

Cyber Security

Fundamental IT Skills

- Computer Hardware Components
- Connection Types and their function
- OS-Independent Troubleshooting
- Understand Basics of Popular Suites
- Basics of Computer Networking

- NFC
- Bluetooth
- WiFi
- Infrared

- MS Office Suite
- iCloud
- Google Suite

- Windows
- Linux
- MacOS

Operating Systems

- Learn following for each
 - Installation and Configuration
 - Different Versions and Differences
 - Navigating using GUI and CLI
 - Understand Permissions
 - Installing Software and Applications
 - Performing CRUD on Files
 - Troubleshooting
 - Common Commands

Networking Knowledge

- Understand the OSI Model
- Common Protocols and their Uses
- Common Ports and their Uses
- SSL and TLS Basics
- Basics of NAS and SAN

Security Skills and Knowledge

- Understand Common Hacking Tools
- Understand Common Exploit Frameworks
- Understand Concept of Defense in Depth
- Understand Concept of Runbooks
- Understand Basics of Forensics
- Basics and Concepts of Threat Hunting
- Basics of Vulnerability Management
- Basics of Reverse Engineering
- Penetration Testing Rules of Engagement
- Perimeter vs DMZ vs Segmentation
- Core Concepts of Zero Trust
- Roles of Compliance and Auditors
- Understand the Definition of Risk
- Understand Backups and Resiliency
- Cyber Kill Chain
- MFA & 2FA
- Honeypots
- Operating System Hardening
- Understand Concept of Isolation
- Basics of IDS and IPS
- Authentication vs Authorization
- Blue / Red / Purple Teams
- False Negative / False Positive
- True Negative / True Positive
- Basics of Threat Intel, OSINT
- Understand Handshakes
- Understand CIA Triad
- Privilege Escalation
- Web Based Attacks and OWASP10
- Learn how Malware works and Types

Tools for Incident Response and Discovery

- dig
- nmap
- ping
- arp
- cat
- dd
- tail
- hping
- head
- grep
- nslookup
- tracert
- winhex
- autopsy
- ipconfig
- curl
- wireshark
- memdump
- FTK Imager

Understand Common Standards

- ISO
- RMF
- NIST
- CIS
- CSF

Using tools for Unintended Purposes

- LOLBAS
- GTFOBINS
- WADCOMS

Learn how to find and use these logs

- Event Logs
- syslogs
- netflow
- Packet Captures
- Firewall Logs

Understand Hardening Concepts

- MAC-based
- NAC-based
- Port Blocking
- Group Policy
- Sinkholes
- ACLs
- Patching
- Jump Server
- Endpoint Security

Understand Common Tools

- VirusTotal
- urlscan
- any.run
- Joe Sandbox
- urlvoid
- WHOIS

Understand Audience

- Stakeholders
- HR
- Legal
- Compliance
- Management

Basics of Cryptography

- Salting
- Hashing
- Key Exchange
- Private vs Public Keys
- PKI
- Obfuscation

Understand Frameworks

- Diamond Model
- Kill Chain
- ATT&CK

Common Distros for hacking

- ParrotOS
- Kali Linux

Understand the following

- SIEM
- SOAR

Secure vs Unsecure Protocols

- FTP vs SFTP
- SSL vs TLS
- IPSEC
- DNSSEC
- LDAPS
- SRTP
- S/MIME

Understand the following Terms

- Antivirus
- Antimalware
- EDR
- DLP
- Firewall & Nextgen Firewall
- HIPS
- NIDS
- NIPS
- Host Based Firewall
- Sandboxing
- EAP vs PEAP
- WPS
- ACL
- WPA vs WPA2 vs WPA3 vs WEP

Understand the Incident Response Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Understand Threat Classification

- Zero Day
- Known vs Unknown
- APT

Attack Types and Differences

- Phishing
- Whishing
- Whaling
- Smishing
- Spam vs Spim
- Shoulder Surfing
- Tailgating
- Dumpster Diving
- Zero day
- Social Engineering
- Reconnaissance
- Impersonation
- Watering Hole Attack
- Drive by Attack
- Typo Squatting
- Brute Force vs Password Spray

Common Attacks

- DoS vs DDoS
- MITM
- CSRF
- Spoofing
- SQL Injection
- XSS
- Evil Twin
- VLAN Hopping
- DNS Poisoning
- Deauth Attack
- Replay Attack
- Rogue Access Point
- Buffer Overflow
- Memory Leak
- Pass the Hash
- Directory Traversal

Cloud Skills and Knowledge

- Understand the Concept of Security in the Cloud
- Understand the differences between cloud and on-premises
- Understand the concept of Infrastructure as Code
- Understand the Concept of Serverless
- Understand the basics and general flow of deploying in the cloud

Understand Cloud Services

- SaaS
- PaaS
- IaaS

Cloud Models

- Private
- Public
- Hybrid

Common Cloud Environments

- AWS
- GCP
- Azure

Common Cloud Storage

- S3
- Dropbox
- iCloud
- Box
- OneDrive
- Google Drive

Keep Learning

- Python
- Go
- JavaScript
- C++
- Bash
- Power Shell

Find the detailed version of this roadmap along with other similar roadmaps

roadmap.sh