RANDORISEC

Training: Penetration Testing

Objective: Learn how to perform penetration tests
Level: beginner/intermediate
Duration: 3 days

1 500 € VAT excluded

Davy Douhine and Guillaume Lopes will deliver a 100% hands-on training to learn and understand the techniques, tips and tools used to perform penetration tests on different targets (web applications, servers, networks, etc.).

- **A VM with the pre-installed tools to cover most of the labs will be provided**

Key Learning Objectives

- ✓ Introduce the pentest workflow
- ✓ Present the OWASP Testing Guide for web applications
- ✓ Introduction to classic buffer overflow exploitation
- ✓ Compromise Windows and Linux machines
- ✓ Exploit real web vulnerabilities

Who Should Attend?

- System and network administrators
- Developers
- Consultants

Prerequisite Knowledge

- Network and Windows/Linux knowledge

Agenda

Day 1

Module 1: Methodology

- Pentest workflow / Tools

Module 2: Information Gathering

- OSINT
  - Search engines
  - Shodan
  - DNS enumeration

Module 3: Port Scanning – Network attacks

- Scanning with Nmap
- Man in the Middle attacks

Module 4: Vulnerability Scanning

- Identify vulnerabilities
- Tools: Nessus and Nmap

Module 5: Password Cracking

- Offline vs Online
- Bruteforce attacks
- Rainbow tables

Day 2

Module 6: Buffer overflow exploitation

- Exploit a classic buffer overflow on Windows

Module 7: Metasploit introduction

- What is Metasploit?
- Basic usage

Module 8: Server-side exploitation

- How to compromise servers with Metasploit

Module 9: Client-side exploitation

- How to compromise workstations with Metasploit

Module 10: Post-exploitation

- Retrieve stored credentials
- Pass the Hash
- Lateral movement

Day 3

Module 11: Exploiting web vulnerabilities

- OWASP Testing Guide / ASVS
- Tools: BurpSuite / SQLmap

Module 12: Introduction to BurpSuite

- How to use it?
- Proxy / Repeater features

Module 13: Injection vulnerabilities

- SQL Injection
- XXE
- Command Injection

Module 14: Client-side issues

- Reflected / Stored XSS
- CSRF

Module 15: Access control

- IDOR
- Directory Traversal
- Logical issues