CODACKER.IR

راهنمای رایگان

کیت شروع هک

هرچیزی که برای شروع لازم داری، یک‌جا: سیستم و ابزار مورد نیاز، ۵۲ ابزار ضروری، و نقشه‌ی راه کامل.

هک به ابزار نیست، به طرز فکره. — این راهنما، شروع همون طرز فکره.

// start_kit

قبل از شروع، این رو بخون

اسکریپت‌کیدی صد تا ابزار نصب می‌کنه و هیچ‌کدوم رو نمی‌فهمه. هکر واقعی ده تا ابزار رو عمیق بلده و دقیقاً می‌دونه هر کدوم چیکار می‌کنه و کِی باید بره سراغش. کل تفاوت همینه — نه بیشتر.

پس این کیت یه لیست خرید نیست که تیک بزنی و رد شی. یه نقشه‌ست که بهت می‌گه چی لازم داری، از کجا شروع کنی، و به چه ترتیبی جلو بری تا وقتت هدر نره.

این کیت رو چطور استفاده کنی

اول از اول تا آخر یه بار بخونش، سریع و بدون توقف، فقط برای اینکه تصویر کامل دستت بیاد. بعد برگرد سراغ بخش سیستم و محیطتو راه بنداز. بعدش لیست ابزارها می‌شه مرجعت — هر وقت به یه ابزار رسیدی، برگرد و ببین جاش تو کدوم دسته‌ست. نقشه‌ی راه رو هم جلوی چشمت نگه دار تا بدونی الان کجای مسیری.

چه سیستمی لازم داری

خیالت راحت باشه: هک کردن سیستم گرون نمی‌خواد. اون تصویری که تو ذهنته از سیستم چند ده میلیونی، برای شروع اصلاً لازم نیست. این حداقل سیستمیه که راحت باهاش راه می‌افتی:

رم	**۸ گیگابایت.** چون کار روی ماشین مجازی انجام می‌شه و باید هم‌زمان دو تا سیستم‌عامل بالا باشه.
پردازنده	**Core i5 نسل ۸ یا بالاتر.**
حافظه	**SSD ۵۱۲ گیگابایت.** سرعتش مهم‌تر از حجمشه.
گرافیک	**انبورد کافیه.** کارت گرافیک مجزا لازم نیست.

این اعداد یعنی چی

این سطح، حد وسطه — نه حداقلِ به‌زور، نه سیستم رویایی. پایین‌تر از این هم می‌شه کار کرد، فقط همه‌چی کندتر پیش می‌ره و حوصله‌ت بیشتر سر می‌ره. بالاتر از این هم چیز جدیدی یاد نمی‌گیری، فقط سریع‌تر همون کارها رو می‌کنی. پس سیستمت رو بهونه نکن.

چرا ماشین مجازی

سیستم‌عامل هکری رو داخل یه ماشین مجازی بالا می‌آری، نه روی سیستم اصلیت. اینجوری سیستم اصلیت دست‌نخورده و امن می‌مونه، هر وقت خواستی محیط تمرینت رو پاک می‌کنی و از صفر می‌سازی، و اگه چیزی خراب شد فقط همون ماشین مجازی خراب شده. برای همینه که رم مهم‌ترین قطعه‌ی این لیسته.

سیستم‌عامل

توزیع‌های مخصوص امنیت، صدها ابزار رو از پیش‌نصب دارن. یعنی به‌جای اینکه هفته‌ها وقت بذاری برای نصب و کانفیگ تک‌تک ابزارها، همون روز اول یه محیط آماده داری و می‌ری سراغ یادگیری. برای هر مرحله یکی مناسبه:

Kali Linux

برای شروع

استانداردترین توزیع امنیتی دنیاست و بیشترین منبع آموزشی هم براش وجود داره — یعنی هر مشکلی بخوری، یکی قبلاً خورده و جوابشو نوشته. برای شروع همینو بگیر.

اوبونتو کاستوم

حرفه‌ای

وقتی جدی‌تر شدی، یه لینوکس تمیز برمی‌داری و فقط ابزارهای خودتو روش می‌چینی. اینجوری دقیقاً می‌دونی چی روی سیستمت هست و چرا. مرحله‌ی بعدیه، نه الان.

Parrot OS

جایگزین

اگه کالی روی سیستمت جواب نداد، این جایگزین خوبیه و تقریباً همون کارها رو می‌کنه. ولی برای شروع، پیشنهاد ما همون کالیه.

روی ویندوز یا مک چطور

لازم نیست ویندوز یا مکت رو پاک کنی. با VMware یا VirtualBox، این سیستم‌عامل‌ها روی هر کدومشون به‌عنوان ماشین مجازی اجرا می‌شن. سیستم اصلیت سر جاشه، محیط هکت هم کنارش بالا می‌آد.

۵۲ ابزار ضروری

این‌ها ابزارهاییه که تو کار واقعی مدام باهاشون سر و کار داری. لازم نیست همه رو یاد بگیری و قطعاً لازم نیست همه رو الان نصب کنی — این لیست مرجعته: وقتی رسیدی به یه موضوع، برگرد ببین ابزارش کدومه و تو کدوم دسته می‌افته.

۱ شبکه network

Nmap	اسکن شبکه و کشف پورت‌ها و سرویس‌های باز.
Wireshark	شنود و تحلیل ترافیک شبکه، بسته به بسته.
Masscan	اسکن پورت خیلی سریع روی رنج‌های بزرگ.
Netcat	چاقوی سوئیسی شبکه؛ اتصال، شنود و انتقال داده.
Tcpdump	ضبط ترافیک از خط فرمان، بدون رابط گرافیکی.
Nessus	اسکنر آسیب‌پذیری برای شبکه و سرورها.
OpenVAS	اسکنر آسیب‌پذیری متن‌باز، جایگزین رایگان Nessus.
Responder	جعل سرویس‌های شبکه‌ی ویندوز برای گرفتن هش.
Impacket	مجموعه اسکریپت پایتون برای کار با پروتکل‌های ویندوز.
Angry IP Scanner	اسکنر ساده و سریع IP برای دید اولیه از شبکه.

۲ وب web

Burp Suite	پروکسی و مهم‌ترین ابزار تست نفوذ وب.
OWASP ZAP	پروکسی و اسکنر وب متن‌باز، جایگزین رایگان برپ.
SQLmap	کشف و بهره‌برداری خودکار از تزریق SQL.
Nikto	اسکن سریع وب‌سرور برای مشکلات و فایل‌های شناخته‌شده.
ffuf	فاز کردن سریع مسیرها، پارامترها و ساب‌دامین‌ها.
Gobuster	پیدا کردن دایرکتوری و فایل‌های مخفی سایت.
Nuclei	اسکن آسیب‌پذیری با قالب‌های آماده و قابل نوشتن.
WPScan	اسکنر تخصصی وردپرس، افزونه‌ها و قالب‌ها.

XSStrike	کشف و تست پیشرفته‌ی آسیب‌پذیری XSS.
Wfuzz	فاز کردن هر بخشی از درخواست HTTP.
Dirsearch	جست‌وجوی مسیرهای پنهان با دیکشنری.
Arjun	پیدا کردن پارامترهای مخفی و مستندنشده‌ی وب.
Amass	نقشه‌برداری سطح حمله و کشف گسترده‌ی ساب‌دامین.
httpx	بررسی سریع زنده بودن و مشخصات هزاران هاست.

۳ وای‌فای wireless

Aircrack-ng	مجموعه‌ی استاندارد حمله و تحلیل شبکه‌های بی‌سیم.
Wifite	اتوماتیک‌کردن حملات وای‌فای با یک دستور.
Reaver	حمله به WPS روترها برای گرفتن پسورد.
Kismet	کشف و پایش شبکه‌های بی‌سیم به‌صورت غیرفعال.
Bettercap	حملات میان‌راهی روی شبکه‌ی سیمی و بی‌سیم.
hcxdumptool	گرفتن هش وای‌فای برای کرک آفلاین.

۴ پسورد و هش password & hash

Hashcat	سریع‌ترین کرکر هش با استفاده از قدرت گرافیک.
John the Ripper	کرکر کلاسیک هش با پشتیبانی از فرمت‌های متنوع.
Hydra	حمله‌ی بروت‌فورس به سرویس‌های لاگین.
Medusa	بروت‌فورس موازی و سریع روی سرویس‌های شبکه.
CeWL	ساخت دیکشنری اختصاصی از محتوای خود سایت هدف.
Crunch	تولید لیست پسورد با الگو و کاراکترهای دلخواه.

۵ بهره‌برداری exploitation

Metasploit	چارچوب اصلی بهره‌برداری با هزاران اکسپلویت آماده.
searchsploit	جست‌وجوی آفلاین در آرشیو اکسپلویت‌های عمومی.
msfvenom	ساخت پیلود سفارشی برای سیستم‌عامل‌های مختلف.

BeEF	بهره‌برداری از مرورگر قربانی بعد از اجرای اسکریپت.
Empire	پسا‌ـبهره‌برداری و کنترل سیستم‌های ویندوزی.

۶ موبایل mobile

MobSF	تحلیل خودکار امنیتی اپلیکیشن‌های اندروید و iOS.
Frida	دستکاری زنده‌ی رفتار اپلیکیشن در حین اجرا.
objection	تست اپ موبایل بدون نیاز به روت یا جیلبریک.
apktool	باز کردن و بازسازی فایل APK برای بررسی کد.

۷ شناسایی و OSINT recon & osint

theHarvester	جمع‌آوری ایمیل، دامنه و نام کارکنان از منابع باز.
Shodan	موتور جست‌وجوی دستگاه‌ها و سرویس‌های متصل به اینترنت.
Maltego	ترسیم گرافیکی ارتباط بین افراد، دامنه‌ها و زیرساخت.
subfinder	کشف سریع ساب‌دامین‌ها از منابع عمومی.
recon-ng	چارچوب شناسایی با ساختاری شبیه متاسپلویت.

۸ سیستم‌عامل پایه base os

Kali Linux	توزیع استاندارد تست نفوذ با ابزارهای از پیش‌نصب.
Parrot OS	توزیع امنیتی سبک‌تر، جایگزین کالی.

نقشه‌ی راه

این ابزارها بدون نقشه فقط یه لیستن. مسیر واقعی ترتیب داره و هر مرحله پیش‌نیاز مرحله‌ی بعدیه — اگه از وسط بپری، اون وسط گیر می‌کنی و فکر می‌کنی مشکل از استعدادته، درحالی‌که مشکل از ترتیبه:

۱

FOUNDATION

هکر صفر

ورود کامل به دنیای هک: لینوکس، وب، شبکه و مهم‌تر از همه ذهنیت هکرها. نقطه‌ی شروع همه‌چیز.

۲

CORE

نتورک پلاس

شبکه و TCP/IP رو از دید مهاجم می‌فهمی. بدون این، بقیه‌ی مسیر فقط حفظ کردن دستوره.

۳

ADVANCED

پایتون

از مصرف‌کننده‌ی ابزار تبدیل می‌شی به سازنده‌ی ابزار. اتوماسیون و اسکریپت‌نویسی امنیتی.

۴

CORE

بش‌اسکریپت و لینوکس

تسلط واقعی روی ترمینال و زنجیر کردن ابزارها به هم. جایی که کارها سریع می‌شن.

۵

ADVANCED

هنر هک

تکنیک‌های عمقی حمله و طرز فکر پشتشون. اینجا دیگه دنبال دستور نیستی، دنبال منطق آسیب‌پذیری.

۶

AI

تست نفوذ با AI

استفاده از هوش مصنوعی برای سرعت دادن به شناسایی، تحلیل و کشف آسیب‌پذیری.

۷

ADVANCED

OWASP Top 10

ده آسیب‌پذیری اصلی وب، عمیق و عملی. زبان مشترک همه‌ی تست نفوذکارهای دنیا.

۸

BUG BOUNTY

باگ‌بانتی

شکار باگ واقعی روی هدف‌های واقعی و رسیدن به درآمد از پلتفرم‌های جهانی.

سه قدم اول

نقشه رو دیدی. حالا این سه تا کار رو انجام بده تا از خوندن بیای بیرون و بیفتی تو مسیر:

STEP ONE

۱

محیطتو بساز

یه ماشین مجازی راه بنداز و کالی رو روش نصب کن. تا وقتی محیطت آماده نشده، بقیه‌ی کارها روی کاغذ می‌مونه.

STEP TWO

۲

اولین ابزار رو اجرا کن

برو سراغ Nmap و یه اسکن ساده بگیر. ببین خروجی چی می‌گه و سعی کن بفهمی هر خطش یعنی چی.

STEP THREE

۳

روی یه محیط قانونی تمرین کن

برو سراغ یه لابراتوار آنلاین که برای همین کار ساخته شده و اولین تمرین واقعیتو انجام بده.

چقدر طول می‌کشه

با تمرین و تکرار، حدود ۶ ماه طول می‌کشه تا به جایی برسی که مستقل کار کنی. اگه وقت کمتری داری، نهایتاً ۸ ماه. این عدد به ساعت مداومی که می‌ذاری بستگی داره، نه به استعدادت. رمزش تداومه — نصف ساعت هر روز، از هشت ساعت آخر هفته جلوتره.

کجا تمرین کنی

خوندن به‌تنهایی کافی نیست؛ باید دستت بره تو کار و خطا بخوری تا یاد بگیری. ولی نه روی سایت مردم — اون کار تمرین نیست، جرمه. برای تمرین، محیط‌هایی هست که دقیقاً برای همین ساخته شدن:

PortSwigger Web Security Academy

بهترین محیط تمرین رایگان دنیا، ساخته‌ی همون تیمی که Burp Suite رو ساخته. صدها لاب از ساده تا حرفه‌ای، بدون نیاز به هیچ نصبی، مستقیم تو مرورگر. اولین XSS واقعیتو همین‌جا می‌زنی.

TryHackMe

جایگزین مبتدی‌پسند با مسیرهای هدایت‌شده. دستت رو می‌گیره و قدم‌به‌قدم جلو می‌بره، مناسب وقتی که هنوز نمی‌دونی از کجا باید شروع کنی.

قانون طلایی

هیچ‌وقت روی سایتی که مال خودت نیست تمرین نکن. هک بدون اجازه جرمه — مهم نیست چقدر بلدی، مهم نیست نیتت چی بوده. همیشه روی محیط قانونی تمرین کن.

قدم بعدی

حالا از کجا شروع کنی؟

این کیت مسیر رو نشونت داد: چی لازم داری، با چه ابزارهایی سر و کار داری، و به چه ترتیبی باید جلو بری. ولی دونستن مسیر با تونستنِ طی کردنش فرق داره. برای اینکه واقعاً طی‌اش کنی، باید پیوسته و از نقطه‌ی درست شروع کنی — نه تیکه‌تیکه از این ویدیو و اون مقاله.

مسترکلاس هک و امنیت

کل نقشه‌ی راه، از هکر صفر تا باگ‌بانتی، پیوسته و به‌ترتیب، یک‌جا. همون مسیری که این کیت نشونت داد.

و وقتی خواستی به درآمد برسی، بخش OWASP و باگ‌بانتی مسیرتو کامل می‌کنه.

codacker.ir/product/hs-masterclass

هک به ابزار نیست، به طرز فکره.