Standalone Quick-Read — Triage & First Actions

Decision (20-30s)

- Open 'Initial Foothold Playbook' + 'nmap_oscp_plus_cheatsheet' first. Determine web vs SMB vs RDP vs other.

Immediate nmap (run now)

```
nmap --top-ports 200 -sS -sV -T4 -oA quick TARGET
nmap -p- -sS -T4 -oA allports TARGET
nmap -sU --top-ports 100 -oA udp_quick TARGET    # if UDP likely
```

Web quick commands

- whatweb http://TARGET:PORT
- curl -I http://TARGET:PORT

```
gobuster dir -u http://TARGET:PORT -w /path/wordlist -x php,html,txt -t 50
ffuf -u http://TARGET:PORT/FUZZ -w /path/wordlist -c -t 50
```

- nikto -h http://TARGET:PORT

SMB / Service quick commands

```
enum4linux -a TARGET
smbclient -L //TARGET -N
```

- smbmap -H TARGET

```
nmap -p 3389 --script rdp-enum-encryption TARGET
```

What to extract (quick)

- Open ports with versions, anonymous access, credential reuse, writable shares, upload endpoints, SQL injection points.
- If initial shell: run linpeas/winpeas and 'sudo -l' or 'whoami /priv' for immediate privesc hints.

Fallbacks & reporting

- If no creds: focus on local misconfig (SUID, weak services, exposed configs).
- Save every command and output using -oA; copy 3 commands + success patterns to your working note.