Cybersecurity Fundamentals

Module 1: Introduction to Cybersecurity

- What is Cybersecurity?
- Importance of Cybersecurity
- CIA Triad (Confidentiality, Integrity, Availability)
- Types of Cyber Attacks
- Threats, Vulnerabilities & Risks
- Roles in Cybersecurity (Blue Team, Red Team, SOC Analyst, etc.)

Module 2: Networking Basics for Cybersecurity

- OSI & TCP/IP Models
- IP Addressing (IPv4/IPv6)
- Subnetting Basics
- DNS, DHCP, ARP, NAT
- Ports & Protocols (TCP/UDP, HTTP, HTTPS, FTP, SSH, etc.)
- MAC vs IP Address
- Firewalls, Switches, Routers

Module 3: Operating System Fundamentals

- Windows OS Basics (CMD, PowerShell)
- Linux Basics (Bash commands, file permissions, process management)
- System Logs & Event Viewer
- User Management
- File Systems and Directories

Module 4: Cyber Threats & Attack Vectors

- Malware (Viruses, Worms, Trojans, Ransomware, Spyware)
- Social Engineering (Phishing, Pretexting, Baiting)
- Man-in-the-Middle Attacks
- Denial of Service (DoS/DDoS)
- Insider Threats
- Password Attacks (Brute Force, Dictionary, Rainbow Table)
- SQL Injection, XSS, CSRF

Module 5: Cryptography Basics

- What is Cryptography?
- Symmetric vs Asymmetric Encryption
- Hashing (MD5, SHA)

- Digital Signatures
- Certificates and Public Key Infrastructure (PKI)
- SSL/TLS and HTTPS

Module 6: Security Tools & Technologies

- Firewalls (Host-based & Network)
- Intrusion Detection and Prevention Systems (IDS/IPS)
- VPNs
- Antivirus/Antimalware
- SIEM (Security Information and Event Management)
- Endpoint Security

Module 7: Web Application Security

- OWASP Top 10
- Input Validation
- Authentication & Authorization flaws
- Session Management Issues
- Secure Coding Practices
- Web Vulnerability Scanners (e.g., OWASP ZAP, Burp Suite)

Module 8: Identity & Access Management (IAM)

- Authentication, Authorization, Accounting (AAA)
- Multi-factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- SSO and LDAP

Module 9: Security Policies & Risk Management

- Security Policies, Procedures & Standards
- Risk Analysis & Assessment
- Incident Response Plan (IRP)
- Business Continuity & Disaster Recovery
- Security Auditing and Compliance (ISO, NIST, GDPR, HIPAA)

Module 10: Ethical Hacking & Penetration Testing

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks (Nmap)
- Enumeration
- Gaining Access (Exploitation basics)
- Maintaining Access
- Covering Tracks
- Kali Linux Basics

- Metasploit Framework

Module 11: Digital Forensics Basics

- What is Digital Forensics?
- Phases: Identification, Preservation, Analysis, Documentation, Presentation
- Forensic Tools (Autopsy, FTK Imager, Volatility)
- Chain of Custody

Module 12: Cloud Security (Basics)

- Introduction to Cloud Models (IaaS, PaaS, SaaS)
- Cloud Risks and Threats
- Shared Responsibility Model
- Security in AWS/Azure/GCP
- Identity and Access Management in the Cloud

Module 13: Cyber Laws & Ethics

- Cybercrime Types
- Data Privacy Laws (GDPR, IT Act India)
- Intellectual Property Rights (IPR)
- Computer Ethics
- Ethical Hacking vs Hacking

Module 14: Career in Cybersecurity

- Cybersecurity Career Paths
- Industry Certifications:
- CompTIA Security+
- CEH (Certified Ethical Hacker)
- CISSP (Advanced)
- CCNA Security
- CHFI
- Resume & Interview Preparation
- Cybersecurity Labs and Practice Platforms (TryHackMe, Hack The Box, etc.

==========

END

==========