TECHONQUER ELITE ETHICAL HACKER Training

Duration: 8 Weeks (4 Classes per Week) | Class Duration: 2 Hours

Week 1: Introduction & Information Gathering

Introduction to Cyber Security & Ethical Hacking

- Cyber Security Basics & Terminologies
- Types of Hackers & Attack Methodologies
- Understanding Cyber Kill Chain & MITRE ATT&CK

Footprinting & OSINT

- Passive & Active Reconnaissance
- Google Dorking & Shodan
- WHOIS, DNS, and Subdomain Enumeration

Network Scanning & Enumeration

- Port Scanning (Nmap, Masscan)
- Banner Grabbing & Fingerprinting
- SMB, SNMP, LDAP & FTP Enumeration

Week 2: Network Hacking & System Exploitation

Packet Sniffing & MITM Attacks

- ARP Poisoning & Spoofing
- Packet Analysis (Wireshark, Tcpdump)
- Session Hijacking & Credential Harvesting

WiFi Hacking & Wireless Security

- Cracking WEP, WPA/WPA2
- PMKID Attack & Evil Twin Attack
- Rogue Access Point & Deauthentication Attacks

Network Exploitation & Firewall Bypassing

- Exploiting SMB, RDP, FTP & SSH
- VLAN Hopping & Port Redirection
- IDS/IPS Evasion Techniques

Week 3: Web Application Hacking (OWASP Top 10)

SQL Injection (SQLi)

- Error-Based, Blind & Time-Based SQLi
- Dumping Data Using SQLMap & Manual Injection
- WAF Bypassing & Advanced SQLi Techniques

Cross-Site Scripting (XSS) & Other Web Attacks

- Reflected, Stored & DOM-Based XSS
- XSS Payload Crafting & Filter Bypassing
- Command Injection, LFI, RFI & Directory Traversal

API & Web Security Misconfigurations

- API Security Testing (GraphQL & REST)
- Broken Authentication & Session Management
- Insecure Deserialization & SSRF

Week 4: System Hacking & Privilege Escalation

Windows & Linux System Exploitation

- Exploiting Windows & Linux Services
- Metasploit for System Hacking
- Reverse Shells & Post Exploitation

Password Cracking & Credential Dumping

- Cracking Hashes (John, Hashcat, Hydra)
- Mimikatz & NTLM Hash Dumping
- Brute Force Attacks & Dictionary Attacks

Privilege Escalation & Persistence

- Linux Privilege Escalation (SUID, Cronjobs, Kernel Exploits)
- Windows Privilege Escalation (Unquoted Service Paths, DLL Hijacking)
- Creating Backdoors & Maintaining Access

Week 5: Wireless, Mobile & Cloud Security

Advanced WiFi Attacks

- WPA3 Cracking & WPS Attacks
- Capturing & Cracking Handshakes
- Evil Twin Attack & Rogue AP Setup

Mobile Application Pentesting

- Android & iOS Pentesting Basics
- APK Reverse Engineering & Code Injection
- Exploiting Insecure Mobile API Calls

Cloud Security & Misconfigurations

- AWS S3 Bucket Enumeration & Data Exfiltration
- Azure & GCP Security Misconfigurations
- Exploiting Cloud Metadata APIs

Week 6: Active Directory & Social Engineering

Active Directory Attacks

- AD Enumeration (BloodHound, CrackMapExec)
- Kerberoasting & AS-REP Roasting Attacks
- Pass-the-Hash, Pass-the-Ticket, Golden Ticket Attacks

Phishing & Social Engineering

- Crafting Phishing Emails & Malicious Links
- Malicious Macros & Office Document Exploits
- USB Drop Attacks & Credential Harvesting

Red Team vs. Blue Team Basics

- Understanding Red & Blue Team Operations
- Basic Incident Response & Log Analysis
- SIEM Tools & Threat Hunting

Week 7: Red Teaming Basics & Post Exploitation

Creating Undetectable Payloads

- Obfuscation & Encoding Techniques
- Using Veil, Shellter & Metasploit Payloads
- PowerShell & Macro-based Payloads

Bypassing Antivirus & EDR

- Signature & Heuristic-Based Detection Evasion
- Process Injection & Memory Manipulation
- AMSI Bypass & UAC Bypass Techniques

Lateral Movement & Data Exfiltration

- Pivoting Using SSH, RDP & Tunneling
- Exploiting Trust Relationships in AD
- Exfiltrating Data Without Detection

Week 8: Capture the Flag (CTF) & Professional Reporting

Web, Network, AD & Cloud CTF Challenges

- Real-World Scenarios for Hacking Practice
- Simulated Red Team Engagements
- Practical CTF Walkthroughs

Professional Pentest Report Writing

- Writing Executive & Technical Reports
- Risk Assessment & CVSS Scoring
- Tools for Automating Reports (Dradis, Faraday)

Career Guidance & Bug Bounty Hunting

- Bug Bounty Platforms (HackerOne, Bugcrowd, Intigriti)
- Freelancing in Cyber Security
- Resume Building & Interview Preparation

Certification: TECHONQUER ELITE ETHICAL HACKER

- **CEH Level + Advanced Practical Skills**
- **Hands-on Labs & Real-World CTF Challenges**
- Practical Red Team & Blue Team Exposure