

5.2.5 Ensure SSH MaxAuthTries is set to 4 or less (Scored)

Profile Applicability

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

Description

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.

Rationale

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit

Run the following command and verify that output MaxAuthTries is 4 or less:

```
# grep "^MaxAuthTries" /etc/ssh/sshd_config  
MaxAuthTries 4
```

Remediation

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

```
MaxAuthTries 4
```

From:

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

Permanent link:

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

Last update: **2017/05/04 10:26**

