5.4.1 Ensure password creation requirements are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_pwquality.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

The following options are set in the `/etc/security/pwquality.conf` file:

- Password Length:
  - `minlen = 14` - password must be 14 characters or more
- Password complexity:
  - `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

    OR

  - `dcredit = -1` - provide at least one digit
  - `ucredit = -1` - provide at least one uppercase character
  - `ocredit = -1` - provide at least one special character
  - `lcredit = -1` - provide at least one lowercase character

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Verify password creation requirements conform to organization policy.

Password length

Run the following command:

```
# grep '^\s*minlen\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minlen = 14
```

Password complexity

Option 1
Run the following command:

```
# grep '^\s*minclass\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
minclass = 4
```

Option 2
Run the following command:

```
# grep -E '^\s*[duol]credit\s*' /etc/security/pwquality.conf
```

Verify the output matches:

```
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

Remediation:

The following setting is a recommend example policy. Alter these values to conform to your own organization's password policies.
Run the following command to install the `pam_pwquality` module:

```
# apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy:

```
minlen = 14
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password complexity to conform to site policy:
Option 1

```
minclass = 4
```

Option 2

```
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Additional Information:

Additional module options may be set, recommendation requirements only cover including `try_first_pass` and `minlen` set to 14 or more.

NOTE: As of this writing it is not possible to customize the maximum number of retries for the creation of a password within recommended methods. The command `pam-auth-update` is used to manage certain PAM configurations via profiles, such as `/etc/pam.d/common-password`. Making a manual change to this file will cause `pam-auth-update` to overwrite it on the next run and is thus against recommendations. Alternatively, `pam_pwquality` (via `/etc/security/pwquality.conf`) fully supports the configuration of the maximum number of retries for a password change with the configuration entry `retry = XXX`. The issue is that the template `/usr/share/pam-configs/pwquality` contains `retry=3` which will override any retry setting in `/etc/security/pwquality.conf` as PAM entries takes precedence. This template file should not be modified as any package update will overwrite the change. Thus it is not possible, in any recommended way, to modify password retries.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003	TA0006	M1027