SEC560

Enterprise Penetration Testing

Fall 2025 Update: The Hybrid Frontier of Enterprise Penetration Testing

The latest SEC560 update brings enterprise-scale penetration testing into the hybrid cloud age. This 2025 refresh modernizes the labs, content, and tooling to reflect how real adversaries operate across on-prem, Azure, and Entra ID environments — preparing students to identify, exploit, and assess real business risks with confidence.

Co-authored by Jeff McJunkin and Jon Gorenflo, the updated course expands coverage of cloud exploitation, introduces new lateral movement and persistence labs, and modernizes every section with current tools, frameworks, and defenses. Students experience the full penetration testing lifecycle — from reconnaissance to domain dominance — through realistic, hands-on enterprise scenarios.

"I took this course in 2019 — since then, the attack surface has changed a lot. It is helpful to be up to date with vulnerable features of systems and what bad actors are doing to exploit these."
—Emy L. | SEC560 Student

New Content

- Expanded coverage of Azure and Entra ID exploitation
- New modules on Kerberos, AD CS, and advanced credential attacks
- Updated cloud privilege escalation and RBAC abuse techniques
- Latest toolchain refresh: Sliver, BloodHound, Impacket, Hashcat 7.0
- Enhanced domain dominance labs covering Golden and Silver tickets

Updated Features

- Apple Silicon support with optimized ARM64 virtual machines
- Modernized lab environments modeled after real enterprise networks
- Streamlined lab instructions and improved clarity for every exercise
- 31 hands-on labs rewritten for clarity, relevance, and modern threats
- Enhanced reporting module on delivering impactful pentest results

Lab Refresh

- Revamped Active Directory and Azure exploitation labs
- New Persistence and Evasion exercises using AMSI and AppLocker bypasses
- Updated Capture the Flag event simulating enterprise-wide compromise
- Improved Command and Control labs using Sliver and Metasploit
- Bonus Cloud Operations lab: running commands in Azure VMs

"Modern penetration testing demands hybrid fluency — on-prem, cloud, and everything in between. The refreshed SEC560 bridges that gap, giving professionals the mindset and technical depth to emulate real adversaries and strengthen organizational defenses."
— Jeff McJunkin | SEC560 Author

For more information: sans.org/SEC560

SANS | GIAC CERTIFICATIONS