Course Plan Overview

- **Duration:** 3 months (12 weeks)
- **Sessions per Week:** 3 (each session lasting 1 hours)
- **Focus Areas:**
    1. **Network VAPT** (Weeks 1–4)
    2. **Web VAPT** (Weeks 5–8)
    3. **CompTIA Security+** (Weeks 9–12)

Detailed Week-by-Week Plan

Month 1: Network VAPT

Week 1: Fundamentals of Networking and Vulnerability Assessment

- Introduction to Networking Basics: Protocols, IP, TCP/UDP
- Overview of Vulnerabilities and Threats in Networks
- Tools and Techniques for Network Scanning (e.g., Nmap, Nessus)
- Lab: Hands-on with Nmap

Week 2: Enumeration and Exploitation

- Network Enumeration: Identifying Hosts and Services
- Vulnerability Identification Using Tools
- Basics of Exploitation (Metasploit Framework)
- Lab: Identifying and Exploiting Weak Protocols

Week 3: Advanced Network Testing Techniques

- Sniffing and MITM Attacks
- Advanced Tools: Wireshark, Responder, and Ettercap
- Penetration Testing Standards (e.g., OWASP, PTES)
- Lab: Simulating Network Attacks in a Controlled Environment

Week 4: Reporting and Mitigation

- Writing Effective VAPT Reports
- Mitigation Strategies for Common Network Vulnerabilities
- Lab: End-to-End Network VAPT Practice

- Assessment: Simulated Network VAPT Project

Month 2: Web VAPT

Week 5: Introduction to Web Security

- HTTP Basics, OWASP Top 10 Vulnerabilities
- Introduction to Web VAPT Tools: Burp Suite, OWASP ZAP
- Lab: Analyzing HTTP Requests

Week 6: Common Web Vulnerabilities

- SQL Injection, XSS, CSRF
- Identification and Exploitation Techniques
- Lab: Exploiting Test Web Applications

Week 7: Advanced Web Testing

- File Upload Vulnerabilities, SSRF, LFI/RFI
- Bypassing Authentication and Authorization Mechanisms
- Lab: Advanced Web Exploitation Scenarios

Week 8: Reporting and Mitigation

- Writing Web VAPT Reports
- Secure Coding Practices and Mitigation
- Lab: End-to-End Web VAPT Practice
- Assessment: Simulated Web VAPT Project

Month 3: CompTIA Security+

Week 9: Security Fundamentals

- Overview of Security Domains: Confidentiality, Integrity, Availability
- Cybersecurity Frameworks and Regulations
- Threat Actors and Attack Vectors

Week 10: Network Security and Architecture

- Securing Network Design: Firewalls, VPNs, IDS/IPS
- Wireless Security Protocols
- Cryptography Basics

Week 11: Operational Security

- Identity and Access Management (IAM)
- Risk Management: Risk Analysis and Policies
- Incident Response and Disaster Recovery

Week 12: Practice Exam and Certification Preparation

- Reviewing Core Security+ Concepts
- Practice Tests and Q&A
- Tips for Taking the Security+ Exam
- Final Assessment: Mock Exam

Key Deliverables

- **Labs:** Weekly hands-on exercises
- **Assignments:** Practical tasks to reinforce learning
- **Assessments:** Project-based evaluations at the end of each module
- **Certification Prep:** Study materials and mock tests for Security+