Course : Nessus, conducting a vulnerability audit

Practical course - 2d - 14h00 - Ref. NES
Price : 1480 € E.T.

Nessus is the benchmark solution for auditing vulnerabilities in information systems. In this course, you will learn how to conduct a vulnerability audit on networks, Web applications, operating systems, equipment and injections of different types of malicious code.

🎯 Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Installing and configuring Nessus
- ✓ Using the Nessus client
- ✓ Conducting a vulnerability audit with Nessus
- ✓ Conduct a configuration audit of Windows and Linux systems

Intended audience

Technicians, system and network administrators and auditors required to perform [[PenTest]".

Prerequisites

Basic knowledge of networks and security.

Course schedule

1 Background and positioning of Nessus

- Terminology and references relating to vulnerabilities (CVE, CWE, CVSS, AWS, CERT, etc.).
- Security audit versus vulnerability audit and penetration test.
- Positioning of different security tools and approaches: intrusion detection, scanner.
- Vulnerability auditing tools (Snort, Suricata, Nessus, OpenVas, Qualys, Acunetix...).
- Network, system and application vulnerability scanning (tools, approach and limitations).
- Introducing Nessus products.
- Client/server operating mode.
- Basic network configuration and scanning.

Hands-on work
Installation, configuration and basic network scanning.

2 Nessus components and architectures

- Nessus architecture and features.
- Plug-in integration: managing and designing plug-ins.
- Deployment of manager, agent.
- License management.

Hands-on work
Configuration and settings. Plug-in management and design.

3 Policy: design and analysis

- Definition of a basic scan policy.
- Define and manage a discovery policy (host, port, service).
- Create, configure and schedule an advanced vulnerability scan.
- Vulnerability scanning operations: scans of vulnerable Web applications, active scans, authenticated scans.
- Web application vulnerability audits.
- Designing a security policy.

Hands-on work
Security policy design and vulnerability audit. Implement a Web platform and audit Web application vulnerabilities.

4 Configuration and vulnerability audits: implementation and analysis

- Principles of configuration auditing.
- Introduction to compliance auditing.
- System audit principles: Windows, Linux/Unix.
- System and virtual environment auditing.
- Reporting and vulnerability analysis.

Hands-on work
Configuration audit of Windows and Linux systems.

Dates and locations

REMOTE CLASS
2026 : 9 Mar., 18 June, 26 Oct.

PARIS LA DÉFENSE
2026 : 9 Mar., 18 June, 26 Oct.