Defensive Cybersecurity Course

🔷 **Level:** Intermediate → Advanced
🔷 **Duration:** 12 weeks (self-paced)
🔷 **Learning Mode:** Hands-on Labs, Theory, and Projects
🔷 **Prerequisites:** Security+ knowledge (basic cybersecurity, networking, system security)

🟢 **Module 1: Foundations of Defensive Security**

📌 **Week 1: Networking & System Security Basics**

- Understanding **OSI & TCP/IP Models** in security
- Deep dive into **firewalls, IDS/IPS, VPNs**
- Secure **Windows & Linux hardening techniques**
- **Active Directory Security 101** (GPO, LDAP, Kerberos, NTLM)

🔷 **Lab:**
✅ Use **pfSense Firewall** to configure IDS/IPS with Suricata
✅ Capture & analyze network traffic using **Wireshark**

🔷 **Project:**
🚀 Secure a Windows/Linux VM by disabling SMBv1, enabling auditing, and configuring a local firewall

---

🟡 **Module 2: Security Operations & SIEM Analysis**

📌 **Week 2-3: SOC & SIEM Fundamentals**

- **How a Security Operations Center (SOC) works**
- **SIEM Log Analysis:** Understanding Windows Event Logs & Sysmon
- **MITRE ATT&CK Framework** for adversary behavior tracking
- Writing **Sigma rules** for detection

🔷 **Lab:**
✅ Set up **Splunk Free Version or Elastic Stack (ELK)**
✅ Analyze **Windows logs using Sysmon & PowerShell logging**

🔷 **Project:**
🚀 Investigate a simulated **PowerShell attack in Windows Event Logs**

🔵 **Module 3: Threat Intelligence & Malware Detection**

📌 **Week 4-5: Threat Intelligence & OSINT**

- **Understanding Cyber Threat Intelligence (CTI) Frameworks** (MITRE ATT&CK, STIX/TAXII)
- **OSINT & Dark Web Monitoring** techniques
- **YARA & Sigma Rules** for detecting malware

🔷 **Lab:**
✅ Collect & analyze **malware intelligence from VirusTotal & HybridAnalysis**
✅ Create **YARA rules** to detect suspicious files

🔷 **Project:**
🚀 Build a **Threat Intelligence Report on a real-world APT attack**

🟠 **Module 4: Incident Response & Digital Forensics**

📌 **Week 6-7: IR & Forensic Fundamentals**

- **Incident Response Life Cycle (NIST & SANS Models)**
- **Memory & Disk Forensics** (Windows & Linux)
- **Malware Reverse Engineering Basics**

🔷 **Lab:**
✅ Use **Volatility Framework** to analyze a memory dump
✅ Investigate a ransomware attack using **Autopsy & FTK Imager**

🔷 **Project:**
🚀 Perform **forensic analysis on a compromised machine** & create an **IR report**

🟣 **Module 5: Advanced Threat Hunting & Adversary Simulation**

📌 **Week 8-9: Proactive Threat Hunting**

- **How to Hunt Threats in SIEM & EDR**
- **Endpoint Security & Detection Engineering**
- **Red vs. Blue Teaming** (TTPs, Atomic Red Team)

🔷 **Lab:**
✅ Deploy **CrowdStrike Falcon or Elastic EDR** & detect threats
✅ Simulate attacks using **MITRE Caldera or Atomic Red Team**

🔷 **Project:**
🚀 Build a **Threat Hunting Playbook for detecting adversaries**

🔴 **Module 6: SOC Automation & Security Engineering**

📌 **Week 10-11: Automation & SIEM Optimization**

- **SOAR (Security Orchestration, Automation, & Response)**
- **Automating threat detection with Python & APIs**
- **Cloud Security & AWS/Azure Sentinel**

🔷 **Lab:**
✅ Use **Cortex XSOAR** to automate threat detection
✅ Write **Python scripts to parse and analyze logs**

🔷 **Project:**
🚀 Develop an **automated security response playbook** using Python & SOAR

⚡ **Final Project (Week 12): Full Security Incident Simulation**

🔷 **Scenario:** Simulate a **real-world cyber attack** and respond as a SOC Analyst
✅ Use SIEM to detect and investigate an attack
✅ Perform digital forensics on infected systems
✅ Create a **detailed Incident Response Report**