OSCP Cheatsheet

General Quick Tips

- Use `tree /F` (Windows) in user folders for quick file tree overview when allowed.

- Always save command outputs (nmap -oA, tool logs) for reproducibility.

- Keep one-page playbooks for: Triage, Web, SMB/AD, PrivEsc Linux, PrivEsc Windows.

- Remove any external links or full exploit scripts from your local exam copy.

Important File Locations (short list)

Windows (examples):
C:\Users\<user>\
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SYSTEM
C:\inetpub\wwwroot\
C:\xampp\htdocs\
%USERPROFILE%\.ssh\authorized_keys

Linux (examples):
/etc/passwd
/etc/shadow
/etc/hosts
/var/www/html/
/etc/apache2/apache2.conf
/etc/mysql/my.cnf
/root/.ssh/
~/.ssh/

Enumeration — Quick Commands

nmap --top-ports 200 -sS -sV -T4 -oA quick <TARGET>
nmap -p 88,389,445,464,636,3268 -sV -Pn -oA ad_ports <TARGET>

enum4linux -a <TARGET>
smbclient -L //<TARGET> -N
smbmap -H <TARGET>
crackmapexec smb <TARGET> -u <USER> -p <PASS> --shares

ldapsearch -x -H ldap://<TARGET> -b "DC=domain,DC=local"

gobuster dir -u http://<TARGET>:<PORT> -w /path/wordlist -x php,html,txt -t 50
ffuf -u http://<TARGET>:<PORT>/FUZZ -w /path/wordlist -t 50
curl -I http://<TARGET>:<PORT>

find / -name '*.kdbx' 2>/dev/null
find / -type f -perm -4000 2>/dev/null # SUID

Active Directory — Quick Checklist

- Check for AD ports (88, 389, 445, 464, 3268).
- Enumerate users, groups, and SPNs; document any accounts allowing preauth-less or AS-REP roastable flags.

- Harvest service account names and note writable shares; document paths to sensitive files.
- If credentials found, test safe access methods (winrm/ssh) and save outputs.

Privilege Escalation — Short Checklists

Linux:
- sudo -l
- find / -perm -u=s -type f 2>/dev/null
- getcap -r / 2>/dev/null
- check cron, /etc/passwd, /etc/shadow, env vars, service configs
- run linpeas/linenum in lab environment to learn patterns (do not run intrusive tools on exam infra unless allowed)

Windows:
- whoami /priv ; whoami /groups
- check scheduled tasks, startup folders, service binaries and unquoted service paths
- search for config files and .xml/.ini files containing credentials
- use automated enumerators for learning only (winpeas) and convert findings into manual steps

Post-Exploitation / Reporting

- Save command history and output files for reporting.
- Capture screenshots or terminal output showing proofs (user.txt, proof files).
- Note exact commands used to obtain each proof.
- Do not exfiltrate real data; follow exam rules about evidence collection.