Certified Ethical Hacker

Duration: 5 days Price: € 3900

Open Schedule

Audience Course Certified Ethical Hacker

The course Certified Ethical Hacker is intended for aspiring cybersecurity professionals who want to learn techniques to find weaknesses in systems before criminals do.

Prerequisites Course Certified Ethical Hacker

General knowledge of computer systems and security problems is sufficient.

Execution of Training Certified Ethical Hacker

In the course Certified Ethical Hacker participants learn the tools and techniques to investigate networks and systems for security problems through hands-on exercises.

Certification course Certified Ethical Hacker

After successfully completing the training, participants will receive a certificate of participation in the course Certified Ethical Hacker. The course meets the requirements for the Certified Ethical Hacker exam of the EC-Council. After the course one can pass this exam with the knowledge gained.

Content Course Certified Ethical Hacker

The course Certified Ethical Hacker covers the basics of information security, the principles of ethical hacking, relevant laws and standard procedures. Afterwards one can certify as Certified Ethical Hacker by taking the exam.

Foot Printing and Reconnaissance

Learn to use the latest techniques to perform foot printing and reconnaissance, a critical phase of the ethical hacking process.

Scanning Networks

Learn network scanning techniques. Learn various enumeration techniques, such as BGP and NFS exploits.

System Hacking

Learn system hacking methodologies like steganography, steganalysis attacks and tracks—used to discover vulnerabilities.

Malware Threats

Learn different types of malware (Trojan, virus, etc.), APT and fileless malware, malware analysis procedure.

Sniffing

Learn to use packet-sniffing techniques to discover network vulnerabilities and to defend against sniffing attacks.

Social Engineering

Learn social engineering techniques, including identifying theft attempts and audit human-level vulnerabilities.

Denial of Service

Learn about different Denial of Service attack techniques, as well as the tools used to audit and protect a target.

Session Hijacking and SQL Injection

Understand session hijacking techniques to discover network-level session management and SQL Injection attacks.

Evading IDS, Firewalls, and Cryptography

Get introduced to firewall, intrusion detection system (IDS), and cryptography attacks.

Hacking Web Servers

Learn about web server attacks, including attack methodology used to audit vulnerabilities in web server infrastructures.

Hacking Wireless Networks

Understand different types of wireless technologies, including encryption and Wi-Fi security tools.

Hacking Mobile Platforms and IoT

Learn Mobile platform attack vectors, IoT and OT attacks, mobile device management and mobile security guidelines.

Cloud Computing

Learn cloud computing concepts and threats, attacks, hacking methodology and cloud security techniques and tools.

Modules Course Certified Ethical Hacker

Module 1 : Intro Ethical Hacking	**Module 2 : Foot Prints**	**Module 3 : Scanning Networks**
Fundamental Security Issues Ethical Hacking Basics Laws and Standard Procedures	Foot Printing Techniques Reconnaissance Techniques Pre-attack Phase	Network Scanning Determining Device State Countermeasures
Module 4 : Enumeration	**Module 5 : Vulnerability Analysis**	**Module 6 : System Hacking**
Enumeration Techniques Border Gateway Protocol Network File Sharing	Security Loopholes Vulnerability assessment Assessment Tools	Hacking Methodologies Steganography Attacks Steganalysis Attacks
Module 7 : Malware Threats	**Module 8 : Sniffing**	**Module 9 : Social Engineering**
Malware Threats Malware Analysis Malware Countermeasures.	Packet-sniffing Techniques Discover Network Vulnerabilities Countermeasures Sniffing Attacks.	Social Engineering Techniques Identify Theft Attempts Human-level Vulnerabilities
Module 10 : Denial-of-Service	**Module 11 : Session Hijacking**	**Module 12 : Evading IDS and Firewalls**
Denial of Service (DoS) Distributed DoS (DDos) Countermeasures and Protections	Session Hijacking Techniques Authentication and Authorization Cryptographic Weaknesses	Intrusion Detection System (IDS) Honeypot Evasion Techniques Perimeter for Weaknesses
Module 13 : Hacking Web Servers	**Module 14 : Hacking Web Apps**	**Module 15 : SQL Injection**
Web Server Attacks Attack Methodology Audit Vulnerabilities	Web Application Attacks Vulnerabilities Web Apps Countermeasures	SQL Injection Attacks Evasion Techniques Injection Countermeasures.
Module 16 : Hacking Wireless	**Module 17 : Hacking Mobile Platforms**	**Module 18 : IoT Hacking**
Wireless Technologies Encryption Threats Wi-Fi Security Tools	Mobile Attack vector Android and iOS Hacking Mobile Security Guidelines	IoT and OT attacks Hacking Methodology Hacking tools
Module 19 : Cloud Computing	**Module 20 : Cryptography**	
Container Technologies Server Less Computing Cloud Computing Threats	Encryption Algorithms Cryptography Tools Cryptography Attacks	