درس ۱۲ از ۱۲

# Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

## NetHunter، کلاود، گزارش‌نویسی و قدم‌های بعدی شغلی امنیت

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



# در درس دوازدهم چه یاد می‌گیرید

- Kali NetHunter: نسخه‌های Rootless، Lite و کامل
- Kali در کلاود — و پالیسی‌های آزمایش فراهم‌کنندگان کلاود
- نوشتن یک گزارش امنیتی حرفه‌ای
- افشای مسئولانه
- شغل‌های امنیت: red، blue، purple، GRC، فارنزیک
- تأییدیه‌ها و مسیرهای یادگیری رایگان
- مرور دوره و پروژه نهایی

# نسخه‌های Kali NetHunter

| نسخه | نیازمندی‌ها | چه می‌گیرید |
|---|---|---|
| NetHunter Rootless | هر گوشی Android، برنامه Termux (بدون root) | خط فرمان Kali در chroot؛ امن‌ترین شروع |
| NetHunter Lite | گوشی root شده (مثلاً Magisk) | ابزارهای بیشتر، برنامه NetHunter، بدون کرنل سفارشی |
| NetHunter (کامل) | دستگاه پشتیبانی‌شده + کرنل سفارشی NetHunter | ویژگی‌های USB/HID، Wi-Fi روی چیپ‌های پشتیبانی‌شده |
| ساعت هوشمند | ساعت‌های پشتیبانی‌شده (مثلاً TicWatch Pro 3) | Kali 2026.3 پشتیبانی wardriving اضافه کرد |
| قانون | همان قانون و اخلاق Kali روی لپ‌تاپ | فقط آزمایش مجاز و لابراتوار خودتان |

# Kali در کلاود

| موضوع | جزئیات |
| --- | --- |
| ایمِج‌ها | ایمِج‌های رسمی Kali روی AWS Marketplace و Microsoft Azure؛ ایمِج Docker |
| کاربردها | ارزیابی منابع کلاود خودتان، لابراتوار با انترنت سریع، کارهای موقت |
| پالیسی فراهم‌کنندگان | AWS، Azure و Google Cloud پالیسی تست نفوذ برای منابع خودتان منتشر می‌کنند |
| هرگز | منابع مشتریان دیگر یا زیرساخت فراهم‌کننده را اسکن نکنید |
| امنیت | فقط کلیدهای SSH، security group را به IP خودتان محدود کنید، بعد از کار متوقف کنید |
| هزینه | اینستَنس‌ها و دیسک‌ها را خاموش یا حذف کنید تا هزینه نشود |

# یک گزارش امنیتی حرفه‌ای

| بخش | محتوا |
| --- | --- |
| خلاصه اجرایی | ۱ صفحه، زبان ساده: خطر کلی، مسائل اصلی، توصیه‌های کلیدی |
| محدوده و روش | چه چیزی، چه وقت و چگونه آزمایش شد، و چه چیزی آزمایش نشد |
| یافته‌ها | عنوان، شدت (مثلاً CVSS)، سیستم‌های تحت تأثیر، توضیح، شواهد |
| تأثیر | یک مهاجم چه می‌تواند بکند — به زبان کسب‌وکار |
| اصلاح | قدم‌های مشخص اصلاح، اولویت، و چگونه اصلاح را تأیید کنیم |
| ضمیمه | خروجی ابزارها، جدول زمانی؛ از دیتای حساس در خود گزارش محافظت کنید |

# یک یافته نمونه (از لابراتوار ما)

```
Finding 1: Outdated FTP service with known vulnerabilities
Severity : Critical (CVSS v3.1 9.8)
Host     : target1 — 192.168.56.20, TCP/21
Evidence : nmap -sV reports 'vsftpd 2.3.4' (scan saved: lab/target1.xml)
Detected : Suricata alert ET SCAN at 21:14 (Kali Purple)
Impact   : Full remote compromise of the server is possible
Fix      : 1) Remove FTP or upgrade to a supported version
           2) Use SFTP instead of FTP (no clear-text passwords)
           3) Firewall: allow only required ports; monitor with IDS
Verify   : nmap -sV 192.168.56.20 shows port 21 closed
```

# افشای مسئولانه

| چه کنیم | قدم |
| --- | --- |
| متوقف شوید. بیشتر کشف نکنید یا به دیتا دسترسی نیابید | تصادفاً چیزی پیدا کردید؟ |
| security.txt (/.well-known/security.txt)، صفحه bug bounty، PSIRT فروشنده | تماس درست را پیدا کنید |
| قدم‌های واضح، تأثیر، حداقل شواهد؛ بدون پست عمومی | خصوصی گزارش دهید |
| معمولاً حدود ۹۰ روز، یا طبق توافق | برای اصلاح وقت بدهید |
| فقط بعد از اصلاح، با توافق مالک منتشر کنید | انتشار را هماهنگ کنید |
| پول نخواهید، تهدید نکنید، دیتای شخصی نگه ندارید | هرگز |

# مسیرهای شغلی امنیت

| مهارت‌هایی که بسازید | کار معمول | مسیر |
| --- | --- | --- |
| لینوکس، شبکه، وب، اسکریپت‌نویسی، گزارش‌نویسی | آزمایش مجاز شبکه، وب، کلاود | Red team / pentester |
| لاگ‌ها، SIEM، IDS، داخل Windows و Linux | نظارت، بررسی هشدارها، پاسخ به حادثه | Blue team / تحلیلگر SOC |
| هر دو طرف؛ چارچوب ATT&CK | بهبود کشف با شبیه‌سازی حمله | Purple team |
| فایل سیستم‌ها، حافظه، chain of custody | بررسی حوادث، حفظ شواهد | فارنزیک دیجیتال / IR |
| چارچوب‌ها (NIST، ISO 27001، CIS)، خودکارسازی | پالیسی‌ها، خطر، سخت‌سازی، امنیت کلاود | GRC / مهندس امنیت |

# تأییدیه‌ها و یادگیری رایگان

| گزینه‌ها | سطح |
| --- | --- |
| CompTIA Linux+، Security+؛ LPI Linux Essentials؛ ISC2 Certified in Cybersecurity (CC) | پایه |
| eJPT، PNPT، OffSec OSCP (PEN-200 — از Kali استفاده می‌کند) | حمله عملی |
| CompTIA CySA+، Blue Team Level 1، SANS/GIAC (GCIH، GCIA) | دفاع |
| LFCS، RHCSA (دوره RHEL ما) | عمق لینوکس |
| اتاق‌های رایگان TryHackMe، picoCTF، OverTheWire، PortSwigger Academy، MyWebUniversity | تمرین رایگان |
| یک portfolio بسازید: گزارش‌های لابراتوار، اسکریپت‌ها روی GitHub (بدون هدف واقعی!) | نکته |

# مرور دوره و پروژه نهایی

- Arch: archinstall، pacman، امنیت AUR، snapshot ها، عیب‌یابی
- Kali: اخلاق و قانون، نصب، متاپکیج‌ها، گشت ابزارها، لابراتوار امن، Purple، NetHunter
- پروژه نهایی بخش ۱: Arch desktop با snapper + مستند کردن برنامه هفتگی
- پروژه نهایی بخش ۲: لابراتوار جدای Kali، یک چرخه purple team، یک گزارش حرفه‌ای
- دوره‌های بعدی: Solaris/OVM، سیستم‌عامل‌های موبایل، سرویس‌های وبی — و RHEL، Debian، Fedora
- یاد بگیرید — به شکل اخلاقی — و به دیگران انتقال دهید

# 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**