



# 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.experteach.de/go/CPENT](http://www.experteach.de/go/CPENT)

### 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.	
<b>Termine in Deutschland</b>	<b>5 Tage</b>	<b>€ 4.150,-</b>
<b>Online Training</b>	<b>5 Tage</b>	<b>€ 4.150,-</b>
<b>Termin/Kursort</b>	Kurssprache Deutsch	
14.09.-18.09.26	14.09.-18.09.26	

Stand 25.03.2026

EC-Council



EXPERTeach



# Inhaltsverzeichnis

## CPENT – Certified Penetration Tester

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

