SEC560: **Enterprise Penetration Testing**

GPEN
Penetration Tester
giac.org/gpen

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- 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

GPEN
Penetration Tester
giac.org/gpen

GIAC Penetration Tester

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

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.

Author Statement

"All security professionals need to understand modern attack tactics and principles. As a defender, incident responder, or forensic analyst, it is important to understand the latest attacks and the mindset of the attacker. In this course, penetration testers, red teamers, and other offensive security professionals will learn tools and techniques to increase the impact and effectiveness of their work. As the lead author for this course, I'm proud to bring my years of security experience (both offensive and defensive) as well as network/system administration experience to the course. We aim to provide a valuable, high-impact penetration testing course designed to teach experienced pen testers new tips, help prepare new penetration testers, and provide background to anyone dealing with penetration testers, Red Teams, or even malicious attackers. I personally enjoy teaching this course and sharing my experience and real-life examples with you."
—Tim Medin

"I think if you genuinely want to learn how exploitation techniques work and how to properly think like a hacker, it would be silly not to attend SEC560."

—Marc Hamilton, **McAfee**

Section Descriptions

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

In this course section, you'll develop the skills needed to conduct a best-of-breed, high-value penetration test. We'll go in-depth on how to build a penetration testing infrastructure that includes all the hardware, software, network infrastructure, and tools you will need to conduct great penetration tests, with specific low-cost recommendations for your arsenal. We'll then cover formulating a pen test scope and rules of engagement that will set you up for success, including a role-play exercise. We'll also dig deep into the reconnaissance portion of a penetration test, covering the latest tools and techniques, including hands-on lab exercises to learn about a target environment, as well as a lab using Spiderfoot to automate the discovery of information about the target organization, network, infrastructure, and users.

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

This course section focuses on the vital task of mapping the target environment s attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities. We look at some of the most useful scanning tools freely available today and run them in numerous hands-on labs to help hammer home the most effective way to use each tool. We ll cover vital techniques for false-positive reduction so that you can focus your findings on meaningful results and avoid the sting of a false positive. And we ll examine the best ways to conduct your scans safely and efficiently. The section includes password guessing attacks, which are a common way for penetration testers and malicious attackers to gain initial access and pivot through the network. This action-packed section concludes with another common way to gain initial access: exploitation. We ll discuss many ways that exploits are used to gain access or escalate privileges, then examine how these exploits are packaged in frameworks like Metasploit and its mighty Meterpreter. You ll learn in-depth how to leverage Metasploit and Meterpreter to compromise target environments.

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

Who Should Attend

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

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

Once you've successfully exploited a target environment, penetration testing gets extra exciting as you perform post-exploitation, gathering information from compromised machines and pivoting to other systems in your scope. In this section we'll discuss a common modern penetration test style, the Assumed Breach, where initial access is ceded to the testers for speed and efficiency. Whether the testers gain access themselves or access is provided, the testers now identify risks that are not visible on the surface. You'll learn tools and techniques to perform privilege escalation attacks to gain elevated access on compromised hosts. Part of post-exploitation includes password dumping, and we 'll perform cleartext password extraction with Mimikatz, and password cracking. You'll learn modern tools and techniques to perform better cracking attacks that will extend or upgrade your access in the target environment.

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 and Control (C2)

This course sections zooms in on moving through the target environment. When attackers gain access to a network, they move, so you'll learn the same techniques used by modern attackers and penetration testers. You ll start by manually executing the techniques used for lateral movement, then move on to automation using a powerful toolset, Impacket, to exploit and abuse network protocols. We'll examine Windows network authentication, and you'll perform a pass-the-hash attack to move through the network without knowing the compromised accout'ss password. We'll examine C2 frameworks and use two widely known ones, [PowerShell] Empire and Sliver; discuss methods of evasion and application control bypasses; and use our access on one system as a pivot to access another system that is not directly from our attacker system.

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

This course section will zoom in on typical Active Directory (AD) lateral movement strategies. You'll gain an in-depth understanding of how Kerberos works and what the possible attack vectors are, including Kerberoasting, Golden Ticket, and Silver Ticket attacks. You'll use credentials found during the penetration test of the target environment to extract all the hashes from a compromised Domain Controller. With full privileges over the on-premise domain, we'll then turn our attention to the cloud and have a look at Azure principles and attack strategies. The integration of Azure AD with the on-premise domain provides interesting attack options, which will be linked to the domain dominance attacks we saw earlier during the course section. We'll wrap up with a discussion on effective reporting and communication with the business.

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

This lively session represents the culmination of the network penetration testing and ethical hacking course. You'll apply all of the skills mastered in the course in a comprehensive, hands-on exercise during which you'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work to achieve your goal to determine whether the target organization's Personally Identifiable Information is at risk. As a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

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