Cyber Security & Ethical Hacking with AI – Course Content – 2 month

---

Module 1: Introduction to Cyber Security

- What is Cyber Security
- Importance of Cyber Security in the Digital Age
- CIA Triad (Confidentiality, Integrity, Availability)
- Cyber Threat Landscape
- Types of Cyber Attacks
- Cyber Laws & Compliance (IT Act, GDPR basics)
- Career Paths in Cyber Security

Module 2: Networking Fundamentals for Security

- Network Basics (LAN, WAN, MAN)
- OSI & TCP/IP Models
- IP Addressing, Subnetting
- Ports & Protocols (HTTP, HTTPS, FTP, SSH, DNS)
- Firewalls, Routers, Switches
- Network Security Basics
- Packet Analysis using Wireshark

Module 3: Operating Systems & Security

Linux Security

- Linux Architecture
- File Permissions & Ownership
- User & Group Management
- Important Linux Security Commands
- Log Monitoring

Windows Security

- Windows Architecture
- User Access Control
- Registry & Services
- Windows Security Tools
- Event Viewer & Logs

Module 4: Introduction to Ethical Hacking

- What is Ethical Hacking
- Types of Hackers
- Hacking Methodology
- Cyber Kill Chain
- Legal & Ethical Considerations
- Penetration Testing vs Vulnerability Assessment

Module 5: Reconnaissance & Information Gathering

- Passive vs Active Reconnaissance
- OSINT Techniques
- Google Dorking
- DNS Enumeration
- WHOIS, Subdomain Enumeration
- Tools: Nmap, Amass, Maltego
- AI-assisted Recon Tools

Module 6: Vulnerability Assessment

- Vulnerability Lifecycle
- CVE, CVSS, NVD
- Automated vs Manual Scanning
- Web, Network & System Vulnerabilities

- Tools: Nessus, OpenVAS
- AI-based Vulnerability Prioritization

Module 7: Web Application Security (OWASP Top 10)

- Introduction to Web Technologies
- OWASP Top 10 Overview
- SQL Injection
- XSS (Stored, Reflected, DOM)
- CSRF
- Authentication & Authorization Issues
- File Upload Vulnerabilities
- Security Misconfigurations
- Hands-on using Burp Suite
- AI-powered Web Vulnerability Detection

Module 8: System & Network Penetration Testing

- Network Attacks
- Password Attacks
- Brute Force & Dictionary Attacks
- Privilege Escalation
- Lateral Movement
- Tools: Metasploit, Hydra, CrackMapExec
- AI-based Attack Pattern Analysis

Module 9: Malware & Exploitation

- Types of Malware
- Malware Lifecycle
- Trojan, Ransomware, Spyware

- Payload Generation
- Antivirus Evasion Basics
- AI-based Malware Detection Techniques
- Static & Dynamic Malware Analysis

Module 10: Mobile Application Security

Android Security

- Android Architecture
- Common Android Vulnerabilities
- APK Analysis
- Tools: MobSF, JADX

iOS Security

- iOS Architecture
- iOS Security Mechanisms
- Common iOS Vulnerabilities
- Secure Coding Practices

Module 11: Cloud Security

- Cloud Computing Models (IaaS, PaaS, SaaS)
- Cloud Security Challenges
- AWS, Azure & GCP Security Basics
- Identity & Access Management (IAM)
- Cloud Misconfigurations
- AI for Cloud Threat Detection

Module 12: AI in Cyber Security

- Introduction to AI & Machine Learning
- AI vs Traditional Security Systems

- AI for Threat Detection
- AI in SIEM & SOC
- Behavioral Analysis using AI
- Anomaly Detection
- Use of ChatGPT & LLMs in Security Automation

Module 13: Defensive Security & SOC Operations

- Blue Team Concepts
- Security Operations Center (SOC)
- SIEM Tools (Splunk, ELK basics)
- Incident Detection & Response
- Log Analysis
- AI-driven SOC Automation

Module 14: Digital Forensics & Incident Response

- Digital Forensics Process
- Evidence Collection & Preservation
- Disk & Memory Forensics
- Network Forensics
- Incident Handling Steps
- Forensic Tools Overview
- AI in Forensics Investigation

Module 15: Secure Coding & DevSecOps

- Secure SDLC
- Common Coding Vulnerabilities
- Secure Coding Practices
- Code Review

- DevSecOps Tools
- CI/CD Security
- AI-assisted Code Vulnerability Scanning

Module 16: Bug Bounty & Real-World Attacks

- Bug Bounty Platforms
- Responsible Disclosure
- Finding Real-World Vulnerabilities
- Writing Professional Bug Reports
- AI Tools for Bug Hunting
- Case Studies

Module 17: Cyber Security Interview Preparation

- Interview Questions (Technical & HR)
- Real-world Scenarios
- Resume Building
- LinkedIn Profile Optimization
- Certifications Roadmap (CEH, Security+, OSCP)

Module 18: Capstone Project

- Real-World Penetration Testing Project
- AI-based Threat Detection Project
- Vulnerability Assessment Report
- Final Presentation & Documentation