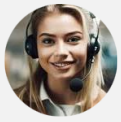
EC-Council Certified Ethical Hacker v13 (CEH v13)

Der weltweit fortschrittlichste Kurs zum ethischen Hacking

Kurs ID: ECCEH Dauer: 1 Tag ab: € 3.950,00 zzgl. MwSt.

Der EC-Council Certified Ethical Hacker v13 (CEH v13) vermittelt ein umfassendes Verständnis der Phasen des ethischen Hackings, der verschiedenen Angriffsvektoren und der präventiven Gegenmaßnahmen. Du lernst, wie Hacker denken und handeln, damit du besser in der Lage bist, deine Sicherheitsinfrastruktur einzurichten und Angriffe abzuwehren. Durch die Vermittlung von Kenntnissen über Systemschwächen und -verwundbarkeiten hilft der CEH-Kurs den Teilnehmern, ihre Organisationen zu schützen und ihre Sicherheitskontrollen zu verstärken, um das Risiko eines bösartigen Angriffs zu minimieren. In diesem Kurs Certified Ethical Hacker v13 (CEH v13) erlangen Sie fundiertes Wissen in 20 Modulen, die die neuesten Technologien, Taktiken und Verfahren im Bereich Ethical Hacking abdecken. Als angehende/r Ethical Hacker erwerben Sie die wesentlichen Kompetenzen, die für den Erfolg in der Cybersicherheit erforderlich sind.



Sie haben Fragen?

+43 50 4510-0
Mo-Do 8-17 Uhr, Fr. 8-14 Uhr

Kursdetails

tecTrain ist ein zertifiziertes Schulungsinstitut nach Ö-Cert, dem Qualitätsrahmen für die Erwachsenenbildung in Österreich

Kursinhalte

- **Module 01: Introduction to Ethical Hacking**
  - Information Security Overview
  - Hacking Concepts

- Ethical Hacking Concepts
- Hacking Methodologies and Frameworks
- Information Security Controls
- Information Security Laws and Standards

- **Module 02: Footprinting and Reconnaissance**
  - Footprinting Concepts
  - Footprinting through Search Engines
  - Footprinting through Internet Research Services
  - Footprinting through Social Networking Sites
  - Whois Footprinting
  - DNS Footprinting
  - Network and Email Footprinting
  - Footprinting through Social Engineering
  - Footprinting Tasks using Advanced Tools and AI
  - Footprinting Countermeasures
- **Module 03: Scanning Networks**
  - Network Scanning Concepts
  - Scanning Tools
  - Host Discovery
  - Port and Service Discovery
  - OS Discovery (Banner Grabbing/OS Fingerprinting)
  - Scanning Beyond IDS and Firewall
  - Source Port Manipulation
  - Network Scanning Countermeasures
- **Module 04: Enumeration**
  - Enumeration Concepts
  - NetBIOS Enumeration
  - SNMP Enumeration
  - LDAP Enumeration
  - NTP and NFS Enumeration
  - SMTP and DNS Enumeration
  - Other Enumeration Techniques
  - Enumeration Countermeasures
- **Module 05: Vulnerability Analysis**
  - Vulnerability Assessment Concepts
  - Vulnerability Assessment Tools
  - Vulnerability Assessment Reports
- **Module 06: System Hacking**
  - Gaining Access
  - Escalating Privileges
  - Maintaining Access
  - Clearing Logs

- **Module 07: Malware Threats**
  - Malware Concepts
  - APT Concepts
  - Trojan Concepts
  - Virus and Worm Concepts
  - Fileless Malware Concepts
  - AI-based Malware Concepts
  - Malware Analysis
  - Malware Countermeasures
  - Anti-Malware Software
- **Module 08: Sniffing**
  - Sniffing Concepts
  - Sniffing Technique: MAC Attacks
  - Sniffing Technique: DHCP Attacks
  - Sniffing Technique: ARP Poisoning
  - Sniffing Technique: Spoofing Attacks
  - Sniffing Technique: DNS Poisoning
  - Sniffing Tools
  - Sniffing Countermeasures
- **Module 09: Social Engineering**
  - Social Engineering Concepts
  - Human-based Social Engineering Techniques
  - Computer-based Social Engineering Techniques
  - Mobile-based Social Engineering Techniques
  - Social Engineering Countermeasures
- **Module 10: Denial-of-Service**
  - DoS/DDoS Concepts
  - Botnets
  - DDoS Case Study
  - DoS/DDoS Attack Techniques
  - DoS/DDoS Attack Countermeasures
- **Module 11: Session Hijacking**
  - Session Hijacking Concepts
  - Application-Level Session Hijacking
  - Network-Level Session Hijacking
  - Session Hijacking Tools
  - Session Hijacking Countermeasures
- **Module 12: Evading IDS, Firewalls, and Honeypots**
  - IDS, IPS, and Firewall Concepts
  - IDS, IPS, and Firewall Solutions
  - Evading IDS/Firewalls
  - Evading NAC and Endpoint Security

    - IDS/Firewall Evading Tools
    - Honeypot Concepts
    - IDS/Firewall Evasion Countermeasures
- **Module 13: Hacking Web Servers**
    - Web Server Concepts
    - Web Server Attacks
    - Web Server Attack Methodology
    - Web Server Attack Countermeasures
    - Patch Management

Voraussetzungen

- Serverkenntnisse Windows sowie Linux-Kenntnisse
- Grundkenntnisse Netzwerk sowie zum TCP/IP Protokoll
- Vorkenntnisse im Bereich Security sind optional, aber von Vorteil

Zielgruppe

- Systemadministratoren und Netzwerkadministratoren
- Fachleute / Beauftragte für Informationssicherheit
- Risiko- / Bedrohungs- / Sicherheitslücken-Analyst
- Fach- und Führungskräfte aus der IT-Sicherheit
- IT-Auditoren
- IT-Sicherheitsberater

Unser CEH-v13 Kurs wird ausschließlich von zertifizierten und erfahrenen EC-Council Trainern in Kooperation mit einem akkreditierten EC-Council Training Center geleitet, der dir die Details und Feinheiten des Ethical Hackings vermittelt.

Abschluß

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.