Advanced Ethical Hacking & Penetration Testing Certified Training Course

15 – 19 February 2027
Barcelona

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Advanced Ethical Hacking & Penetration Testing Certified Training Course

Ref: 103600311_99499 **Date:** 15 – 19 February 2027 **Location:** Barcelona **Fees:** 6500 Euro

Overview

Organizations face persistent digital threats targeting enterprise infrastructure, confidential data, and web platforms. Practical ethical hacking and penetration testing practices allow security teams to discover, analyze, and remediate technical vulnerabilities prior to unauthorized exploitation. This programme develops technical assessment competencies across network vulnerability scanning, web application security testing, and system penetration workflows. Technical practitioners analyze defensive postures using Kali Linux toolkits, the Open Source Security Testing Methodology Manual OSSTMM, and the Penetration Testing Execution Standard PTES. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Cybersecurity analysts and systems engineers responsible for technical vulnerability assessments.
- IT security managers overseeing enterprise defense architectures and audit reviews.
- Network administrators and system engineers tasked with hardening perimeter infrastructure.
- Software developers and web application testers seeking secure code validation techniques.
- Information security consultants and auditors conducting structured penetration assessments.

Departments and Industries

This course supports technical teams responsible for vulnerability management, infrastructure defense, and system auditing across technology-reliant sectors.

- Cybersecurity and IT Security Operations Teams
- Risk, Compliance, and Information Governance Units
- Software Engineering and Application Security Groups
- Systems Infrastructure and Network Engineering Divisions
- Banking, Financial Services, and Insurance Institutions
- Healthcare, Telecommunications, and Technology Enterprises

Learning Objectives

By the end of this course, participants will be able to:

- Execute structured penetration testing workflows aligned with OSSTMM and PTES guidelines.
- Deploy Kali Linux security utilities to discover active hosts, running services, and perimeter weaknesses.
- Identify and exploit common web application flaws including cross-site scripting and SQL injection.
- Perform threat modeling and attack surface analysis across enterprise network topologies.
- Execute privilege escalation and lateral movement techniques in controlled lab environments.

• Compile professional penetration testing documentation with actionable remediation plans.

Course Agenda

Day 1: Foundations and Assessment Methodologies

• Cybersecurity Principles and Penetration Testing Scope Definition
• Framework Alignment using OSSTMM and PTES Security Standards
• Network Security Fundamentals and Baseline Host Reconnaissance
• Cryptographic Primitives and Secure Transport Verification
• Kali Linux Environment Configuration and Toolchain Setup
• Legal Guidelines, Rules of Engagement, and Authorization Scopes

Day 2: Reconnaissance and Vulnerability Mapping

• Passive Information Gathering using Open-Source Intelligence Sources
• Active Network Scanning and Port Probing Techniques
• Vulnerability Identification across Network Nodes and Services
• Web Application Attack Surface Mapping and Parameter Discovery
• Threat Modeling Protocols and Risk Prioritization Matrices
• OSSTMM Operational Security Metrics and Baseline Auditing

Day 3: Exploitation and System Penetration

• Attack Vector Selection and Perimeter Defense Evasion Techniques
• Server-Side Exploit Execution and Remote Code Execution Analysis
• Client-Side Exploits, Spear Phishing Vectors, and Social Engineering Testing
• Web Vulnerability Exploitation: SQL Injection and Cross-Site Scripting
• Wireless Network Auditing and WiFi Encryption Security Assessment
• Exploit Verification and Controlled Proof-of-Concept Development

Day 4: Post-Exploitation and Remediation Planning

• Post-Exploitation Footholds and Persistence Establishment Methods
• Local System Privilege Escalation across Windows and Linux Environments
• Internal Network Pivoting and Lateral Movement Methodologies
• Forensic Footprint Management and Testing Artifact Removal
• Defensive Countermeasure Implementation and Patch Management Strategy
• Technical Penetration Test Reporting and Stakeholder Debriefing

Day 5: Practical Exercises and Security Frameworks

- Multi-Stage Penetration Testing Lab Execution and Target Scenarios
- Enterprise Attack Simulation and Real-World Vector Analysis
- Risk Assessment Integration and Technical Policy Alignment
- Security Certification Standards and Knowledge Domains Review
- Emerging Attack Vectors, Cloud Considerations, and Defensive Trends
- Assessment Debrief, Technical Q&A, and Remediation Walkthrough

Practical Exercises

Participants complete hands-on activities to resolve operational challenges and build execution plans.

- Suggested activity: Configure Kali Linux tools to map active hosts and open service ports across a subnet.
- Suggested activity: Execute a simulated web application test to identify and remediate SQL injection vulnerabilities.
- Suggested activity: Perform privilege escalation on a test machine using misconfigured permissions.
- Suggested activity: Draft an executive-level penetration testing findings report with risk ratings and remediation timelines.

FAQs

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have foundational knowledge of networking protocols, operating system commands, and basic information security concepts. Practical exposure to Linux command-line environments is beneficial.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session runs for approximately 4 to 5 hours, totaling 20 to 25 instructional and lab hours over the five-day period.

What tools will be provided for the penetration testing labs?

The training guides participants through standard open-source and distribution-packaged security tools, focusing on Kali Linux utilities, web application testing proxies, and OSSTMM-aligned evaluation checklists.

Conclusion

Participants conclude this programme with structured, practical competencies in discovering, validating, and documenting security vulnerabilities across network and web environments. By applying OSSTMM and PTES testing standards, security professionals strengthen organizational resilience, mitigate technical exposures, and protect critical assets against evolving cyber threats.