

# Forum:[Hack Forums](#)

Thread: [Free pentesting and hacking learning pathway](#)

ryan\_10o0 - June 15, 2025, 4:31 am

Entering the field of penetration testing (often referred to as "pentesting") can be exciting and rewarding. Here's a structured learning pathway to help you become a proficient pentester:

## ### 1. Foundational Knowledge

- Basic IT Skills
  - Learn about operating systems (Windows, Linux)
  - Understand networking concepts (TCP/IP, subnetting, routing)
  - Familiarize yourself with hardware components and how they work together
- Programming/Scripting
  - Choose a programming language (Python, JavaScript, or C) to understand the basics of coding.
  - Learn scripting languages (Bash, PowerShell) to automate tasks.

## ### 2. Networking Knowledge

- Deep Dive into Networking
  - Understand how networks operate, including different protocols (HTTP, HTTPS, FTP, DNS).
  - Learn about firewall configurations, VPNs, and how different types of network devices work.
- Study Network Security
  - Get to know common network attacks (Man-in-the-Middle, DDoS).
  - Understand how to secure a network.

## ### 3. Understanding Security Fundamentals

- Cybersecurity Basics
  - Familiarize yourself with basic security principles (CIA triad: Confidentiality, Integrity, Availability).
  - Understand threats, vulnerabilities, and how exploits work.
- Security Certifications
  - Consider obtaining certifications such as CompTIA Security+ to validate your foundational knowledge.

## ### 4. Learn About Ethical Hacking

- Study Ethical Hacking Practices
  - Read about the legal and ethical aspects of hacking.
  - Familiarize yourself with common ethical hacking methodologies (OWASP, NIST).

## ### 5. Tools of the Trade

- Common Penetration Testing Tools
  - Learn how to use tools like Nmap (network scanning), Metasploit (exploitation framework), Burp Suite (web application testing), and Wireshark (network traffic analysis).
- Vulnerability Assessment Tools
  - Work with tools like Nessus or OpenVAS for identifying vulnerabilities.

## ### 6. Practical Skills and Labs

- Hands-on Practice
  - Set up a lab environment (use virtual machines or cloud-based environments).

- Use platforms like Hack The Box, TryHackMe, or CTF (Capture The Flag) challenges to practice penetration testing skills.
- Vulnerable Web Applications
  - Experiment with vulnerable applications like DVWA (Damn Vulnerable Web Application), OWASP Juice Shop, or WebGoat.

#### ### 7. Advanced Topics

- Web Application Penetration Testing
  - Understand common web vulnerabilities (SQL Injection, Cross-Site Scripting, CSRF).
  - Learn to perform web app security assessments.
- Network Penetration Testing
  - Explore advanced techniques like wireless hacking, social engineering, and reverse engineering.
- Post-Exploitation Techniques
  - Learn how to maintain access and pivot within a network after exploitation.

#### ### 8. Certifications in Pentesting

- Obtain Relevant Certifications
- Consider certifications specifically for pentesting such as:
  - Certified Ethical Hacker (CEH)
  - Offensive Security Certified Professional (OSCP)
  - CompTIA PenTest+
  - GIAC Penetration Tester (GPEN)

#### ### 9. Stay Current

- Follow Industry Trends
  - Keep learning and stay updated on the latest security news, threats, and techniques.
  - Subscribe to cybersecurity blogs, podcasts, and forums.
- Network with Professionals
  - Join cybersecurity communities, attend conferences, and participate in local meetups.

#### ### 10. Practical Experience

- Internships or Entry-Level Positions
  - Seek internships or junior roles in cybersecurity to gain real-world experience.
- Build a Portfolio
  - Document your projects, write articles, or share your experience in the cybersecurity community.

#### ### Conclusion

Becoming a proficient penetration tester requires a combination of theoretical knowledge, practical skills, and continuous learning. It's a field that is always evolving, so commitment to lifelong learning and staying updated with the latest trends in cybersecurity is crucial. Good luck on your pentesting journey!

**HerrWinston** - June 19, 2025, 2:42 pm

this might just be the pathway i will save and use as my progression bar