SEC560: **Enterprise Penetration Testing™**

GPEN
Penetration Tester
giac.org/gpen

6 Day Program | 38 CPEs | Laptop Required

You Will Be Able To

- Conduct comprehensive reconnaissance using OSINT techniques, DNS enumeration, breach data analysis, and infrastructure mapping to identify attack surfaces and gather intelligence on target organizations
- Exploit authentication weaknesses through credential stuffing, password spraying, and hash-based attacks against both on-premises and Azure/Entra ID environments
- Perform post-exploitation activities including credential harvesting with Mimikatz, establishing command and control with Sliver and Metasploit, and escalating privileges on Windows and Linux systems
- Execute Active Directory attacks including Kerberoasting, BloodHound attack path analysis, and Active Directory Certificate Services exploitation to achieve domain privilege escalation
- Move laterally through enterprise networks using pass-the-hash, Impacket, SSH tunneling, and C2 pivoting techniques to reach high-value targets across network boundaries
- Maintain persistent access through registry modifications, scheduled tasks, services, and WMI while evading modern defenses including AMSI, AV/EDR detection, and application control solutions
- Achieve domain dominance through DCSync, skeleton keys, golden tickets, silver tickets, and exploit Azure RBAC permissions and managed identities in cloud environments

"SEC560 introduces the whole process of penetration testing from the start of engagement to the end."

—Barry Tsang, **Deloitte**

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

SEC560 training teaches students how to conduct comprehensive enterprise penetration tests that mirror real-world attacks. Starting with reconnaissance and scanning, students progress through gaining initial access, post-exploitation, privilege escalation, lateral movement, and maintaining persistence while evading detection. This course emphasizes practical, hands-on techniques using industry-standard tools including Nmap, Metasploit, Sliver, BloodHound, Impacket, and Mimikatz. Students learn both on-premises Active Directory attacks and cloud-based Azure/Entra ID exploitation. Each section includes multiple labs reinforcing concepts through realistic scenarios against purpose-built vulnerable environments. The course culminates in a Capture-the-Flag competition where students apply all learned techniques across multiple-target networks, demonstrating mastery of the complete penetration testing lifecycle from initial foothold through domain dominance.

Business Takeaways

- Validate security controls by conducting realistic penetration tests that identify exploitable vulnerabilities before malicious attackers discover them
- Understand actual attacker techniques and tactics to prioritize security investments based on real-world threat scenarios rather than theoretical risks
- Assess multi-factor authentication implementation to identify single-factor authentication services that represent high-risk entry points into enterprise environments
- Evaluate Active Directory security posture by identifying privilege escalation paths, certificate services misconfigurations, and Kerberos authentication vulnerabilities
- Test detection and response capabilities by measuring how quickly security teams identify and respond to post-exploitation activities and lateral movement
- Meet compliance requirements and demonstrate due diligence by conducting regular penetration tests that document security posture improvements over time
- Develop internal penetration testing capabilities that reduce dependence on external consultants while building organizational security expertise

Authors Statement

"SEC560 represents decades of combined penetration testing experience from its author team. We've designed this course to bridge the gap between theoretical security knowledge and practical penetration testing skills. Every technique taught has been validated through real-world engagements, and the labs reflect actual vulnerabilities and misconfigurations we encounter in enterprise environments. Our goal is not just to teach you how to use tools, but to develop your penetration testing mindset—the ability to identify attack paths, chain vulnerabilities, and think creatively while maintaining ethical boundaries. By the end of this course, you'll have the practical skills and confidence to conduct professional penetration tests that provide real value to organizations seeking to improve their security posture."
—Jeff McJunkin & Jon Gorenflo

Section Descriptions

SECTION 1: Miniature Engagement, Recon, and Scanning

Section 1 opens by demonstrating a complete credential stuffing attack, establishing the penetration testing mindset and terminology, then covers building testing infrastructure, Linux fundamentals, and the pre-engagement process including scope, Rules of Engagement, and documented permission. This section covers the reconnaissance phase in detail, using OSINT to gather intelligence on organizations, infrastructure, employees, and breached credentials. Section 1 concludes with scanning, covering TCP and UDP protocols and the tools professional penetration testers need to master—Masscan for fast port discovery and Nmap for comprehensive enumeration—to find target networks, active hosts, ports, and services.

TOPICS: Penetration Testing Frameworks and Methodology; Infrastructure Setup and Linux Essentials; Pre-engagement and Rules of Engagement; OSINT and Reconnaissance Techniques; Port Scanning with Masscan and Nmap

SECTION 2: Scanning and Initial Access

Section 2 continues scanning coverage with Nmap's advanced capabilities including version detection, operating system fingerprinting, and the Nmap Scripting Engine for vulnerability detection and service enumeration. This section addresses the critical initial access phase through multiple attack vectors, covering password guessing attacks against SMB and SSH, comprehensive Azure and Entra ID reconnaissance and password spraying, network-based attacks using Responder to capture and relay authentication, and exploitation frameworks including Metasploit and Meterpreter for deploying payloads and establishing command and control on compromised systems.

TOPICS: Nmap Version and OS Detection; Nmap Scripting Engine and Vulnerability Scanning; Password Guessing and Spraying Attacks; Azure and Entra ID Reconnaissance; Network Protocol Attacks with Responder; Exploitation with Metasploit Framework

SECTION 3: Post-Exploitation

Section 3 addresses critical post-exploitation activities performed after gaining initial access. Students learn password and credential access techniques including password representations, obtaining password hashes from Windows systems using Metasploit and Mimikatz, and offline password cracking with Hashcat. The section covers modern command and control using the Sliver C2 framework, payload generation and delivery including evasion techniques, and comprehensive situational awareness for both Linux and Windows systems using tools like Seatbelt. Section 3 concludes with Windows privilege escalation techniques that identify and exploit misconfigurations to escalate from standard user to administrative access.

TOPICS: Credential Harvesting and Password Dumping; Offline Password Cracking with Hashcat; Command and Control with Sliver; Payload Generation and Delivery; Windows and Linux Situational Awareness; Windows Privilege Escalation Techniques

SECTION 4: Post-Exploitation

Section 4 covers Kerberos authentication fundamentals and exploiting it through Kerberoasting attacks to crack service account passwords offline. Students use BloodHound for graph-based attack path analysis and exploit Active Directory Certificate Services misconfigurations (ESC1, ESC4, ESC8) to achieve domain privilege escalation. This section covers lateral movement techniques from both Windows and Linux platforms, including native tools, SSH tunneling, and the Impacket toolkit for authenticated remote execution. Section 4 concludes with Pass-the-Hash attacks for credential reuse and pivoting techniques using Metasploit and C2 frameworks to reach systems across network boundaries.

TOPICS: CKerberos Authentication and Kerberoasting; BloodHound for Attack Path Analysis; Active Directory Certificate Services Exploitation; Lateral Movement from Windows and Linux; Impacket Toolkit Usage; Pass-the-Hash and Pivoting Techniques

SECTION 5: Persistence and Evading Controls

Section 5 covers persistence mechanisms including registry keys, scheduled tasks, services, and WMI event consumers to maintain access through reboots, then addresses evading modern defenses by bypassing AMSI, AV/EDR detection, and application controls like AppLocker using techniques such as MSBuild abuse. This section includes effective penetration testing reporting practices before diving into advanced Active Directory attacks—Pass-the-Ticket, Overpass-the-Hash, and achieving domain dominance through DCSync, skeleton keys, and NTDS.dit extraction. Section 5 concludes with Golden and Silver ticket forgery for ultimate domain control, OpenID authentication exploitation, and transitions to cloud security by covering Azure/Entra ID authentication mechanisms, infrastructure, command execution on Azure VMs, and exploiting Azure RBAC permissions and managed identities.

TOPICS: Persistence Mechanisms and Techniques; Bypassing AMSI, AV/EDR, and Application Controls; Penetration Testing Reporting Best Practices; Advanced Kerberos and Domain Dominance Attacks; Golden and Silver Ticket Forgery; Azure Infrastructure and RBAC Exploitation

SECTION 6: Capture the Flag and Next Steps

Section 6 provides hands-on application of all skills learned throughout the course in a team-based Capture-the-Flag (CTF) competition across multiple target networks. After the CTF, this section guides students on next steps for continuing their penetration testing journey, including cloud penetration testing resources, GIAC GPEN exam preparation strategy, building effective home labs for ongoing practice, and advanced training environments like Game of Active Directory that provide documented exploit paths for mastering Active Directory attacks.

TOPICS: Capture-the-Flag Competition; Cloud Penetration Testing Resources; GIAC GPEN Exam Preparation; Building Home Lab Environments; Advanced Training and Practice

Who Should Attend

SEC560 is designed for security professionals who need to conduct penetration tests or assess their organization's security posture:

- Penetration testers and ethical hackers
- Security analysts and engineers
- IT professionals transitioning to offensive security roles
- Red team operators
- Security consultants performing network assessments
- System administrators responsible for hardening enterprise environments
- Incident responders seeking to understand attacker techniques
- Security architects designing defensive controls
- Compliance auditors requiring technical security validation

NICE Framework Work Roles

- Security Control Assessor (OPM 612)
- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Exploitation Analyst (OPM 121)
- Mission Assessment Specialist (OPM 112)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)

"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**