5.4.2 Ensure system accounts are non-login (Scored)

Profile Applicability

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

Description

There are a number of accounts provided with Ubuntu that are used to manage applications and are not intended to provide an interactive shell.

Rationale

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, Ubuntu sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to `/sbin/nologin`. This prevents the account from potentially being used to run any commands.

Audit

Run the following script and verify no results are returned:

```
egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" &&
$1!="shutdown" && $1!="halt" && $3<1000 && $7!="/usr/sbin/nologin" &&
$7!="/bin/false") {print}'
```

Remediation

Set the shell for any accounts returned by the audit script to `/usr/sbin/nologin`:

```
# usermod -s /usr/sbin/nologin <user>
```

The following script will automatically set all user shells required to `/usr/sbin/nologin` and lock the `sync`, `shutdown`, and `halt` users:

```
```

```
#!/bin/bash
for user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do
 if [ $user != "root" ]; then
  usermod -L $user
  if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ];
then
   usermod -s /usr/sbin/nologin $user
  fi
 fi
done
```