Linux (Quick Reference)

Tip: Spaces matter: wrap folders in quotes, e.g. `cd "My Folder"`.

Remote Access

`ssh` **Example:** `ssh user@host -p 2222`
Remote login to a machine.

- `-p` port (sometimes not 22).
- `-i` identity key file (private key).

`scp` **Example:** `scp -P 2222 user@host:~/file.txt .`
Copy files over SSH.

- `-P` port (capital P).
- `-r` recursive copy of folders.

Navigating the Terminal

`pwd` **Example:** `pwd`
Show current folder.
`ls` **Example:** `ls -lah`
List files (including hidden).

- `-l` long listing (perms/owner/size/time).
- `-a` include dot (hidden) files.
- `-h` human-readable sizes.

`cd` **Example:** `cd /path/to/folder`
Change folders (use quotes if spaces).

Searching & Viewing Files

`cat` **Example:** `cat notes.txt`
Print a file quickly.
`less` **Example:** `less -N bigfile.txt`
Scroll a file (q quits).
`tail` **Example:** `tail -n 50 file.log`
Last lines (add `-f` to follow).
`find` **Example:** `find ~/data -type f -name 'users.txt'`
Search by name (use `-type f` files, `-iname` ignore case).
`grep` **Example:** `grep -Rni keyword ~/data`
Search inside files (`-R` recursive, `-n` lines, `-i` ignore case).

Piping & Redirection

`|` **Example:** `cat file.txt | grep -i error`
Send output from one command into another.

- `>` overwrite output: `echo hi > out.txt`
- `»` append output: `echo hi » out.txt`
- `2>/dev/null` hide errors (stderr).

Creating & Moving Files

`mkdir` **Example:** `mkdir -p ~/work/output`
Create folders.

- `-p` create parents, no error if exists.

`mv` **Example:** `mv report.txt ~/work/output/`
Move/rename (use `-i` prompt, `-v` verbose).
`cp` **Example:** `cp -a src/ backup/`
Copy (use `-a` preserve, `-r` recursive).

Permissions & Validation

`chmod` **Example:** `chmod +x script.sh`
Make a script executable.
`sudo` **Example:** `sudo -l`
List allowed admin commands.
`chown` **Example:** `sudo chown user:group script.sh`
Change owner/group.
`lsattr` **Example:** `lsattr important.txt`
Show attributes (**immutable** means "locked").
`chattr` **Example:** `sudo chattr -i important.txt`
Remove immutable (`-i`); `+i` adds it.
`md5sum` **Example:** `md5sum file.bin`
Check integrity with a hash.
`base64` **Example:** `base64 -d < secret.b64`
Decode Base64 text to bytes.

Windows (Quick Reference)

Explore & Read

`Get-ChildItem` **Example:** `Get-ChildItem -Force`
List files (including hidden).

- `-Force` show hidden/system.
- `-Recurse` walk folders.

`Set-Location` **Example:** `Set-Location C:\\Temp`
Change directory.
`Get-Content` **Example:** `Get-Content .\\notes.txt`
Print a file.

- `-Tail 50` last 50 lines.
- `-Wait` follow like `tail -f`.

Search & Filter

`Select-String` **Example:** `Get-ChildItem -Recurse | Select-String keyword`
Search inside files (grep-like).

- `-CaseSensitive` exact matching.
- `-SimpleMatch` no regex.

`Where-Object` **Example:** `gci . | Where-Object Length -gt 10MB`
Filter objects by properties (size, name, etc.).

Run Scripts (Policy)

`powershell` **Example:** `powershell -ExecutionPolicy Bypass -File .\\script.ps1`
Run scripts even if policy blocks it.

- `-ExecutionPolicy Bypass` ignore policy for this run.
- `-NoProfile` faster, fewer surprises.

Decode Bytes (Simple)

`Char to int` **Example:** `[int][char]'A'`
Convert a character to its numeric code (ASCII/Unicode).

Scheduled Tasks

`Get-ScheduledTask` **Example:** `Get-ScheduledTask`
List scheduled tasks.
`Disable-ScheduledTask` **Example:** `Disable-ScheduledTask -TaskName 'TaskName'`
Safest: disable a task.
`Unregister-ScheduledTask` **Example:** `Unregister-ScheduledTask -TaskName 'TaskName' -Confirm:\$false`
Remove a task.

Move & Hash

`New-Item` **Example:** `New-Item -ItemType Directory .\\Drop`
Create a folder.
`Move-Item` **Example:** `Move-Item .\\src\\file.bin .\\Drop\\`
Move a file.
`Get-FileHash` **Example:** `Get-FileHash .\\Drop\\file.bin -Algorithm SHA256`
Verify file hash.

- `-Algorithm` SHA256, MD5, etc.

Piping (PowerShell Style)

`|` **Example:** `Get-Process | Sort-Object CPU -Desc | Select-Object -First 5`
Pipes **objects** (not raw text).
`|` **Example:** `1..5 | ForEach-Object { [char](\$_+64) } -join "`
Transform each item, then join into a string.

- `Select-Object` pick columns / first N.
- `Where-Object` filter (like grep).
- `ForEach-Object` transform each item.
- `Select-String` search inside text (grep-like).

Cryptography (Quick Reference)

Tip: When stuck, use CyberChef: `https://gchq.github.io/CyberChef/`

Base Encodings

Base64 — **Example:** `SGVsbG8=`
Identify: Chars `A-Z a-z 0-9 + /`; often ends with = padding

Base32 — **Example:** `JBSWY3DP`
Identify: Chars `A-Z 2-7`; often ends with = padding

Base58 — **Example:** `3mJr7AoUXx2Wqd`
Identify: No `0 O I l`; common in crypto addresses

Base64url — **Example:** `eyJhbGciOiJIUzI1NiJ9`
Identify: Like Base64 but uses `- _` (no `+ /`); common in JWT

Numeric & Hex

Binary — **Example:** `01001000 01101001`
Identify: Only `0/1` (often grouped in 8s)

Hex (Base16) — **Example:** `4a6f686e`
Identify: Only `0-9 a-f`; often even length

Octal — **Example:** `0755`
Identify: Digits 0–7; shows up in perms like 755

Web & Text Escapes

URL (%HH) — **Example:** `hello%20world%21`
Identify: Contains %HH sequences (H = hex digit)

HTML entities — **Example:** `<script>`
Identify: Starts with & like `<` or `&#60;`

Unicode escapes — **Example:** `\u0041\u0042`
Identify: Sequences like `\u0041` or `\x41`

Classic Ciphers

ROT13
Identify: Letters-only text; key is fixed (13)
Example: `PT: HELLO Key: 13 CT: URYYB`

Caesar shift
Identify: Like ROT13 but key can be 1–25
Example: `PT: HELLO Key: 3 CT: KHOOR`

Atbash
Identify: Alphabet reversed; no key (A↔Z)
Example: `PT: HELLO Key: (none) CT: SVOOL`

Vigenère
Identify: Keyed shifts; ciphertext looks like letters; try if a key is hinted
Example: `PT: ATTACKATDAWN Key: LEMON CT: LXFOPVEFRNHR`

XOR
Identify: Often shown as hex; key may repeat across text
Example: `PT: FLAG Key: 0x20 CT: flag`

Hashes (Not Encryption)

MD5 — **Example:** `5d41402abc4b2a76b9719d911017c592`
Identify: 32 hex chars

SHA1 — **Example:** `da39a3ee5e6b4b0d3255bfef95601890afd80709`
Identify: 40 hex chars

SHA256 — **Example:** `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`
Identify: 64 hex chars

bcrypt — **Example:** `$2y$10$abcdefghijklmnopqrstuv`
Identify: Starts with $2a$/$2b$/$2y$

Hack (Recon & Cracking)

Tip: Scan first, then enumerate what you find. Keep notes as you go.

Host Enumeration (First 2 Minutes)

`whoami` — **Example:** `whoami`
Who you are (current user).

`id` — **Example:** `id`
Your groups (useful for permissions).

`ip` — **Example:** `ip a`
Network interfaces + IPs.

`ss` — **Example:** `ss -tulpn`
What services are listening (ports).

`uname` — **Example:** `uname -a`
Kernel / system info.

Network Recon (nmap)

`Discover hosts` — **Example:** `nmap -sn 192.168.1.0/24`
Host discovery only (`-sn`), no ports.

`Service scan` — **Example:** `nmap -p- -sV TARGET`
All ports (`-p-`) + versions (`-sV`).

`Quick scripts` — **Example:** `nmap -sC -sV TARGET`
Default scripts (`-sC`) for common checks.

`Save output` — **Example:** `nmap -sV -oN scan.txt TARGET`
Write output to a file (`-oN`).

Web Enumeration (gobuster)

`Dir brute force` — **Example:** `gobuster dir -u http://TARGET:PORT -w wordlist.txt`
Find hidden paths.

- `-x php,txt,bak` try extensions.
- `-t 50` threads.
- `-o out.txt` save results.

`Quick requests` — **Example:** `curl -s -L http://TARGET:PORT/path`
Pull pages fast.

- `-s` silent, `-L` follow redirects.
- `-I` headers only.

Extra Web Checks

`Headers` — **Example:** `curl -sI http://TARGET:PORT/`
See server + redirects.

`Robots` — **Example:** `curl -s http://TARGET:PORT/robots.txt`
Common "hidden paths" hint.

`Tech clues` — **Example:** `curl -s http://TARGET:PORT/ | head`
Quick peek at HTML.

Password Cracking

`unshadow` — **Example:** `unshadow /etc/passwd /etc/shadow`
Merge account list + hashes into one file for cracking.
/etc/passwd: usernames/UIDs/shells (usually no hashes).
/etc/shadow: password hashes

`John` — **Example:** `john -wordlist=words.txt hashes.txt`
Try a wordlist.

- `-format=` set hash type if needed.
- `-show` display cracked creds.
- `-rules` mutate words (bonus flags).

`Hashcat` — **Example:** `hashcat -m 0 -a 0 hashes.txt words.txt`
GPU cracking (optional): tune `-m` mode + `-a` attack.

Useful Wordlists

`Common lists` — **Example:** `ls /usr/share/wordlists/`
Where wordlists often live.

`Make one` — **Example:** `sort -u words.txt > clean.txt`
Deduplicate a wordlist.