EC-Council Certified Penetration Testing Professional C|PENT AI (CPENT)

ID CPENT **Preis** CHF 6'200.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

Der Kurs richtet sich an diejenigen, die sich intensiv mit Angriffen und deren Abwehr auf das eigene Netzwerk befassen: Penetrationstester, Ethical Hacker, Berater für Informationssicherheit, Security-Tester und -Analytiker, Administratoren (Netzwerk, Firewall, System), Experten für Risikobewertung.

Voraussetzungen

Zwingend vorausgesetzt wird umfassendes Wissen über Penetrationstests in verschiedenen Disziplinen: Windows, IoT, Inline-Abwehr, Automatisierung, Betriebstechnologie und fortgeschrittenen Fähigkeiten in der binären Nutzung. Wer die Zertifizierung anstrebt muss darauf vorbereitet sein, dass nicht nur automatisierte Tools, sondern auch manuelle Fähigkeiten getestet werden.

Kursziele

Das weltweit umfassendste Penetration Testing-Programm

- Pentesting mit KI-Fähigkeiten – Abdeckung aller Phasen des Penetration Tests
- Einzigartiger, multidisziplinärer Kurs – Testen Sie Ihre Fähigkeiten praxisnah
- CPENT vs. andere Zertifizierungen – Vollständige, praxisorientierte Methodik statt reiner Theorie
- Projekt-Scoping & Reporting – Auftragsdefinition, Aufwandsschätzung & professionelle Präsentation der Ergebnisse
- Vielseitige Ausbildung – Entwickelt, um Experten für Red Teaming & offensive Sicherheit zu formen
- Hybrid-Lernansatz – Kombination aus geführtem Training und flexiblem Selbststudium
- 100% praxisorientiert – CTF-Herausforderungen, über 100 Übungen & Live-Cyber-Labs
- Echte Szenarien, echte Fähigkeiten – Infiltrieren, Risiken bewerten & umsetzbare Berichte erstellen
- VAPT-Ready – Bereiten Sie sich und Ihre Organisation auf reale Bedrohungen & Compliance-Anforderungen vor

Hinweise zur Prüfung

Dieser Kurs bereitet die Teilnehmer auf das Examen zum CPENT vor. Diese rein praktische Prüfung wird online durchgeführt und überwacht. Die Dauer der Prüfung beträgt 24 h und kann in einer (24 h) oder zwei (2x12 h) Sessions durchgeführt werden. Im Anschluss an das Examen muss der Kandidat einen Report zum Examen schreiben und innerhalb von sieben Tagen nach dem Examen einreichen. Wer den Test mit einem sehr guten Ergebnis abschliesst, erhält als Bonus neben dem CPENT-Zertifikat auch die LPT (Licensed Penetration Tester)-Zertifizierung:

- Mehr als 70 % -> CPENT
- Mehr als 90 % -> LPT (Licensed Penetration Tester).

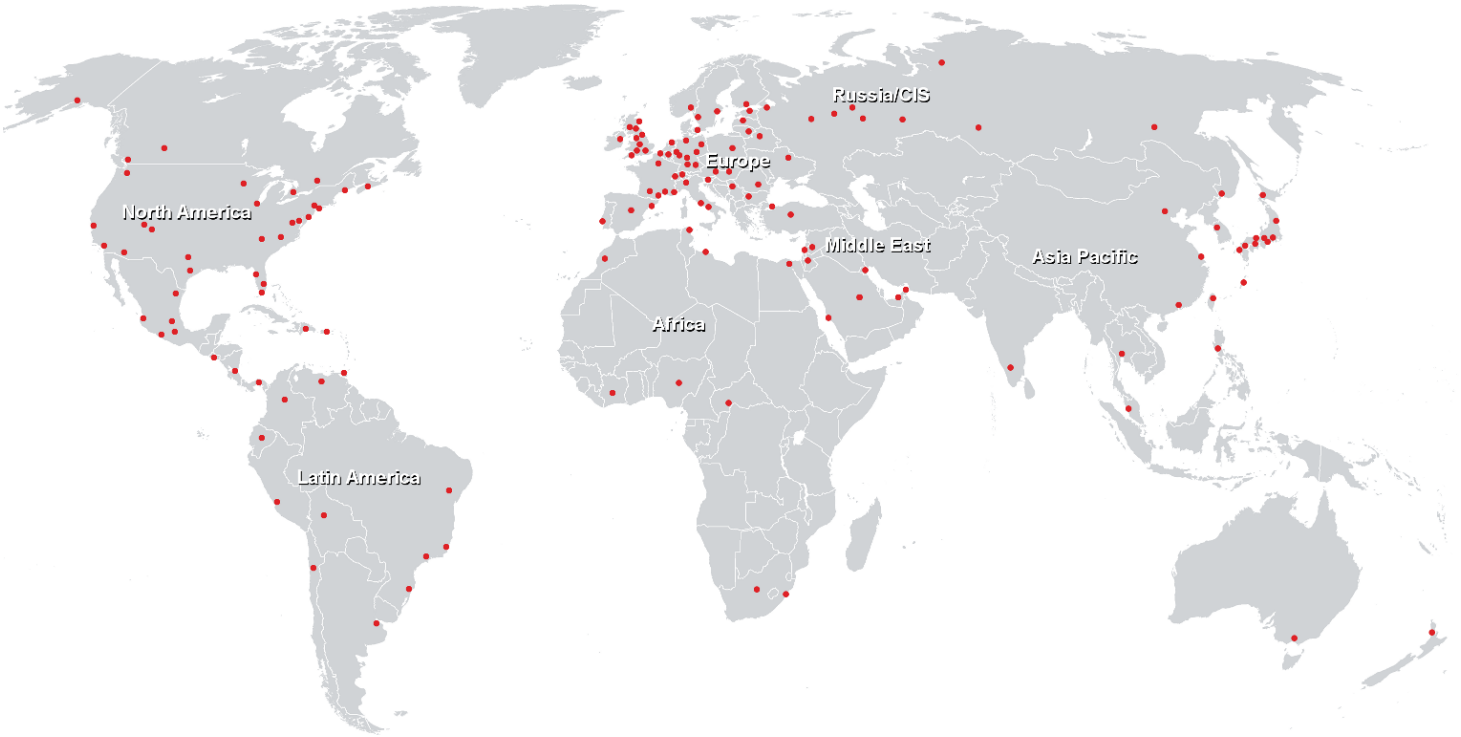
Die Prüfungsgebühr ist im Kurspreis enthalten.

Kursinhalt

- Module 01: Introduction to Penetration Testing and Methodologies
- Module 02: Penetration Testing Scoping and Engagement
- Module 03: Open Source Intelligence (OSINT) and Attack Surface Mapping
- Module 04: Social Engineering Penetration Testing
- Module 05: Web Application Penetration Testing
- Module 06: API and Java Web Token Penetration Testing
- Module 07: Perimeter Defense Evasion Techniques
- Module 08: Windows Exploitation and Privilege Escalation
- Module 09: Active Directory Penetration Testing
- Module 10: Linux Exploitation and Privilege Escalation
- Module 11: Reverse Engineering, Fuzzing and Binary Exploitation
- Module 12: Lateral Movement and Pivoting
- Module 13: IoT Penetration Testing
- Module 14: Report Writing and Post Testing Actions

EC-Council Certified Penetration Testing Professional C|PENT AI (CPENT)

Weltweite Trainingscenter



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