CYBERSECURITY

Ethical hacking · Real lab work · AI-powered security

Course Modules

1. Foundations (Module 0)

Key Topics:

- Cyber security fundamentals
- Linux distributions and use in cybersecurity
- Linux file system, structure, and Bash environment
- Windows file system and batch environment
- Virtualization basics

2. Introduction to Ethical Hacking (Module 1)

Key Topics:

- Information security fundamentals
- Types and classification of cyber attacks
- Hacker classes and ethical hacking principles
- AI in ethical hacking (ChatGPT use cases, AI tools)
- CEH methodology and frameworks
- Cyber Kill Chain
- MITRE ATT&CK framework
- Information assurance and risk management
- Threat intelligence lifecycle
- Incident management
- Compliance: PCI DSS, HIPAA, SOX, GDPR, DPA

3. Footprinting & Reconnaissance (Module 2)

Key Topics:

- Reconnaissance concepts
- Google hacking and OSINT
- People search and social media footprinting
- Dark web footprinting

- WHOIS, DNS, Traceroute
- Email and social engineering footprinting
- Competitive intelligence gathering
- AI-powered OSINT tools

4. Scanning Networks (Module 3)

Key Topics:

- Network scanning concepts
- Host discovery and port scanning
- Service and OS detection (banner grabbing)
- Scanning beyond firewalls and IDS
- AI-assisted scanning techniques
- Detection and prevention of scans

5. Enumeration (Module 4)

Key Topics:

- NetBIOS, SNMP, LDAP, NFS, SMTP, DNS, RPC, SMB enumeration
- Linux and Windows user enumeration
- DNSSEC zone walking and cache snooping
- AI-based enumeration
- Enumeration countermeasures

6. Vulnerability Analysis (Module 5)

Key Topics:

- Vulnerability classification
- CVSS and vulnerability databases
- Vulnerability management lifecycle
- Scanning and assessment tools
- Reporting and analysis
- AI-powered vulnerability assessment

7. System Hacking (Module 6)

Key Topics:

- Password cracking and attacks
- Metasploit framework
- Buffer overflow attacks
- Active Directory enumeration
- Privilege escalation (Windows and Linux)
- Keyloggers, spyware, rootkits
- Steganography and detection
- Post-exploitation and persistence
- Covering tracks and log clearing

8. Malware Threats (Module 7)

Key Topics:

- Trojans, viruses, worms, ransomware
- APT (Advanced Persistent Threat) lifecycle
- Fileless and AI-based malware
- Static and dynamic malware analysis
- Malware detection and countermeasures

9. Sniffing (Module 8)

Key Topics:

- Packet sniffing fundamentals
- MAC flooding, ARP poisoning, DHCP starvation
- Man-in-the-Middle (MITM) attacks
- VLAN hopping and STP attacks
- DNS poisoning
- Sniffer detection and defenses

10. Social Engineering (Module 9)

Key Topics:

- Human-based and computer-based attacks
- Phishing and impersonation
- Mobile social engineering
- Identity theft
- AI-driven social engineering
- Countermeasures and security awareness

11. Denial of Service (DoS / DDoS) (Module 10)

Key Topics:

- DoS vs DDoS concepts
- Botnets and attack techniques
- DDoS toolkits
- Detection and protection tools/services

12. Session Hijacking (Module 11)

Key Topics:

- Application vs network-level hijacking
- TCP/IP hijacking, RST attacks, blind hijacking
- Session ID compromise
- Detection and prevention

13. Evading IDS, Firewalls & Honeypots (Module 12)

Key Topics:

- Web server architecture and vulnerabilities
- Banner grabbing and footprinting
- Directory brute forcing
- DNS hijacking and cache poisoning
- Web server attack tools
- Detection and defense

14. Hacking Web Servers (Module 13)

Key Topics:

- Web server architecture and vulnerabilities
- Banner grabbing and footprinting
- Directory brute forcing
- DNS hijacking and cache poisoning
- Web server attack tools
- Detection and defense

15. Hacking Web Applications (Module 14)

Key Topics:

- OWASP Top 10 (2021)
- Web app hacking methodology
- Access control and client-side bypass
- API and web services attacks
- Fuzzing and encoding techniques
- Security testing tools
- AI in web app hacking

16. SQL Injection (Module 15)

Key Topics:

- SQLi types: error-based, union, blind
- SQLi methodology
- Detection and exploitation
- Evasion techniques
- Countermeasures and tools
- AI-assisted SQLi

17. Hacking Wireless Networks (Module 16)

Key Topics:

- Wi-Fi standards and encryption
- Wireless threats and attacks
- WPA / WPA2 cracking
- Rogue access point attacks
- Wireless security tools and countermeasures

18. Hacking Mobile Platforms (Module 17)

Key Topics:

- OWASP Mobile Top 10 (2024)
- Android and iOS attack vectors
- Rooting and jailbreaking
- Mobile malware and SMiShing
- OTP and 2FA hijacking
- Mobile Device Management (MDM)
- Mobile security tools

19. IoT & OT Hacking (Module 18)

Key Topics:

- IoT/OT architecture and protocols
- OWASP IoT Top 10
- IoT/OT vulnerabilities and attacks
- IIoT and IT/OT convergence
- IoT/OT hacking tools and defenses

20. Cloud Computing Security (Module 19)

Key Topics:

- Cloud, edge, and fog computing
- Containers, Docker, Kubernetes
- Serverless security
- OWASP Cloud Top 10
- AWS, Azure, GCP attack methods
- IAM privilege escalation
- Container vulnerabilities
- Cloud security tools and controls

21. Cryptography (Module 20)

Key Topics:

- Hashing and digital signatures
- PKI and certificates
- Email and disk encryption
- Blockchain security
- Cryptanalysis methods
- Quantum cryptography and attacks
- Cryptography tools