Professional Cybersecurity, Ethical Hacking & Advanced VAPT Program

Program Overview

This program of, "Cyber Security – Theory, Practical & VAPT (Beginner to Advanced)," provides a structured, lab-driven introduction to core cybersecurity concepts, networks, operating systems, ethical hacking, cyber security, and vulnerability assessment and penetration testing (VAPT). Learners work in a controlled lab using Kali Linux, Windows, and intentionally vulnerable operating systems, websites, and applications, with live demonstrations of industry-standard hacking tools such as Nmap, Gobuster, Nikto, Burp Suite, SQLmap, and Metasploit. The program gradually takes students from fundamentals and legal/ethical frameworks through networking, OS and scripting skills, ethical hacking phases, hands-on VAPT workflows, Red vs Blue teaming, and professional-grade reporting.

Learning Objectives

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

1. Explain key cybersecurity concepts, threat types, and the CIA triad, and connect them to real-world cyber incidents.
2. Describe different categories of hackers, their motives, and the legal and ethical boundaries governing ethical hacking and penetration testing.
3. Compare Windows, Linux, and macOS from a security perspective and set up secure, isolated labs using Kali Linux (live, persistent USB, VM, and dual-boot).
4. Demonstrate foundational networking knowledge, including network devices, topologies, OSI/TCP-IP models, IP addressing, and common security controls.
5. Use Linux and Windows command lines effectively and write basic Bash, Batch, and PowerShell scripts to automate security-related tasks.
6. Apply the full ethical hacking lifecycle (reconnaissance, scanning, gaining and maintaining access, and covering tracks) in a safe lab environment.
7. Conduct structured VAPT on vulnerable operating systems, websites, and applications using demonstrated hacking tools (Nmap, Netdiscover, Gobuster, DirBuster, Dirsearch, Nikto, Burp Suite, SQLmap, Metasploit, etc.).
8. Differentiate Red, Blue, and Purple team roles and analyze attack–defense scenarios from both offensive and defensive perspectives.

9. Produce clear, industry-style VAPT reports that document findings, evidence, risk ratings, and remediation recommendations.

Course Outcomes

After successfully completing this course, learners will be able to:

1. CO1: Articulate core cybersecurity principles, major attack types, and relevant legal and ethical frameworks, and relate them to contemporary cyber incidents.
2. CO2: Configure and operate secure lab environments using Kali Linux, Windows, virtualization, and encrypted storage for ethical hacking and VAPT practice.
3. CO3: Apply networking, OS, and scripting skills to execute basic offensive (Red Team) activities and implement defensive (Blue Team) controls.
4. CO4: Execute end-to-end ethical hacking and VAPT methodologies on intentionally vulnerable OS, websites, and applications, leveraging hands-on demonstrations of common hacking tools across all phases (reconnaissance, scanning, exploitation, post-exploitation, and reporting).
5. CO5: Distinguish and coordinate Red, Blue, and Purple team responsibilities in practical scenarios, demonstrating collaborative security improvement.
6. CO6: Prepare professional VAPT reports with structured methodology, detailed technical findings, prioritized risks, and actionable remediation guidance.

Overall Course Information

Item	Details
Course Title	Professional Cybersecurity, Ethical Hacking & Advanced VAPT Internship Program
Duration	
Mode	Blended: Theory + Hands-on Labs (Kali Linux, Windows, Vulnerable OS/Web Apps)
Prerequisites	Basic computer literacy, familiarity with OS (Windows) and simple networking concepts
Trainer	Er. Abinash Barik

Consolidated Course Syllabus (Modules + Outcomes)

Mod. No.	Module Title	Detailed Topics	Hours	What Students Will Learn (Module Learning Outcomes)
1	Cybersecurity Fundamentals & Roles	Why Cybersecurity Is Important; What Is Cybersecurity; CIA Triad (Confidentiality, Integrity, Availability); Types of Cybersecurity (Network, Application, Information/Data, Cloud, Endpoint, Operational Security, IoT Security); real incidents (WannaCry, Target breach, SolarWinds); advantages of strong cybersecurity; brief roles: Ethical Hacker, Penetration Tester, Red Team, Blue Team, Purple Team.	4	Explain why cybersecurity is critical for individuals, organizations, and nations; describe the CIA triad and different cybersecurity domains; identify key roles (Red, Blue, Purple Team, Ethical Hacker, Pen Tester) and how they interact in an ethical hacking lifecycle.
2	Cyber Threat Landscape	Types of Cyber Attacks (Malware, Phishing & Spear Phishing, Ransomware, DDoS, Man-in-the-Middle, SQL Injection, Zero-Day, Social Engineering); Types of Malware (Virus, Worm, Trojan, Ransomware, Spyware, Adware, Logic Bomb, Rootkit, Backdoor, Keylogger); attack flows, notable examples; signs of infection, malware removal steps.	4	Classify major cyber attacks and malware types; map real-world attacks to techniques and vectors; outline detection signs and basic response steps; relate typical Red Team techniques to appropriate Blue Team countermeasures.
3	Hackers, Motives, Ethics & Laws	Types of Hackers (White/Black/Grey/Blue/Green/Red hats, Script Kiddies, Hacktivists, State/Nation-Sponsored, Malicious Insider/Whistleblower); Motives of Hackers (financial gain, espionage, hacktivism, revenge, challenge/fun, disruption, crypto mining, recruitment); Ethics of a Hacker (code of ethics, qualities of ethical hacker); Ethical vs Criminal hacking; Challenges of Cybersecurity & steps to avoid; Cyber Laws (Indian IT Act 2000 Sections 43, 66, 66C, 66D, 66E, 66F, 67, 70, 72; GDPR, CFAA, CCPA, HIPAA).	4	Differentiate hacker categories based on intent and authorization; analyze attacker motivations; apply codes of ethics to ethical hacking practice; explain key cyber laws and why written authorization is mandatory; connect White Hat/Red Team actions to legal boundaries and Blue Team obligations.
4	Operating Systems for Security	OS overview and comparison (Windows, macOS, Linux: developer, cost, GUI/CLI, file systems, security posture, typical cyber uses); features of each OS; how each OS is useful in cybersecurity (Windows as target, macOS dev, Kali Linux for ethical hacking); OS installation: Live Mode USB, Live + Persistence USB (detailed Kali persistence steps with Rufus + LUKS), VMware/VirtualBox installation from ISO, Dual Boot (internal/external HDD/SSD).	4	Compare Windows, macOS, and Linux from a security perspective; select suitable OS for specific cybersecurity tasks; perform (or document) secure installations of Kali via Live, persistent USB, VM, and dual boot setups; understand where Red and Blue workflows rely on each OS.
5	Networking Essentials for Cybersecurity	Basics of Networking (definition & working, packetized communication, example email flow); key networking terms (node, link, packet, protocol, IP, MAC, bandwidth, latency); network architectures (Client-Server, P2P); network devices (router, switch, hub, bridge, gateway, firewall, IDS/IPS, NAC, SIEM); goals & uses of networks; classification of networks (PAN, LAN, MAN, WAN); transmission media (UTP/STP, coaxial, fiber, radio, microwave, infrared); ownership/access control (private, public, VPN); Internet, Extranet, Intranet.	4	Explain how data moves across a network; distinguish key network devices and where they appear in real topologies; classify networks by geography, medium, and ownership; recognize where attackers and defenders operate in a networked environment.
6	Network Models & Network Security	OSI model (7 layers, PDUs, devices, protocols); TCP/IP model (4 layers, mapping and data flow); physical & data-link topics (topologies, transmission modes: simplex/half/full duplex, bandwidth vs	4	Map protocols and attacks to OSI/TCP-IP layers; perform basic subnetting and IP classification; explain TCP vs UDP

		throughput); IP addressing & subnetting (IPv4 vs IPv6, classful addressing, private vs public IP, IP threats & IP hiding/protection); Transport layer (TCP/UDP, 3-way handshake); Session/Presentation/Application layers (well-known ports, SSL/TLS, WWW, DNS, CDN); Network Security (firewall, IDS/IPS, VPN, NAC, SIEM, segmentation, WAF, email security gateway); Wi-Fi & Bluetooth standards + Wi-Fi security (WEP/WPA/WPA2/WPA3).		behavior; identify appropriate security controls for each layer (firewalls, VPNs, IDS/IPS, WAFs, SIEM, Wi-Fi security); understand Red attack vectors and Blue defenses at each layer.
7	Commands, Scripting & Automation	Basic OS commands (navigation, file/dir, text processing, network, processes, system info) in Linux (Bash) and Windows (CMD/PowerShell); Linux file permissions (r/w/x, owner-group-others, chmod/chown/chgrp, SUID/SGID/sticky bit); Bash scripting fundamentals (variables, conditionals, loops, functions, grep/sed/awk/cut/sort/uniq/wc/head/tail, I/O redirection, pipes); Windows Batch scripts (backup automation, age program, prank/educational scripts); PowerShell scripting (variables, loops, Read-Host, file operations, security cmdlets: Get-Process, Stop-Process, Get-EventLog, Get-NetTCPConnection, Get-LocalUser, Get-Acl); practical automation scripts from the practical handbook.	4	Use Linux and Windows command lines effectively for security tasks; configure and audit file permissions; write basic Bash, Batch, and PowerShell scripts for automation; articulate how these scripts can support both Red Team tasks (e.g., recon automation) and Blue Team tasks (e.g., log collection, backup).
8	Practical Lab Foundation & Secure Lab Setup	Ethical hacking introduction (definitions: Ethical Hacker, Penetration Tester, Red Team, Blue Team, Purple Team, CVE, Zero-Day); legal boundaries & non-negotiable rules (scope, written permission, logging, safe environments); Kali Live USB with encrypted persistence (step-by-step with Rufus, LUKS); Kali VMware installation sequence; Linux password reset via GRUB (boot parameter modification, single-user mode, adding new password, reboot), securing GRUB (password-protected GRUB, config steps); Windows password reset/boot-ISO discussion and Blue hardening: BitLocker, Secure Boot, BIOS password, LAPS, Credential Guard; OS command recap.	4	Set up a safe ethical hacking lab using Kali Linux in USB/VM environments; reset and secure Linux passwords using GRUB; understand the risk of physical bypass on Windows and how Blue Team defenses (BitLocker, Secure Boot, BIOS passwords, LAPS, Credential Guard) mitigate them; internalize legal constraints in lab work.
9	Phases of Ethical Hacking with Red/Blue Actions	Phases: Reconnaissance, Scanning/Enumeration, Gaining Access, Maintaining Access, Clearing Tracks; detailed recon (passive/active, OSINT, Google dorks, WHOIS, DNS, Shodan, WAFW00F, theHarvester, Sublist3r, ExifTool), blue recon defenses; scanning (Netdiscover, Nmap, Gobuster, DirBuster, Dirsearch, Nikto); gaining access (phishing, email spoofing, SQLi, password cracking, DoS/DDoS, MitM, ESP32 Evil Twin, Rubber Ducky PIN brute-force, insider attacks); maintaining access (web shells, backdoors, cron/scheduled tasks, privilege escalation); covering tracks (clearing logs on Windows & Linux, anti-forensics; centralized logging and blue-team hardening checklist).	5	Describe and apply the 5 phases of ethical hacking in order; perform basic recon, scanning, exploitation, persistence, and covering tracks in controlled lab environments; clearly separate Red Team actions from Blue Team detection and hardening strategies at each phase.
10	VAPT on Vulnerable OS, Websites & Apps	VAPT lifecycle aligned with ethical hacking phases: planning & scoping (rules of engagement, legal), information gathering & threat modeling, vulnerability assessment (scanning OS, services, web apps, APIs, DBs), exploitation (manual + tools), post-exploitation, validation & re-testing, reporting; lab focus: using vulnerable OS/VMs and deliberately vulnerable web apps (e.g., DVWA-like) to practice OS-level and web VAPT; tools: Nmap, Netdiscover, Gobuster, DirBuster, Dirsearch, Nikto,	5	Conduct a structured VAPT on vulnerable OS and web applications from scoping to retest; choose appropriate tools for each stage (recon, scanning, exploitation); interpret and prioritize vulnerabilities; understand how VAPT feeds both

		Burp Suite, SQLmap, Metasploit; OWASP-style issues (SQLi, XSS, weak auth, misconfigurations); mapping each action to Red Team (executing tests) and Blue Team (fixing, patching, monitoring).		offensive (Red) and defensive (Blue) improvement cycles.
12	VAPT Reporting & Documentation	Importance of professional reporting; structure of a VAPT/penetration test report: cover page & legal scope, executive summary, methodology, environment & tools, detailed findings (title, description, affected assets, evidence/output, risk rating, CVSS, impact, likelihood, exploitation steps, PoC), remediation and recommendations, appendices (scans, screenshots, logs); mapping all labs (Recon, Scanning, Exploitation, Persistence, Covering Tracks, Blue hardening) into a final capstone report; ethical disclosure and handling of sensitive data.	4	Produce a clear, professional VAPT report aligned with industry expectations; organize findings logically with evidence and risk ratings; write actionable remediation guidance; adhere to ethical disclosure practices when handling vulnerabilities and data.

Fundamentals, Ethics & OS Basics

Day	Duration	Topics / Activities	Module Mapping
Day 1	3 hrs	Why Cybersecurity Is Important; What Is Cybersecurity; CIA Triad; Types of Cybersecurity; real incidents; short introduction to Ethical Hacker, Pen Tester, Red/Blue/Purple teams.	M1
Day 2	3 hrs	Types of Cyber Attacks; Malware categories and flows; Ransomware lifecycle; DDoS types; MitM; SQL Injection; Zero-Day & Social Engineering; infection signs and basic malware removal steps.	M2
Day 3	3 hrs	Types of Hackers; Motives of Hackers; Ethics of a Hacker; Ethical vs Criminal hacking; Challenges of Cybersecurity & mitigation; Cyber Laws (IT Act sections, GDPR, CFAA, CCPA, HIPAA); Skills required to become a security professional.	M3

OS Installation & Networking Foundations

Day	Duration	Topics / Activities	Module Mapping
Day 4	3 hrs	OS comparison (Windows/macOS/Linux); features and security; OS installation methods: Live Mode USB, Live + Persistence USB (detailed Kali persistent USB with LUKS), VMware/VirtualBox installation, Dual Boot internal/external; lab/demo: Kali Live USB + VMware setup.	M4
Day 5	3 hrs	Networking basics (definition, working, email data path); key terms (node, link, packet, protocol, IP, MAC, bandwidth, latency); network architectures (Client-Server, P2P); network devices (router, switch, hub, bridge, gateway, firewall, IDS/IPS, NAC, SIEM); goals & uses of networks; classification (PAN, LAN, MAN, WAN; guided/unguided; private/public/VPN; Internet/Extranet/Intranet); activity: draw and label a small office network.	M5
Day 6	3 hrs	OSI model (7 layers, protocols, devices); TCP/IP model (4 layers, mapping); physical/data link concepts (topologies, transmission modes, bandwidth); Wi-Fi & Bluetooth standards; Wi-Fi security protocols (WEP/WPA/WPA2/WPA3); exercise: map attacks like SQLi, ARP poisoning, DDoS, MitM, Evil Twin to OSI/TCP-IP layers.	M6

IP, Commands, Scripting & Lab Foundations

Day	Duration	Topics / Activities	Module Mapping
Day 7	3 hrs	Network layer & IP addressing (IPv4 vs IPv6, classful addressing, private vs public IP, subnetting basics, IP lookup commands); Transport layer (TCP/UDP, 3-way handshake); Session/Presentation/Application layers (ports, SSL/TLS, WWW, DNS, CDN); Network Security elements (firewall, IDS/IPS, VPN, NAC, SIEM, segmentation, WAF, email gateway); lab: IP-focused CLI practice (ip a, ifconfig, ipconfig, ping, traceroute/tracert, nslookup/dig, netstat/ss, arp -a).	M6
Day 8	3 hrs	OS commands – Linux vs Windows (navigation, file/dir, text processing, network commands, processes, system info); Linux file permissions (representation, chmod, chown/chgrp, SUID/SGID/sticky bit); history & environment variables commands; lab: permissions and command practice in Kali (set scripts executable, protect SSH keys, apply sticky bit).	M7
Day 9	3 hrs	Introduction to scripting & automation; Linux Bash scripting fundamentals; Windows Batch scripting (backup script, age classification script, educational “virus” demo); PowerShell scripting (variables, loops, file operations, security cmdlets); lab: implement Linux file-sorting and age scripts; run PowerShell backup script.	M7

Ethical Hacking Phases, VAPT Intro & Hardenin

Day	Duration	Topics / Activities	Module Mapping
Day 10	3 hrs	Introduction to Ethical Hacking (definitions incl. Red/Blue/Purple team, CVE, Zero-Day); legal boundaries & non-negotiable rules; Kali Live USB + VMware recap; Linux password reset via GRUB (modify boot parameters, enter single-user mode, set password); securing GRUB with password; Windows password reset/boot-ISO overview; Blue Team hardening (BitLocker, Secure Boot, BIOS password, LAPS, Credential Guard).	M8
Day 11	3 hrs	Phase 1 – Reconnaissance and OSINT: Google dorking cheat sheet; OSINT framework; WHOIS; DNS queries; Shodan; WAFW00F; theHarvester; Sublist3r; ExifTool; Blue recon defenses (information exposure reduction, metadata cleaning, DMARC/SPF/DKIM, OSINT monitoring); lab: OSINT on lab-safe domains.	M9
Day 12	3 hrs	Phase 2 – Scanning & Enumeration: Netdiscover host discovery; Nmap scan types and output interpretation; Gobuster/DirBuster/Dirsearch; Nikto; mapping scan results to vulnerabilities; VAPT lifecycle introduction (scope, recon, scanning, exploitation, post-exploitation, retest, reporting); lab: Netdiscover/Nmap on lab subnet with vulnerable OS; run Gobuster/Nikto on lab web app.	M9, M10

Gaining Access, Red vs Blue, VAPT & Reporting

Day	Duration	Topics / Activities	Module Mapping
Day 13	3 hrs	Phase 3 – Gaining Access: phishing concepts; email spoofing and mail authentication (SPF/DKIM/DMARC); SQL Injection basics & SQLmap; password cracking (Hashcat/John); DoS/DDoS; MitM (ARP poisoning, SSL stripping, rogue AP); ESP32 Evil Twin Wi-Fi lab; Rubber Ducky PIN brute-force simulation; insider attacks; lab: SQLi tests on vulnerable web app (SQLmap/manual), observe MitM/Evil Twin demo and detection.	M9, M10
Day 14	3 hrs	Phase 4 – Maintaining Access: web shells, backdoors, cron/Task Scheduler persistence, privilege escalation; Phase 5 – Covering Tracks: clearing logs in Windows/Linux, anti-forensics; Blue Team responses (centralized logging, immutable logs, SIEM, EDR, blue toolkit); Red Teaming vs Blue Teaming consolidation: definitions, roles, comparison table, case-mapping of previous labs into Red vs Blue sequences.	M9, M11
Day 15	3 hrs	VAPT Reporting & Capstone: report structure (scope, executive summary, methodology, environment & tools, detailed findings, risk ratings, remediation, appendices); capstone lab: prepare a VAPT report for vulnerable OS/web/app used in labs, separating Red findings and Blue remediation plans; peer review of reports.	M12

Evaluation & Deliverables Checklist

You can keep your scheme flexible; this version explicitly includes hacking tools demonstrations.

1. Class Participation & Quizzes (10–15%)

- Short quizzes on:
  - Cybersecurity fundamentals, threats, and malware.
  - Networking basics and OSI/TCP-IP.
  - Hacker types, ethics, and cyber laws.
- Observation of engagement during live hacking tools demonstrations (e.g., questions and ability to interpret basic tool outputs).

2. Lab Exercises & Practical Checkpoints (30–35%)

- OS and lab setup tasks (Kali Live/persistent USB, VMs, dual boot; Linux/Windows password reset and hardening).
- Networking and CLI labs (IP addressing, network commands, Linux permissions, Bash/PowerShell/Batch scripting).
- Ethical hacking phase labs:
  - Recon and OSINT on lab-safe domains using tools such as WHOIS, Shodan, theHarvester, WAFW00F, Sublist3r, ExifTool.
  - Scanning and enumeration on vulnerable OS/VMs using Netdiscover, Nmap, Gobuster/DirBuster/Dirsearch, Nikto.
  - Initial exploitation labs on vulnerable web apps with SQLmap and Burp Suite (basic SQLi, input validation and auth weaknesses).!

3. Mini VAPT Assignment(s) (20–25%)

- Individual or small-group VAPT on a provided vulnerable OS or web app.
- Required deliverables:
  - Defined scope and rules of engagement.
  - Tool plan and usage (e.g., Nmap for discovery, Gobuster/DirBuster/Dirsearch and Nikto for web mapping, Burp Suite and SQLmap for exploitation, Metasploit where appropriate).
  - Evidence of findings (screenshots, command outputs, logs, brief notes on exploitation steps).

4. Hacking Tools Demonstration & Reflection (10–15%)

- Guided demonstration sessions where the instructor showcases:
  - Discovery and scanning (Netdiscover, Nmap).
  - Web and directory fuzzing (Gobuster, DirBuster, Dirsearch, Nikto).
  - Web exploitation and automation (Burp Suite, SQLmap, Metasploit modules) against vulnerable OS/web apps.
- Short reflection sheet or checklist from each learner:
  - Tool purpose and phase mapping (recon, scanning, exploitation, post-exploitation).
  - At least one key observation from each demo (e.g., how a specific vulnerability was identified or exploited).

5. Red vs Blue Team Exercise (10–15%)

- Scenario-based activity where:
  - Red side documents a simple attack path using the demonstrated tools (e.g., Nmap → Gobuster → SQLmap/Burp).
  - Blue side proposes detections, hardening, and monitoring (e.g., firewall rules, WAF, SIEM alerts, log review).
- Short written mapping of each step to Red/Blue responsibilities.

6. Final VAPT Capstone Project & Report (25–30%)

- End-to-end VAPT on an assigned vulnerable OS/website/app already used in labs.
- Final deliverables:
  - Formal VAPT report (scope, methodology, environment, detailed findings, CVSS or similar rating, remediation, appendices).
  - Clear evidence of tool usage across stages (screenshots/logs from Nmap, web scanners, Burp Suite/SQLmap/Metasploit where relevant).
  - Optional short presentation or viva explaining the attack chain, tool choices, and proposed defensive measures from a Blue Team perspective.