EC Council – CEH
Certified Ethical Hacker

Days: 5

Prerequisites: To succeed in this course, students should have a foundational understanding of cybersecurity concepts and basic IT skills. No prior ethical hacking experience is required, but familiarity with information security practices will be beneficial.

Audience: This course is designed for IT professionals, security enthusiasts, and anyone looking to become certified ethical hackers. It is ideal for those aiming to build careers in cybersecurity, IT auditing, penetration testing, and ethical hacking.

Description: The Certified Ethical Hacker (CEH) v13 program offers the most in-demand ethical hacking certification, equipping students with cutting-edge skills to identify, exploit, and secure vulnerabilities. Powered by AI, this comprehensive course integrates artificial intelligence techniques to automate threat detection, vulnerability analysis, and predictive defenses. Through hands-on labs, real-world scenarios, and AI-powered tools, students will learn how to combat modern cyber threats and stay ahead of cybercriminals. CEH v13 is globally recognized, accredited by the U.S. DoD 8140, and ranked among the top certifications in cybersecurity. By the end of this course, participants will master the five phases of ethical hacking—reconnaissance, scanning, gaining access, maintaining access, and covering tracks—enhanced with AI capabilities.

Course Objectives

In this course, you will:

- Gain in-depth knowledge of ethical hacking methodologies, integrated with AI-driven techniques.
- Master AI-powered tools to automate tasks and increase efficiency in threat detection and response.
- Understand how to exploit and secure vulnerabilities in systems, applications, and AI-driven technologies.
- Develop skills in penetration testing, vulnerability scanning, and system hacking.
- Engage in real-world scenarios through live labs and hacking competitions, putting your knowledge into practice.

OUTLINE:

LESSON 1: INTRODUCTION TO ETHICAL HACKING

- Topic A: Learn the fundamentals of ethical hacking and key information security concepts.
- Topic B: Explore relevant laws and regulations governing ethical hacking.

LESSON 2: FOOTPRINTING AND RECONNAISSANCE

- Topic A: Perform footprinting and reconnaissance using advanced AI-powered tools.
- Topic B: Identify security vulnerabilities during the pre-attack phase.

EC Council – CEH Certified Ethical Hacker

LESSON 3: SCANNING NETWORKS

- Topic A: Use AI to perform network scanning and detect vulnerabilities.
- Topic B: Learn countermeasures to defend against network scanning attacks.

LESSON 4: ENUMERATION

- Topic A: Discover network resources and services using enumeration techniques.
- Topic B: Explore AI tools for detecting and exploiting enumeration vulnerabilities.

LESSON 5: VULNERABILITY ANALYSIS

- Topic A: Perform vulnerability assessments with AI-enhanced scanning tools.
- Topic B: Learn various vulnerability analysis techniques and countermeasures.

LESSON 6: SYSTEM HACKING

- Topic A: Use AI to automate system hacking processes.
- Topic B: Implement methods to gain access, escalate privileges, and cover tracks.

LESSON 7: MALWARE THREATS

- Topic A: Understand and analyze AI-driven malware threats.
- Topic B: Learn about Advanced Persistent Threats (APTs), fileless malware, and mitigation strategies.

LESSON 8: SNIFFING

- Topic A: Perform packet sniffing and use AI to automate detection of sniffing attacks.
- Topic B: Apply countermeasures to protect against network sniffing.

LESSON 9: SOCIAL ENGINEERING

- Topic A: Learn the psychology behind social engineering and AI-enhanced phishing attacks.
- Topic B: Identify and mitigate social engineering vulnerabilities.

LESSON 10: DENIAL-OF-SERVICE (DOS) ATTACKS

- Topic A: Learn AI techniques for detecting and mitigating DoS and Distributed DoS (DDoS) attacks.
- Topic B: Explore tools for auditing systems for potential DoS vulnerabilities.

LESSON 11: SESSION HIJACKING

- Topic A: Discover session hijacking techniques and how AI can be used to enhance detection.
- Topic B: Implement countermeasures to protect session data.

LESSON 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

- Topic A: Master AI-powered evasion techniques for bypassing firewalls and intrusion detection systems (IDS).
- Topic B: Learn how to detect and prevent evasion attempts using AI.

LESSON 13: HACKING WEB SERVERS

- Topic A: Exploit vulnerabilities in web server infrastructures using AI-enhanced tools.
- Topic B: Apply countermeasures to protect against web server attacks.

LESSON 14: HACKING WEB APPLICATIONS

- Topic A: Identify and exploit web application vulnerabilities using AI-driven methods.
- Topic B: Implement countermeasures to defend against web application attacks.

EC Council – CEH
Certified Ethical Hacker

LESSON 15: SQL INJECTION

- Topic A: Use AI to automate SQL injection attacks and evasion techniques.
- Topic B: Apply countermeasures to prevent SQL injection vulnerabilities.

LESSON 16: HACKING WIRELESS NETWORKS

- Topic A: Learn how to hack and secure wireless networks with AI-powered tools.
- Topic B: Implement encryption techniques and defend against wireless network attacks.

LESSON 17: HACKING MOBILE PLATFORMS

- Topic A: Exploit vulnerabilities in mobile platforms (Android, iOS) using AI.
- Topic B: Apply countermeasures for mobile security threats.

LESSON 18: INTERNET OF THINGS (IOT) HACKING

- Topic A: Use AI to hack IoT devices and secure them against advanced threats.
- Topic B: Explore vulnerabilities in operational technology (OT) systems.

LESSON 19: CLOUD COMPUTING

- Topic A: Explore cloud computing vulnerabilities and hacking methodologies using AI tools.
- Topic B: Learn how to secure cloud infrastructures from evolving threats.

LESSON 20: CRYPTOGRAPHY

- Topic A: Master cryptographic techniques and AI-powered cryptography attacks.
- Topic B: Learn how to implement cryptographic countermeasures and defenses.

APPENDIX A: CERTIFIED ETHICAL HACKER V13 AI-POWERED TOOLS

- ShellGPT
- ChatGPT
- FraudGPT
- WormGPT
- DeepExploit
- And more!