دوره جامع هک قانونمند و مهندسی امنیت سایبری

Advanced Cybersecurity & Ethical Hacking

Complete Career Training Program

راهنمای کامل و گام‌به‌گام برای تبدیل شدن به یک مهندس امنیت حرفه‌ای

از صفر مطلق تا متخصص امنیت سایبری

این دوره توسط تیم امنیت صفر و یک سایبر طراحی شده است

هشدار قانونی: این سند صرفاً برای آموزش امنیت سایبری قانونمند تهیه شده است

هرگونه استفاده غیرقانونی از مطالب بر عهده کاربر می‌باشد

این دوره مسیر شغلی شما را از یک فرد مبتدی تا یک مهندس امنیت حرفه‌ای طراحی کرده است

مسیر یادگیری : نقشه راه مهندس امنیت

این بخش نقشه راه شما برای تبدیل شدن به یک مهندس امنیت سایبری حرفه‌ای است.

مسیر یادگیری به ۶ مرحله تقسیم شده است :

مرحله	مدت زمان	مهارت ها	خروجی
Foundation	۳-۴ ماه	Linux, Networking, Python, Windows	فرد مبتدی آماده
Recon	۲ ماه	OSINT, Scanning, Enumeration	شناساگر حرفه‌ای
Exploitation	۴-۵ ماه	Vuln Assessment, MSF, Web Hacking, AD	تست‌کننده نفوذ
Advanced	۳-۴ ماه	Malware, C2, Cloud, Mobile, Red Team	مهندس امنیت پیشرفته
Defense	۲ ماه	Blue Team, Forensics, IR, SIEM	مهندس امنیت کامل
Professional	مداوم	Certs, CTF, Bug Bounty, Community	متخصص امنیت حرفه‌ای

نکات کلیدی برای موفقیت :

- یک محیط آزمایشگاهی (Home Lab) بسازید و هر مبحث را تمرین کنید
- بعد از هر فصل، تمرینات انتهای آن را کامل انجام دهید
- روزانه حداقل ۳-۲ ساعت تمرین عملی داشته باشید
- در پلتفرم‌های TryHackMe و HackTheBox عضو شوید
- از یک دفترچه یادداشت (Pentest Journal) برای ثبت یادگیری استفاده کنید
- در جامعه امنیتی شرکت کنید (Discord, Telegram, Conferences)
- هر مبحثی که یاد می‌گیرید، به دیگران آموزش دهید

محیط آزمایشگاهی پیشنهادی :

ماشین‌های مجازی (VM)

مهاجم (Attacker) :

Kali Linux (ابزارهای تست نفوذ)

Parrot OS (جایگزین Kali)

Commando VM (ویندوز برای هک)

قربانیان (Targets) :

Metasploitable 2 (لینوکس آسیب‌پذیر)

Metasploitable 3 (ویندوز آسیب‌پذیر)

DVWA / OWASP BWA (برنامه وب آسیب‌پذیر)

VulnHub / Proving Grounds (ماشین‌های CTF)

شبکه :

VMWare یا VirtualBox با Internal Network

Raspberry Pi + Pi-Hole برای DNS

Windows Server 2019 برای AD