Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

EC-Council

The Certified Ethical Hacker (CEHv13)

CODE:	LENGTH:	PRICE:
ECC_CEH13	40 Hours (5 days)	kr39,900.00

Description

Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges.
Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:
Advanced Knowledge: As an AI-powered Certified Ethical Hacker, you'll possess in-depth knowledge of ethical hacking methodologies, enhanced with cutting-edge AI techniques.
AI Integration: You'll effectively integrate AI across every phase of ethical hacking, from reconnaissance and scanning to gaining access, maintaining access, and covering your tracks.
Automation and Efficiency: You'll leverage AI to automate tasks, boost efficiency, and detect sophisticated threats that traditional methods might overlook.
Proactive Defense: With AI at your disposal, you'll be equipped for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks before they happen.
In C|EH v13, you will not only master AI-driven cybersecurity but also learn to hack AI systems. This comprehensive training equips you with cutting-edge AI-driven skills, enhancing your ability to execute cybersecurity tasks with up to 40% greater efficiency, while significantly boosting your productivity.
The C|EH v13 is a specialized, one-of-akind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry. This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, handson lab and practice range experience.
New Focus Areas and Trends in C|EH v13
Trained to think outside the box with a hacker's mindset, individuals who pursue the Certified Ethical Hacker (C|EH) v13 thoroughly explore top OWASP attacks, active directory breaches, the vulnerability of traditional encryption to quantum computing, the growing ransomware threat, and other emerging risks, equipping learners with strategies to implement zero trust architecture and other cybersecurity measures. C|EH v13 is comprehensive with the latest knowledge, providing cybersecurity professionals with the skills, tools, techniques, and strategies to defend against trending, modern, and complex cyber threats effectively and efficiently.
Active Directory Attacks
Ransomware Attacks and Mitigation
AI and Machine Learning in Cybersecurity
Critical Infrastructure Vulnerabilities
Extended Detection and Response (XDR)
Quantum Computing Risks and Attacks
Post-Quantum Cryptography
Deepfake Threats
Zero Trust Architecture
Cloud Security
IoT Security Challenges
Critical Infrastructure Vulnerabilities

Objectives

Armed with your attack platform (Parrot OS) and a plethora of tools used by ethical hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP, and experience the real thing in a controlled environment with no consequences. It's the ultimate learning experience to support your career as an ethical hacker! Each phase builds on the last as you progress through your ABCDorg engagement.
Phase 1
Vulnerability assessment:

Footpringing & Reconnaissance
Scanning
Enumeration
Vulnerability Analysis
Phase 2
Gaining access:
System Hacking
Malware Threats
Sniffing
Social Engineering
Denial-of-Service
Phase 4
Mobile, IoT, OT Exploitation:
Hacking Wireless
Networks
Hacking Mobile
Platforms
IoT Hacking
OT Hacking
Cloud Computing
Cryptography
Phase 3
Perimeter and Web App Exploitation:
Session Hijacking
Evading IDS
Firewalls
Honeypots
Hacking Web
Servers
Hacking Web
Applications
SQL Injection

Prerequisites

You need only an internet connection, and can compete through your browser.
We provide the attack platform, targets and all the required tools. You bring the skills to win!

Programme

Module 01
Introduction to Ethical Hacking
Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Module 02
Footprinting and Reconnaissance
Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking.
Module 03
Scanning Networks
Learn different network scanning techniques and countermeasures.
Module 04
Enumeration
Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
Module 05
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 are also included.
Module 06
System Hacking
Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
Module 07
Malware Threats
Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

Module 08
Sniffing
Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.
Module 09
Social Engineering
Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
Module 10
Denial-of-Service
Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
Module 11
Session Hijacking
Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
Module 12
Evading IDS, Firewalls, and Honeypots
Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
Module 13
Hacking Web Servers
Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.
Module 14
Hacking Web Applications
Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.
Module 15
SQL Injection
Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
Module 16
Hacking Wireless Networks
Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.
Module 17
Hacking Mobile Platforms
Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
Module 18
IoT Hacking
Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
Module 19
Cloud Computing
Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.
Module 20
Cryptography
Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

Test and Certification

Knowledge Exam
4 Hours
Multiple-Choice Exam
Skills Exam
6 Hours
20 Practical Challenges
CEH Knowledge-Based Exam
The CEH knowledge-based exam is a four-hour exam with 125 multiple-choice questions. It will test your skills in information security threats, attack vectors, attack detection, attack prevention, procedures, methodologies, and more! This exam is recognized worldwide as the original and most trusted tactical cybersecurity certification exam.
CEH Practical Exam

The CEH Practical exam is the world's first ethical hacking practical exam to have ANAB and US DoD approval. The CEH Practical is a 6-hour, 100% hands-on exam delivered in our Cyber Range that requires you to demonstrate the skills and abilities of ethical hacking techniques.
In the CEH Practical, you have a limited time to complete 20 challenges that test your proficiency in a performance-based cyber range.
This exam is NOT a simulation and incorporates a live corporate network of VMs and applications with solutions to uncover vulnerabilities.

CEH Master

Upon successfully completing both the C|EH Knowledge-based Exam and the C|EH Practical Exam, the C|EH (Master) designation is awarded. A C|EH (Master) signifies a high level of proficiency in ethical hacking knowledge, skills, and abilities, with a total of 6 hours of testing to prove their competency. The top 10 performers in both the C|EH Knowledge-based Exam and C|EH Practical Exam are featured on the C|EH Master Global Ethical Hacking Leader Board.

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.