

Cybersecurity Student Pack

5 guides in one

CTF Starter · Bug Bounty Recon · Linux Commands

WiFi Pentesting Lab · Interview Prep

Real commands, real steps, real workflows —
not another recycled cheat sheet

ICYWALL
icywall.tech

Copyright & License

© 2025–2026 ICYWALL (icywall.tech). All rights reserved.

This document is licensed to the individual purchaser for personal, non-transferable use only. Each downloaded copy is watermarked with the buyer’s email address and payment ID.

You may NOT:

- Share, forward, resell, or redistribute this PDF or any part of it
- Upload it to file-sharing sites, Telegram/Discord/WhatsApp groups, or any public place
- Remove or alter the watermark, or claim this work as your own
- Share your download link or purchase credentials with others

Unauthorized distribution is traceable through the watermark embedded in your copy and may result in license termination and legal action under applicable copyright law.

Disclaimer: This pack is provided for educational purposes and authorized security testing only. The techniques described can cause damage or may be illegal when used without permission. Always obtain explicit written authorization before testing any system you do not own. The authors and ICYWALL accept no liability for misuse. You are solely responsible for complying with the laws of your jurisdiction.

Contents

A Linux Command Essentials	3
A.1 Filesystem map — where things live	3
A.2 Move around and look at things	3
A.3 Permissions — read them like a pentester	3
A.4 Processes and packages	3
A.5 Networking	3
A.6 Text processing — the real superpower	3
A.7 Users and identity	4
B Recon & Scanning	5
B.1 nmap — the one you must know cold	5
B.2 What the output looks like — read it	5
B.3 Fast mass scanning	5
B.4 DNS enumeration	5
B.5 Packet capture	5
C Bug Bounty Recon Pipeline	6
C.1 Step 1 — Subdomain enumeration (go wide)	6
C.2 Step 2 — Which are alive?	6
C.3 What the pipeline looks like running	6
C.4 Step 3 — Ports and services	6
C.5 Step 4 — Collect every known URL	6
C.6 Step 5 — JavaScript files are gold	6
C.7 Step 6 — Content discovery (find what isn’t linked)	7
C.8 Step 7 — Automated vuln checks	7
C.9 The whole pipeline as one-liners	7
C.10 What to actually look for	7
C.11 Write reports that get accepted	7
D WiFi & Network Pentesting Lab	8
D.1 Lab requirements	8
D.2 Monitor mode	8
D.3 Discover networks	8

D.4	Capture a WPA2 handshake	8
D.5	What the capture looks like	8
D.6	Crack the handshake	8
D.7	PMKID attack — no client needed	8
D.8	bettercap — the modern Swiss knife	9
D.9	Defending against this (say it in interviews)	9
E	CTF Starter Guide	10
E.1	Categories at a glance	10
E.2	The universal methodology (works on any box)	10
E.3	Web enumeration reflexes	10
E.4	Your first 10 challenges — the roadmap	10
E.5	Forensics & stego reflexes	10
E.6	Crypto & encoding reflexes	11
E.7	What catching a shell looks like	11
E.8	Reverse shells — memorize two	11
E.9	Linux privesc quick checklist	11
F	Interview Prep	12
F.1	Rapid-fire definitions	12
F.2	Explain-the-vuln questions (the interview way)	12
F.3	Ports you must know by heart	12
F.4	Networking questions	12
F.5	Scenario questions	13
F.6	Stand out	13
G	Quick Reference Appendix	14
G.1	Wordlist locations (Kali)	14
G.2	One-liners that save minutes	14
G.3	Free practice platforms	14
G.4	The tools this pack uses (all in Kali)	14

A Linux Command Essentials

Linux is the operating system underneath nearly everything you will touch: servers, CTF boxes, cloud instances, and Kali itself. This section is not a man page dump — it is the set of commands you will actually type every day, with examples that work.

A.1 Filesystem map — where things live

/etc	System configuration (/etc/passwd, /etc/ssh/)
/var	Logs and variable data (/var/log/)
/home	User home directories
/tmp	Temp files — cleared on reboot, world-writable
/usr/bin, /usr/sbin	Programs (user vs. admin)
/opt	Optional/third-party software
/root	Home of the root user
/proc	Live process/kernel info (/proc/cpuinfo)

A.2 Move around and look at things

```
cd /var/log          # change directory      pwd    # where am I
ls -lah              # list all, human sizes, details
find / -name flag.txt 2>/dev/null          # find a file anywhere
find / -perm -4000 2>/dev/null             # SUID binaries (privesc!)
cat file.txt          # whole file          less file.txt    # paged view
head -n 20 app.log     # first 20          tail -f app.log   # follow live
wc -l wordlist.txt     # count lines        file mystery.bin  # identify type
```

A.3 Permissions — read them like a pentester

Permissions print as `rwrx-rx-x` = owner / group / others. Numeric form: read=4, write=2, execute=1.

```
chmod 755 script.sh    # rwrx-rx-x : owner all, others read+run
chmod 600 ~/.ssh/id_rsa # private keys must be owner-only
chmod u+s /usr/bin/x    # SUID: runs as file owner (privesc vector)
chown user:group file   # change owner
ls -la /etc/shadow      # should be root-only; if readable -> jackpot
```

World-writable scripts run by cron and SUID binaries are the two classic privilege-escalation finds on Linux boxes.

A.4 Processes and packages

```
ps aux | grep apache  # find a process      kill -9 PID    # force kill
top / htop            # live process view   jobs / bg / fg
systemctl status ssh  # service state      systemctl restart nginx
systemctl enable --now ssh # start now + on boot
apt update && apt install nmap # Debian/Kali packages
dpkg -l | grep ssh    # list installed
```

A.5 Networking

```
ip a                # interfaces & IPs (replaces ifconfig)
ip r                # routes / default gateway
ss -tlnp            # listening TCP ports + owning process
ping -c 4 target    # reachability          traceroute target
curl -I https://site # headers only          curl -sL site -o out
wget -q file -O out  # download              dig example.com ANY
nc -lvnp 4444        # listener / nc target 80 # connect
scp file user@host:/tmp # copy over SSH      ssh -i key user@host
```

A.6 Text processing — the real superpower

```
grep -R "password" /etc/ 2>/dev/null # search files recursively
grep -i "admin" access.log # case-insensitive
cat log | cut -d' ' -f1 | sort | uniq -c | sort -rn # top IPs
awk '{print $1, $7}' access.log # columns
```