# SEC560: Network Penetration Testing and Ethical Hacking

**GPEN**
Penetration Tester
giac.org/gpen

6 Day Program | 36 CPEs | Laptop Required

## You Will Be Able To

- Apply a detailed, four-step methodology to your web application penetration tests: reconnaissance, mapping, discovery, and exploitation
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives
- Manually discover key web application flaws
- Use Python to create testing and exploitation scripts during a penetration test
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization
- Create configurations and test payloads within other web attacks
- Fuzz potential inputs for injection attacks
- Explain the impact of exploitation of web application flaws
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application
- Perform a complete web penetration test during the Capture-the-Flag exercise to bring techniques and tools together into a comprehensive test

**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 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 task head-on.

### SEC560 IS THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step by step and end to end. 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. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, 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 safely, efficiently, and with great skill.

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

You'll learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser-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, 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. Finally, we focus deep on the technological heart of most organizations, the Windows Domain. We'll cover the technical details of Kerberos and Active Directory and use that for Domain Dominance!

### EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test and on the final day 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, demonstrating the skills you've gained in this course.

**"SEC560 provides practical, how-to material that I can use daily in my penetration testing activities – not only technically, but also from a business perspective."**

— Steve Nolan, **General Dynamics**

# 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

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 finish the module covering vital techniques for false-positive reduction, so you can focus your findings on meaningful results and avoid the sting of a false positive. And we examine the best ways 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; Identifying Insecurities in Windows with GhostPack Seatbelt; False-Positive Reduction; Netcat for the Pen Tester; Initial Access; Password Guessing, Spraying, and Credential Stuffing

## 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

## SECTION 3: Exploitation

In this course 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. You'll also analyze the topic of anti-virus evasion to bypass the target organization's security measures, as well as methods for pivoting through target environments, all with a focus on determining the true business risk of the target organization.

**TOPICS:** Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages; Strategies and Tactics for Anti-Virus Evasion and Application Control Bypass; In-Depth Meterpreter Analysis, Hands-On; Implementing Port Forwarding Relays for Merciless Pivots; How to Leverage PowerShell Empire to Plunder a Target Environment; Lateral Movement with WMI and SC

## SECTION 4: Password Attacks and Merciless Pivoting

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. This course section zooms in on pillaging target environments and building formidable hands-on command line skills. We'll then turn our attention to password cracking attacks, as well as numerous options for plundering password hashes from target machines, including the great Mimikatz Kiwi tool. We'll cover password cracking techniques and strategies using both John the Ripper and Hashcat. In addition, we'll look at pivoting techniques using SSH and the routing features in Metasploit. We'll cover Windows command line skills in-depth, including PowerShell's awesome abilities for post-exploitation. The course section wraps up with a discussion on effective reporting and communication with the business.

**TOPICS:** Password Attack Tips; Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems; Pivoting through Target Environments; Extracting Hashes and Passwords from Memory with Mimikatz Kiwi; PowerShell's Amazing Post-Exploitation Capabilities; Tips for Effective Reporting

## SECTION 5: Domain Domination and Web App Pen Testing

In this course section, we'll zoom in on typical Active Directory lateral movement strategies. You'll get an in-depth understanding of how Kerberos works and what the possible attack vectors are. We'll look at typical local privilege escalation techniques and User Account Control bypasses. We'll also map the internal domain structure using BloodHound to identify feasible attack paths. We'll use Mimikatz to perform domain dominance attacks, where domain replication is used to fully compromise the domain. 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.

**TOPICS:** Kerberos Authentication Protocol; Poisoning Multicast Name Resolution with Responder; Domain Mapping and Exploitation with Bloodhound; Effective Domain Privilege Escalation; Persistent Administrative Domain Access; Azure Authentication Principles and Attacks; Azure AD Integration with On-Premise Domain; Azure Applications and Attack Strategies

## SECTION 6: Penetration Test and Capture-the-Flag Workshop

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 so far in a full-day, hands-on workshop 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 with a team to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) 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 Risks; Merciless Pivoting; Analyzing Results to Understand Business Risk and Devise Corrective Actions