Masters Program in Advanced Cybersecurity (6 Months)

Program Overview:

This program is designed to equip learners with in-depth knowledge and hands-on experience in advanced cybersecurity concepts, tools, and practices. The course is industry-aligned and prepares students for globally recognized certifications and real-world cybersecurity challenges.

Course Structure:

- Duration: 6 Months (24-26 Weeks)
- Format: 3 sessions per week (2 theory + 1 lab/practical)
- Outcome: Capstone Project + Certification Prep

Module 1: Cybersecurity Fundamentals (Weeks 1-3)

- Introduction to cybersecurity & threat landscape
- CIA triad: Confidentiality, Integrity, Availability
- Cybersecurity laws, ethics, and compliance (GDPR, HIPAA)
- Risk management and security policies

Module 2: Network Security (Weeks 4-6)

- OSI model & TCP/IP fundamentals
- Firewalls, VPNs, and proxy servers
- IDS/IPS: Snort, Suricata setup and demo
- Network scanning: Nmap, Wireshark
- Introduction to Zero Trust Architecture

Module 3: OS & Endpoint Security (Weeks 7-9)

- Hardening Windows & Linux systems

- Endpoint Detection & Response (EDR)

- Patch management, group policy objects (GPOs)

- Antivirus & anti-malware strategies

Module 4: Ethical Hacking & Penetration Testing (Weeks 10-12)

- Footprinting & reconnaissance

- Vulnerability scanning and exploitation

- Metasploit Framework usage

- Web App Security: OWASP Top 10 (2023)

- Red teaming vs. Blue teaming exercises

Module 5: Cloud Security (Weeks 13-15)

- Cloud computing models (SaaS, PaaS, IaaS)

- Shared responsibility model

- Cloud IAM and policy enforcement

- Securing AWS, Azure, and GCP workloads

- Hands-on: AWS GuardDuty, CloudTrail, Security Hub

Module 6: Application Security & DevSecOps (Weeks 16-18)

- Secure SDLC principles

- Static and dynamic code analysis (SAST/DAST)

- DevSecOps pipeline setup (Jenkins, GitHub Actions)

- Supply chain attacks & software bill of materials (SBOM)

Module 7: Cryptography & Secure Communications (Weeks 19-20)

- Symmetric & asymmetric cryptography

- Digital certificates and PKI

- TLS/SSL, HTTPS, VPN tunneling

- Trends in post-quantum cryptography

Module 8: Security Operations & Incident Response (Weeks 21-22)

- SOC operations overview

- SIEM tools: Splunk, ELK Stack, Microsoft Sentinel

- Threat intelligence and hunting

- Incident response lifecycle & forensics tools

Module 9: Threats & Malware Analysis (Weeks 23-24)

- MITRE ATT&CK and STRIDE frameworks

- Malware types and vectors

- Static and dynamic malware analysis

- Sandbox environments and behavioral analysis

Module 10: Capstone Project & Certification Prep (Weeks 25-26)

- End-to-end real-world scenario project

- Incident response case study & documentation

- Certification preparation:

- CompTIA Security+

- CEH (Certified Ethical Hacker)

- ISC2 Certified in Cybersecurity

- Intro to CISSP/CISM for advanced learners

Labs & Tools Required:

- Virtualization: VirtualBox/VMware

- Pen Testing: Kali Linux, Metasploit, Burp Suite
- Monitoring: Wireshark, Snort, Suricata
- Cloud: AWS Free Tier, Azure Student Credits
- DevSecOps: GitHub, Jenkins, SonarQube
- Malware Analysis: Cuckoo Sandbox, REMnux
- SIEM: Splunk Free, ELK Stack

Assessment & Assignments Structure:

- Weekly Quizzes: Short MCQs & scenario-based questions
- Lab Submissions: Screenshots & reports
- Midterm Evaluation: Practical + written
- Capstone Project: Team-based real-world case
- Final Presentation: Project demo + Q&A
- Mock Tests: For Security+, CEH

This curriculum is designed to blend theoretical knowledge with hands-on skills to prepare students for cybersecurity careers or advanced certifications.