

Submission File: Linux Systems Administration Homework

Ensure permissions on sensitive files

Permissions on `/etc/shadow` should allow only `root` read and write access:

- **Command to inspect permissions**:

```
ls -ld /etc/shadow
```

- **Command to Set Permissions (if needed)**:

```
sudo chmod 600 /etc/shadow
```

Permissions on `/etc/gshadow` should allow only `root` read and write access:

- **Command to inspect permissions**:

```
ls -ld /etc/gshadow
```

- **Command to Set Permissions (if needed)**:

```
sudo chmod 600 /etc/gshadow
```

Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else `read` access only:

- **Command to inspect permissions**:

```
ls -ld /etc/group
```

- **Command to Set Permissions (if needed)**:

```
sudo chmod 644 /etc/group
```

Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else `read` access only:

- **Command to inspect permissions**:

```
ls -ld /etc/passwd
```

- **Command to set permissions (if needed)**:

```
sudo chmod 644 /etc/passwd
```

Create user accounts

Add user accounts `sam`, `joe`, `amy`, `sara`, and `admin`

- **Command to add each user account (please include all 5)**:

```
sudo useradd sam
```

```
sudo useradd joe
```

```
sudo useradd amy
```

```
sudo useradd sara
```

```
sudo useradd admin
```

Force users to create 16 character passwords incorporating numbers and symbols

- **Command to edit `pwquality.conf` file**:

```
sudo vi /etc/security/pwquality.conf
```

- **Updates to configuration file**:

go to `'minlen'`

change `'8'` for `'16'`

press the `'Esc'` key

press `':'` then `'x'`

Force passwords to expire every 90 days:

- ****Command to set each new user's password to expire in 90 days (please include all 5)**:**

```
sudo chage -M 90 joe
sudo chage -M 90 sam
sudo chage -M 90 amy
sudo chage -M 90 sara
sudo chage -M 90 admin
```

Ensure that only the `admin` has general sudo access:

- ****Command to add `admin` to the `sudo` group**:**

```
sudo usermod -aG sudo admin
```

Create user group and collaborative folder

Add a `engineers` group to the system.

- ****Command**:**

```
sudo groupadd engineers
```

Add users `sam`, `joe`, `amy`, and `sara` to the managed group

- ****Command to add users to `engineers` group (please include all 4)**:**

```
sudo usermod -aG engineers sam
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy
sudo usermod -aG engineers sara
```

Create a shared folder for this group at `/home/engineers`

- ****Command to create the shared folder**:**

```
sudo mkdir -p /home/engineers/wrench
```

Change the group on the engineers directory to the `engineers` group

- ****Command to change ownership of engineer's shared folder to engineer group**:**

```
sudo chown -R sam /home/engineers/wrench
sudo chown -R amy /home/engineers/wrench
sudo chown -R sara /home/engineers/wrench
sudo chown -R joe /home/engineers/wrench
```

Add the `SGID` bit and the `sticky` bit to allow collaboration between engineers in this directory

- ****Command to set SGID and sticky bit to shared folder**:**

```
sudo chmod g+s /home/engineers/wrench
sudo chmod +t /home/engineers/wrench
```

Lynis auditing

Install and run `lynis`

- ****Command to install `lynis`**:**

```
sudo apt install lynis
```

- ****Command to see options:****

```
sudo lynis
```

- ****Command to run an audit****

```
sudo lynis audit system
```

Provide a report from `lynis` output on what more could be done to harden the system.

- ****Screenshot of report output**:**

```
=====
Lynis security scan details:

Hardening index : 55 [#####          ]
Tests performed : 241
Plugins enabled : 1

Components:
- Firewall           [V]
- Malware scanner    [V]

Lynis Modules:
- Compliance Status  [?]
- Security Audit     [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat

=====
Notice: Lynis update available
Current version : 262   Latest version : 275
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
=====
```

Bonus: Check for Root Kits

Install and run `chkrootkit`.

- ****Command to install `chkrootkit`****

```
sudo apt install chkrootkit -y
```

- **Command to see options:**

sudo /usr/sbin/chkrootkit --help

- **Command to run expert mode:**

sudo /usr/sbin/chkrootkit

- **Screenshot of End of Sample Output:**

```
! gdm      2301 tty1  /usr/lib/gnome-settings-daemon/gsd-power
! gdm      2302 tty1  /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm      2303 tty1  /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm      2306 tty1  /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm      2310 tty1  /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm      2317 tty1  /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm      2327 tty1  /usr/lib/gnome-settings-daemon/gsd-sound
! gdm      2331 tty1  /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm      2260 tty1  /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm      2218 tty1  /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm      2229 tty1  /usr/lib/ibus/ibus-dconf
! gdm      2385 tty1  /usr/lib/ibus/ibus-engine-simple
! gdm      2232 tty1  /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmIn 2540 tty2  /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmIn 2538 tty2  /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmIn 2553 tty2  /usr/lib/gnome-session/gnome-session-binary --application-service
! sysadmIn 2743 tty2  /usr/bin/gnome-shell
! sysadmIn 3917 tty2  /usr/bin/gnome-software --gapplication-service
! sysadmIn 2894 tty2  /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmIn 2895 tty2  /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmIn 2899 tty2  /usr/lib/gnome-settings-daemon/gsd-color
! sysadmIn 2900 tty2  /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmIn 2906 tty2  /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmIn 2902 tty2  /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmIn 2904 tty2  /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmIn 2909 tty2  /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmIn 2851 tty2  /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmIn 2853 tty2  /usr/lib/gnome-settings-daemon/gsd-power
! sysadmIn 2858 tty2  /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmIn 2930 tty2  /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmIn 2859 tty2  /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmIn 2860 tty2  /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmIn 2862 tty2  /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmIn 2867 tty2  /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmIn 2869 tty2  /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmIn 2871 tty2  /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmIn 2874 tty2  /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmIn 2764 tty2  /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmIn 2768 tty2  /usr/lib/ibus/ibus-dconf
! sysadmIn 3055 tty2  /usr/lib/ibus/ibus-engine-simple
! sysadmIn 2772 tty2  /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmIn 2904 tty2  nautilus-desktop
! root     13510 pts/0 /bin/sh /usr/sbin/chkrootkit
! root     14171 pts/0 ./chkutmp
! root     14173 pts/0 ps aux tty,ruser,args -o tty,pid,ruser,args
! root     14172 pts/0 sh -c ps aux "tty,ruser,args" -o "tty,pid,ruser,args"
! root     13509 pts/0 sudo /usr/sbin/chkrootkit
! sysadmIn 3144 pts/0 bash
chkutmp: nothing deleted
Checking OSX_RSPLOU...
sysadmIn@UbuntuDesktop:~$
```