CA305: Enterprise Pentesting

31 Instructional Hours 41 CPEs 10 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE TO ADVANCED

This course provides a comprehensive introduction to enterprise penetration testing, focusing on how large organizations assess and strengthen their cybersecurity posture through simulated real-world attacks. It explores the evolution, importance, and methodologies of penetration testing, including reconnaissance techniques, vulnerability exploitation, and adversary emulation. Learners are guided through both theoretical foundations and practical tools used in modern security assessments, such as Nmap, Shodan, and recon-ng. The course also emphasizes real-world considerations, including legal constraints, responsible disclosure, and the role of advanced persistent threats (APTs), equipping learners with a holistic understanding of enterprise-level offensive security practices.

You Will Be Able To

- Conduct structured enterprise penetration testing engagements using industry-recognized phases and methodologies
- Perform passive and active reconnaissance using OSINT techniques and specialized tools
- Identify, analyze, and exploit vulnerabilities to assess real-world security risks
- Differentiate between penetration testing and vulnerability assessments and apply both appropriately
- Understand and emulate adversary behavior using MITRE ATT&CK and adversary emulation frameworks
- Apply ethical, legal, and responsible disclosure practices in cybersecurity engagements

Who Should Attend

This course is designed for aspiring and intermediate cybersecurity professionals who want to develop practical skills in penetration testing within enterprise environments. It is suitable for individuals with a basic understanding of networking and operating systems who are looking to transition into offensive security roles or enhance their ability to assess and defend complex IT infrastructures. The course is also valuable for security analysts and IT professionals seeking to understand attacker methodologies and improve organizational security posture.

Relevant Combat Roles

- Penetration Tester (Ethical Hacker)
- Red Team Operator
- Cybersecurity Analyst
- Threat Intelligence Analyst
- Security Consultant
- Incident Response Analyst

Topics Covered

Foundations of enterprise penetration testing, including its importance and the impact of corporate data breaches

Penetration testing methodologies, engagement phases, and types (black-box, gray-box, white-box)

Comparison of penetration testing and vulnerability assessment, along with legal considerations and responsible disclosure

Digital reconnaissance, OSINT techniques, and use of tools such as Nmap, Shodan, WHOIS, and Nikto

Network scanning, enumeration, vulnerability identification, and adversary emulation with threat modeling

Advanced concepts including APTs, attack lifecycle, MITRE ATT&CK framework, and security assessment limitations

Labs

Adversary Emulation & MITRE ATT&CK Operations
(CALDERA automation, ATT&CK mapping, and ATT&CK Navigator usage)

Enterprise Reconnaissance & Network Enumeration
(OSINT investigations, Nmap scanning, DNS enumeration, and infrastructure discovery)

Post-Exploitation & Defense Evasion Techniques
(PowerShell Empire usage, obfuscation techniques, and stealth operations)

Advanced Exploitation & Windows Tradecraft
(buffer overflow exploitation, LOLBins abuse, and privilege escalation)