Cybersecurity Development Roadmap (14 Months)

Month 1-2: Foundations of Cybersecurity + Basic Linux + Networking

- Introduction to Cybersecurity principles, CIA triad, threat landscape
- Install & use Linux (Ubuntu/Kali), basic commands, file system, permissions
- Networking basics: IP, DNS, MAC, TCP/IP, OSI model, ports, firewalls, NAT
- Tools: Wireshark, Nmap (basics)

Month 3-4: System Security + Bash Scripting + Cryptography

- File system security, users & groups, process & memory management
- Bash scripting basics: variables, loops, conditions, automation
- Cryptography: symmetric/asymmetric, hashing, SSL/TLS, common algorithms
- GPG, OpenSSL usage

Month 5-6: Web App Security + Ethical Hacking Basics + Burp Suite

- Web architecture (frontend/backend/API)
- OWASP Top 10: XSS, SQLi, CSRF, SSRF, IDOR, etc.
- Burp Suite setup & usage, intercept, scanner, repeater, intruder
- DVWA, Juice Shop for practice

Month 7-8: Penetration Testing + Tools + Python for Security

- Kali Linux, Recon-ng, Nmap (advanced), Nikto, Metasploit (basic)
- Intro to Pen Testing methodology: Recon, Scanning, Gaining Access, Maintaining
- Python scripting: requests, BeautifulSoup, socket, Scapy

Month 9-10: Malware Analysis + Reverse Engineering Basics

- Malware types, lifecycle, behavior analysis (static/dynamic)

- Tools: Ghidra, x64dbg, Procmon, PEStudio
- Assembly intro, strings, syscalls, DLL injection basics

Month 11-12: Blue Teaming + SOC + SIEM + Incident Response

- SIEM tools: Splunk/ELK/Wazuh
- Log analysis, detection rules, threat hunting basics
- MITRE ATT&CK, Indicators of Compromise (IoCs)
- IR lifecycle: Preparation, Detection, Containment, Eradication, Recovery

Month 13-14: Certifications + Projects + Career Preparation

- Choose path: Red Team (OSCP, CEH), Blue Team (CompTIA Sec+, CySA+)
- Resume, LinkedIn, GitHub setup with projects
- Final project: Vulnerable lab setup, exploit chain documentation, blue team defense
- Mock interviews, CTFs, TryHackMe/HTB advanced rooms