SEC560: Enterprise Penetration Testing

Course Overview

As a cybersecurity professional, you have a unique responsibility to identify and understand your organization s vulnerabilities and work diligently to mitigate them before the bad actors pounce. Are you ready? SEC560, the flagship SANS course for penetration testing, fully equips you to take this task head-on.

In SEC560, you will learn how to plan, prepare, and execute a penetration test in a modern enterprise. Using the latest penetration testing tools, you will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice your skills. You'll then be able to take what you've learned in this course back to your office and apply it immediately.

This course is designed to strengthen penetration testers and further add to their skillset. The course is also designed to train system administrators, defenders, and others in security to understand the mindset and methodology of a modern attacker. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. Both the offensive teams and defenders have the same goal: keep the real bad guys out.

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

Job Roles

- Security Control Assessor
- System Testing and Evaluation Specialist
- Vulnerability Assessment Analyst
- Pen Tester
- Exploitation Analyst
- Mission Assessment Specialist
- Target Developer
- Cyber Ops Planner

Intended Audience

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

Duration

6 Days

Certifications

GPEN

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

SEC560: Enterprise Penetration Testing

APPLIED TECHNOLOGY ACADEMY

Course Outline

SECTION 1: Comprehensive Pen Test Planning, Scoping, and Recon

TOPICS: The Mindset of the Professional Pen Tester; Building a World-Class Pen Test Infrastructure; Creating Effective Pen Test Scopes and Rules of Engagement; Detailed Recon Using the Latest Tools; Mining Search Engine Results; Reconnaissance of the Target Organization, Infrastructure, and Users; Automating Reconnaissance with Spiderfoot

SECTION 2: In-Depth Scanning and Initial Access

TOPICS: Tips for Awesome Scanning; Nmap In-Depth: The Nmap Scripting Engine; Version Scanning with Nmap; False-Positive Reduction; Netcat for the Pen Tester; Gaining Initial Access; Password Guessing, Spraying, and Credential Stuffing; Exploitation and Exploit Categories; Exploiting Network Services and Leveraging Meterpreter

SECTION 3: Assumed Breach, Post-Exploitation, and Passwords

TOPICS: Assumed Breach Testing; Post-Exploitation; Situational Awareness on Linux and Windows; GhostPack s Seatbelt; Password Attack Tips; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi; Effective Password Cracking with John the Ripper and Hashcat; Poisoning Multicast Name Resolution with Responder

SECTION 4: Lateral Movement and Command & Control (C2)

TOPICS: Lateral Movement; Running Commands Remotely; Attacking and Abusing Network Protocols with Impacket; Command and Control (C2) Frameworks and Selecting the One for You; Using the Adversary Emulation and Red Team Framework, Sliver; Post-Exploitation with [PowerShell] Empire; Anti-Virus and Evasion of Defensive Tools; Application Control Bypasses Using Built-In Windows Features; Implementing Port Forwarding Relays via SSH for Merciless Pivots; Pivoting through Target Environments with C2

SECTION 5: Domain Domination and Azure Annihilation

TOPICS: Kerberos Authentication Protocol; Kerberoasting for Domain Privilege Escalation and Credential Compromise; Persistent Administrative Domain Access; Obtaining NTDS.dit and Extracting Domain Hashes; Golden and Silver Ticket Attacks for Persistence; Additional Kerberos Attacks including Skeleton Key, Over-Pass-the-Hash, and Pass-the-Ticket; Effective Domain Privilege Escalation; Azure and Azure AD Reconnaissance; Azure Password Attacks and Spraying; Understanding Azure Permissions; Running Commands on Azure Hosts; Tunneling with Ngrok; Lateral Movement in Azure; Effective Reporting and Business Communication

SECTION 6: Penetration Test and Capture-the-Flag Exercise

TOPICS: Applying Penetration Testing and Ethical Hacking Practices End-to-End; Detailed Scanning to Find Vulnerabilities and Avenues to Entry; Exploitation to Gain Control of Target Systems; Post-Exploitation to Determine Business Risk; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise

Course Objectives

- Properly plan and prepare for an enterprise penetration test
- Perform detailed reconnaissance to aid in social engineering, phishing, and making well-informed attack decisions
- Scan target networks using best-of-breed tools to identify systems and targets that other tools and techniques may have missed
- Perform safe and effective password guessing to gain initial access to the target environment, or to move deeper into the network
- Exploit target systems in multiple ways to gain access and measure real business risk
- Execute extensive post-exploitation to move further into the network
- Use Privilege Escalation techniques to elevate access on Windows or Linux systems, or even the Microsoft Windows Domain
- Perform internal reconnaissance and situational awareness tasks to identify additional targets and attack paths
- Execute lateral movement and pivoting to further extend access to the organization and identify risks missed by surface scans
- Crack passwords using modern tools and techniques to extend or escalate access
- Use multiple Command and Control (C2, C&C) frameworks to manage and pillage compromised hosts
- Attack the Microsoft Windows domain used by most organizations
- Execute multiple Kerberos attacks, including Kerberoasting, Golden Ticket, and Silver Ticket attacks
- Conduct Azure reconnaissance
- Azure AD password spraying attacks
- Execute commands in Azure using compromised credentials
- Develop and deliver high-quality reports

GIAC Penetration Tester (GPEN)

The GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies. GPEN certification holders have the knowledge and skills to conduct exploits and engage in detailed reconnaissance, as well as utilize a process-oriented approach to penetration testing projects.

- Comprehensive Pen Test Planning, Scoping, and Recon
- In-Depth Scanning and Exploitation, Post-Exploitation, and Pivoting
- In-Depth Password Attacks and Web App Pen Testing