Backtracking to user.txt — Sanitized (Exam-safe)

Sanitization note: This file is an exam-safe reference. It contains only high-level guidance, allowed verification commands, and documentation reminders. No exploit PoCs, credential-dump sequences, or external writeups are included.

Why backtrack?

- You sometimes obtain root before locating the initial user's flag. Both user.txt and root.txt may be required for full credit.
- If root is obtained without user.txt, document the steps and then locate user.txt for full evidence.

Steps to backtrack to user.txt (sanitized)

1) Identify likely user accounts
   - Linux: ls /home/ ; cat /etc/passwd | grep /home
   - Windows: dir C:\Users\ ; net user

2) Search common flag locations (document findings)
   - Linux: cat /home/<username>/user.txt (check with appropriate permissions)
   - Windows: type C:\Users\<username>\Desktop\user.txt

3) Investigate artifacts for context (document only)
   - Look for configuration files, user-owned files, shell histories, or job scripts that indicate user activity. Record file paths and

4) Switch user context if permitted and necessary
   - Linux: use 'su <username>' or 'sudo -u <username> bash' (only if you have valid credentials/permission)
   - Windows: use 'runas /user:<username> cmd.exe' (only if valid credentials available)

5) Re-evaluate the privilege path
   - The user's environment may reveal missed enumeration steps; document what you learn and update your report.

6) Evidence & reporting
   - When you find user.txt, capture a screenshot or saved terminal output showing: target IP, the flag content (as required), a

Quick checklist (copy-paste)

- ls /home/ ; cat /etc/passwd | grep /home
- cat /home/<username>/user.txt 2>/dev/null
- dir C:\Users\ ; type C:\Users\<username>\Desktop\user.txt
- Document file paths, timestamps, and outputs for reporting
- If switching user context, record exact commands and timestamps

Sanitization: This document is sanitized for exam use. It contains only allowed verification commands and process guidance. No exploit instructions, credential-dumping commands, or external writeups are present.