After Getting Credentials — Sanitized (Exam-safe)

Sanitization note: This document is an exam-safe, sanitized reference. It contains only high-level process guidance, allowed command templates for verification, and triage checklists. All explicit exploit steps, post-exploitation PoCs, tool-specific attack sequences, and external links have been removed.

1) Test credentials across services (syntax examples)

- Verify credentials on common services where applicable: SMB, WinRM/remote management, HTTP logins, FTP, SSH.
- Example verification syntax (tool usage only, not exploit steps):
  * SMB: 'smbclient -L //<target> -U <user>' to list shares (if allowed)
  * HTTP: attempt login on web panels using provided credentials
  * FTP: connect with credentials to port 21
  * SSH/RDP: only if ports 22/3389 open and per exam rules
- Record exact command and outputs for reporting if access is successful.

2) Use remote access strategically

- Prefer remote-management interfaces (e.g., WinRM) for script-friendly enumeration when permitted.
- RDP/SSH provide interactive shells but consider transfer and tooling limitations.
- If remote login is used, document steps, timestamps, and outputs for reporting.

3) Enumerate with credentials (high-level checks)

- Gather context: whoami / id ; hostname ; environment info
- Enumerate users, groups, and machine lists at a high level (domain queries or local equivalents). Avoid including automate
- Check available shares, service configurations, scheduled tasks/cron jobs, and accessible files. Document locations and p
- Do not run intrusive credential-dumping or automated exploitation tools unless explicitly allowed by exam policy.

4) Decision matrix (high-level)

Situation: Got creds + no shell access
Next move: Check SMB shares, web panels, FTP, WinRM (as allowed)

Situation: Got creds + RDP/SSH available
Next move: Use GUI/interactive shell only if necessary; prefer remote enumeration when possible

Situation: AD user credentials
Next move: Perform non-intrusive AD enumeration to map access and potential privilege paths; document findings

5) Host & Domain checks (sanitized guidance)

- Identify whether account is domain or local: check environment variables and contextual info (e.g., USERDOMAIN, whoam
- If in AD, prioritize discovery: list visible shares, domain groups, and accessible machines (record results).
- Avoid running domain-wide automated attacks or dumping domain secrets unless exam policy explicitly allows and you do

6) Sessions, logged-on users & shares (examples)

- Useful checks (syntax examples):
  * Query logged-on users and sessions via built-in commands (e.g., 'query user', 'qwinsta /server:<hostname>' where availa
  * List shares and open files using native commands (e.g., 'net view', 'net share')
- Record outputs; convert any automated findings into manual verification steps.

7) ACLs, object permissions, and GPOs (high-level)

- Check for interesting ACLs and permissions that may indicate privilege escalation paths; record object names and permiss
- Do not execute automated ACL exploit tools unless explicitly permitted; instead document findings for manual review.

8) Credential handling & policy

- When you find credentials or secrets, document file paths and context. Do NOT exfiltrate or transfer real sensitive data.
- If transferring tools is required, follow exam policy and get explicit permission; prefer built-in utilities for verification.

9) Living off the land (LoL) and persistence (policy-first)

- Use built-in OS utilities for verification and minimal interaction. Avoid creating persistence or modifying system state unless
- If persistence is required by the exam task, follow instructions and document exactly what you changed.

Sanitization: This file was created by sanitizing user-provided notes. It contains only high-level process guidance, allowed verification command templates, and triage checklists. No step-by-step exploit sequences, PoC code, or external writeups are included.