CertKit: Certified Ethical Hacker (CEH) v11

Certified Ethical Hacker CEH v11 will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization. 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 you will be better positioned to setup your security infrastructure and defend against future attacks. An understanding of system weaknesses and vulnerabilities helps organizations strengthen their system security controls to minimize the risk of an incident.

Who should attend:
The Certified Ethical Hacking training course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

CertKit content:

- E-learning courses:
  - CEH v11: Cybersecurity Basics, Attacks & Information Warfare
  - CEH v11: Cyber Kill Chain, TTPs, Behaviors & Threat Hunting
  - CEH v11: Hacking Phases & Concepts
  - CEH v11: Risk Management, Cyber Threat Intelligence & Threat Modeling
  - CEH v11: Incident Management, ML, AI & Regulations
  - CEH v11: Footprinting, Google Dorks, Search Engines & Sub-domains
  - CEH v11: Recon Tools & Tactics
  - CEH v11: Metadata, Wordlists, Email, WHOIS & DNS Recon
  - CEH v11: Footprinting and Social Engineering Recon & Countermeasures
  - CEH v11: Network Scanning, TCP, Host Discovery & Port/Service Scanning
  - CEH v11: Nmap TCP Scans
  - CEH v11: Nmap IP Scans
  - CEH v11: Scan Optimization, OS Identification & IDS/Firewall Evasion
  - CEH v11: NetBIOS, SMB, SNMP & LDAP Enumeration
  - CEH v11: NTP, NFS, SMTP & FTP Enumeration
  - CEH v11: Vulnerability Assessment, Management & Classification
  - CEH v11: Vulnerability Assessment Types, Models, Tools & Reports
  - CEH v11: CEH Hacking Methodology & Windows Authentication
  - CEH v11: Passwords Attacks, Extraction & Cracking
  - CEH v11: Buffer Overflows, Privilege Escalation & System Access
  - CEH v11: Steganography & Avoiding Detection
  - CEH v11: Malware, Threats, Trojans, & Viruses
  - CEH v11: Fileless Malware, Malware Analysis & Countermeasures
  - CEH v11: Sniffing & Poisoning
  - CEH v11: Social Engineering, Insider Threats & Identity Theft
  - CEH v11: DoS, DDoS, Volumetric & Protocol Attacks
  - CEH v11: App Layer Attacks, Botnets & DoS Countermeasures
  - CEH v11: Hijacking Concepts & Countermeasures
  - CEHv11: Intrusion Prevention and Detection, Firewalls & Honeypots
  - CEHv11: Web Server Hacking, Attacks & Attack Methodologies
  - CEHv11: Web Application Attacks & Vulnerabilities
  - CEHv11: CSRF, IDOR, LFI & RFI Attacks
  - CEHv11: Web Application Hacking and Login Attacks
  - CEHv11: XSS, Web Shells, APIs & Webhooks
  - CEHv11: SQL Injection Concepts & Attacks
  - CEHv11: SQL Injection & SQLMap
  - CEHv11: Wireless Concepts, Threats & Hacking Tools
  - CEHv11: Wireless Hacking & Countermeasures
  - CEHv11: Mobile Hacking, OS Security & Device Management
  - CEHv11: IoT Threats, Vulnerabilities, Attack Tools & Countermeasures
  - CEHv11: Operational Technology Concepts, Attack Tools & Countermeasures
  - CEHv11: Cloud Computing, Containers, Hacking & Security Controls
  - CEHv11: Cryptography, Algorithms, Implementations & Tools
  - CEHv11: PKI, Cryptanalysis & Attack Countermeasures

- Online Mentor
- TestPrep Exam simulation
- Tips & Tricks
- Practice Labs (option)
    - The Ethical Hacker Practice Lab gives users the opportunity to gain hands-on experience of the skills required to perform key ethical hacking procedures. Ethical hacking (also known as penetration testing) is a simulated cyber-attack designed to exploit security vulnerabilities within a network and systems. Individuals conducting ethical hacking locate those vulnerabilities and attempt to exploit them. For example, this might involve breaching web applications, protocols, Application Programming Interfaces (APIs), servers and firewalls, plus anything else on a network that could be open to potential exploitation. The objective is to identify vulnerabilities that could be targeted by a malicious agent and exploit those vulnerabilities to simulate the damage that might be caused. In the workplace, this intelligence is used to mitigate the effects of a cyber-attack and to inform changes to security policies, procedures and infrastructure.