6.1.11 Ensure no unowned files or directories exist (Scored)

Profile Applicability

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

Description

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale

A new user who is assigned the deleted user's user ID or group ID may then end up “owning” these files, and thus have more access on the system than was intended.

Audit

Run the following command and verify no files are returned:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -
xdev -nouser
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `–local` option to df is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nouser
```

Remediation

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

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

Permanent link:
https://secscan.acron.pl/ubuntu1604/6/1/11

Last update: **2017/05/04 13:09**