Cyber Security for Ethical Hackers & Pentesters v2

Program Overview

Cyber Security for Ethical Hackers & Pentesters v2 is a structured training program designed to build practical and theoretical knowledge in cybersecurity, ethical hacking, Vulnerability Assessment, and Penetration Testing (VAPT). The program begins with cybersecurity foundations, operating systems, Linux and Windows commands, scripting, networking, IP addressing, protocols, and network security before progressing to the five phases of ethical hacking.

Learners develop an understanding of reconnaissance, scanning and enumeration, controlled exploitation in authorized lab environments, persistence concepts, log-analysis awareness, security hardening, and professional VAPT report writing. The program emphasizes ethical conduct, legal authorization, documentation, remediation, and defensive thinking throughout the assessment process.

Learning Objectives

By the end of the program, learners will be able to:

- Understand core cybersecurity principles, including the CIA Triad, types of cyber threats, malware, safe cyber practices, cyber laws, and ethical responsibilities.
- Explain how Windows, Linux, and macOS operate, and use Kali Linux safely through virtual machines, live USB, persistent USB, or dual-boot environments.
- Use Linux and Windows command-line utilities for file management, process monitoring, networking, permissions, system administration, and log review.
- Create basic Bash, Windows Batch, and PowerShell scripts for automation and security-related administration tasks.
- Understand networking fundamentals, including OSI and TCP/IP models, IP addressing, subnetting, ports, protocols, network devices, Wi-Fi security, and network diagnostics.
- Perform passive and active reconnaissance in authorized environments using public-information, DNS, WHOIS, subdomain, metadata, and technology-profiling methods.
- Conduct host discovery, port scanning, service detection, vulnerability scanning, and web enumeration in approved lab environments.
- Understand controlled vulnerability validation concepts involving web application testing, SQL injection, XSS, password security testing, phishing awareness, MitM risks, and DoS/DDoS concepts.
- Explain post-exploitation, persistence, privilege-escalation, log-management, anti-forensic awareness, endpoint hardening, and centralized logging concepts from both attacker and defender perspectives.
- Prepare professional VAPT reports containing scope, methodology, asset inventory, findings, severity, evidence, business impact, remediation recommendations, and retest status.

Course Outcomes

Outcome	Description
CO1	Explain cybersecurity fundamentals, cyber threats, malware types, hacker categories, safe practices, cyber laws, and ethical hacking principles.
CO2	Configure and use a safe cybersecurity practice environment using Kali Linux, VMware/VirtualBox, Live USB, or persistent USB methods.
CO3	Apply Linux, Windows, and PowerShell commands for basic system administration, file management, networking, permissions, process review, and security-related tasks.
CO4	Demonstrate fundamental Bash, Batch, and PowerShell scripting skills for automation activities.
CO5	Analyze network communication using networking concepts such as OSI, TCP/IP, ports, protocols, IPv4/IPv6, subnetting, DNS, and network security controls.
CO6	Conduct authorized reconnaissance and information gathering using WHOIS, Google Dorks, Shodan, theHarvester, Sublist3r, ExifTool, DNS tools, and WAFW00F.
CO7	Perform authorized network and web enumeration using Netdiscover, Nmap, Nessus/OpenVAS, Gobuster, DirBuster, Dirsearch, and Nikto.
CO8	Explain controlled exploitation and attack concepts in lab environments, including SQL injection, XSS, password testing, phishing, email spoofing, DDoS, MitM, Evil Twin, and insider threats.
CO9	Identify persistence, privilege-escalation, backdoor, logging, anti-forensics, and hardening concepts relevant to both offensive and defensive security operations.
CO10	Produce a structured VAPT report with evidence, risk classification, business impact, remediation guidance, and retest validation.

Overall Course Information

Item	Details
Course Title	Cyber Security for Ethical Hackers & Pentesters v2
Duration	
Mode	Blended: Theory + Hands-on Labs
Prerequisites	Basic computer literacy, familiarity with OS (Windows) and simple networking concepts
Trainer	Er. Abinash Barik

Module 1: Cybersecurity Basics

Module	Module Title	Key Topics	Tools / Key Concepts
1.1	Introduction to Cybersecurity	Definition, importance of cybersecurity, protection of systems, networks, applications, and data from attacks, theft, damage, and unauthorized access	Cybersecurity fundamentals
1.2	Importance of Cybersecurity	Data protection, financial security, business continuity, national security, trust, reputation, legal compliance, and secure digital growth	Risk management, compliance
1.3	CIA Triad	Confidentiality, Integrity, Availability; balancing security controls and availability requirements	Encryption, hashing, backups, failover
1.4	Types of Cybersecurity	Network, application, information/data, cloud, endpoint, operational security, and IoT security	Firewall, IDS, IPS, VPN, MFA, EDR, DLP, SIEM, CASB
1.5	Types of Cyber Attacks	Malware, phishing, ransomware, DDoS, MitM, SQL injection, zero-day exploits, and social engineering	Antivirus, WAF, VPN, IDS/IPS
1.6	Malware	Virus, worm, Trojan, ransomware, spyware, adware, logic bomb, rootkit, backdoor, and keylogger	Anti-malware, antivirus, backup and recovery
1.7	Types of Hackers	White hat, black hat, grey hat, blue hat, green hat, red hat, script kiddie, hacktivist, state-sponsored attacker, and malicious insider	Authorization, ethical hacking
1.8	Motives of Hackers	Financial gain, espionage, hacktivism, revenge, challenge, disruption, cryptomining, and recruitment	Threat awareness
1.9	Cybersecurity Challenges	Evolving attacks, insider threats, IoT risks, cloud complexity, supply-chain attacks, social engineering, zero days, and skills gap	Zero Trust, least privilege, segmentation
1.10	Safe Cyber Practices	Strong passwords, password managers, MFA, safe email handling, software updates, secure downloads, encryption, VPN, secure Wi-Fi, backups, and social-media safety	BitLocker, FileVault, VPN, firewall
1.11	Cyber Laws	IT Act 2000; Sections 43, 66, 66C, 66D, 66E, 66F, 67, 70, and 72; GDPR, CFAA, CCPA, HIPAA	Legal compliance, privacy
1.12	Ethics of a Hacker	Written authorization, defined scope, confidentiality, responsible reporting, documentation, non-destructive testing, and legal compliance	Rules of engagement
1.13	Skills for Security Professionals	Networking, operating systems, programming, scripting, cryptography, security tools, communication, problem-solving, and continuous learning	Python, Bash, PowerShell, SQL, C/C++, JavaScript

Module 2: Operating Systems, Commands & Scripting

Module	Module Title	Key Topics	Tools / Commands
2.1	Operating System Fundamentals	Role of operating systems; comparison of Windows, macOS, and Linux	Windows, macOS, Linux
2.2	Windows Operating System	Windows features, Registry, Active Directory awareness, PowerShell, Event Logs, Defender, Firewall, BitLocker, and Hyper-V	CMD, PowerShell, BitLocker, Windows Defender
2.3	macOS Operating System	UNIX-based architecture, Terminal, Gatekeeper, XProtect, FileVault, sandboxing, Time Machine, and Apple ecosystem integration	Terminal, FileVault, Gatekeeper

2.4	Linux Operating System	Linux architecture, distributions, command-line use, packages, user permissions, process management, and Kali Linux use in cybersecurity	Kali Linux, Bash, apt, yum/dnf, pacman
2.5	OS Installation Methods	Live mode, live USB persistence, VMware/VirtualBox, internal dual boot, and external HDD/SSD booting	Kali Linux ISO, Rufus, balenaEtcher, VMware, VirtualBox
2.6	Kali Live USB With Persistence	Kali Live USB creation, persistent storage concepts, encrypted persistence, boot menu awareness, and secure storage	Rufus, Kali Linux Live ISO, LUKS, cryptsetup
2.7	Virtualization	Host OS, guest OS, hypervisor, virtual machine setup, snapshots, virtual lab safety, and isolated testing environments	VMware Workstation/Player, VirtualBox
2.8	Password Reset Awareness	Linux GRUB recovery concepts, Windows recovery-media awareness, physical-access risks, and endpoint-hardening methods	GRUB, BitLocker, Secure Boot, BIOS/UEFI controls
2.9	Navigation & Directory Commands	Path navigation, directory listing, hidden files, folder creation, copying, moving, renaming, and deletion	cd, pwd, ls, dir, mkdir, cp, mv, rm, del
2.10	File and Text Processing	File viewing, file editing, search, filtering, sorting, text extraction, and monitoring logs	cat, less, more, nano, grep, sed, awk, cut, sort, uniq, head, tail
2.11	Network Commands	IP configuration, connectivity testing, DNS lookups, route tracing, active connections, ARP tables, DHCP release/renew, and cache clearing	ip a, ipconfig, ping, dig, nslookup, traceroute, tracert, netstat, ss, arp
2.12	System and Process Commands	Process listing, process termination, disk and memory checks, logged-in users, system information, restart, shutdown, and scheduling	ps aux, tasklist, kill, taskkill, df, du, free, who, w, crontab, schtasks
2.13	Linux File Permissions	Owner, group, others; read, write, execute permissions; octal permissions; ownership; SUID, SGID, and Sticky Bit	chmod, chown, chgrp
2.14	Bash Scripting	Variables, user input, conditions, loops, functions, file tests, command substitution, redirection, piping, and automation	Bash, grep, sed, awk, pipes, redirection
2.15	Windows Batch Scripting	Variables, user input, conditional statements, loops, file operations, and basic automation	.bat, .cmd, SET, ECHO, IF, FOR
2.16	PowerShell Scripting	Variables, conditions, loops, functions, file operations, processes, services, network information, user accounts, and event logs	Get-Process, Stop-Process, Get-EventLog, Get-NetIPAddress, Get-NetTCPConnection, Get-Service, Invoke-WebRequest
2.17	Automation Activities	File sorting, backup automation, basic user-input scripts, and security-focused Windows/Linux automation concepts	Bash, Batch, PowerShell, robocopy, find, mkdir, mv
2.18	Active Directory Basics	Domains, users, groups, policies, and introductory Active Directory lab practice	Active Directory lab concepts

This module develops practical operating-system, command-line, permissions, virtualization, and scripting skills required for security operations and ethical hacking labs.

Module 3: Networking

Module	Module Title	Key Topics	Protocols / Tools
3.1	Basics of Networking	Networks, nodes, links, packets, protocols, IP addresses, MAC addresses, bandwidth, and latency	TCP/IP, Ethernet, Wi-Fi
3.2	Network Data Flow	Packet creation, addressing, routing, packet forwarding, and reassembly at the destination	Routers, packets, IP addresses
3.3	Network Architecture	Client-server and peer-to-peer architectures, advantages, limitations, and examples	Web server, file server, BitTorrent
3.4	Network Devices	Router, switch, hub, bridge, gateway, firewall, NIC, repeater, modem, and wireless access point	Routers, switches, firewalls
3.5	Goals and Uses of Networks	Communication, resource sharing, centralized data access, internet access, cost efficiency, scalability, reliability, and security	VPN, firewall, SIEM
3.6	Network Classification	PAN, LAN, MAN, WAN; private network, public network, and VPN	Bluetooth, Ethernet, Wi-Fi, VPN
3.7	Transmission Media	Guided media: UTP, STP, coaxial, fiber optic; unguided media: radio, microwave, infrared	Ethernet cable, fiber, Wi-Fi, microwave
3.8	Internetworks	Internet, intranet, extranet, access control, and organizational use cases	TCP/IP, HTTP
3.9	Network Topologies	Bus, star, ring, mesh, tree, and hybrid topologies	Hub, switch, network layouts
3.10	Transmission Modes	Simplex, half-duplex, and full-duplex communication	Keyboard/monitor, walkie-talkie, telephone
3.11	OSI Model	Physical, Data Link, Network, Transport, Session, Presentation, and Application layers	Ethernet, IP, TCP, UDP, SSL/TLS, HTTP
3.12	TCP/IP Model	Application, Transport, Internet, and Network Access layers; mapping with OSI model	HTTP, FTP, SMTP, DNS, DHCP, TCP, UDP, IP
3.13	Physical Layer	Signals, media, bandwidth, throughput, NICs, cables, repeaters, hubs, and modems	Cables, NIC, antennas
3.14	Data Link Layer	Frames, MAC addressing, CRC, flow control, Ethernet, Wi-Fi, PPP, HDLC, CSMA/CD, and CSMA/CA	Ethernet, IEEE 802.11, PPP
3.15	Network Layer	Logical addressing, routing, packet forwarding, fragmentation, reassembly, NAT, and routing protocols	IP, ICMP, ARP, RIP, OSPF, BGP
3.16	IPv4 and IPv6	Address formats, address space, headers, NAT, DHCP, SLAAC, and address security	IPv4, IPv6, DHCP, SLAAC
3.17	Public and Private IP Addresses	Public/private IP comparison, RFC 1918 ranges, loopback address, and NAT	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 127.0.0.1
3.18	Subnetting	Subnet masks, CIDR notation, network address, broadcast address, usable host range, and subnetting calculations	/24, 255.255.255.0
3.19	Transport Layer	End-to-end delivery, segmentation, reassembly, ports, flow control, error recovery, and TCP three-way handshake	TCP, UDP, SYN, SYN-ACK, ACK
3.20	Session Layer	Session establishment, synchronization, maintenance, dialog control, and termination	NetBIOS, RPC, PPTP
3.21	Presentation Layer	Encoding, translation, encryption, decryption, compression, SSL/TLS, SSL stripping, and downgrade attacks	SSL/TLS, ASCII, Unicode, JPEG, ZIP

3.22	Application Layer	HTTP, HTTPS, FTP, SMTP, DNS, DHCP, POP3, IMAP, SSH, Telnet, RDP, WWW, and CDN	HTTP/HTTPS, DNS, SMTP, SSH, RDP
3.23	Common Ports and Services	Security relevance of common ports and services	FTP 20/21, SSH 22, Telnet 23, SMTP 25, DNS 53, HTTP 80, HTTPS 443, SMB 445, RDP 3389
3.24	Network Diagnostics	IP configuration, gateway checks, DNS tests, connectivity tests, route tracing, local listening ports, and ARP review	ip a, ipconfig, ping, dig, nslookup, traceroute, tracert, ss, netstat, arp -a
3.25	Network Security	Physical, technical, and administrative security; segmentation; access control; monitoring and incident detection	Firewall, IDS, IPS, VPN, NAC, SIEM, EDR, WAF
3.26	Wi-Fi and Bluetooth Standards	Wi-Fi generations, WEP/WPA/WPA2/WPA3, Bluetooth versions, wireless risks, and secure wireless use	IEEE 802.11, WPA2, WPA3, Bluetooth BLE

This module provides the networking knowledge needed to understand data flow, ports, services, protocol weaknesses, network scanning, and network-defense concepts.

Module 4: VAPT & Ethical Hacking Phases

Module	Module Title	Key Topics	Recommended Tools
Pre-Module	**VAPT & Ethical Hacking Foundation**	Ethical hacking and VAPT concepts; penetration tester, red team, blue team, purple team; CVE and zero-day awareness; legal boundaries; written authorization; scope; rules of engagement; documentation and responsible disclosure	Kali Linux, VMware, VirtualBox, Rufus, balenaEtcher
Module 4.1	**Phase 1: Reconnaissance / Footprinting / Information Gathering**	Passive and active reconnaissance; IP ranges; domains; DNS records; hosting details; employee details; technology stack; public documents; physical-location intelligence; attack-surface mapping	WHOIS, Google Dorks, Shodan, Maltego, theHarvester, Nmap
4.1.1	Passive Reconnaissance	Public-information gathering from websites, search engines, social media, job portals, public documents, WHOIS information, and DNS records	Google Dorks, WHOIS, Shodan, Maltego, OSINT Framework
4.1.2	Google Dorking & OSINT	Indexed pages, exposed documents, login pages, admin panels, directory listings, cached pages, public error messages, and information exposure	Google Dorks, OSINT Framework
4.1.3	DNS and WHOIS Enumeration	Domain registration, name servers, A, MX, NS, SOA, TXT, SPF, DKIM, DMARC, and reverse-DNS checks	whois, nslookup, dig, DomainTools
4.1.4	Technology Profiling	Publicly exposed hosts, services, products, ports, technology stack, and WAF identification	Shodan, WAFW00F
4.1.5	Email and Subdomain Discovery	Email harvesting, employee information, subdomain enumeration, and asset discovery	theHarvester, Sublist3r
4.1.6	Metadata Analysis	Metadata extraction from public documents, including author names, software details, internal paths, and GPS information	ExifTool
4.1.7	Reconnaissance Defenses	Information exposure controls, metadata removal, DNS security, DMARC, and secure public-information management	ExifTool, DNS controls

Module 4.2	**Phase 2: Scanning & Enumeration**	Host discovery, port scanning, service discovery, OS detection, vulnerability scanning, web-directory enumeration, web-server scanning, network mapping, and scan-output interpretation	Netdiscover, Nmap, Nessus, OpenVAS, Gobuster, DirBuster, Dirsearch, Nikto
4.2.1	Host Discovery	Authorized local network discovery; live-host identification and ARP-based discovery	Netdiscover, arp -a, Nmap
4.2.2	Port Scanning	TCP, UDP, SYN, ACK, XMAS, top-port, all-port, and targeted port scans	Nmap
4.2.3	Service and Version Detection	Detection of running services, version details, operating-system identification, and misconfiguration indicators	Nmap
4.2.4	Nmap Scripts and Reports	Nmap NSE scripts, vulnerability scripts, and scan-output saving for assessment evidence	Nmap, NSE
4.2.5	Vulnerability Scanning	Identifying known vulnerabilities, outdated software, insecure SSL/TLS, missing patches, and exposed services	Nessus, OpenVAS, Nmap NSE
4.2.6	Web Directory Enumeration	Identifying directories, files, admin paths, backup files, and exposed web resources	Gobuster, DirBuster, Dirsearch
4.2.7	Web Server Scanning	Web-server weakness identification, configuration review, and common web vulnerability checks	Nikto

Module 4.3	**Phase 3: Gaining Access / Exploitation — Lab Only**	Controlled vulnerability validation in approved labs; web testing; SQL injection; XSS concepts; password testing; phishing awareness; email spoofing; DDoS awareness; MitM awareness; Evil Twin lab; Rubber Ducky simulation; insider threats	Metasploit Framework, Burp Suite, SQLmap, Hydra, Hashcat, John the Ripper
4.3.1	Web Application Testing	HTTP request analysis, authentication checks, input validation, session analysis, and controlled web vulnerability validation	Burp Suite
4.3.2	SQL Injection	SQL injection concepts, database risks, parameterized queries, input validation, and WAF-based prevention	SQLmap, Burp Suite
4.3.3	Cross-Site Scripting	XSS concepts, browser-side risks, malicious client-side scripts, and prevention awareness	Burp Suite
4.3.4	Password Security Testing	Brute-force, dictionary, password-hash concepts, password-cracking labs, and defense strategies	Hydra, Hashcat, John the Ripper
4.3.5	Metasploit Framework	Controlled exploitation framework use in dedicated training labs	Metasploit Framework
4.3.6	Phishing Awareness	Phishing, spear phishing, whaling, vishing, smishing, phishing indicators, and prevention	Email safety concepts
4.3.7	Email Spoofing & Authentication	Email spoofing concepts; SPF, DKIM, DMARC, mail-server records, and prevention	dig, nslookup, DNS tools
4.3.8	DoS/DDoS Awareness	Volumetric, protocol, and application-layer DDoS concepts, botnets, prevention, and mitigation	Firewall, rate limiting, DDoS mitigation
4.3.9	MitM Awareness	ARP poisoning, rogue Wi-Fi, DNS spoofing, SSL stripping, MitM risks, and preventive controls	VPN, HTTPS, certificate controls
4.3.10	Evil Twin Lab	Authorized ESP32/NodeMCU Evil Twin lab concepts, Wi-Fi risks, and safe lab procedures	ESP32, NodeMCU
4.3.11	Rubber Ducky Simulation	PIN brute-force simulation awareness, automated-input risks, prevention, and endpoint security	Rubber Ducky simulation device
4.3.12	Insider Threats	Insider threat types, misuse of authorized access, risk impact, and defensive controls	Access controls, least privilege, logging

Module 4.4	**Phase 4: Maintaining Access / Post-Exploitation**	Persistence concepts, backdoors, web shells, scheduled tasks, cron jobs, Registry persistence, privilege escalation, account persistence, and defensive detection	Netcat, Cron, Windows Registry, Scheduled Tasks
4.4.1	Backdoors & Web Shell Concepts	Hidden access mechanisms, web-shell concepts, risks, and defensive identification	Netcat, web-shell concepts
4.4.2	Scheduled Tasks & Cron Jobs	Persistence through Windows Scheduled Tasks and Linux cron jobs; defensive review	Task Scheduler, Cron
4.4.3	Registry Persistence	Windows Registry persistence concepts and defensive inspection	Windows Registry
4.4.4	Privilege Escalation	User-to-admin/root escalation concepts and insecure configuration awareness	Linux permissions, Windows privileges
4.4.5	Persistence Detection	Detecting unauthorized users, startup entries, scheduled tasks, services, and suspicious persistence mechanisms	net user, Task Scheduler, Cron, Event Viewer

Module 4.5	**Phase 5: Covering Tracks / Cleaning Up / Defensive Forensics**	Log-clearing concepts, removal of temporary files and tools, Registry traces, anti-forensics awareness, detection gaps, centralized logging, and system hardening	Event Viewer, Linux logs, auditd, PowerShell, Bash
4.5.1	Windows Log Awareness	Windows Event Log review, suspicious activity, user-account events, and endpoint monitoring	Event Viewer, Get-EventLog, PowerShell
4.5.2	Linux Log Awareness	Linux logs, audit records, authentication logs, log review, and security monitoring	Linux logs, auditd, Bash
4.5.3	Anti-Forensic Concepts	Log deletion, log manipulation, tool removal, file deletion, Registry changes, and defensive detection methods	Logs, Event Viewer, auditd

Module 4.6	**VAPT Report Writing & Remediation**	Professional report preparation based on all phases; scope, methodology, tools, findings, severity, evidence, impact, remediation, conclusion, and retesting	Nmap output, Nessus/OpenVAS results, Burp Suite evidence, screenshots, logs
4.6.1	Scope and Methodology	Authorization, in-scope and out-of-scope assets, test period, constraints, rules of engagement, and methodology	Scope document, test log
4.6.2	Asset Inventory	Domains, IP addresses, subdomains, open ports, services, applications, and identified technologies	Nmap, Shodan, theHarvester, Sublist3r
4.6.3	Vulnerability Findings	Finding title, affected asset, description, technical details, evidence, and classification	Scanner results, screenshots, logs
4.6.4	Risk and Severity Analysis	Critical, High, Medium, Low, and Informational classification; confidentiality, integrity, availability, and business impact assessment	CIA Triad, risk analysis
4.6.5	Proof of Concept	Non-destructive evidence demonstrating the validated finding in an approved environment	Burp Suite, Nmap, SQLmap, screenshots
4.6.6	Remediation Recommendations	Patching, secure configuration, MFA, encryption, segmentation, secure coding, WAF, monitoring, backups, and awareness training	Firewall, WAF, SIEM, IDS/IPS, MFA
4.6.7	Retest and Closure	Validation of fixes, retest evidence, residual-risk documentation, and finding closure	Retest outputs, screenshots, updated scan reports

The final VAPT module uses the structured five-phase ethical-hacking approach and concludes with report writing, remediation planning, and retesting.