# Exam-Safe Reference — Sanitized (OSCP/OSCP+)

**Sanitization note:** This document is an exam-safe, sanitized reference. It contains only generic command templates, triage checklists, and high-level process notes. All explicit exploit sequences, PoC scripts, step-by-step post-exploitation commands, and external links have been removed.

## Recon (External & DNS) — Examples (syntax only)

- host <domain> ; host -t mx <domain>
- host -t txt <domain>
- whois <domain> or whois <ip>
- dnsrecon -d <domain> -t std
- dnsenum <domain>
- nslookup <name> <ip>

## IP → Hostname Enumeration (examples)

- for ip in $(cat list.txt); do host $ip; done
- for ip in $(seq 200 254); do host <prefix>.$ip; done | grep -v "not found"

## Website Recon (syntax only)

- nmap -p80 --script=http-enum <ip>
- gobuster dir -u http://<ip> -w /usr/share/wordlists/common.txt -t 50
- curl http://<ip>/robots.txt
- whatweb http://<ip>

## Vulnerability Scanning — Nmap (safe guidance)

- nmap -sV -p <port> --script "vuln" <ip>
- Do NOT execute external PoC scripts during the exam unless explicitly allowed and verified locally.

## SQL / MySQL — Basic syntax (reference)

- mysql -u <user> -p'<pass>' -h <ip> -P 3306
- Basic checks: SELECT version(); SHOW DATABASES;
- Use sqlmap only as a tool for testing and per exam rules: sqlmap -u 'http://<ip>/page.php?id=1' --dbs

## Password Attacks — Policy & Syntax

- Use brute-force / password-spray only if explicitly permitted in the exam rules.
- Example tool syntax (do not treat as a step-by-step guide): hydra -l <user> -P /path/wordlist ssh://<ip>

## Post-Access & Privilege Enumeration — High-level (safe)

- After obtaining access, document context: whoami / id ; hostname ; uname -a
- Check for credential artifacts and config files; record file paths and permissions (do NOT run automated dumping tools unle
- Enumerate services, scheduled tasks/cron, sudo permissions, and local accounts
- Convert any automated tool findings into manual verification steps for reporting

## Active Directory — High-level Guidance (sanitized)

- Domain discovery examples: net user /domain ; net group /domain
- Use PowerView / BloodHound as lab learning tools; document findings concisely (do not include automated collection outp
- Collect SPN names and domain-related indicators (record names only; do not perform intrusive automated attacks without

## Lateral Movement & Credentials — Policy-first notes

- If credentials are found, verify access methods (SMB/WinRM/SSH) using documented allowed tools and record exact com
- Do not paste or use external walkthroughs or PoC scripts; document all steps and evidence for reporting.

## Summary Triage Flow (quick)

1) nmap triage → 2) identify high-value service (web/smb/sql/winrm) → 3) focused enumeration →
4) look for exposed creds/configs → 5) attempt safe access methods → 6) document outputs and timestamps

Sanitization: This file was created by sanitizing user-provided notes. It contains only generic command templates, triage checklists, and high-level process notes. No step-by-step exploit procedures, PoC scripts, or external writeups are included.