



CPENT

Certified Penetration Tester

Mit dem Certified Penetration Tester (CPENT) hat EC-Council eine neue Zertifizierung zum Penetration-Testing auf den Markt gebracht. Mit diesem Programm werden Qualifikationslücken geschlossen und die berufliche Rolle eines Penetration-Testers und Sicherheitsanalysten abgebildet. Für diese Berufsfelder ist Out-of-Box-Denken erforderlich, da die Herausforderungen einem progressiven Ansatz folgen, bei dem die nächste Herausforderung schwieriger ist als die vorherige.

In diesem Training lernen die Teilnehmer, wie ein effektiver Penetration-Test in einer Unternehmensnetzwerkumgebung durchgeführt wird, die angegriffen, ausgenutzt, umgangen und verteidigt werden muss. Wer bisher nur in flachen Netzwerken gearbeitet hat, wird seine Fähigkeiten durch die Live-Übungen des CPENT auf die nächste Stufe heben, indem die Methoden zum Pen-Test eines IoT-Systems, OT-Systems, zum Schreiben eigener Exploits und zum Erstellen eigener Tools vermittelt werden. Es wird aufgezeigt, wie auf versteckte Netzwerke zugegriffen werden kann und wie man mit angepassten Skripten/Exploits in die innersten Segmente eines Netzwerks gelangt.

Dieser Kurs bereitet Sie 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).

Kursinhalt

- Advanced Window Attacks
- Attacking IoT Systems
- Writing Exploits: Advanced Binaries Exploitation
- Bypassing a Filtered Network
- Pentesting Operational Technology (OT)
- Access Hidden Networks with Pivoting
- Double Pivoting
- Privilege Escalation
- Evading Defense Mechanisms
- Attack Automation with Scripts
- Build Your Armory: Weaponize Your Exploits
- Write Professional Reports

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.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.ch/go/CPEN

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

CPENT

Training	Preise zzgl. MwSt.
Termine in der Schweiz	5 Tage
Online Training	5 Tage CHF 4.395,-
Termine auf Anfrage	

Stand 24.02.2024

EC-Council



EXPERTech



Inhaltsverzeichnis

CPENT – Certified Penetration Tester

Module 01: Introduction to Penetration Testing	Appendix I: Active Directory Pen Test
Module 02: Penetration Testing Scoping and Engagement	Appendix J: Database Penetration Testing
Module 03: Open Source Intelligence (OSINT)	Appendix K: Mobile Device Penetration Testing
Module 04: Social Engineering Penetration Testing	
Module 05: Network Penetration Testing - External	
Module 06: Network Penetration Testing - Internal	
Module 07: Network Penetration Testing - Perimeter Devices	
Module 08: Web Application Penetration Testing	
Module 09: Wireless Penetration Testing	
Module 10: IoT Penetration Testing	
Module 11: OT/SCADA Penetration Testing	
Module 12: Cloud Penetration Testing	
Module 13: Binary Analysis and Exploitation	
Module 14: Report Writing and Post Testing Actions	
Appendix A: Penetration Testing Essential Concepts	
Appendix B: Fuzzing	
Appendix C: Mastering Metasploit Framework	
Appendix D: PowerShell Scripting	
Appendix E: Bash Environment and Scripting	
Appendix F: Python Environment and Scripting	
Appendix G: Perl Environment and Scripting	
Appendix H: Ruby Environment and Scripting	

