Web Recon & Enumeration

Basic scanning (syntax examples)

- nmap -sC -sV -Pn -oN nmap.txt <target_ip>

- whatweb <target_ip>

Directory / virtualhost discovery (syntax examples)

- gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html -t 50 -o gobuster.txt

- ffuf -u http://<target_ip>/FUZZ -w /usr/share/wordlists/common.txt -e .php,.html,.txt -o ffuf.txt

Extra web tools (examples)

- nikto -h http://<target_ip>

- httpx -c <target> # quick tech detection

- curl -I http://<target_url> # inspect headers

- manual source/JS review in browser

Identifying vulnerability vectors (conceptual clues — syntax only)

- LFI: check for file-include patterns (note suspicious parameters; do not run exploit payloads)

- File upload: test existence and file handling behavior; log responses and allowed extensions

- RCE / command injection: look for evidences (behavioural clues), then follow lab-tested verification workflows

- SQLi: use safe tests or sqlmap with caution (tool usage only; follow exam policy)

- SSTI: look for template markers (e.g., {{ }}) in response content

- SSRF: note URL plumbing; verify internal reachability only per policy

- Auth bypass: check for default creds / weak login behavior; avoid using external walkthroughs

CMS detection (syntax examples)

- whatweb <target>

- wpscan --url http://<target> --enumerate u # use responsibly and per exam rules

Exploit & payload policy (important)

- Do NOT paste or run unverified exploit PoCs from public sites during the exam.

- If a custom exploit is required, test and verify in your lab first; in exam, prefer documented, minimal verification steps and record all outputs.

- Avoid storing full web-shell code or reverse-shell payloads in live exam notes.

Common post-foothold checklist (before escalation)

- Stabilize shell (TTY upgrade syntax only): python3 -c 'import pty; pty.spawn("/bin/bash")'

- Record context: whoami; id; uname -a; ip a

- Basic enumeration: sudo -l ; ps aux ; find / -perm -4000 2>/dev/null

- Search for config files and credential artifacts; document paths (do not run credential-dump tools unless permitted)

- Prefer built-in tools for verification; if transferring tools is necessary, follow exam policy for allowed methods