Cybersecurity Professional Program Outline: Basic to Intermediate

This program is designed to provide students with the foundational knowledge and practical skills required to understand common cyber threats, protect digital assets, and begin a career in the cybersecurity field.

Module 1: Foundations of Cybersecurity (The Basics)

This module introduces the core concepts and principles that govern the field of cybersecurity.

- **1.1 Introduction to Cybersecurity**
  - What is Cybersecurity? (Definition, Scope, and Importance)
  - The CIA Triad: **C**onfidentiality, **I**ntegrity, and **A**vailability
  - The Security Governance, Risk, and Compliance (GRC) Landscape
- **1.2 Types of Threats and Actors**
  - Common Threats: Malware (Viruses, Ransomware, Spyware, Trojans), Phishing, DDoS
  - Threat Actors: Script Kiddies, Hacktivists, Organized Crime, Nation-States
- **1.3 Understanding Networking Fundamentals**
  - TCP/IP Model vs. OSI Model
  - IP Addressing, Subnetting, and Ports
  - Introduction to Firewalls, Routers, and Switches
- **1.4 Cryptography Basics**
  - Symmetric vs. Asymmetric Encryption
  - Hashing and Digital Signatures
  - Practical uses of TLS/SSL

Module 2: Network and System Security

Focuses on securing the infrastructure that digital assets rely on, including networks and operating systems.

- **2.1 Securing Operating Systems (OS)**
  - Patch Management and Configuration Hardening (Windows/Linux)
  - User Account Control (UAC), Least Privilege Principle
  - System Auditing and Log Review
- **2.2 Network Defense**
  - Firewall Configuration and Rulesets (Stateful vs. Stateless)
  - Introduction to Intrusion Detection/Prevention Systems (IDS/IPS)
  - Virtual Private Networks (VPNs) and Secure Remote Access

- **2.3 Wireless Network Security**
  - Understanding Wi-Fi Security Protocols (WEP, WPA2, WPA3)
  - Best practices for securing Access Points (APs)
  - Wireless attack vectors (e.g., Evil Twin)
- **2.4 Cloud Security Concepts**
  - Introduction to Cloud Service Models (IaaS, PaaS, SaaS)
  - Shared Responsibility Model

Module 3: Offensive Security: An Introduction to Ethical Hacking

This module provides a necessary introduction to the mindset and tools used by attackers, focusing on ethical and legal applications.

- **3.1 The Ethical Hacking Methodology**
  - Reconnaissance and Footprinting (Passive vs. Active)
  - Scanning and Enumeration (Nmap)
  - Gaining Access (Exploitation Overview)
  - Maintaining Access and Covering Tracks
- **3.2 Web Application Security Fundamentals**
  - The OWASP Top 10 (Introduction)
  - Understanding Injection Attacks (SQL Injection)
  - Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)
- **3.3 Password Attacks**
  - Brute-Force vs. Dictionary Attacks
  - Rainbow Tables and Password Cracking Tools (e.g., Hashcat, John the Ripper)
  - Defensive measures: Hashing, Salting, and Multi-Factor Authentication (MFA)
- **3.4 Social Engineering**
  - Common techniques (Pretexting, Baiting, Quid Pro Quo)
  - Defending against social engineering attacks

Module 4: Security Operations and Incident Response (Intermediate Topics)

This module shifts the focus to the operational aspects of cybersecurity—detection, analysis, and response.

- **4.1 Security Monitoring and Analysis**
  - Introduction to Security Information and Event Management (SIEM) systems
  - Understanding Log Files and Event Correlation
  - Introduction to Packet Analysis (using tools like Wireshark)

- **4.2 Vulnerability Management**
  - Vulnerability Scanning Tools (e.g., Nessus, OpenVAS)
  - Risk Prioritization and Remediation Planning
  - The Common Vulnerability Scoring System (CVSS)
- **4.3 Incident Response (IR) Life Cycle**
  - Preparation, Detection & Analysis, Containment, Eradication & Recovery, Post-Incident Activity
  - Developing an Incident Response Plan
- **4.4 Digital Forensics Fundamentals**
  - The Chain of Custody
  - Collecting and Preserving Digital Evidence
  - Basic file system analysis

Module 5: Governance, Risk, and Compliance (GRC) and Future Trends

The final module covers the business and legal aspects of cybersecurity and looks ahead at emerging areas.

- **5.1 Risk Management**
  - Identifying and Analyzing Risk (Qualitative vs. Quantitative)
  - Risk Treatment Strategies (Avoid, Transfer, Mitigate, Accept)
- **5.2 Compliance and Regulatory Frameworks**
  - Introduction to Major Regulations (e.g., GDPR, HIPAA, CCPA)
  - Security Frameworks (e.g., ISO 27001, NIST CSF)
- **5.3 Emerging Cybersecurity Trends**
  - The Internet of Things (IoT) Security
  - Operational Technology (OT) and Industrial Control Systems (ICS) Security
  - Artificial Intelligence (AI) and Machine Learning (ML) in security
- **5.4 Career Paths in Cybersecurity**
  - Review of major roles (Analyst, Engineer, Consultant, Auditor)
  - Certification pathways (e.g., CompTIA Security+, CEH, CISSP)

This outline provides a structured path for learners to move from basic awareness to a solid intermediate understanding of key cybersecurity domains.