Nmap & Recon Cheat-sheet — OSCP+ (Exam-ready)

Compact commands, workflows, and quick notes — paste into your exam sheet

1) Nmap essentials (memorize these)

• Discovery & basic scans:

```
nmap -sS -Pn -p- -T4 -oA OUTNAME IP    # TCP SYN scan, skip host discovery, all TCP ports
```

```
nmap -sT -Pn -p- -T3 -oA OUTNAME IP    # TCP connect (no root)
```

```
nmap -sU -Pn -p- -T4 -oA OUTNAME IP    # UDP (very slow — target specific ports)
```

```
nmap -sn IP/24 -oA discovery            # Ping sweep (host discovery only)
```

• Service/version, default scripts, OS detection:

```
nmap -sS -sV -sC -O -Pn -p PORTS -T4 -oA OUTNAME IP
```

• Aggressive / comprehensive:

```
nmap -p- -sS -T4 --min-rate=500 -sV -A -oA OUTNAME IP
```

• Output options (always use): -oN, -oX, -oG, -oA

2) NSE — categories & high-value scripts

• Categories: default, safe, discovery, auth, vuln, intrusive
• Useful scripts: smb-enum-shares, smb-enum-users, smb-vuln-ms17-010, http-enum, http-methods, ftp-anon, dns-zone-transfer, snmp-info, ssl-cert
• Run categories: nmap -sV --script "vuln or auth or discovery" -oA OUTNAME IP

3) Fast recon workflow (exam sequence)

• 1) Discovery: nmap -sn IP/24 -oA discovery
• 2) Quick top ports: nmap --top-ports 200 -sS -sV -T4 -oA quick IP
• 3) All-port if needed: nmap -p- -sS -T4 -oA allports IP
• 4) Service enumerate: nmap -p <ports> -sV -sC -O -oA svc_enum IP
• 5) Targeted NSE: nmap -p <ports> -sV --script "auth or vuln or discovery" -oA nse IP

4) Service-specific enumeration (fast commands)

• HTTP / Web:

```
nmap -p 80,443,8080 -sV --script http-enum,http-title,http-methods -oA web IP
```

```
gobuster dir -u http://IP:PORT -w /path/wordlist -x php,html,txt -t 50
```

```
ffuf -u http://IP:PORT/FUZZ -w /path/wordlist -c -t 50
```

• SMB / Windows:

```
enum4linux -a IP
```

```
smbclient -L //IP -N
```

```
smbmap -H IP
```

```
crackmapexec smb IP -u user -p pass --shares
```

- SSH / FTP / DNS / SNMP / Databases quick commands included in PDF

5) Parsing & processing outputs

- Use -oG for greppable output and -oX for XML to import into reporting tools.
- Example: grep Up OUT.gnmap | awk '{print $2}'
- Always save -oA and copy important lines to your report.

6) Tools & follow-ups

- Web: gobuster, ffuf, whatweb, nikto, sqlmap
- SMB/Windows: enum4linux, smbclient, smbmap, crackmapexec, impacket
- Local privesc: linPEAS.sh, linEnum.sh
- AD: BloodHound/SharpHound, ldapsearch, crackmapexec

7) Prioritization & trade-offs

- Fast wins: --top-ports 1000 → enumerate → run -sV -sC on interesting ports
- Comprehensive but slow: -p- and -sU only if time allows
- NSE scripts: run discovery/default first; vuln scripts can be intrusive

8) Short cheat-list (memorize these)

```
nmap -sn 10.10.10.0/24 -oA discovery
```

```
nmap --top-ports 200 -sS -sV -T4 -oA quick 10.10.10.123
```

```
nmap -p- -sS -T4 -oA allports 10.10.10.123
```

```
nmap -p 22,80,139,445 -sV -sC -O -oA svc_enum 10.10.10.123
```

```
nmap -p 80,443 --script http-enum,http-methods -oA web 10.10.10.123
```

```
nmap -p 139,445 --script "smb-enum-shares,smb-enum-users,smb-vuln-ms17-010" -oA smb
10.10.10.123
```

9) Exam etiquette & risks

- Some NSE scripts are intrusive — they may crash services. Use only if allowed.
- Document every command you ran and why — reproducibility is scored.

Generated cheat-sheet — keep commands verbatim in your notes. Save outputs with -oA. Good luck on OSCP+!