

## 5.4.1.2 Ensure minimum days between password changes is 7 or more (Scored)

### Profile Applicability

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

### Description

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

### Rationale

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

### Audit

Run the following command and verify `PASS_MIN_DAYS` is 7 or more:

```
# grep PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 7
```

Verify all users with a password have their minimum days between password change set to 7 or more:

```
# egrep ^[^\:]+\:[^\!*] /etc/shadow | cut -d: -f1
<list of users>
# chage --list <user>
Minimum number of days between password change : 7
```

### Remediation

Set the `PASS_MIN_DAYS` parameter to 7 in `/etc/login.defs`:

```
PASS_MIN_DAYS 7
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

## Notes

You can also check this setting in `/etc/shadow` directly. The 5th field should be 7 or more for all users with a password.

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/ubuntu1604/5/4/1/2>

Last update: **2017/05/04 11:14**

