Certified Ethical Hacking Training Program

(Offensive & Defensive Security) – Duration 3 Months

Module 01 - Introduction to Information Security & 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.

Key Topics:

- Introduction to Information, Security & Hacking
- What is Core Model of Information Security
- CIA Triad
- Goal of Information Security
- Introduction to Ethical Hacking
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who is a Hacker?
- Types of Hacker & Their Classes
- Hacking Methodology
- What is Vulnerability
- How to Perform Vulnerability Assessment
- What is Penetration Testing?
- Difference Between Vulnerability Assessment (VA) & Penetration Testing (PT)
- Why Penetration Testing
- Penetration Testing Tools & Methodology
- What are the Security Policies & Their Types

Module 02 - Introduction to Networking & Their Terminologies

Cover the fundamentals of Computer Networking, Including the Networking Device, TCP/IP Ports & Protocols used in communication with the knowledge of Networking Devices.

Key Topics:

- What is Network
- What is Networking
- Types of Networking
- Network Diagram & Structures
- What is IP Address
- Types of IP Address
- Classes of IP Address
- Types of Networking Devices (Routers, Switches, Access Point)
- What is OSI Model & TCP/IP Model
- Basics of Data Communication
- TCP vs UDP
- TCP/IP Three Way Handshake

- TCP Communication Flags
- What is MAC
- Types of MAC
- What is MAC Address
- What are Communication Ports
- Common Protocols (HTTP, HTTPS, FTP, DHCP, DNS, SMTP Etc.)

Module 03 – KALI Linux / Parrot OS & Their Fundamentals

Kali Linux / Parrot OS are the Linux Based Operating System which is designed & developed for the Ethical Hacker / Penetration Tester / Cyber Security Expert. Covers the Understanding & Use of these OS including Installation & Configuration for Cyber Security in an offensive way.

Key Topics:

- Introduction of Kali Linux
- Installation & Configuration of Kali Linux
- Use of Kali Linux in GUI & CLI Environment
- Kali Linux / Parrot OS Most Common & Useful Commands
- Types of User Accounts
- Managing User Accounts and Password Security
- Installation & Uninstallation of Programs & Software
- Network Configuration in Kali Linux / Parrot OS
- Compression & Decompression of Files (tar, zip, rar, gz & 7z)
- What is the File & Directory (Folder) Permissions
- Modify Files/Directory permissions using CHMOD
- Default available services

Module 04 – System Hacking / OS Hacking (Desktop Security)

Learn about the various system hacking methodologies. Operating System Architecture & their Working and NT Security Architecture Model and Covering tracks including used to discover system vulnerabilities.

Key Topics:

- Introduction of OS
- Types of OS
- Windows Vs Linux
- What is User Account
- Types of User Accounts
- Local Rights & Privileges
- Windows Security Architecture & Models
- Linux Security Architecture
- Logon Process in Windows NT
- Logon Process in Linux
- Windows NT Security Architecture Components (LSA, SAM, SRM)
- Overall Desktop Security
- Windows User Accounts Hacking

- Linux User Account Hacking
- Escalating User Accounts Privileges
- Cracking Passwords
- Types of Password Cracking Attacks
- Introduction of Windows Registry
- Registry Editing (Automatic & Manual)
- Steps to Creating Registry Values
- Group Policy Introduction
- Create Policy
- Windows Vulnerabilities & Threats
- Various Tools for Password Cracking
- Covering Tracks

Module 05 – Footprinting & Reconnaissance (Information Gathering)

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:

- Footprinting Concepts and Methodology
    - What is Footprinting
    - Objectives of Footprinting

- Footprinting Using Search Engines
    - Finding Company's External & Internal URL
    - Collect Location & Other Information
    - People Search on Social Networking Sites & through Job Sites

- Website Footprinting
    - Technology Used in Websites
    - Cloning/Mirroring of Entire Website
    - Tools for Mirroring/Cloning Websites
    - Extract Information i.e., Email or Phone No.

- Email Footprinting
    - Email Header Analysis
    - Email Tracking / Header Analysis Tools

- WHOIS Footprinting
    - WHOIS Lookup online
    - WHOIS Lookup Tools (Desktop Applications)

- DNS Footprinting
    - Using NSLookup
    - DNS Lookup Tools

- Network Footprinting
    - Details in **SCANNING** Module

- Footprinting Using Google
    - Details in **GOOGLE Hacking** Module

- Footprinting Using Social Engineering
    - Details in **SOCIAL Engineering** Module

- Footprinting Tools

    - Google
    - Maltego
    - Shodan
    - NMAP
    - Other Footprinting & Reconnaissance Tools

Module 06 – Google Hacking (Advance Googling / Art of Googling)

This Module Covers the Advance Use of Google Searching that is also known as Google Hacking or Art of Googling. Learn to use the advance Google Searching Vectors known as Google Dorks.

Key Topics:

- Introduction of Google & Google Hacking
- What a Hacker can do with Google Hacking?
- Google Basics & Advance Searching Techniques
- Google Advance Search Operators
- What are Google Dorks
- Create your own Google Dorks
- Finding Directory Listing through Google Dorks
- Locating Sensitive & Juicy Information
- Locating Admin Login Pages
- Camera Intrusions
- Finding Resources Using Google Advance Operator
- Google Hacking Tools

Module 07 – Scanning Networks

Learn different Network Scanning Techniques & Countermeasures. This Module Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls and standard procedures. Hands-On Lab Exercises to Perform host, port, services and OS discovery on the target network & Perform scanning on the target network beyond IDS and firewall.

Key Topics:

- Scanning Networks: Concepts and Methodology

- Check for Live Systems
    - ICMP Scanning
    - Ping Sweep Method & Tools

- Daemon Banner Grabbing
    - What is Daemon Banner
    - How to Grab Daemon Banner
    - Daemon Banner Grabbing Tools

- NMAP
    - What is NMAP
    - Scanning Methods & Techniques of NMAP
    - NMAP Advance / Script Scanning

- Check for Open Ports
    - Types of Ports
    - Most Common / Well Known Ports
    - Different Methods to Check for Open Ports
        - Three Way Handshake
        - Full Open Scan (TCP Connect Scan)
        - Stealth Scan (Half Open Scan)
        - XMAS Scan
        - FIN Scan
        - NULL Scan
        - UDP Scan
        - Windows Scan Etc.
        - Scan with Custom Flags

- Scanning Beyond IDS
    - Firewall Bypassing Scanning Methods
    - IDS / IPS Evasion Techniques

- Scan for Vulnerability
    - Details in **Vulnerability Analysis** Module

Module 08 – Enumeration

Enumeration is a Follow-On Steps once Scanning is complete & is used to identify Computer Names, Usernames & Shares. This Module Covers various enumeration techniques, such as FTP (File Transfer Protocol), Network File Sharing (NFS) Etc exploits, and associated countermeasures. Scanning & Enumerations are always discussed together because many hacking tools perform both.

Key Topics:

- Enumeration Concepts
    - Introduction of Enumeration
    - Tools for Enumeration

- Enumeration of Most Common Services & Protocols Such as:
    - NetBIOS, FTP, SSH, SNMP, LDAP, Telnet, MySQL, DNS, SMB, SMTP Etc.

- UNIX/Linux Enumeration
- Web Enumeration
- Subdomain Enumeration
- Enumeration Tools

Module 09 – Web Security (Proxies, TOR, Anonymity & Spoofing)

Learn how to Hide or Spoof your identity over the network using various methods of Spoofing.

Key Topics:

- Challenges for Hackers
- Concepts of Don’t Get Caught
- What is Proxy
- Types of Proxies
- What is IP Spoofing

- IP Spoofing with Different Types of Proxies
- Proxy Chaining and Switching
- What is TOR Network
- Spoofing with TOR
- What is MAC Spoofing
- Spoof MAC Address Manually
- MAC Spoofing with Tools (Windows, Linux)
- Operating System Spoofing
- Browser Spoofing

Module 10 – Vulnerability Analysis & Vulnerability Assessment

Learn how to identify security loopholes in a target organization’s network, communication infrastructure, and end systems. Covers Different types of vulnerability assessment and vulnerability assessment tools.

Key Topics:

- Introduction of Vulnerability
- What is Threat, Vulnerability, Payloads & Exploit
- Vulnerability Analysis Vs Vulnerability Assessment
- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Assessment Reports
- Nmap Vulnerability Scanning Techniques
- WPScan for WordPress Vulnerability
- Vulnerability Assessment Tools
    - NMAP
    - WPSCAN
    - Acunetix Vulnerability Scanner (Windows)
    - Uniscan (Linux)
    - Nikto (Linux)
    - Burp Suite Etc.

Module 11 – Hacking Web Server / Penetration Testing

Learn about Penetration Testing and their types. Penetration Testing is the Follow-On Steps once Vulnerability Assessment Completed. This Module Covers Web Server Pentesting & Attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Key Topics:

- Introduction of Penetration Testing
- Types of Penetration Testing
- White Box, Grey Box, Black Box Pentesting
- Sample Penetration Testing Report
- Manual Vs Automated Penetration Testing

- Introduction of Web Server
- Web Server Concepts
- How To Create a Web Server
- Python Module for Web Server
- Services for Webserver
- How to get IP Address of Remote Machine with your own Web Server
- How to Search for Exploits
- Fundamentals of Metasploit Framework (An Exploitation Tool)
    - Metasploit Architecture
    - Msfconsole
    - Search Exploits in Metasploit Framework
    - What are payloads
    - Exploitation With Metasploit
    - What is Meterpreter
    - Use of Meterpreter
    - External Exploits and Payloads in Metasploit Framework
- Payload Creation
- Penetration Testing / Hacking Without Metasploit
- Use of exploit-db.org
- Discovering Risks & Misconfiguration in Web Servers
- Web Defacement
- Penetration Testing Tools
- Countermeasures of Server Hacking
    - Patch Management
    - Patch Management Tools

Module 12 – Network Sniffing

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

Key Topics:

- Sniffing Concepts
    - What is Sniffing
    - How Sniffer Works
    - Types of Sniffing
    - Protocols Responsible for Sniffing

- Man in the Middle (MITM) Attack

- MAC Attacks
    - What is MAC Flooding
    - MAC Flooding Tools

- DHCP Attacks
    - What is DHCP
    - How DHCP Works

- ARP Poisoning
    - What is ARP
    - Works of Address Resolution Protocol (ARP)
    - What is ARP Poisoning
    - APR (Address Resolution Protocol Poisoning Route) Attack
    - Tools ARP Poisoning Attack

- Spoofing Attacks
    - All Spoofing Methods covers in Module **Web Security**

- DNS Poisoning
    - DNS Poisoning Techniques
    - DNS Cache Poisoning

- Sniffing Tools
- Countermeasures
- Sniffing Detection Techniques

Module 13 – Session Hijacking / Cookie Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Key Topics:

- Session Hijacking Concepts
    - What is Session ID
    - How to know the Session ID
    - Introduction of Session ID Hijacking
    - Types of Session ID Hijacking

- Web Application-Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures

Module 14 – Social Engineering Attacks

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

Key Topics:

- Social Engineering - Introduction
    - What is Social Engineering
    - Common Factors to make social engineering much effective
    - Social Engineering Impact on Organisation
    - Key Factors to become victim of Social Engineering Attack

- Types of Social Engineering
    - Shoulder Surfing
    - Dumpster Diving
    - Piggybacking/Tailgating
    - Quid Pro Quo i.e., Tech Support Scams
    - Honeytraps i.e., Romance Scams
    - Scareware
    - Phishing
    - Spear Phishing
    - Smishing and Vishing
    - Pretexting
    - Whaling
    - Road Apple Attack

- Insider Threats
    - Terminated/Disgruntled Employee
- Impersonation on Social Networking Sites
    - Identity Theft
- Social Engineering Tools
- Countermeasures

Module 15 – Malware (Malicious Software) Threats

Learn different types of Malwares such as Trojans, viruses, and worms as well as system auditing for malware attacks, malware analysis, and countermeasures.

Key Topics:

- Introduction to Malwares
- Types of Malwares
    - Virus
    - Worms
    - Trojans (RAT – Remote Administration Tools)
    - Spyware (Keyloggers)
    - Botnet
    - Logic Bombs
    - Spyware
- What is VIRUS
    - Types of Viruses
    - Batch Virus
    - Create Simple Virus
- What is Worm
- Virus Vs Worms
- Trojan Concepts
    - What is Trojan
    - Type of Trojan
    - Create & Deploy Trojans on Windows & Linux Environment
    - Detection & Protection from Trojans
- Spyware (Keylogger)
    - Types of Spyware
    - Practical Demonstration of Spyware
    - Prevention from Spywares
- Installing Bots on Target Machines
- Working of Bots
- Malware Detection & Prevention
- Anti-malware Strategies

Module 16 – Denial of Service (DOS)

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.

Key Topics:

- Introduction to DOS & D-DOS Attack
    - What is DOS Attack
    - What is DDOS Attack
    - Understand the methodology of DOS/D-DOS

- Types & Techniques of DOS/D-DOS Attack
    - Ping of Death Attack
    - Land Attack
    - Smurf Attack
    - Tear Drop Attack
    - SYN Flood Attack
    - HTTP Flood Attack
    - UDP Flood Attack
    - ICMP Flood Attack

- Botnet Distribution
    - What is Botnet
    - Botnet Planting Strategies
    - How to detect Botnet

- DOS/D-DOS Tools
- Identification & Prevention Techniques & Tools

Module 17 – Data Security / Cryptography

Learn about Protection of Data with the concept of Backup (Online/Offline), Restore, Erasing Techniques & Cryptography Techniques that include Encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), Disk & Drive Encryption, Encryption/Decryption, Steganography, Hashing attacks, and Data Recovery Tools.

Key Topics:

- Introduction of Data Security
- Data Security Concepts
    - Physical Security
    - Data Backup / Data Restore
    - Data Recovery
    - Data Encryption
    - Data Hiding (Steganography)

- Data Backup Strategies
    - Online Data Backup
    - Offline Data Backup

- Data Recovery
    - What is Data Recovery
    - Deleted Data Recovery
    - Formatted Data Recovery
    - Partition Recovery

- Data Erasing

- Cryptography Concepts
    - Types of Cryptography
    - Types of Encryptions
    - Encryption Algorithms
        - DES
        - Triple DES (3DES)
        - AES
        - RSA

    - Cryptography Tools

- Hashing
    - Hashing Concepts
    - Encryption Vs Hashing
    - Types of Hashing
        - MD5
        - SHA

- Steganography
    - Overview
    - Steganography techniques
    - Types of steganography
    - Steganalysis
    - Steganography detection tool

- Data Security Frameworks

Module 18 – SQL Injection

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts. Perform an SQL Injection attack against MySQL to extract database & Detect SQL Injection vulnerabilities using various SQL Injection detection tools.

Key Topics:

- SQL Injection Concepts
    - What is SQL Injection Attack
    - Impact of SQL Injection Attack

- How to Hunt for SQL Injection Vulnerability
- Types of SQL Injection
    - Error Based SQLi
    - Union-Based SQLi
    - Time Based SQLi
    - Boolean SQLi
    - Blind SQLi

- SQL Injection Methodology
- Evasion Techniques
- SQL Injection Tools
    - Sqlmap
    - Sqlninja
    - NoSQLMap

- Countermeasures
    - Input Validation
    - Escaping Inputs
    - Sanitizing Inputs

Module 19 – Web Application Hacking & Penetration Testing (WAPT)

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

Key Topics:

- Web Application Concepts
    - Introduction to Web Application
    - Working of Web Application
    - Web App Architecture
    - Components of Web App
- Web Application Threats
- OWASP Top 10 Web Application Security Risk
- Web Application Hacking Methodology
- Web Application Hacking Attacks
- Web Application Footprinting & Recon
- Cross Site Scripting (XSS)
    - Introduction of XSS
    - Types of XSS
    - How to Hunt for XSS
- File Inclusion
    - What is File Inclusion (FI)
    - Types of File Inclusion
    - Remote File Inclusion (RFI)
    - Local File Inclusion (LFI)
- Bruteforce Attacks
- Directory Fuzzing
- Cross Site Request Forgery (CSRF)
- Directory Traversal / Path Traversal
- File Upload Vulnerability
- Command Injection
- Broken Access Control
- Parameter Tampering
- Server Level Access with Web App Vulnerability
- Reverse Shell
- Simple Backdoor Shell
- Protection & Countermeasures

Module 20 – Hacking Wireless Networks

Understand Different Types of Wireless Technologies, Including Encryption, Threats, Hacking Methodologies, Hacking Tools, Wi-Fi Security Tools, And Countermeasures.

Key Topics:

- Introduction to Wireless Networks
- What is WLAN
- 802.11 Standards for WLAN
- Types of Wireless Networks
- Access Point
- SSID
- Wireless Terminologies
- Types of Wireless Encryption
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Protection & Countermeasures

Module 21 – Firewall Security & Evasion, Honeypot, IDS/IPS/IDPS

Get introduced to firewall, intrusion detection system (IDS), intrusion prevention system (IPS) and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures. Bypass Windows Firewall, firewall rules using tunnelling & antivirus.

Key Topics:

- Firewall
    - Introduction of Firewall
    - Working of Firewall
    - Type of Firewall
        - Host Based Firewall
        - Network Based Firewall
    - Firewall Evasion Techniques & Tools

- Create your own Firewall
    - Firewall Rules & Policy
    - User Management
    - Bandwidth Management
    - Quota Management
    - Traffic Policy
    - HTTP Policy

- Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)
    - Introduction to IDS & IPS
    - Types of IDS/IPS
        - HIDS
        - NIDS
    - Log Monitoring & Analysing
    - Evading IDS/IPS Techniques

- Honeypots
    - Introduction of Honeypots
    - Types of Honeypots
        - Production Honeypot
        - Research Honeypot
    - Setup Honeypots

Module 22 – Virtual Private Network (VPN)

Learn how VPN works and discover protocols like PPTP, L2TP, IPsec and SSL. Build your own VPN network by yourself.

Key Topics:

- Introduction to VPN
- Application & Requirements of VPN
- Protocols of VPN
- Tunnelling Mechanism in VPN
- Models of VPN
- OpenVPN
- Setup your own VPN Server
- VPN Security Issues
- VPN Threats

Module 23 – Router Configuration & Security

Understand the basics of Routers & their types with configuration of router by using static & dynamic routing protocol. How to secure routers & security with routing.

Key Topics:

- Router Concepts
  - Introduction of Router
  - Working of Router
  - Types of Routers

- Routing Protocols
  - Default Routing Protocol
  - Static Routing Protocol
  - Dynamic Routing Protocol

- Simulators of Router
  - Configuration of Router
  - Create a Network Structure with Router

- Network Address Translation

- Router Security

Module 24 – Cyber Forensics & Crime Investigation

Understand the basics of Routers & their types with configuration of router by using static & dynamic routing protocol. How to secure routers & security with routing.

Key Topics:

- Cyber Crime
  - What is Cyber Crime
  - Classification of Cyber Crime
  - Prevention of Cyber Crime

- Cyber Forensics
  - Cyber Forensics: Detailed View
  - What is Digital Evidence
  - Challenges of Forensic Science
  - Preservation of Digital Evidence
  - Forensic Tools & Software
  - Basic Approach

Module 25 – Email Security

Learn how Email works, components of email, email services & protocols. Understand the Email Clients & Their Security. Email Spoofing, Email Tracking & Header Analysis Tools.

Key Topics:

- Introduction
- History of E-Mail
- Email Addresses
- How E-Mail Works?

- Various mail servers
- E-Mail Protocols
- Email Clients
- Setup & Secure Email Clients
- Analysis of Email Headers
- Email Tracking
- What is Spamming
- Ways to prevent spam
- Security threats to your email communications (recent updates)
- Setup Email Filter
- Security Policies

Module 26 – Hacking Mobile Platforms

Learn Mobile platform attack vector, android hacking, mobile device management, mobile security guidelines, and security tools.

Key Topics:

- Mobile platform attack vectors
- Hacking Android OS
  - Android Rooting
  - Hack an Android device by creating binary payloads
  - Hack an Android device by creating APK file
  - Payload Creation & Exploitation with msfvenom & Metasploit framework
- Android Spywares
- Android Trojans
- Securing Android Devices

Module 27 – Introduction of IoT Hacking & Security

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Key Topics:

- IoT Concepts
- IoT Attacks
  - Hacking CCTV Cameras
  - IoT Hacking with Shodan

- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures

Module 28 – Introduction of Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

Key Topics:

- Concepts of Cloud Computing
- Types of Cloud Computing Services
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)

    - Software as a Service (SaaS)

- Cloud Computing Deployment Model
- Serverless Computing
- Cloud Attacks
- Cloud Hacking
- Countermeasures

Module 29 – Cyber Laws and Indian IT Act

Learn & Understand about Cyber Law that is also called IT Law is the law regarding Information-technology including computers and the internet.

Key Topics:

- Cyber Law & IT Acts
    - Introduction
    - Why Cyber Law in India
    - Importance of Cyber Law
- IT Act 2000
- Important Sections of IT Act 2000
    - Section 65
    - Section 66
    - Section 66D
    - Section 66E
    - Section 66F
    - Section 67
    - Section 69
    - Section 43A
- Conclusions