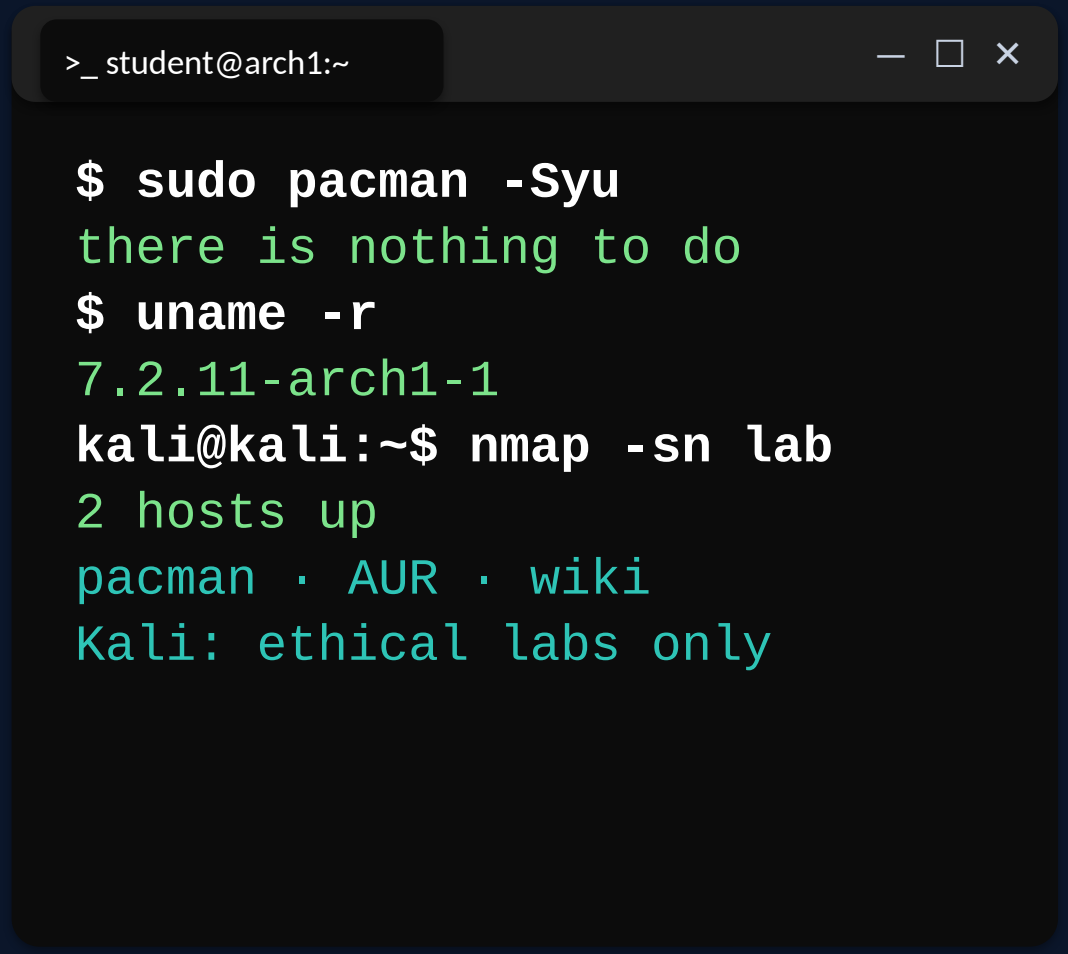


LESSON 10 OF 12

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

A Tour of Kali Tools: Recon, Web, Passwords, Wireless & Forensics

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

What You Will Learn in Lesson 10

- The phases of an authorized assessment
- Reconnaissance: Nmap on your lab network
- Web testing basics: Burp Suite, Nikto, Gobuster on DVWA
- Passwords: why strong hashes and long passwords matter
- Traffic analysis with Wireshark
- Wireless: what Kali can test — and the legal limits
- Forensics: Autopsy and the forensic boot mode

Phases of an Authorized Assessment

Phase	Goal	Example tools
0. Authorization	Written permission, scope, rules	Documents — not software
1. Reconnaissance	Find hosts and services in scope	nmap, whatweb, theHarvester (OSINT)
2. Vulnerability analysis	Find weaknesses	nikto, nuclei, OpenVAS/GVM
3. Verification	Prove risk safely, within the rules	Burp Suite, Metasploit (lab)
4. Reporting	Explain findings and fixes	Notes, screenshots, report template
Defender view	Same steps show what to patch and monitor	Kali Purple (lesson 11)

Reconnaissance: Nmap (lab only)

```
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
```

Web Testing Basics (on DVWA / Juice Shop)

Tool	What it does	Defender lesson
Burp Suite (Community)	Proxy to view and modify browser requests	Never trust input from the client
whatweb	Identify web technologies and versions	Hide/patch version banners
nikto	Check for common web server misconfigurations	Remove default files, harden configs
gobuster / ffuf	Find hidden directories in your lab app	Don't rely on 'secret' URLs
sqlmap	Test SQL injection in the lab	Use parameterized queries
OWASP Top 10	The main classes of web risks	Secure coding guidance

Passwords and Hashes (your own test hashes)

```
# 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
```

Traffic Analysis with 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
```

Wireless: What Kali Can Test — and the Limits

Topic	Details
Hardware	USB Wi-Fi adapter with monitor mode support (VMs need USB passthrough)
Tools	aircrack-ng suite, kismet, wifite, bettercap
What it shows	Weak WPA2 passphrases, WPS flaws, rogue access points
Defender lesson	WPA3 or WPA2 with a long passphrase; disable WPS; update router firmware
LEGAL LIMIT	Only YOUR OWN access point or written authorization — never neighbors, cafés, schools
Also illegal	Jamming or deauthenticating others' devices

Forensics: Autopsy and Forensic Mode

```
# 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
```

Summary and Homework

- Phases: authorization, recon, analysis, verification, report
- nmap -sn / -sV on 192.168.56.0/24 only; save with -oA
- Web: Burp, whatweb, nikto, gobuster, sqlmap on DVWA/Juice Shop
- Passwords: long passphrases + slow hashes + MFA; Wireshark shows clear-text risks
- Wireless & capture only on your own networks; forensics on images
- Homework: scan target1, list its services, and write 3 'how to fix' recommendations

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.