Cybersecurity Fundamentals – Advanced Syllabus (6 Weeks)

Course Duration: 6 Weeks
Skill Level: Beginner to Intermediate
Certifications Aligned:

- ISC2 **Certified in Cybersecurity (CC)**
- Cisco **CyberOps Associate**
- (Preparation for CompTIA Security+ foundations)

Week 1: Introduction to Cybersecurity & Core Principles

Topics Covered:

- What is cybersecurity? Why it matters today
- Threat landscape: Nation-state, hacktivists, insiders
- Core security concepts
- Cybersecurity roles and domains
- Risk, Threat, and Vulnerability
- CIA Triad: Confidentiality, Integrity, Availability

Lab:

- Using a Threat Intelligence feed (Cisco Talos, VirusTotal) to identify indicators of compromise (IOCs)
- Threat modeling basic exercise using STRIDE

Week 2: Networking Fundamentals & Security Technologies

Topics Covered:

- Network architecture and protocols (TCP/IP, UDP, DNS, DHCP)
- OSI vs TCP/IP Model

- Network segmentation, VLANs, firewalls
- Common network attacks (MITM, ARP spoofing, DNS poisoning)
- IP addressing and subnetting for security analysis

Lab:

- Wireshark: Analyze traffic for malicious patterns
- Packet Tracer (Cisco): Configure VLANs and access control lists (ACLs)

Week 3: Access Control, Identity & Authentication

Topics Covered:

- Authentication, Authorization, and Accounting (AAA)
- Identity and Access Management (IAM)
- Password policy, MFA, biometrics
- Role-based access control (RBAC)
- Active Directory basics
- Cloud identity basics (Azure AD, IAM in AWS)

Lab:

- Windows VM: Configure Group Policy and User Rights
- Configure MFA for a cloud-based lab (e.g., using Azure/Microsoft 365 trial)

Week 4: Malware, Threats, and Endpoint Protection

Topics Covered:

- Malware types: Virus, Worm, Trojan, Ransomware, Rootkit
- Threat actors and motivations
- Defense in depth and endpoint security
- Antivirus vs EDR vs XDR
- Security controls (technical, administrative, physical)

Lab:

- Install and analyze malware behavior in a sandboxed virtual machine
- Use Sysinternals tools to detect malicious processes

Week 5: Security Operations & Incident Response (CyberOps Focus)

Topics Covered:

- Security Operations Center (SOC) roles & tiers (L1, L2, L3)
- Incident Response lifecycle (NIST Framework)
- SIEM (Security Information and Event Management)
- Log analysis and event correlation
- Indicators of Compromise (IOCs) and MITRE ATT&CK framework

Lab:

- Splunk: Analyze logs from a simulated attack
- Cisco Packet Tracer: Create IDS/IPS rules
- Use open-source SIEM (like Wazuh or Security Onion)

Week 6: Governance, Risk & Compliance + Review for Certification

Topics Covered:

- Security policies and frameworks (NIST, ISO/IEC 27001, COBIT, CIS Controls)
- Risk management: Qualitative vs Quantitative
- Data classification and handling
- Privacy laws: GDPR, HIPAA, etc.
- Business continuity and disaster recovery

Lab:

- Create a risk assessment matrix for a small organization
- Write a sample incident response plan

Supplementary Labs & Practice (Weekly Add-ons)

- **Capture The Flag (CTF):** Weekly CTF challenges from platforms like TryHackMe or Hack The Box
- **Cisco CyberOps Simulations:** Case scenarios using Packet Tracer & log file analysis
- **ISC2 CC Domain Quizzes & Labs:** Focused domain-by-domain CC test practice

Final Week Project & Certification Readiness

- **Capstone Project:** Simulated Cyber Attack and Response Exercise
  - Students must identify, analyze, respond, and report on a simulated intrusion.
  - Report must include threat identification, logs, affected systems, response strategy, and mitigation steps.
- **Certification Prep:**
  - Full-length practice exam for **ISC2 CC**
  - Full-length practice exam for **Cisco CyberOps Associate**
  - Resume and LinkedIn profile workshop with Cybersecurity focus

Domains Mapped to ISC2 CC Certification

Domain	Covered in
1. Security Principles	Week 1 & 6
2. Business Continuity (BC), DR	Week 6
3. Access Controls Concepts	Week 3
4. Network Security	Week 2
5. Security Operations	Week 5

Tools and Platforms Used:

- Wireshark
- Cisco Packet Tracer

- Splunk (or free cloud instance)
- TryHackMe / HackTheBox (Beginner paths)
- Microsoft Azure Free Tier
- Security Onion or Wazuh
- VirtualBox or VMware Workstation Player