Network Security (45 days)

🔰 Week 1: Cybersecurity & IT Fundamentals
Cybersecurity Basics + CIA Triad
Understand how systems, networks, and data are protected along with core security principles.
Types of Hackers + Attack Overview
Learn attacker types and common threats like phishing, malware, ransomware.
IT & Operating System Basics
Build a strong foundation of how systems and OS (Windows/Linux) work.

🐧 Week 2: Linux Fundamentals
Linux Installation & Setup
Create your own lab using VirtualBox/VMware.
Basic Commands & File System
Learn navigation, file handling, and directory structure.
Permissions & User Management
Control access and manage users securely.
Networking Commands
Practice tools like ping, ifconfig, netstat.

🌐 Week 3: Networking Basics (Part 1)
OSI Model & TCP/IP Model
Understand how data travels across networks.
IP Addressing & Subnetting
Learn device identification and network segmentation.
DNS, DHCP Basics
Understand how IPs are assigned and domains resolved.

🌐 Week 4: Networking Basics (Part 2)
ARP, MAC Address
Learn device-to-device communication in a network.
Ports & Protocols
Understand HTTP, HTTPS, FTP, SSH, and their roles.
Network Devices & Topologies
Learn routers, switches, and how networks are structured.
Revision & Practice
Strengthen all networking concepts.

🔐 Week 5: Network Security Fundamentals
Firewalls & IDS/IPS
Learn how threats are monitored and blocked.
VPN & NAT
Understand secure communication and IP translation.
Network Attacks
Study MITM, sniffing, spoofing techniques.
Secure Protocols
Learn encrypted communication (HTTPS, SSH).
WIFI penetration -MITM

🛠️ Week 6: Security Tools (Part 1)
Wireshark
Analyze network traffic at packet level.
Nmap
Perform network scanning and service detection.
Netcat & Banner Grabbing
Learn network debugging and information gathering.
Hands-on Practice
Combine tools in lab scenarios.

🛠️ Week 7: Security Tools (Part 2)
Burp Suite Basics
Intercept and test web application traffic.
Password Attacks (Concepts)
Learn brute force and dictionary attack basics.
Reconnaissance & Scanning
Gather and analyze target information.
Vulnerability Assessment
Identify system weaknesses.

⚔️ Week 8: Ethical Hacking & Projects
Basic Exploitation
Understand how vulnerabilities are used (lab-based).
Social Engineering
Learn human-focused attack techniques.
Mini Projects
Build a network scanner and practice packet sniffing.
Lab Practice
Apply all hacking concepts safely.

🛸 Week 9: Incident Response & Final Prep
Incident Response Process
Learn how to handle attacks step-by-step.
Log Analysis
Detect suspicious activities using logs.
Lab Setup (Kali Linux)
Prepare a full penetration testing environment.
Revision + Mock Interviews
Final preparation for job readiness.

🎯 Weekly Routine
🕒 1–2 hours theory + practical (Mon–Fri)
 Practice on TryHackMe / Hack The Box
📝 Maintain notes + revise commands