4.1.12 Ensure use of privileged commands is collected (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

Rationale

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit

Run the following command replacing <partition> with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print \ "-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F
auid!=4294967295 \ -k privileged" }'
```

Verify all resulting lines are in the `/etc/audit/audit.rules` file.

Remediation

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows:
`-F path=“ $1 ”` - will populate each file name found through the find command and processed by awk.
`-F perm=x` - will write an audit record if the file is executed.
`-F auid>=1000` - will write a record if the user executing the command is not a privileged user.

`-F auid!= 4294967295` - will ignore Daemon events

All audit records should be tagged with the identifier “privileged”.

Run the following command replacing <partition> with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print \ "-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F
auid!=4294967295 \ -k privileged" }'
```

Add all resulting lines to the `/etc/audit/audit.rules` file.