4.1.5 Ensure events that modify user/group information are collected (Scored)

Profile Applicability

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

Description

Record events affecting the `group`, `passwd` (user IDs), `shadow` and `gshadow` (passwords) or `/etc/security/opasswd` (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier “identity” in the audit log file.

Rationale

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit

Run the following command and verify output matches:

```
# grep identity /etc/audit/audit.rules
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Remediation

Add the following lines to the /etc/audit/audit.rules file:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
```

```
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```