Mastering Ethical Hacking

Course Overview

Welcome to this course on Practical Ethical Hacking. To enjoy this course, you need nothing but a positive attitude and a desire to learn. No prior hacking knowledge is required.

Requirements

1. Join Our Official Telegram
2. Basic IT knowledge.
3. A minimum of 8GB of RAM is suggested.
4. For Lab Build: A minimum of 16GB of RAM is suggested. Students can still participate in the course but may experience slow lab environments.

Course Curriculum

- ▢ Module 01 - Introduction to Ethical Hacking
- 01 - Information Security Overview
- 02 - Information Security Threats and Attack Vectors
- 03 - Hacking Concepts
- 04 - Penetration Testing Concepts
- 05 - Information Security Controls
- 06 - Information Security Laws and Standards

- [ ] Module 02 - Footprinting and Reconnaissance
  - 01 - Footprinting Concepts
  - 02 - Footprinting through Search Engines
  - 03 - Footprinting through Web Services
  - 04 - Footprinting through Social Networking Sites
  - 05 - Website Footprinting
  - 06 - Email Footprinting
  - 07 - Competitive Intelligence
  - 08 - Whois Footprinting
  - 09 - DNS Footprinting
  - 10- Network Footprinting
  - 11- Footprinting through Social Engineering
  - 12 - Footprinting Tools
  - 13 - Countermeasures

- [ ] Module 03 - Scanning Networks
  - 01 - Network Scanning Concepts
  - 02 - Scanning Tools
  - 03 - Scanning Techniques
  - 04 - Scanning Beyond IDS and Firewall
  - 05 - Banner Grabbing

- [ ] Module 04 - Enumeration
  - 01 - Enumeration Concepts
  - 02 - NetBIOS Enumeration
  - 03 - SNMP Enumeration
  - 04 - LDAP Enumeration
  - 05 - NTP Enumeration
  - 06 - SMTP Enumeration and DNS Enumeration
  - 07 - Enumeration Countermeasures
  - 08 - Other Enumeration Techniques

▢ Module 05 - Vulnerability Analysis

- 01 - Vulnerability Assessment Concepts
- 02 - Vulnerability Assessment Solutions
- 03 - Vulnerability Scoring Systems
- 04 - Vulnerability Assessment Tools
- 05 - Vulnerability Assessment Reports

▢ Module 06 - System Hacking

- 01 - System Hacking Concepts
- 02 - Cracking Passwords
- 03 - Escalating Privileges
- 04 - Executing Applications
- 05 - Hiding Files
- 06 - Covering Tracks
- 07 - Penetration Testing

▢ Module 07 - Malware Threats

- 01 - Malware Concepts
- 02 - Trojan Concepts
- 03 - Virus and Worm Concepts
- 04 - Malware Analysis
- 05- Countermeasures
- 06- Anti-Malware Software

▢ Module 08 - Sniffing

- 01- Sniffing Concepts
- 02- Sniffing Technique: MAC Attacks
- 03- Sniffing Technique: DHCP Attacks
- 04- Sniffing Technique: ARP Poisoning
- 05- Sniffing Technique: Spoofing Attacks

- 06- Sniffing Technique: DNS Poisoning
- 07- Sniffing Tools
- 08- Countermeasures
- 09- Sniffing Detection Techniques

▢ Module 09- Social Engineering
- 01 - Social Engineering Concepts
- 02 - Social Engineering Techniques
- 03- Insider Threats
- 04 - Impersonation on Social Networking Sites
- 05 - Identity Theft
- 06 - Countermeasures

▢ Module 10- Denial-of-Service
- 01 - DoS/DDoS Concepts
- 02 - DoS/DDoS Attack Techniques
- 03 - Botnets
- 04 - DDoS Case Study
- 05 - DoS/DDoS Attack Tools
- 06 - Countermeasures
- 07 - DoS/DDoS Protection Tools

▢ Module 11- Session Hijacking
- 01- Session Hijacking Concepts
- 02- Application Level Session Hijacking
- 03- Network Level Session Hijacking
- 04- Session Hijacking Tools
- 05- Countermeasures

▢ Module 12 - Evading IDS, Firewalls, and Honeypots

- 01- IDS, Firewall, and Honeypot Concepts
- 02- IDS, Firewall, and Honeypot Solutions
- 03- Evading IDS
- 04- Evading Firewalls
- 05- IDS/Firewall Evading Tools
- 06- Detecting Honeypots
- 07- IDS/Firewall Evasion Countermeasures

▢ Module 13- Hacking Web Servers
- 01- Web Server Concepts
- 02- Web Server Attacks
- 03- Web Server Attack Methodology
- 04- Web Server Attack Tools
- 05- Countermeasures
- 06- Patch Management
- 07- Web Server Security Tools

▢ Module 14- Hacking Web Applications
- 01 - Web App Concepts
- 02 - Web App Threats
- 03 - Hacking Methodology
- 04 - Web Application Hacking Tools
- 05 - Countermeasures
- 06 - Web App Security Testing Tools
- 07 - Web App Pen Testing

▢ Module 15- SQL Injection
- 01 - SQL Injection Concepts
- 02 - Types of SQL Injection
- 03 - SQL Injection Methodology
- 04 - SQL Injection Tools

- 05 - Evasion Techniques
- 06 - Countermeasures

▢ Module 16- Hacking Wireless Networks
- 01 - Wireless Concepts
- 02 - Wireless Encryption
- 03 - Wireless Threats
- 04 - Wireless Hacking Methodology
- 05 - Wireless Hacking Tools
- 06 - Bluetooth Hacking
- 07 - Countermeasures
- 08 - Wireless Security Tools
- 09 - Wi-Fi Pen Testing

▢ Module 17- Hacking Mobile Platforms
- 01- Mobile Platform Attack Vectors
- 02- Hacking Android OS
- 03- Hacking iOS
- 04- Mobile Spyware
- 05- Mobile Device Management
- 06- Mobile Security Guidelines and Tools
- 07- Mobile Pen Testing

▢ Module 18- IoT Hacking
- 01- IoT Concepts
- 02- IoT Attacks
- 03- IoT Hacking Methodology
- 04- IoT Hacking Tools
- 05- Countermeasures
- 06- IoT Pen Testing

- [ ] Module 19- Cloud Computing
  - 01 - Cloud Computing Concepts
  - 02 - Cloud Computing Threats
  - 03 - Cloud Computing Attacks
  - 04 - Cloud Security
  - 05 - Cloud Security Tools
  - 06 - Cloud Penetration Testing

- [ ] Module 20- Cryptography
  - 01- Cryptography Concepts
  - 02- Encryption Algorithms
  - 03- Cryptography Tools
  - 04- Public Key Infrastructure (PKI)
  - 05- Email Encryption
  - 06- Disk Encryption
  - 07- Cryptanalysis
  - 08- Countermeasures

- [ ] Skill up EXAM
- [ ] Certification

⚠Non-Disclosure Agreement (NDA) Disclaimer⚠

This training program on ethical hacking is intended for educational purposes only. The techniques, methodologies, and information shared in this training are meant to increase understanding and awareness of cybersecurity practices and ethical hacking concepts. It is important to note the following:

1. Legal and Ethical Use: The techniques and knowledge gained from this training should be used only for legal and ethical purposes. Participants are strictly prohibited from engaging in any malicious,

illegal, or unauthorized activities using the information acquired from this training.

2. Respect for Privacy and Consent: Participants must always respect the privacy of individuals and obtain proper authorization before testing or assessing any systems, networks, or devices. Unauthorized access to systems is illegal and unethical.

3. No Guarantees: While efforts are made to provide accurate and up-to-date information, no guarantees are made regarding the accuracy, completeness, or timeliness of the content. The training content may not cover all possible scenarios or reflect the latest developments in the field.

4. No Liability: The trainers and organizers of this training program are not liable for any actions taken by participants based on the knowledge gained from this training. Participants assume full responsibility for their actions and the consequences thereof.

5. Independent Research: Participants are encouraged to conduct their own independent research and due diligence before implementing any techniques or methodologies discussed in the training.

By participating in this ethical hacking training program, you acknowledge that you have read and understood this disclaimer. You agree to use the knowledge gained from this training responsibly, within legal and ethical boundaries. The trainers and organizers of this training program are not responsible for any misuse or misinterpretation of the information provided.

⚠⚠⚠This disclaimer is an integral part of the training program and applies to all participants.⚠⚠⚠