Ethical Hacking Course Module

Module-1 – Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

> Elements of Information Security

> Cyber Kill Chain Methodology

> MITRE ATT&CK Framework

> Hacker Classes

> Ethical Hacking

> Information Assurance (IA)

> Risk Management

> Incident Management

Module-2 – Basic Networking

NETWORK BASICS,

OSI & TCP/IP MODE

NETWORK TOPOLOGY

NETWORK DEVICE

IP SUBNETTING

PORTS & PROTOCOL

Module-3 - Introduction To Kali Linux

What is kali linux

How to use kali

Purpose of using kali linux

Basic commends of kali

Instllation & setup kali

Module-4 - Introduction To Virtualization & Lab Setup

>What is Virtual Machine
>What is VMware
>What is Virtual Box
>Install VMware
>Install Kali Linux
>Install Windows OS

Module-5 - Reconnaissance and Foot printing

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Key topics covered:

- Perform foot printing on the target network using search engines, web services, and social networking sites
- Perform website, email, whois, DNS, and network foot printing on the target network
- Collecting DMZ info, wayback machine , etc…

Module-6 – Scanning

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Key topics covered:

> Perform host, port, service, and OS discovery on the target network

> Perform scanning on the target network beyond IDS and firewall

Module-7 – Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures

Key topics covered:

> Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration

Module-8 - Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

- Perform vulnerability research using vulnerability scoring systems and databases
- Perform vulnerability assessment using various vulnerability assessment tools

Module-9 – System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

> Perform Online active online attack to crack the system's password

> Perform buffer overflow attack to gain access to a remote system

> Clear Windows and Linux machine logs using various utilities

Key topics covered:

> Vulnerability Scanning using Nessus Exploit using Metasploit

> Network Scanning using Nmap

> Windows 10 Hacking

> Windows 10 UAC Bypass

Module-10 – Malware Threats

Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

> Gain control over a victim machine using Trojan

> Infect the target system using a virus

> Perform static and dynamic malware analysis

Key topics covered:

> Malware, Components of Malware

> APT

> Trojan

> Types of Trojans

> Exploit Kits

> Virus

> Virus Lifecycle

> Types of Viruses

> Ransomware

> Computer Worms

> Fileless Malware

> Malware Analysis

> Static Malware Analysis

> Dynamic Malware Analysis

> Virus Detection Methods

> Trojan Analysis

> Virus Analysis

> Fileless Malware Analysis

> Anti-Trojan Software

> Antivirus Software

> Fileless Malware Detection Tools

Module-11- Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

> Perform MAC flooding, ARP poisoning, MITM and DHCP starvation attack

> Spoof a MAC address of Linux machine

> Perform network sniffing using various sniffing tools

> Detect ARP poisoning in a switch-based network

Key topics covered:

> Network Sniffing

> Wiretapping

> MAC Flooding

> DHCP Starvation Attack

> ARP Spoofing Attack

> ARP Poisoning

> ARP Poisoning Tools

> MAC Spoofing

> STP Attack

> DNS Poisoning

> DNS Poisoning Tools

> Sniffing Tools

> Sniffer Detection Techniques

> Promiscuous Detection Tools

Module-12 - Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

> Perform social engineering using Various Techniques

Key topics covered:

>Phishing Attack

>Facebook and Instagram Phishing
>Setoolkit usages

> Spoof a MAC address of a Linux machine

> Detect a phishing attack

> Audit an organization's security for phishing attacks

Module-13 - Denial-Of-Service

Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

> Perform a DoS and DDoS attack on a target host

> Detect and protect against DoS and DDoS attacks

Key topics covered:

> DoS Attack, DDoS Attack

> Botnets

> DoS/DDoS Attack Techniques

> DoS/DDoS Attack Tools

> DoS/DDoS Attack Detection Techniques

> DoS/DDoS Protection Tools

Module-14 – Penetration Testing

What is Penetration Testing
Types of Penetration Testing
What is white box Penetration Testing
What is Black Box Penetration testing

Module-15 - Introduction Of Web Hacking

- Web Application Architecture

- Web Application Threats

- OWASP Top 10 Application Security Risks – 2021

- Web Application Hacking Methodology

Module-16 - Sql Injetions

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Key topics covered:

- SQL Injection

- Types of SQL injection

    - Get Method
    - Post method

- Blind SQL Injection

- SQL Injection Methodology

- SQL Injection Tools

  - Automation & Manual Tools For Sqli

Module-17 – Xss Attacks

What is Cross Site Scripting Vulnerability?

Where you can find out XSS Vulnerability

Types of XSS

Demo of XSS

Module-18 - Wifi Hacking

Learn about wireless encryption, wireless hacking methodologies and tools, and WiFi security tools

- Foot Print a wireless network
- Perform wireless traffic analysis
- Crack WEP, WPA, and WPA2 networks
- Create a rogue access point to capture data packets (Day 16)

Module-19 – Website Hacking & Webserver Hacking

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

- Perform web application reconnaissance using various tools
- Perform web spidering
- Perform web application vulnerability scanning
- Perform a brute-force attack
- Detect web application vulnerabilities using various web application security tools

Module-20 - Mobile Hacking

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

> Hack an Android device by creating binary payloads

> Exploit the Android platform through ADB

> Hack an Android device by creating APK file

> Secure Android devices using various Android security tools