

6.1.3 Ensure permissions on /etc/shadow are configured (Scored)

Profile Applicability

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

Description

The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale

If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

Audit

Run the following command and verify Uid is 0/root, Gid is <gid>/shadow, and Access is 640 or more restrictive:

```
# stat /etc/shadow  
Access: (0640/-rw-r-----) Uid: ( 0/ root) Gid: ( 42/ shadow)
```

Remediation

Run the following command to set permissions on /etc/shadow:

```
# chown root:shadow /etc/shadow  
# chmod o-rwx,g-wx /etc/shadow
```

From:

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

Permanent link:

<https://secscan.acron.pl/ubuntu1604/6/1/3>

Last update: **2017/05/04 12:53**

