Cyber Security Internship Curriculum (3 Months + Mini Project)

Month 1: Cyber Security Fundamentals

Week 1: Introduction to Cyber Security

- What is Cyber Security
- Types of Cyber Attacks
- CIA Triad (Confidentiality, Integrity, Availability)
- Cyber Laws & Ethics
- Basics of Networking

Week 2: Networking & Security Basics

- OSI & TCP/IP Models
- IP Addressing
- Ports & Protocols
- Firewalls & IDS/IPS
- Network Security Basics

Week 3: Linux & System Basics

- Introduction to Linux
- Linux File System
- Basic Linux Commands
- User & Permission Management
- Process Management

Week 4: Security Concepts

- Malware Types (Virus, Worm, Trojan)
- Phishing & Social Engineering
- Password Attacks
- Encryption & Hashing Basics

Month 2: Ethical Hacking & Tools

Week 5: Footprinting & Reconnaissance

- Information Gathering
- Google Dorking
- WHOIS, DNS Enumeration

Week 6: Scanning & Enumeration

- Nmap Scanning
- Vulnerability Scanning
- Service Enumeration

Week 7: System Hacking

- Password Cracking Basics
- Brute Force Attacks
- Privilege Escalation
- Covering Tracks (Theory)

Week 8: Web Application Security

- Web Application Architecture
- OWASP Top 10
- SQL Injection
- XSS, CSRF
- Burp Suite Basics

Month 3: Advanced Security & Mini Project

Week 9: Wireless & Network Attacks

- Wi-Fi Security
- WPA/WPA2 Attacks
- Man-in-the-Middle Attacks

Week 10: Security Operations (SOC)

- Introduction to SOC

- SIEM Tools Basics
- Log Analysis
- Incident Response

Week 11–12: Mini Project

- Project Planning
- Practical Implementation
- Reporting & Documentation
- Presentation

Mini Project Ideas

- Vulnerability Assessment Report
- Web Application Security Testing
- Phishing Attack Simulation (Ethical)
- Network Scanning & Security Analysis

Internship Outcomes

- Strong Cyber Security Fundamentals
- Hands-on Ethical Hacking Skills
- Real-time Tool Experience
- Internship Certificate
- Career Guidance & Interview Prep