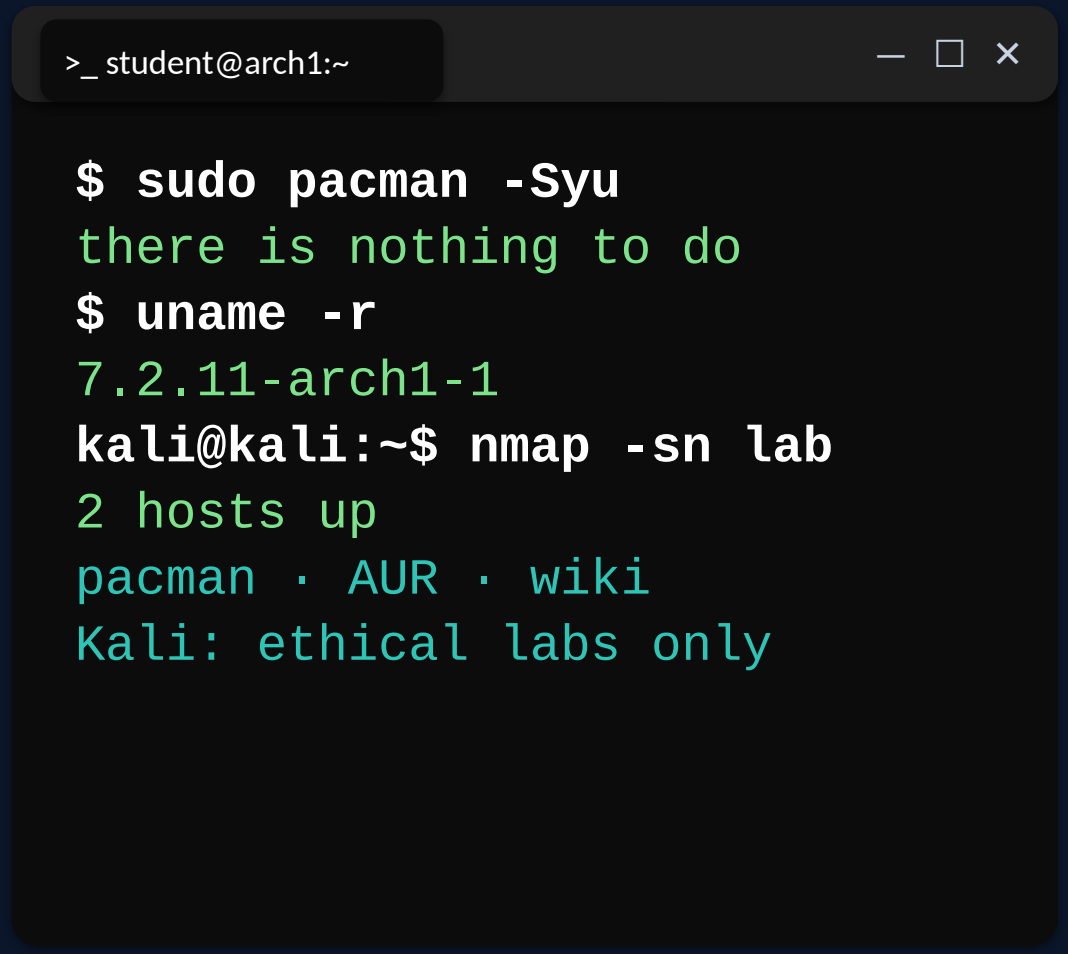


LESSON 12 OF 12

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

NetHunter, Cloud, Reporting & Security Career Next Steps

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

What You Will Learn in Lesson 12

- Kali NetHunter: Rootless, Lite and full editions
- Kali in the cloud — and cloud providers' testing policies
- Writing a professional security report
- Responsible disclosure
- Security careers: red, blue, purple, GRC, forensics
- Certifications and free learning paths
- Course review and final project

Kali NetHunter Editions

Edition	Requirements	What you get
NetHunter Rootless	Any Android phone, Termux app (no root)	Kali command line in a chroot; safest start
NetHunter Lite	Rooted phone (e.g. Magisk)	More tools, NetHunter app, still no custom kernel
NetHunter (full)	Supported device + custom NetHunter kernel	USB/HID attacks, Wi-Fi injection on supported chips
Smartwatch	Supported watches (e.g. TicWatch Pro 3)	Kali 2026.3 added wardriving support
Rule	Same law and ethics as Kali on a laptop	Authorized testing and your own lab only

Kali in the Cloud

Topic	Details
Images	Official Kali images on AWS Marketplace and Microsoft Azure; Docker image
Use cases	Assess YOUR cloud resources, labs with fast internet, temporary engagements
Provider policies	AWS, Azure and Google Cloud publish penetration-testing policies for your own resources
Never	Scan other customers' resources or the provider's infrastructure
Security	SSH keys only, restrict security groups to your IP, stop instances when done
Cost	Shut down or delete instances and disks to avoid charges

A Professional Security Report

Section	Contents
Executive summary	1 page, plain language: overall risk, top issues, key recommendations
Scope & methodology	What was tested, when, how, and what was NOT tested
Findings	Title, severity (e.g. CVSS), affected systems, description, evidence
Impact	What an attacker could do — in business terms
Remediation	Concrete steps to fix, priority, and how to verify the fix
Appendix	Tool output, timelines; protect sensitive data in the report itself

Example Finding (from our lab)

```
Finding 1: Outdated FTP service with known vulnerabilities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
```

Responsible Disclosure

Step	What to do
Found something by accident?	Stop. Do not explore further or access data
Find the right contact	security.txt (/.well-known/security.txt), bug bounty page, vendor PSIRT
Report privately	Clear steps, impact, minimal evidence; no public posts
Give time to fix	Commonly about 90 days, or as agreed
Coordinate publication	Publish only after a fix, with the owner's agreement
Never	Demand money, threaten, or keep personal data

Security Career Paths

Path	Typical work	Skills to build
Red team / pentester	Authorized testing of networks, web, cloud	Linux, networking, web, scripting, report writing
Blue team / SOC analyst	Monitoring, alert triage, incident response	Logs, SIEM, IDS, Windows & Linux internals
Purple team	Improve detections with attack simulations	Both sides; ATT&CK framework
Digital forensics / IR	Investigate incidents, preserve evidence	File systems, memory, chain of custody
GRC / security engineer	Policies, risk, hardening, cloud security	Frameworks (NIST, ISO 27001, CIS), automation

Certifications and Free Learning

Level	Options
Foundations	CompTIA Linux+, Security+; LPI Linux Essentials; ISC2 Certified in Cybersecurity (CC)
Hands-on offense	eJPT, PNPT, OffSec OSCP (PEN-200 — uses Kali)
Defense	CompTIA CySA+, Blue Team Level 1, SANS/GIAC (GCIH, GCIA)
Linux depth	LFCS, RHCSA (our RHEL course)
Free practice	TryHackMe free rooms, picoCTF, OverTheWire, PortSwigger Academy, MyWebUniversity
Tip	Build a portfolio: lab write-ups, reports, scripts on GitHub (no real targets!)

Course Review and Final Project

- Arch: archinstall, pacman, AUR safety, snapshots, troubleshooting
- Kali: ethics & law, install, metapackages, tools tour, safe lab, Purple, NetHunter
- Final project part 1: Arch desktop with snapper + weekly routine documented
- Final project part 2: isolated Kali lab, one purple-team cycle, one professional report
- Next courses: Solaris/OVM, mobile OSes, web-based services — and RHEL, Debian, Fedora
- Learn it — ethically — then pass it on

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.