CompTIA Penetration Testing (PENTEST+)

ID PENTEST+ **Prix** sur demande **Durée** 5 jours

A qui s'adresse cette formation

If you're an intermediate level cyber security professional tasked with penetration testing, this course is ideal for you.

Pré-requis

Before attending this course, you should have:

- Network+, Security+ or equivalent knowledge
- A minimum of 2-3 years of hands-on information security or related experience

Objectifs

You'll learn to:

- customise assessment frameworks
- report penetration test findings
- communicate recommended strategies

On this course, you'll prepare for the CompTIA PenTest+ exam The performance-based PenTest+ exam involves hands-on simulations, proving you've moved beyond theory and have the practical skills to carry out penetration testing techniques.

Achieving this certification qualifies you for a role as a:

- Penetration Tester
- Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability

Contenu

Planning and Scoping

- Explain the importance of planning for an engagement
- Explain key legal concepts.
- Explain the importance of scoping an engagement properly.
- Explain the key aspects of compliance-based assessments.

Information Gathering and Vulnerability Identification

- Given a scenario, conduct information gathering using appropriate techniques
- Given a scenario, perform a vulnerability scan.
- Given a scenario, analyse vulnerability scan results
- Explain the process of leveraging information to prepare for exploitation.
- Explain weaknesses related to specialised systems

Attacks and Exploits

- Compare and contrast social engineering attacks
- Given a scenario, exploit network-based vulnerabilities
- Given a scenario, exploit wireless and RF-based vulnerabilities
- Given a scenario, exploit application-based vulnerabilities
- Given a scenario, exploit local host vulnerabilities
- Summarise physical security attacks related to facilities
- Given a scenario, perform post-exploitation techniques

Penetration Testing Tools

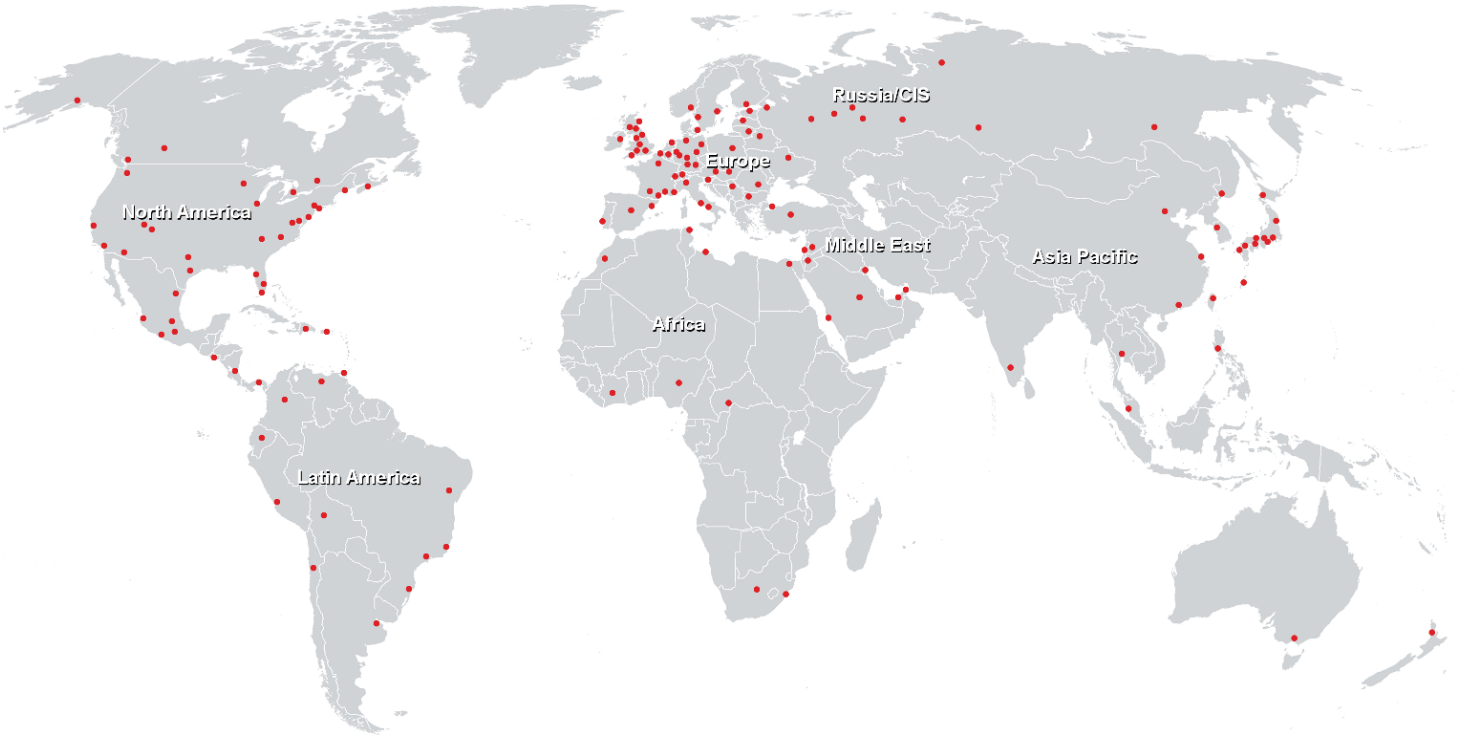
- Given a scenario, use Nmap to conduct information gathering exercises
- Compare and contrast various use cases of tools
- Given a scenario, analyse tool output or data related to a penetration test
- Given a scenario, analyse a basic script (limited to Bash, Python, Ruby, and PowerShell)

Reporting and Communication

- Given a scenario, use report writing and handling best practices
- Explain post-report delivery activities
- Given a scenario, recommend mitigation strategies for discovered vulnerabilities
- Explain the importance of communication during the penetration testing process

CompTIA Penetration Testing (PENTEST+)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch