🛡️ Cybersecurity Journey Roadmap (Beginner to Intermediate)

✅ Step 1: Understand the Basics of Cybersecurity

Goal: Learn what cybersecurity is, its types, importance, and core principles (CIA triad – Confidentiality, Integrity, Availability).
Resources:

- Google Cybersecurity Certificate (Free Trial): https://grow.google/certificates/cybersecurity/
- Simplilearn Free Course: https://www.simplilearn.com/learn-cyber-security-basics-skillup
- YouTube: “Cyber Security Full Course – Simplilearn”

Practice:

- Write your own definitions of the CIA triad.
- Research 3 real-world cyberattack examples and identify what went wrong.

✅ Step 2: Learn Networking Fundamentals

Goal: Understand how the internet works (IP, DNS, ports, HTTP/HTTPS, etc.).
Resources:

- Cisco Networking Basics: https://www.netacad.com/
- YouTube: “Networking for Beginners” by NetworkChuck
- Free Book: *Computer Networking: Principles, Protocols and Practice*

Practice:

- Use Wireshark to analyze local network traffic.
- Try ipconfig / ifconfig commands to explore your system’s network info.

✅ Step 3: Learn Operating Systems (Linux & Windows)

Goal: Gain comfort with Linux and Windows from a cybersecurity point of view.
Resources:

- OverTheWire Bandit Wargame: https://overthewire.org/wargames/bandit/
- Linux Journey: https://linuxjourney.com/
- YouTube: “Linux Basics for Hackers” by NetworkChuck

Practice:

- Install Kali Linux or Ubuntu in VirtualBox.
- Practice with commands like ls, chmod, grep, chown.

✅ Step 4: Learn About Threats & Attacks

Goal: Understand threats like phishing, DDoS, malware, SQLi, XSS.
Resources:

- OWASP Top 10: https://owasp.org/www-project-top-ten/
- YouTube: "Types of Cyber Attacks Explained" – Tech Raj
- Book: *Cybersecurity and Cyberwar* (by P.W. Singer & Allan Friedman)

Practice:

- Set up and test vulnerabilities using DVWA or Juice Shop.
- Create a safe mock phishing page (educational purpose only).

✅ Step 5: Learn Programming (Python)

Goal: Automate tasks, create scripts for scanning, brute-force, and log analysis.
Resources:

- Google's Python Crash Course: https://developers.google.com/edu/python
- Book: *Black Hat Python*
- Platforms: Replit, Jupyter Notebooks

Practice:

- Write a simple port scanner using socket in Python.
- Create a basic brute-force simulator for passwords.

✅ Step 6: Web Application Security

Goal: Learn to exploit/test web apps and prevent vulnerabilities.
Resources:

- PortSwigger Web Security Academy: https://portswigger.net/web-security
- OWASP Juice Shop: https://owasp.org/www-project-juice-shop/
- **Practice:** Run XSS and SQL injection attacks on Juice Shop/DVWA in a safe environment.

✅ Step 7: Ethical Hacking & Tools

Goal: Learn tools like Nmap, Burp Suite, Metasploit, Nikto.
Resources:

- TryHackMe Beginner Paths: https://tryhackme.com/
- HackTheBox Academy: https://academy.hackthebox.com/
- YouTube: LiveOverflow, STÖK, The Cyber Mentor

Practice:

- Perform a port scan on localhost using Nmap.
- Try “Pre-Security” and “Complete Beginner” rooms on TryHackMe.

✅ Step 8: Cybersecurity Certifications

Goal: Validate your skills and improve job-readiness.
Popular Certifications:

- CompTIA Security+
- Google Cybersecurity Certificate
- CEH (Certified Ethical Hacker)
- TryHackMe and HackTheBox Certificates

✅ Step 9: Build a Portfolio

Goal: Show what you’ve learned to the world.
Ideas:

- Create a GitHub profile and upload your scripts/tools.
- Write blog posts on Medium or GitHub Pages explaining hacks.
- Share TryHackMe writeups or CTF solutions.
- Participate in Bug Bounty platforms (HackerOne, Bugcrowd).