# Cyber Security & Forensics

3-Months Crash Course

**Month 1: Foundations of Cyber Security**

**Week 1: Introduction to Cyber Security**

- Theory (2 days): Understanding basic concepts and historical overview
- Practical (3 days): Basic hands-on exercises to demonstrate cyber threats and security importance

**Week 2: Fundamentals of Networking**

- Theory (2 days): Overview of TCP/IP and OSI model
- Practical (3 days): Network configuration exercises, packet analysis labs

**Week 3: Operating System Security**

- Theory (2 days): Introduction to operating systems and security features
- Practical (3 days): Hands-on tasks securing OS, user authentication setup

**Week 4: Cryptography**

- Theory (2 days): Basics of cryptography, symmetric vs. asymmetric encryption
- Practical (3 days): Encryption/decryption exercises, PKI implementation

**Month 2: Advanced Cyber Security Concepts**

**Week 5: Web Security**

- Theory (2 days): Common web vulnerabilities, secure coding practices
- Practical (3 days): Web application security testing, firewall configurations

**Week 6: Network Security**

- Theory (2 days): IDPS, firewalls, VPNs
- Practical (3 days): Setting up and configuring IDPS, firewall rules, VPN setup

**Week 7: Threat Detection and Incident Response**

- Theory (2 days): Introduction to threat intelligence, incident response

- Practical (3 days): Incident simulation exercises, SIEM tool setup and analysis

**Week 8: Wireless Security**

- Theory (2 days): Wireless network vulnerabilities, encryption protocols
- Practical (3 days): Wireless network penetration testing, securing wireless networks

**Month 3: Cyber Forensics and Ethical Hacking**

**Week 9: Introduction to Cyber Forensics**

- Theory (2 days): Digital forensics process, evidence acquisition
- Practical (3 days): Image acquisition, chain of custody exercises

**Week 10: File System Forensics**

- Theory (2 days): Understanding file systems, file recovery techniques
- Practical (3 days): File system analysis, metadata examination

**Week 11: Network Forensics**

- Theory (2 days): Capturing and analyzing network traffic, investigating network-based attacks
- Practical (3 days): Network traffic analysis, investigating network intrusions

**Week 12: Ethical Hacking and Penetration Testing**

- Theory (2 days): Introduction to ethical hacking, reconnaissance
- Practical (3 days): Vulnerability scanning, exploitation, reporting