1 ORDER OF OPERATIONS

Enumerate: What type of system is this? (`cat /etc/os-release` to see distribution/version). What users are on the system? What services are running? What ports are open? `ss -tulnp` lists listening tcp/udp ports with owning process.
Firewall: Install UFW. `sudo ufw allow ssh`. Allow other required services: For Jenkins: allow 8080/tcp; For OpenVPN: allow 1194/udp; For web servers: allow 443/tcp.
User Management: List users: (look for users with shells/hashes). `sudo cat /etc/passwd` and `sudo cat /etc/shadow`. Expire unneeded. Change passwords.
Verify Packages: Debian: `sudo dpkg --verify`. REHL: `sudo rpm -Va`.
Update Packages: Debian: `apt update && apt upgrade -y`. RHEL: apt = yum (dnf on Fedora).
Secure service: Check configuration. Manage users (if applicable).
Install and Configure Auditd: Monitor and defend. Watch logs. Keep looking for badness.
Deny red team tooling: Strip interpreters/compilers/relay tools a scored service does not use (see below).

2 USERS

useradd [name]: Creates a user account.
- `-m`: Creates a home folder for the user.

passwd [user]: Change a user's password.
chpasswd: Batch update passwords (format: `user:pass`).
- *Direct usage:* Run `sudo chpasswd`, type list, press `Ctrl+D` to save changes.
- *File usage:* `sudo chpasswd < list.txt`

usermod [user]: Modify a user account.
- `-aG [group]`: Add user to a group (e.g., sudo/wheel).
- `--expiredate 1`: Completely disable the account.
- `--expiredate 2030-01-01`: Reactivate expired account.

su [user]: Switch user. `sudo su` = become root.
find / -name authorized_keys: Find allowed SSH keys.
who -a: Show logged in users, session PIDs, and remote IPs.

3 NETWORKING

ip a: List all network interfaces and their addresses.
netstat: Print network connections and routing tables.
- `-tulnp`: Show listening tcp/udp ports and processes.
- `-tupan`: Show listening and outbound connections.

ufw: Uncomplicated firewall.
- *Setup:* `sudo apt install ufw -y`, `sudo ufw allow ssh`, `sudo ufw enable`.
- *Allow port:* `sudo ufw allow port/protocol`.
- *Examples:* `sudo ufw allow 443/tcp`, `sudo ufw allow 53/udp`.

firewalld (RHEL/CentOS/Fedora):
- *Status:* `firewall-cmd --state`
- *Allow Service:* `firewall-cmd --permanent --add-service=http`
- *Allow Port:* `firewall-cmd --permanent --add-port=8080/tcp`
- *Apply:* `firewall-cmd --reload`
- *List Rules:* `firewall-cmd --list-all`

nmap [host(s)]: Network scanner.
Example: `nmap -A 10.0.10.0-255` (OS, Service, Scan).
nmap (Local Scan):
- `nmap -sV 10.0.10.0/24`: Scan local subnet for service versions.
- `nmap -A [host]`: OS detection, service version, script scanning.
- `nmap -p- [host]`: Scan all 65535 ports.

4 FILE PERMISSIONS

chown [user] [file]: Change the owner of a file.
chmod: Change file permissions.
- *Symbolic:* `u`=User/Owner, `g`=Group, `o`=Other, `a`=All, `r`=read, `w`=write, `x`=execute
- *Numeric:* 1=execute, 2=write, 4=read.
- *Example:* `chmod 740 file` (Owner=7=rwx, Group=4=r, Other=0=—).
- *Example:* `chmod a+x file` (Give everyone execute).

5 IMPORTANT FILES

/etc/passwd: List of all users.
/etc/shadow: List of user password hashes.
/etc/sudoers & /etc/sudoers.d: Defines sudo permissions. `ALL ALL=(ALL) ALL` means all users can use sudo. Use `visudo` to edit.
/etc/group: Lists all groups and their members.
/var/log/auth.log & **/var/log/syslog**: Auth and system logs.
tail -f [file]: Watch log for new events in real-time.

6 AUDITD, AUREPORT, AUSEARCH

Setup: `sudo apt install auditd`, `curl -O [rules]`, `mv` to `/etc/audit/rules.d/`, `sudo service auditd restart`.
aureport -i: Reports info on audit logs.
- `-x --summary`: Show run counts for executables (Check for malware).
- `-au`: Authentication attempts. `-u`: User commands.
- `-h`: Connected hosts. `-f --summary`: Files opened.
- `-tm`: Terminals used. `-m`: User modifications.

ausearch -i: Search the audit logs.
- `-k [key]`: Search by event key (rootcmd, susp_activity).
- `-p [pid]`: Events related to a specific process ID.
- `-m [type]`: Message type (LOGIN, EXECVE, ADD_USER).

7 SYSTEMD & CRON

systemctl: Manage system services.
- `list-units --type=service`: List all services.
- `enable/disable/restart [srv]`: Persistence/state.
- `status [srv]`: Show if service is active or failed.

/etc/systemd/: Look for weird unit files in system/user dirs; disable if bad.
Cron: Command scheduler. Remove unauthorized entries.
- *Root crontabs:* `/etc/crontab`, `/etc/cron.d/`.
- *User crontabs:* `/var/spool/cron/`.

8 DENY RED TEAM TOOLING

Most of red team's toolkit depends on what's already sitting on the box. Confirm nothing scored needs an item, then remove it and log the change.
- **Python:** Ansible's default connection plugin needs a Python interpreter on the managed node; most red team post-ex/staging scripts assume one too. `apt remove --purge python3` (or `chmod 000` the binary + `apt-mark hold` python3) breaks both.
- **Perl, Ruby, other unused interpreters:** same idea, lower prevalence.
- **Compilers (gcc, cc, make, build-essential):** rarely needed at runtime. Blocks on-box compilation of an exploit or implant.
- **netcat/ncat/socat, if unused:** the default pivot/reverse-shell relay. Check startup scripts and cron first.
- **SSH client (not server) on hosts that never SSH out:** removes a lateral-movement path, leaves inbound access alone.
- `find / -perm -4000 -o -perm -2000 2>/dev/null`: SUID/SGID binaries vs. a known-good list; an unexpected one is a ready-made LOLBin.

9 MALWARE: YARA & CLAMAV

Yara: Malware classification tool.
- *Setup:* `sudo apt install yara -y`, `git clone [rules]`.
- *Usage:* `yara [rules] [target] [-r] -w`.
- *Ex:* `yara rules/malware_index.yar / -r` (Full scan).

ClamAV: `apt install clamav`.
- `freshclam`: Update signature database.
- `clamscan`: Run a scan (may fail on low memory).

10 PROCESSES & THREAT HUNTING

ps -aux: List all running processes.
top: Live resource usage.
kill [pid]: Kill a process.
killall [name]: Kill all by name (e.g. `killall perl`).
Everything in Linux is a file (/proc/[pid]/):

- `cwd`: Current working dir of process.
- `cmdline`: Arguments used to run the program.
- `exe`: The executable (even if deleted from disk).
- `environ`: Environment variables (look for USER).

11 AWS NACLS & SECURITY GROUPS

AWS NACLs: Enable GuardDuty + CloudTrail. Check S3 perms and IAM roles. Check EC2 IAM roles. Setup SGs for RDS/Lambda.

AWS Security Groups: Stateful. Only allow ssh and required services in. Only allow https and dns out. Disallow all outbound after updates.

12 SSHD & PAM

Config: `/etc/ssh/sshd_config` (Check `.d/*.conf` overrides).

- `AllowUsers user1 user2`: Limit login access.
- `PermitRootLogin no`: Disable root SSH.
- `PermitEmptyPasswords no`: Require passwords for all logins.

PAM: Config `/etc/pam.conf`, `/etc/pam.d`.

- Check configs for ssh, su. `dpkg -V` catches changes.
- Look for **"sufficient"**: Verify if module called is legitimate.
- *Complexity*: `minlen=8`, `dcredit=-1`, `enforce_for_root`.