EC-Council Certified Ethical Hacking v12 (CEH)

Exam-ID: **312-50**

Seminar-ID: **ETHACK**

Your key takeaways

Sie glauben, dass Ihr Netzwerk optimal gesichert ist? Nach Besuch des Kurses werden Sie die Sicherheit Ihres Netzwerkes in einem ganz anderen Licht sehen und haben nicht nur gelernt die Schwachstellen Ihres Netzwerks zu erkennen, sondern auch dieses optimal gegen Angriffe zu sichern. Denn - um einen Hacker zu bekämpfen, muss man denken wie einer.

Wer ist ein Certified Ethical Hacker?
Ein Certified Ethical Hacker ist ein Spezialist*in, der*die typischerweise in einer Red Team-Umgebung arbeitet und sich auf Angriffe auf Computersysteme und den Zugang zu Netzwerken, Anwendungen, Datenbanken und andere kritische Daten auf gesicherten Systemen konzentriert. Ein CEH versteht Angriffsstrategien, den Einsatz von kreativen Angriffsvektoren und weiß um die Fähigkeiten und die Kreativität böswilliger Hacker.
Im Gegensatz zu böswilligen Hackern, arbeiten Certified Ethical Hacker mit Erlaubnis der Systemeigentümer und ergreifen alle Vorsichtsmaßnahmen, um sicherzustellen, dass die Ergebnisse vertraulich bleiben. Bug Bounty Researchers sind Profi-Ethical Hacker, die ihre Angriffstechniken einsetzen, um Schwachstellen in den Systemen aufzudecken.

Certified Ethical Hacker (CEH) Version 12
CEH bietet ein tiefes Verständnis der Ethical Hacking-Phasen, der verschiedenen Angriffsvektoren und präventive Gegenmaßnahmen. Sie werden lernen, wie Hacker böswillig denken und handeln, damit werden Sie besser in der Lage sein, Ihre Sicherheitsinfrastruktur einzurichten und künftige Angriffe abzuwehren. Systemschwächen und Schwachstellen zu verstehen, hilft Organisationen, Systemsicherheitskontrollen zu etablieren, um das Risiko eines Zwischenfalls zu minimieren.

CEH wurde gebaut, um eine praktische Umgebung und einen systematischen Prozess über alle

Ethical Hacking-Domänen und Methodiken zu legen, um die Arbeit eines Ethical Hackers ausführen zu können.

Selbstverständlich werden alle Übungen innerhalb eines Schulungsnetzes durchgeführt, es wird kein reales Netzwerk angegriffen.
Sie werden nach dem Seminar verstehen, wie Perimeter-Verteidigung funktioniert, scannen und attackieren während des Seminars ihr Übungsnetzwerk um im Anschluss daran zu erkennen bzw. zu erlernen, welche Schritte notwendig sind, um ein System gegen Angriffe abzusichern.

Nach Abschluss des Trainings haben die Teilnehmer*innen Kenntnisse zu folgenden Themen:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking

- Cloud Computing
- Cryptography

Hinweis zu den Trainingszeiten:

- Theorie und Demos werden von Montag bis Freitag in der Zeit von 9:00-17:00 durchgearbeitet
- zusätzlich haben die Teilnehmer die Möglichkeit freiwillig in der Zeit von Montag bis Donnerstag 17:00-19:00 das erworbene Wissen mit iLabs zu vertiefen.

Zur Information: Das Ziel eines Seminars im Bereich Ethical Hacking und der erfolgreichen Abwehr von Angriffen auf Netzwerke besteht darin, die Kursteilnehmer ausschließlich zu Testzwecken mit Hacking Tools vertraut zu machen. Wir gehen davon aus, dass Sie die neu erworbenen Fähigkeiten keinesfalls für illegale oder böswillige Angriffe verwenden und diese auch keinesfalls einsetzen werden, um Computersysteme zu schädigen und so EC-Council im Hinblick auf den Einsatz bzw. Missbrauch dieser Tools, egal mit welcher Absicht, schadlos zu halten.

Assessment Test

Target Groups

- Information Security Analyst / Administrator*in
- Information Assurance (IA) Security Officer*in
- Information Security Manager / Specialist*in
- Information Systems Security Engineer / Manager*in
- Information Security Professionals / Officers

- Information Security / IT Auditors
- Risk / Threat / Vulnerability Analyst*in
- System Administrator*in
- Network Administrators and Engineer*in

Prior knowledge

ca. zwei Jahre Berufserfahrung in der IT-Sicherheit
Grundkenntnisse von Linux und/oder Unix sowie Erfahrungen mit den einschlägigen Protokollen des TCP/IP-Stacks sollten vorhanden sein
gute Betriebssystemkenntnisse von Microsoft Windows Client Systemen sowie Windows Server

Important information
Dieses Training behandelt die aktuelle Version CEHv12 und bereitet auf die Prüfung 312-50 CEH Exam vor. Testfragen: 125 Testdauer: 4 Stunden Testform: Multiple Choice Testanbieter: VUE bei ETC Wien oder Graz
Das Examen ist im Kurspreis inkludiert!

Dates & Options

Date	Duration	City	Offer	Price
08.07.2024-12.07.2024	5 days	Wien	Preis (Präsenz)	€3.995,-
08.07.2024-12.07.2024	5 days	Wien	Preis (Online)	€3.995,-
11.11.2024-15.11.2024	5 days	Wien	Preis (Präsenz)	€3.995,-
11.11.2024-15.11.2024	5 days	Wien	Preis (Online)	€3.995,-