دوره کامل · ۱۲ درس

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

archinstall، pacman، AUR،
ابزارهای Kali و لابراتوار امن

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



درس ۱ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

Arch و Kali: نسخه‌های rolling، فلسفه و کاربرد هر کدام

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



در درس اول چه یاد می‌گیرید

- نسخه rolling در مقابل نسخه ثابت
- Arch Linux: Arch Way، سادگی و کنترول کاربر
- Kali Linux: یک جعبه‌ابزار امنیتی بر اساس Debian testing
- هر کدام کجا مناسب است — و کجا نیست
- اخلاق و قانون آزمایش امنیت
- پلان دوره و لابراتوار

Rolling در مقابل نسخه ثابت

	ثابت (Debian، Ubuntu LTS، RHEL)	Rolling (Arch، Kali)
نسخه‌ها	نسخه‌های اصلی هر ۲ تا ۳ سال	نسخه بزرگ ندارد؛ بسته‌ها پیوسته آپدیت می‌شوند
جدیدترین نرم‌افزار	در زمان انتشار ثابت، فقط اصلاحات امنیتی	چند روز یا هفته بعد از upstream
ارتقا	ارتقاهای بزرگ نسخه	کوچک و مکرر (pacman -Syu / apt full-upgrade)
خطر	بسیار پایدار، نرم‌افزار قدیمی‌تر	گاهی خرابی؛ اخبار را بخوانید
رسانه نصب	ایمِج‌های نسخه نقطه‌ای	snapshot ماهانه ISO (Arch)، فصلی (Kali)
بهترین برای	سرورها، سازمان‌ها، پایداری طولانی‌مدت	علاقه‌مندان، developer ها، لابراتوارها، جعبه‌ابزارهای خاص

Arch Linux در یک نگاه

Arch Linux	مورد
۲۰۰۲، Judd Vinet؛ اداره توسط جامعه، رهبر انتخابی	شروع
سادگی، مدرن بودن، عمل‌گرایی، محوریت کاربر، تطبیق‌پذیری	Arch Way
2026.11.01 — Linux 7.2.11، systemd 262.1، Archinstall 4.5	ISO فعلی
pacman + مخازن رسمی (core، extra، multilib) + AUR	بسته‌ها
Arch Wiki — مفید برای هر توزیع لینوکس	مستندات
رسماً x86-64 (ARM از طریق پروژه جدای Arch Linux ARM)	معماری‌ها

Kali Linux در یک نگاه

Kali Linux	مورد
OffSec (Offensive Security)؛ جانشین BackTrack (2013)	ساخته
Debian testing ← شاخه 'kali-rolling'	پایه
Kali 2026.3 (Oct 2026): Linux 7.1، پیش‌فرض Xfce، KDE Plasma 6.7، GNOME	فعلی
تست نفوذ، تحقیق امنیتی، فارنزیک، مهندسی معکوس	هدف
بیش از ۶۰۰ ابزار در متاپکیج‌ها (kali-linux-default، large-، everything-)	ابزارها
VM، نصب مستقیم، live USB، WSL، کلاود، ARM، Android (NetHunter)	اجرا روی

هر کدام کجا مناسب است

Kali	Arch	استفاده
نه — desktop عمومی نیست	بله — اگر کنترول را دوست دارید	**desktop روزانه / لپ‌تاپ developer**
کمی	عالی	**یادگیری اینکه لینوکس واقعاً چگونه کار می‌کند**
نه	به ندرت (نسخه ثابت بهتر است)	**سرورهای تولید**
بله — استاندارد	ممکن (مخزن BlackArch)	**لابراتوار امنیت، CTF، تأییدیه‌ها**
بله (حالت بوت forensic)	—	**فارنزیک / پاسخ به حادثه**
نه	بله (Steam؛ SteamOS بر اساس Arch است)	**بازی**

اخلاق و قانون: قوانین نیمه Kali

چرا	قانون
دسترسی بدون اجازه در بیشتر کشورها جرم است	فقط سیستم خودتان یا با اجازه کتبی
آزمایش خارج از محدوده هم بدون اجازه است	داخل محدوده و زمان توافق‌شده
VM های عمداً آسیب‌پذیر، بدون کاربران واقعی	تمرین فقط در لابراتوار جدای خودتان
نیت خوب دفاع قانونی نیست	مکتب، کارفرما، ISP، Wi-Fi همسایه: نه بدون اجازه
محرمانگی و افشای مسئولانه	محافظت از دیتا؛ گزارش مسئولانه
هدف سیستم‌های امن‌تر برای همه است	دفاع را یاد بگیرید، نه فقط حمله

پلان دوره

نیمه Kali	درس‌ها	نیمه Arch	درس‌ها
هدف، اخلاق، قانون، نسخه‌ها	۷	نسخه‌های rolling و فلسفه	۱
نصب Kali: VM، USB، WSL	۸	نصب Arch (archinstall)	۲
kali-rolling، متاپکیج‌ها، tweaks	۹	pacman، مخازن، mirror ها، کلیدها	۳
گشتی در ابزارها (در لابراتوار شما)	۱۰	AUR، PKGBUILD، helper ها	۴
لابراتوار امن و Kali Purple	۱۱	اداره درست Arch	۵
NetHunter، گزارش‌نویسی، شغل‌ها	۱۲	خانواده Arch و عیب‌یابی	۶

لابراتوار دوره

استفاده	شبکه	سیستم	میزبان
درس‌های ۲ تا ۶	NAT، 10.0.0.51	Arch Linux (VM، UEFI)	arch1
درس‌های ۷ تا ۱۲	NAT + host-only 192.168.56.10	Kali Linux 2026.3 (VM)	kali
هدف تمرین (آفلاین)	host-only 192.168.56.20	VM آسیب‌پذیر (Metasploitable 2)	target1
تمرین وب	host-only 192.168.56.30	DVWA / Juice Shop (کانتینر)	target2
قبل از تغییرات snapshot	8 GB+ رم، 80 GB دیسک	VirtualBox / KVM / VMware	میزبان
sudo		student (Arch)، kali (Kali)	کاربران

خلاصه و کارخانگی

- Rolling = آپدیت پیوسته، جدیدترین نرم‌افزار، اخبار را بخوانید
- Arch: ساده، تحت کنترول کاربر، pacman + AUR، Arch Wiki
- Kali: جعبه‌ابزار امنیتی OffSec بر اساس Debian testing؛ 2026.3 فعلی
- Arch برای یادگیری/desktop؛ Kali برای کار امنیتی مجاز و لابراتوار
- اخلاق: سیستم خودتان یا اجازه کتبی، محدوده، لابراتوار جدا
- کارخانگی: Arch ISO و ایمِج Kali VM را دانلود کنید؛ شبکه host-only را بسازید

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

درس ۲ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

نصب Arch Linux با archinstall (و آنچه انجام می‌دهد)

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



در درس دوم چه یاد می‌گیرید

- دانلود و تأیید ISO ماهانه
- بوت محیط live: شبکه، زمان، کیبورد
- archinstall: دیسک‌ها، Btrfs، bootloader، کاربران، profile
- انتخاب کرنل‌ها، صدا، شبکه و بسته‌های اضافی
- بوت اول: آپدیت، سرویس‌ها، microcode، آمادگی AUR
- نصب دستی: pacstrap، genfstab، arch-chroot
- چه وقت دستی و چه وقت archinstall

دانلود و تأیید ISO

```
# From archlinux.org/download (or a mirror close to you)
$ ls
archlinux-2026.11.01-x86_64.iso  archlinux-2026.11.01-x86_64.iso.sig  sha256sums.txt
$ sha256sum -c sha256sums.txt --ignore-missing
archlinux-2026.11.01-x86_64.iso: OK
$ gpg --auto-key-locate clear,wkd -v --locate-external-key pierre@archlinux.org
$ gpg --verify archlinux-2026.11.01-x86_64.iso.sig
gpg: Good signature from "Pierre Schmitz <pierre@archlinux.org>"
# On an existing Arch system: pacman-key -v archlinux-...iso.sig
# Write to USB: dd bs=4M if=archlinux-...iso of=/dev/sdX status=progress oflag=sync
```

محیط Live

```
root@archiso ~ # ls /sys/firmware/efi/efivars >/dev/null && echo UEFI
UEFI
root@archiso ~ # loadkeys us                    # keyboard layout (e.g. de, fr)
root@archiso ~ # ip -br link                    # wired works automatically (DHCP)
root@archiso ~ # iwctl                          # Wi-Fi:
[iwd]# station wlan0 scan
[iwd]# station wlan0 connect "MyWiFi"
root@archiso ~ # ping -c3 archlinux.org
root@archiso ~ # timedatectl                     # NTP sync should be active
root@archiso ~ # archinstall
```

archinstall: انتخاب‌های کلیدی منو

مورد منو	انتخاب ما برای arch1
زبان Archinstall / Locales	English؛ کیبورد us؛ en_US.UTF-8 locale
Mirror ها و مخازن	mirror های کشور شما؛ 'multilib' را برای Steam/Wine فعال کنید
تنظیم دیسک	طرح Best-effort روی Btrfs → /dev/vda با subvolume + فشرده‌سازی
رمزگذاری دیسک	اختیاری: LUKS با passphrase (روی لپ‌تاپ توصیه می‌شود)
Swap	zram (سوآپ فشرده در RAM) — پیش‌فرض
Bootloader	systemd-boot (UEFI) — یا GRUB برای BIOS/ویژگی‌های پیشرفته
Hostname	arch1
رمز / root حساب کاربر	root قفل بماند؛ کاربر 'student' به عنوان superuser (sudo)

archinstall: Profile، کرنل‌ها و بیشتر

گزینه‌ها	مورد منو
Desktop (GNOME، KDE Plasma، Xfce، Hyprland، COSMIC ...)، Server، یا Minimal	Profile
متن‌باز (Intel/AMD/nouveau) یا ماژول‌های کرنل باز NVIDIA	درایور گرافیک
PipeWire (توصیه‌شده)	صدا
linux (جدیدترین) + linux-lts به عنوان پشتیبان	کرنل‌ها
NetworkManager (desktop) یا systemd-networkd (سرور)	تنظیم شبکه
vim git base-devel openssh man-db	بسته‌های اضافی
منطقه زمانی شما؛ هماهنگی خودکار زمان روشن	منطقه زمانی / NTP
user_configuration.json را برای نصب‌های تکرارپذیر ذخیره می‌کند	ذخیره تنظیمات

بوت اول

```
[student@arch1 ~]$ sudo pacman -Syu                # full system upgrade
[student@arch1 ~]$ systemctl --failed
[student@arch1 ~]$ sudo systemctl enable --now sshd   # Arch names it sshd
[student@arch1 ~]$ lscpu | grep 'Vendor ID'
[student@arch1 ~]$ pacman -Q intel-ucode amd-ucode 2>/dev/null   # CPU microcode
[student@arch1 ~]$ sudo pacman -S --needed base-devel git       # for the AUR (lesson 4)
[student@arch1 ~]$ sudo pacman -S pacman-contrib reflector man-db
[student@arch1 ~]$ sudo systemctl enable --now paccache.timer   # clean old packages
[student@arch1 ~]$ cat /etc/os-release | head -3
```

در زیر: نصب دستی

```
# What archinstall does, step by step (simplified)
# fdisk/parted: 1 GB EFI (vfat) + root
mkfs.fat -F32 /dev/vda1 ; mkfs.btrfs /dev/vda2
mount /dev/vda2 /mnt ; mount --mkdir /dev/vda1 /mnt/boot
pacstrap -K /mnt base linux linux-firmware intel-ucode vim networkmanager sudo
genfstab -U /mnt >> /mnt/etc/fstab
arch-chroot /mnt
  ln -sf /usr/share/zoneinfo/Asia/Kabul /etc/localtime ; hwclock --systohc
  sed -i 's/^#en_US.UTF-8/en_US.UTF-8/' /etc/locale.gen ; locale-gen
  echo arch1 > /etc/hostname ; mkinitcpio -P
  bootctl install    # + loader entries ;  useradd -m -G wheel student ; passwd student
  EDITOR=vim visudo  # uncomment: %wheel ALL=(ALL:ALL) ALL ; systemctl enable NetworkManager
```

دستی یا archinstall؟

چه وقت	انتخاب
یک Arch استاندارد و کارا در ۱۵ دقیقه می‌خواهید؛ تنظیمات JSON تکرارپذیر	archinstall
می‌خواهید هر قدم را یاد بگیرید، یا طرح‌های غیرعادی لازم دارید (LVM/RAID خاص، کلیدهای Secure Boot)	دستی
همان نتیجه: Arch ساده، بدون باقی‌مانده نصب‌کننده — سیستم مال شماست	هر دو
یک بار نصب دستی را در VM برای یادگیری انجام دهید، بعد روزانه از archinstall استفاده کنید	نکته
wiki.archlinux.org/title/Installation_guide	مرجع

خلاصه و کارخانگی

- تأیید: sha256sum + gpg --verify (یا pacman-key -v)
- live ISO: loadkeys، iwctl برای Wi-Fi، ping، timedatectl
- archinstall: Btrfs، systemd-boot، کاربر با sudo، profile، linux + linux-lts
- بوت اول: pacman -Syu، sshd، microcode، base-devel، paccache.timer
- دستی: pacstrap → genfstab → arch-chroot → mkinitcpio → bootloader
- کارخانگی: arch1 را با archinstall نصب کنید؛ JSON را ذخیره کنید؛ یک نصب دستی را در VM دوم امتحان 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

درس ۳ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

pacman: بسته‌ها، مخازن، mirror ها و کلیدها

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



در درس سوم چه یاد می‌گیرید

- عملیات pacman: S-، R-، Q-، F-، U- و گزینه‌های آن‌ها
- یک قانون: فقط ارتقای کامل (pacman -Syu)
- مخازن رسمی: core، extra، multilib (و testing)
- Mirror ها با reflector
- امضای بسته‌ها، archlinux-keyring و pacman-key
- فایل‌های .pacsave / .pacnew و pacdiff
- Cache، برگرداندن نسخه و Arch Linux Archive

عملیات pacman

معنی	فرمان
همگام‌سازی دیتابیس‌ها (y) و ارتقای همه چیز (u) — فرمان روزانه	pacman -Syu
نصب از مخازن (S = sync)	pacman -S nginx
جستجوی مخازن / معلومات بسته مخزن	pacman -Ss / -Si nginx
حذف + وابستگی‌های غیرضروری (s) + بکاپ تنظیمات (n)	pacman -Rns nginx
پرسش نصب‌شده‌ها: فهرست / معلومات / فایل‌ها	pacman -Q / -Qi / -Ql nginx
کدام بسته مالک این فایل است؟	pacman -Qo /usr/bin/ssh
جستجوی فایل در بسته‌های نصب‌نشده (بعد از pacman -Fy)	pacman -F bin/dig
نصب یک فایل بسته محلی یا دانلودشده	pacman -U ./pkg.pkg.tar.zst

pacman روزمره

```
[student@arch1 ~]$ sudo pacman -Syu
:: Synchronizing package databases...
 core / extra / multilib is up to date
:: Starting full system upgrade...
Packages (14) linux-7.2.11.arch1-1 mesa-1:26.2.6-1 systemd-262.1-1 ...
:: Proceed with installation? [Y/n] y
[student@arch1 ~]$ sudo pacman -S --needed htop btop fastfetch
[student@arch1 ~]$ pacman -Qe | wc -l           # explicitly installed
[student@arch1 ~]$ pacman -Qdtq                 # orphans (unneeded deps)
[student@arch1 ~]$ sudo pacman -Rns $(pacman -Qdtq)
[student@arch1 ~]$ pacman -Qkk openssh 2>&1 | tail -1   # verify files
```

یک قانون: ارتقای ناقص ممنوع

انجام ندهید	انجام دهید
sudo pacman -Sy بعد pacman -S somepkg	sudo pacman -Syu (هر چند روز)
نگه داشتن کتابخانه‌های اصلی برای ماه‌ها	sudo pacman -Syu somepkg (ارتقا + نصب)
ارتقای کورکورانه در زمان یک کار مهم	قبل از آپدیت‌های بزرگ archlinux.org/news را بخوانید
مخلوط کردن بسته‌ها از snapshot های مختلف	بعد از آپدیت kernel/systemd/glibc ری‌استارت
Arch فقط سیستم‌های کاملاً به‌روز را پشتیبانی می‌کند — ارتقای ناقص لینک کتابخانه‌ها را می‌شکند	چرا

مخازن و pacman.conf

```
[student@arch1 ~]$ grep -v '^#' /etc/pacman.conf | grep -v '^$'
[options]
HoldPkg     = pacman glibc
Architecture = auto
Color
ParallelDownloads = 5
SigLevel    = Required DatabaseOptional
[core]
Include = /etc/pacman.d/mirrorlist
[extra]
Include = /etc/pacman.d/mirrorlist
[multilib]                    # 32-bit libs: Steam, Wine (uncomment to enable)
Include = /etc/pacman.d/mirrorlist
# core-testing / extra-testing: for testers only
```

Mirror های سریع با reflector

```
[student@arch1 ~]$ sudo pacman -S reflector
[student@arch1 ~]$ sudo cp /etc/pacman.d/mirrorlist /etc/pacman.d/mirrorlist.bak
[student@arch1 ~]$ sudo reflector --country 'United States' --protocol https \
      --latest 20 --sort rate --save /etc/pacman.d/mirrorlist
[student@arch1 ~]$ head -5 /etc/pacman.d/mirrorlist
Server = https://mirror.example.edu/archlinux/$repo/os/$arch
[student@arch1 ~]$ sudo vim /etc/xdg/reflector/reflector.conf
[student@arch1 ~]$ sudo systemctl enable --now reflector.timer   # weekly refresh
[student@arch1 ~]$ sudo pacman -Syyu    # force-refresh databases after changing mirrors
```

امضای بسته‌ها و کلیدها

```
[student@arch1 ~]$ pacman -Qi archlinux-keyring | grep Version
[student@arch1 ~]$ sudo pacman-key --list-keys | grep -c pub
# Error: 'signature from ... is unknown trust' / 'invalid or corrupted package'
[student@arch1 ~]$ sudo pacman -Sy archlinux-keyring && sudo pacman -Su
# Long-offline machine? Update the keyring first, then the rest.
[student@arch1 ~]$ systemctl list-timers | grep archlinux-keyring   # automatic refresh
# Last resort — reinitialize:
[student@arch1 ~]$ sudo rm -r /etc/pacman.d/gnupg && sudo pacman-key --init \
      && sudo pacman-key --populate archlinux
```

فایل‌های .pacnew، Cache و برگرداندن نسخه

```
warning: /etc/pacman.conf installed as /etc/pacman.conf.pacnew
[student@arch1 ~]$ sudo DIFFPROG='vim -d' pacdiff        # merge new defaults

[student@arch1 ~]$ du -sh /var/cache/pacman/pkg
[student@arch1 ~]$ sudo paccache -rk2                    # keep 2 versions per package

# Downgrade a package that broke something
[student@arch1 ~]$ ls /var/cache/pacman/pkg/ | grep mesa
[student@arch1 ~]$ sudo pacman -U /var/cache/pacman/pkg/mesa-1:26.2.5-1-x86_64.pkg.tar.zst
# Not in cache? archive.archlinux.org/packages/m/mesa/
# Then report the bug and upgrade again when it is fixed
```

خلاصه و کارخانگی

- S- نصب، R- حذف، Q- پرسش، F- فایل‌ها، U- فایل محلی
- همیشه ارتقای کامل: pacman -Syu (هرگز S- + Sy-)
- pacman.conf: ParallelDownloads، Color؛ multilib ،extra ،core
- reflector + reflector.timer برای mirror های سریع
- خطاهای keyring: اول pacman -Sy archlinux-keyring
- کارخانگی: multilib را فعال کنید، reflector را اجرا کنید، orphan ها را پیدا کنید، یک pacnew. را با pacdiff ادغام 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

درس ۴ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

AUR: PKGBUILD، makepkg، helper ها و امنیت

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



در درس چهارم چه یاد می‌گیرید

- AUR چیست — و چه نیست
- خواندن یک PKGBUILD: چه چیزی را بررسی کنیم
- ساختن دستی با git + makepkg
- AUR helper ها: yay و paru
- آپدیت امن بسته‌های AUR
- حوادث واقعی بدافزار AUR و چگونه از خود محافظت کنیم
- نوشتن PKGBUILD خودتان

AUR در یک نگاه

جزئیات	مورد
PKGBUILD های ارسالی جامعه (دستور ساخت)، نه بسته‌های باینری	چیست
aur.archlinux.org — جستجو، کامنت‌ها، رأی‌ها، نگهدارنده، آخرین آپدیت	کجا
هر کسی آپلود می‌کند؛ Arch بدها را حذف می‌کند؛ بدون بازبینی قبلی	چه کسی
Arch پشتیبانی نمی‌کند: شما مسئول آنچه می‌سازید هستید	پشتیبانی
رأی زیاد، نگهدارنده فعال، آپدیت اخیر، منبع از upstream واقعی	نشانه‌های خوب
Google Chrome، VS Code (باینری)، Spotify، نسخه‌های توسعه git- زیاد	محبوب

خواندن یک PKGBUILD

```
pkgname=hello-mwu
pkgver=1.0
pkgrel=1
pkgdesc='Friendly greeting from MyWebUniversity'
arch=('any')
url='https://www.mywebuniversity.com'
license=('MIT')
depends=('bash')
source=("https://example.com/hello-$pkgver.tar.gz")   # <- real upstream?
sha256sums=('<sha256-of-the-tarball>')                 # <- not SKIP for releases
package() {
  install -Dm755 "$srcdir/hello.sh" "$pkgdir/usr/bin/hello-mwu"
}
# CHECK: source URLs, checksums, curl/wget in functions, *.install scripts
```

ساختن دستی: git + makepkg

```
[student@arch1 ~]$ sudo pacman -S --needed base-devel git
[student@arch1 ~]$ git clone https://aur.archlinux.org/yay-bin.git
[student@arch1 ~]$ cd yay-bin
[student@arch1 yay-bin]$ less PKGBUILD            # READ IT
[student@arch1 yay-bin]$ git log --oneline | head  # who changed what, recently?
[student@arch1 yay-bin]$ makepkg -si              # build, install deps (-s), install (-i)
==> Making package: yay-bin ...
==> Validating source files with sha256sums... Passed
==> Finished making: yay-bin ...
# Never run makepkg as root — it refuses to
```

AUR Helper ها: yay و paru

کار	yay	paru
نوشته‌شده با	Go	Rust
جستجوی مخازن + AUR	yay -Ss name	paru -Ss name
نصب	yay -S name	paru -S name
ارتقای همه (مخازن + AUR)	yay (= yay -Syu)	paru (= paru -Syu)
بازبینی diff های PKGBUILD	yay --diffmenu / editmenu	به طور پیش‌فرض diff نشان می‌دهد
پاک‌سازی	yay -Yc	paru -c
قانون	هرگز با sudo استفاده نکنید؛ باز هم هر PKGBUILD و diff را بخوانید	

آپدیت امن بسته‌های AUR

```
[student@arch1 ~]$ paru                              # repos first, then AUR
:: Looking for AUR upgrades...
 aur/google-chrome  141.0-1 -> 142.0-1
:: Review changes? [Y/n] y                          # diff of PKGBUILD shown
[student@arch1 ~]$ pacman -Qm                        # list foreign (AUR) packages
[student@arch1 ~]$ paru -Gc google-chrome            # read the AUR comments
# After big repo updates (e.g. Python, ICU, Qt) rebuild affected AUR packages:
[student@arch1 ~]$ paru -S --rebuild <package>
# Orphaned/abandoned on the AUR? Consider an official alternative or Flatpak
```

بدافزار AUR: چه اتفاقی افتاد و چگونه محافظت کنیم

جزئیات	رویداد / قانون
سه بسته AUR با trojan دسترسی از راه دور پیدا و حذف شد	جولای 2025
خبر Arch: حادثه فعال بسته‌های مخرب AUR	June 12, 2026
نام‌های جعلی '-bin'؛ منبع از سرور ناشناس	الگو
PKGBUILD، .install و git log را بخوانید؛ مخازن رسمی/Flatpak	محافظت
رأی، عمر و نگهدارنده را بررسی کنید؛ مواظب بسته‌های نو	محافظت
حذف بسته، تغییر رمزها/کلیدها، نصب دوباره	اگر آلوده شدید

نوشتن PKGBUILD خودتان

```
[student@arch1 ~]$ mkdir hello-mwu && cd hello-mwu
[student@arch1 hello-mwu]$ printf '#!/usr/bin/bash\necho Hello from MyWebUniversity\n' \
      > hello.sh
[student@arch1 hello-mwu]$ vim PKGBUILD   # source=('hello.sh'); package() {...}
[student@arch1 hello-mwu]$ updpkgsums      # fill in sha256sums (pacman-contrib)
[student@arch1 hello-mwu]$ namcap PKGBUILD # lint (pacman -S namcap)
[student@arch1 hello-mwu]$ makepkg -si
[student@arch1 hello-mwu]$ hello-mwu
Hello from MyWebUniversity
[student@arch1 hello-mwu]$ makepkg --printsrcinfo > .SRCINFO   # needed to publish
```

خلاصه و کارخانگی

- PKGBUILD = AUR های جامعه، پشتیبانی‌نشده، بدون بازبینی قبلی
- PKGBUILD، .install و git log را قبل از ساختن بخوانید
- git clone + makepkg -si؛ هرگز به عنوان root
- yay / paru: ارتقای مخازن + AUR؛ diff ها را بازبینی کنید؛ بدون sudo
- حوادث بدافزار (2025، Jun 2026): مخازن رسمی/Flatpak را ترجیح دهید، رأی‌ها را بررسی کنید
- کارخانگی: yay-bin یا paru-bin را دستی بسازید؛ hello-mwu را بنویسید و بسازید

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

درس ۵ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

اداره درست Arch: آپدیت‌ها، اخبار، snapshot ها و desktop ها

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



در درس پنجم چه یاد می‌گیرید

- یک برنامه نگهداری هفتگی
- اخبار Arch و مداخلات دستی
- snapshot های خودکار Btrfs با snapper + snap-pac
- بوت یک snapshot و برگشت
- desktop ها، display manager ها و Flatpak
- اصول امنیتی که Arch به شما می‌سپارد: فایروال، آپدیت‌ها، SSH
- بکاپ و نگه داشتن فهرست بسته‌ها

یک برنامه نگهداری هفتگی

#	قدم	فرمان
۱	اول اخبار را بخوانید	archlinux.org/news (یا لیست arch-announce / RSS)
۲	ارتقای کامل	sudo pacman -Syu (یا paru برای مخازن + AUR)
۳	ادغام تغییرات تنظیمات	sudo pacdiff
۴	بررسی مشکلات	systemctl --failed ; journalctl -b -p err
۵	پاک‌سازی	paccache -rk2 ; pacman -Qdtq | sudo pacman -Rns -
۶	ری‌استارت بعد از kernel/systemd/mesa	uname -r در مقابل pacman -Q linux
نکته	هفتگی ارتقا دهید، نه ماهانه	قدم‌های کوچک آسان‌تر از پرش‌های بزرگ اصلاح می‌شوند

اخبار Arch: مداخلات دستی (مثال‌هایی از 2026)

درس	خبر	تاریخ
امنیت: فوراً ارتقا دهید	php ≥ 8.5.12 / php-legacy ≥ 8.3.36 (RCE)	2026-10-21
امنیت: فوراً ارتقا دهید	ca-certificates-mozilla ≥ 3.131.1-1 (CA آسیب‌دیده)	2026-10-21
قدم‌ها را دنبال کنید	virtualbox-ext-vnc ≥ 7.2.12-2: مداخله دستی	2026-07-21
بسته‌های AUR را بازبینی کنید	حادثه فعال بسته‌های مخرب AUR	2026-06-12
مسیرها تغییر می‌کنند	varnish حالا vinyl-cache است	2026-05-25
قبل از هر Syu-	archlinux.org/news، RSS، arch-announce	چگونه

Snapshot های خودکار: snapper + snap-pac

```
[student@arch1 ~]$ findmnt -no FSTYPE /          # needs Btrfs root
btrfs
[student@arch1 ~]$ sudo pacman -S snapper snap-pac
[student@arch1 ~]$ sudo snapper -c root create-config /
[student@arch1 ~]$ sudo snapper -c root set-config TIMELINE_LIMIT_DAILY=7 \
      NUMBER_LIMIT=20
[student@arch1 ~]$ sudo systemctl enable --now snapper-timeline.timer \
      snapper-cleanup.timer
[student@arch1 ~]$ sudo pacman -S htop            # snap-pac makes pre/post snapshots
[student@arch1 ~]$ sudo snapper -c root list | tail -3
  42 | pre  |    | ... | pacman -S htop
  43 | post | 42 | ... | htop
```

بوت یک Snapshot و برگشت

```
# GRUB: sudo pacman -S grub-btrfs ; sudo systemctl enable --now grub-btrfsd
#   → 'Arch Linux snapshots' submenu in GRUB lets you boot a snapshot read-only
# systemd-boot / Limine: use limine-snapper-sync or boot from the ISO

# Undo only the changes of one pacman transaction (pre 42 → post 43):
[student@arch1 ~]$ sudo snapper -c root undochange 42..43

# Full rollback of / to snapshot 42 (then reboot):
[student@arch1 ~]$ sudo snapper -c root rollback 42
[student@arch1 ~]$ sudo reboot
# Note: /home is a separate subvolume — your files are not rolled back
```

Desktop ها، Display Manager ها و Flatpak

```
[student@arch1 ~]$ sudo pacman -S plasma-meta sddm konsole dolphin   # KDE Plasma 6.8
[student@arch1 ~]$ sudo systemctl enable sddm
# or GNOME:  sudo pacman -S gnome gdm && sudo systemctl enable gdm
[student@arch1 ~]$ sudo pacman -S pipewire pipewire-pulse wireplumber
[student@arch1 ~]$ sudo pacman -S noto-fonts noto-fonts-cjk noto-fonts-emoji \
      vazirmatn-fonts                    # Persian/Dari font
[student@arch1 ~]$ sudo pacman -S flatpak
[student@arch1 ~]$ flatpak install flathub org.libreoffice.LibreOffice
[student@arch1 ~]$ sudo pacman -S power-profiles-daemon bluez bluez-utils
[student@arch1 ~]$ sudo systemctl enable --now bluetooth
```

اصول امنیتی که Arch به شما می‌سپارد

```
# No firewall is enabled by default on Arch
[student@arch1 ~]$ sudo pacman -S ufw && sudo ufw default deny incoming
[student@arch1 ~]$ sudo ufw allow ssh && sudo systemctl enable --now ufw && sudo ufw enable
# SSH hardening
[student@arch1 ~]$ printf 'PermitRootLogin no\nPasswordAuthentication no\n' | \
      sudo tee /etc/ssh/sshd_config.d/10-hardening.conf
[student@arch1 ~]$ sudo systemctl restart sshd
# Security advisories
[student@arch1 ~]$ sudo pacman -S arch-audit && arch-audit   # known CVEs installed
# No automatic updates: you upgrade (weekly!) — never auto-upgrade a rolling system blindly
```

بکاپ و یک فهرست بسته

```
[student@arch1 ~]$ pacman -Qqen > ~/pkglist-repo.txt      # explicit, official repos
[student@arch1 ~]$ pacman -Qqem > ~/pkglist-aur.txt       # explicit, AUR/foreign
# Reinstall on a new machine:
[student@arch1 ~]$ sudo pacman -S --needed - < pkglist-repo.txt
[student@arch1 ~]$ paru -S --needed - < pkglist-aur.txt

# Snapshots are NOT backups — copy data to another disk or server:
[student@arch1 ~]$ rsync -aHAX --delete ~/ /mnt/backup/student/
[student@arch1 ~]$ sudo pacman -S borg     # deduplicated, encrypted backups
[student@arch1 ~]$ borg init -e repokey /mnt/backup/borg && borg create /mnt/backup/borg::{now} ~/
```

خلاصه و کارخانگی

- هفتگی: اخبار، pacman -Syu، pacdiff، بررسی، پاک‌سازی، ری‌استارت
- قبل از ارتقا archlinux.org/news را بخوانید (مداخلات دستی)
- snapper + snap-pac: snapshot های pre/post در هر اجرای pacman
- برگشت: بوت grub-btrfs، snapper undochange / rollback
- Arch به طور پیش‌فرض هیچ چیز را فعال نمی‌کند: desktop، فایروال، بلوتوث انتخاب شماست
- کارخانگی: snapper را روی arch1 تنظیم کنید؛ یک بسته را خراب و برگردانید؛ فهرست بسته‌ها را ذخیره 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

درس ۶ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

خانواده Arch و عیب‌یابی: EndeavourOS، CachyOS، SteamOS

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



در درس ششم چه یاد می‌گیرید

- توزیع‌های بر اساس Arch و تفاوت‌های آن‌ها
- EndeavourOS، CachyOS، Manjaro، SteamOS، Garuda
- روش عیب‌یابی برای یک نسخه rolling
- نجات با ISO: mount، arch-chroot، اصلاح
- خرابی‌های رایج: kernel/initramfs، bootloader، keyring، GPU
- کمک گرفتن: Arch Wiki، فورم‌ها، bug tracker
- مرور نیمه Arch

خانواده Arch

توزیع	چه اضافه می‌کند	مخازن Arch؟
EndeavourOS	نصب‌کننده Calamares، چند ابزار کمکی؛ «Arch با شروع دوستانه»	بله، مستقیم (+ مخزن کوچک خودش)
CachyOS	کارایی: کرنل‌های تنظیم‌شده، بسته‌های بهینه x86-64-v3/v4	بازسازی + مخازن خودش
Manjaro	مخازن تأخیری/آزمایش‌شده خودش، ابزارهای خودش (pamac، mhwd)	نه — شاخه‌های خودش
SteamOS 3	سیستم بازی Valve برای Steam Deck؛ تغییرناپذیر، آپدیت A/B	snapshot خودش از Arch
Garuda	Btrfs + snapshot پیش‌فرض، ابزارهای بازی، desktop های پرزرق‌وبرق	Arch + Chaotic-AUR
BlackArch	بیش از ۲٬۸۰۰ ابزار امنیتی به شکل مخزن روی Arch	مخزن افزودنی

روش عیب‌یابی برای نسخه‌های Rolling

```
# 1. What changed? Look at the last pacman transactions
[student@arch1 ~]$ grep -E 'upgraded|installed' /var/log/pacman.log | tail -20
# 2. Is it already known? Check archlinux.org/news and the forum
# 3. Read the logs
[student@arch1 ~]$ journalctl -b -p err ; journalctl -b -1 -p err   # this / last boot
[student@arch1 ~]$ sudo dmesg -T --level=err,warn
# 4. Isolate: other kernel (linux-lts)? new user? snapshot from before?
# 5. Fix: downgrade from cache, roll back snapshot, or apply the news steps
[student@arch1 ~]$ sudo pacman -U /var/cache/pacman/pkg/<pkg-previous-version>.pkg.tar.zst
# 6. Report upstream / Arch bug tracker if it is a real bug
```

نجات با ISO و arch-chroot

```
# Boot the Arch ISO (same or newer than the installed system)
root@archiso ~ # lsblk -f
root@archiso ~ # cryptsetup open /dev/vda2 root      # only if LUKS
root@archiso ~ # mount -o subvol=@ /dev/vda2 /mnt     # Btrfs root subvolume
root@archiso ~ # mount /dev/vda1 /mnt/boot
root@archiso ~ # arch-chroot /mnt
[root@archiso /]# pacman -Syu                          # finish an interrupted upgrade
[root@archiso /]# mkinitcpio -P                        # rebuild initramfs
[root@archiso /]# bootctl update   (or grub-mkconfig -o /boot/grub/grub.cfg)
[root@archiso /]# exit ; umount -R /mnt ; reboot
```

خرابی‌های رایج و اصلاح‌ها

علامت	دلیل احتمالی	اصلاح
Kernel panic / بدون init بعد از آپدیت	ارتقای قطع‌شده، initramfs خراب	ISO → arch-chroot → pacman -Syu → mkinitcpio -P
'unknown filesystem' / ماژول‌ها نیستند	کرنل بوت‌شده ≠ ماژول‌های نصب‌شده	بعد از ارتقای کرنل ری‌استارت؛ linux-lts نگه دارید
منوی بوت نیست / bootloader رفته	آپدیت firmware ورودی‌های EFI را ریست کرد	arch-chroot → bootctl install / grub-install
Invalid or corrupted package (PGP)	keyring قدیمی	pacman -Sy archlinux-keyring && pacman -Su
صفحه سیاه بعد از آپدیت درایور GPU	تغییر NVIDIA/Mesa (مثلاً 590 پشتیبانی Pascal را حذف کرد)	TTY (Ctrl+Alt+F3)، اخبار، nvidia-580xx (AUR) یا برگرداندن
دیسک پر	cache بسته‌ها، ژورنال‌ها، snapshot ها	paccache -rk1؛ journalctl --vacuum-size؛ snapper delete

کمک گرفتن به روش Arch

چگونه خوب بپرسیم	کجا
اول جستجو کنید — بیشتر جواب‌ها آنجا هستند (و روی توزیع‌های دیگر هم کار می‌کنند)	Arch Wiki
قوانین فورم را بخوانید؛ آنچه امتحان کردید را نشان دهید؛ خروجی متنی، نه عکس	فورم‌ها (bbs.archlinux.org)
journalctl -b | curl -F 'file=@-' https://0x0.st (یا paste.rs)	اشتراک لاگ‌ها
gitlab.archlinux.org — باگ‌های بسته‌سازی؛ upstream برای باگ‌های برنامه	Bug tracker
#archlinux روی Libera.Chat برای سؤالات سریع	Matrix / IRC
EndeavourOS، CachyOS و Manjaro فورم‌های خودشان را دارند — اول آنجا بپرسید	مشتقات

مرور نیمه Arch

مهارت‌های کلیدی	درس
rolling در مقابل ثابت؛ Arch Way؛ جای Arch و Kali؛ اخلاق	۱
تأیید ISO؛ archinstall (Btrfs، systemd-boot، profile)؛ قدم‌های نصب دستی	۲
pacman -S/-R/-Q/-F/-U؛ فقط ارتقای کامل؛ reflector؛ keyring؛ pacdiff؛ cache	۳
AUR: خواندن PKGBUILD؛ makepkg -si؛ yay/paru؛ آگاهی از بدافزار	۴
برنامه هفتگی؛ اخبار Arch؛ snapper + snap-pac؛ desktop؛ فایروال؛ بکاپ	۵
خانواده Arch؛ روش عیب‌یابی؛ نجات با ISO و arch-chroot؛ کمک گرفتن	۶

خلاصه و کارخانگی

- EndeavourOS ≈ Arch + نصب‌کننده؛ CachyOS = کارایی؛ Manjaro = مخازن خودش
- SteamOS 3 بر اساس Arch است؛ BlackArch ابزارهای امنیتی اضافه می‌کند
- روش: pacman.log، اخبار، لاگ‌ها، جدا کردن، اصلاح، گزارش
- نجات: ISO، mount، arch-chroot، bootloader / mkinitcpio -P / pacman -Syu
- خوب بپرسید: اول Wiki، خروجی نه عکس، فورم مشتق برای مشتقات
- کارخانگی: در یک VM با snapshot، arch1 initramfs را خراب کنید و از ISO نجات 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

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

درس ۸ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

نصب Kali: VM، نصب مستقیم، Live USB و WSL

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



در درس هشتم چه یاد می‌گیرید

- چرا VM برای یادگیری بهترین است
- دانلود و تأیید ایمِج‌های Kali
- وارد کردن VM آماده؛ قدم‌های امنیتی ورود اول
- شبکه VM: NAT + شبکه لابراتوار host-only
- نصب‌کننده: انتخاب desktop و ابزارها
- Live USB با persistence رمزگذاری‌شده
- Kali روی WSL و در Docker

Kali را برای یادگیری کجا اجرا کنیم

گزینه	مزایا	معایب
VM (توصیه‌شده)	جدا، snapshot، شبکه لابراتوار host-only، ریست آسان	رم لازم دارد (4 GB+ برای Kali)
Live USB	قابل حمل، بدون نصب، حالت forensic	کُندتر؛ persistence باید تنظیم شود
نصب مستقیم	دسترسی کامل سخت‌افزار (کارت Wi-Fi، GPU)	بدون snapshot؛ با استفاده روزانه مخلوط
WSL	ابزارهای CLI سریع روی Windows	دسترسی محدود به شبکه؛ نه برای Wi-Fi
کلاود	انترنت سریع، موقت	هزینه دارد؛ فراهم‌کنندگان پالیسی آزمایش دارند

دانلود و تأیید

```
# kali.org/get-kali — choose: Virtual Machines / Installer / Live / WSL / ARM
$ ls
kali-linux-2026.3-virtualbox-amd64.7z   SHA256SUMS   SHA256SUMS.gpg
$ wget -q -O - https://archive.kali.org/archive-key.asc | gpg --import
$ gpg --verify SHA256SUMS.gpg SHA256SUMS
gpg: Good signature from "Kali Linux Archive Automatic Signing Key ..."
$ sha256sum -c SHA256SUMS --ignore-missing
kali-linux-2026.3-virtualbox-amd64.7z: OK
$ 7z x kali-linux-2026.3-virtualbox-amd64.7z
# Download only from kali.org (or its official mirrors / torrents)
```

وارد کردن VM و ورود اول

```
# VirtualBox: Machine > Add > kali-linux-2026.3-virtualbox-amd64.vbox
# VMware: open the .vmx ; QEMU/KVM: import the .qcow2 in virt-manager
# Login: kali / kali  — change it NOW
kali@kali:~$ passwd
kali@kali:~$ sudo apt update && sudo apt full-upgrade -y
kali@kali:~$ sudo dpkg-reconfigure keyboard-configuration   # if needed
kali@kali:~$ sudo timedatectl set-timezone Asia/Kabul
kali@kali:~$ sudo systemctl disable --now ssh 2>/dev/null   # off unless needed
kali@kali:~$ cat /etc/os-release | grep VERSION
VERSION="2026.3"
# Take a VM snapshot: 'clean-2026.3'
```

شبکه VM برای یک لابراتوار امن

هدف	نوع	Adapter
انترنت برای آپدیت (در زمان تمرین قابل غیرفعال شدن)	NAT	Adapter 1
شبکه لابراتوار: Kali + هدف‌های عمداً آسیب‌پذیر	Host-only 192.168.56.0/24	Adapter 2
VM های آسیب‌پذیر هرگز نباید به شبکه خانه یا انترنت برسند	فقط Host-only	هدف‌ها
Kali (و هدف‌ها) را روی LAN واقعی شما می‌گذارد — نه برای تمرین	Bridged	پرهیز
eth0 = NAT (x.10.0.2)، eth1 = لابراتوار (192.168.56.10)	ip -br a ; ip route	بررسی
بعد بازگردانید — لابراتوار را پاک نگه می‌دارد	قبل از هر تمرین	Snapshot ها

نصب‌کننده Kali

صفحه	انتخاب
نوع نصب	Graphical install (بر اساس Debian Installer)
کاربر	نام کاربری و رمز قوی خودتان (بدون ورود root)
پارتیشن‌بندی	Guided — use entire disk؛ LVM رمزگذاری‌شده روی لپ‌تاپ توصیه می‌شود
Desktop	Xfce (پیش‌فرض)، GNOME، KDE Plasma، یا هیچ
ابزارها	top10، default، large، everything (متاپکیج‌ها، درس ۹)
Bootloader	GRUB روی دیسک اصلی
نکته	NetInstaller در زمان نصب بسته‌های فعلی را دانلود می‌کند

Live USB با Persistence رمزگذاری‌شده

```
# Write the live ISO (destroys the USB stick!)
$ sudo dd if=kali-linux-2026.3-live-amd64.iso of=/dev/sdX bs=4M status=progress conv=fsync
# Create a persistence partition in the free space
$ sudo fdisk /dev/sdX            # n, p, 3, <enter>, <enter>, w
$ sudo cryptsetup luksFormat /dev/sdX3
$ sudo cryptsetup open /dev/sdX3 my_usb
$ sudo mkfs.ext4 -L persistence /dev/mapper/my_usb
$ sudo mkdir -p /mnt/my_usb && sudo mount /dev/mapper/my_usb /mnt/my_usb
$ echo '/ union' | sudo tee /mnt/my_usb/persistence.conf
$ sudo umount /mnt/my_usb && sudo cryptsetup close my_usb
# Boot menu: 'Live USB Encrypted Persistence'  |  'Live (forensic mode)'
```

Kali روی WSL و در Docker

```
PS C:\> wsl --install -d kali-linux
PS C:\> wsl -d kali-linux
kali@DESKTOP:~$ sudo apt update && sudo apt full-upgrade -y
kali@DESKTOP:~$ sudo apt install -y kali-linux-default     # tools (large download)
kali@DESKTOP:~$ sudo apt install -y kali-win-kex && kex --win -s   # desktop

$ docker pull docker.io/kalilinux/kali-rolling
$ docker run --rm -it kalilinux/kali-rolling /bin/bash
root@1a2b3c:/# apt update && apt install -y kali-linux-headless
# Containers start minimal — install only the tools you need
```

خلاصه و کارخانگی

- VM برای یادگیری بهترین است: جدا، snapshot، لابراتوار host-only
- فقط از kali.org دانلود کنید؛ SHA256SUMS + gpg را تأیید کنید
- ورود اول: kali/kali را تغییر دهید، full-upgrade، snapshot
- دو adapter: NAT (آپدیت) + host-only (لابراتوار)؛ هدف‌ها فقط host-only
- نصب‌کننده: Xfce/GNOME/KDE + مجموعه ابزارها؛ live USB با persistence رمزگذاری‌شده؛ WSL؛ Docker
- کارخانگی: Kali VM را وارد کنید، رمز را تغییر دهید، شبکه host-only را تنظیم کنید، snapshot 'clean' بگیرید

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

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

درس ۱۰ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

گشتی در ابزارهای Kali: شناسایی، وب، رمزها، بی‌سیم و فارنزیک

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



در درس دهم چه یاد می‌گیرید

- مراحل یک ارزیابی مجاز
- شناسایی: Nmap روی شبکه لابراتوار شما
- اصول آزمایش ویب: Burp Suite، Nikto، Gobuster روی DVWA
- رمزها: چرا hash های قوی و رمزهای طولانی مهم هستند
- تحلیل ترافیک با Wireshark
- بی‌سیم: Kali چه چیزی را می‌تواند آزمایش کند — و محدودیت‌های قانونی
- فارنزیک: Autopsy و حالت بوت forensic

مراحل یک ارزیابی مجاز

ابزارهای نمونه	هدف	مرحله
اسناد — نه نرم‌افزار	اجازه کتبی، محدوده، قوانین	**۰. اجازه**
nmap، whatweb، theHarvester (OSINT)	پیدا کردن میزبان‌ها و سرویس‌ها در محدوده	**۱. شناسایی**
nikto، nuclei، OpenVAS/GVM	پیدا کردن ضعف‌ها	**۲. تحلیل آسیب‌پذیری**
Burp Suite، Metasploit (لابراتوار)	اثبات امن خطر، داخل قوانین	**۳. تأیید**
یادداشت‌ها، عکس صفحه، قالب گزارش	توضیح یافته‌ها و اصلاح‌ها	**۴. گزارش**
Kali Purple (درس ۱۱)	همان قدم‌ها نشان می‌دهد چه چیزی patch و نظارت شود	**دید مدافع**

شناسایی: Nmap (فقط لابراتوار)

```
kali@kali:~$ ip -br a | grep eth1            # confirm you are on the lab network
eth1  UP  192.168.56.10/24
kali@kali:~$ nmap -sn 192.168.56.0/24        # which lab hosts are up?
Nmap scan report for 192.168.56.20  Host is up.
Nmap scan report for 192.168.56.30  Host is up.
kali@kali:~$ nmap -sV -T3 192.168.56.20      # services and versions on target1
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1
80/tcp open  http    Apache httpd 2.2.8
kali@kali:~$ nmap -sV -oA ~/lab/target1 192.168.56.20   # save results for the report
```

اصول آزمایش وب (روی DVWA / Juice Shop)

درس مدافع	چه کاری می‌کند	ابزار
هرگز به ورودی کلاینت اعتماد نکنید	proxy برای دیدن و تغییر درخواست‌های مرورگر	Burp Suite (Community)
banner نسخه را پنهان/patch کنید	شناسایی فناوری‌ها و نسخه‌های وب	whatweb
فایل‌های پیش‌فرض را حذف، تنظیمات را سخت کنید	بررسی تنظیمات اشتباه رایج وب سرور	nikto
به URL های «مخفی» تکیه نکنید	پیدا کردن فولدرهای پنهان در برنامه لابراتوار	gobuster / ffuf
از parameterized query استفاده کنید	آزمایش SQL injection در لابراتوار	sqlmap
راهنمای کودنویسی امن	دسته‌های اصلی خطرهای وب	OWASP Top 10

رمزها و Hash ها (hash های آزمایشی خودتان)

```
# Create YOUR OWN test hashes to learn why password strength matters
kali@kali:~$ echo -n 'summer2026' | sha256sum
kali@kali:~$ mkpasswd -m yescrypt 'summer2026'     # modern Linux hash (slow on purpose)
$y$j9T$...
kali@kali:~$ hashid '<hash>'                       # identify a hash type
kali@kali:~$ ls /usr/share/wordlists/               # rockyou.txt.gz etc.
# Lesson for defenders:
#   short/common passwords fall to wordlists in seconds
#   long passphrases + slow hashes (yescrypt, bcrypt, Argon2) + MFA resist attacks
#   never store plain or fast-hashed (MD5/SHA1) passwords
```

تحلیل ترافیک با Wireshark

```
kali@kali:~$ sudo usermod -aG wireshark kali     # capture without root (log in again)
kali@kali:~$ wireshark &                          # GUI: capture on eth1 (lab)
kali@kali:~$ tshark -i eth1 -c 20 -f 'port 21'    # CLI capture of lab FTP
# Display filters:
#   ip.addr == 192.168.56.20      http.request      ftp      tls.handshake
# Lesson: FTP and plain HTTP send passwords in clear text — use SFTP/HTTPS
# Capture only on networks you own or are authorized to monitor
```

بی‌سیم: Kali چه چیزی را آزمایش می‌کند — و محدودیت‌ها

موضوع	جزئیات
سخت‌افزار	Wi-Fi USB adapter با پشتیبانی monitor mode (VM به USB passthrough نیاز دارد)
ابزارها	مجموعه aircrack-ng، kismet، wifite، bettercap
چه نشان می‌دهد	passphrase های ضعیف WPA2، نقص‌های WPS، access point های جعلی
درس مدافع	WPA3 یا WPA2 با passphrase طولانی؛ WPS را خاموش؛ firmware روتر را آپدیت کنید
محدودیت قانونی	فقط access point خودتان یا اجازه کتبی — هرگز همسایه، کافه، مکتب
همچنین غیرقانونی	jam کردن یا قطع کردن دستگاه‌های دیگران

فارنزیک: Autopsy و حالت Forensic

```
# Boot Kali live in 'forensic mode': no auto-mount, no swap, no disk writes
kali@kali:~$ sudo apt install -y kali-tools-forensics
kali@kali:~$ sudo dc3dd if=/dev/sdb hash=sha256 of=/cases/usb.img log=/cases/usb.log
kali@kali:~$ sha256sum /cases/usb.img            # verify the image matches the log
kali@kali:~$ autopsy                              # web UI: new case, add usb.img
kali@kali:~$ binwalk firmware.bin ; exiftool photo.jpg
# Work on the IMAGE, never the original evidence; keep a chain-of-custody record
```

خلاصه و کارخانگی

- مراحل: اجازه، شناسایی، تحلیل، تأیید، گزارش
- nmap -sn / -sV فقط روی 192.168.56.0/24؛ ذخیره با -oA
- ویب: Burp، whatweb، nikto، gobuster، sqlmap روی DVWA/Juice Shop
- رمزها: passphrase طولانی + hash کُند + MFA؛ Wireshark خطر متن آشکار را نشان می‌دهد
- بی‌سیم و capture فقط روی شبکه‌های خودتان؛ فارنزیک روی ایمِج‌ها
- کارخانگی: target1 را اسکن کنید، سرویس‌ها را فهرست کنید، و ۳ توصیه «چگونه اصلاح کنیم» بنویسید

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

درس ۱۱ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

ساختن لابراتوار تمرین امن و دفاع با Kali Purple

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



در درس یازدهم چه یاد می‌گیرید

- طراحی لابراتوار: جداسازی، هدف‌ها، snapshot ها
- ساختن شبکه host-only
- هدف‌های تمرینی: Metasploitable، DVWA، Juice Shop در کانتینر
- قوانین امنیت لابراتوار و یک دفترچه لابراتوار
- Kali Purple: نسخه دفاعی
- کشف فعالیت لابراتوار با Suricata و لاگ‌ها
- Purple teaming: حمله، کشف، اصلاح، تکرار

طراحی لابراتوار

بخش	انتخاب ما	چرا
Hypervisor	VirtualBox یا KVM/virt-manager	رایگان، snapshot، شبکه‌های داخلی
شبکه	Host-only 192.168.56.0/24، بدون راه به اینترنت	هدف‌ها به LAN یا اینترنت شما نمی‌رسند
مهاجم	kali (192.168.56.10) + NAT برای آپدیت	در زمان تمرین می‌توانید NAT را خاموش کنید
هدف‌ها	target1 Metasploitable 2 (.20)، target2 کانتینرها (.30)	عمداً آسیب‌پذیر — هرگز باز نگذارید
مدافع	Kali Purple VM (.40) یا Suricata روی target2	ترافیک خودتان را از طرف آبی ببینید
Snapshot ها	'clean' روی هر VM	بعد از هر تمرین ریست کنید

ساختن شبکه Host-only

```
# VirtualBox
$ VBoxManage hostonlyif create                          # -> vboxnet0
$ VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask 255.255.255.0
$ VBoxManage modifyvm target1 --nic1 hostonly --hostonlyadapter1 vboxnet0
$ VBoxManage modifyvm kali --nic2 hostonly --hostonlyadapter2 vboxnet0

# KVM / libvirt: an isolated network (no <forward>)
$ cat lab.xml
<network><name>lab</name><ip address='192.168.56.1' netmask='255.255.255.0'/></network>
$ sudo virsh net-define lab.xml && sudo virsh net-start lab && sudo virsh net-autostart lab
# Verify from target1: ping 8.8.8.8 must FAIL
```

هدف‌های تمرینی

```
# target1: Metasploitable 2 (download from its official SourceForge page)
#   Import the VMDK, host-only NIC ONLY, login msfadmin/msfadmin (lab only!)

# target2: vulnerable web apps in containers (on an isolated VM)
student@target2:~$ docker run -d --name dvwa -p 8080:80 vulnerables/web-dvwa
student@target2:~$ docker run -d --name juice -p 3000:3000 bkimminich/juice-shop
student@target2:~$ docker ps --format '{{.Names}} {{.Ports}}'
dvwa   0.0.0.0:8080->80/tcp
juice  0.0.0.0:3000->3000/tcp
# Browse from Kali: http://192.168.56.30:8080  and  http://192.168.56.30:3000
```

قوانین امنیت لابراتوار

تمرین	قانون
فقط host-only؛ با آزمایش ping تأیید کنید	هدف‌ها هرگز روی انترنت
کاربران، رمزها و فایل‌های جعلی	بدون دیتای واقعی در لابراتوار
هر تمرین تمیز شروع می‌شود	قبل snapshot، بعد بازگردانی
تاریخ، هدف، فرمان‌ها، نتایج، آنچه یاد گرفتید	یک دفترچه لابراتوار نگه دارید
بدون shared folder یا clipboard به میزبان	نمونه‌های بدافزار فقط در VM جدا
هدف‌ها عمداً آسیب‌پذیر — و جدا — می‌مانند	Kali را آپدیت کنید، نه هدف‌ها را

Kali Purple: نسخه دفاعی

ابزارهای نمونه در Kali Purple	بخش (NIST CSF)
کشف دارایی‌ها و آسیب‌پذیری‌ها (nmap، GVM/OpenVAS)	Identify
سخت‌سازی، فایروال‌ها، تنظیمات امن	Protect
Suricata و Zeek (IDS شبکه)، Elastic/OpenSearch SIEM، Arkime	Detect
TheHive (مدیریت پرونده)، Cortex، playbook ها	Respond
بکاپ‌ها، بازگردانی و درس‌های آموخته	Recover
Kali Purple ISO، یا: sudo apt install kali-linux-purple / kali-tools-detect	نصب

فعالیت لابراتوار خودتان را با Suricata کشف کنید

```
purple@purple:~$ sudo apt install -y suricata
purple@purple:~$ sudo vim /etc/suricata/suricata.yaml    # af-packet: interface: eth1
purple@purple:~$ sudo suricata-update                   # download open rule sets
purple@purple:~$ sudo systemctl enable --now suricata
# From kali: nmap -sV 192.168.56.20   (your own lab scan)
purple@purple:~$ sudo tail -f /var/log/suricata/fast.log
[**] ET SCAN Suspicious inbound to mySQL port 3306 [**] 192.168.56.10 -> .20
purple@purple:~$ jq 'select(.event_type=="alert") | .alert.signature' \
      /var/log/suricata/eve.json | sort | uniq -c | sort -rn | head
```

Purple Teaming: حمله، کشف، اصلاح، تکرار

قدم	مثال در لابراتوار ما
۱. حمله (red)	target1 را با nmap -sV اسکن کنید؛ سرویس قدیمی FTP را پیدا کنید
۲. کشف (blue)	آیا Suricata هشدار داد؟ آیا لاگ target1 اتصال‌ها را نشان می‌دهد؟
۳. بهبود کشف	قوانین را تنظیم کنید، لاگ‌ها را به SIEM بفرستید
۴. اصلاح	روی یک کاپی target1: سرویس را خاموش/ارتقا دهید، قانون فایروال اضافه کنید
۵. تکرار	اسکن را دوباره اجرا کنید: سرویس رفته، هشدار هنوز کار می‌کند
۶. گزارش	بنویسید چه پیدا کردید، چه دیدید، و چه اصلاح کردید

خلاصه و کارخانگی

- شبکه host-only و جدا؛ تأیید کنید هدف‌ها به انترنت نمی‌رسند
- هدف‌ها: Metasploitable 2، DVWA، Juice Shop — عمداً آسیب‌پذیر، هرگز باز نیستند
- امنیت: بدون دیتای واقعی، snapshot، دفترچه لابراتوار، بدافزار فقط در VM جدا
- Kali Purple: NIST CSF — شناسایی، محافظت، کشف، پاسخ، بازیابی
- Suricata اسکن‌های لابراتوار شما را کشف می‌کند؛ purple teaming = حمله، کشف، اصلاح، تکرار
- کارخانگی: لابراتوار را بسازید، جداسازی را تأیید کنید، یک چرخه purple team اجرا و یک گزارش یک صفحه‌ای بنویسید

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

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