NEXIO Online Akademie GmbH

# Ethical Hacking für IT-Profis: Praktische Penetrationstests und Sicherheit mit der CompTIA PenTest+ Zertifizierung

Sonstiges · Anbieter: NEXIO Online Akademie GmbH

FÖRDERUNG & KOSTEN

**Kurspreis: 5.932 €**

Förderfähig über: Bildungsgutschein

AZAV-zertifizierter Bildungsträger — Förderung durch die Agentur für Arbeit möglich

## Kursdaten auf einen Blick

| | |
|---|---|
| **Durchführung** | Online |
| **Lernformat** | Zeitgebunden |
| **Dauer** | 8 Wochen in Vollzeit |
| **Unterrichtssprache** | Deutsch |
| **Kursstart** | Startet jede Woche |
| **Vorkenntnisse** | Grundlegende Kenntnisse |
| **Abschluss** | International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat bzw. Teilnahmebescheinigung |

## Bildungsträger & Kontakt

**NEXIO Online Akademie GmbH**

Am Herrschaftsweiher 11, 67071 Ludwigshafen am Rhein

Telefon: 0800 100 87 34

E-Mail: beratung@nexio-akademie.de

Web: https://nexio-akademie.de

Kurs online ansehen

## 01 Kursbeschreibung

Erweitern Sie Ihre beruflichen Möglichkeiten mit der CompTIA PenTest + Zertifizierung, die Sie praxisnah auf die Herausforderungen moderner IT-Sicherheitsanalysen vorbereitet. Diese Weiterbildung vermittelt Ihnen umfassende Kenntnisse in den Bereichen Schwachstellenbewertung, Angriffstechniken, Informationsbeschaffung und Sicherheitskontrollen. Sie lernen, Sicherheitslücken systematisch zu erkennen, zu analysieren und effektive Schutzmaßnahmen zu ergreifen. Der CompTIA PenTest + richtet sich an IT-Profis, die ihre Expertise im Ethical Hacking und bei Penetrationstests vertiefen möchten, um IT-Infrastrukturen gezielt zu sichern. Mit dieser Zertifizierung qualifizieren Sie sich als gefragte:r Spezialist:in für Sicherheitsanalysen und Schutzstrategien in komplexen IT-Umgebungen. Gestalten Sie aktiv die Zukunft der IT-Sicherheit mit dem CompTIA PenTest+!

## 02 Lehrplan & Module

### 1. Planung und Umfang von Penetrationstests

Du lernst, wie Penetrationstests geplant und vertraglich abgesichert werden, etwa durch Scope, Rules of Engagement und Einverständniserklärungen. Dazu gehören auch rechtliche Rahmenbedingungen und die Abstimmung mit dem Auftraggeber.

### 2. Informationsbeschaffung und Aufklärungstechniken

Du setzt passive und aktive Methoden der Informationsbeschaffung ein, etwa OSINT, DNS-Abfragen und die Auswertung öffentlich verfügbarer Daten. So erstellst Du ein Bild der Angriffsfläche eines Zielsystems.

### 3. Schwachstellenbewertung und Risikoeinschätzung

Du führst Schwachstellenscans durch, interpretierst die Ergebnisse und bewertest Schwachstellen nach Schweregrad, etwa mit CVSS. Außerdem lernst Du, Fehlalarme zu erkennen und Risiken für das Unternehmen einzuordnen.

### 4. Exploitation von Netzwerken und Systemen

Du lernst Angriffstechniken auf Netzwerke und Systeme kennen, etwa das Ausnutzen von Diensten, Fehlkonfigurationen und Passwortschwächen. Dabei arbeitest Du in Laborumgebungen mit gängigen Exploit-Frameworks.

### 5. Post-Exploitation und Privilegienausweitung

Du lernst, was nach einem erfolgreichen Zugriff folgt, darunter Rechteausweitung, laterale Bewegung und Persistenz. Ebenso geht es um das Aufräumen nach dem Test und das Dokumentieren der Angriffswege.

### 6. Berichtserstellung und Kommunikation der Ergebnisse

Du erstellst einen strukturierten Testbericht mit Management Summary, technischen Befunden, Risikobewertung und Handlungsempfehlungen. Zudem übst Du, Ergebnisse verständlich gegenüber Technik und Management zu kommunizieren.

### 7. Netzwerkscanning und Serviceerkennung

Mit Werkzeugen wie Nmap führst Du Port- und Netzwerkscans durch und identifizierst laufende Dienste, Versionen und Betriebssysteme. Du lernst verschiedene Scantechniken und ihre Auswirkungen auf das Zielnetz kennen.

### 8. Webanwendungssicherheit und Tests

Du testest Webanwendungen auf typische Schwachstellen wie SQL-Injection, Cross-Site-Scripting und fehlerhafte Authentifizierung, orientiert an den OWASP Top 10. Dabei setzt Du Proxy-Werkzeuge zur Analyse von Anfragen und Antworten ein.

### 9. Wireless-Netzwerksicherheit und Angriffsmethoden

Du lernst Sicherheitsmechanismen von WLANs wie WPA2 und WPA3 kennen und analysierst typische Angriffe wie Rogue Access Points, Deauthentifizierung und das Knacken schwacher Schlüssel. Daraus leitest Du Schutzmaßnahmen ab.

### 10. Social Engineering und physische Sicherheitsaspekte

Du lernst Methoden des Social Engineering wie Phishing, Pretexting und Tailgating kennen und wie sie in Tests eingesetzt werden. Dazu gehört auch die Prüfung physischer Sicherheitsmaßnahmen wie Zutrittskontrollen und Schlösser.

### 11. Einsatz von Penetrationstest-ToolsAngriffstechniken und Exploit-Methoden

Du arbeitest mit typischen Werkzeugen für Scans, Passwortangriffe, Webtests und Exploitation und lernst ihre Einsatzgebiete kennen. Darüber hinaus übst Du verschiedene Angriffstechniken und Exploit-Methoden in einer sicheren Testumgebung.

### 12. Cloud- und Virtualisierungsumgebungen analysieren

Du analysierst Cloud-Umgebungen und virtualisierte Systeme auf Fehlkonfigurationen, unsichere Zugriffsrechte und Schwachstellen in Containern. Ebenso lernst Du die Besonderheiten von Tests bei Cloud-Anbietern und deren Vorgaben kennen.

### 13. Sicherheitskontrollen und Gegenmaßnahmen bewerten

Du bewertest technische, organisatorische und physische Sicherheitskontrollen auf ihre Wirksamkeit. Daraus leitest Du passende Gegenmaßnahmen wie Härtung, Patching, Segmentierung und Monitoring ab.

### 14. Schwachstellenmanagement und Nachverfolgung

Du lernst den Kreislauf des Schwachstellenmanagements kennen, von der Erkennung über die Priorisierung bis zur Behebung und Nachprüfung. Dabei geht es auch um Retests und die Dokumentation offener Punkte.

### 15. Vorbereitung auf die externe Prüfung

Du wiederholst die Prüfungsinhalte der CompTIA PenTest+, bearbeitest Übungsfragen und performance-basierte Aufgaben und lernst das Prüfungsformat kennen. So identifizierst Du gezielt verbleibende Wissenslücken.

## 03 Enthaltene Zertifikate

**Trägerzertifikat: International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat bzw. Teilnahmebescheinigung**

## 04 Voraussetzungen

### Vorkenntnisse

**Niveau: Grundlegende Kenntnisse**

Vorausgesetzt werden gute Deutschkenntnisse auf dem Mindestniveau von B2. Englischkenntnisse auf dem Niveau B2 sind notwendig, da sowohl die Lernmittel als auch die Zertifizierungsprüfung in Englisch bearbeitet werden müssen. Zwingend erforderlich sind fundierte Kenntnisse im Umgang mit PC-Systemen generell sowie im Bereich der Netzwerktechnik und der IT-Sicherheit. Eine Ausbildung in diesem Bereich (z. B. als Fachinformatiker:in - Systemintegration o. ä.) bzw. ein Studium sind von Vorteil.

## 05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende

Mögliche Berufsbilder: Penetration Tester, IT-Sicherheitsbeauftragter, IT-Sicherheitsadministrator

NÄCHSTER SCHRITT

### Kursdetails online ansehen und Anbieter kontaktieren

NEXIO Online Akademie GmbH · Am Herrschaftsweiher 11, 67071 Ludwigshafen am Rhein
0800 100 87 34 · beratung@nexio-akademie.de · https://nexio-akademie.de

Online ansehen