■ THE MOST EXTREME, NO-TOPIC-LEFT, 6-MONTH CYBERSECURITY ROADMAP ■

This roadmap is designed so that **after 6 months you will be able to answer ANY interview question — Blue Team, Red Team, Networking, OS, Cloud, Security Tools, SIEM, Pentesting, forensics, malware, frameworks, EVERYTHING.**

■■ **WARNING:** This roadmap is **very intense**.
But if you follow it, **you will become the most dangerous job-ready cybersecurity candidate before graduation.**

■ MASTER RULE FOR 6 MONTHS

Every week must include:

```
Theory → Hands-on lab → Project → Notes → GitHub → LinkedIn Post
```

The more you document → the more valuable you become.

■ 6-MONTH ULTRA FULL-COVERAGE ROADMAP

Every topic asked in cybersecurity interviews is covered here.

■ MONTH 1 — FOUNDATIONS (NO WEAKNESS ALLOWED)

✔ Computer Fundamentals • ✔ Networking • ✔ Operating Systems • ✔ Linux • ✔ Windows Administration

What to master

- OSI/TCP-IP Models
- Subnetting
- DNS, DHCP, NAT, VPN
- TCP vs UDP, Ports
- Routing + Switching Basics
- Linux file system, permissions, SSH
- Windows Registry, Event Viewer, AD basics

Mandatory Tools

- VirtualBox / VMware
- Wireshark
- Linux terminal
- Windows CMD + PowerShell

Projects

- Hardened Linux OS build

- Setup secure Linux + Windows virtual lab
- Wireshark analysis report on 5 attacks

■ GitHub Upload: Lab documentation + troubleshooting reports

■ MONTH 2 — FULL CYBER FUNDAMENTALS + SECURITY BASICS

✔ CIA Triad • ✔ SOC basics • ✔ Authentication/Authorization • ✔ Zero Trust • ✔ Threats, Attacks, Vulnerabilities • ✔ Firewalls & IDS/IPS • ✔ Security Policies

Key Concepts

- Cryptography basics
- Malware types
- Web attacks (XSS, SQLi, CSRF)
- Network attacks (MITM, ARP, DDOS)
- Email/Phishing attack chain

Tools

- Nmap
- Burp Suite
- Nessus
- OpenVAS
- OSINT Framework

Projects

- Recon + Vulnerability Assessment Report
- Firewall + IDS setup in lab
- Detect phishing email & reverse-analyze

■ MONTH 3 — BLUE TEAM / SOC ENGINEERING

✔ Detection & Monitoring • ✔ SIEM • ✔ Threat Intelligence • ✔ SOC Processes • ✔ Incident Response • ✔ Forensics Basics

Master Topics

- MITRE ATT&CK;
- NIST frameworks
- Defense in Depth
- Kill Chain Model
- Log Analysis
- Packet Analysis

Tools

- Splunk / Wazuh / Elastic SIEM
- Autopsy (Forensics)
- Sysmon
- Suricata

Projects

- Build a SOC Home Lab
- Detect brute force attack using SIEM
- Malware investigation & forensic report
- Build detection rules (Sigma + YARA)

■ Upload: Real Incident Response Report (gold for interview)

■ MONTH 4 — RED TEAM / PENTESTING

✔ Web Pentesting • ✔ Network Pentesting • ✔ Active Directory Pentesting • ✔ Vulnerability Exploitation • ✔ Post-Exploit + Privilege Escalation

Topics

- OWASP Top 10
- Enumeration → Exploitation → Priv Esc → Pivoting
- Password attacks
- AD exploitation

Tools

- Burp Suite
- Metasploit

- SQLmap
- Hydra
- Responder
- BloodHound

Labs

- TryHackMe Jr Pen Tester Path
- HackTheBox (10 easy + 3 medium boxes)

Projects

- Web Pentesting Report (DVWA / Juice Shop)
- AD Attack + Mitigation Documentation
- Full Pentesting Report (with screenshots)

■ MONTH 5 — CLOUD SECURITY + DEVSECOPS

✔ Cloud fundamentals • ✔ IAM Security • ✔ VPC Networking • ✔ Security Groups • ✔ Containers & Kubernetes security • ✔ CI/CD security

Platforms

- AWS preferred (Azure optional)
- Docker
- Kubernetes

Topics

- Shared responsibility model
- WAF + GuardDuty
- Logging & Monitoring in cloud
- Secrets management

Tools

- AWS Console / CloudTrail
- Trivy / Grype
- Snyk
- Harbor Registry
- Kubescape

Projects

- Deploy vulnerable app in AWS → Attack → Detect → Fix
- Container image scanning pipeline
- Secure CI/CD pipeline design

■ MONTH 6 — ADVANCED DOMAIN + INTERVIEW-KILLER SKILLS

✔ Governance / Risk / Compliance • ✔ Linux Hardening Deep • ✔ Windows Hardening Deep • ✔ Zero Trust Architecture • ✔ Identity Security • ✔ Resume + Portfolio + Interview Mastery

Why this month matters
Most candidates get eliminated because they can't answer:
- "How would you secure a company end-to-end?"
- "Design a security architecture for a small/medium/large org"
- "Walk me through how you handled an incident"

You will be ready.

Final MEGA CAPSTONE

DESIGN + IMPLEMENT + DOCUMENT SECURITY FOR A FULL ORGANIZATION

Includes:
- Network Diagram
- Firewall rules
- Zero Trust Access
- SIEM + SOC monitoring
- Cloud Security
- Backup Strategy
- IAM Structure
- Incident Response Playbook
- Risk Assessment

■ Upload to GitHub • ■ Make demo video (unlisted YouTube) • ■ Pin it to resume + LinkedIn

■ WHAT YOU WILL KNOW AFTER 6 MONTHS

By following this, you will be able to answer ANY interview question in:

- Networking — ✔ Master
- Operating Systems — ✔ Master
- Linux Security — ✔ Master
- Windows Security — ✔ Master
- Web Pentesting — ✔ Master
- Network Pentesting — ✔ Master
- Active Directory — ✔ Master
- SIEM — ✔ Master
- Incident Response — ✔ Master
- Threat Hunting — ✔ Master
- Malware & Forensics — ✔ Master
- Cloud Security — ✔ Master
- DevSecOps — ✔ Master
- Security Frameworks — ✔ Master
- GRC — ✔ Master

■ FINAL GUARANTEE IF YOU FOLLOW THIS

After 6 months you will have:
✔ Full SOC lab
✔ Full Pentesting lab
✔ 20+ GitHub projects
✔ 3 incident response reports
✔ 10+ TryHackMe/HackTheBox labs
✔ Cloud security project
✔ Capstone architecture project
✔ LinkedIn + GitHub portfolio

✔ Resume ready for ANY cybersecurity role

→ **You will never fear ANY cybersecurity interview again.**

■ Final step

Tell me how many hours you can study per day:

■ 2 hours/day
■ 3–4 hours/day
■ 5+ hours/day

I will convert this 6-month roadmap into a daily timetable, including:
- What to study each day
- Which lab to do
- Which project to build
- Which resource to use

Reply with your number. The warrior schedule will begin. ■■■