TECHONQUER

LIVE ONLINE TRAINING

COURSE SYLLABUS

Red Team Training

A live, hands-on program covering web, API and network attacks, advanced Active Directory exploitation, Android pentesting basics, SIEM basics and AI security basics, ending with a full red team capstone and professional reporting.

Duration **3 Months**	Mode **Live online**	Level **Advanced**
Mentor **Mayank**	Fee **Rs 10,000**	Payment **Rs 5,000 + Rs 5,000**

Requirements

- Basic networking and Linux knowledge
- Basic understanding of how web applications work
- Laptop with minimum 8GB RAM (16GB recommended)

Skills You Will Master

01	**Web and API Exploitation**	OWASP Top 10, SQLi, XSS, SSRF, BOLA, JWT and GraphQL attacks
02	**Network Penetration Testing**	Service exploitation, privilege escalation, pivoting and tunneling
03	**Advanced Active Directory**	Kerberoasting, delegation abuse, AD CS, DCSync, Golden and Silver Tickets
04	**Android, SIEM and AI Security**	APK analysis and Frida, SIEM detection awareness, LLM prompt injection
05	**Red Team Reporting**	Capstone engagement, evidence collection and professional reports

Course Modules

01 Red Team Fundamentals and Reconnaissance

Learn how real red team engagements are planned, scoped and run.

- Red teaming vs penetration testing vs vulnerability assessment
- Rules of engagement, scoping, legal authorization and OPSEC basics
- Cyber Kill Chain and MITRE ATT&CK for adversary emulation
- Passive and active reconnaissance, OSINT and attack surface mapping
- Subdomain, port and service enumeration

Tools and Labs: Kali Linux, Nmap, Amass, Subfinder, theHarvester, Shodan

02 Web Application Attacks

Find and exploit the web flaws attackers use for initial access.

- OWASP Top 10 in practice on real vulnerable applications
- SQL injection, XSS, command injection and SSTI
- Authentication bypass, session flaws and IDOR
- SSRF, file inclusion and insecure file upload
- Business logic flaws and chaining bugs for higher impact

Tools and Labs: Burp Suite, ffuf, sqlmap, Gobuster

03 API Security Testing

Test REST and GraphQL APIs the way modern applications are attacked.

- OWASP API Security Top 10
- BOLA and BFLA (broken object and function level authorization)
- JWT attacks, broken authentication and token flaws
- Mass assignment, excessive data exposure and rate limit bypass
- GraphQL introspection and query abuse

Tools and Labs: Burp Suite, Postman, jwt_tool, Arjun

04 Network Penetration Testing

Move from an external foothold to full internal network compromise.

- Network scanning, service enumeration and vulnerability discovery
- Exploiting common services: SMB, FTP, SSH, RDP and databases
- Linux and Windows privilege escalation
- Password attacks, hash cracking and credential reuse
- Pivoting and tunneling into segmented networks

Tools and Labs: Nmap, Metasploit, NetExec, Hashcat, Ligolo-ng, Chisel

05 Active Directory Attacks (Advanced)

Compromise enterprise Windows domains with advanced, real world AD attack chains.

- AD enumeration and attack path mapping with BloodHound
- Kerberoasting, AS-REP Roasting and password spraying
- Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash
- Delegation abuse: unconstrained, constrained and RBCD
- AD CS abuse with Certipy (ESC1 to ESC8)
- ACL abuse, DCSync, Golden and Silver Tickets
- Lateral movement, domain persistence and forest trust attacks

Tools and Labs: BloodHound, Impacket, Rubeus, Mimikatz, Certipy, NetExec

06 Android Pentesting Basics

Get started with mobile application security testing on Android.

- Android architecture, APK structure and app permissions
- Lab setup with an emulator and ADB
- Static analysis: decompiling and reviewing APKs
- Dynamic analysis and runtime hooking basics
- SSL pinning bypass basics and traffic interception
- OWASP Mobile Top 10: insecure storage, hardcoded secrets, exported components

Tools and Labs: ADB, jadx, MobSF, Frida, Objection, Burp Suite

07 SIEM Basics for Red Teamers

Understand what defenders see, so you can operate quietly and report like a professional.

- How a SOC works and how a SIEM detects attacks
- Log sources: Windows event logs, Sysmon, network and web logs
- Mapping your attack activity to common detections
- Detection aware operations and basic OPSEC
- Reducing noise and avoiding easy alerts
- Purple teaming basics: working with the blue team

Tools and Labs: Splunk, Wazuh, Sysmon

08 AI Security Basics

Learn to test AI powered applications, the newest attack surface.

- How LLM applications work: prompts, context, tools and RAG
- OWASP Top 10 for LLM Applications
- Direct and indirect prompt injection
- Jailbreaks, system prompt leakage and sensitive data exposure
- Insecure output handling and excessive agency in AI agents

Tools and Labs: AI application test labs, Burp Suite, LLM red teaming exercises

09 Capstone and Red Team Reporting

Run a full engagement from recon to domain compromise, then write it up like a professional.

- End to end simulation: web or API foothold all the way to Domain Admin
- Chaining vulnerabilities across web, network and Active Directory
- Evidence and screenshot collection and building the attack narrative
- Writing clear executive summaries for non-technical stakeholders
- Detailed technical findings with steps to reproduce
- Risk rating with CVSS and practical remediation guidance

Tools and Labs: Full red team toolchain, professional report template

Program Details

Total fee	Rs 10,000
At registration	Rs 5,000, paid online to reserve your seat
After one month	Remaining Rs 5,000
Duration	3 months, live online
Mentor	Mayank
Recordings	Provided for revision
Included	Live classes, hands-on labs, 1-to-1 mentor support, capstone and placement assistance

Placement Assistance

Red team focused CV building, technical mock interviews, report writing practice and regular sharing of job and internship openings throughout the program.

No job guarantee. The program makes you job ready through practical skills and interview preparation. Final selection depends on individual performance and employer criteria.

Why Learn Red Teaming with Techonquer

Attacker Mindset
Learn full attack chains, not isolated tricks, from recon to domain admin.

Advanced Active Directory
Go deep into Kerberos, delegation, AD CS and domain persistence.

Modern Attack Surface
Web, API, Android, SIEM awareness and AI security in one program.

Live and Hands-On
Real labs, 1-to-1 mentor support and a full capstone engagement.

Ready to enroll?

Fee Rs 10,000 | Rs 5,000 at registration, Rs 5,000 after one month
Visit **techonquer.org/red-team-training**
Email: info@techonquer.org | WhatsApp: +91 63670 98233

Syllabus details may be updated to keep the content current. Training is provided for authorized, ethical security testing only.