

هک قانونمند (Ethical Hacking)

صفر و یک سایبر

مفاهیم پایه امنیت

قبل از هر هکی، باید بفهمی امنیت یعنی چی:

- CIA Triad
 - محرمانگی (Confidentiality)
 - یکپارچگی (Integrity)
 - دسترس پذیری (Availability)
- تفاوت Threat / Vulnerability / Risk
- هکر کیه؟
 - White Hat
 - Gray Hat
 - Black Hat

شبکه (خیلی مهم)

حداقل شبکه رو باید مسلط باشی:

- TCP/IP
- OSI Model
- IP, MAC, Port
- DNS, DHCP
- پروتکل ها:
- HTTP / HTTPS
- FTP
- SSH
- SMTP

سیستم عامل ها

لینوکس (اولویت بالا)

- کار با ترمینال
- دستورات پایه:
ls cd chmod chown grep nano vim
- مدیریت سرویس ها
- Permission ها

ویندوز

- ساختار فایل ها
- Registry
- User & Group
- Services

وب و برنامه نویسی پایه

لازم نیست برنامه نویسی حرفه ای باشی، ولی اینا رو باید بدونی:

- HTML / CSS
- JavaScript (XSS)
- PHP (
- SQL (

مفاهیم وب و HTTP

- Request / Response
- GET / POST
- Cookies & Sessions
- Headers
- Status Code ها (۲۰۰، ۴۰۳، ۵۰۰ و ...)

آشنایی با آسیب پذیری ها (OWASP Top 10)

مهم ترین بخش برای شروع:

- SQL Injection
- XSS
- CSRF
- Broken Authentication
- File Upload Vulnerability
- LFI / RFI
- Command Injection

ابزارهای پایه هک

اول یاد بگیر چی کار می کنن، بعد استفاده:

- Kali Linux
- Nmap
- Burp Suite
- Metasploit
- Wireshark

متدولوژی تست نفوذ

یاد بگیر هک بی نظم نیست:

۱. Reconnaissance
۲. Scanning
۳. Gaining Access
۴. Maintaining Access
۵. Reporting

پیشنهاد مسیر یادگیری

۱. Network + Linux
۲. Web + HTTP
۳. OWASP Top 10
۴. ابزارها
۵. Lab تمرینی

