TECHONQUER

BASIC TO ADVANCED PROGRAM

Cybersecurity Mastery.

Ethical Hacking, VAPT, Web and API Security, WiFi Security, SOC Operations and Android Security. **6 levels, 21 modules.** Live classes on **Friday, Saturday and Sunday**, with **lifetime access** to every recording.

Level 1	Networking, operating systems, scripting and security fundamentals
Level 2	Ethical hacking: recon, system hacking, network attacks, social engineering
Level 3	VAPT, web and application security, API security, infrastructure testing
Level 4	WiFi security and Android mobile security in 3 focused classes
Level 5	SOC and blue team: SIEM, incident response, threat hunting, forensics
Level 6	Cloud security and red team basics

W techonquer.org
E info@techonquer.org
P +91 63670 98233

How the program runs

Live weekend batches, so working professionals and students can attend without disturbing the weekday schedule.

FRI SAT SUN Three live instructor led classes every week, with labs and doubt solving in the same session.

Lifetime Access to every class recording, notes and lab files. Miss a class, watch the recording and continue.

WHAT THE PROGRAM INCLUDES

- 21 modules across 6 levels
- 4 capstone projects with reports
- Guided home lab setup
- Certification roadmap

CURRICULUM AT A GLANCE

LEVEL	FOCUS	MODULES
Level 1	Foundations	01 - 04
Level 2	Ethical hacking	05 - 09
Level 3	VAPT, web and application security	10 - 13
Level 4	Wireless and mobile security	14 - 15
Level 5	SOC and blue team	16 - 19
Level 6	Advanced topics	20 - 21

LEVEL 01

Foundations

Modules 01 - 04

01 IT and Networking Basics

- How computers, operating systems and the internet work
- OSI and TCP/IP models, IP addressing, subnetting, MAC addresses
- Protocols: HTTP and HTTPS, DNS, DHCP, FTP, SSH, SMTP, ARP, ICMP
- Firewalls, routers, switches, VPNs, proxies and NAT
- Wireshark basics and packet analysis

02 Operating Systems

- Linux: file system, permissions, users, processes, bash commands
- Windows: registry, services, Active Directory basics, PowerShell basics
- Virtualisation with VirtualBox and VMware
- Building a home lab from zero

03 Programming and Scripting

- Python: basics, sockets, requests, automation scripts
- Bash scripting and PowerShell basics
- SQL basics and reading simple JavaScript and PHP

LEVEL 01

Foundations (continued)

Modules 01 - 04

04 Security Fundamentals

- CIA triad, threats, vulnerabilities, risk and attack types
- Cryptography: hashing, symmetric and asymmetric encryption, digital signatures, SSL and TLS
- Authentication, MFA and access control
- Frameworks: NIST, ISO 27001, MITRE ATT&CK

LEVEL 02

Ethical Hacking

Modules 05 - 09

05 Ethical Hacking Methodology

- Types of hackers and the legal side of testing
- Phases: reconnaissance, scanning, gaining access, maintaining access, covering tracks, reporting
- Lab setup: Kali Linux, Metasploitable, DVWA, Hack The Box, TryHackMe

LEVEL 02

Ethical Hacking (continued)

Modules 05 - 09

06 Information Gathering

- Passive recon: OSINT, Google dorking, Shodan, theHarvester, Maltego
- Active recon: Nmap, Netcat, DNS enumeration
- Vulnerability scanning with Nessus and OpenVAS

07 System Hacking

- Password attacks: brute force, dictionary, Hydra, John the Ripper, Hashcat
- Enumeration of SMB, SNMP, LDAP and NetBIOS
- Exploitation with Metasploit
- Privilege escalation on Linux and Windows
- Persistence and post exploitation concepts

08 Network Attacks

- Sniffing, ARP spoofing, MITM concepts, DNS spoofing
- DoS and DDoS concepts and defences
- Session hijacking
- IDS, IPS and firewall evasion concepts

LEVEL 02 Ethical Hacking (continued) — Modules 05 - 09

09 Social Engineering and Malware Basics

- Phishing, vishing and pretexting, awareness and simulation
- Types of malware: virus, worm, trojan, ransomware, RAT
- Basic static and dynamic analysis in a sandbox

LEVEL 03 VAPT and Application Security

Modules 10 - 13

10 Web Application Security

- OWASP Top 10: injection, broken authentication, XSS, CSRF, IDOR, SSRF, security misconfiguration, XXE, insecure deserialisation
- SQL injection, manual and with sqlmap
- Tools: Burp Suite, OWASP ZAP, ffuf, Nikto, Gobuster
- File upload, LFI and RFI, command injection
- Business logic flaws, authentication and session testing

11 API Security

- REST, SOAP and GraphQL basics
- OWASP API Top 10
- Testing with Postman and Burp Suite

LEVEL 03

VAPT and Application Security (continued)

Modules 10 - 13

12 VAPT Process

- Scoping, rules of engagement and NDAs
- Vulnerability assessment against penetration testing
- Black box, grey box and white box testing
- Types: web, network, mobile, cloud, internal and external
- Risk rating with CVSS and CWE and CVE
- Report writing: executive summary, technical findings, proof of concept, remediation
- Retesting and closure

13 Network and Infrastructure VAPT

- Internal and external network pentesting
- Active Directory attacks: Kerberoasting, Pass the Hash, BloodHound, lateral movement
- Firewall and configuration review
- Server hardening

LEVEL 04

Wireless and Mobile Security

Modules 14 - 15

14 WiFi Security and Hacking

- Wireless standards: 802.11 a, b, g, n, ac and ax
- Encryption: WEP, WPA, WPA2, WPA3
- Monitor mode and packet capture with the Aircrack-ng suite
- WEP, WPA and WPA2 attacks: handshake capture and cracking, PMKID
- Evil Twin and Rogue AP, deauthentication attacks, WPS weaknesses
- Enterprise WiFi and captive portal attacks
- Tools: Aircrack-ng, Wifite, Kismet, Bettercap
- Defence: WPA3, strong passphrases, WIDS and WIPS, network segmentation

15 Mobile Security, Android, 3 classes

- **Class 1** Android architecture, sandbox, permissions, APK structure, app components, emulator and rooted device lab, OWASP Mobile Top 10
- **Class 2** Decompiling APKs with apktool and jadx, manifest review, MobSF scanning, hardcoded secrets, insecure storage, Burp proxy interception
- **Class 3** Frida and Objection, SSL pinning and root detection bypass, Drozer, practice on InsecureBankv2 and DIVA, short mobile VAPT report, iOS overview

LEVEL 05

SOC and Blue Team

Modules 16 - 19

16 SOC Fundamentals

- SOC structure: L1, L2 and L3 analysts and incident responders
- Log sources: Windows Event Logs, Syslog, firewall, proxy and EDR logs
- Cyber Kill Chain and MITRE ATT&CK mapping

17 SIEM and Monitoring

- Splunk, Elastic (ELK), Wazuh or Microsoft Sentinel
- Writing queries, alerts, correlation rules and dashboards
- Alert triage, false positives and escalation

18 Incident Response and Threat Hunting

- IR lifecycle: preparation, detection, containment, eradication, recovery, lessons learned
- Phishing email analysis and malware triage
- Threat intelligence: IOCs, VirusTotal, MISP, AbuseIPDB
- Basic threat hunting hypotheses
- Digital forensics basics: disk and memory with Autopsy and Volatility

LEVEL 05

SOC and Blue Team (continued)

Modules 16 - 19

19 Defensive Tools

- EDR and XDR, IDS and IPS with Snort and Suricata, and Zeek
- Network monitoring and honeypots

LEVEL 06

Advanced Topics

Modules 20 - 21

20 Cloud Security

- AWS, Azure and GCP misconfigurations, IAM, S3 exposure
- Docker and Kubernetes basics

21 Red Team Basics

- C2 concepts, evasion concepts, adversary emulation, purple teaming

PRACTICE PLATFORMS

TryHackMe, Hack The Box, PortSwigger Web Security Academy, OverTheWire, VulnHub, PicoCTF, CyberDefenders, LetsDefend, Blue Team Labs Online.

CAPSTONE PROJECTS

01 Full VAPT of a vulnerable web app with a professional report

02 Home SOC lab on Wazuh or Splunk with attack simulation and detection

03 WiFi security assessment in your own lab

04 Android app security test, static and dynamic, with a short report

CERTIFICATION PATH, OPTIONAL

STAGE	CERTIFICATIONS
Beginner	CompTIA Network+ and Security+, CEH
Intermediate	eJPT, PNPT, CompTIA CySA+, BTL1
Advanced	OSCP, CRTP, GPEN and GCIH

Book your seat

Talk to the team for the batch date, fees and seats left.

techonquer.org

info@techonquer.org

+91 63670 98233