4.1.3 Ensure auditing for processes that start prior to auditd is enabled (Scored)

Profile Applicability

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

Description

Configure `grub` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit

Run the following command and verify that each linux line has the `audit=1` parameter set:

```
# grep "^\s*linux" /boot/grub2/grub.cfg
enabled
```

Remediation

Edit `/etc/default/grub` and add audit=1 to GRUB_CMDLINE_LINUX:

```
GRUB_CMDLINE_LINUX="audit=1"
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig > /boot/grub2/grub.cfg
```

Notes

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.