Cybersecurity Knowledge Kit
From Scratch to Advanced Level

A structured learning roadmap for entry-level to advanced cybersecurity engineers. This document is designed to build strong fundamentals, practical skills, and industry-ready expertise.

1. Computing & Networking Foundations (Absolute Beginner)

- How computers work: CPU, memory, storage, processes, threads
- Operating systems basics: Linux vs Windows vs macOS
- File systems, permissions, users, groups
- Networking fundamentals: OSI & TCP/IP models
- IP addressing, subnetting, CIDR notation
- Common protocols: HTTP/HTTPS, DNS, FTP, SMTP, SSH
- Ports and services, stateful vs stateless communication
- Basic command-line usage (Linux & Windows)

2. Linux & Windows Internals for Security

- Linux directory structure and permissions (chmod, chown, umask)
- Processes, services, cron jobs, systemd
- Windows architecture: registry, services, Event Viewer
- User Account Control (UAC) and privilege escalation concepts
- Logging and auditing basics (syslog, Windows Event Logs)
- Hardening basics for Linux and Windows systems

3. Programming & Scripting for Security Engineers

- Python fundamentals for automation and analysis
- Bash scripting for Linux automation
- PowerShell basics for Windows security
- Understanding APIs and JSON
- Regex fundamentals for log and data analysis
- Writing simple security automation scripts

4. Core Cybersecurity Concepts

- CIA triad: Confidentiality, Integrity, Availability
- Threats, vulnerabilities, risks, and exploits
- Attack surface and threat modeling
- Security controls: preventive, detective, corrective
- Defense-in-depth strategy
- Common security frameworks overview (NIST, ISO 27001)

5. Network & Web Application Security

- Firewalls, IDS, IPS, WAF concepts
- Packet analysis basics (Wireshark)
- HTTP request/response lifecycle

- Common web vulnerabilities (OWASP Top 10)
- Authentication vs authorization
- Session management, cookies, tokens (JWT)
- TLS/SSL fundamentals

6. Endpoint & OS Security

- Antivirus, EDR, XDR concepts
- Endpoint hardening techniques
- Malware types: virus, worm, trojan, ransomware
- Basic malware analysis concepts (static vs dynamic)
- Persistence mechanisms in Linux and Windows

7. Identity, Access & Authentication

- IAM fundamentals
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- OAuth, SAML, OpenID Connect basics
- Secrets, keys, certificates management

8. Cloud & Container Security (Intermediate)

- Shared responsibility model
- AWS/Azure/GCP security basics
- IAM roles, policies, least privilege
- Network security in cloud (VPC, Security Groups)
- Docker & container security fundamentals
- Kubernetes security basics

9. Security Operations & Monitoring

- What is a SOC and how it operates
- SIEM concepts and log correlation
- Alert triage and incident prioritization
- Threat intelligence feeds
- Indicators of Compromise (IOCs)
- Basic incident response lifecycle

10. Vulnerability Management & Ethical Hacking

- Vulnerability scanning concepts
- Common tools: Nmap, Nessus, OpenVAS
- Introduction to penetration testing
- Exploitation basics (Metasploit overview)
- Responsible disclosure and ethics

11. Cryptography Essentials

- Symmetric vs asymmetric encryption
- Hashing and digital signatures

- Key management fundamentals
- Common crypto mistakes
- Understanding real-world crypto usage

12. Advanced Cybersecurity Topics

- Threat hunting fundamentals
- Advanced persistent threats (APT)
- Zero Trust Architecture
- Security automation & SOAR
- Detection engineering
- Security data engineering basics

13. Hands-on Practice & Career Preparation

- Building a home lab (VMs, Docker, cloud free tiers)
- Capture The Flag (CTF) platforms
- Bug bounty fundamentals
- Writing security reports
- Interview preparation topics
- Continuous learning mindset

Final Notes

Cybersecurity is a continuous learning field. Master fundamentals first, then specialize in domains such as SOC, cloud security, penetration testing, or security engineering. Hands-on practice and real-world exposure are essential for growth.