■ 100-Day Cybersecurity, Virtual Networking & Role Preparation Challenge

This structured 100-day roadmap covers Networking, Cybersecurity, Virtual Networking, and preparation for NOC, SOC, and other security roles. Mark off each day as you complete the tasks to build strong career-ready skills.

Phase 1: Networking Foundations (Days 1–20) [NOC Prep]

Day 1–2: OSI & TCP/IP models

Day 3–4: IP addressing, Subnetting

Day 5–6: Switching, Routing basics

Day 7–8: DNS, DHCP, ARP

Day 9–10: Common Protocols (HTTP, HTTPS, FTP, SSH, SNMP)

Day 11–12: VLANs, NAT, VPNs

Day 13–14: Wireless Networking & Security

Day 15–16: Network Monitoring (Ping, Traceroute, Netstat)

Day 17–18: Hands-on: Cisco Packet Tracer / GNS3 labs

Day 19–20: NOC Role Prep: Incident logging, escalation flow, uptime monitoring

Phase 2: Cybersecurity Basics (Days 21–40) [SOC Prep]

Day 21–22: CIA Triad, Security Principles

Day 23–24: Threats, Vulnerabilities, Exploits

Day 25–26: Firewalls, IDS/IPS concepts

Day 27–28: Authentication, MFA, Access Control

Day 29–30: Encryption basics (SSL/TLS, AES, RSA)

Day 31–32: Common Attacks (SQLi, XSS, CSRF)

Day 33–34: SIEM Introduction (Splunk, ELK)

Day 35–36: SOC Tiers 1–3 responsibilities

Day 37–38: Log Analysis & Event Correlation

Day 39–40: SOC Role Prep: Incident handling lifecycle, SOC playbooks

Phase 3: Virtual Networking & Cloud Security (Days 41–70) [Cloud Engineer Prep]

Day 41–42: Virtualization Basics (VMware, VirtualBox, Hyper-V)

Day 43–44: Virtual Switches, vLANs, Virtual Routing

Day 45–46: Software Defined Networking (SDN)

Day 47–48: Cloud Networking (AWS VPC, Azure VNet, GCP)

Day 49–50: Cloud Firewalls & Security Groups

Day 51–52: IAM (Identity & Access Management)

Day 53–54: VPNs in cloud environments

Day 55–56: Container Networking (Docker, Kubernetes)

Day 57–58: Zero Trust Architecture

Day 59–60: Cloud monitoring & logging (CloudTrail, Azure Monitor)

Day 61–62: Hands-on: Deploy secure VPC with subnets & firewall rules

Day 63–64: Cloud Security Engineer Prep: Shared Responsibility Model

Day 65–66: Cloud Incident Response

Day 67–68: Multi-cloud & Hybrid Security

Day 69–70: Role Prep Case Study: Design secure hybrid cloud

Phase 4: Advanced Cybersecurity (Days 71–85) [Analyst/Pen Tester Prep]

Day 71–72: Penetration Testing basics

Day 73–74: Recon tools (Nmap, Nessus, Burp Suite)

Day 75–76: Exploitation & Privilege Escalation

Day 77–78: Threat Hunting Techniques

Day 79–80: Forensics & Evidence Collection

Day 81–82: Red Team vs Blue Team

Day 83–84: SOC Automation (SOAR platforms)

Day 85: Cybersecurity Analyst Prep: Build an incident report portfolio

Phase 5: Integration & Career Prep (Days 86–100) [Capstone]

Day 86–87: Secure Network Design (NOC/SOC collaboration)

Day 88–89: DevSecOps in cloud environments

Day 90–91: Security Compliance (ISO 27001, NIST, PCI DSS)

Day 92–93: IoT & Edge Security

Day 94–95: AI in Cybersecurity & Threat Detection

Day 96–97: Mock Incident Response Tabletop Exercise

Day 98: NOC Final Task: Monitor & report uptime/alerts

Day 99: SOC Final Task: Analyze logs, detect threats, respond

Day 100: Capstone Project: Design & present a Secure Enterprise Network (On-prem + Cloud) with role-based responsibilities (NOC, SOC, Analyst)

■ Congratulations! By completing this 100-day challenge, you will have gained networking, cybersecurity, cloud, and role-specific skills to prepare for NOC, SOC, Cloud Engineer, and Cyber Analyst positions.