CEHv13 AI - Certified Ethical Hacker v13 Artificial Intelligence

1. Module: Introduction to Ethical Hacking

- Information security
- CIA Triad, Security Standards
- What is Hacking
- Types of Hacking
- Phases of Hacking
- IT laws and Rules
- Cyber Threat
- Cyber Kill Chain
- Deep web and Dark web
- Deep fake Threat
- Hacking Group
- Famous Hacker
- AI role in Hacking

2. Module: Information Gathering

- Collect information of target URL
- OSIENT framework
- User Recon Techniques

2.1 Active Information Gathering

- Collect information using Automated Tools
- Foot printing through Social Engineering
- Network Foot printing

2.2 Passive Information Gathering

- Collect information through Automated Tools
- Domain Recon Technique
- Email Recon Technique
- Whois Foot printing
- Google Hacking dB

3. Module: In-Depth Scanning

- Collect information about Network
- Host Discovery
- Scanning for Open Ports and Services
- Types of Port Scanning
- TCP and UDP Scanning
- Understanding the TCP Three-Way Handshake
- Port Status Types
- TCP SYN Scan
- TCP Connect Scan
- NULL, FIN, and XMAS Scans
- NULL Scan
- FIN Scan
- XMAS Scan
- TCP ACK Scan
- Responses
- UDP Port Scan
- Anonymous Scan Types
- IDLE Scan
- Scanning for a Vulnerable Host
- Performing an IDLE Scan with NMAP
- TCP FTP Bounce Scan
- Service Version Detection
- Active Scanning
- Passive Scanning
- OS Scanning
- Nmap
- Hping3, angryip-scanner
- Recon-ng

4. Module: Enumeration and Exploit

- Introduction to Enumeration
- DNS Enumeration
- SMB Enumeration o
- SMTP Enumeration
- FTP Enumeration
- SSH Enumeration
- Telnet Enumeration
- HTTP Enumeration
- VNC Enumeration
- SNMP Enumeration
- MYSQL Enumeration
- Load Balancer Detector

5. Module: Vulnerability Scanning

- Introduction of Vulnerability ,Bug and Payload
- Vulnerability Scoring System
- Tool for Vulnerability Scanning
- WPScan , Nessus
- Acunetix, Qualys, Crashtest, Nikto, MSF-Pro, NSE Script, Pentest toolbox etc.

6. Module: System Hacking

- Introduction to System Hacking
- Objectives of system hacking
- NTLM and KERBEROS Authentication Process
- Gaining Access
- Escalating Privileges
- Windows Password Cracking
- Linux Password Cracking
- Tools Commonly Used in System Hacking

7. Module: Malware Threats

- Introduction to Malware
- Malware Concepts
- Types of Trojans
- VIRUS , Worms
- RAT's and Rootkits
- Malware Analysis

8. Module: Sniffing & Spoofing

- Introduction to Sniffing Concepts
- Type of Sniffing
- Sniffing Tools
- DNS Spoofing
- SSL Pinging
- DHCP and MAC Flooding
- MAC and ARP Attacks
- Ettercap and Buttercup

9. Module: Social Engineering

- Introduction to Social Engineering
- Social Engineering Concepts
- Computer-based Techniques (with AI integration)
- Human-based Techniques
- Mobile-based Techniques
- Phishing web-pages
- Mirroring
- Phishing Emails

10. Module: Denial-of-Service

- Introduction to DOS and DDOS Attack
- Techniques of DOS and DDOS
- Tool for DOS and DDOS
- HOIC
- LOIC
- Prevention DOS and DDOS

11. Module: Session Hijacking

- Introduction to Session Hijacking
- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Compromising Session IDs
- Blind Hijacking
- Session Hijacking Tools
- Detection Methods and Tools
- Prevention Session Hijacking Attack

12. Module: Evading IDS, Firewalls & Honeypots

- Introduction to Firewall
- Types of Firewall
- Working Process of Firewall
- IDS and IPS
- Working Process of IDS and IPS
- Set Firewall Rules in windows and Linux OS
- Honeypots
- Detecting & Evading Honeypots

13. Module: Hacking Web Servers

- Web Server Fundamentals
- Web APIs
- Attack on web server
- Mirroring websites
- Prevention Web Server to direct Attacks

14. Module: SQL Injection Attack

- Introduction of SQL and Database
- Understand SQL queries
- Authentication Bypass
- Manual Testing on live website
- Error-based SQL injection
- UNION-based SQL Injection
- Blind SQL Injection
- Time-based SQL Injection

15. Module: Hacking Web Applications

- Web Application Overview
- Web Application Frameworks
- OWASP TOP 10
- DVWA Lab
- Burp-Suite and OWASP Zap
- SANS 25

16. Module: Hacking Wireless Networks

- Introduction of Wireless Networks
- Wireless Concepts
- Types of Wi-Fi
- Wi-Fi Encryption
- WPA-1 , WPA-2 and WPA-3
- Antenna and types of Antenna
- Working Process of Antenna
- Crack Wi-Fi password

17. Module: Hacking Mobile Platforms

- Mobile Application Frameworks
- OWASP TOP 10 Mobile Risks
- Anatomy of a Mobile Attack
- Mobile platform attack vectors
- SMiShing, Rooting, Android exploitation

18. Module: IOT Hacking

- IOT Concepts
- OWASP TOP 10 IOT Risks
- IOT Hacking Methodology
- IOT Attack Countermeasures
- OT Concepts & Attacks
- OT Hacking Methodology

19. Module: Cloud Computing

- Introduction of Cloud Computing
- Cloud Computing Methodology
- Cloud Deployment Models
- Benefits of Cloud Computing
- Challenges in Cloud Computing
- S3 Buckets
- EC2 Instances

20. Module: Cryptography

- Introduction of Cryptography
- Types of Cryptographic Techniques
- Encryption and Encoding
- Types of Encryption
- Hashing Algorithms
- Digital Certificates
- Steganography