Cyber Security Roadmap with Timeline

Phase 1: Fundamentals (1-2 Months)

- Learn basics of Networking (OSI Model, TCP/IP, DNS)
- Understand Operating Systems (Windows, Linux)
- Study basic Cryptography concepts (encryption, hashing, PKI)
- Familiarize with Virtual Machines and Sandboxing

Phase 2: Security Concepts & Tools (2-3 Months)

- Learn about Firewalls, VPNs, IDS/IPS
- Understand common attack vectors (Phishing, Malware, Ransomware)
- Use tools like Wireshark, Nmap, Metasploit
- Explore Web Security basics (OWASP Top 10)

Phase 3: Hands-on Security Skills (3-4 Months)

- Practice Penetration Testing and Vulnerability Assessment
- Perform Ethical Hacking in lab environments
- Understand Incident Response and Digital Forensics basics
- Work with SIEM tools (Splunk, ELK Stack)

Phase 4: Advanced Topics (3-4 Months)

- Learn about Cloud Security (AWS, Azure security best practices)
- Study Malware Analysis and Reverse Engineering
- Understand Secure Software Development Lifecycle (SDLC)
- Explore Threat Hunting and Advanced Persistent Threats (APTs)

Continuous Learning & Career Prep

- Earn certifications (CompTIA Security+, CEH, OSCP, CISSP)
- Participate in CTFs (Capture The Flag) competitions
- Contribute to open-source security projects
- Follow industry trends via blogs, podcasts, and research papers