Credential verification — Exam-safe reference

Policy first:

- Do NOT perform password-sprays or brute-force attacks unless the exam rules permit them.

- Test only with provided or legitimately obtained credentials; document every command and output.

Quick steps (conceptual)

1) Note credentials: e.g., Given: bob / Password123 — record them immediately.

2) Verify credentials non-intrusively on likely Windows/AD hosts:

   - Test SMB shares (example syntax): smbclient -L //<IP> -U '<user>'   # lists shares

   - Test remote management (example syntax): crackmapexec winrm <IP> -u <user> -p '<pass>'   # reports access

   - Test LDAP binding (example syntax): ldapsearch -x -h <IP> -D '<user@domain>' -w '<pass>' -b 'dc=domain,dc=local'

3) Check which hosts accept the credentials — record hostnames/IPs and whether the account has elevated privileges.

4) Prefer script-friendly remote interfaces (WinRM) for further enumeration if allowed; avoid GUI/RDP unless necessary.

5) Reporting: for each host where creds work, save the exact command you ran, the output, timestamp, and a short note of what you attempted next.

Tool usage examples (syntax only — adapt per host)

```
- smbclient -L //<IP> -U '<user>'

- crackmapexec smb <IP> -u '<user>' -p '<pass>'          # info-only query

- crackmapexec winrm <IP> -u '<user>' -p '<pass>'

- evil-winrm -i <IP> -u <user> -p '<pass>'               # use only if allowed by exam rules

- ldapsearch -x -h <IP> -D '<user@domain>' -w '<pass>' -b 'dc=domain,dc=local'
```