ADVANCED ETHICAL HACKING CURRICULUM

Outcome of the Course

1. Develop a strong foundation in cybersecurity and ethical hacking practices.
2. Acquire practical skills and knowledge that are directly applicable to real-world scenarios.
3. Enhance learners' employability by gaining expertise in a high-demand field.
4. Understand the importance of ethical considerations in cybersecurity practices.
5. Gain access to cutting-edge tools and resources used in the industry.
6. Interact with industry experts and professionals, fostering networking opportunities.

Stage 1: Fill Technical Gaps

Module 1: Fundamentals of Ethical Hacking

Module 2: Pentest Lab setup and OS Dos Command

Module 3: Basic Networking

Stage 2: Reconnaissance

Module 4: Foot printing

Module 5: Network Scanning

Module 6: Enumeration

Stage 3: Exploitation

Module 7: System Hacking

Module 8: Post Exploitation

Module 9: Malware and Threats

Stage 4: Cyber Threats

Module 10: Web Hacking

Module 11: Social Engineering

Module 12: Mobile Hacking

Stage 5: Network Attack

Module 13: Sniffing and Spoofing

Module 14: Denial of Service

Module 15: Wireless Hacking

Stage 6: Network Security Essentials

Module 16: IDS, Firewalls, and Honeypots

Module 17: Cryptography & Steganography

Stage 1:

Module 1: Fundamentals Ethical Hacking

This module describes all methods, techniques, approaches and standards used by attackers. Moreover, will give an overview of the Risk, threats and Vulnerabilities.

Key Pointers:

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts and their Types
- Penetration Testing Concepts and their Types
- Scope of Ethical Hacking

Module 2: Pentest Lab and Dos Command

This module will help the candidate to implement the Virtual lab environment for hands-on learning including basic OS installation for Windows and Linux platforms.

Key Pointers:

- Fundamental of VMware and Virtual Box
- VM Network Setting (NAT/Bridge/Host-only)
- Virtualization of Windows and Linux
- Installation of Kali Linux
- Command Kung-fu for Windows and Linux

Tools: VMware and Virtual Box OS: Windows, Linux and Kali Linux

Module 3: Basic Networking

This module will help to understand well-known Ports and Protocols used in network concepts. Although it will focus on key areas of networking required for the Network Hacking Concept.

Key Pointers:

- Fundamental IP Address & Subnet Mask
- Network Devices
- OSI Layer Model vs TCP|IP Model
- ARP, ICMP, TCP, UDP protocol
- TCP Flags
- TCP 3-way handshake
- Well known Services Port

Stage 2:

In this stage, the trainer will focus on various techniques and tools used for information gathering to perform Recon with the help of Footprinting, network Scanning and Enumeration by providing conceptual and practical sessions on the following Modules.

Module 4: Footprinting

In this module, the candidate will learn how to gather information against their target with the help of online tools available on the Internet to fetch the information available on the web.

Key Pointers:

- OSINT Framework
- Email Footprinting
- DNS Footprinting
- Web FootPrinting
- Google Hacking Database

Tools: Shodan, Whois, DNS Dumpster, Exploit DB, Hunter, iplogger, OSINT, Httrack and similar alternative tools

Module 5: Network Scanning

This module will help the candidate to learn network scanning to identify live hosts, OS, ports, installed services and their versions.

Key Pointers:

- Host Discovery
- OS Fingerprinting
- Subnet Scanning
- Default Scan
- Stealth Scan
- TCP Scan

- UDP Scan
- Specific port Scan
- ALL port Scan
- Version Scan
- Script Scan
- Decoy Scan
- Fast Scan
- Time Scan
- Aggressive Scan

Tools: Nmap, netdiscover, Zenmap, advanced IP scanner and similar alternative tools.

Module 6: Enumeration

This module will help the candidate to collect gather juicy information for installed services running inside a host machine.

Key Pointers:

- NetBios Enumeration
- FTP Enumeration
- SMB Enumeration
- Telnet Enumeration
- SMTP Enumeration

Tools: Nmap, Rpcclient, SMBmap, SMBclient, NBTScan and similar alternative tools

Stage 3:

In this stage, the trainer will focus on various tools and techniques used by hackers to compromise the target machine by providing a conceptual and practical session on the following Modules.

Module 7: System Hacking

The module primarily focuses on techniques used by an attacker to compromise the target machine with the help of Metasploit Framework and other tools.

Key Pointers:

- Scanning Vulnerability
- Exploiting Vulnerability
- Password Brute Force
- Creating Malicious File Type (eg: Exe, Elf, apk)
- Metasploit Framework – Auxiliaryes, Exploits, Payloads Post Modules & meterpreter
- Msfvenom Framework

Tools: Metasploit, Msfvenom, Netcat

Module 8: Post Exploitation

This module will help the candidate complete the objective of Hacking a system from an attacker's point of view.

Key Pointers:

- Post Enumeration
- Gathering System information
- Gathering User Information
- Download and Upload operations
- Process Migrate
- Web Camera Hacking
- Collect Stored Credentials (System, Browser, Wifi)
- Privilege Escalation to gain Administrator Access

- Hashdump
- Clear Event logs
- Persistence to maintain permanent access

Tools: Metasploit Post Modules

Module 9: Malware and Threats

This Module will help candidates to understand the different behaviours of various types of malware and analysis malicious process behind their execution.

Key Pointers:

- Malware Concept
- Techniques used for Spreading Malware
- Trojan Concept Vs Virus and Worm
- Payload Binders and Crypter
- Countermeasures
- Malicious Process Analysis

Tools: Trojans RAT, Virus Total, TCP View, Process Explorer, Ad blocker

Stage 4:

Module 10: Web Hacking

This module will define Standards and tools used by hackers to exploit websites by injecting malicious code or commands.

Key Pointers:

- Introduction to Web Server and Web Applications
- Well Know web servers and CMS
- Introduction to OWASP
- Website Scanning
- Introduction to burpsuite
- SQL injection
- Cross-Site Scripting
- Remote command Execution
- Brute Force

Tools: Wappalyzer, Burpsuite, Sqlmap, Nikto

Module 11: Social Engineering

This module will focus on techniques used by attackers to perform social engineering to gather target-sensitive information through phishing and impersonation.

Key Pointers:

- Social Engineering Concepts
- Social Engineering Techniques
- Email Spoofing
- Geolocation

- Credential Harvesting
- Haveibeenpwned
- Detect a phishing attack

Tools: Social Engineering Toolkit, Phishtank, Mxtool box, Iplogger

Module 12: Mobile Hacking

This Module will focus on the real-time application used to compromise the mobile device to spy on someone's activity.

Key Pointers:

- Kali Linux NetHunter
- Generating Malicious APK
- Fake SMS
- Fake caller
- Key loggers
- Introduction to Rooted Devices
- Trace Phone Location
- Anonymous Chat Application
- Network Mapper
- Wi-Fi Kill

Tools: Nirsoft, Fing, Online Application, Net hunter

Stage 5:

In this stage, the trainer will focus on well-known network attacks to perform MITM and DOS attacks and countermeasures used for prevention.

Module 13: Sniffing & Spoofing

This module will help the candidate to understand network attacks executed by attackers on less secure Protocols to conduct Man-in-middle attacks.

Key Pointers:

- Introduction Sniffing and Its Types
- Spoofing
- Man-in-the-Middle Attack
- ARP Poisoning
- DNS Poisoning
- Password Sniffing
- HTTP Password Capture
- Telnet Password Capture
- FTP Password Capture

Tools: Ettercap, Wireshark and similar alternatives tools

Module 14: Denial of Services

This module helps candidates to understand the Dos and DDOs attacks. It also explains countermeasures followed in organizations for protecting jewel assets.

Key Pointers:

- Introduction of DOS Attack & Its Types
- Distributed Denial of Service DDOS
- Botnet
- DOS Attack

- SYN Flood
- ICMP Flood
- UDP Flood
- TCP Flood
- Blue Screen Death Attack

Tools: Golden-eye, Hping3, Metasploit Framework

Module 15: Wireless Hacking

This module helps the candidate to understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and counter measures.

Key Pointers:

- Introduction to Wireless standard IEEE
- Introduction to WIFI Security & Protocols
- Detect Hidden SSID
- Monitor mode Vs promiscuous mode
- Capture WPA/WPA2 Handshake
- WPA/WPA2 Password cracking
- Evil Twin
- Dump Wifi Credentials

Tools: Alpha wifi Adapter, Airgeddon

ZStage 6:

In this stage, the trainer will focus on Network Security Essential by describing the countermeasure used for network attacks by providing a conceptual and practical session on the following Modules.

Module 16: IDS, Firewalls, and Honeypots

This module helps the candidate learn various types of security tools and applications used to protect the organization from cyber-attacks.

Key Pointers:

- Introduction to IDS, IPS Firewall, DMZ & Honeypots
- Honey Bot, Kfsensor
- Windows Advanced Firewall Rules
- Evading Firewall
- Event Log Management
- Fundamentals of DLP

Tools: Windows ACL, Linux Iptables, Event Viewer, Kfsensor, Snort

Module 17: Cryptography & Steganography

This module helps candidates to understand how secure the entire communication is or choose the covert mode for making secret communication.

Key Pointers:

- Introduction to Information Security & CIA Model
- Basic Concept of Encoding
- Base64
- Binary
- Hexa Decimal
- Basic Concept of Steganography
- Image, audio and file-based Steganography
- Introduction to Cryptography

- Cesar cypher
- Rot 13
- Modern Cryptography
- AES Symmetric Encryption
- PGP Asymmetric Encryption
- Basic Concept of Hashing
- Hash Calculator
- Signature Compression

Tools: Steghide, PowerShell, Online Tools

Tools List (will be used Stage-wise):

1. VMware and Virtual Box OS: Windows, Linux and Kali Linux
2. Shodan, Whois, DNS Dumpster, Exploit DB, Hunter, iplogger, OSINT, Httrack and similar alternative tools
3. Nmap, netdiscover, Zenmap, advanced IP scanner and similar alternative tools.
4. Nmap, Rpcclient, SMBmap, SMBclient, NBTScan and similar alternative tools
5. Metasploit, Msfvenom, Netcat
6. Metasploit Post Modules
7. Trojans RAT, Virus Total, TCP View, Process Explorer, Ad blocker
8. Wappalyzer, Burpsuite, Sqlmap, Nikto
9. Social Engineering Toolkit, Phishtank, Mxtool box, Iplogger
10. Nirsoft, Fing, Online Application, Net hunter
11. Ettercap, Wireshark and similar alternatives tools
12. Golden-eye, Hping3, Metasploit Framework
13. Alpha wifi Adapter, Airgeddon
14. Windows ACL, Linux Iptables, Event Viewer, Kfsensor, Snort
15. Steghide, PowerShell, Online Tools