

5.2.8 Ensure SSH root login is disabled (Scored)

Profile Applicability

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

Description

The PermitRootLogin parameter specifies if the root user can log in using ssh(1). The default is no.

Rationale

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit

Run the following command and verify that output matches:

```
# grep "^PermitRootLogin" /etc/ssh/sshd_config  
PermitRootLogin no
```

Remediation

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

```
PermitRootLogin no
```

From:

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

Permanent link:

<https://secscan.acron.pl/ubuntu1604/5/2/8>

Last update: **2017/05/04 10:31**

