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
- Analyst für Informationssicherheit 1
- Infosec-Sicherheitsadministrator
- Cybersecurity-Analyst (Stufe 1, Stufe 2 und Stufe 3)
- Ingenieur für Netzwerksicherheit
- SOC-Sicherheitsanalytiker
- Netzwerktechniker
- Senior Sicherheitsberater
- Manager für Informationssicherheit
- Senior SOC-Analyst
- Lösungsarchitekt
- Berater für Cybersicherheit
- Cyber Defense Analyst
- Analyst für Schwachstellenbewertung
- Warnung Analyst
- All-Source-Analyst
- Cyber Defense Incident Responder
- Spezialist für Forschung und Entwicklung
- Senior Cloud Security Analyst
- Risikomanagement für Dritte:
- Analyst für Bedrohungsjagd
- Penetrationstester
- Ausbilder für Cybersecurity
- Red Team Spezialist
- Beauftragter für Datenschutz und Privatsphäre
- SOAR-Ingenieur
- AI-Sicherheitsingenieur
- Senior IAM-Ingenieur
- PCI-Sicherheitsberater
- Analyst für Ausbeutung (EA)
- Ingenieur/Analytiker für Zero-Trust-Lösungen
- Kryptographie-Ingenieur
- AI/ML Sicherheitsingenieur
- Sicherheitsspezialist für maschinelles Lernen
- AI-Penetrationstester
- KI/ML-Sicherheitsberater
- Berater für Krypto-Sicherheit

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

Verstärken Sie Ihren Vorsprung als zertifizierter Ethical Hacker mit KI-Fähigkeiten:

Fortgeschrittenes Wissen: Als KI-gestützter Certified Ethical Hacker verfügen Sie über fundiertes Wissen über ethische Hacking-Methoden, ergänzt durch modernste KI-Techniken.
KI-Integration: Sie werden KI in jeder Phase des ethischen Hackings effektiv integrieren, von der Aufklärung und dem Scannen bis hin zur Erlangung und Aufrechterhaltung des Zugriffs und dem Verwischen Ihrer Spuren.
Automatisierung und Effizienz: Sie werden KI nutzen, um Aufgaben zu automatisieren, die Effizienz zu steigern und ausgeklügelte Bedrohungen zu erkennen, die mit herkömmlichen Methoden übersehen werden könnten.
Proaktive Verteidigung: Mit KI sind Sie für die proaktive Suche

nach Bedrohungen, die Erkennung von Anomalien und prädiktive Analysen gerüstet, um Cyberangriffe zu verhindern, bevor sie passieren.

Wie C|EH v13 Powered by AI Ihre Cybersecurity-Karriere neu definiert

- Erleben Sie das weltweit erste KI-gestützte Ethical-Hacking-Programm
- Beherrschen Sie die fünf Phasen des ethischen Hackings mit integrierter KI
- Erzielen Sie 40 % Effizienz und verdoppeln Sie Ihre Produktivität mit KI-gesteuerten Fähigkeiten
- Lernen Sie, wie man KI-Systeme hackt
- Werden Sie ein KI-Experte mit praktischen Übungen zum Üben von KI-Fähigkeiten
- Beherrschen der neuesten fortschrittlichen Angriffstechniken, Trends und Gegenmassnahmen
- Sammeln Sie praktische Erfahrungen mit 221 Laboren, Angriffsvektoren und Hacking-Tools
- Erfahrung mit über 550 Angriffstechniken
- Entdecken Sie mehr als 4.000 kommerzielle Hacker- und Sicherheitstools
- Folgen Sie einem einzigartigen Vier-Phasen-Lernkonzept: Lernen, Zertifizieren, Engagieren, Bewerben
- Üben Sie das Hacken einer echten Organisation in einem Live-Cyber-Bereich
- Validieren Sie Ihre Fähigkeiten in einer 6-stündigen praktischen Prüfung oder einer 4-stündigen wissensbasierten Prüfung
- Messen Sie sich mit Hackern in globalen CTF-Wettbewerben zu den neuesten Themen
- Erwerben Sie die weltweit anerkannte Ethical-Hacking-Zertifizierung Nr. 1
- Erlangung einer Zertifizierung, die von U.S. DoD 8140, ANAB 17024 und NCSC genehmigt und akkreditiert ist
- Erfüllung der strengen Standards von NICE 2.0 und des NIST Framework
- Sie erhalten die Möglichkeit, von Top-Organisationen angestellt zu werden, darunter Fortune-500-Unternehmen, Regierungsbehörden und Firmen des Privatsektors.

Kursinhalt

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.

CEH v13 ist nicht nur eine Zertifizierung, sondern ein umfassendes Erlebnis. CEH kombiniert ein umfassendes, wissensbasiertes Training mit praxisnahen Übungen, um eine umfassende Lernerfahrung zu gewährleisten. Sie werden in einer kontrollierten Umgebung mit realen Zielen, Tools und anfälligen Systemen arbeiten und so reale Fähigkeiten erwerben, die Sie befähigen, Ihr Fachwissen in jedem Szenario selbstbewusst anzuwenden. Machen Sie sich bereit, die Art und Weise, wie Sie die digitale Welt hacken und schützen, zu verändern!

Einführung in Ethical Hacking

Lernen Sie die Grundlagen und Schlüsselthemen der Informationssicherheit kennen, einschliesslich der Grundlagen von Ethical Hacking, Informationssicherheitskontrollen, relevanten Gesetzen und Standardverfahren.

Footprinting und Erkundung

Lernen Sie, wie man die neuesten Techniken und Tools für Footprinting und Reconnaissance einsetzt, eine kritische Phase vor einem Angriff beim Ethical Hacking.

Scannen von Netzwerken

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

Aufzählung

Lernen Sie verschiedene Enumerationstechniken kennen, einschliesslich Border Gateway Protocol (BGP) und Network File Sharing (NFS) Exploits und zugehörige Gegenmassnahmen.

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 werden ebenfalls behandelt.

System Hacking

Lernen Sie die verschiedenen System-Hacking-Methoden kennen, die zur Aufdeckung von System- und Netzwerkschwachstellen verwendet werden, einschliesslich Steganografie, Steganalyse-Angriffe und wie man Spuren verwischt.

Malware-Bedrohungen

Lernen Sie verschiedene Arten von Malware (Trojaner, Viren, Würmer usw.), APT und dateilose Malware, Malware-Analyseverfahren und Malware-Gegenmassnahmen kennen.

Schnüffeln

Erfahren Sie mehr über Packet-Sniffing-Techniken und deren Einsatz zur Aufdeckung von Netzwerkschwachstellen 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

Lernen Sie die verschiedenen Session-Hijacking-Techniken kennen, mit denen Sitzungsverwaltung, Authentifizierung, Autorisierung und kryptografische Schwachstellen auf Netzwerkebene aufgedeckt und entsprechende Gegenmassnahmen ergriffen werden können.

Umgehen von IDS, Firewalls und Honeypots

Erfahren Sie mehr über Firewalls, Intrusion Detection Systems (IDS) und Techniken zur Umgehung von Honeypots sowie über die Tools, mit denen ein Netzwerk auf Schwachstellen überprüft werden kann, und über 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 Hacking-Methode zur Überprüfung von Schwachstellen in Webanwendungen und Gegenmassnahmen.

SQL-Einschleusung

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

Hacken von drahtlosen Netzwerken

Erfahren Sie mehr über verschiedene Arten der Verschlüsselung, Bedrohungen, Hacking-Methoden, Hacking-Tools, Sicherheitstools und Gegenmassnahmen für drahtlose Netzwerke.

Hacken von mobilen Plattformen

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

IoT-Hacking

Lernen Sie verschiedene Arten von Angriffen auf das Internet der Dinge (IoT) und die Betriebstechnologie (OT), Hacking-Methoden, Hacking-Tools und Gegenmassnahmen kennen.

Cloud Computing

Lernen Sie verschiedene Cloud-Computing-Konzepte, wie Container-Technologien und serverloses Computing, verschiedene Cloud-Computing-Bedrohungen, Angriffe, Hacking-Methoden sowie Cloud-Sicherheitstechniken und -tools.

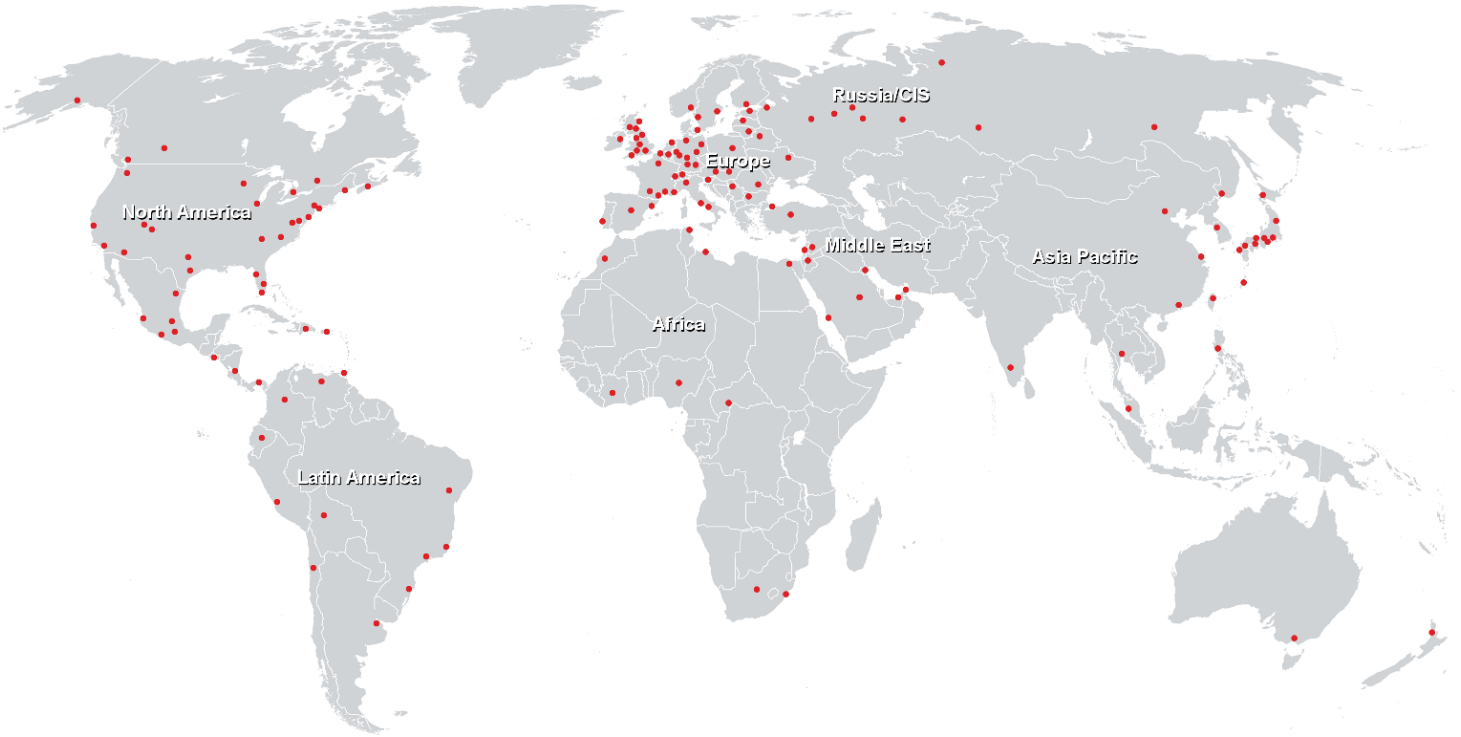
Kryptographie

EC-Council Certified Ethical Hacking (CEH)

Erfahren Sie mehr über Verschlüsselungsalgorithmen, Kryptographie-Tools, Public Key Infrastructure (PKI), E-Mail-Verschlüsselung, Festplattenverschlüsselung, Kryptographie-Angriffe und Kryptoanalysetools.

EC-Council Certified Ethical Hacking (CEH)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

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

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