EC-Council Certified Ethical Hacking (CEH)

ID CEH **Preis** CHF 5'500.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

- Prüfer für Informationssicherheit auf mittlerer Ebene
- Cybersecurity Auditor
- Sicherheitsbeauftragter
- IT-Sicherheitsadministrator
- Cyber Defense Analyst
- Analyst für Schwachstellenbewertung
- Warnung Analyst
- Analyst für Informationssicherheit 1
- Sicherheitsanalytiker L1
- Infosec-Sicherheitsadministrator
- Cybersecurity Analyst Stufe 1, Stufe 2 und Stufe 3
- Ingenieur für Netzwerksicherheit
- SOC-Sicherheitsanalytiker
- Sicherheitsanalytiker
- Netzwerktechniker
- Senior Sicherheitsberater
- Manager für Informationssicherheit
- Senior SOC-Analyst
- Lösungsarchitekt
- Berater für Cybersicherheit

Voraussetzungen

Um die EC-Council CEH Zertifizierungsprüfung ablegen zu können, hat der Kandidat zwei Möglichkeiten:

Besuchen Sie das offizielle Network Security Training von EC-Council:

Wenn ein Kandidat eine offizielle EC-Council-Schulung entweder in einem akkreditierten Schulungszentrum, über die iClass-Plattform oder an einer anerkannten akademischen Einrichtung absolviert hat, ist der Kandidat berechtigt, die entsprechende EC-Council-Prüfung abzulegen, ohne den Bewerbungsprozess zu durchlaufen.

Versuchen Sie die Prüfung ohne offizielles EC-Council Training:

Um zur EC-Council CEH-Prüfung zugelassen zu werden, ohne an einer offiziellen Netzwerksicherheitsschulung teilzunehmen, muss der Kandidat mindestens 2 Jahre Berufserfahrung im Bereich der Informationssicherheit haben. Wenn der Kandidat über die erforderliche Berufserfahrung verfügt, kann er ein Antragsformular zusammen mit US$?100.–, einer nicht erstattungsfähigen Gebühr, einreichen.

Kursziele

Das C|EH® v12-Programm hilft Ihnen, durch die praktische C|EH®-Praxisumgebung reale Erfahrungen im ethischen Hacken zu sammeln. Der C|EH® Engage stattet Sie mit den Fähigkeiten aus, die Sie brauchen, um zu beweisen, dass Sie das Zeug zu einem grossartigen ethischen Hacker haben. Neu in C|EH® v12 werden die Studenten ihre erste emulierte Ethical Hacking Übung absolvieren. Dieser 4-Phasen-Einsatz verlangt von den Teilnehmern kritisches Denken und das Testen der erworbenen Kenntnisse und Fähigkeiten, indem sie in jeder Phase eine Reihe von Flaggen erfassen und die Live-Anwendung von Fähigkeiten und Fertigkeiten in einer folgenlosen Umgebung durch EC-Councils neue Cyber Range demonstrieren. Nach Abschluss des Trainings und der praktischen Übungen können Sie mit dem C|EH® Engage alles Gelernte in einem simulierten Ethical Hacking Einsatz anwenden. Diese 4-teilige Sicherheitsprüfung gibt Ihnen die Möglichkeit, ein echtes ethisches Hacking von Anfang bis Ende gegen ein simuliertes Unternehmen durchzuführen. Mit unserem Capture-the-Flag-Stil werden Sie Ihren Einsatz wie folgt abschliessen Beantwortung von "Flaggen"-Fragen, während Sie vorankommen.

Your Mission

Egal, ob Sie zum ersten Mal dabei sind oder Ihre Fähigkeiten verfeinern, machen Sie sich bereit, Ihr Wissen über ethisches Hacken wie nie zuvor zu testen! Nachdem Sie in den praktischen Übungen geübt haben, ist es an der Zeit, Ihr Wissen anzuwenden, in die Rolle eines Hackers zu schlüpfen und die Schwachstellen in ABCDorg zu finden - alles in unserem C|EH® Engage (Übungsgelände).

Zielsetzungen:

Bewaffnet mit Ihrer Angriffsplattform, Parrot OS, und einer Fülle von Tools, die von Ethical Hackern verwendet werden, werden Sie sich auf eine 4-teilige Aufgabe einlassen, um die Sicherheitslage von ABCDorg zu bewerten. Verfolgen Sie den Prozess, üben Sie Ihre TTP und erleben Sie den Ernstfall in einer kontrollierten Umgebung ohne Konsequenzen - die ultimative Lernerfahrung, um Ihre Karriere als Ethical Hacker zu unterstützen! Jede Phase baut auf der letzten auf, während Sie durch Ihren ABCDorg-Einsatz fortschreiten.

PHASE 1 Bewertung der Anfälligkeit

- Fussdruck &
- Anerkennung
- Scannen
- Aufzählung
- Schwachstellenanalyse

PHASE 2 Zugang erhalten

- System Hacking
- Malware-Bedrohungen
- Schnüffeln
- Sozialtechnik
- Denial-of-Service

PHASE 3 Perimeter und Webanwendung ausnutzen

- Session Hijacking
- Umgehen von IDS
- Firewalls
- Honigtöpfe
- Hacken von Webservern
- Hacking von Webanwendungen
- SQL-Injektion

PHASE 4 Mobile, IoT, OT Betrieb

- Hacken von drahtlosen Netzwerken
- Hacken von mobilen Plattformen
- IoT-Hacking
- OT-Hacking
- Cloud Computing
- Kryptographie

Kursinhalt

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 im Bereich der Cybersicherheit erfolgreich zu sein. Die 12. Version des C|EH® wird in einem sorgfältig zusammengestellten Trainingsplan vermittelt, der sich in der Regel über fünf Tage erstreckt, und wird ständig weiterentwickelt, um mit den neuesten Betriebssystemen, Exploits, Tools und Techniken Schritt zu halten. Die im Trainingsprogramm behandelten Konzepte sind zu 50/50 zwischen wissensbasiertem Training und praktischer Anwendung in unserem Cyber-Bereich aufgeteilt. Jede im Training besprochene Taktik wird durch schrittweise Übungen in einer virtualisierten Umgebung mit Live-Zielen, Live-Tools und anfälligen Systemen unterstützt. Dank unserer Labortechnologie kann jeder Teilnehmer sein Wissen in einer umfassenden praktischen Übung erlernen und anwenden.

20 Module, die Ihnen helfen, die Grundlagen des Ethical Hacking zu beherrschen und sich auf die C|EH-Zertifizierungsprüfung vorzubereiten

Einführung in Ethical Hacking

Vermittlung der Grundlagen der wichtigsten Themen in der Welt der Informationssicherheit, einschliesslich der Grundlagen des Ethical Hacking, der Informationssicherheitskontrollen, der einschlägigen Gesetze und Standardverfahren.

Fussabdruck und Erkundung

Lernen Sie, wie Sie mit den neuesten Techniken und Tools Footprinting und Rekognoszierung durchführen, eine kritische Phase vor einem Angriff im ethischen Hacking-Prozess.

Scannen von Netzwerken

Lernen Sie verschiedene Netzwerk-Scan-Techniken und Gegenmassnahmen kennen.

Aufzählung

Lernen Sie verschiedene Enumerationstechniken, wie z. B. Border Gateway Protocol (BGP) und Network File Sharing (NFS) Exploits, und die dazugehörigen Gegenmassnahmen kennen.

Schwachstellenanalyse

Lernen Sie, wie Sie Sicherheitslücken im Netzwerk, in der Kommunikationsinfrastruktur und in den Endsystemen eines Unternehmens identifizieren können. Verschiedene Arten der Schwachstellenbewertung und Tools zur Schwachstellenbewertung.

System Hacking

Lernen Sie die verschiedenen System-Hacking-Methoden kennen, darunter Steganografie, Steganalyse-Angriffe und das Verwischen von Spuren, die zur Aufdeckung von System- und Netzwerkschwachstellen verwendet werden.

Malware-Bedrohungen

Lernen Sie verschiedene Arten von Malware (Trojaner, Viren, Würmer usw.), APT und dateilose Malware, Verfahren zur Malware-Analyse und Gegenmassnahmen für Malware.

Schnüffeln

Erfahren Sie mehr über Packet-Sniffing-Techniken und wie man sie einsetzt, um Schwachstellen im Netzwerk zu entdecken, sowie über Gegenmassnahmen zur Abwehr von Sniffing-Angriffen.

Sozialtechnik

Lernen Sie Social-Engineering-Konzepte und -Techniken kennen und erfahren Sie, wie Sie Diebstahlsversuche erkennen, Schwachstellen auf menschlicher Ebene prüfen und Gegenmassnahmen vorschlagen können.

Denial-of-Service

Lernen Sie verschiedene Denial of Service (DoS)- und Distributed DoS (DDoS)-Angriffstechniken sowie die Tools kennen, die zur Überprüfung eines Ziels und zur Entwicklung von DoS- und DDoS-Gegenmassnahmen und -Schutzmassnahmen verwendet werden.

Session Hijacking

Verstehen der verschiedenen Session-Hijacking-Techniken, mit denen Sitzungsverwaltung, Authentifizierung, Autorisierung und kryptografische Schwachstellen auf Netzwerkebene aufgedeckt werden, sowie der damit verbundenen Gegenmassnahmen.

Umgehen von IDS, Firewalls und Honeypots

Sie erhalten eine Einführung in die Techniken zur Umgehung von Firewalls, Intrusion Detection Systemen (IDS) und Honeypots sowie in die Tools, die zur Überprüfung eines Netzwerks auf Schwachstellen verwendet werden, und in Gegenmassnahmen.

Hacken von Webservern

Erfahren Sie mehr über Angriffe auf Webserver, einschliesslich einer umfassenden Angriffsmethodik zur Prüfung von Schwachstellen in Webserver-Infrastrukturen und Gegenmassnahmen.

Hacking von Webanwendungen

Erfahren Sie mehr über Angriffe auf Webanwendungen, einschliesslich einer umfassenden Methodik zum Hacken von Webanwendungen, um Schwachstellen in Webanwendungen und Gegenmassnahmen zu prüfen.

SQL-Einschleusung

Erfahren Sie mehr über SQL-Injection-Angriffe, Umgehungstechniken und SQL-Injection-Gegenmassnahmen.

Hacken von drahtlosen Netzwerken

Verstehen verschiedener Arten von Drahtlostechnologien, einschliesslich Verschlüsselung, Bedrohungen, Hacking-Methoden, Hacking-Tools, Wi-Fi-Sicherheitstools und Gegenmassnahmen.

Hacken von mobilen Plattformen

Lernen Sie Angriffsvektoren für mobile Plattformen, Android- und iOS-Hacking, Verwaltung mobiler Geräte, Richtlinien für mobile Sicherheit und Sicherheitstools.

IoT-Hacking

Lernen Sie verschiedene Arten von IoT- und OT-Angriffen, Hacking-Methoden, Hacking-Tools und Gegenmassnahmen kennen.

Cloud Computing

Lernen Sie verschiedene Cloud-Computing-Konzepte kennen, z. B. Container-Technologien und serverloses Computing, verschiedene Cloud-Computing-Bedrohungen, Angriffe, Hacking-Methoden sowie Cloud-Sicherheitstechniken und -Tools.

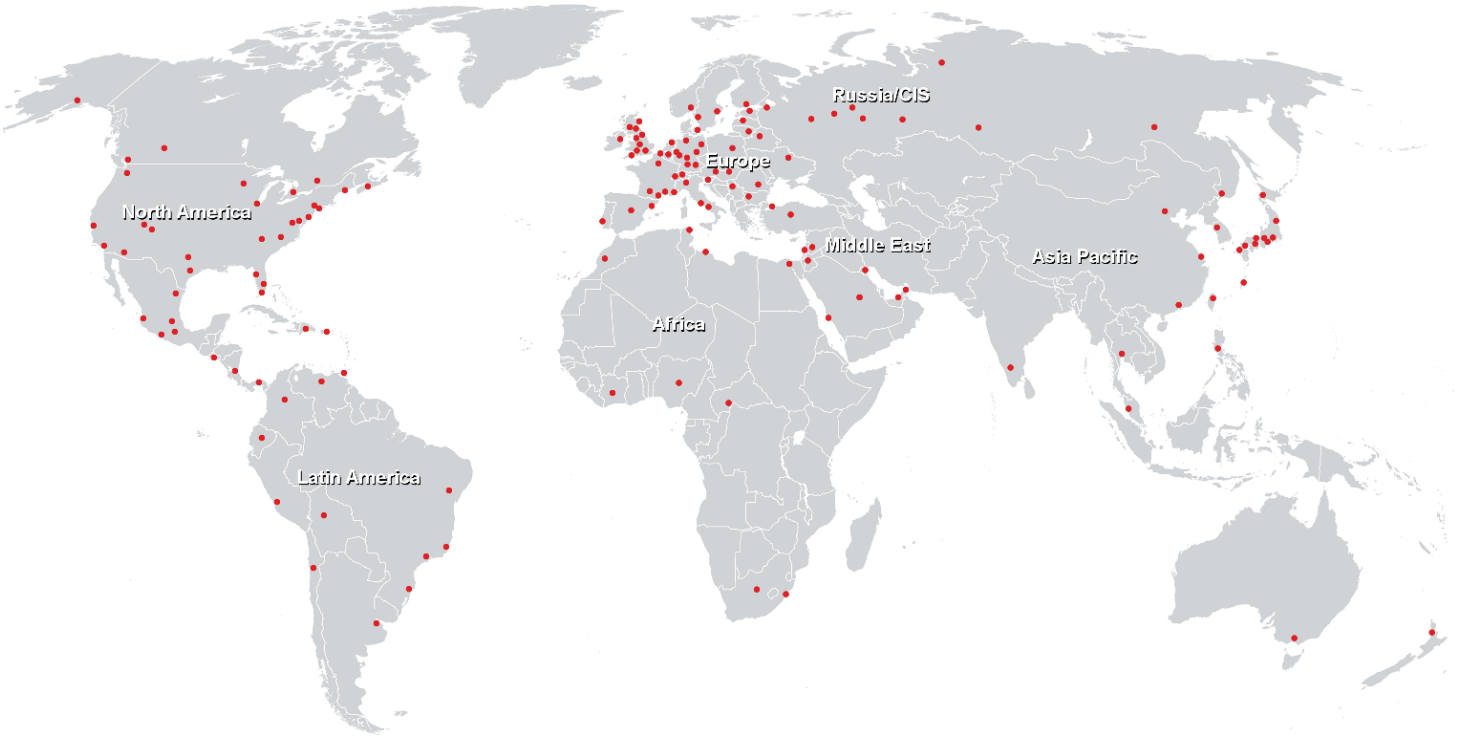
Session Hijacking

Verstehen der verschiedenen Session-Hijacking-Techniken, mit denen Sitzungsverwaltung, Authentifizierung, Autorisierung und kryptografische Schwachstellen auf Netzwerkebene aufgedeckt

werden, sowie der damit verbundenen Gegenmassnahmen.

EC-Council Certified Ethical Hacking (CEH)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch