5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Scored)

Profile Applicability

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

Description

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to root.

Rationale

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users.

Audit

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/ssh/sshd_config
Access: (0600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/ubuntu1604/5/2/1

Last update: **2017/05/04 10:12**