EC-Council Certified Ethical Hacker (CEH) v13

Duration
5 Days

EC-Council

Course Overview

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.

Course Objectives

- Find and fix Weaknesses: Discover how hackers exploit systems and learn how to keep your data safe.
- Become a security expert: Master the top tools and techniques needed to strength your organization's security.
- Protect your reputation: Learn to proactively prevent data breaches and safeguard your customers' trust.
- Master ethical hacking with AI: Leverage AI-driven techniques to enhance your ethical hacking skills and stay ahead of cyber threats.

Course Prerequisites

There are no prerequisites for this course.

Course Outline

1. **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.

2. **Footprinting and Reconnaissance**
   - Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking.

3. **Scanning Networks**
   - Learn different network scanning techniques and countermeasures.

4. **Enumeration**
   - Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.

5. **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.

6. **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.

7. **Malware Threats**
   - Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

8. **Sniffing**
   - Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

9. **Social Engineering**
   - Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

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.

11. **Session Hijacking**
    - Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

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.

13. **Hacking Web Servers**
    - Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

14. **Hacking Web Applications**
    - Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.

15. **SQL Injection**
    - Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.

16. **Hacking Wireless Networks**
    - Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

17. **Hacking Mobile Platforms**
    - Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

18. **IoT Hacking**
    - Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

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.

20. **Cryptography**
    - Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.