Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Certified Ethical Hacker (CEHv11)

CODE:	LENGTH:	PRICE:
ECC_CEH11	40 Hours (5 days)	€3,395.00

Description

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."
Certified Ethical Hacker (CEH) Version 11 Update:
CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks.
Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.
CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure. In its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

Objectives

• Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
• Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
• Network scanning techniques and scanning countermeasures.• Enumeration techniques and enumeration countermeasures.
• Vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems.
• System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
• Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
• Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
• Social engineering techniques and how to identify theft attacks to audit humanlevel vulnerabilities and suggest social engineering countermeasures.
• DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
• Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
• Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
• Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
• SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
• Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
• Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
• Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
• Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
• Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
• Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
• Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Audience

• Information Security Analyst / Administrator
• Information Assurance (IA) Security Officer
• Information Security Manager / Specialist
• Information Systems Security Engineer / Manager
• Information Security Professionals / Officers
• Information Security / IT Auditors
• Risk / Threat/Vulnerability Analyst
• System Administrators
• Network Administrators and Engineers

Programme

Module 01 Introduction to Ethical Hacking**Module 02** Footprinting and Reconnaissance**Module 03** Scanning Networks
Module 04 Enumeration**Module 05** Vulnerability Analysis**Module 06** System Hacking**Module 07** Malware Threats
Module 08 Sniffing**Module 09** Social Engineering**Module 10** Denial-of-Service**Module 11** Session Hijacking
Module 12 Evading IDS, Firewalls, and Honeypots**Module 13** Hacking Web Servers**Module 14** Hacking Web Applications
Module 15 SQL Injection**Module 16** Hacking Wireless Networks**Module 17** Hacking Mobile Platforms
Module 18 IoT and OT Hacking**Module 19** Cloud Computing**Module 20** Cryptography

Test and Certification

To be eligible to challenge the EC-Council CEH certification examination, the candidate has two options:
Attend Official Network Security Training by EC-Council:
If a candidate has completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.
Attempt the Exam without Official EC-Council Training:
In order to be considered for the EC-Council CEH exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with USD 100.00, a non-refundable fee

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.