CertKit: Certified Ethical Hacker (CEH) v10 (update)

The Certified Ethical Hacker (CEH) program is the most comprehensive ethical hacking course on the globe to help information security professionals grasp the fundamentals of ethical hacking. The hacking course outcome helps you become a professional who systematically attempts to inspect network infrastructures with the consent of its owner to find security vulnerabilities which a malicious hacker could potentially exploit. This hacking course helps you assess the security posture of an organization by identifying vulnerabilities in the network and system infrastructure to determine if unauthorized access is possible.

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:
    - Certified Ethical Hacker - CEHv10: Ethical Hacking Overview and Threats
    - Certified Ethical Hacker - CEHv10: Hacking Concepts
    - Certified Ethical Hacker - CEHv10: Security Controls
    - Certified Ethical Hacker - CEHv10: Security Controls Part 2
    - Certified Ethical Hacker - CEHv10: Pentesting, Laws, and Standards
    - Certified Ethical Hacker - CEHv10: Footprinting
    - Certified Ethical Hacker - CEHv10: Host Discovery and Scanning with Nmap
    - Certified Ethical Hacker - CEHv10: ProxyChains and Enumeration
    - Certified Ethical Hacker - CEHv10: Vulnerability Analysis Concepts and Tools
    - Certified Ethical Hacker - CEHv10: Password Attacks
    - Certified Ethical Hacker - CEHv10: Password Attacks Part 2
    - Certified Ethical Hacker - CEHv10: Privilege Escalation
    - Certified Ethical Hacker - CEHv10: Covert Data Gathering
    - Certified Ethical Hacker - CEHv10: Hidden Files and Covering Tracks
    - Certified Ethical Hacker - CEHv10: Malware Threats
    - Certified Ethical Hacker - CEHv10: Malware Distribution
    - Certified Ethical Hacker - CEHv10: Network Sniffing
    - Certified Ethical Hacker - CEHv10: Social Engineering
    - Certified Ethical Hacker - CEHv10: Denial of Service
    - Certified Ethical Hacker - CEHv10: Session Hijacking
    - Certified Ethical Hacker - CEHv10: Evading IDS, Firewalls, and Honeypots
    - Certified Ethical Hacker - CEHv10: Evading IDS, Firewalls, and Honeypots Part 2
    - Certified Ethical Hacker - CEHv10: Evading IDS, Firewalls, and Honeypots Part 3
    - Certified Ethical Hacker - CEHv10: Hacking Web Servers
    - Certified Ethical Hacker - CEHv10: Common Web App Threats
    - Certified Ethical Hacker - CEHv10: Common Web App Threats Part 2
    - Certified Ethical Hacker - CEHv10: Practical Web App Hacking
    - Certified Ethical Hacker - CEHv10: SQL Injection
    - Certified Ethical Hacker - CEHv10: SQL Injection Types and Tools
    - Certified Ethical Hacker - CEHv10: Wireless Hacking Concepts
    - Certified Ethical Hacker - CEHv10: Wireless Hacking Tools
    - Certified Ethical Hacker - CEHv10: Wireless Hacking Common Threats
    - Certified Ethical Hacker - CEHv10: Cracking and Mobile Hacking
    - Certified Ethical Hacker - CEHv10: IoT Concepts
    - Certified Ethical Hacker - CEHv10: IoT Attacks
    - Certified Ethical Hacker - CEHv10: IoT Hacking and Countermeasures
    - Certified Ethical Hacker - CEHv10: Clouding Computing Concepts
    - Certified Ethical Hacker - CEHv10: Cloud Computer Attacks
    - Certified Ethical Hacker - CEHv10: Cryptography Concepts
    - Certified Ethical Hacker - CEHv10: Cryptography Concepts Part 2
    - Certified Ethical Hacker - CEHv10: Cryptography Concepts Part 3
    - Certified Ethical Hacker - CEHv10: Cryptography Attacks

- 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 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