Road map

Welcome to this comprehensive **Ethical Hacking Mastery Roadmap** with practical timelines, expert tips, powerful tools, and **100% free resources**. This plan is designed for those dedicating **6–8 hours daily** to learning.t tips, and **100% free resources**. This plan is designed for those dedicating **6–8 hours daily** to learning.

🧭 Phase 1: Foundation (Months 1–3)

🔧 Skills:

- Linux & Bash
- Networking Basics (TCP/IP, HTTP, DNS)
- Python Programming
- Cybersecurity Fundamentals

📚 Free Resources:

- OverTheWire: Bandit – Linux practice
- Cisco Networking Basics – TCP/IP
- Python for Beginners (freeCodeCamp)
- Cybrary - Intro to IT & Cybersecurity

💡 Tips:

- Practice Linux daily (2h minimum)
- Build small Python tools (port scanner, simple keylogger)
- Use TryHackMe - Introduction to Cyber Security

🛠️ Phase 2: Offensive Security (Months 4–6)

🔧 Skills:

- Web App Hacking (SQLi, XSS, SSRF)
- Network Sniffing & Recon (Nmap, Wireshark)
- Social Engineering (OSINT, phishing)
- Kali Linux Tools

📚 Free Resources:

- OWASP Top 10
- HackTricks Wiki
- Wireshark Tutorial
- TryHackMe: Web Fundamentals
- MIT OpenCourseware - Computer Systems Security

💡 Tips:

- Focus 2h daily on real lab practice (HackTheBox, TryHackMe)
- Write pentest reports for your findings

💣 Phase 3: Malware & Cryptography (Months 7–10)

🔧 Skills:

- Malware Writing (RATs, keyloggers)
- Cryptography (RSA, AES, hashing)
- Evasion techniques
- Basic C/C++ and Assembly

📚 Free Resources:

- Malware Unicorn RE 101
- Crypto101 Book

- Reverse Engineering for Beginners (PDF)
- TryHackMe: Malware Analysis

💡 Tips:

- Reverse sample malware (in sandbox only!)
- Write your own ransomware clone (don't distribute it)

🔍 Phase 4: Advanced Exploitation (Months 11–14)

🔧 Skills:

- Reverse Engineering (Ghidra, IDA Free)
- Buffer Overflow, Shellcode
- Exploit Development
- Binary Fuzzing

📚 Free Resources:

- Exploit Development on TryHackMe
- Ghidra 101
- LiveOverflow Exploit Dev YouTube Series

💡 Tips:

- Try HackTheBox "Buffer Overflow" boxes
- Start with Linux binaries before moving to Windows

🧬 Phase 5: Real-World Hacking & Bug Bounties (Months 15–18)

🔧 Skills:

- Bug Bounty Hunting

- OSINT + Recon Automation
- C2 Frameworks (e.g., Cobalt Strike alternatives)
- Red Team Methodology

📚 Free Resources:

- HackerOne Hacking 101
- Bug Bounty Hunter Roadmap (by zseano)
- NahamSec YouTube Channel

💡 Tips:

- Automate recon with tools like Amass, Subfinder
- Write full bug reports to practice disclosure

💻 Optional: Hardware & IoT Hacking (Parallel Anytime)

🔧 Skills:

- Arduino/ESP32 basics
- USB sniffing
- RFID/NFC exploitation
- Rubber Ducky scripting

📚 Free Resources:

- Hackster.io Projects
- Hak5 YouTube

💡 Tips:

- Start with Arduino & ESP32
- Buy cheap IoT devices to hack safely

🧠 Practice Platforms (All Levels)

Platform	Focus Area
TryHackMe	Guided labs, beginner to advanced
Hack The Box	Real-world CTFs and networks
VulnHub	Offline VMs for local labs
Root-Me	Challenge-based learning
PicoCTF	Beginner CTF challenges
CTFtime.org	Real-time CTF events

🏆 Optional Certifications (After 18 Months)

Cert	Focus	Cost	Notes
OSCP	Penetration Testing	$1599	Gold standard
eJPT	Entry-level PenTesting	$200	Good start
CEH	Ethical Hacking	$$$	HR-friendly, but not hands-on

Notes