Certified Ethical Hacker Master (CEHM)

Description

Strengthen Your Skills with the Certified Ethical Hacker Master (CEHM) Certification

The Certified Ethical Hacker Master (CEHM) certification is aimed at IT security experts who have already obtained the prestigious CEH V12 certification. This advanced training program deepens your ethical hacking skills through real-world attack scenarios. You will have access to over 100 labs to refine your cybersecurity attack and defense techniques. This course also prepares you for the challenging CEH Master exam, which rigorously tests your ability to identify vulnerabilities and secure systems. The CEHM training is designed for professionals aiming to stand out in the field of cybersecurity.

A Certification for IT Security Experts

By taking this course, you will master advanced tools and techniques to conduct penetration tests, analyze security flaws, and secure networks. With a hands-on approach and access to cutting-edge tools, you'll be ready to face the current challenges in information systems security.

Course Content
Module 1: Introduction to Ethical Hacking

- Information security elements
- The Cyber Kill Chain methodology
- MITRE ATT&CK® knowledge base
- Types of hackers
- Ethical hacking
- Information Assurance (IA)
- Risk management
- Incident management
- PCI DSS, HIPPA, SOX, and GDPR regulations

Module 2: Footprinting and Reconnaissance

- Perform footprint analysis of the target network using search engines, web services, and social media sites
- Gather website, email, whois, DNS, and network footprints on the target network

Module 3: Network Scanning

- Detect hosts, ports, services, and operating systems on the target network
- Conduct network scans beyond IDS and firewalls

Module 4: Enumeration Phase

- Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP enumeration

Module 5: Vulnerability Analysis

- Perform vulnerability research using vulnerability assessment systems and databases
- Conduct vulnerability assessments using various vulnerability assessment tools

Module 6: System Hacking

- Execute dynamic online attacks to discover a system’s password
- Perform buffer overflow attacks to access a remote system
- Escalate permissions using privilege escalation tools
- Escalate privileges on a Linux machine
- Hide data using steganography
- Delete Windows and Linux logs using various tools
- Hide artifacts in Windows and Linux

Module 7: Malware Threats

- Take control of a victim machine using a Trojan horse
- Infect a target system using a virus
- Perform static and dynamic malware analysis

Module 8: Sniffing Attacks

- Execute MAC Flooding, ARP Poisoning, MITM, and DHCP Starvation attacks
- Spoof the MAC address of a Linux machine
- Perform network sniffing using various tools
- Detect poisoning attacks in a switched network

Module 9: Social Engineering

- Conduct social engineering using various techniques
- Spoof the MAC address of a Linux machine
- Detect phishing attacks
- Audit a company's security to detect phishing attacks

Module 10: Denial of Service (DoS) Attacks

- Conduct DoS and DDoS attacks on a target host
- Detect and respond to DoS and DDoS attacks

Module 11: Session Hijacking

- Perform session hijacking using multiple tools
- Detect session hijacking

Module 12: Bypassing IDS, Firewalls, and Honeypots

- Bypass a Windows firewall
- Bypass firewall rules using tunnels
- Bypass antivirus systems

Module 13: Web Server Hacking

- Perform reconnaissance on a web server using multiple tools
- Enumerate information about a web server
- Decrypt FTP credentials using dictionary attack methods

Module 14: Web Application Hacking

- Perform web application reconnaissance using multiple tools
- Create a web spider
- Perform a web application vulnerability scan
- Execute a brute force attack
- Conduct a Cross-site Request Forgery (CSRF) attack
- Identify XSS vulnerabilities in web applications
- Detect vulnerabilities in web applications using various security tools

Module 15: SQL Injections

- Perform an SQL injection attack against MSSQL to extract databases
- Detect SQL injection vulnerabilities using multiple tools

Module 16: Wireless Network Hacking

- Footprint a wireless network
- Analyze wireless communications
- Hack a WEP, WPA, and WPA2 network
- Create a rogue access point to capture data packets

Module 17: Mobile Device Hacking

- Hack an Android device via binary payload creation
- Exploit the Android platform via ADB
- Hack an Android device by creating an APK file
- Secure Android devices using various Android security tools

Module 18: IoT and OT Hacking

- Collect information using online footprinting tools
- Capture and analyze data streams on IoT devices

Module 19: Cloud Computing

- Enumerate S3 buckets using multiple tools
- Exploit open S3 buckets
- Escalate an IAM user’s privileges by exploiting poorly defined user policies

Module 20: Cryptography

- Calculate MD5 hashes
- Encrypt files and text messages

- Create and use self-signed certificates
- Encrypt email and disk
- Perform cryptographic analysis using multiple tools

Documentation

- Digital course material included

Exam

- This course prepares to the Certified Ethical Hacker (Practical) certification
- In order to receive the Certified Ethical Hacker (Practical) certification, learners must pass two exams: 312-50 (ECC EXAM).
- Number of questions: 125
- Duration: 4 hours
- If you wish to take the exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- Cybersecurity Analysts
- Internal and External Auditors
- Network and Telecom Administrators
- System Administrators
- Network and Telecom Engineers
- System Engineers

Prerequisites

- Strong knowledge of cybersecurity concepts
- Understanding of ethical hacking basics (CEH V12 required)
- Mastery of network scanning and vulnerability analysis techniques
- Proficiency with penetration testing tools
- Familiarity with network protocols (TCP/IP, DNS, HTTP)

Objectives

- Master advanced ethical hacking techniques
- Identify and exploit vulnerabilities in target systems
- Conduct DDoS attacks and malware analysis
- Perform penetration tests on wireless and mobile networks
- Secure web servers and web applications
- Exploit security flaws in cloud environments
- Pass the CEH Master exam and earn certification

Description
Certified Ethical Hacker Master (CEHM) training
Niveau
Avancé
Classroom Registration Price (CHF)
5900
Virtual Classroom Registration Price (CHF)
5650
Duration (in Days)

5
Reference
CEHM