Refined Learning Plan to Become a Professional Penetration Tester (Free & Self-Taught Path)

🌟Overview

This revised plan incorporates your feedback and strengthens areas like scripting, cloud, mobile, API hacking, and reporting, with realistic free alternatives to paid certifications. It structures the roadmap around real-world job roles, ensures hands-on learning, and provides a path from junior pentester to advanced red teamer.

🌧️Phase 1: Foundations (Networking, Scripting, Linux, and Windows Basics)

Duration: 3 Weeks (merge with Phase 2 if already comfortable)

Key Skills:

- Networking fundamentals: IP, ports, TCP vs. UDP, firewalls, NAT.
- Essential tools: `ping`, `traceroute`, `netstat`, `ipconfig/ifconfig`, Wireshark.
- Linux basics: File permissions, processes, package management.
- Windows basics: Registry, services, PowerShell fundamentals.
- Scripting: Basic Python (automation), Bash (Linux automation), PowerShell (Windows scripting).

Free Resources:

- Cisco Networking Basics
- OverTheWire: Bandit
- FreeCodeCamp Python Course
- HackTricks Book for cheatsheets

🌧️Phase 2: Web & API Pentesting

Duration: 2 Months

Key Skills:

- OWASP Top 10: XSS, SQLi, SSRF, Insecure Deserialization, File Uploads.
- API Hacking: OWASP API Top 10, JWT, tokens, API fuzzing.
- Tools: Burp Suite (Community), OWASP ZAP, Postman, dirsearch.
- Post-exploitation: Web shells, creating users, data exfiltration basics.
- Automation: Build simple Python tools to enumerate parameters, test headers, etc.

Free Resources:

- PortSwigger Web Security Academy
- Juice Shop
- Bugcrowd University
- OWASP ZAP Docs

🌧️Phase 3: Network Pentesting & Privilege Escalation

Duration: 2 Months

Key Skills:

- Tools: Nmap, Netcat, Wireshark, enum4linux, SMBclient.
- Windows PrivEsc: AlwaysInstallElevated, unquoted service paths, DLL hijacking.
- Linux PrivEsc: SUID/SGID, weak permissions, cron jobs, PATH hijacking.
- Basic buffer overflows.
- Write scripts to parse `LinPEAS` or `WinPEAS` output for common weaknesses.

Free Resources:

- GTFOBins
- LOLBAS
- VulnHub: Kioptrix, Basic Pentesting
- TryHackMe: Linux PrivEsc

🌧️Phase 4: Active Directory Pentesting

Duration: 1.5 Months

Key Skills:

- AD Enumeration: BloodHound, SharpHound, LDAP basics.
- Attacks: AS-REP Roasting, Kerberoasting, DCSync, Pass-the-Hash.
- Lateral movement: PsExec, WinRM, RDP.
- Persistence: GPO abuse, registry manipulation.
- Create PowerShell scripts for recon, backdoor deployment.

Free Resources:

- TryHackMe: Attacktive Directory
- [HackTheBox Machines Tagged "Active Directory"]
- Windows Server 2019 Eval ISO + VirtualBox

🌧️Phase 5: Post-Exploitation, Evasion & Specialization

Duration: 1.5 Months

Core Topics:

- Evasion: AV/EDR bypass, obfuscation, encrypted payloads.
- Data Exfiltration: Covert channels, DNS tunneling.
- Command & Control (C2): Sliver framework (community edition).
- Specializations:
- **Red Team**: AD persistence, phishing, C2 management.
- **Bug Bounty**: Advanced web exploitation, logic flaws, chained attacks.
- **Reverse Engineering**: Ghidra, GDB, writing shellcode.

Free Resources:

- MITRE ATT&CK Framework
- MalDev Academy (Free)
- LiveOverflow YouTube
- Sliver Framework Docs

🌧️Bonus: Cloud & Mobile Security

Add-on Modules (Optional but Valuable)

Cloud:

- S3 bucket misconfigurations.
- IAM Role privilege escalation.
- Azure AD basics.

Free Resources: - Flaws.Cloud - TryHackMe: AWS Pentesting

Mobile:

- Android APK decompiling, traffic interception.
- OWASP Mobile Top 10.

Free Tools: - JADX, MobSF, Frida

🌧️Soft Skills: Reporting, Documentation & Ethics

Why It Matters:

- In real-world jobs, being able to write clear, professional reports is a must.

• Ethics keeps you legally safe and professionally respected.

Practice: - Document every lab/CTF as a pentest report (Executive Summary + Findings + Recommendations). - Study real pentest report templates. - Read and follow HackerOne Disclosure Guidelines

---

🌧️Proof of Skill (Without Paying)

• **GitHub**: Upload scripts, tools, and write-ups.
• **LinkedIn**: Share CTF completions, lessons, and blog posts.
• **TryHackMe/HTB Profile**: Publically visible accomplishments.
• **Write Reports**: Share PDFs (redacted) of your test reports for CTFs.

🌧️Timeline Suggestion (Flexible)

Month	Goal
1	Phase 1 + Phase 2 merged if basics are known
2	Finish Web/API Pentesting fully
3	Deep Network + PrivEsc Exploitation
4	Active Directory Pentesting
5	Evasion + Choose Specialization
6	Portfolio, Reporting, Practice Labs & Cloud/Mobile add-on

💐Final Advice

• Keep everything hands-on.
• Share everything you learn (LinkedIn, GitHub).
• Always play ethically and legally.
• Start small, stay consistent, finish strong.

If you follow this, you can become a **Junior Pentester**, Bug Bounty Hunter, or Red Team Apprentice without paying for elite courses.