COMPLETE ADVANCED

CYBER SECURITY TRAINING

LIVE 2 MONTHS LIVE TRAINING

GREYHAT INSTITUTE

Vikram Kumar — Trainer

AI-Powered Cyber Security & Ethical Hacking Course

From Zero to Intermediate-Level Cybersecurity Skills

Module 1 – Introduction to Ethical Hacking

Module 2 – Networking for Hackers

Module 3 – Lab Setup - VMware & VM Roles

Module 4 – Essential Kali Linux

Module 5 – Advanced IP Addressing

Module 6 – Information Gathering & Reconnaissance

Module 7 – Network Scanning

Module 8 – Vulnerability Analysis + Malware Threats

Module 9 – Wi-Fi Hacking

Module 10 – System Hacking

Module 11 – Social Engineering

Module 12 – Advanced Attacks & Web Security

Module 13 – Dark Web & Deep Web Access

Complete Modules

Module 1: Introduction to Ethical Hacking

Foundation concepts and first class overview

- ✅What is Ethical Hacking and Why it Matters
- ✅Legal and Ethical Considerations
- ✅Career Opportunities in Cybersecurity
- ✅Course Overview and Learning Path

Module 2: Networking for Hackers

Core networking concepts and packet analysis

- ✅OSI & TCP/IP models and how data flows
- ✅TCP/UDP and common services (HTTP, DNS, SSH)
- ✅Capture and inspect packets with Wireshark
- ✅IP addressing, MAC address fundamentals
- ✅Network devices: routers, switches, firewalls
- ✅Firewalls, ACLs, VLANs, and network segmentation

Module 3: Lab Setup - VMware & VM Roles

Setting up your complete hacking lab environment

- ✅VMware setup - host and isolate lab VMs
- ✅Kali Linux - attacker workstation for pentesting
- ✅Windows Server 2022 - realistic target with server services
- ✅Metasploitable2 - intentionally vulnerable practice target
- ✅Snapshots & troubleshooting - restore lab states

Module 4: Essential Kali Linux

Master the hacker's operating system

- ✅Basic navigation commands - move between files and folders
- ✅User & sudo setup - create users and give sudo permissions
- ✅File permissions - manage access with chmod & chown
- ✅Package management - install and update tools with apt
- ✅Network commands - check and troubleshoot connections

Module 5: Advanced IP Addressing

Deep dive into network addressing and subnetting

- ✅Understanding public vs private IPs and their uses
- ✅Subnetting in detail: dividing networks and calculating ranges
- ✅Gateway, broadcast, and network addresses explained
- ✅NAT (Network Address Translation) and network connections
- ✅IP configuration in lab VMs and troubleshooting

Module 6: Information Gathering & Reconnaissance

OSINT and intelligence gathering techniques

- ✅Active & Passive Techniques: collect public data vs probe targets
- ✅OSINT Tools: Shodan, theHarvester, Recon-ng for discovery
- ✅WHOIS & DNS: domain owner, DNS records, subdomains
- ✅Email Reconnaissance: find emails, verify headers
- ✅Organize Findings: save outputs and build asset lists

Module 7: Network Scanning

Discover hosts, ports, and running services

- ✅Purpose: discover hosts, open ports, running services (ethical, lab-only)
- ✅Port scanning with Nmap: basic scans, service/version detection
- ✅Banner grabbing & service enumeration with netcat, Nmap
- ✅UDP vs TCP scanning & scan timing optimization
- ✅Interpreting results and NSE scripts

Module 8: Vulnerability Analysis + Malware Threats

Assess vulnerabilities and create/analyze malware

- ✅Vulnerability assessment: scan, identify CVEs, assess impact
- ✅Prioritization: CVSS, asset value, and exploitability ranking
- ✅Safe malware analysis: static & dynamic analysis in sandbox
- ✅Create malware and exploit Windows systems
- ✅Mitigation & reporting: patching, hardening, remediation

Module 9: Wi-Fi Hacking

Practical Wi-Fi hacking, common attacks, and how to defend networks

✅Wireless reconnaissance: find nearby networks, SSIDs, and connected devices
✅Handshake capture & cracking: record Wi-Fi handshakes and try offline password guesses
✅MITM basics: create fake access points to demonstrate risks (for lab use only)
✅WPA/WPA2/3 essentials: differences, strong passwords, and why WPA3 is safer
✅Remediation & hardening: secure settings, guest networks, and monitoring for intruders

Module 10: System Hacking

Advanced system penetration techniques

✅System hacking techniques and methodologies
✅Privilege escalation basics and advanced techniques
✅Post-exploitation analysis and persistence
✅Authentication attacks & defenses
✅Remediation & system hardening

Module 11: Social Engineering

Human psychology and social media exploitation

✅Introduction to Social Engineering fundamentals
✅Location Tracking techniques and tools
✅Social Media hacking and OSINT gathering
✅Email & Phishing Awareness and detection
✅Mitigation & Best Practices for defense

Module 12: Advanced Attacks & Web Security

DDoS, sniffing, and web application vulnerabilities

- ✅DDoS Attack techniques and mitigation strategies
- ✅Sniffing & traffic analysis using Wireshark defensively
- ✅Web vulnerabilities (OWASP): SQLi, XSS, broken auth
- ✅Insecure file upload and directory traversal
- ✅Web application security testing and remediation

Module 13: Dark Web & Deep Web Access

Anonymous browsing and complete internet anonymity

- ✅Understanding Dark Web vs Deep Web differences
- ✅Tor Browser and Anonymous Access techniques
- ✅VPN setup & use-cases for enhanced privacy
- ✅Proxy types & setup overview for anonymity
- ✅Complete anonymity techniques on the internet

Tools covered

Hands-On Projects You'll Work On

- OSINT Investigation Challenge – Find public data using OSINT tools
- Vulnerability Scan Report – Perform scan using Nessus & OpenVAS
- Social Engineering Simulation – Craft a phishing email in a lab
- Windows Server 2022 Lab – Create domain, add users, set permissions
- Hack WIFI - capture the hash and crack it.

Career Pathways Section

- Possible Roles: SOC Analyst, Penetration Tester, Cybersecurity Consultant, Network Security Engineer
- Average Salary in India: ₹3–8 LPA for beginners

Course Highlights / Bonuses

Example:

✅ Lifetime Access to Notes & Tools
✅ Free Career Guidance Session
✅ Private Student Community Access
✅ Post-Course Support for Queries

After completion of this course you will get a certificate.

For Any Query

- **Website:** https://greyhatinstitute.in/
- **WhatsApp:** +91 9334494170
- **Youtube**: https://www.youtube.com/@VikramSecureTech
- **Instagram:** https://www.instagram.com/greyhatinstitute/
- **Facebook:** https://www.facebook.com/greyhatinstitute
- **Linkedin:** https://www.linkedin.com/in/vikram-barnwal-50965030a/