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

فصل یک

طرز فکر هکری و مبانی امنیت

قبل از یادگیری ابزارها، باید طرز فکر یک هکر را یاد بگیرید.

هکرها متفاوت فکر می‌کنند، خارج از چارچوب می‌بینند و هرگز تسلیم نمی‌شوند

طرز فکر هکری (Hacker Mindset)

پنج اصل طرز فکر هکری :

۱. تفکر جانبی (Lateral Thinking): همیشه به راه‌های جایگزین فکر کنید. اگر یک در بسته است، دنبال پنجره، زیرزمین یا سقف بگردید.

۲. کنجکاوی سیری‌ناپذیر: بپرسید "چرا؟" و "اگر ... چه می‌شود؟". همه چیز را تست کنید.

۳. پشتکار: اولین تلاش معمولاً شکست می‌خورد. دهمین تلاش ممکن است موفق شود.

۴. خلاقیت: بهترین هک‌ها ترکیبی از چند تکنیک ساده است، نه یک تکنیک پیچیده.

۵. یادگیری مادام‌العمر: امنیت سایبری هر روز تغییر می‌کند. اگر امروز یاد نگیرید، فردا عقب هستید.

طبقه‌بندی هکرها و تفاوت‌ها :

نوع	مجوز	هدف	محدودیت
White Hat	دارد	بهبود امنیت	اخلاق و قانون
Black Hat	ندارد	سود شخصی	هیچ
Grey Hat	مبهم	کشف و افشا	متغیر
Red Team	دارد	تست امنیت	قوانین درگیری
Blue Team	مسئولیت	دفاع	سیاست ها

چرخه کامل تست نفوذ (PTES Standard)

مرحله	فعالیت ها	خروجی
Pre-Engagement	قرارداد ، محدود ، قوانین	SOW, ROE, NDA
Intelligence Gathering	OSINT ، شناسایی	پروفایل هدف
Threat Modeling	تحلیل تهدید ، سناریو	سناریوهای حمله
Vulnerability Analysis	اسکن ، تایید دستی	لیست آسیب پذیری
Exploitation	بهره برداری	دسترسی اولیه
Post-Exploitation	افزایش دسترسی ، pivot	تصاحب هدف
Reporting	گزارش فنی و مدیریتی	گزارش نهایی

آشنایی با محیط آزمایشگاهی (Hands-On Lab Setup)

گام به گام راه‌اندازی آزمایشگاه شخصی :

گام ۱ : نصب VirtualBox/VMware

دانلود VirtualBox

https://www.virtualbox.org/wiki/Downloads

نصب Extension Pack برای USB 3.0 و RDP

VBoxManage extpack install Oracle_VM_VirtualBox_Extension_Pack

تنظیم Internal Network

File > Tools > Network Manager > Create Host-Only Network

آدرس : 192.168.56.1/24

گام ۲ : نصب Kali Linux

دانلود Kali Linux

https://www.kali.org/get-kali/#kali-virtual-machine

تنظیمات VM

+RAM: 4GB

CPU: 2 Cores

Disk: 80GB

Network: Host-Only + NAT

به‌روزرسانی Kali

sudo apt update && sudo apt full-upgrade -y

sudo apt install kali-linux-headless یا kali-linux-everything

گام ۳ : نصب ماشین‌های هدف

Metasploitable 2

https://sourceforge.net/projects/metasploitable/files/Metasploitable2

OWASP BWA (Broken Web Applications)

https://sourceforge.net/projects/owaspbwa

Windows 10/11 (با مجوز)

۱. دانلود ISO از Microsoft

۲. نصب در VM با حداقل ۴GB RAM

۳. غیرفعال کردن Windows Defender و Firewall

گام ۴ : راه‌اندازی Docker برای تمرین وب

نصب Docker

sudo apt install docker.io docker-compose -y

DVWA (Damn Vulnerable Web Application)

git clone https://github.com/digininja/DVWA.git

cd DVWA

docker-compose up -d

دسترسی: http://127.0.0.1:4280

bwapp

docker run -d -p 80:80 raesene/bwapp

Juice Shop (OWASP)

docker run -d -p 3000:3000 bkimminich/juice-shop

دسترسی : http://127.0.0.1:3000

گام ۵: راه‌اندازی AD برای تمرین

راه‌اندازی Active Directory با Vagrant

پیش‌نیاز : نصب Vagrant و VirtualBox

```
mkdir ad-lab && cd ad-lab

vagrant init
```

سپس Vagrantfile را با محتوای زیر ایجاد کنید

```
|Vagrant.configure("2") do |config

"config.vm.box = "gusztavvargadr/windows-server-2019-standard

"config.vm.hostname = "DC01

"config.vm.network "private_network", ip: "192.168.56.10

|config.vm.provider "virtualbox" do |vb

"vb.memory = "4096

vb.cpus = 2

end

end

vagrant up
```

تمرینات جامع فصل ۱

⚠ این تمرینات را کامل انجام دهید و خروجی را ذخیره کنید:

۱. VirtualBox + Kali Linux نصب کنید و اسکرین‌شات بگیرید

۲. در Kali به‌روزرسانی کامل انجام دهید و عکس بگیرید

۳. یک VM دیگر (Metasploitable 2) نصب کنید

۴. از هر دو VM یک snapshot بگیرید (برای بازگشت در صورت خرابی)

۵. با دستور ping ارتباط بین Kali و Metasploitable را چک کنید

۶. یک Docker نصب کنید و DVWA را اجرا کنید

۷. در Kali: sudo apt install -y nmap hydra john gobuster ffuf

۸. یک دفترچه یادداشت روزانه (Pentest Journal) شروع کنید

۹. در TryHackMe ثبت‌نام کنید و ماژول "Introduction to Cyber Security" را کامل کنید

۱۰. یک فایل Markdown با عنوان "My Security Journey" ایجاد کنید و اهداف خود را بنویسید