SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™

GXPN
Exploit Researcher & Advanced Pen Tester
giac.org/gxpn

6 Day Program | 46 CPEs | Laptop Required

You Will Be Able To

- Advanced network attack methodologies
- Custom exploit development techniques, using AI to assist
- Exploit mitigation bypass strategies
- Modern fuzzing implementations
- Post-exploitation advancement tactics
- Return-oriented programming mastery
- Cryptographic weakness assessment

Business Takeaways

- Network access control evasion
- Using AI to assist with bug hunting
- Advanced IPv6 security implications
- TLS/SSL security and MFA considerations
- Assessment of cryptographic implementations
- Routing and switching attack vectors
- Escaping restricted desktops and post-exploitation

"The exploit development taught in SEC660 is a very useful, niche, hard to find and learn skill—which makes it very valuable."

—Christian Nicholson, **KPMG**

Expert-Level Security Assessment: Advanced Methods in Penetration Testing

Learn advanced penetration testing skills and explore sophisticated attack vectors and exploit development. This course spans network infrastructure attacks, cryptographic implementation testing, product security testing, advanced post-exploitation techniques, and custom exploit writing for both Windows and Linux environments, using AI to assist. Hands-on labs provide practical experience with fuzzing, return-oriented programming, exploit mitigation bypasses, and real-world application exploitation.

Attackers are becoming more clever and their attacks more complex. To keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. This course provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and furnishes an environment to perform these attacks in numerous hands-on scenarios. The course goes far beyond simple scanning for low-hanging fruit and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

SEC660 starts off by introducing advanced penetration concepts and providing an overview to prepare students for what lies ahead. The focus of section one is on network attacks, especially the areas often left untouched by testers. Topics include accessing, manipulating, and exploiting the network. Covered attacks include NAC, VLANs, OSPF, ARP, IPv6, TLS/SSL, MFA bypass, and others. Section two starts with a technical module on performing penetration testing against various cryptographic implementations, then turns to PowerShell and post-exploitation, escaping Linux restricted environments and Windows restricted desktop environments. Day three jumps into product security penetration testing, Scapy for packet crafting, network and application fuzzing, and code coverage techniques. Sections four and five are spent exploiting programs on the Linux and Windows operating systems. You will learn to identify privileged programs, redirect the execution of code, reverse-engineer programs to locate vulnerable code, obtain code execution for administrative shell access, and defeat modern operating system controls such as ASLR, canaries, and DEP using ROP and other techniques. Local and remote exploits, as well as client-side exploitation techniques, are covered. You will learn how to leverage AI to assist in bug hunting, running your own local LLM. The final course section is devoted to numerous penetration testing challenges that require students to solve complex problems and capture flags.

Among the biggest benefits of SEC660 is the expert-level hands-on guidance provided through the labs and the additional time allotted each evening to reinforce daytime material and master the exercises.

"SEC660 is the right balance between theory and practice; it's hands-on, not too hard, but also not too easy."

— Anton Ebertzeder, **Siemens AG**

Section Descriptions

SECTION 1: Network Attacks for Penetration Testers

Relationships between networked devices present unique attack vectors. In the first section, security professionals explore access manipulation, protocol exploitation, and device compromise across the LAN. Vulnerabilities can be patched, but relationships can be manipulated, making these skills crucial for comprehensive security testing.

TOPICS: Network Access Control Evasion; Custom Protocol Manipulation Methods; Advanced IPv6 Security Implications; TLS/SSL Security Considerations; OSPF Routing Attack Vectors

SECTION 2: Crypto and Post-Exploitation

In this section, security professionals explore cryptographic exploitation and post-compromise techniques in restricted environments. Topics include cipher operations, implementation flaws, privilege escalation, and lateral movement.

TOPICS: Cryptographic Implementation Testing; Identify Patterns in Standard and Custom Encryption; CBC Vulnerability Exploitation; Hash-Length Extension Attacks; Endpoint Restriction Bypasses

SECTION 3: Product Security Testing and Fuzzing

In Section 3, security professionals focus on modern product security testing, protocol manipulation, and fuzzing. Topics include custom fuzzing grammars, network protocols, file formats, and code coverage analysis for testing effectiveness.

TOPICS: Protocol State Manipulation; Automated Fuzzing Optimization; Product Security Testing; Code Coverage Measurement; Wireless Data Leakage Testing Mutation Fuzzing; Optimizing Your Fuzzing Time with Smart Target Selection; Automating Target Monitoring while Fuzzing with Sulley; Source Code-Assisted Binary Fuzzing and Code Coverage Measurement Using AFL++; Block-Based Code Coverage Techniques Using DynamoRio

SECTION 4: Exploiting Linux for Penetration Testers

Linux exploitation is increasingly relevant in the era of AI-assisted vulnerability research. In this section, professionals explore memory management, privilege escalation, SUID exploits, and advanced bypass techniques like ROP and ASLR evasion. You will use a local LLM to assist in bug discovery and exploitation.

TOPICS: Stack Memory Management; AI-Assisted Bug Discovery; 32-Bit and 64-Bit Exploitation; Defeating Exploit Mitigations; Return-Oriented Programming

SECTION 5: Exploiting Windows for Penetration Testers

Windows systems remain prevalent in enterprise environments, necessitating a deep understanding of Windows-specific security features. In this section, practitioners examine process structures, exception handling, and API interactions. Content covers stack-based attacks, DEP bypass, and ROP chains, with special attention given to client-side exploitation.

TOPICS: Windows OS Protection Analysis; Stack Exploitation Fundamentals; ROP Chain Construction; Client-Side Attack Vectors; Shellcode Development

SECTION 6: Capture The Flag!

Students face escalating difficulties across Linux and Windows systems, shellcode challenges, crypto challenges, and much more. The scoring system provides immediate feedback on successful exploitation, with point values reflecting real-world complexity and impact.

TOPICS: Multi-Vector Attack Planning; Escalation Path Identification; Network Attack Implementation; System Compromise Techniques; Post-Exploitation Methods

Who Should Attend

- Network and systems penetration testers
- Incident handlers
- Application developers
- IDS engineers

NICE Framework Work Roles

- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Adversary Emulation Specialist/ Red Teamer (OPM 541)
- Exploitation Analyst (OPM 121)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)

GXPN
Exploit Researcher & Advanced Pen Tester
giac.org/gxpn

GIAC Exploit Researcher and Advanced Penetration Tester

The GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) certification validates a practitioner's ability to pinpoint and mitigate significant security flaws in systems and networks. GXPN certification holders are qualified to conduct advanced penetration tests that improve system security by modeling the behavior of attackers, leveraging expert knowledge to demonstrate and mitigate the business risk posed by these threats.

- Network-based attacks
- Cryptography-based attacks
- Escalation and client-side attacks
- Handling restricted environments
- Scapy, fuzzing, and source code analysis
- Shellcode and memory basics
- Windows and Linux stack overflows
- Defeating advanced stack protections on Windows and Linux