Pentest 101: Fundamentals of Ethical Hacking in Security

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

- Security Analysts,
- Entry-level Penetration Testers
- System Administrators
- IT professionals looking for a first experience in ethical hacking

Training objectives

- Understand the basics of penetration testing and ethical hacking
- Discover the main tools and frameworks used in pentest
- Practice identifying and exploiting vulnerabilities in a controlled environment
- Develop basic skills in communicating results

Summary

This introductory training provides participants with the essential principles of penetration testing, combining conceptual understanding with practical exercises. Learners will become familiar with the tools, methodologies and practices of report writing, providing a solid foundation for more advanced training in ethical hacking.

Course outline

Module 1: Introduction to Ethical Hacking and Penetration Testing

- Definitions, Scope and Ethics of the Pentest
- Legal and Regulatory Environment
- Overview of Common Attack Vectors

Module 2: Methodologies and Frameworks

-

© 2026

Reconnaissance and Information Collection

- Vulnerability Analysis and Scanning
- Basics of Exploitation
- Post-Exploitation and Maintaining Access

Module 3: Tools of the Trade

- Nmap, Metasploit, Burp Suite, Wireshark
- Hands-on Workshop: Scanning a Target
- Best Practices for a Secure Test Environment

Module 4: Reporting and Insights

- Structuring a Pentest Report
- Communicating Risks to Technical and Non-Technical Stakeholders
- Avenues for Future Certifications and Learnings

Approach and methodology

Structured lectures to understand the fundamental concepts of penetration testing and ethical hacking. Demonstrations of the tools and methodologies used in pentesting to illustrate the concepts. Practical exercises promoting the handling of tools and the practical application of basic techniques. Laboratories or controlled environments to practice identifying and exploiting vulnerabilities. Case studies or concrete examples to help understand real cybersecurity issues. Report writing practice in order to structure and communicate the results of a penetration test.

Prerequisites

Basic knowledge of networks and operating systems

Recommendations

Familiarity with command line use (Linux/Windows) an asset

© 2026