SEC560: Network Penetration Testing and Ethical Hacking

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

The Must-Have Course for Every Well-Rounded Security Professional

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. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job masterfully, safely, and efficiently.

Learn the Best Ways to Test Your Own Systems Before the Bad Guys Attack

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.

Equipping Security Organizations with Comprehensive Penetration Testing and Ethical Hacking Know-How

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. We won't just cover run-of-the-mill options and configurations, we'll also go over less-well-known-but-super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post exploitation, password attacks, wireless, 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. The final portion of the class includes a comprehensive hands-on lab, conducting a full-day penetration test against a target organization.

giac.org

sans.org/cyber-guardian

sans.edu

"SANS is really the only information security training available and is therefore valuable on its own. The wide subject areas, relating to pen-testing, are what makes SEC560 particularly valuable."
-Nicholas Capalbo, Federal Reserve of New York

Who Should Attend

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

You Will Be Able To

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined, and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize a scanning tool such as Nmap to conduct comprehensive network sweeps, port scans, OS fingerprinting, and version scanning to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Configure and launch a vulnerability scanner such as Nessus so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using connection-making tools such as Netcat and packet crafting tools such as Scapy
- Utilize the Windows and Linux command 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

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

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

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

560.2 HANDS ON: In-Depth Scanning

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

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

560.3 HANDS ON: Exploitation and Post-Exploitation

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

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

560.4 HANDS ON: Password Attacks & Merciless Pivoting

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

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

560.5 HANDS ON: Wireless and Web Apps Penetration Testing

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

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

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

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

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

SEC560 COIN

SEC560 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

Summit
sans.org/summit

Community SANS
sans.org/community

Mentor Program
sans.org/mentor

OnSite
sans.org/onsite

vLive
sans.org/vlive

Simulcast
sans.org/simulcast

OnDemand
sans.org/ondemand

SelStudy
sans.org/selfstudy