درس ۹ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

اصول Kali: kali-rolling، متاپکیج‌ها و kali-tweaks

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



در درس نهم چه یاد می‌گیرید

- مخازن و شاخه‌های Kali: kali-rolling، last-snapshot، experimental
- آپدیت امن Kali
- متاپکیج‌ها: core، headless، default، large، everything
- گروه‌های ابزار: kali-tools-web، forensics-، wireless- ...
- kali-tweaks: shell، متاپکیج‌ها، مخازن، مجازی‌سازی، سخت‌سازی
- پالیسی سرویس‌های شبکه Kali و کاربر غیر root
- پیدا کردن مستندات برای هر ابزار

مخازن و شاخه‌های Kali

```
kali@kali:~$ cat /etc/apt/sources.list
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
# kali-rolling        : default, continuously updated from Debian testing
# kali-last-snapshot  : the last quarterly release (2026.3) — more stable
# kali-experimental   : packages under test (not for daily use)
# kali-bleeding-edge  : built from upstream git (for testers)
kali@kali:~$ apt policy | grep -E 'kali-(rolling|last)' | head -3
# NEVER add Debian/Ubuntu repos to Kali — it breaks the system ("FrankenDebian")
```

آپدیت امن Kali

```
kali@kali:~$ sudo apt update
kali@kali:~$ apt list --upgradable | wc -l
kali@kali:~$ sudo apt full-upgrade -y           # Kali needs full-upgrade, not upgrade
kali@kali:~$ sudo apt autoremove --purge
kali@kali:~$ [ -f /var/run/reboot-required ] && echo 'reboot needed'
kali@kali:~$ grep VERSION= /etc/os-release
# VM? Take a snapshot before big upgrades; old VM (months)? update keyring first:
kali@kali:~$ sudo wget https://archive.kali.org/archive-keyring.gpg \
      -O /usr/share/keyrings/kali-archive-keyring.gpg
```

متاپکیج‌ها: چه مقدار Kali می‌خواهید؟

اندازه	چه می‌گیرید	متاپکیج
کوچک	سیستم پایه Kali، بدون ابزار	kali-linux-core
متوسط	ابزارهای پیش‌فرض بدون GUI (سرور، WSL، کانتینر)	kali-linux-headless
~ 10 GB+	مجموعه استاندارد روی ایمِج‌های نصب‌کننده/VM	kali-linux-default
بزرگ	پیش‌فرض + ابزارهای بسیار بیشتر	kali-linux-large
بسیار بزرگ	هر ابزار بسته‌سازی‌شده	kali-linux-everything
کوچک	ده ابزار محبوب‌تر	kali-tools-top10

گروه‌های ابزار (kali-tools-*)

```
kali@kali:~$ apt-cache search --names-only '^kali-tools-' | sort
kali-tools-crypto-stego         kali-tools-information-gathering
kali-tools-database             kali-tools-passwords
kali-tools-forensics            kali-tools-reverse-engineering
kali-tools-fuzzing              kali-tools-sniffing-spoofing
kali-tools-hardware             kali-tools-social-engineering
kali-tools-identify             kali-tools-vulnerability
kali-tools-protect / respond / detect / recover   (Kali Purple, defensive)
kali-tools-web                  kali-tools-wireless
kali@kali:~$ apt show kali-tools-forensics | grep Depends | tr ',' '\n' | head
kali@kali:~$ sudo apt install -y kali-tools-forensics
```

kali-tweaks

چه کاری می‌کند	منو
نصب/حذف مجموعه ابزارها با checkbox	Metapackages
تغییر / mirror فعال کردن kali-experimental یا bleeding-edge (با احتیاط)	Network Repositories
Zsh (پیش‌فرض) یا Bash؛ prompt یک‌خطی یا دوخطی	Shell & Prompt
نصب ابزارهای guest (VirtualBox، VMware، QEMU/Spice)	Virtualization
پیش‌فرض‌های قوی SSH، حالت سازگاری گسترده برای پروتکول‌های قدیمی (لاپراتوار)	Hardening
تنظیمات کرنل، مثلاً پورت‌های ممتاز برای کاربران غیر root	Kernel / misc

سرویس‌ها، کاربر غیر root و Undercover

```
# Kali policy: network services are DISABLED by default and don't start at boot
kali@kali:~$ systemctl is-enabled ssh postgresql apache2 2>/dev/null
disabled
kali@kali:~$ sudo systemctl start postgresql        # start only when needed
kali@kali:~$ sudo systemctl enable --now ssh        # only if you really need it
# Non-root by default since 2020.1 — use sudo for admin tasks
kali@kali:~$ id ; sudo -l | tail -2
kali@kali:~$ sudo apt install -y kali-root-login     # not recommended
# Undercover mode: Windows-like look in public places
kali@kali:~$ kali-undercover
```

مستندات برای هر ابزار

چگونه	منبع
man nmap ; man -k password	صفحه‌های man
tool --help یا tool -h	کمک داخلی
هر ابزار بسته‌سازی‌شده: توضیح، بسته‌ها، فرمان‌ها، مثال‌ها	kali.org/tools
نصب، عیب‌یابی، پالیسی‌ها، NetHunter، Purple	kali.org/docs
README، مثال‌ها و changelog ها روی سیستم شما	/usr/share/doc/<pkg>
مستندات رسمی (مثلاً nmap.org/book، راهنماهای OWASP)	پروژه‌های upstream

خلاصه و کارخانگی

- kali-rolling (پیش‌فرض) یا kali-last-snapshot؛ هرگز مخازن Debian/Ubuntu اضافه نکنید
- آپدیت با apt full-upgrade؛ اول snapshot؛ روی VM های قدیمی keyring را تازه کنید
- متاپکیج‌ها: core < headless < default < large < everything؛ top10
- گروه‌های kali-tools–* بر اساس کار؛ گروه‌های Purple برای دفاع
- kali-tweaks: متاپکیج‌ها، مخازن، shell، مجازی‌سازی، سخت‌سازی
- کارخانگی: kali-tweaks را اجرا کنید؛ kali-tools-forensics را نصب کنید؛ kali.org/tools را برای ۳ ابزار بخوانید

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