CYBER SECURITY & PENETRATION TESTING — COMPLETE A TO Z MASTER GUIDE (ADVANCED VERSION)

VERSION 2.0 — WITH ALL PLATFORMS, SOURCES, YOUTUBE CHANNELS, ROADMAPS & PRACTICE LINKS

===

1. INTRODUCTION

Cyber Security ka main goal hota hai systems, networks, websites, mobile apps, servers, cloud, sab ko protect karna.

Penetration Testing uska practical offensive side hota hai jisme hackers ki tarah attack karke vulnerabilities find ki jaati hain.

===

2. WHY THIS FIELD IS THE BEST RIGHT NOW

• Bhid (competition) sabse kam

• Demand sabse zyada (India + International)

• Salary highest in IT

• Remote jobs easily available

• Freelance + Bug bounty = Extra earning

===

3. FULL A–Z ROADMAP (BEGINNER $\rightarrow$ EXPERT)

STEP 1: Computer Basics + Networking

• Computer fundamentals

• Windows + Linux

• Networking (IP, DNS, MAC, Protocols)

• Tools: CMD, PowerShell, Terminal

FREE SOURCES:

• FreeCodeCamp

• Cisco CCNA YouTube Notes

• Professor Messer – YouTube

===

STEP 2: Learn Linux (Master Level Required)

• Commands

• File permissions

• Bash scripting basics

• Networking in Linux

FREE SOURCES:

• TryHackMe – Linux Fundamentals

• DistroTube (YouTube)

• NetworkChuck (YouTube)

==

STEP 3: Networking Deep Learning

• TCP/IP

• Routing

• Firewalls

• Proxies

• VPN

• Ports & protocols

FREE SOURCES:

• YouTube – The Cyber Mentor

• FreeCodeCamp Linux/Networking playlists

==

STEP 4: Cyber Security Fundamentals

• CIA Triad

• Vulnerabilities

• Malware

• Phishing

• Sniffing

• DoS, SQLi, XSS basics

FREE SOURCES:

- TryHackMe – Pre-Security Path

- OWASP Web Security Testing Guide

- John Hammond (YouTube)

==

STEP 5: Web Application Security (OWASP TOP 10)

Topics:

- SQLi

- XSS

- CSRF

- SSRF

- LFI & RFI

- IDOR

- Authentication flaws

- Security misconfig

FREE SOURCES:

- PortSwigger Academy

- TryHackMe – Web Fundamentals

- HackTricks (GitHub)

==

STEP 6: Penetration Testing Practical

Phases:

- Reconnaissance

- Enumeration

- Scanning

- Exploitation

- Post-exploitation

- Privilege Escalation

TOOLS:

- Nmap

• Burp Suite

• Wireshark

• Metasploit

• Hydra

• Gobuster / Dirsearch

• Nessus

FREE SOURCES:

• HackTheBox Academy (Free)

• TryHackMe – Offensive Pentesting

• TCMSecurityAcademy (YT)

==

STEP 7: Bug Bounty Hunting

PLATFORMS:

• HackerOne

• BugCrowd

• Intigriti

• Federacy

• YesWeHack

FREE SOURCES:

• Bug Bounty Hunter Roadmap – YouTube

• NahamSec (BEST YouTube Channel)

• InsiderPhD (YT)

• LiveOverflow (YT)

==

STEP 8: Real Practice Platforms (ALL FREE/PAID)

• TryHackMe — Best for beginners

• HackTheBox — Intermediate to advanced

• PortSwigger Academy — Web security expert

• PicoCTF — CTF for beginners

- OverTheWire — Linux + CTF

- Root-Me — Realistic challenges

- CyberDefenders — SOC Analysis practice

- BlueTeamLabs — SOC, SIEM labs

- LetsDefend — SOC Analyst path

==

STEP 9: Certifications (OPTIONAL BUT USEFUL)

Affordable:

- eJPT (BEST for beginners)

- TCM Security – Practical Ethical Hacking

- Google Cybersecurity Certificate

Expensive:

- OSCP (Advanced)

- CEH (Industry recognized)

==

STEP 10: Build a Cyber Portfolio

- GitHub pe projects

- Vulnerability write-ups

- Tools you created

- TryHackMe/HackTheBox profile

- Web portfolio website

==

STEP 11: Job & Internship Platforms

- LinkedIn

- Internshala

- Indeed

- Naukri

- naukri.com

- AngelList (startups)

Roles:

• Cyber Security Intern

• SOC Analyst L1

• Junior Pentester

• Security Analyst

==

4. DAILY PRACTICE ROUTINE (HIGHLY EFFECTIVE)

• 1 hour Linux

• 1 hour Networking

• 1 hour TryHackMe/HackTheBox

• 30 min Bug Bounty

• Every week – 1 write-up

• Every month – 1 project

==

5. FULL RESOURCE LIST (ALL BEST SOURCES)

YOUTUBE CHANNELS (TOP QUALITY):

• John Hammond

• NahamSec

• LiveOverflow

• Stök (Bug bounty)

• IppSec (HackTheBox walkthroughs)

• The Cyber Mentor

• NetworkChuck

• HuskyHacks

PRACTICE SITES:

• TryHackMe

• HackTheBox

• PortSwigger Web Academy

- Root-Me

- PicoCTF

- LetsDefend

- CyberDefenders

DOCUMENTATION & BLOGS:

- OWASP.org

- HackTricks

- GTFOBins

- RedTeamNotes

- PayloadAllTheThings

===

6. EXPECTED TIMELINE

- 1–2 months → Basics complete

- 2–4 months → Web + Pentesting

- 4–6 months → Bug bounty + SOC

- 6–8 months → JOB READY

===

7. SALARY STRUCTURE

- Internship = ■5,000–■20,000

- SOC Analyst = ■20,000–■40,000

- Pentester = ■40,000–■1,00,000

- Bug Bounty = Unlimited (■10k to ■5 lakh per bug possible)

===

8. FINAL ADVICE

- Certificate se zyada SKILL matter karta hai

- Daily practice = guaranteed job

- Report writing seekho

- Portfolio strong banao

- Consistency rakho — cyber me growth sabse fast hai

==

This is the Advanced V2.0 A–Z Cyber Security & Pentesting Master Guide.