3.4.5 Ensure permissions on /etc/hosts.deny are 644 (Scored)

Profile Applicability

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

Description

The `/etc/hosts.deny` file contains network information that is used by many system applications and therefore must be readable for these applications to operate.

Rationale

It is critical to ensure that the `/etc/hosts.deny` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit

Run the following command and verify `Uid` and `Gid` are both `0/root` and Access is `644`:

```
# stat /etc/hosts.deny
Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation

Run the following commands to set permissions on `/etc/hosts.deny`:

```
# chown root:root /etc/hosts.deny
# chmod 644 /etc/hosts.deny
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/centos7/3/4/5

Last update: **2017/05/05 17:08**