CEHv12

Certified Ethical Hacker

Bitte beachten Sie: *Für den C|EHv12 wurde ein neues Konzept umgesetzt, das aus den vier Stufen 1-Learn, 2-Certify, 3-Engage und 4-Complete besteht. Der unten beschriebene Kurs und die zugehörige Prüfung stehen für die Stufen 1-Learn bzw. 2-Certify. Weitere Informationen dazu finden Sie in unserer Zertifizierungsübersicht sowie in dieser C|EH Broschüre.*

Das C|EH® v12-Schulungsprogramm umfasst 20 Module, die verschiedene Technologien, Taktiken und Verfahren abdecken und angehenden ethischen Hackern das Kernwissen vermitteln, das sie benötigen, um in der Cybersicherheit erfolgreich zu sein.

Die 12. Version des C|EH® wird durch einen sorgfältig kuratierten Schulungsplan bereitgestellt, der sich normalerweise über fünf Tage erstreckt, und entwickelt sich weiter, um mit den neuesten Betriebssystemen, Exploits, Tools und Techniken Schritt zu halten.

Die im Schulungsprogramm behandelten Konzepte sind 50/50 zwischen wissensbasiertem Training und praktischer Anwendung durch unser Cyber-Angebot aufgeteilt. Jede in der Schulung besprochene Taktik wird durch Schritt-für-Schritt-Übungen unterstützt, die in einer virtualisierten Umgebung mit Live-Zielen, Live-Tools und anfälligen Systemen durchgeführt werden. Durch unsere Labortechnologie erhält jeder Teilnehmer umfassende praktische Übungen, um sein Wissen zu erlernen und anzuwenden.

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

Von diesem Kurs profitieren insbesondere Sicherheitsbeauftragte, Prüfer, Sicherheitsexperten, Websiteadministratoren sowie alle, die für die Sicherheit von Netzwerkinfrastrukturen zuständig sind.

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.

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.

CEHv12 Pro

Im Kurspreis ist die **CEHv12 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 CEHv12.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/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 CHF 4.395,-**
Online Training	**5 Tage CHF 4.395,-**

Termin/Kursort — Kurssprache Deutsch

17.06.-21.06.24	HY Hamburg	16.09.-20.09.24	HY Online
17.06.-21.06.24	HY Online	16.12.-20.12.24	HY Frankfurt
16.09.-20.09.24	HY Frankfurt	16.12.-20.12.24	HY Online

CEHv12

EC-Council

Stand 19.03.2024

ExperTeach

Inhaltsverzeichnis

CEHv12 – 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 AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch