Certified Lead Penetration Testing Professional | Ethical Hacking Training Course

4 – 8 January 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified Lead Penetration Testing Professional | Ethical Hacking Training Course

Ref: 103600300_225127 **Date:** 4 – 8 January 2027 **Location:** Addis Ababa **Fees:** 6000 Euro

Course Overview:

The Certified Lead Penetration Testing Professional | Ethical Hacking Training Course is a comprehensive training program designed to equip professionals with the expertise needed to conduct, manage, and lead penetration tests. Unlike standard cybersecurity training, this course emphasizes hands-on penetration testing while incorporating advanced cybersecurity strategies, cybersecurity risk assessment, and incident handling and response. Participants will gain practical experience in network security testing, web application security testing, mobile security penetration testing, and social engineering penetration testing. The course covers penetration testing methodologies, security vulnerability assessment, and red team cybersecurity training, ensuring participants develop both technical and managerial skills.

Through ethical hacking and pen testing techniques, professionals will learn to identify, assess, and mitigate security risks, enhancing their organization's IT security framework. The program follows an interactive methodology, blending theoretical knowledge with real-world applications, using the latest pen testing tools and techniques. By the end of the training, participants will be prepared for penetration testing certification, boosting their careers as certified cybersecurity professionals.

Target Audience:

- Ethical hackers and penetration testers
- Cybersecurity professionals
- IT security auditors
- Incident response teams
- IT infrastructure and network security engineers
- Risk management and compliance officers
- IT managers and security consultants

Targeted Organizational Departments:

- IT Security and Cybersecurity
- Risk and Compliance
- Incident Response and Forensics
- IT Governance
- Enterprise Security Teams
- Software Development and Secure Coding Teams

Targeted Industries:

- Banking and Financial Services
- Healthcare and Pharmaceuticals
- Government and Defense
- Telecommunications
- Technology and IT Services
- Retail and E-commerce
- Energy and Utilities

Course Offerings:

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

- Conduct network penetration testing and IT infrastructure security testing
- Perform web application security testing and secure web application testing
- Master mobile security penetration testing and cyber threat analysis
- Implement cybersecurity compliance testing and risk assessments
- Utilize penetration testing methodologies and industry frameworks
- Identify and mitigate security exploits and prevention measures
- Lead incident handling and response teams effectively

Training Methodology:

This course follows an interactive and practical training methodology designed to ensure participants develop both technical and analytical skills. The training integrates hands-on penetration testing exercises, real-world case studies, and problem-solving activities to enhance learning. Participants will engage in live demonstrations of pen testing tools and techniques, red team cybersecurity training scenarios, and group discussions to foster collaboration. The methodology also includes comprehensive capture-the-flag challenges, enabling learners to apply their skills in simulated environments. Through a structured blend of theoretical lessons and practical applications, participants will gain the necessary expertise to execute and lead penetration testing engagements effectively.

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Fundamentals of Penetration Testing

- Topic 1: Introduction to penetration testing certification
- Topic 2: Cybersecurity risk assessment fundamentals
- Topic 3: Penetration testing methodologies overview
- Topic 4: Case study enterprise security testing
- Topic 5: Ethical hacking principles and real-world applications
- Reflection & Review: Reviewing key concepts and real-world applications

Day 2: Ethical Hacking and Exploitation Techniques

- Topic 1: Ethical hacking and pen testing principles
- Topic 2: Security vulnerability assessment methods
- Topic 3: IT security certification course essentials
- Topic 4: Practical incident handling and response
- Topic 5: Advanced exploitation techniques
- Reflection & Review: Recap of key techniques and learning outcomes

Day 3: Network and Web Security Testing

- Topic 1: Network penetration testing deep dive
- Topic 2: Secure web application testing hands-on exercises
- Topic 3: Red team cybersecurity training simulation
- Topic 4: Advanced penetration testing tools
- Topic 5: Case study on enterprise network security
- Reflection & Review: Practical discussion on tested security methodologies

Day 4: Social Engineering and Mobile Security

- Topic 1: Social engineering penetration testing techniques
- Topic 2: Mobile security penetration testing methods
- Topic 3: Cyber defense training case studies
- Topic 4: Cybersecurity compliance testing best practices
- Topic 5: Secure coding and application security testing
- Reflection & Review: Understanding risks in social engineering and mobile security

Day 5: Final Assessments and Capture-the-Flag

- Topic 1: Full-scale enterprise security testing scenario
- Topic 2: Final cyber threat analysis presentation
- Topic 3: Capture-the-flag challenge and certification assessment
- Topic 4: Pen testing tools and real-world application review
- Topic 5: Incident response and post-assessment strategies
- Reflection & Review: Key takeaways and application in professional settings

FAQ:

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

Participants should have a basic understanding of IT security principles and some experience with networking or ethical hacking concepts.

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

Each day’s session lasts approximately 4-5 hours, totaling 20-25 hours of training across one week.

How does penetration testing help organizations prevent cyber threats?

Penetration testing simulates real-world attacks to identify security vulnerabilities, helping organizations strengthen their cybersecurity risk assessment and incident response strategies.

How This Course is Different from Other Penetration Testing Courses:

This course stands out by combining practical penetration testing techniques, ethical hacking bootcamp-style learning, and comprehensive cybersecurity compliance testing. It provides a hands-on, structured approach to enterprise security testing, equipping participants with the necessary skills to lead professional penetration testing projects with confidence.