AD Quick-Read — Triage & First Actions

Decision (20-60s)

- Open 'is this part of AD or not' first. Look for 389/636 (LDAP), 88 (Kerberos), 445 (SMB), 464 (Kerberos pw-change).
- If AD: follow this AD checklist.

Immediate nmap (run now)

```
nmap --top-ports 200 -sS -sV -T4 -oA quick TARGET      # fast service triage
nmap -p 88,389,445,464,636,3268 -sV -sC -Pn -oA ad_ports TARGET
nmap -p- -sS -T4 --min-rate=500 -oA allports TARGET     # only if quick found nothing
```

AD quick commands (copy-paste)

```
enum4linux -a TARGET
ldapsearch -x -H ldap://TARGET -b "dc=domain,dc=local" '(objectClass=*)'  # quick LDAP probe
crackmapexec ldap TARGET -u '' -p '' --shares
crackmapexec smb TARGET -u USER -p PASS --shares --local-auth
rpcclient -U "" TARGET -c 'enumdomusers'
```

What to extract (quick)

- Domain controllers, SPNs, users with AD privileges, writable shares, accessible LDAP, service account names (for AS-REP/AS-REP roast).
- If creds found: try winrm: 'winrm -hostname TARGET -u DOMAIN\\user -p Pass' or use 'evil-winrm -i TARGET -u user -p pass'.

Next steps (30-60s each)

- Run SharpHound collection if allowed (BloodHound), focus on Creds → Lateral → DA paths.
- If Kerberos: try AS-REP roast and Kerberoasting (GetTGS_ATTACK).
- Document commands & outputs to report immediately.

Generated quick-read — use as first files to open during triage.