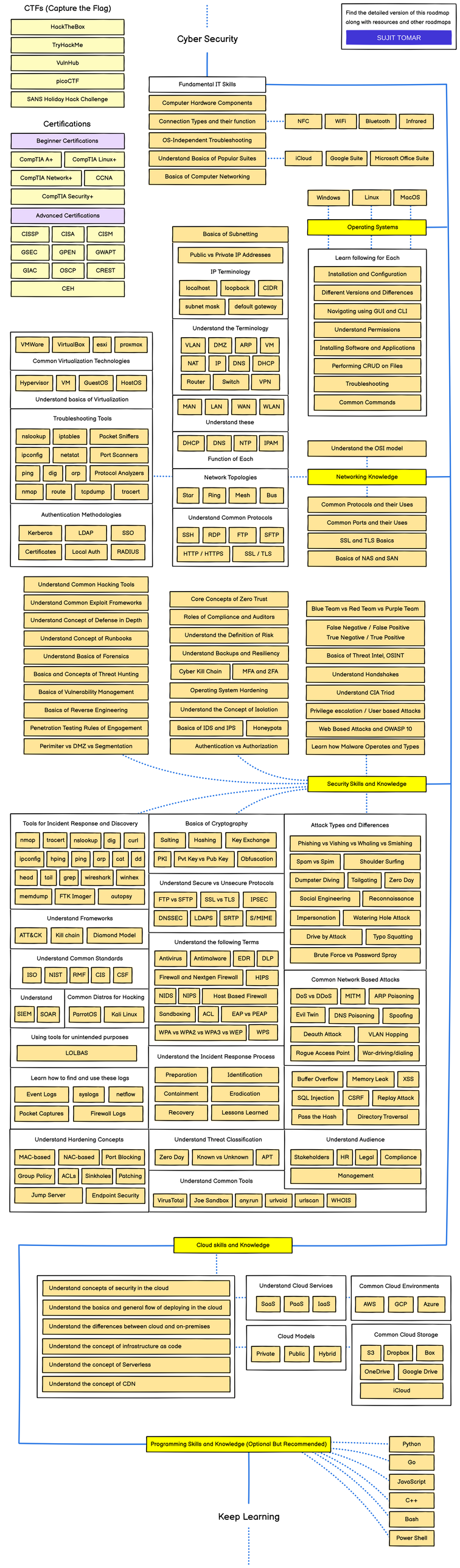
CTFs (Capture the Flag)
HackTheBox
TryHackMe
VulnHub
picoCTF
SANS Holiday Hack Challenge
Certifications
Beginner Certifications
CompTIA A+
CompTIA Linux+
CompTIA Network+
CCNA
CompTIA Security+
Advanced Certifications
CISSP
CISA
CISM
GSEC
GPEN
GWAPT
GIAC
OSCP
CREST
CEH
Cyber Security
Find the detailed version of this roadmap along with resources and other roadmaps
SUJIT TOMAR
Fundamental IT Skills
Computer Hardware Components
Connection Types and their function
NFC
WiFi
Bluetooth
Infrared
OS-Independent Troubleshooting
Understand Basics of Popular Suites
iCloud
Google Suite
Microsoft Office Suite
Basics of Computer Networking
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
Basics of Subnetting
Public vs Private IP Addresses
IP Terminology
localhost
loopback
CIDR
subnet mask
default gateway
Understand the Terminology
VLAN
DMZ
ARP
VM
NAT
IP
DNS
DHCP
Router
Switch
VPN
MAN
LAN
WAN
WLAN
Understand these
DHCP
DNS
NTP
IPAM
Function of Each
Network Topologies
Star
Ring
Mesh
Bus
Understand Common Protocols
SSH
RDP
FTP
SFTP
HTTP / HTTPS
SSL / TLS
VMWare
VirtualBox
esxi
proxmox
Common Virtualization Technologies
Hypervisor
VM
GuestOS
HostOS
Understand basics of Virtualization
Troubleshooting Tools
nslookup
iptables
Packet Sniffers
ipconfig
netstat
Port Scanners
ping
dig
arp
Protocol Analyzers
nmap
route
tcpdump
tracert
Authentication Methodologies
Kerberos
LDAP
SSO
Certificates
Local Auth
RADIUS
Understand the OSI model
Networking Knowledge
Common Protocols and their Uses
Common Ports and their Uses
SSL and TLS Basics
Basics of NAS and SAN
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
Perimiter 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 and 2FA
Operating System Hardening
Understand the Concept of Isolation
Basics of IDS and IPS
Honeypots
Authentication vs Authorization
Blue Team vs Red Team vs Purple Team
False Negative / False Positive
True Negative / True Positive
Basics of Threat Intel, OSINT
Understand Handshakes
Understand CIA Triad
Privilege escalation / User based Attacks
Web Based Attacks and OWASP 10
Learn how Malware Operates and Types
Security Skills and Knowledge
Tools for Incident Response and Discovery
nmap
tracert
nslookup
dig
curl
ipconfig
hping
ping
arp
cat
dd
head
tail
grep
wireshark
winhex
memdump
FTK Imager
autopsy
Understand Frameworks
ATT&CK
Kill chain
Diamond Model
Understand Common Standards
ISO
NIST
RMF
CIS
CSF
Understand
SIEM
SOAR
Common Distros for Hacking
ParrotOS
Kali Linux
Using tools for unintended purposes
LOLBAS
Learn how to find and use these logs
Event Logs
syslogs
netflow
Packet Captures
Firewall Logs
Basics of Cryptography
Salting
Hashing
Key Exchange
PKI
Pvt Key vs Pub Key
Obfuscation
Understand 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 and Nextgen Firewall
HIPS
NIDS
NIPS
Host Based Firewall
Sandboxing
ACL
EAP vs PEAP
WPA vs WPA2 vs WPA3 vs WEP
WPS
Understand the Incident Response Process
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned
Attack Types and Differences
Phishing vs Vishing vs Whaling vs Smishing
Spam vs Spim
Shoulder Surfing
Dumpster Diving
Tailgating
Zero Day
Social Engineering
Reconnaissance
Impersonation
Watering Hole Attack
Drive by Attack
Typo Squatting
Brute Force vs Password Spray
Common Network Based Attacks
DoS vs DDoS
MITM
ARP Poisoning
Evil Twin
DNS Poisoning
Spoofing
Deauth Attack
VLAN Hopping
Rogue Access Point
War-driving/dialing
Buffer Overflow
Memory Leak
XSS
SQL Injection
CSRF
Replay Attack
Pass the Hash
Directory Traversal
Understand Hardening Concepts
MAC-based
NAC-based
Port Blocking
Group Policy
ACLs
Sinkholes
Patching
Jump Server
Endpoint Security
Understand Threat Classification
Zero Day
Known vs Unknown
APT
Understand Common Tools
VirusTotal
Joe Sandbox
any.run
urlvoid
urlscan
WHOIS
Understand Audience
Stakeholders
HR
Legal
Compliance
Management
Cloud skills and Knowledge
Understand concepts of security in the cloud
Understand the basics and general flow of deploying 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 concept of CDN
Understand Cloud Services
SaaS
PaaS
IaaS
Cloud Models
Private
Public
Hybrid
Common Cloud Environments
AWS
GCP
Azure
Common Cloud Storage
S3
Dropbox
Box
OneDrive
Google Drive
iCloud
Programming Skills and Knowledge (Optional But Recommended)
Python
Go
JavaScript
C++
Bash
Power Shell
Keep Learning