CompTIA Penetration Testing (PENTEST+)

ID PENTEST+ **Preis** auf Anfrage **Dauer** 5 Tage

Voraussetzungen

Vor der Teilnahme am Kurs sollten Sie über folgende Vorkenntnisse verfügen:

- Network+, Security+ oder äquivalente Kenntnisse
- Mindestens 2-3 Jahre Praxiserfahrungen in der Informationssicherheit oder verwandten Bereichen

Kursziele

Sie lernen:

- Anpassung von Assessment Frameworks
- Reporting von Penetration Test Ergebnissen
- Kommunikation empfohlener Strategien

Im Kurs werden Sie auf die CompTIA PenTest+-Prüfung vorbereitet. Die leistungsbasierte PenTest+-Prüfung beinhaltet praktische Simulationen. Sie müssen beweisen, dass Sie über die Theorie hinausgehende, praktische Fähigkeiten haben, um Penetration Testing Techniken auszuführen.

Die PenTest+-Zertifizierung qualifiziert Sie für Positionen in diesen Bereichen:

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

Kursinhalt

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

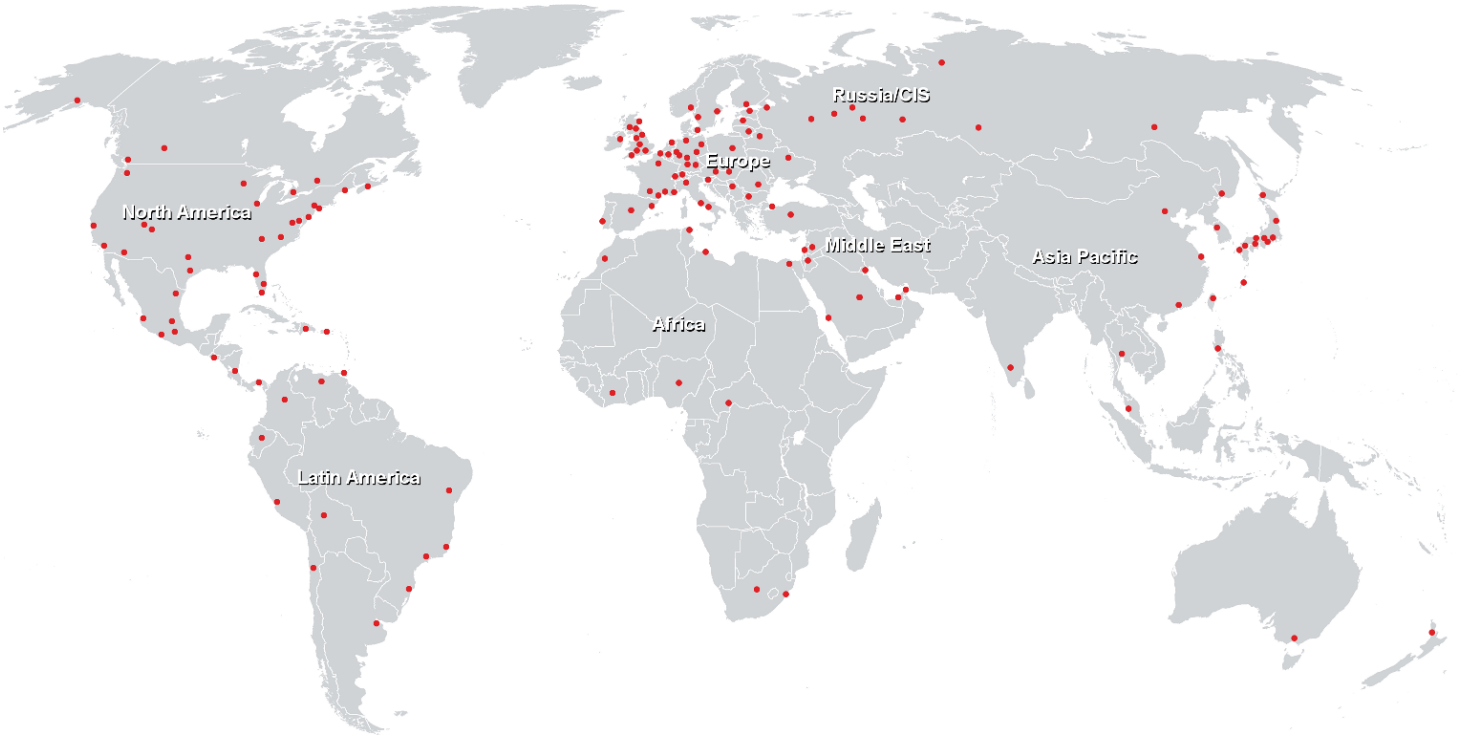
- Given a scenario, use Nmap to conduct information gathering exercises
- Compare and contrast various use cases of tools
- Given a scenario, analyse tool output or data related to a penetration test
- Given a scenario, analyse a basic script (limited to Bash, Python, Ruby, and PowerShell)

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+)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

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

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