

Ultimate Cybersecurity Roadmap (2025 Edition)

Step 1: Build Strong Fundamentals (1-2 Months)

- Networking Basics: Learn TCP/IP, HTTP/HTTPS, DNS, VPN, Firewalls
- Linux & Command Line: Master essential Linux commands, scripting
- Programming: Python, Bash, JavaScript, C/C++ (for later exploit development)

Step 2: Learn Cybersecurity Concepts (2-3 Months)

- Ethical Hacking: Learn reconnaissance, scanning, enumeration, exploitation
- Web Security: Master OWASP Top 10 (SQLi, XSS, IDOR, SSRF, etc.)
- Bug Bounty: Use tools like Subfinder, Amass, Burp Suite, SQLmap

Step 3: Red Teaming & Advanced Pentesting (3-4 Months)

- Active Directory: Work with BloodHound, Mimikatz, Impacket
- Exploit Development: Learn buffer overflows, shellcode writing
- Cloud Security: Learn AWS, GCP, Azure security concepts

Step 4: Real-World Experience & Automation (Ongoing)

- Develop custom security tools (Python, Bash)
- Contribute to open-source, write blogs, and share knowledge
- Certifications (Optional): eJPT, OSCP, CRTP, CRT0

Step 5: Placement & Career Growth

- Apply for internships/jobs in security
- Keep hunting bugs & building security projects
- Network with professionals on LinkedIn, Twitter, Discord

Final Tips

- Focus on hands-on learning more than theory
- Document everything (Notes, Blogs, GitHub)
- Stay updated with security news, CVEs, and trends