CYBERUNIVERSITY
by DataScientest

Ethical hacking - level 1 Program

Ethical hacking - level 1

This training will teach you techniques to assess the security level of your information system.
You will learn how to apply measures and rules to combat hacking and identify the mechanisms behind major attacks.

TARGET AUDIENCE

- System and network technicians and administrators
- Security architects
- Security integrators
- Cybersecurity students
- Security managers
- Security auditors

PREREQUISITES

- Knowledge of networks and Windows/Linux systems
- CISR1

Duration: 5 days

TRAINING PROGRAM

1 - HACKING PRINCIPLES:

- Definition
- Typology of attackers
- Terminology

2 - HACKING METHODOLOGY:

- PTES
- OWASP
- OSSTMM
- Red Team / Blue Team
- Unified Kill Chain

3 - AUDIT PREPARATION + REPORT:

- Contract
- Context and scope
- Laws
- Pentester's toolkit
- Setting up in the cloud
- How to organize a report

4 - ATTACK VECTORS:

- Virus / Worm / Trojan horse
- Backdoor
- Spyware / Keylogger
- Exploit
- Rootkit
- Ransomware
- Spam / Phishing / Hoax
- Spearphishing
- Botnet
- Network and vulnerability scanners

5 - OSINT:

- Introduction to OSINT
- OSINT methodology
- Example: Google Dorks / Email search / Subdomain search

6 - ACTIVE RECONNAISSANCE
- Principle
- Methodology
- Practical exercises: Nmap, Metasploit, Scapy

7 - VULNERABILITIES
- MITRE ATT&CK Framework
- Vulnerability Scanning
- Social Engineering
- CVE (Common Vulnerabilities and Exposures)

8 - TYPES OF ATTACKS
- Network Exploitation (MITM - Man in the Middle)
- Social Engineering/Phishing/Deepfake
- Server-side Attacks (Exploiting CVEs, Cracking, Bruteforce)

9 - WEB & WEB APPLICATION HACKING
- Principle
- Methodology
- Types of attacks: Client-side, Back-end

10 - FRONT-END ATTACKS
- OWASP Top 10
- Exploiting Vulnerabilities

11 - ADVANCED ATTACKS
- Creating Payloads
- Customizing Exploits
- Implementing Pivoting
- Browser Exploitation

12 - POST-EXPLOITATION
- Implementing Data Exfiltration Techniques
- Command & Control (C&C)
- Privilege Escalation
- Performing Local Enumeration
- Erasing Traces

13 - REPORTING
- Example of a report
- Analyzing a report
- Communication and presenting results

14 - HANDS-ON EXERCISE
- Pentesting in a lab environment
- Writing the report

15 - FOCUS ON SPECIFIC TECHNIQUES
- Hacking Wi-Fi
- Hacking Cloud environments
- Hacking IoT (Internet of Things) devices
- Hacking Mobile devices

LEARNING OBJECTIVES

By the end of the training, participants will be able to:
- **Understand the hacker's methodology**
- **Learn the terminology related to hacking**
- **Apply the attacker's cycle in practice**
- **Write a pentest report**