# Complete Roadmap to Learn Ethical Hacking

## Introduction

This roadmap will guide you through the journey of becoming an ethical hacker. From networking basics to certifications, it covers all the essential topics to start and excel in the field of cybersecurity.

## 1. Understand the Basics of Networking

Learn Networking Concepts:

- TCP/IP, UDP, DNS, HTTP, HTTPS, FTP, SMTP
- Subnetting and Network Address Translation (NAT)

Learn Network Security Tools:

- Wireshark: Network traffic analysis
- Nmap: Network scanning and mapping

## 2. Master Operating Systems

Linux (Essential for hacking):

- Learn basic Linux commands (ls, cd, grep, find, chmod)
- Understand file systems, shell scripting, and permissions

Windows:

- Explore the Windows registry and file systems
- Learn about PowerShell for automation and security testing

## 3. Programming & Scripting

Languages to Learn:

- Python: For automating tasks and exploit development

- Bash: For scripting on Linux

- JavaScript: For understanding web vulnerabilities

- C/C++: For understanding exploits and buffer overflows

Resources:

- Codecademy, freeCodeCamp, or W3Schools for structured learning

## 4. Learn Web Application Security

Key Topics:

- SQL Injection, XSS, CSRF, File Inclusion, Broken Authentication

Tools:

- Burp Suite: For web vulnerability scanning

- OWASP ZAP: Open-source web application scanner

Study the OWASP Top 10: Understand the most critical web vulnerabilities.

## 5. Understand Cybersecurity Fundamentals

- Learn how firewalls, IDS/IPS, and antivirus software work

- Understand data encryption, hashing, and cryptography concepts

- Study basic concepts of malware analysis (viruses, worms, trojans)

Ethical Hacking Basics:

- Phases of Ethical Hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks

## 6. Learn Penetration Testing

- Follow frameworks like PTES (Penetration Testing Execution Standard)

- Practice hands-on with real-world scenarios and tools

## 7. Use Ethical Hacking Tools

Reconnaissance Tools:

- Maltego, Shodan, Google Dorking

Exploitation Tools:

- Metasploit, Exploit-DB

Password Cracking Tools:

- John the Ripper, Hashcat

Wireless Hacking Tools:

- Aircrack-ng, Wifiphisher

## 8. Explore Specific Domains

Network Penetration Testing:

- Learn about VLANs, VPNs, and wireless network penetration

Web Application Penetration Testing:

- Master tools like SQLmap and Nikto

Mobile Hacking:

- Explore tools like Drozer and learn Android/iOS vulnerabilities

## 9. Gain Certifications

- Certified Ethical Hacker (CEH)
- CompTIA Security+
- Offensive Security Certified Professional (OSCP)
- Certified Information Systems Security Professional (CISSP)

## 10. Practice Real-World Scenarios

Platforms for Hands-On Practice:

- TryHackMe, Hack The Box, CTF challenges (e.g., OverTheWire)

Build a Home Lab:

- Use tools like VirtualBox to set up virtual machines and simulate attacks

## 11. Stay Updated

- Follow cybersecurity blogs and forums (e.g., BleepingComputer, KrebsOnSecurity)
- Join communities like Reddit (r/hacking) and LinkedIn groups

## 12. Legal and Ethical Boundaries

- Understand cybersecurity laws and regulations in your country

- Learn about data privacy laws like GDPR and CCPA

## Timeline

1-3 Months: Networking basics and OS fundamentals

4-6 Months: Programming, web security, and ethical hacking basics

6-12 Months: Practice tools, specialize in a domain, and get certified

1 Year+: Contribute to open-source projects, join bug bounty programs, and advance your skills.