Day 32

Exploitation Analyst

Restrict users from using the old password:

Why is old password reuse a bad practice?

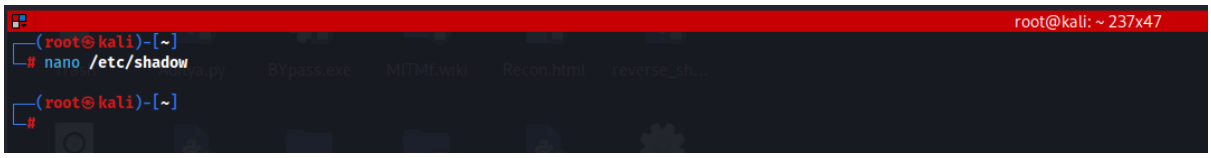
Reusing old passwords defeats the purpose of changing them. Here's why:

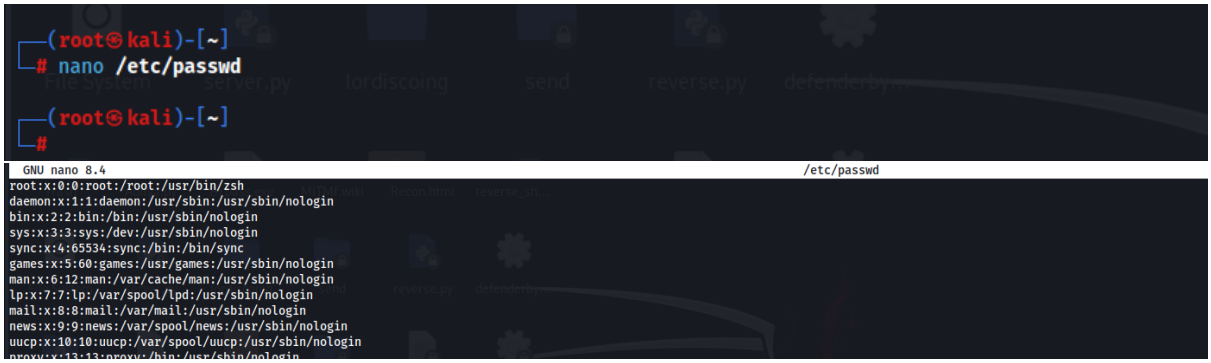
1. **Predictability**: Users often rotate through a small set of familiar passwords. Attackers who compromise one can guess future ones.
2. **Brute-force risk**: If an old password leaks, the user might reuse it again — making brute-force or credential stuffing attacks more effective.
3. **Security hygiene**: Preventing reuse encourages genuinely new passwords, reducing long-term exposure

Where are passwords stored in Linux?

Passwords are not stored in plaintext.

In Linux, passwords are securely stored as hashes in /etc/shadow, which is only readable by root, unlike /etc/passwd, which is world-readable and meant for general user info. /etc/security/opasswd stores hashes of old passwords to prevent reuse, enhancing password security and hygiene.

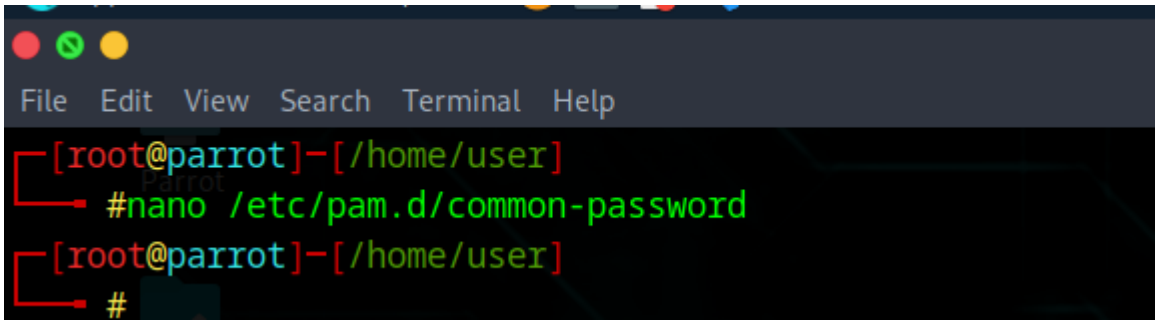




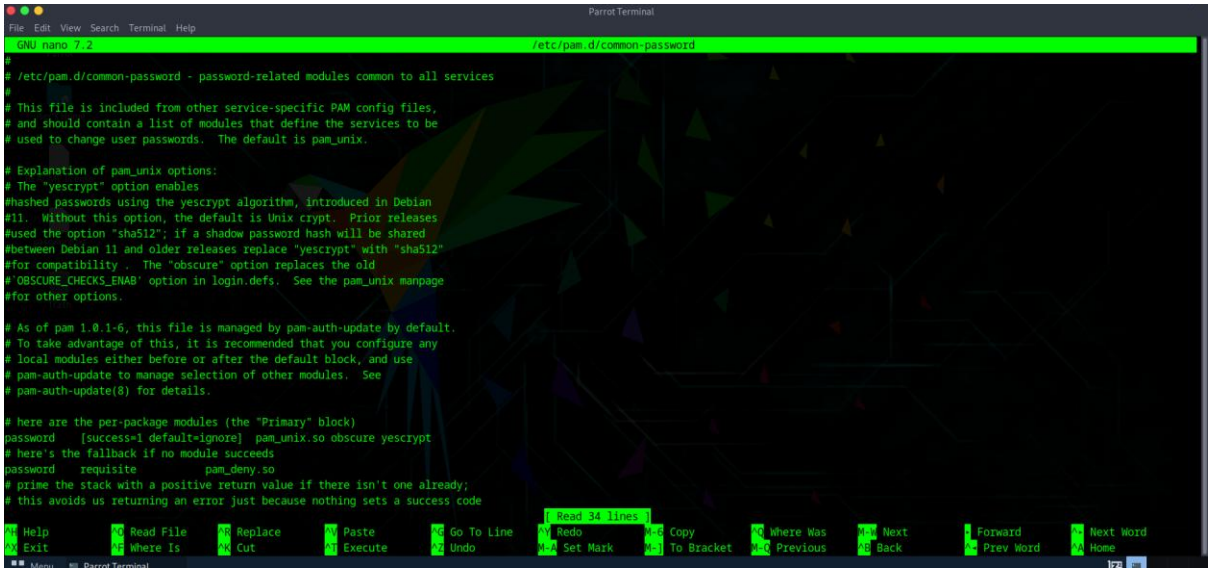
Steps to Restrict users from using the old password:

Steps:

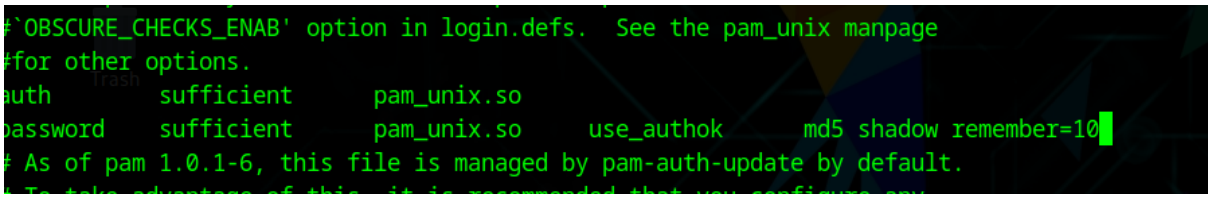
Open the common-password file in pam.d:



Following screen will appear:



Scroll down and add the following line:



This configuration ensures secure password handling in Linux. The OBSCURE_CHECKS_ENAB setting enforces strong password rules, while shadow stores passwords securely. The remember=10 option prevents users from reusing their last 10 passwords. Using sufficient helps improve efficiency by skipping further checks once authentication succeeds.