ForumDE
Code your career

CYBER SECURITY & ETHICAL HACKING

Syllabus

What you'll learn on this Cyber Security & Ethical Hacking journey

1. Foundations — Systems, Networking & Basics

Master Linux, Windows, and networking fundamentals while learning Bash, PowerShell, and Python scripting for security tasks

2. Core Security & Reconnaissance

Learn how attackers gather information and perform reconnaissance using tools like nmap, the Harvester, Shodan, and Burp Suite.

3. Web App Security & Exploitation

Dive deep into OWASP Top 10 vulnerabilities like SQLi, XSS, and CSRF. Practice with Burp Suite, SQLMap, and PortSwigger labs.

4. Network, System & Privilege Escalation

Learn vulnerability scanning, exploitation, privilege escalation, and post-exploitation techniques using Metasploit and BloodHound.

5. Wireless, Mobile & Specialized Areas

Explore wireless security, mobile app analysis, API & cloud security, and social engineering fundamentals — ethically and safely.

6. Reporting, Certifications & Real Projects

Build professional pentesting reports, understand compliance and legal boundaries, and prepare for certifications or bug bounty work.

Month 1 — Foundations: Systems, Networking & Basics

- Lecture 1: Introduction to Cyber Security
- Linux Fundamentals — File System, Permissions, Shell
- Windows Basics & PowerShell Essentials
- Networking: TCP/IP, DNS, DHCP, ARP, HTTP/HTTPS, SSL/TLS
- Python Scripting for Security Automation
- Hands-on: Setting Up Dual VMs (Kali + Ubuntu/Windows)

Month 2 — Core Security Concepts & Reconnaissance

- Footprinting & OSINT Techniques
- Active vs Passive Reconnaissance
- Scanning & Enumeration with Nmap, Masscan
- Understanding Web Technologies & HTTP Requests
- Common Vulnerabilities (OWASP + Network)
- Tools: nmap, netcat, whois, theHarvester, Shodan, Burp Suite
- Hands-on: Recon Reports for DVWA / Juice Shop

Month 3 — Web Application Security & Exploitation

- OWASP Top 10 Deep Dive (SQLi, XSS, CSRF, etc.)
- Authentication & Session Attacks
- Input Validation & Logic Flaws
- Tools: Burp Suite, SQLMap, ZAP, Postman
- Hands-on: Exploiting OWASP Juice Shop & DVWA
- Writeups & Remediation Techniques

Month 4 — Network, System & Privilege Escalation

- Vulnerability Scanning (Nessus, OpenVAS)
- Exploitation Basics with Metasploit
- Windows Domain, SMB, Kerberos, LDAP
- Lateral Movement & Persistence
- Privilege Escalation (LinPEAS, WinPEAS)
- Hands-on: Compromising and Escalating in Lab VMs

Month 5 — Wireless, Mobile & Specialized Areas

- Wireless Security (WEP/WPA/WPA2/WPA3)
- Mobile App Security (Android/iOS)
- API Security & Cloud Misconfigurations (AWS, IAM)
- Social Engineering & Phishing Awareness (Ethical)
- Tools: aircrack-ng, Wireshark, MobSF, mitmproxy
- Hands-on: Wi-Fi Cracking, Cloud Misconfig Labs

Month 6 — Reporting, Certifications & Real Work

- Writing Professional Pentest Reports
- Legal, Compliance & Responsible Disclosure
- Soft Skills: Client Communication & Reporting
- Bug Bounty Platforms: HackerOne, Bugcrowd
- Portfolio Building: Writeups, GitHub & Medium
- Career Prep: SOC Analyst, Pentester, Red Team Intern

DURATION OF COURSE	**6 MONTHS**
FEES OF THE COURSE	**₹34,999**

Apart from above course details, we will also deliver below: -

- *We will guide you what kind of questions can be asked in interview.*
- *We will help you in building your resume.*
- *We will take mock interview to prepare you for real time interview.*
- ***Upon completion of the course, learners will be issued a formal certificate recognizing their achievement.***
- ***The total duration of the course is five months.***
- ***All sessions will be conducted through live online classes.***
- ***Gain valuable insights from an industry veteran with more than ten years of hands-on experience.***

Sharing of videos to another person is strictly prohibited.

Contact us For Admission or Queries: -

+91-70429 28331

+91-98018 30173