CEHv13

Certified Ethical Hacker

Mit dem Kurs CEHv13 erhalten Sie Zugang zur weltweit ersten Ethical-Hacking-Zertifizierung, die von KI unterstützt wird. Durch die Integration von KI in alle fünf Phasen des Ethical Hacking ermöglicht Ihnen CEHv13 eine 40 % höhere Effizienz und eine Verdopplung Ihrer Produktivität bei Cybersecurity-Aufgaben.

Das einzigartige Konzept „Lernen, Zertifizieren, Engagieren und Wetteifern" führt Sie zur Beherrschung von Ethical Hacking. Sie sammeln praktische Erfahrungen in über 220 Übungen, über 550 Angriffstechniken und über 4.000 Tools und testen Ihre Fähigkeiten in globalen Capture the Flag (CTF)-Wettbewerben.

Mit 20 hochmodernen Modulen erwerben Sie die Kernkompetenzen, die Sie benötigen, um die Cybersicherheitslandschaft zu beherrschen. C|EH hält nicht nur Schritt - es ist führend und entwickelt sich mit den neuesten Betriebssystemen, Exploits, Tools und Hacking-Techniken weiter, um sicherzustellen, dass Sie der Zeit immer einen Schritt voraus sind.

Tauchen Sie ein in die Zukunft der Cybersicherheit mit einer Schulung, die KI in alle fünf Phasen des ethischen Hackings integriert, von der Aufklärung und dem Scannen bis hin zur Erlangung des Zugangs, der Aufrechterhaltung des Zugangs und dem Verwischen von Spuren. Sie werden die Macht der KI nutzen, um Ihre Hacking-Techniken zu verbessern und KI-Systeme zu stören - und so Ihre Effizienz in der Cybersicherheit zu verzehnfachen.

Bestätigen Sie Ihr Fachwissen mit einer 6-stündigen praktischen oder 4-stündigen wissensbasierten Prüfung. Erwerben Sie eine Top-Zertifizierung, die von U.S. DoD 8140, ANAB 17024 und NCSC anerkannt ist und den NICE 2.0- und NIST-Standards entspricht.

Weitere Informationen dazu finden Sie in unserer Zertifizierungsübersicht sowie in dieser C|EH Broschüre.

Kursinhalt
- Introduction to Ethical Hacking
- Foot Printing 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

Zielgruppe
- Informationssicherheitsanalysten und -spezialisten
- Informationssicherheitsmanager und -beauftragte
- Ingenieure und Manager für Informationssystemsicherheit
- Sicherheitsbeauftragte für Informationssicherung (IA)
- IT- und Informationssicherheitsauditoren
- Risiko-, Bedrohungs- und Schwachstellenanalysten
- Systemadministratoren
- Netzwerkadministratoren und -ingenieure

Voraussetzungen
Es gibt keine spezifischen Voraussetzungen für das C|EH-Programm, aber es wird mindestens 2 Jahre IT-Sicherheitserfahrung empfohlen, bevor Sie an einem C|EH-Trainingsprogramm und damit an diesem Kurs teilnehmen.

Kursziel
Erhöhen Sie Ihren Vorsprung als zertifizierter ethischer Hacker mit KI-Fähigkeiten.

- **Fortgeschrittenes Wissen**: Als KI-gestützter Certified Ethical Hacker verfügen Sie über fundierte Kenntnisse der Methoden des Ethical Hacking, ergänzt durch modernste KI-Techniken.
- **KI-Integration**: Sie werden KI in jeder Phase des Ethical Hacking effektiv integrieren, von der Erkundung und dem Scannen bis hin zur Erlangung und Aufrechterhaltung des Zugriffs und dem Verwischen Ihrer Spuren.
- **Automatisierung und Effizienz**: Sie nutzen KI, um Aufgaben zu automatisieren, die Effizienz zu steigern und ausgefeilte Bedrohungen zu erkennen, die bei herkömmlichen Methoden übersehen werden könnten.
- **Proaktive Verteidigung**: Mit KI sind Sie für die proaktive Suche nach Bedrohungen, die Erkennung von Anomalien und die vorausschauende Analyse gerüstet, um Cyberangriffe zu verhindern, bevor sie passieren.

Prüfung

Wenn Sie den Kurs abgeschlossen und bei EC-Council bewertet haben, erhalten Sie von uns ohne weitere Kosten einen Voucher für die Prüfung „Certified Ethical Hacker 312-50", die Sie im Nachgang in einem VUE Testcenter ablegen können.

CEHv13 Pro

Im Kurspreis ist die **CEHv13 Pro** Version enthalten, die folgendes beinhaltet:

- elektronische Kursunterlagen sowie die nächste Version der elektronischen Kursunterlagen
- Prüfungsvoucher
- 3x Prüfungswiederholungen
- 5x Ethical Hacking Videokurse
- 6 Monate Zugang zum offiziellen Labor
- CEH Engage

Weiterführende Informationen

Mit unserem CEH Kurs zum Certified Ethical Hacker – Alle Informationen zum CEHv13.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**ECCE**

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.

Training		**Preise zzgl. MwSt.**	
Termine in Deutschland		**5 Tage**	**€ 3.995,-**
Online Training		**5 Tage**	**€ 3.995,-**
Termin/Kursort		Kurssprache Deutsch	
19.05.-23.05.25	HY Frankfurt	22.09.-26.09.25	HY Frankfurt
19.05.-23.05.25	HY Online	22.09.-26.09.25	HY Online
30.06.-04.07.25	HY Hamburg	24.11.-28.11.25	HY München
30.06.-04.07.25	HY Online	24.11.-28.11.25	HY Online

CEHv13

EC-Council

Stand 08.04.2025

ExperTeach

Inhaltsverzeichnis

CEHv13 – Certified Ethical Hacker

Introduction to Ethical Hacking
Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Foot Printing and Reconnaissance
Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Scanning Networks
Learn different network scanning techniques and countermeasures.

Enumeration
Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

Vulnerability Analysis
Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.

System Hacking
Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Malware Threats
Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Sniffing
Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Social Engineering
Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Denial-of-Service
Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Session Hijacking
Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Evading IDS, Firewalls, and Honeypots
Get introduced to firewall, intrusion detection system (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Hacking Web Servers
Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hacking Web Applications
Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

SQL Injection
Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Hacking Wireless Networks
Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Hacking Mobile Platforms
Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

IoT and OT Hacking
Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Cloud Computing
Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

Cryptography
Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de