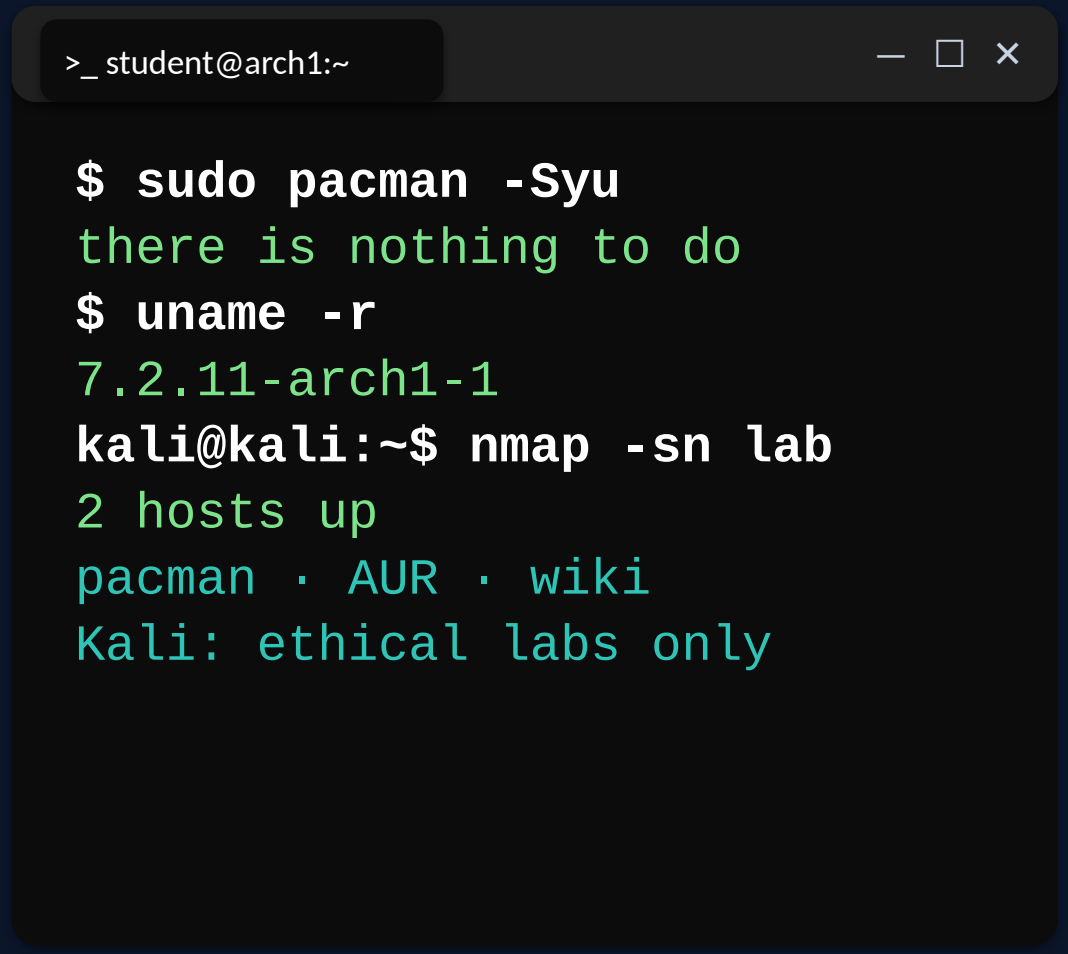


LESSON 4 OF 12

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

The AUR: PKGBUILD, makepkg, Helpers & Staying Safe

Full Course · Arch 2026.11 · Kali 2026.3 (Nov 2026)

What You Will Learn in Lesson 4

- What the AUR is — and what it is not
- Reading a PKGBUILD: what to check
- Building by hand with git + makepkg
- AUR helpers: yay and paru
- Updating AUR packages safely
- Real AUR malware incidents and how to protect yourself
- Writing your own PKGBUILD

The AUR at a Glance

Item	Details
What	Community-submitted PKGBUILDs (build recipes), not binary packages
Where	aur.archlinux.org — search, comments, votes, maintainer, last updated
Who	Any user can upload; Arch staff remove bad ones, but there is no pre-review
Support	Unsupported by Arch: you are responsible for what you build
Good signs	Many votes, active maintainer, recent update, source from the real upstream
Popular	Google Chrome, VS Code (binary), Spotify, many -git development versions

Reading a 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
```

Build by Hand: 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 Helpers: yay and paru

Task	yay	paru
Written in	Go	Rust
Search repos + AUR	yay -Ss name	paru -Ss name
Install	yay -S name	paru -S name
Upgrade all (repos + AUR)	yay (= yay -Syu)	paru (= paru -Syu)
Review PKGBUILD diffs	yay --diffmenu / editmenu	Shows diffs by default
Clean	yay -Yc	paru -c
Rule	Never use sudo with them; still READ every PKGBUILD and diff	

Updating AUR Packages Safely

```
[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
```

AUR Malware: What Happened and How to Protect Yourself

Event / Rule	Details
July 2025	Three AUR packages with malware (remote-access trojan) found and removed
June 12, 2026	Arch news: active AUR malicious packages incident — review recent commits
Pattern	Fake '-bin' or popular-sounding names; source points to an unknown server
Protect	Read PKGBUILD + .install + git log; prefer official repos and Flatpak
Protect	Check votes, age and maintainer; be wary of brand-new packages
If infected	Remove the package, rotate passwords/keys, reinstall from trusted media

Write Your Own PKGBUILD

```
[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
```

Summary and Homework

- AUR = community PKGBUILDs, unsupported, no pre-review
- Read PKGBUILD, .install and git log BEFORE building
- git clone + makepkg -si; never as root
- yay / paru: repo + AUR upgrades; review diffs; no sudo
- Malware incidents (2025, Jun 2026): prefer official repos/Flatpak, check votes
- Homework: build yay-bin or paru-bin by hand; write and build hello-mwu

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.