5.3.3 Ensure password reuse is limited (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.
Note that these change only apply to accounts configured on the local system.

Audit

Run the following commands and ensure the remember option is '5' or more and included in all results:

```
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/password-auth
password sufficient pam_unix.so remember=5
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/system-auth
password sufficient pam_unix.so remember=5
```

Remediation

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the `remember` option and conform to site policy as shown:

```
password sufficient pam_unix.so remember=5
```

Notes

Additional module options may be set, recommendation only covers those listed here.