5.3.4 Ensure password hashing algorithm is SHA-512 (Scored)

Profile Applicability

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

Description

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Note that these change only apply to accounts configured on the local system.

Audit

Run the following commands and ensure the sha512 option is included in all results:

```
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/password-auth
password sufficient pam_unix.so sha512
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/system-auth
password sufficient pam_unix.so sha512
```

Remediation

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the `sha512` option for `pam_unix.so` as shown:

```
password sufficient pam_unix.so sha512
```

Notes

Additional module options may be set, recommendation only covers those listed here.
If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# cat /etc/passwd | awk -F: '( $3 >= 1000 && $1 != "nfsnobody" ) { print $1 }' | xargs -n 1 chage -d 0
```