COMPREHENSIVE CYBER SECURITY SYLLABUS

FROM BASIC TO ADVANCE

MODULE 1: FOUNDATIONS OF CYBERSECURITY (BASIC)

1. Core Concepts and Terminology

- **The CIA Triad**: Confidentiality, Integrity, and Availability.
- **Key Concepts**: Risk, Vulnerability, Threat, Exploit, Attack Vector, Risk Management.
- **Security Principles**: Defence in Depth, Principle of Least Privilege, Zero Trust.
- **Ethics and Law**: Understanding legal boundaries, ethical hacking guidelines, and compliance (e.s., GDPR, HIPAA).

2. Common Cyber Threats & Attacks

- **Malware**: Viruses, Worms, Trojans, Ransomware, Spyware.
- **Social Engineering**: Phishing, Vishing, Smishing, Baiting, Pretexting.
- **Network Attacks**: Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM).
- **Web-Based Attacks**: SQL Injection (SQLi), Cross-Site Scripting (XSS) (basic overview).

3. IT & Networking Fundamentals

- **Networking Basics**: The OSI Model, TCP/IP Protocol Suite, IP Addressing (IPv4/IPv6), subnetting.
- **Network Hardware**: Routers, Switches, Hubs, Firewalls (basic function).
- **Operating Systems**:
- **Windows**: File system (NTFS), permissions, command line (CMD/PowerShell).
- **Linux:** File system (ext4), permissions, basic shell commands (ls, cd, pwd, grep, chmod)

MODULE 2: DEFENSIVE & OFFENSIVE CORE (INTERMEDIATE)

1. Network Security

- **Defensive Architecture:** Firewalls (Stateful, Next-Gen), Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS).
- **Secure Networking**: Virtual Private Networks (VPNs), Network Segmentation, DMZ Demilitarized Zone).
- **Wireless Security**: WEP, WPA, WPA2/3, common attacks (e.g., Evil Twin).

2. Cryptography

- **Core Concepts**: Encryption, Decryption, Hashing, Steganography.
- **Types of Encryptions**:
  - a) **Symmetric**: AES, DES.
  - b) **Asymmetric**: RSA, Public Key Infrastructure (PKI).
- **Protocols**: SSL/TLS, SSH, PGP.
- **Hashing Algorithms**: MD5, SHA-1, SHA-256.

3. Identity and Access Management (IAM)

- **Core Principles**: Identification, Authentication, Authorization, Accountability.
- **Authentication Methods**: Multi-Factor Authentication (MFA), Biometrics, Tokens.
- **Access Control Models**: DAC, MAC, RBAC (Role-Based Access Control).

4. Ethical Hacking & Penetration Testing

- **Phases of Hacking:**
  1. Reconnaissance (Active vs. Passive, OSINT).
  2. Scanning (Nmap, Nessus).
  3. Gaining Access (Exploitation, Metasploit).
  4. Maintaining Access (Persistence, Backdoors).
  5. Covering Tracks (Log clearing).
- **Vulnerability Assessment**: Identifying and ranking vulnerabilities**.**

5. Web Application Security

- **OWASP Top 10**: In-depth review of the most critical web vulnerabilities (e.g., injection, Broken Authentication, XSS, Insecure Deserialization).
- **Tools**: Burp Suite, OWASP ZAP.

MODULE 3: SECURITY OPERATIONS & ANALYSIS (ADVANCED)

1. Security Operations (SecOps)

- **Security Operations Center (SOC):** Roles and responsibilities (Analyst Tiers 1-3).
- **SIEM**: Security Information and Event Management (e.g., Splunk, QRadar).
- **Log Analysis**: Collecting, correlating, and analyzing logs from various sources.

2. Incident Response (IR)

- **IR Lifecycle**: Preparation, Identification, Containment, Eradication, Recovery, lesson learned.
- **Playbooks**: Creating and using step-by-step guides for common incidents.

3. Digital Forensics

- **Core Concepts**: Chain of Custody, data acquisition (disk/memory), analysis.
- **Tools**: Autopsy, Volatility, The Sleuth Kit.
- **File System Forensics**: Analyzing NTFS, ext4, FAT file systems.

4. Malware Analysis

- **Static Analysis**: Analyzing a malicious file without running it (examining strings, headers).
- **Dynamic Analysis** (Sandboxing): Running malware in a safe, isolated environment to observe its behaviour (network calls, file changes).
- **Tools**: Wireshark, Process Monitor, Ghidra, IDA Pro (introduction).

5. Cloud Security

- **Cloud Models**: IaaS, PaaS, SaaS.
- **Shared Responsibility Model**: Understanding who is responsible for security provider vs. customer).
- **Cloud-Native Security**: Securing containers (Docker, Kubernetes), serverless functions, and cloud IAM.

MODULE 4: SPECIALIZATIONS & EMERGING TRENDS (EXPERT)

1. Advanced Penetration Testing

- **Exploit Development**: Writing custom exploits for discovered vulnerabilities.
- **Bypassing Defenses**: Evading antivirus (AV), firewalls, and EDR (Endpoint Detection and response).
- **Active Directory Exploitation**: Common attacks in a Windows enterprise environment (e.g., Kerberoasting, Pass-the-Hash).

2. Reverse Engineering

- **Software Reversing**: Decompiling and debugging applicaΘons to understand their inner workings.
- **Assembly Language (x86/ARM)**: Basic understanding for malware analysis and exploit dev

3. Governance, Risk, and Compliance (GRC)

- **Security Frameworks**: NIST Cybersecurity Framework, ISO 27001/27002.
- **Risk Assessment**: Qualitative and Quantitative risk analysis.
- **Compliance & Auditing**: Ensuring the organization adheres to legal and regulatory requirements.

4. IoT & Operational Technology (OT) Security

- **IoT Security**: Securing "smart" devices, firmware analysis.
- **OT/ICS Security**: ProtecΘng industrial control systems (e.g., SCADA) in critical infrastructure.

5. AI & Machine Learning in Cybersecurity

- **Defensive AI:** Using ML for anomaly detection, user behaviour analytics (UBA).
- **Offensive AI**: How AI can be used to automate and enhance attacks (e.g., generative phishing).