درس ۷ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

Kali Linux: هدف، اخلاق، قانون و نسخه‌ها

دوره کامل · Arch 2026.11 · Kali 2026.3 (Nov 2026)



در درس هفتم چه یاد می‌گیرید

- Kali برای چیست — و برای چه نیست
- تاریخچه کوتاه: از BackTrack تا Kali 2026.3
- قانون: دسترسی بدون اجازه جرم است
- متخصصان چگونه کار می‌کنند: اجازه، محدوده، قوانین تعامل
- راه‌های قانونی تمرین: لابراتوارها، CTF، برنامه‌های bug bounty
- نسخه‌های Kali: نصب‌کننده، live، VM، WSL، کلاود، ARM، NetHunter، Purple
- انتخاب نسخه درست برای لابراتوار شما

Kali برای چیست — و برای چه نیست

Kali نیست	Kali برای
یک desktop روزانه یا اولین لینوکس مبتدی	تست نفوذ و ارزیابی آسیب‌پذیری مجاز
ابزاری برای دسترسی به حساب‌ها یا دستگاه‌های دیگران	یادگیری امنیت در لابراتوار خودتان، CTF، تأییدیه‌ها
به طور پیش‌فرض ناشناس (Tails نیست)	فارنزیک دیجیتال (حالت forensic به دیسک‌ها دست نمی‌زند)
جایگزین patch کردن و دفاع خوب	کار دفاعی: Kali Purple (SOC، IDS، SIEM)
ابزار «هک» که بدون مهارت و اجازه کار کند	محققان، دانشجویان، تیم‌های red، blue و purple

تاریخچه کوتاه Kali

رویداد	سال
BackTrack (بر اساس Ubuntu/Slackware) — نسخه قبلی	2006–2012
Kali Linux 1.0 توسط Offensive Security، بازسازی‌شده روی Debian	2013
Kali Rolling: آپدیت پیوسته از Debian testing	2016
Xfce desktop پیش‌فرض شد؛ حالت 'Undercover'	2019.4
کاربر پیش‌فرض غیر root (kali)؛ یک ایمِج نصب‌کننده	2020.1
Kali Purple (دفاعی) معرفی شد؛ NetHunter گسترش یافت	2022–2023
Oct 2026: Linux 7.1، اسکریپت‌های ساخت تازه، ۶ ابزار نو، آپدیت desktop	2026.3

قانون: دسترسی بدون اجازه جرم است

قانون نمونه	مکان
Computer Fraud and Abuse Act (CFAA)؛ قوانین جرایم کمپیوتری ایالتی	ایالات متحده
Computer Misuse Act 1990	بریتانیا
دستورالعمل حملات علیه سیستم‌های معلوماتی؛ قوانین ملی	اتحادیه اروپا
قوانین جزایی و جرایم سایبری ملی — قانون کشور خود را بررسی کنید	افغانستان و منطقه
اسکن، حدس رمز یا رهگیری ترافیک بدون اجازه می‌تواند غیرقانونی باشد	همه جا
این معلومات عمومی است، نه مشوره حقوقی — برای وضعیت خود از وکیل بپرسید	یادداشت

متخصصان چگونه کار می‌کنند

چه چیزی دارد	بخش
امضاشده توسط مالک سیستم (نه فقط یک کارمند)؛ چه کسی، چه چیزی، چه وقت	اجازه کتبی
دقیقاً کدام IP ها، دامنه‌ها و برنامه‌ها — و چه چیزی خارج از محدوده است	محدوده
تکنیک‌های مجاز، ساعات آزمایش، بدون DoS، مدیریت دیتا، شرایط توقف	قوانین تعامل
تماس اضطراری اگر چیزی خراب شد؛ گزارش فوری یافته‌های حیاتی	تماس‌ها
شواهد را رمزگذاری کنید، دیتای شخصی را کم کنید، بعد از کار حذف کنید	مدیریت دیتا
یافته‌ها، خطر، شواهد و راه اصلاح — محصول واقعی یک آزمایش	گزارش

راه‌های قانونی تمرین

گزینه	مثال‌ها
لابراتوار خودتان	Kali + VM های عمداً آسیب‌پذیر روی شبکه host-only (درس ۱۱)
برنامه‌های آسیب‌پذیر	DVWA، OWASP Juice Shop، WebGoat، Metasploitable 2/3
لابراتوارهای آنلاین	TryHackMe، Hack The Box، PortSwigger Web Security Academy، OffSec Proving Grounds
مسابقات CTF	picoCTF (مبتدیان)، تقویم CTFtime.org، CTF های مکتب و پوهنتون
برنامه‌های bug bounty	HackerOne، Bugcrowd، Intigriti — فقط داخل محدوده منتشرشده هر برنامه
آموزش رایگان	MyWebUniversity، OWASP، SANS Cyber Aces، مستندات فروشندگان

نسخه‌های Kali

بهترین برای	نسخه
نصب مستقیم یا VM سفارشی؛ انتخاب desktop و مجموعه ابزارها	نصب‌کننده (+ NetInstaller)
VirtualBox، VMware، QEMU/KVM، Hyper-V — سریع‌ترین شروع (kali/kali)	ایمِج‌های آماده VM
Kali را با خود ببرید؛ حالت forensic؛ persistence رمزگذاری‌شده اختیاری	Live USB (+ persistence)
Kali داخل Windows؛ Win-KeX برای desktop	WSL (Windows)
ایمِج‌های AWS/Azure؛ docker.io/kalilinux/kali-rolling	کلاود و کانتینر
Raspberry Pi و بوردهای دیگر	ARM
گوشی‌های Android (درس ۱۲)	NetHunter
نسخه لابراتوار دفاعی SOC / (درس ۱۱)	Kali Purple

خلاصه و کارخانگی

- Kali: آزمایش مجاز، یادگیری، فارنزیک، دفاع — نه desktop روزانه
- BackTrack، Kali (2013)، rolling (2016)، غیر root (2020)، 2026.3
- دسترسی بدون اجازه جرم است (CFAA، Computer Misuse Act، قوانین محلی)
- متخصصان: اجازه کتبی، محدوده، قوانین تعامل، گزارش
- تمرین قانونی: لابراتوار خودتان، DVWA/Juice Shop، TryHackMe/HTB، CTF، bug bounty در محدوده
- کارخانگی: صفحه محدوده یک برنامه bug bounty را بخوانید؛ ایمِج Kali VM را دانلود کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید