strategically about a Security Information and Event Management (SIEM) system. These logs are a core component of any Security Operations Center (SOC). The key functions of a SOC are discussed along with how to design, build, operate, and mature security operations for your organization. The incident response process is discussed in relation to identifying, containing, eradicating, and recovering from security incidents. This leads into a discussion of longer-term disaster recovery and business continuity planning. Finally, the course ends with a war game that simulates an actual incident. This tabletop simulation contains a number of injects or points at which students are presented with additional information to which they can respond. After dealing with the incident itself, the simulation concludes with a game focused on choosing appropriate security controls to mitigate future incidents.

**Topics:** Logging and Monitoring, Security Operations Center, Incident Response, Contingency Planning, War Game
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.

**You Will Be Able To**

I Develop security strategic plans that incorporate business and organizational drivers

I Develop and assess information security policy

I Use management and leadership techniques to motivate and inspire your teams

**Frank Kim**

*SANS Senior Instructor*

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:

I **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.

I **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.

I **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.

**You Will Be Able To**

I Develop security strategic plans that incorporate business and organizational drivers

I Develop and assess information security policy

I Use management and leadership techniques to motivate and inspire your teams

**Frank Kim**

*SANS Senior Instructor*

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
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

“**This training is valuable because it shines a light on the many business aspects of security, while also providing excellent guidance for applying learnings in real life.**”

— Alyssa DeVita, Marriott

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team lead or management responsibilities
You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate technology law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard)

“I wish I’d taken LEG523 four years ago, so that our policy and governance could have been enhanced sooner.”

— Tom Siu, Case Western Reserve University

Benjamin Wright
SANS Senior Instructor

LEG523 is constantly updated to address changing trends and current events. Here’s a sampling of what’s new:

- Sample contract clauses requiring cybersecurity for the Danish government, consistent with the General Data Protection Regulation (GDPR)
- Court decision showing how to improve an official investigation using artificial intelligence
- Unique and indispensable training for GDPR Data Protection Officers
- Form contract for inviting outside incident responders – including police, contractors, National Guard, or civil defense agencies anywhere in the world – to help with a cyber crisis
- The European Union’s new GDPR and its impact around the world

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 to 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
Course Day Descriptions

**DAY 1: Fundamentals of Data Security Law and Policy**
The first day is an introduction to law and IT that serves as the foundation for discussions during the rest of the course. We survey the general legal issues that must be addressed in establishing best information security practices, then canvas the many new laws on data security and evaluate information security as a field of growing legal controversy. We will cover computer crime and intellectual property laws when a network is compromised, as well as emerging topics such as honeypots. We will look at the impact of future technologies on law and investigations in order to help students factor in legal concerns when they draft enterprise IT security policies. For example, students will debate what the words of an enterprise policy would mean in a courtroom. The course also dives deep into the legal question of what constitutes a “breach of data security,” for purposes of notifying others about it or for other reasons. The course includes a case study on the drafting of policy to comply with the Payment Card Industry Data Security Standard (PCI). Students learn how to choose words more carefully and accurately when responding to cybersecurity questionnaires from regulators, cyber insurers and corporate customers.

**DAY 2: E-Records, E-Discovery and Business Law**
IT professionals can advance their careers by upgrading their expertise in the hot fields of e-discovery and cyber investigations. Critical facets of those fields come forward in course day two. We will focus on the use of computer records in disputes and litigation, with a view to teaching students how to manage requests to turn over e-records to adversaries (i.e., e-discovery), manage implementation of a “legal hold” over some records to prevent their destruction, and coordinate with legal counsel to develop workable strategies to legal challenges. Transactions that used to be conducted on paper are now done electronically, so commercial law now applies to computer security. The IT function within an enterprise has become the custodian of an enterprise’s business records. You will learn how to craft sound policy for the retention and destruction of electronic records like email, text messages, and social networking interactions. We will provide methods for balancing the competing interests in electronic records management, including costs, risks, security, regulations and user cooperation. Law and technology are changing quickly, and it is impossible for professionals to comprehend all the laws that apply to their work. But they can comprehend overarching trends in law, and they can possess a mindset for finding solutions to legal problems. A key goal of this course day is to equip students with the analytical skills and tools to address technology law issues as they arise, both in the United States and around the world. Special attention is devoted to European data protection laws (see the white paper by Benjamin Wright on the European Union’s new General Data Protection Regulation). The course is chock full of actual court case studies dealing with privacy, computer records, digital evidence, electronic contracts, regulatory investigations, and liability for shortfalls in security. The purpose of the case studies is to draw practical lessons that students can take back to their jobs.

**DAY 4: The Law of Data Compliance: How to Conduct Investigations**
Information security professionals and cyber investigators operate in a world of ambiguity, rapid change, and legal uncertainty. To address these challenges, this course day presents methods to analyze a situation and then act in a way that is ethical and defensible and reduces risk. Lessons will be invaluable to the effective and credible execution of any kind of investigation, be it internal, government, consultant, security incident, or any other. The lessons also include method and justifications for maintaining the confidentiality of an investigation. The course surveys white-collar fraud and other misbehaviors with an emphasis on the role of technology in the commission and prevention of that fraud. It teaches IT managers practical and case-study-driven lessons about the monitoring of employees and employee privacy. IT is often expected to “comply” with many mandates, whether stated in regulations, contracts, internal policies or industry standards (such as PCI-DSS). This course teaches many broadly applicable techniques to help technical professionals establish that they and their organizations are in fact in compliance, or to reduce risk if they are not in perfect compliance. The course draws lessons from models such as the Sarbanes-Oxley Act. As IT security professionals take on more responsibility for controls throughout an enterprise, it is natural that they worry about fraud, which becomes a new part of their domain. This day covers what fraud is, where it occurs, what the law says about it and how it can be avoided and remedied. Indeed, the primary objective of Sarbanes-Oxley is not to keep hackers out; it is to snuff out fraud inside the enterprise. Scattered through the course are numerous descriptions of actual fraud cases involving technology. The purpose is to acquaint the student with the range of modern business crimes, whether committed by executives, employees, suppliers or whole companies. More importantly, the course draws on the law of fraud and corporate misconduct to teach larger and broader lessons about legal compliance, ethical hacking and proper professional conduct in difficult case scenarios. Further, the course teaches how to conduct forensics investigations involving social, mobile and other electronic media. Students learn how to improve the assessment and interpretation of digital evidence, such as evidence of a breach or other cyber event.

**DAY 5: Applying Law to Emerging Dangers: Cyber Defense**
Knowing some rules of law is not the same as knowing how to deal strategically with real-world legal problems. This day is organized around extended case studies in security law: break-ins, investigations, piracy, extortion, rootkits, phishing, botnets, espionage and defamation. The studies lay out the chronology of events and critique what the good guys did right and what they did wrong. The goal is to learn to apply principles and skills to address incidents in your day-to-day work. The course includes an in-depth review of legal responses to the major security breaches at TIA, Target, and Home Depot, and looks at how to develop a Bring Your Own Device (BYOD) policy for an enterprise and its employees. The skills learned are a form of crisis management, with a focus on how your enterprise will be judged in a courtroom, by a regulatory agency, or in a contract relationship. Emphasis will be on how to present your side of a story to others, such as law enforcement, Internet gatekeepers, or the public at large, so that a security incident does not turn into a legal casus. In addition to case studies, the core material will include tutorials on relevant legislation and judicial decisions in such areas as privacy, negligence, contracts, e-investigations, computer crime and offensive countermeasures. LEG523 is increasingly global in its coverage, so although this course day centers around U.S. law, non-U.S. law and the roles of government authorities outside the United States will be examined, as well. At the end of this course section, the instructor will discuss a few sample questions to help students prepare for the GIAC exam associated with this course (GLEG).
SEC540: Cloud Security and DevOps Automation

SEC540 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications.

Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications. Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software. SEC540 provides in-depth analysis of the Amazon Web Services (AWS) toolchain, while lightly covering comparable services in Microsoft Azure. Using the CI/CD toolchain, students build a cloud infrastructure that can host containerized applications and microservices. Hands-on exercises analyze and fix cloud infrastructure and application vulnerabilities using security services and tools such as API Gateway, Identity and Access Management (IAM), CloudFront Signing, Security Token Service (STS), Key Management Service (KMS), managed WAF services, serverless functions, CloudFormation, AWS Security Benchmark, and much more.

Who Should Attend
- Anyone working in 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 to migrate DevOps workflows to the cloud, specifically Amazon Web Services (AWS)
- Anyone interested in leveraging cloud application security services provided by AWS
- Developers
- Software architects
- Operations engineers
- System administrators
- Security analysts
- Security engineers
- Auditors
- Risk managers
- Security consultants

“Mind-blowing! If you are a traditional security architect, tip-toeing around DevOps, get into SEC540. It takes you into the depths of DevSecOps and sets you up for the future!”

— Jatin Sachdeva, Cisco

Greg is a principal consultant with Optiv Security, Inc. where he helps clients secure their applications by performing penetration tests, secure code reviews, and risk assessments. Greg’s responsibilities over the course of his career have included: application architecture and security, infrastructure design and implementation, performance diagnostics, and security research. In his time with SANS, Greg has authored application security content related to secure coding for web and mobile applications, threat awareness, and top development design flaws as well as contributing to DevSecOps and cloud security content.

@appsecegreg
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 ICS 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 ICS 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 ICS, 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 ICS environments. The course will help develop cybersecurity-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.

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

@meas
Cyber Defense 2-Day Course

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 (CSC) as documented by the Center for Internet Security (CIS). The Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the U.S. military and other government agencies (including the 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. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566: Implementing and Auditing the Critical Security Controls – In-Depth.

The Critical Security Controls can be found at [www.cisecurity.org/controls](http://www.cisecurity.org/controls). You will find the full document describing the Critical Security Controls posted at the Center for Internet Security.

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

SEC455: SIEM Design and Implementation

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, but using those 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 nimble 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.

SEC455 serves as an important primer to those who are unfamiliar with the architecture of an Elastic-based SIEM. Students who have taken or plan to take additional cyber defense courses may find SEC455 to be a helpful supplement to the advanced concepts in courses such as SEC555. In addition, the material discussed in this course will enable students to not only build a new SIEM, but improve and supplement their already existing implementations, producing a more efficient solution that provides the answers they need more quickly and at a lower cost. The overall goal is to show students how to design and modify a SIEM, improve upon their current solution, and reach their original defensive goal – catching adversary activity in their environment.
Penetration Testing 2-Day Courses

NEW! SEC564: Red Team Exercises & Adversary Emulation

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world adversaries in order to train and measure the effectiveness of the people, processes, and technology used to defend organizations. SEC564 will provide you with the skills to manage and operate a Red Team, conduct Red Team exercises and adversary emulations, and understand the role of the team and its importance in security testing.

Built on the fundamentals of penetration testing, Red Team exercises use a comprehensive approach to gain a holistic view of an organization’s security posture in order to improve its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team exercises significantly improve an organization’s security posture and controls, hone its defensive capabilities, and measure the effectiveness of its security operations.

Red Team exercises require a different approach from a typical security test and rely heavily on well-defined TTPs, which are critical to successfully emulating a realistic adversary. The Red Team exercises and adversary emulation results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against a real adversary, and identify where security strengths and weaknesses exist across people, processes, and technology.

Whether you support a defensive or offensive role in security, understanding how Red Team exercises can be used to improve security is extremely valuable. This intensive two-day course will explore Red Team concepts in-depth, provide the required fundamentals of adversary emulation, and help you improve your organization’s security posture.

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.

Author Statement

“Metasploit is the most popular free exploitation tool available today. It is in widespread use by penetration testers, vulnerability assessment personnel, auditors, and real-world threat actors. However, most of its users rely on and understand only about 10 percent of its functionality, not realizing the immensely useful other features that Metasploit offers. This course will enable students to master the 10 percent they currently rely on (applying it in a more comprehensive and safe manner), while unlocking the other 90 percent of features they can then apply to make their tests more effective. By attending this course, students will learn how to make a free tool achieve the power of many much more costly commercial tools.”

— Jeff McJunkin

For course updates, prerequisites, special notes, or laptop requirements, visit sans.org/sansfire/courses
Management 2-Day Courses

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.

“This training will assist me and my team with putting a much better security awareness program in place. The maturity model is a great resource.” — James Pomeroy, Seim Johnson LL

NEW! MGT521: Driving Cybersecurity Change – Establishing a Culture of Protect, Detect and Respond

Cybersecurity is no longer just about technology – it is ultimately about organizational change. This means change not only in how people think about security, but in what they prioritize and how they act, from the Board of Directors on down. Organizational change is a field of management study that enables organizations to analyze, plan, and then improve their operations and structures by focusing on people and culture.

MGT521 will teach leaders how to leverage the principles of organizational change, enabling them to develop, maintain and measure a security-driven culture. Through hands-on, real-world instruction and a series of interactive labs and exercises in which you will apply the concepts of organizational change to a variety of different security initiatives, you will quickly learn how to embed cybersecurity into your organizational culture.
**DevSecOps 2-Day Course**

**SEC534: Secure DevOps: A Practical Introduction**

This course explains the fundamentals of DevOps and how DevOps teams can build and deliver secure software. You will learn DevOps principles, practices, and tools and how they can be leveraged to improve the reliability, integrity, and security of systems.

Using lessons from successful DevOps security programs, we will explain how Secure DevOps can be implemented. Students will gain hands-on experience using popular open-source tools such as Puppet, Jenkins, GitLab, Vault, Grafana, and Docker to automate Configuration Management (“Infrastructure as Code”), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance (“Compliance as Code”), and Continuous Monitoring. The lab environment starts with a CI/CD pipeline that automatically builds, tests, and deploys infrastructure and applications.

Leveraging the Secure DevOps toolchain, students perform a series of labs injecting security into the CI/CD pipeline using a variety of security tools, patterns, and techniques.

**You Will Learn:**

- Foundations and principles of DevOps, Continuous Delivery, and Continuous Deployment
- The security risks and challenges posed by DevOps
- The keys to successful DevOps security programs
- How to build security into Continuous Delivery and Continuous Deployment
- The tools, patterns, and techniques of security automation in DevOps
- How to secure your build and deployment environment and tool chain
- How to leverage Infrastructure as Code for secure configuration management and provisioning
- How manual security practices (risk assessments, audits, and pen tests) can be adapted to continuously changing environments, and the important role that they still play
- Security risks and challenges posed by containers, and how to secure container technology
- How to automate compliance in DevOps, using the DevOps Audit Defense Toolkit

**Hosted Course**

**NEW! HOSTED: Successful InfoSec Consulting**

Becoming a consultant seems like a dream: high pay, freedom, fascinating work and more. These can all be true, but there is more to the reality: as a consultant you are running a business and you need clients!

What does a successful consultant need to know? How do you find clients? How do you get started? This course answers these questions and more.

The course is based on Ted Demopoulos’ nearly three decades of experience as an independent InfoSec consultant, extensive interviews with dozens of other successful consultants, and surveys of those interested in InfoSec consulting.

**Topics include:**

- The myth versus the reality of consulting. Consulting is a great choice for many people, but not for everyone. Is it for you?
- The three different consulting models. Full-time independent consulting is but one successful model.
- The basics: setting up the business. As a consultant you are running a business. Although different legal jurisdictions have different requirements, there are many commonalities. Beyond legal requirements, business know-how is also required.
- A consultant needs clients. We go over the easiest way to get clients, with plenty of real-life examples, and numerous other ways of acquiring clients.
- Setting yourself up for long-term success. It is common for consultants to be successful for 3-5 years and then for their connections to dry up. Here we examine how consultants can achieve long-term success.
- How to grow beyond six figures. The conventional wisdom is that consultants can only make so much money, since they are selling their time. Yet there are consultants who make seven figures and beyond. How do they do it?
Welcome Reception
Kick off your SANSFIRE 2020 experience at the Welcome Reception. Be part of this premier event and join the industry’s most powerful gathering of cybersecurity professionals. Share stories, make connections and learn how to make the most of your week in Washington, DC. Come join your colleagues for a fun, relaxing evening.

General Session – Welcome to SANS
Dr. Johannes Ullrich
Join us for a 30-minute overview to help you get the most out of your SANS training experience. You will receive event information and learn about programs and resources offered by SANS. This brief session will answer many questions and get your training experience off to a great start. This session will be valuable to all attendees but is highly recommended for first-time attendees.

KEYNOTE: The State of the Internet: Handler Lightning Talks and Honeypot Install Fest
Dr. Johannes Ullrich, ISC Director, Marcus Sachs, and Internet Storm Center Handlers
The new decade has started with a bang, with many different and significant vulnerabilities fighting for our attention. Security teams already stretched thin have to move quickly to make decisions that focus on the vulnerabilities that matter to their network – rather than on vulnerabilities that create the most tweets. How do you find out what matters? The Internet Storm Center struggles daily with that question. Sometimes we get it right and sometimes we don’t. This exciting opening session at SANSFIRE 2020 features a series of fast-paced lightning talks by ISC handlers sharing their most recent lessons learned. One of the tools that helps us figure out what matters is our network of honeypots. Volunteers around the world operate these honeypots, and data are shared publicly in close to real-time. We want to help you be part of this fantastic project, so we will walk you through the process of installing the sensor in your network. We’ll have some Raspberry Pi’s on hand to give away, or you can bring your own (a virtual machine also will do). All are welcome to participate, and no particular prior knowledge is required.

Maldocs: A Bit of Blue, A Bit of Red
Didier Stevens, SANS Internet Storm Center Handler
In this talk, Didier Stevens will show you how to use his free, open-source tools to analyze malicious PDFs and Office documents. He’ll also talk about how you can leverage your analysis with IOCs as a blue teamer, but also leverage your analysis for red team exercises.

Leveraging CALDERA to the Max – Additional Development!
Erik Van Buggenhout
CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. It generates plans during operation using a planning system and a pre-configured adversary model based on the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™) project. These features allow CALDERA to dynamically operate over a set of systems using variable behavior, which better represents how human adversaries perform operations than systems that follow prescribed sequences of actions. CALDERA 2.0. released by MITRE in April 2019, includes a larger focus on “extendibility.” During this talk, we will leverage these features for maximum effect, highlight some interesting improvement opportunities in CALDERA, and focus on how to develop additional plugins and features. Some of the topics we’ll touch upon include:

- How can we improve CALDERA’s reporting engine?
- How can we build additional abilities for MITRE CALDERA to increase the ATT&CK™ coverage of the tool?
- How can we adapt CALDERA to work around common security controls in place at organizations?

Arcane Web and Mobile Application Vulnerabilities
Bojan Zdrnja, Senior Internet Storm Center Handler
In this presentation, Bojan Zdrnja, CTO of the Croatian information security company INFIGO IS, will go through some not-so-common but still devastating web and mobile application vulnerabilities. Bojan’s team performs almost 200 application penetration tests per year and finds a lot of critical vulnerabilities that are often overlooked not only by developers, but also by penetration testers. We will not cover the common vulnerabilities such as XSS and SQL injection that everyone should (but don’t always) know about, but will instead turn to less commonly known vulnerabilities and attack vectors on both web and mobile applications. It does not matter if you are on the red, blue, or purple team – details about discussed vulnerabilities will help improve your application security knowledge.

Hacking the SRUM and Other Devious New Ways to Interrogate Windows
Alissa Torres
Data is king! With increasing granularity, Windows 10+ tracks user, application and network activity, geolocation and power consumption. Operating System (OS) monitoring is now in hyperdrive, with modern performance and usability features fueled by metrics-laden databases and log files. The forensic implications of this level of OS endpoint monitoring are broad-reaching. Yet, put on your red-team armband and consider the gold an attacker can unearth from these same data sources. This talk exposes the newest and most data-rich endpoint artifacts (SRUM, Windows.edb, ActivitiesCache.db, Clipboard History, etc) and the tools available for remote collection and parsing.
Examining the Case of Coalfire Penetration Testers Charged with Criminal Trespass
Benjamin Wright

Coalfire had a contract to do penetration testing for the Iowa State Court Administration. When two Coalfire penetration testers broke into a rural county courthouse, the sheriff arrested them. The county attorney charged them with criminal trespass! Come participate in a legal discussion of this “arresting” story.

Cloud Security Attacks and Defenses: Cybersecurity 101?
Frank Kim

Join us for a walk through of the Capital One breach. We will demonstrate how the attacker compromised Amazon Web Services virtual machine credentials, gained access to privileged resources, and exfiltrated data from the account. The conversation will then shift to a post-mortem discussion about cloud security controls that could have prevented or limited the blast radius of the attack.

Virtuous Cycles: Rethinking the SOC for Long-term Success
John Hubbard

Many Security Operations Centers (SOCs) have a burnout problem that leads to negativity and constant turnover. With the increasing cybersecurity talent shortage, keeping the people we have will only become increasingly important. The problem is that “Tier 1” and other SOC roles seem destined to burn people out. So, what do we do? While the field of psychology understands the factors that cause burnout, many SOCs do not take the time to do the research and create an environment to fight it. Though meticulously defined process and tiering may be the norm, does it lead to sacrificing quality in the long term? Using science-backed research on intrinsic motivation and studies on SOC burnout factors, this talk makes the case that it’s time to reconsider how we structure SOCs in order to create long-term success, that benefits both the individual and the organization.

The CIS Critical Controls – Security Basics (with PowerShell) on a Zero Dollar Budget
Rob Vandenbrink, SANS Internet Storm Center Handler

The CIS Critical Controls are recognized as a good start in setting up a defensible infrastructure. They are platform/OS agnostic, aren’t driven by vendor agendas, and are very much community and volunteer driven. In this talk, we’ll discuss a typical organization that we’d see in many security engagements. We’ll discuss the various Critical Controls and how implementing them might look specifically for our example company’s blue team. Most of the defenses that we’ll be discussing will be implemented using PowerShell scripts (all of which will be posted and freely available). For each of the Controls, we’ll discuss the typical attacks that these actions head off – either “in the wild” attacks or attacks in a pen test setting, along with how the defense works. We’ll discuss the tech, the politics, implementation issues, and why these controls are so important. As always, be prepared for lots of live demos of how the Controls work in a real company. Come out for some blue team goodness! Defend all the things!

Neutralized Incident and the Materialized Incident
To Know or Not to Know: The Difference Between the Neutralized Incident and the Materialized Incident
Manuel Humberto Santander Pelaez, SANS Internet Storm Center Handler

It is common to see a lot of cyber attacks daily. We clearly know that the question within our company is or whether not we will be attacked, but when will we be attacked. The market currently shows a high mean time to detect (MTTD) and high mean time to respond (MTTR), which ultimately increases the impact of cyber risk to the business. Are we aware of the unknown risks? Can we identify them before they materialize? Can we detect an attacker in the early stages of the cyber kill chain before the attacker successfully performs the action on the targets? Join Manuel to learn how to generate cyber threat intelligence products by generating indicators of compromise of anomalies detected in the network through the use of open-source tools and machine learning algorithms.

Catch and Release: Phishing Techniques for the Good Guys
Jan Kopriva, SANS Internet Storm Center Handler

Since e-mail is the most common attack vector used by attackers, knowledge of effective phishing techniques is indispensable for penetration testers, red teamers, and security professionals as well. In this presentation we will go over the most effective phishing techniques used by attackers today and the methods to defeat them. We will also take a look at techniques and tricks not yet used in the wild, which will allow us to get our messages past anti-phishing and anti-malware scans of e-mail security gateways.

Coffee & Donuts with the College Students
Join us for coffee, donuts, and conversation with SANS Technology Institute staff and students. Learn about SANS’ regionally accredited master’s degree and graduate certificate programs for InfoSec professionals and its undergraduate certificate program for people who want to launch a career in cybersecurity. Find out if the class you’re taking this week or GIAC certifications you’ve earned may be applied towards a graduate or undergraduate program. Visit www.sans.edu for complete information on curriculum, admissions, and funding options.
SIEMtervention: Moving SIEM from Collection to Detection
Justin Henderson
Commercial off-the-shelf products are rarely the majestic unicorn the vendor makes them out to be. As security professionals, we all have our fair share of complaints about the SIEM we invested in and the functionality promised. But what if we told you that with actionable dashboards, log enrichment, and tactical analytics, we can save your frustration and give added value to your investment?

Moving Past Just Googling It: Harvesting and Using OSINT
Micah Hoffman
Every day we search for things on the Internet. Defenders research a domain or IP that contains malware. Attackers look for email addresses for an upcoming phishing campaign. DFIR people examine locations and usernames that they acquired from a subject’s computer. Policy and compliance people examine the risk that employees in their organizations might bring to work. Recruiters scour the Internet looking for candidates. And normal people shop, date, geolocate, post, tweet, and otherwise send a huge amount of data to the public Internet. Come join Micah Hoffman as we examine how open-source intelligence (OSINT) can reveal interesting content about your work and personal lives.

Kerberos And Attacks 101
Tim Medin
Want to understand how Kerberos works? Would you like to understand modern Kerberos attacks? If so, then join Tim Medin as he walks you through how to attack Kerberos with ticket attacks and Kerberoasting. We will cover the basics of Kerberos authentication and then show you how the trust model can be exploited for persistence, pivoting, and privilege escalation.

A Walk Through Logs Hell
Xavier Mertens, Internet Storm Center Handler
Once upon a time, an ogre called “SIEM” was invented...
Today, if your organization does not have a SIEM, you look like the “Little Tom Thumb” among your peers. During InfoSec meetups, many people like to brag about the power of the monster they deployed: “We can ingest 5K events per second!” or “We index 3TB a day!” That may seem impressive, but that is not necessarily the case. Are you sure that you can still find the needle from a haystack? Being involved with such technologies and environments for a while, we’ve had the opportunity to face many situations where the ogre SIEM was not able to return interesting data due to misconfigurations, topology changes, lack (or absence) of logs, wrong normalization and many other issues. Managing logs and events is not an easy job. During this presentation, we’ll describe nightmare stories that you could also face in your organization. And, of course, we’ll provide some ideas to prevent them.

Modern Information Security: Forget Cyber, It’s All About AppSec
Adrien de Beaupre
This discussion will focus on how modern information security has evolved and what we will need to move into the 21st century. We need a new paradigm in security with a workforce that understands application security, which is the new frontier.

The Hacker’s Apprentice
Mark Baggett
Mark Baggett has built an escape room in his house! In this presentation, Mark will describe how he used Python, smart-home Internet of Things devices, and a few puzzles to build it. And he’ll show how you too can install some pretty cool automation in your home, even without a lot of smart home devices.
## Future Events

### SANS Training Events

<table>
<thead>
<tr>
<th>Location</th>
<th>City, State</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>St. Louis</td>
<td>St. Louis, MO</td>
<td>Mar 8-13</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas, TX</td>
<td>Mar 9-14</td>
</tr>
<tr>
<td>Norfolk</td>
<td>Norfolk, VA</td>
<td>Mar 16-21</td>
</tr>
<tr>
<td>San Francisco</td>
<td>San Francisco, CA</td>
<td>Mar 16-27</td>
</tr>
<tr>
<td>Seattle</td>
<td>Seattle, WA</td>
<td>Mar 23-28</td>
</tr>
<tr>
<td>Philadelphia</td>
<td>Philadelphia, PA</td>
<td>Mar 30 – Apr 4</td>
</tr>
</tbody>
</table>

### SANS 2020

<table>
<thead>
<tr>
<th>Location</th>
<th>City, State</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bethesda</td>
<td>Bethesda, MD</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Minneapolis</td>
<td>Minneapolis, MN</td>
<td>Apr 14-19</td>
</tr>
<tr>
<td>Boston Spring</td>
<td>Boston, MA</td>
<td>Apr 20-25</td>
</tr>
<tr>
<td>Pen Test Austin</td>
<td>Austin, TX</td>
<td>Apr 27 – May 2</td>
</tr>
<tr>
<td>Baltimore Spring</td>
<td>Baltimore, MD</td>
<td>Apr 27 – May 2</td>
</tr>
</tbody>
</table>

### Security West

<table>
<thead>
<tr>
<th>Location</th>
<th>City, State</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>N. VA – Alexandria</td>
<td>Alexandria, VA</td>
<td>May 17-22</td>
</tr>
<tr>
<td>San Antonio</td>
<td>San Antonio, TX</td>
<td>May 17-22</td>
</tr>
<tr>
<td>Atlanta Spring</td>
<td>Atlanta, GA</td>
<td>May 26-31</td>
</tr>
<tr>
<td>Nashville Spring</td>
<td>Nashville TN</td>
<td>May 26-31</td>
</tr>
<tr>
<td>Chicago Spring</td>
<td>Chicago IL</td>
<td>Jun 1-6</td>
</tr>
<tr>
<td>New Orleans</td>
<td>New Orleans LA</td>
<td>Jun 8-13</td>
</tr>
<tr>
<td>Las Vegas</td>
<td>Las Vegas NV</td>
<td>Jun 8-13</td>
</tr>
</tbody>
</table>

### SANS Summit Events

<table>
<thead>
<tr>
<th>Event</th>
<th>City, State</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Security</td>
<td>Dallas, TX</td>
<td>May 27 – Jun 3</td>
</tr>
<tr>
<td>Rocky Mountain HackFest</td>
<td>Denver CO</td>
<td>Jun 1-8</td>
</tr>
<tr>
<td>DFIR</td>
<td>Austin TX</td>
<td>Jul 16-23</td>
</tr>
</tbody>
</table>

### Community SANS Events

Local, single-course events are also offered throughout the year via SANS Community. Visit sans.org/community for up-to-date Community course information.

---

### Take SANS Training Anytime, Anywhere with SANS OnDemand

More than 45 of the most popular SANS courses are available in our online training format OnDemand with no travel required. All OnDemand courses 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

Visit www.sans.org/ondemand to learn more about your OnDemand training options.
Hotel Information

Washington Marriott Wardman Park
2660 Woodley Road, NW  |  Washington, DC  20008
202-328-2000
sans.org/sansfire/location

When you arrive at the Washington Marriott Wardman Park, you’ll find a charming neighborhood in the heart of Washington, DC filled with amazing restaurants and quaint shops. With a Metro stop just outside the doors and area airports close by, it’s a premier city destination just two Metro stops from everything DC has to offer.

Top three reasons to stay at the Washington Marriott Wardman Park
1. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
2. By staying at the Washington Marriott Wardman Park, 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 Washington Marriott Wardman Park that you won’t want to miss!

Special Hotel Rates Available

A special discounted rate of $219 S/D plus applicable taxes will be honored based on space availability.

The SANSFIRE 2020 group rate is less than the prevailing government per diem rate in Washington, D.C. for June 2020. No identification will be required to secure a room in the group block at or below the per diem rate. All rates include high-speed Internet in your room and are only available through May 21, 2020.

Registration Information

Register online at sans.org/sansfire

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 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.

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 pay for GIAC certification exams. Contact SANS for more detailed information about our Voucher Program: sans.org/vouchers

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 May 27, 2020. 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.

Pay Early and Save*

Use code EarlyBird20 when registering early

<table>
<thead>
<tr>
<th>Date</th>
<th>Discount</th>
<th>Date</th>
<th>Discount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 22</td>
<td>$300</td>
<td>May 13</td>
<td>$150</td>
</tr>
</tbody>
</table>

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

SANS SIMULCAST

Live stream content directly from the classroom and interact with peers and in-class moderators. Simulcast includes four months of access to your course recordings and labs, and unlimited subject-matter-expert support. Visit sans.org/sansfire/attend-remotely for more details.
### Courses – 5-6 Days

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Dates</th>
<th>Fee</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
<th>Add NetWars Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC401</td>
<td>Introduction to Cyber Security</td>
<td></td>
<td>$5,790</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC402</td>
<td>Security Essentials Bootcamp Style</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC450</td>
<td>Blue Team Fundamentals: Security Operations and Analysis</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC460</td>
<td>Enterprise Threat and Vulnerability Assessment</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC487</td>
<td>Open-Source Intelligence (OSINT) Gathering and Analysis</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC501</td>
<td>Advanced Security Essentials – Enterprise Defender</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC503</td>
<td>Intrusion Detection In-Depth</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC504</td>
<td>Hacker Tools, Techniques, Incidents, and Incident Handling</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC505</td>
<td>Securing Windows and PowerShell Automation</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC506</td>
<td>Securing Linux/Unix</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC511</td>
<td>Continuous Monitoring and Security Operations</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC530</td>
<td>Defensible Security Architecture and Engineering</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC540</td>
<td>Cloud Security and DevOps Automation</td>
<td></td>
<td>$6,300</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC545</td>
<td>Cloud Security Architecture and Operations</td>
<td></td>
<td>$5,790</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC555</td>
<td>SIEM with Tactical Analytics</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC560</td>
<td>Network Penetration Testing and Ethical Hacking</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC566</td>
<td>Implementing and Auditing the Critical Security Controls – In-Depth</td>
<td></td>
<td>$5,790</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC573</td>
<td>Automating Information Security with Python</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC599</td>
<td>Defeating Advanced Adversaries – Purple Team Tactics &amp; Kill Chain Defenses</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC617</td>
<td>Wireless Penetration Testing and Ethical Hacking</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC642</td>
<td>Adv. Web App Pen Testing, Ethical Hacking &amp; Exploitation Techniques</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC660</td>
<td>Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>SEC760</td>
<td>Advanced Exploit Development for Penetration Testers</td>
<td></td>
<td>$7,320</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>TBT570</td>
<td>Team-Based Training - Blue Team and Red Team Dynamic Workshop</td>
<td></td>
<td>$7,310</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR498</td>
<td>Battlefield Forensics &amp; Data Acquisition</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR500</td>
<td>Windows Forensic Analysis</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR508</td>
<td>Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR526</td>
<td>Advanced Memory Forensics &amp; Threat Detection</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR527</td>
<td>Advanced Network Forensics: Threat Hunting, Analysis &amp; Incident Response</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR578</td>
<td>Cyber Threat Intelligence</td>
<td></td>
<td>$5,790</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR585</td>
<td>Smartphone Forensic Analysis In-Depth</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>FOR610</td>
<td>Reverse-Engineering Malware:Malware Analysis Tools and Techniques</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT414</td>
<td>SANS Training Program for CISSP® Certification</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT512</td>
<td>Security Leadership Essentials for Managers</td>
<td></td>
<td>$6,300</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>MGT514</td>
<td>Security Strategic Planning, Policy, and Leadership</td>
<td></td>
<td>$6,300</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>LEG523</td>
<td>Law of Data Security and Investigations</td>
<td></td>
<td>$5,790</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
<tr>
<td>ICS410</td>
<td>ICS/SCADA Security Essentials</td>
<td></td>
<td>$6,720</td>
<td>$799</td>
<td>$799</td>
<td>$1,420</td>
</tr>
</tbody>
</table>

### Skill-Based Short Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Fee</th>
<th>Add GIAC Cert</th>
<th>Add OnDemand</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC440</td>
<td>Critical Security Controls: Planning, Implementing, and Auditing</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>SEC455</td>
<td>SIEM Design &amp; Implementation</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>SEC534</td>
<td>Secure DevOps: A Practical Introduction</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>SEC564</td>
<td>Red Team Exercises &amp; Adversary Emulation</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>SEC580</td>
<td>Metasploit Kung Fu for Enterprise Pen Testing</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>MGT415</td>
<td>A Practical Introduction to Cyber Security Risk Management</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>MGT433</td>
<td>SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>MGT521</td>
<td>Driving Cybersecurity Change – Establishing a Culture of Protect, Detect and Respond</td>
<td>$2,100</td>
<td>$315</td>
<td></td>
</tr>
<tr>
<td>HOSTED</td>
<td>Successful InfoSec Consulting</td>
<td>FREE</td>
<td>$1,795</td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Core NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>Cyber Defense NetWars Tournament – Tournament Entrance Fee</td>
<td>FREE</td>
<td>$1,795</td>
<td></td>
</tr>
<tr>
<td>SPECIAL</td>
<td>DFIR NetWars Tournament – Tournament Entrance Fee</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EARLY BIRD DISCOUNTS**

Pay for any long course using the code **EarlyBird20** at checkout by April 22nd to get $300 OFF or by May 13th to get $150 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 sans.org/join

**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.

**@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.

**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.

**WhatWorks Webcasts**
SANS WhatWorks webcasts feature powerful customer experiences in resolving specific IT security issues.

**Tool Talks**
Tool Talks demonstrate how commercial tools can be used to solve or mitigate IT security problems.

**Course Demos**
Test drive more than 40 SANS courses and decide which is right for you. Our demos are delivered via the SANS OnDemand platform, and give you a close look at a course’s contents, pace, and features. sans.org/demo

**Other Free Resources** (SANS.org account is not 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)

**SAVE $300** Register and pay by April 22nd
Use code EarlyBird20

sans.org/sansfire

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

NALT-BRO-SANSFIRE20