Security Engineer Roadmap (2025 Edition)

Level 1: Foundations (03 months)

- Learn Linux (Ubuntu, Kali) & Windows basics

- Networking: IP, TCP/UDP, Ports, DNS, HTTP, etc.

- Tools: nmap, ping, traceroute, netstat, ifconfig/ip

Level 2: Cybersecurity Fundamentals (36 months)

- CIA Triad, Threat Types: Malware, DDoS, Phishing

- Vulnerability Management & Threat Models

- Platforms: TryHackMe (Cyber Defence Path), YouTube (NetworkChuck, John Hammond)

Level 3: Hands-On Skills (69 months)

- Setup home lab (Ubuntu Server, Windows Server)

- Learn and practice with tools: Wireshark, Burp Suite, Nessus, Fail2Ban, Splunk

Level 4: Real-World Defense Skills (912 months)

- Learn SIEM tools (Splunk, ELK), IDS/IPS (Snort, Suricata)

- Log analysis, firewall hardening, patch management

Level 5: Certifications (1 Year+)

- Entry-Level: Security+, eJPT

- Mid-Level: CySA+, SC-200, BTL1

- Advanced: CISSP, OSCP

Level 6: Build Projects & Get Hired

- Deploy SIEM + Honeypot

- Hardened Linux server with documentation
- Write threat reports, upload to GitHub

Entry Job Roles:

- SOC Analyst, Security Engineer, Threat Hunter, Blue Team Analyst

Tools Youll Use:

- Suricata, Snort, Splunk, Graylog, pfSense, VirusTotal, CrowdStrike

Tips:

- Join communities: Red Team Village, Discord servers
- Follow experts: @IppSec, @TheCyberMentor, @HackerSploit