1. Introduction To Ethical Hacking & Its Scope

Module 1 - Introduction to Hacking, Ethical Hacking & cyber threats.

Module 2 - CIA Triad

Module 3 - IT Laws in India & outside India

Module 4 -What is Hacking & what who are Hackers

Module 5 -Various types of Hackers

Module 6 -Scope for Ethical Hackers

Module 7 -Scope in cyber security in India & Outside India

Module 8 -How to become an Ethical Hacker [My Secret Way]

2. Setting Up Own Virtual Hacking Lab

Module 9 -Introduction to Linux OS & its importance in Ethical Hacking

Module 10 -Hardware & Software requirements for virtual hacking lab

Module 11-Introduction to Virtual Machines (VMware & VirtualBox) & Kali Linux

Module 12 -Difference between Live OS, Dual Boot & VMware

Module 13 -Downloading Kali Distro for Dual Boot, Live & VMware

Module 14 -Configuring VMware For Kali Linux (2020.2)

Module 15 -Installation Of Kali Linux (2020.2) in VMware using Typical & Custom Mode

Module 16 -Understanding NAT vs Bridge vs Host-Only vs Internal network adapters

Module 17 -Installing Metasploitable in VMware

3. Mastering The Concept:

Module 18 -Concept of 3-Way Handshake [SYN / ACK / FIN]

Module 19 -Concept of Cache & Cookies

Module 20 -Concept of DNS & its Working

Module 21 -Concept of Packets & Traceroute

Module 22 -Concept of Ping & TTL Value

Module 23 -Concept of TCP / UDP / ICMP

Module 24 -Concept of IP & Ports

Module 25 -Some more Concepts...

4.Learning Kali Linux (Basic To Advanced)

Module 26 -Introduction to Kali Linux [Detailed]

Module 27 -Configuring Kali default repository

Module 28 -Learning commands like vi, nano, vim, touch, cat, who, head, tail & more...

Module 29 -Learning Users, Groups, Shadow, Passswd & more Kali commands

Module 30 -Permissions in Linux [Read, Write & Execute]

File sharing between Kali [in VMware] & Windows using 3 different methods

Module 31 -Learning about various Kali Important tools

Module 32 -Kali Linux Advanced

Module 33 -More Kali Practicals & Practices

5.Information Gathering / Reconnaissance

Module 34 -Introduction to footprinting & reconnaissance

Module 35 -Website reconnaissance

Module 36 -Whois reconnaissance

Module 37 -Arin Whois & IP blocks

Module 38 -Builtwidth & viewdnsinfo

Module 39 -Wappalyzer

Module 40 -hping3 , dnsenum & dmitry

Module 41 -Lazyrecon,Sn1per & theharvester

Module 42 -Maltego & Redhawk & more...

Module 43 -Google Dorks & Google Hacking Database

Module 44 -Pentest-Tools

Module 45 -Nslookup

Module 46 -Call Spoofing

Module 47 -Email Tracking

Module 48 -More Reconnaissance Topics & Practicals

6.Become Anonymous On Internet

Module 49 -Understanding Tor & its working

Module 50 -Understanding Tor Nodes & Relays

Module 51 -Dark Web on Tor Network

 Module 52 -Installing Tor Browser in Windows

Module 53 -Installing & Configuring Tor Browser [GUI] in Kali Linux

Module 54 -Installing & Configuring Tor [command line] in Kali Linux

Module 55 -Configuring Tor to Run As Root in Kali Linux

Module 56 -Configuring Proxychain with Tor

Module 57 -Configuring Kalitorify & nipe.pl

Module 58 -Becoming Anonymous Using Tor [IP Hiding]

Module 59 -More Anonymity Topics & Practicals

7.Scanning Techniques

Module 60 -Introduction to Scanning in Ethical Hacking

Module 61 -Scanning Tools & Methodology

Module 62 -Learning about Ports & their states

Module 63 -Well Known, Registered & Dynamic Ports

Module 64 -Use Of Ping

Module 65 -Angry IP Scanner

Module 66 -Banner Grabbing

Module 67 -Netcat & Curl

Module 68 -Using Wafw00f

Module 69 -Introduction to Nmap

Module 70 -Scan Types

Module 71 -Installing Nmap in windows & Kali linux

Module 72 -Nmap - Advanced Port Scanning

Module 73 -Nmap - Firewall Bypass

Module 74 -Nmap - NSE (Nmap Scripting Engine)

Module 75 -Nmap - Cheat Sheets

Module 76 -Nmap - Open Ports, Service Name & versions

Module 77 -Understanding Vulnerability, Exploit & Payload

Module 78 -Finding Open Ports exploits using searchsploit/metasploit

Module 79 -Exploiting Open Ports [For example FTP port 21]

Module 80-Exploiting Open port 21 using Metasploitable

Module 81-Using Zenmap in Windows

Module 82-More Scanning Topics & Practicals

8.Enumeration

Module 83-Introduction to Enumeration

Module 84 -Protection Rings & Protection Domain

Module 85 -The working Of Kernel

Module 86 -Understanding Windows Architecture

Module 87 -Windows Security Elements

Module 88-SIDs, RIDs, SRM, SAM Database, LSASS, NetBIOS

Module 89-NetBIOS Enumeration

Module 90-NetBIOS Enumerator & nbtstat Tool in Windows

Module 91-nbtscan in Kali Linux

Module 92-Understanding Security Identifiers & Relative Identifiers

Module 93-Understanding ACL [Access Control List] & ACE [Access Control Entries]

Module 94-Enumeration Countermeasures

Module 95 -More Enumeration Topics & Practicals

9.System Hacking & Password Cracking

Module 96-Introduction to System Hacking

Module 97-Introduction to Password Cracking

Module 98-Password Guessing & Complexity

Module 99-hash-identifier

Module 100-Hashing

Module 101-LM / NTLM

Module 102-Dictionary Attack

Module 103-Bruteforce Attack

Module 104-Hybrid Attack

Module 105-Rainbow Attack

Module 106-Stealing SAM Databse

Module 107-Creating Own Password List using Crunch in Kali

Module 108-Cracking Zip File Password using John The Ripper

Module 109-Using hashcat

Module 110-Cracking Windows password using L0phtcrack

Module 111-Cracking windows password using KonBoot

Module 112-Cracking Kali Linux Root/Login Password

Module 113-Using Ophcrack

Module 114 -Introduction to Keyloggers

Module 115-Software & Hardware Keyloggers

Module 116-Using Keyloggers to get passwords & credentials

Module 117-Introduction to Encryption

Module 118-Symmetric & Asymmetric

Module 119-Encryption Algorithms

Module 120-Use of pwdump

Module 121-More System Hacking & Password Cracking Topics & Practicals

10.Social Engineering - Human Hacking

Module 122-Introduction To Social Engineering or Human Hacking

Module 123-Why social engineering is master of all other attacks

Module 124-Types of Social Engineering Attack

Module 125-Human & Computer Based social engineering attacks

Module 126-Identity Theft

Module 127-Social Engineering using Android Lost

Module 128-Email Spoofing/Fake Mail

Module 129-Hiding malicious links in Email

Module 130-Introduction to Phishing

Module 131-Phishing Techniques

Module 132-Phishing Campaign with Lucy Security

Module 133-Social Engineering Countermeasures

Module 134-More Social Engineering topics & practicals

11.DOS/DDOS Attacks

Module 135-Introduction to DOS/DDOS [Denial Of Services]

Module 136-DOS Attack Types

Module 137-Smurf & Fraggle DOS Attack

Module 138-SYN Flood & Ping Of Death DOS Attack

Module 139-DDOS Attacks using Zombie PC

Module 140-Introduction to Botnets

Module 141-DOS on Live Website

Module 142-DOS using Goldeneye

Module 143-Slowloris Attack

Module 144-slowhttp

Module 145-torshammer

Module 146-Countermeasures Of DOS/DDOS

Module 147-More DOS Topics & Practicals

12.Sniffing

Module 148-Introduction to Sniffing

Module 149-Sniffing techniques in Kali Linux

Module 150-dsniff

Module 151-Password Sniffing

Module 152-Using Ettercap to Sniff user passwords [HTTP]

Module 153-Using Bettercap to Sniff passwords [HTTPs]

Module 154-ARP Spoofing

Module 155-DNS Spoofing

Module 156-Sniffing with Wireshark

Module 157-Sniffing Countermeasures

Module 158-More Sniffing topics & practicals

13.Metasploit Advanced [Making Trojans]

Module 159-Introduction to Metasploit

Module 160-Practicing Metasploit Framework [msf]

Module 161-searchsploit [Hunting for exploits]

Module 162-cvedetails & exploit-db

Module 163-Understanding LHOSTS,LPORT,RHOSTS & RPORT

Module 164-Exploiting Windows XP using Metasploit

Module 165-Exploiting Windows 7 using Metasploit

Module 166-Exploiting Windows 10 using Metasploit

Module 167-Privilege Escalation

Module 168-User Access Control in Windows

Module 169-Bypassing UAC

Module 170 -Making payload persistence

Module 171-Encoding of Payload

Module 172-Introduction to Crypters

Module 173-Making FUD payload using Metasploit

Module 174-Other FUD making techniques & tools

Module 175-More Metasploit Topics & Practicals

14.Wireless Hacking

Module 176-Introduction to Wireless Hacking

Module 177-Understanding Wireless Networks

Module 178-WEP [Wired Equivalent Privacy]

Module 179-WPA & WPA2

Module 180-Difference between WEP, WPA & WPA2

Module 181-WPS [Wi-fi Protected Setup]

Module 182-Wifi Encryptions & Breaking

Module 183-Setting Wireless Pentesting Environment in VMware

Module 184-Choosing best Wireless External Adapter

Module 185-Monitor mode & Packet Injection

Module 186-Discovering Wi-fi Networks using Wireless Adapter

Module 187-WEP Cracking

Module 188-Use of Aircrack & Airmon

Module 189-WPA/WPA2 Cracking [Manual]

Module 190-WPA/WPA2 Cracking [Automatic]

Module 191 -Wi-fi Phishing

Module 192 -More wireless cracking topics & practicals

15.Android Hacking [Basic]

Module 193 -Introduction To Android Hacking

Module 194 -Rooting & Flashing

Module 195 -One Click Root

Module 196-Introducing Android Studio

Module 197-Android Virtual Device Manager [AVD Manager]

Module 198-Creating Your first latest virtual Android Device

Module 199-Configuring Xposed Framework

Module 200-Using Modules In Xposed Framework

Module 201-Custom ROM Flash

Module 202-Custom Recovery [TWRP]

Module 203-SuperSu

Module 204-More Android Hacking Topics & Practicals

16.Android Pentesting [Advanced]

Module 205-Introduction to Android Pentesting

Module 206-Linux Kernel In Android

Module 207-Setting Up Android Pentesting Lab

Module 208-Creating first Custom Android Device for Pentesting

Module 209-Rooting your virtual Android Device

Module 210-Setting up Xposed Framework & Google Play services

Module 211-Setting Up SSL Unpinning

Module 212-Setting up Burp Suite for Android Phone

Module 213-Configuring Burp Suite For Chrome in Android

Module 214 -Intercepting Android Chrome Browser in Burp Suite

Module 215 -Intercepting Android Applications in Burp Suite

Module 216 -Hunting on Android Applications [like zomato, nykaa, Flipkart & others]

Module 217 -Android Pentesting - Parameter Tampering

Module 218-Android Pentesting - No Rate Limit

Module 219-Android Pentesting - Long password DOS Attack

Module 220 -Android Pentesting - XSS & IDOR

Module 221 -Android Pentesting - More Bugs Testing

Module 222 -More Android Pentesting Topics & Practicals

17.Red-Hat Enterprise Linux [RHEL]

Module 223-Introduction to Red-Hat Enterprise Linux Distro

Module 224 -Installing RHEL in VMware Workstation

Module 225-Creating Yum Server/Repository [Local]

Module 226-Elinks & Hidden directory

Module 227-Understanding Linux Partitions

Module 228-Creating New Partitions using fdisk

Module 229 -Formatting Of Partitions

Module 230 -Mounting of Partitions

Module 231 -Permanent Mounting Devices

Module 232 -Understanding rpm

Module 233 -UUID/blkid & fstab

Module 234 -Understanding /etc/shadow & /etc/passwd

Module 235-Hashes in /etc/shadow

Module 236-Making swap partitions

Module 237-New kernel installation

Module 238 -Creating & Configuring Apache server

Module 239-Creating & Configuring FTP Server

Module 240-Creating & configuring SSH Server

Module 241-Breaking RHEL Login Password

Module 242-More RHEL topics & practicals

18.Bug Bounty | WAPT

Module 243 -Introduction to WAPT / Bug Bounty / Penetration Testing

Module 244-Setting Up Lab For Bug Bounty

Module 245-Using Hackerone, Bugcrowd & Openbugbounty

Module 246-Choosing the right target with large scope area

Module 247-Configuring Kali for Bug Bounty

Module 248-Setting Up Burp Suite for Bug Bounty

Module 249-Recon Techniques

Module 250-Subdomain Enumeration

Module 251-Sorting The Unique

Module 252-Detecting The Live Subdomains

Module 253-Subdomain Takeover

Module 254-Screenshots Of Subdomains

Module 255-Directory Bruteforcing

Module 256-Bug Bounty Data

Module 257-Github Recon Techniques

Module 258-No rate limit

Module 259-Long password DOS Attack

Module 260-Password Reset Poisoning

Module 261-Wordpress Hunting

Module 262-Obsecure Email Vulnerability

Module 263-XSS [Cross Site Scripting] Vulnerability

Module 264 -IDOR Vulnerability

Module 265-SQL Injection [Manual & Automatic]

Module 266-More Bug Bounty Topics & Practicals