**LỘ TRÌNH HỌC PENTESTER (12-18 THÁNG)**

*Dành cho người mới bắt đầu, 4-6 giờ/tuần*

**1. Giai đoạn 1: Nền tảng cơ bản (0-3 tháng)**

* Linux cơ bản: Lệnh cơ bản (ls, cd, grep), cài Kali Linux trên máy ảo.
* Mạng: Mô hình TCP/IP, giao thức (HTTP, DNS), dùng Wireshark, nmap.
* Lập trình: Python (cú pháp cơ bản, script quét port), HTML/JavaScript (cấu trúc web).
* Tài liệu: TryHackMe (Linux Fundamentals, Network Fundamentals), FreeCodeCamp (Python), W3Schools (HTML).
* Thực hành: OverTheWire Bandit (Level 0-10), quét mạng giả lập.

**2. Giai đoạn 2: Pentest cơ bản (4-8 tháng)**

* Quy trình pentest: Thu thập thông tin (nmap, theHarvester), quét lỗ hổng, khai thác.
* Web pentest: SQL Injection, XSS, dùng Burp Suite, OWASP ZAP.
* Khai thác: Metasploit, Hydra, SQLmap trên Metasploitable.
* Tài liệu: TryHackMe (OWASP Top 10, Metasploit), PortSwigger Web Security Academy.
* Thực hành: Hack The Box (Starting Point), PicoCTF, DVWA (web vulnerabilities).

**3. Giai đoạn 3: Chuyên sâu và chứng chỉ (9-18 tháng)**

* Nâng cao: Privilege escalation, Active Directory, SSRF, XXE.
* Chứng chỉ: Chuẩn bị OSCP (Offensive Security), eJPT (nếu mới).
* Hồ sơ: Viết blog (Medium, GitHub), thử bug bounty (HackerOne).
* Tài liệu: Hack The Box (máy Medium), TryHackMe (OSCP Prep), HackTricks.
* Thực hành: Root 5-10 máy Hack The Box, viết báo cáo pentest.

**Lưu ý**

* Chỉ thực hành trên lab hợp pháp (TryHackMe, Hack The Box, VulnHub).
* Tham gia cộng đồng: VN Security, group Telegram, Discord TryHackMe.
* Theo dõi tiến độ: Ghi chú các kỹ năng đã học, máy đã root.