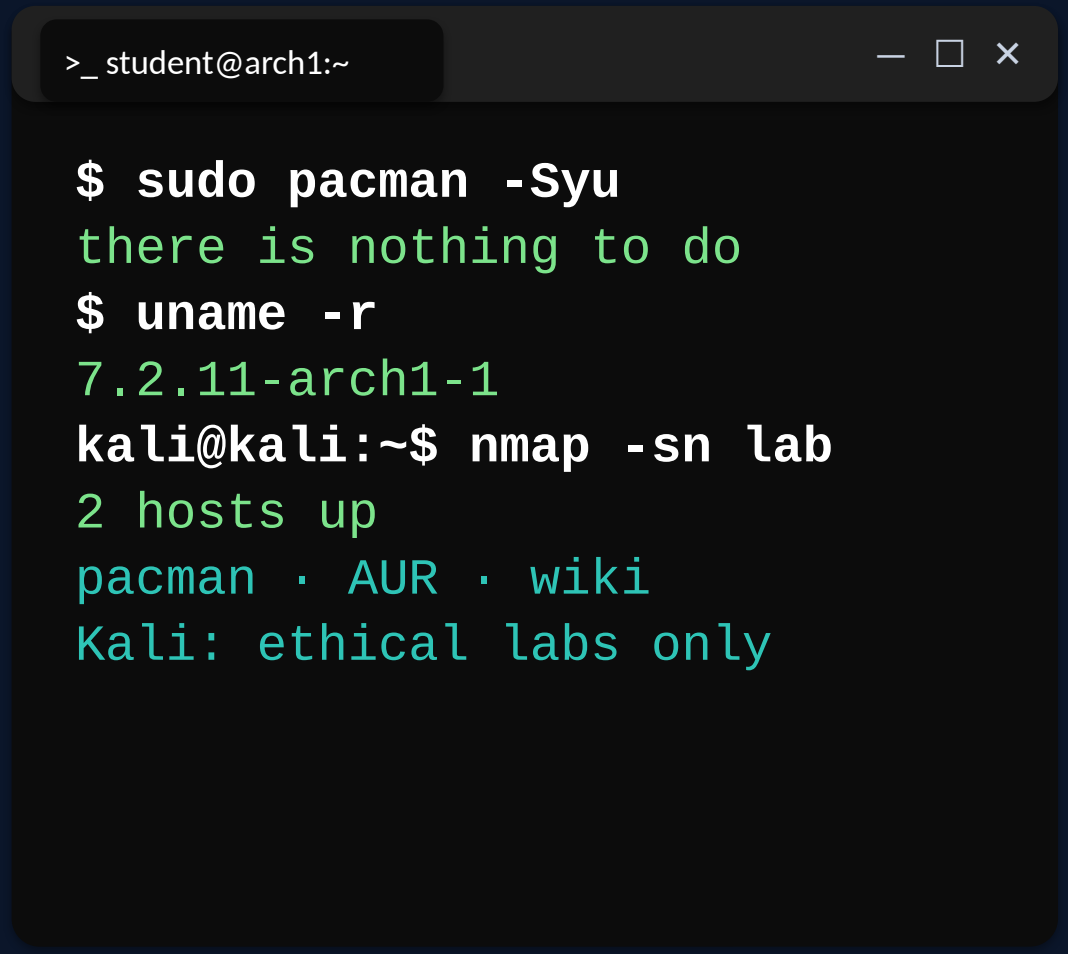


LESSON 11 OF 12

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

Building a Safe Practice Lab & Defending with Kali Purple

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

What You Will Learn in Lesson 11

- Lab design: isolation, targets, snapshots
- Building the host-only network
- Practice targets: Metasploitable, DVWA, Juice Shop in containers
- Lab safety rules and a lab notebook
- Kali Purple: the defensive edition
- Detecting lab activity with Suricata and logs
- Purple teaming: attack, detect, fix, repeat

Lab Design

Part	Our choice	Why
Hypervisor	VirtualBox or KVM/virt-manager	Free, snapshots, internal networks
Network	Host-only 192.168.56.0/24, no DHCP to the internet	Targets can't reach your LAN or the internet
Attacker	kali (192.168.56.10) + NAT for updates	Disable NAT during exercises if you like
Targets	target1 Metasploitable 2 (.20), target2 containers (.30)	Intentionally vulnerable — never expose
Defender	Kali Purple VM (.40) or Suricata on target2	See your own traffic from the blue side
Snapshots	'clean' on every VM	Reset after each exercise

Build the Host-only Network

```
# 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
```

Practice Targets

```
# 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
```

Lab Safety Rules

Rule	Practice
Targets never on the internet	Host-only only; verify with a ping test
No real data in the lab	Fake users, fake passwords, fake files
Snapshot before, restore after	Every exercise starts clean
Keep a lab notebook	Date, goal, commands, results, what you learned
Malware samples only in isolated VMs	No shared folders or clipboard to the host
Update Kali, not the targets	Targets stay vulnerable on purpose — and isolated

Kali Purple: The Defensive Edition

Area (NIST CSF)	Example tools in Kali Purple
Identify	Asset and vulnerability discovery (nmap, GVM/OpenVAS)
Protect	Hardening, firewalls, secure configurations
Detect	Suricata and Zeek (network IDS), Elastic/OpenSearch SIEM, Arkime
Respond	TheHive (case management), Cortex, playbooks
Recover	Backups, restore and lessons learned
Install	Kali Purple ISO, or: sudo apt install kali-linux-purple / kali-tools-detect

Detect Your Own Lab Activity with Suricata

```
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: Attack, Detect, Fix, Repeat

Step	Example in our lab
1. Attack (red)	Scan target1 with nmap -sV; find the old FTP service
2. Detect (blue)	Did Suricata alert? Does target1's log show the connections?
3. Improve detection	Tune rules, add log forwarding to the SIEM
4. Fix	On a copy of target1: disable/upgrade the service, add a firewall rule
5. Repeat	Re-run the scan: service gone, alert still fires
6. Report	Write what you found, what you saw, and what you fixed

Summary and Homework

- Host-only, isolated network; verify targets cannot reach the internet
- Targets: Metasploitable 2, DVWA, Juice Shop — deliberately vulnerable, never exposed
- Safety: no real data, snapshots, lab notebook, malware only in isolated VMs
- Kali Purple: NIST CSF — identify, protect, detect, respond, recover
- Suricata detects your own lab scans; purple teaming = attack, detect, fix, repeat
- Homework: build the lab, verify isolation, run one purple-team cycle and write a 1-page report

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.