After Initial Access (short checklist)

1) Stabilize shell (if reverse shell)

- Use a TTY upgrade: python3 -c 'import pty; pty.spawn("/bin/bash")'
- Ctrl-Z → stty raw -echo; fg
- export TERM=xterm-256color

2) Basic enumeration (immediate)

- whoami; id; hostname
- uname -a; cat /etc/issue
- ip a / ifconfig
- ps aux
- sudo -l
- find / -perm -4000 2>/dev/null
- cat /home/*/user.txt 2>/dev/null

3) Search for credential artifacts (document only)

- grep -ri "password" /etc /var /home 2>/dev/null
- check web config locations (e.g., /var/www/html/config.*) and record paths
- list accessible files; DO NOT run automated dumping tools unless exam policy allows

4) PrivEsc concept checklist (do not include PoCs)

- Check sudo rules, SUID binaries, world-writable scripts, cron jobs, service configs
- If kernel exploit seems the only path, document and get explicit permission first

5) Windows post-access (safe checks)

- whoami; whoami /groups; systeminfo; hostname
- net users ; dir C:\Users\
- check Scheduled Tasks: schtasks /query /fo LIST /v

- search for config files and credential-like files; record paths