1.1.5 Ensure noexec option set on /tmp partition (Scored)

Profile Applicability

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

Description

The noexec mount option specifies that the filesystem cannot contain executable binaries.

Rationale

Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /tmp.

Audit

If a /tmp partition exists run the following command and verify that the noexec option is set on /tmp:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to add noexec to the /tmp mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount /tmp:

```
# mount -o remount,noexec /tmp
```

Notes

`systemd` includes the `tmp.mount` service which should be used instead of configuring `/etc/fstab`. Mounting options are configured in the Options setting in `/etc/systemd/system/tmp.mount`.