Intermediate Cybersecurity Curriculum

1. Operating System Security and Hardening

Module 1: Fundamentals of OS Security

- Role of the Operating System in Security
- Common OS Vulnerabilities and Threats

Module 2: Hardening Techniques

- Disabling Unused Services and Ports
- Registry and Group Policy Modifications (Windows)
- Security Benchmarks (CIS, STIG)

Module 3: Patch and Update Management

- Importance of Timely Patching
- WSUS and Linux Patch Management Tools

Module 4: Secure Boot and Integrity Checks

- BIOS/UEFI Configuration
- Secure Boot Mechanism and TPM

Module 5: Endpoint Protection and Control

- Host-Based Firewalls
- Antivirus and EDR Solutions

Module 6: Auditing and Logging

- Setting Up Local and Centralized Logs
- Audit Policy Configuration

Module 7: OS-Specific Security Measures

- Linux Hardening (SELinux, AppArmor)

- Windows Defender, BitLocker

2. Intermediate Networking and Secure Protocols

Module 1: Network Architecture and Components

- Switches, Routers, Firewalls, and Proxies
- Layered Network Defense Model

Module 2: TCP/IP and Port Security

- TCP/IP Stack and Packet Flow
- Common Port Attacks and Protection

Module 3: Secure Communication Protocols

- HTTPS, TLS, SSH, and IPsec
- Protocol Vulnerabilities (e.g., SSL downgrade)

Module 4: VPN Technologies

- Types of VPNs (SSL, IPSec, Site-to-Site)
- Secure Remote Access Best Practices

Module 5: Network Access Control (NAC)

- 802.1X and Role-Based Access
- Network Segmentation and Isolation

Module 6: Wireless Network Security

- WPA2/WPA3 Encryption
- Rogue AP Detection and Mitigation

Module 7: Traffic Monitoring and Packet Analysis

- Protocol Analyzers (Wireshark)
- Capturing and Interpreting Network Traffic

3**. Security Architecture and Design**

Module 1: Principles of Secure Architecture

- Least Privilege, Defense-in-Depth
- Secure by Design and Default

Module 2: Security Zones and DMZ

- Designing Perimeter and Internal Zones
- Use of Firewalls and Bastion Hosts

Module 3: Authentication and Authorization Design

- Single Sign-On (SSO), MFA, and Identity Federation
- Role-Based and Attribute-Based Access Control

Module 4: Secure System and Network Design

- Segmentation and Isolation Techniques
- Zero Trust Architecture Basics

Module 5: Secure Software and Application Design

- Secure Development Lifecycle (SDLC)
- Web App Design Flaws and OWASP Top 10

Module 6: Redundancy and High Availability

- Load Balancing, Clustering
- Fault Tolerance in Critical Systems

Module 7: Security Architecture Review

- Threat Modeling and Design Reviews
- Security Requirements Traceability Matrix

4. **Threats, Vulnerabilities & Cyber Attacks**

Module 1: Understanding Threat Actors and Vectors

- Insider vs. Outsider Threats

- Common Attack Vectors (Email, Web, USB)

Module 2: Malware Types and Behaviors

- Viruses, Worms, Trojans, Ransomware
- Persistence and Obfuscation Techniques

Module 3: Vulnerability Categories

- Misconfigurations, Unpatched Systems
- Code Injections, Buffer Overflows

Module 4: Exploitation and Post-Exploitation

- Privilege Escalation and Lateral Movement
- Common Tools (Mimikatz, Cobalt Strike)

Module 5: Reconnaissance and Scanning

- Passive and Active Recon
- Network and Vulnerability Scanning (Nmap, Nessus)

Module 6: Social Engineering and Insider Threats

- Phishing, Pretexting, and Baiting
- Detecting and Preventing Insider Attacks

Module 7: Case Studies and Real-World Incidents

- Analysis of Famous Breaches
- Lessons Learned and Indicators of Compromise

6. Introduction to Ethical Hacking & Pentesting

Module 1: Foundations of Ethical Hacking

- Principles, Laws, and Scope of Ethical Hacking
- Types of Hackers and Penetration Testing Phases

Module 2: Information Gathering and Reconnaissance

- OSINT Techniques and Tools

- Scanning Networks with Nmap

Module 3: Vulnerability Identification

- Common Vulnerability Types (OWASP Top 10)
- Tools for Scanning and Enumeration

Module 4: Exploitation Basics

- Exploiting Weak Passwords and Misconfigurations
- Intro to Metasploit and Exploitation Frameworks

Module 5: Post-Exploitation and Reporting

- Maintaining Access and Covering Tracks
- Creating Basic Pentest Reports

7. Data Protection and Access Control

Module 1: Principles of Data Security

- Confidentiality, Integrity, Availability (CIA Triad)
- Data Classification and Labeling

Module 2: Access Control Models and Mechanisms

- Role-Based, Attribute-Based, and Discretionary Access Control
- Identity and Authentication Mechanisms

Module 3: Encryption Fundamentals

- Symmetric vs. Asymmetric Encryption
- Common Protocols (SSL/TLS, SSH, PGP)

Module 4: Data Loss Prevention (DLP)

- Endpoint and Network DLP Tools
- Policy Creation and Monitoring

Module 5: Secure Data Storage and Disposal

- Encryption at Rest and In Transit
- Data Wiping and Destruction Techniques