Cybersecurity Roadmap
Your Learning Path

Think of learning cybersecurity like **learning to drive a car**. First understand how the car works, then learn the roads, then advanced techniques.

Stage 1: How Computers Work (Operating Systems)

Like learning how the engine works before driving

What to Learn:

- File systems and how files are organized
- Processes running in the background
- Users and permissions
- Command line basics
- How programs run

Why: Most security work happens through the command line, not clicking buttons.

Stage 2: Linux - The Security Tool

What to Learn:

- Basic commands (cd, ls, cat, grep)
- File permissions (chmod, chown)
- Package management (apt, yum)
- Bash scripting basics

- Common directories (/etc, /var, /home)

Note: Get comfortable with **Kali Linux** - it's built for security testing.

Resources:
https://www.amazon.com/Linux-Basics-Hackers-Networking-Scripting/dp/1593278551

Why: Almost every hacking tool runs on Linux. Most servers run Linux.

Stage 3: How Computers Talk (Networking)

Like understanding how roads and traffic work

What to Learn:

- IP Addresses - home addresses for computers
- Protocols (TCP/IP, HTTP, DNS) - traffic laws for data
- Ports - different doors on a computer
- How the internet works
- Subnets and routing

Why: Everything in cybersecurity happens over a network.

Stage 4: How Websites Work (Web Fundamentals)

Like understanding how shops operate

What to Learn:

- HTML/CSS basics
- How browsers work
- Client vs Server
- HTTP requests
- Cookies and sessions
- APIs

Why: Most attacks happen through websites.

Stage 5: Secret Codes (Cryptography)

Like learning how locks work

What to Learn:

- Encryption basics
- Symmetric vs Asymmetric encryption
- Hashing
- Common algorithms (AES, RSA, SHA-256)
- Digital signatures
- SSL/TLS (HTTPS)

Resources: https://www.amazon.com/Cryptography-Dummies-Chey-Cobb/dp/0764541889 (zidon ka image)

Why: Crypto protects everything - passwords, websites, messages.

Now Let's Get Into Actual Hacking

You've built your foundation. Now apply it to real security work.

Stage 6: Breaking Into Web Apps (Web Pentesting)

Why Start Here: After learning the basics, there are many paths you can take in cybersecurity. But web application pentesting is the best starting point because:

- Most companies have web apps - there's tons of practice material
- You can start making money through bug bounties relatively quickly
- It's the most in-demand skill in the security market

Key Resources:

- **OWASP Top 10** - Most common web vulnerabilities
- **PortSwigger Web Security Academy** - Free hands-on labs
- **DVWA / Juice Shop** - Practice apps to legally break
- **TryHackMe / HackTheBox** - Real scenarios
- **Book Suggested:** The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws