**5.Cyber Security**

**(Name : K.M.Iqbal, Duration : 20weeks – 200 Hours, lessons - 17)**

Here’s a **general employability-focused syllabus for Cybersecurity**, designed to prepare you for roles like **Cybersecurity Analyst**, **Security Engineer**, **Penetration Tester**, and **Security Consultant**. This syllabus aligns with industry certifications like **CompTIA Security+**, **Certified Ethical Hacker (CEH)**, **CISSP**, and **Certified Information Security Manager (CISM)**.

**Topics Covered:**

**1. Introduction to Cybersecurity**

* Cybersecurity Fundamentals
* CIA Triad (Confidentiality, Integrity, Availability)
* Key Security Concepts and Terminologies
* Cybersecurity Threat Landscape
* Types of Cyber Attacks (Phishing, Ransomware, DDoS, etc.)
* Attack Vectors and Motives
* Cybersecurity Frameworks and Standards
* NIST, ISO 27001, COBIT, CIS Controls

**2. Networking Fundamentals for Security**

* Networking Basics
* OSI and TCP/IP Models
* IP Addressing and Subnetting
* Protocols (TCP, UDP, HTTP, FTP, DNS)
* Network Topologies and Architectures
* Network Devices and Their Roles
* Routers, Switches, Firewalls, IDS/IPS
* VPNs and Secure Communication
* Network Monitoring and Traffic Analysis

**3. Security Architecture and Design**

* System Architecture and Security Models
* Security by Design Principles
* Defense in Depth and Least Privilege
* Zero Trust Architecture
* Endpoint and Server Security
* Secure Network Design
* DMZs, VLANs, and Network Segmentation
* Cloud Security Principles and Architecture

**4. Threats, Vulnerabilities, and Risk Management**

* Threat Intelligence and Analysis
* Threat Hunting and Indicators of Compromise (IOCs)
* Vulnerability Assessment and Management
* Vulnerability Scanning with Nessus and OpenVAS
* Patch Management Best Practices
* Risk Management Frameworks
* Risk Assessment and Mitigation
* Business Impact Analysis (BIA)
* Incident Response and Recovery
* Incident Response Lifecycle
* Forensic Investigation Techniques

**5. Identity and Access Management (IAM)**

* Authentication, Authorization, and Accounting (AAA)
* Identity Management Solutions
* Active Directory and LDAP
* Single Sign-On (SSO) and Multi-Factor Authentication (MFA)
* Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
* Identity Federation and Access Tokens (OAuth, SAML)

**6. Cryptography and Encryption**

* Cryptographic Concepts
* Symmetric vs. Asymmetric Encryption
* Hashing (MD5, SHA-256) and Digital Signatures
* Public Key Infrastructure (PKI)
* Certificates and Certificate Authorities (CAs)
* SSL/TLS Protocols and HTTPS
* Data Encryption Techniques
* File and Disk Encryption (BitLocker, VeraCrypt)
* End-to-End Encryption in Communication

**7. Application and Web Security**

* Web Application Security Concepts
* OWASP Top Ten Vulnerabilities
* SQL Injection, XSS, CSRF
* Secure Coding Practices
* Input Validation and Output Encoding
* Error Handling and Logging
* API Security and Best Practices
* Security Testing and Code Review
* Web Application Firewalls (WAF) and Content Security Policies

**8. Ethical Hacking and Penetration Testing**

* Penetration Testing Methodologies
* Reconnaissance, Scanning, Exploitation, Post-Exploitation
* Tools and Techniques
* Metasploit, Burp Suite, Nmap, Nikto
* Exploit Development and Payloads
* Social Engineering Techniques and Countermeasures
* Reporting and Documentation of Penetration Test Results

**9. Malware Analysis and Reverse Engineering**

* Types of Malware (Viruses, Worms, Ransomware, Trojans)
* Static and Dynamic Malware Analysis
* Analyzing Malware Behavior and Signatures
* Sandboxing and Automated Analysis Tools
* Reverse Engineering Techniques
* Using Tools like IDA Pro and Ghidra
* De-obfuscating and Unpacking Malware

**10. Security Operations and Monitoring**

* Security Information and Event Management (SIEM)
* Implementing and Managing SIEM Systems (Splunk, ELK)
* Analyzing Logs and Detecting Anomalies
* Intrusion Detection and Prevention Systems (IDPS)
* Signature-Based and Anomaly-Based Detection
* Honeypots and Deception Technologies
* Threat Hunting and Advanced Persistent Threat (APT) Detection
* Network Traffic Analysis with Wireshark and Zeek

**11. Data Privacy and Protection**

* Data Classification and Data Loss Prevention (DLP)
* Privacy Laws and Regulations
* GDPR, CCPA, HIPAA
* Data Masking, Tokenization, and Anonymization
* Privacy Impact Assessments and Data Governance

**12. Cybersecurity in Cloud and Virtual Environments**

* Cloud Security Challenges and Solutions
* AWS, Azure, Google Cloud Security Features
* Container Security (Docker, Kubernetes)
* Image Scanning and Runtime Security
* Virtualization Security Concepts
* Hypervisor Security and Virtual Network Segmentation

**13. Governance, Risk, and Compliance (GRC)**

* Compliance Standards and Regulations
* PCI-DSS, SOX, HIPAA, GDPR
* Auditing and Monitoring for Compliance
* Policy and Procedure Documentation
* Security Awareness Training and Human Factors

**14. Cyber Incident Response and Management**

* Incident Response Lifecycle (Preparation, Detection, Containment, Eradication, Recovery)
* Creating and Maintaining an Incident Response Plan
* Digital Forensics and Investigation Techniques
* Chain of Custody and Evidence Handling
* Analyzing Disk Images and Memory Dumps
* Disaster Recovery and Business Continuity Planning

**15. Real-World Projects and Hands-On Labs**

* **Project 1:** Building a Secure Network with Firewalls and VPN
* **Project 2:** Conducting a Penetration Test and Writing a Report
* **Project 3:** Implementing SIEM with ELK for Log Monitoring
* **Project 4:** Performing Malware Analysis and Reverse Engineering
* **Project 5:** Setting Up MFA and Identity Management in a Corporate Environment

**16. Certification Preparation**

* **Certified Ethical Hacker (CEH)**
* Practice Exams and Simulation Tests
* Real-Life Scenarios and Case Studies

**17. Soft Skills and Interview Preparation**

* Communication Skills for Security Professionals
* Writing Effective Incident and Threat Reports
* Problem-Solving in High-Stress Situations
* Mock Interviews and Problem-Solving Drills

**Educational Background**

* **Bachelor’s Degree** in:
* **BE / B.Tech / B.Sc / BCA in Cyber Security, IT, or CS**
* **Master’s Degree**
* **M.Tech/M.Sc in Cyber Security, Information Security**