5.2.3 Ensure SSH LogLevel is set to INFO (Scored)

Profile Applicability

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

Description

The `INFO` parameter specifies that login and logout activity will be logged.

Rationale

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically *not* recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information. `INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

Audit

Run the following command and verify that output matches:

```
# grep "^LogLevel" /etc/ssh/sshd_config
LogLevel INFO
```

Remediation

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel INFO
```

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

Permanent link:
https://secscan.acron.pl/ubuntu1604/5/2/3

Last update: **2017/05/04 10:14**