5.2.15 Ensure SSH access is limited (Scored)

Profile Applicability

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

Description

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

AllowUsers

The `AllowUsers` variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of comma separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

AllowGroups

The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric group IDs are not recognized with this variable.

DenyUsers

The `DenyUsers` variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of comma separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

DenyGroups

The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric group IDs are not recognized with this variable.

Rationale

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit

Run the following commands and verify that output matches for at least one:

```
# grep "^AllowUsers" /etc/ssh/sshd_config
AllowUsers <userlist>
# grep "^AllowGroups" /etc/ssh/sshd_config
AllowGroups <grouplist>
# grep "^DenyUsers" /etc/ssh/sshd_config
DenyUsers <userlist>
# grep "^DenyGroups" /etc/ssh/sshd_config
DenyGroups <grouplist>
```

Remediation

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

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```