Cyber Security Roadmap

Credit: www.maxoncodes.com

1. Foundation (Beginner)

Networking Basics: Learn OSI model, TCP/IP, ports, DNS, ping, dig, nslookup.
OS Fundamentals: Linux commands (ls, ps, chmod, ifconfig), Windows PowerShell (Get-Process, Test-Connection).
Python Scripting: Example scripts for port scanning.
Cyber Hygiene: Strong passwords, MFA, updates, phishing awareness.
Hands-on labs: Set up VirtualBox VMs for Linux and Windows, perform basic network tests.

2. Core Security Concepts (Intermediate)

CIA Triad & Risk Management: Confidentiality, Integrity, Availability, Threat vs Vulnerability.
Cryptography: AES symmetric encryption, SHA256 hashing examples.
Web Security: OWASP Top 10, SQLi, XSS, CSRF prevention.
Defensive Tools: Nmap, Wireshark, Burp Suite scans.
Hands-on Tasks: Run lab scans, capture network packets, hash verification.

3. Practical Skills Development (Hands-on)

Lab Setup: VirtualBox/VMware with Ubuntu, Windows, Kali Linux, Metasploitable.
CTF Challenges: TryHackMe, HackTheBox, document each solved challenge.
Red/Blue Team Exercises: Offensive and defensive practice.
Example Commands: Nmap scans, netcat reverse shell, file search in lab environment.

4. Advanced Cyber Security

Malware Analysis & Reverse Engineering: Static/dynamic analysis, strings, PE header, sandbox testing.
Digital Forensics & Incident Response: Disk imaging, memory analysis, timeline reconstruction.
Threat Intelligence & SOC Operations: IoCs, MITRE ATT&CK mapping, ELK dashboards.
Cloud Security: AWS/Azure IAM practice, misconfiguration testing.

5. Specializations

Penetration Testing / Red Team, Blue Team / SOC Analyst, Malware Analyst, Cloud Security Engineer, Forensics Investigator.
Choose specialization based on your interest after mastering fundamentals and intermediate skills.

6. Career Roadmap & Conclusion

Certifications Timeline: CompTIA ITF, Network+, Security+, OSCP, CISSP.
Resources: TryHackMe, HackTheBox, Coursera, Pluralsight, Reddit r/netsec, GitHub.
Conclusion: Hands-on practice, documentation, continuous learning are keys to becoming a

cyber security expert.

FAQ

Q1: Which path to start?
A: Begin with fundamentals like networking, Linux, Python, web security.

Q2: Do I need certifications?
A: Helpful but hands-on labs and portfolio are more valuable.

Q3: Best programming language?
A: Python, Bash, PowerShell.

Q4: How to practice safely?
A: Use isolated labs and sandbox environments only.

Q5: How long to become proficient?
A: 6-12 months for intermediate, 2-3 years for advanced.

Q6: Best resources?
A: TryHackMe, HackTheBox, Coursera, Pluralsight, GitHub, forums.