

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

CISSPCISAGCISMGSECGPENGWAPT

GIACOSCPCREST

CEH

VMWareVirtualBoxesxiproxmox

Common Virtualization Technologies

HypervisorVMGuestOSHostOS

Understand basics of Virtualization

Troubleshooting Tools

nslookupiptablesPacket Sniffers

ipconfignetstatPort Scanners

pingdigarpProtocol Analyzers

nmaproutetcpdumptracert

Authentication Methodologies

KerberosLDAPSSO

CertificatesLocal AuthRADIUS

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

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

Basics of Subnetting

Public vs Private IP Addresses

IP Terminology

localhostloopbackCIDR

subnet maskdefault gateway

Understand the Terminology

VLANDMZARPVM

NATIPDNSDHCP

RouterSwitchVPN

MANLANWANWLAN

Understand these

DHCPDNSNTPIPAM

Function of Each

Network Topologies

StarRingMeshBus

Understand Common Protocols

SSHRDPSFTP

HTTP / HTTPSSSL / TLS

Core Concepts of Zero Trust

Roles of Compliance and Auditors

Understand the Definition of Risk

Understand Backups and Resiliency

Cyber Kill ChainMFA and 2FA

Operating System Hardening

Understand the Concept of Isolation

Basics of IDS and IPSHoneypots

Authentication vs Authorization

Find the detailed version of this roadmap along with resources and other roadmaps

https://roadmap.sh

NFCWiFiBluetoothInfrared

iCloudGoogle SuiteMicrosoft Office Suite

WindowsLinuxMacOS

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

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

nmaptracertnslookupdigcurl

ipconfighpingpingarpcatdd

headtailgrepwiresharkwinhex

memdumpFTK Imagerautopsy

Understand Frameworks

ATT&CKKill chainDiamond Model

Understand Common Standards

ISONISTRMFCISCSSF

UnderstandCommon Distros for Hacking

SIEMSOARParrotOSKali Linux

Using tools for unintended purposes

LOLBAS

Learn how to find and use these logs

Event Logssyslogsnetwork

Packet CapturesFirewall Logs

Understand Hardening Concepts

MAC-basedNAC-basedPort Blocking

Group PolicyACLsSinkholesPatching

Jump ServerEndpoint Security

Basics of Cryptography

SaltingHashingKey Exchange

PKIPvt Key vs Pub KeyObfuscation

Understand Secure vs Unsecure Protocols

FTP vs SFTPSSL vs TLSIPSEC

DNSSECLDAPSSRTPS/MIME

Understand the following Terms

AntivirusAntimalwareEDRDLP

Firewall and Nextgen FirewallHIPS

NIDSNIPSHost Based Firewall

SandboxingACLSEAP vs PEAP

WPA vs WPA2 vs WPA3 vs WEPWPS

Understand the Incident Response Process

PreparationIdentification

ContainmentEradication

RecoveryLessons Learned

Understand Threat Classification

Zero DayKnown vs UnknownAPT

Understand Common Tools

VirusTotalJoe Sandboxany.runurlvoidurlscanWHOIS

Attack Types and Differences

Phishing vs Vishing vs Whaling vs Smishing

Spam vs SpimShoulder Surfing

Dumpster DivingTailgatingZero Day

Social EngineeringReconnaissance

ImpersonationWatering Hole Attack

Drive by AttackTypo Squatting

Brute Force vs Password Spray

Common Network Based Attacks

DoS vs DDoSMITMARP Poisoning

Evil TwinDNS PoisoningSpoofing

Deauth AttackVLAN Hopping

Rogue Access PointWar-driving/dialing

Buffer OverflowMemory LeakXSS

SQL InjectionCSRFReplay Attack

Pass the HashDirectory Traversal

Understand Audience

StakeholdersHRLegalCompliance

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

SaaSaaSaaS

Cloud Models

PrivatePublicHybrid

Common Cloud Environments

AWSGCPAzure

Common Cloud Storage

S3DropboxBox

OneDriveGoogle Drive

iCloud

Programming Skills and Knowledge (Optional But Recommended)

Python

Go

JavaScript

C++

Bash

Power Shell

Keep Learning