Penetration Testing Career Roadmap

From Beginner to Professional Pentester

Duration: 12-18 Months
Updated: December 2025

Month 1-3: Foundations

What to Learn

- Linux basics (Ubuntu/Kali)
- Networking fundamentals (TCP/IP, DNS, HTTP)
- Programming basics (Python, Bash)
- Web technologies (HTML, JavaScript, PHP)

Hands-On Practice

- Set up Kali Linux VM
- Learn command line
- Write simple Python scripts
- Build basic website

Resources

- TryHackMe (Free tier)
- OverTheWire: Bandit
- YouTube: NetworkChuck, John Hammond
- Book: "Linux Basics for Hackers"

Goal

Complete 20 TryHackMe beginner rooms

Month 4-6: Core Security Skills

What to Learn

- OWASP Top 10 vulnerabilities
- Web application security
- Network scanning (Nmap)
- Burp Suite basics
- SQL injection
- XSS attacks

Hands-On Practice

- HackTheBox easy machines (5-10)
- DVWA (Damn Vulnerable Web App)
- WebGoat exercises
- Capture simple CTF flags

Certifications to Consider

- **CompTIA Security+** (optional but recommended)

Resources

- PortSwigger Web Security Academy (Free)
- OWASP resources
- PentesterLab (Free intro paths)

Month 7-9: Intermediate Skills

What to Learn

- Privilege escalation (Linux & Windows)
- Active Directory basics
- Metasploit Framework
- Password cracking
- Reverse shells
- Post-exploitation techniques

Hands-On Practice

- HackTheBox medium machines

- VulnHub VMs
- TryHackMe Offensive Pentesting path
- Practice CTFs

Certifications to Consider

- **CEH (Certified Ethical Hacker)** - Good for job market
- **eJPT (eLearnSecurity Junior Pentester)** - Practical

Resources

- TJ Null's OSCP-like machines list
- IppSec YouTube walkthroughs
- Cybrary courses

Goal

Pass CEH or eJPT certification

Month 10-12: Advanced Preparation

What to Learn

- Buffer overflow exploitation
- Advanced enumeration
- Scripting for automation
- Report writing
- Methodology (PTES, OWASP)

Hands-On Practice

- OSCP-like machines (30+ machines)
- Practice buffer overflow repeatedly
- Write professional reports
- Join bug bounty programs (HackerOne, Bugcrowd)

Certifications to Consider

- **OSCP (Offensive Security Certified Professional)** - Industry gold standard

Resources

- Offensive Security Proving Grounds
- TryHackMe OSCP prep rooms
- HTB retired machines

Goal

Schedule and pass OSCP exam

Month 13-18: Professional Level

What to Learn

- Advanced Active Directory attacks
- Cloud security (AWS, Azure)
- Mobile app pentesting
- API security testing
- Red team tactics

Hands-On Practice

- Bug bounties (earn your first $100)
- Real penetration tests (internship/junior role)
- Contribute to security tools
- Build portfolio

Certifications to Consider

- **PNPT (Practical Network Penetration Tester)**
- **CRTP (Certified Red Team Professional)**
- **CRTA (Certified Red Team Analyst)**
- **BSCP (Burp Suite Certified Professional)**

Career Steps

- Apply for junior pentester roles
- Build LinkedIn profile
- Share writeups on Medium/GitHub

- Network at security conferences

Goal

Land first paid pentester position

Essential Tools to Master

Reconnaissance:

- Nmap
- Gobuster/Dirbuster
- Nikto

Exploitation:

- Metasploit
- Burp Suite
- SQLmap

Post-Exploitation:

- Mimikatz
- LinPEAS/WinPEAS
- PowerSploit

Utilities:

- Netcat
- Wireshark
- Hashcat/John the Ripper

Learning Platforms

Free

- TryHackMe (limited free)
- HackTheBox (limited free)
- PortSwigger Academy
- OverTheWire
- PicoCTF

Paid (Worth It)

- TryHackMe Premium (262/month)
- HackTheBox VIP ($2253/month)

Weekly Study Schedule

Monday-Friday (2-3 hours/day)

- 1 hour: Theory/reading
- 1-2 hours: Hands-on labs

Saturday (4-6 hours)

- CTF challenges
- HackTheBox/TryHackMe machines
- Practice exam prep

Sunday (2-4 hours)

- Write reports
- Document learnings
- Build portfolio
- Review week's progress

Key Milestones Checklist

Beginner ✓

- [ ] Set up Kali Linux
- [ ] Complete 50 TryHackMe rooms
- [ ] Solve 5 HackTheBox easy machines
- [ ] Understand OWASP Top 10
- [ ] Write first penetration test report

Intermediate ✓

- [ ] Pass Security+ or CEH
- [ ] Complete 20 HackTheBox machines
- [ ] Master Burp Suite

- [ ] Perform SQL injection manually
- [ ] Escalate privileges on 10 systems

Advanced ✓

- [ ] Pass CRTP/CRTA certification
- [ ] Complete 50+ vulnerable machines
- [ ] Submit first bug bounty
- [ ] Build personal lab environment
- [ ] Create GitHub portfolio

Professional ✓

- [ ] Pass OSCP certification
- [ ] Land junior pentester job
- [ ] Complete real penetration test
- [ ] Earn $500+ from bug bounties
- [ ] Present at local security meetup
- [ ] Mentor other beginners

Job Search Timeline

Month 12-13: Prepare

- Update resume with skills/certs
- Build GitHub with writeups
- Create LinkedIn profile
- Join local security groups

Month 14-15: Apply

- Apply to 20+ junior pentester roles
- Network at conferences/meetups
- Do informational interviews
- Consider internships

Month 16-18: Interview & Land Job

- Technical interviews (expect practical tests)

- Demonstrate hands-on skills
- Show passion and continuous learning
- Accept first offer (negotiate salary)

Common Mistakes to Avoid

❌ Jumping to advanced tools without basics
❌ Only watching tutorials (no hands-on)
❌ Giving up after failing once
❌ Skipping report writing practice
❌ Not documenting your learning
❌ Isolating yourself (join communities!)
❌ Focusing only on certifications
❌ Not building a portfolio

Success Tips

✅ **Consistency beats intensity** - 2 hours daily > 14 hours on Sunday
✅ **Learn to fail** - You'll get stuck often, that's normal
✅ **Document everything** - Keep notes, screenshots, commands
✅ **Join communities** - Discord, Reddit (r/netsec), local groups
✅ **Build in public** - Share writeups, help others
✅ **Stay legal** - Only test what you're authorized to test
✅ **Focus on fundamentals** - Master basics before advanced
✅ **Network actively** - Attend meetups, conferences, webinars

Support & Community

Discord Servers:

- TryHackMe Official
- HackTheBox Official
- The Cyber Mentor

Reddit:

- r/netsec
- r/AskNetsec
- r/oscp

Twitter (X) Follow:

- @TJ_Null
- @thecybermentor
- @IppSec
- @0xdf_

Final Advice

> "The journey from beginner to pentester is not about talent. It's about **persistence, curiosity, and consistent effort**. Start today, fail often, learn always."

Your Next Step: Complete the CloudMints lab, document your process, and share your writeup. That's your Day 1.

Questions? synnefo.in
Updates: Follow @synnefo.academy on Instagram

Good luck on your journey! 🚀

This roadmap is based on real career transitions from 100+ successful pentesters. Adjust timeline based on your availability and learning pace.