CYBERIUM

# CERTIFIED ETHICAL HACKER

# CEHv13 AI

# INTRODUCTION

The Certified Ethical Hacker version 13 Artificial Intelligence (CEHv13 AI) certification exam administered by EC-Council evaluates candidates' expertise in ethical hacking methodologies, tools, and techniques. This course is a highly regarded credential in the cybersecurity industry. Its importance can be summarized through several key aspects:

## Comprehensive Knowledge of Cybersecurity

The CEH course provides extensive knowledge about the latest security threats, vulnerabilities, and attack vectors. It equips individuals with the skills to think and act like a hacker, understanding the mindset and techniques used to breach systems.

## Skill Development in Ethical Hacking

Participants in the CEH course learn practical skills in ethical hacking. They gain hands-on experience with tools and methodologies used to test and defend networks and systems, which is crucial for identifying and mitigating security risks effectively.

## Industry Recognition

The CEH certification is globally recognized and respected by employers in the IT and cybersecurity sectors. Holding this certification validates an individual's expertise and commitment to cybersecurity, making them more attractive to potential employers and enhancing career prospects.

## Regulatory and Compliance Requirements

Many industries are subject to strict regulatory requirements regarding data security. CEH certification helps organizations comply with these regulations by ensuring that their staff are well-trained in the latest security practices and standards.

## Staying Current with Evolving Threats

The CEH course is continually updated to reflect the latest trends and technologies in cybersecurity. This ensures that certified professionals are knowledgeable about current threats and defense mechanisms, making them valuable assets in the rapidly changing cybersecurity landscape.

# CEHv13 Exam Overview

The CEHv13 AI Master Exam comprises two sections: Practical Exam and Multiple-Choice Questions (MCQ) Exam.

In the MCQ section, candidates face 125 questions covering a broad spectrum of cyber security topics. These questions gauge theoretical understanding across areas such as Footprinting, Port and Vulnerability Scanning, Enumeration, System Hacking, Sniffing, Social Engineering, Malware Threats, Cryptography, Exploiting Web Application vulnerabilities, Cloud Computing, etc. Candidates must select the correct response from the provided options.

The practical segment consists of 20 hands-on challenges set in simulated environments. Here, candidates encounter scenarios mirroring real-world cyber security situations. They must showcase their skills by performing tasks like port scanning, identifying vulnerabilities, conducting penetration tests, exploiting security weaknesses, analyzing network traffic, applying steganography, cryptography, password cracking, and implementing security measures. This section assesses the practical application of their knowledge and proficiency using various tools and methodologies in real-time cyber security scenarios.

Attending the CEH training from CyberiumX will equip you with the skills and expertise necessary to excel in ethical hacking, positioning you as a vital asset in the rapidly evolving cybersecurity landscape.

## Course Duration- 50 Hours

# CERTIFIED ETHICAL HACKER (CEH) SYLLABUS

## Module 01- Introduction to Ethical Hacking

1. **Basics of Information Security**
2. **Hacker Types and Ethical Hacking Practices**
3. **Phases involved in Ethical Hacking**
4. **Understanding Cyber Kill Chain Methodology**
5. **Exploring MITRE ATT&CK Framework**
6. **Classification of Cyber Attacks**
7. **Managing Risks in Security**
8. **Handling Security Incidents**
9. **Information Assurance (IA)**
10. **Overview of PCI DSS**
11. **Understanding SOX**
12. **HIPAA and Its Relevance**
13. **Concepts of AI, ML and DL**

- **Practical:**

1. **Setting up a secure hacking environment using virtual machines and labs.**

## Module 02- Footprinting and Reconnaissance

1. **Search Engine based Footprinting**
2. **Social Media based Footprinting**
3. **Web Services**
4. **DNS Footprinting**
5. **Network Footprinting**
6. **Website Footprinting**
7. **Email Footprinting**
8. **Whois Lookups**

- **Practical:**

1. **Using search engines, social media, and specialized tools for online footprinting.**
2. **Employing reconnaissance techniques like OSINT, WHOIS information gathering, WayBack machine, Google Dorking, IMINT and Email footprinting.**

## Module 03- Network Scanning

1. Discovering Hosts
2. Scanning Ports
3. Identifying Operating Systems
4. Service Version Detection
5. Vulnerability Scanning

- **Practical:**

1. Utilizing Nmap for recognizing open ports, services, and vulnerabilities.

## Module 04- Enumeration

1. Identifying Service Vulnerabilities
2. Brute-forcing Credentials of various services
3. Exploring SSH and Telnet
4. Understanding SMTP Enumeration
5. RDP and VNC Enumeration
6. Investigating SMB
7. Examining FTP
8. Investigating DNS

- **Practical:**

1. Extracting information like usernames, shares, and resources using various tools.
2. Identifying exploits for vulnerable services.
3. Introduction to Metasploit Framework.
4. Brute-Force attacks using Hydra.

## Module 05- Vulnerability Analysis

1. Understanding the Vulnerability Assessment Life Cycle
2. Researching vulnerabilities through scoring systems and databases
3. Conducting vulnerability assessments using tools like Nessus, nikto, Burp Suite Professional

- **Practical:**

1. Performing vulnerability scans using tools like Nessus, Nikto, or OpenVAS.

## Module 06- System Hacking

1. Executing active attacks to crack password hashes of Windows and Linux OS
2. Bypassing Authentication on Linux and Windows machines
3. Exploiting vulnerabilities to gain remote system access
4. Escalating Privileges on Linux and Windows
5. Concealing data through Steganography
6. Using Malwares for persistent access.
7. Clearing logs on Windows and Linux machines using various utilities
8. Hiding artifacts within Windows and Linux systems

- **Practical:**

1. Cracking passwords using tools like John the Ripper or Hashcat.
2. Exploiting system vulnerabilities in a controlled environment.
3. Generating malicious Payloads.
4. Tools for Steganography
5. Tools for covering tracks on various OS.

## Module 07- Malware Threats

1. Understanding Malware and its Components
2. Overview of Trojan Horses
3. Different Types of Trojans
4. Gaining control through Trojans
5. Exploring Viruses
6. Introduction to Ransomware
7. Understanding Computer Worms
8. Keyloggers and Spywares
9. Analysis of Malware
10. Static and Dynamic Malware Analysis
11. Techniques for Detecting Malwares
12. Antivirus Software

- **Practical:**

1. Working with various malwares like Trojan horses, Ransomware, etc.
2. Identifying and protecting systems from Malware threats.

## Module 08- Sniffing

1. Network Sniffing
2. MAC Flooding
3. DHCP Starvation Attack
4. ARP Spoofing Attack
5. ARP Poisoning (Man-in-the-middle)
6. Tools for ARP Poisoning
7. MAC Address Spoofing
8. DNS Poisoning and relevant tools
9. Sniffing Tools
10. Detection Techniques for Sniffing

- **Practical:**

1. Packet sniffing using Wireshark or Tcpdump for network traffic analysis.
2. Executing Man-in-the-Middle attack using ARP poisoning
3. Performing MAC spoofing
4. Conducting DHCP attacks

## Module 09- Social Engineering Attack

1. Executing social engineering through various techniques
2. Linux machine MAC address spoofing
3. Identifying phishing attacks
4. Evaluating an organization's security against phishing
5. Key topics include-
6. Different Types of Social Engineering
7. Human, Computer, and Mobile-based Social Engineering
8. Phishing Attacks and Tools
9. Insider Threats and Attacks
10. Identity Theft

- **Practical:**

1. Simulating phishing attacks to demonstrate social engineering tactics.
2. Embedding a malicious link

## Module 10- Denial-of-Service (DoS)

1. **DoS Attacks**
2. **Distributed DoS (DDoS) Attacks**
3. **Understanding Botnets**
4. **Techniques used in DoS/DDoS Attacks**
5. **Ping of Death attack**
6. **Smurf attack**
7. **SYN flood attack**
8. **Slowloris attack**
9. **Tools used in DoS/DDoS Attacks**

- **Practical:**

1. **Simulating DoS attacks using tools like LOIC, hping3, or Metasploit Framework to understand their impact on systems and networks.**

## Module 11- Session Hijacking

1. **Understanding Sessions and Cookies**
2. **Exploring Session Hijacking**
3. **Varieties of Session Hijacking**
4. **Differentiating Spoofing and Hijacking**
5. **Application-Level Session Hijacking**
6. **Client-Side Attacks**
7. **Session Replay Attacks**
8. **Tools for Session Hijacking**

- **Practical:**

1. **Demonstrating session hijacking exercises to gain control of active HTTP connections and illustrate associated risks.**

## Module 12- Evading IDS, Firewalls, and Honeypots

1. Understanding Defensive Devices- IDS, Firewalls, Honeypots
2. Intrusion Detection System (IDS) Overview
3. Firewall Concepts
4. Honeypot Functionality
5. Circumventing Firewall Rules
6. Strategies for Evading IDS and Firewalls

- **Practical:**

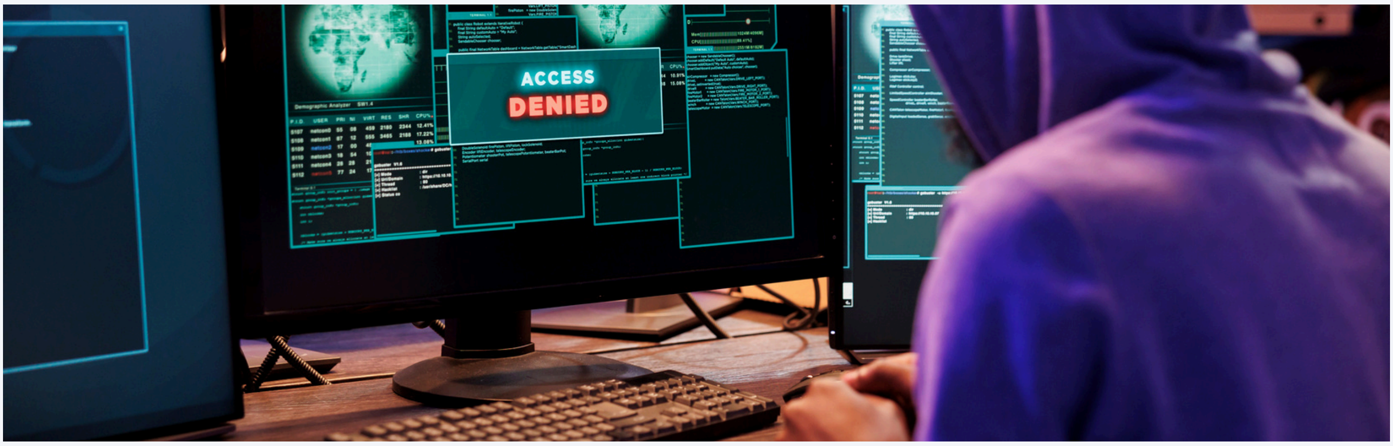
1. Exploring IDS functions using Snort
2. Understanding Firewalls using Firewalld and Windows Firewalls
3. Exploring Honeypots
4. Implementing techniques to bypass IDS and Firewalls to understand their limitations.

## Module 13- Hacking Web Servers

1. Understanding Web Architecture
2. Functions of Web Servers
3. Attacks on Web Servers
4. DNS Server Hijacking
5. Defacement of Websites
6. Methodologies for Attacking Web Servers
7. Patch Management
8. Tools for Web Server Attacks
9. Tools for Enhancing Web Server Security

- **Practical:**

1. Identifying vulnerabilities in web servers (like Apache, Nginx) and exploiting them.



# Module 14- Hacking Web Applications

1. Web Application Architecture
2. Threats to Web Applications
3. SQL Injection
4. Cross-Site Scripting (XSS)
5. Directory Traversal
6. Command Injection
7. File Upload Vulnerabilities
8. Server-Side Request Forgery (SSRF)
9. Cross-Site Request Forgery (CSRF)
10. Broken Authentication
11. Broken Access Control
12. Clickjacking
13. OWASP Top 10 Application Security Risks – 2021
14. Methodology for Hacking Web Applications
15. Web Shells
16. Web Application Security Measures

- **Practical:**

1. Assessing web application security using Burp Suite.
2. Exploiting web application vulnerabilities like Cross-Site Scripting, Directory Traversal, File Upload, CSRF, SSRF, Command Injection, etc.

# Module 15- SQL Injection Attack

1. Understanding SQL Injection
2. Varieties of SQL Injection
3. Error-Based SQL Injection
4. Union-Based SQL Injection
5. Blind SQL Injection
6. Methodology for SQL Injection
7. Tools for SQL Injection

- **Practical:**

1. Executing SQL injection exercises against vulnerable web applications to retrieve or manipulate data.
2. Understanding different types of SQL Injection like Error, Union, and Blind-based attacks.

# Module 16- Hacking Wireless Networks

1. Wireless Network Terminology
2. Characteristics of Wireless Networks
3. Wireless Encryption Standards (WEP, WPA, WPA2, WPA3)
4. Threats to Wireless Networks
5. Methodology for Hacking Wireless Networks
6. Techniques for Cracking Wi-Fi Passwords
7. Evil-Twin Attacks
8. Jamming Signal Attack
9. De-Authentication Attack
10. Threats Associated with Bluetooth

- Practical-

1. Conducting wireless network password cracking attacks.
2. Employing tools like aircrack-ng suite for various wireless attacks.

# Module 17- Hacking Mobile Platforms

1. Attack Vectors for Mobile Platforms
2. App Sandboxing, SMS Phishing Attack (SMiShing)
3. Android Rooting
4. Hacking Techniques for Android Devices
5. Android Security Tools
6. Jailbreaking iOS
7. Hacking Methods for iOS Devices
8. Tools for iOS Device Security
9. Bring You Own Device (BYOD)
10. Mobile Device Management (MDM)
11. Tools for Mobile Security

- Practical:

1. Exploring various mobile threats (malware, phishing, etc.) and implementing countermeasures.
2. Generating malicious Payloads for mobile devices.
3. Exploring attacks like DoS, SMS/call bombing, Port scanning, etc.

# Module 18- IoT and OT Hacking

1. IoT Architecture
2. IoT Communication Models
3. Vulnerabilities in IoT
4. Methodology for Hacking IoT
5. Tools for Hacking IoT
6. Introduction to OT
7. IT/OT Convergence and IIoT
8. Vulnerabilities in ICS and OT
9. Attacks on OT
10. Methodology for Hacking OT
11. Tools for Hacking OT
12. Tools for OT Security

- **Practical:**

1. Identifying and analyzing IoT and OT devices within a network using tools like Shodan, search engines, or network scanning techniques.
2. Conducting vulnerability scanning and analysis of IoT and OT devices using specialized tools like Nessus, nmap, etc.

# Module 19- Cloud Computing

1. Cloud Computing Overview
2. Types of Cloud Computing Services
3. Cloud Deployment Models
4. Cloud Architecture
5. Cloud Service Providers
6. Containers
7. Docker
8. Cloud-Based Attacks
9. Cloud Network Security
10. Controls for Cloud Security

- **Practical:**

1. Understanding Cloud platforms like AWS.
2. Exploring AWS EC2 service for deploying a virtual machine.

# Module 20- Cryptography

1. Introduction to Cryptography
2. Encryption Algorithms
3. Types of Encryption
4. Hashing
5. MD5 and SHA Hash Calculation
6. Cryptographic Tools
7. Public Key Infrastructure (PKI)
8. Email Encryption
9. Disk Encryption
10. Cryptography Attacks
11. Countermeasures for Attacks

- **Practical:**

1. Hands-on practice with encryption and decryption using tools like OpenSSL or PGPtool.
2. Practical experience with Hashing using tools like hashmyfiles, hashcalc, etc.
3. Understanding password cracking using CrackStation.
4. Exploring different Encoding methods like Base64, ROT13, Morse code, etc.