

Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. **Permissions on /etc/shadow should allow only root read and write access.**
 - **Command to inspect permissions:** `ls -l /etc/shadow.`
 - **Command to set permissions (if needed):** `sudo chmod u=rw /etc/shadow`
2. **Permissions on /etc/gshadow should allow only root read and write access.**
 - **Command to inspect permissions:** `ls -l /etc/gshadow`
 - **Command to set permissions (if needed):** `sudo chmod u=rw /etc/gshadow`
3. **Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.**
 - **Command to inspect permissions:** `ls -l /etc/group`
 - **Command to set permissions (if needed):** `sudo chmod u=rw,g=r,o=r /etc/group`
4. **Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.**
 - **Command to inspect permissions:** `ls -l /etc/passwd`
 - **Command to set permissions (if needed):** `sudo chmod u=rw,g=r,o=r /etc/passwd`

Step 2: Create User Accounts

1. **Add user accounts for sam, joe, amy, sara, and admin.**
 - **Command to add each user account (include all five users):** `sudo adduser sam, sudo adduser joe, sudo adduser amy, sudo adduser sara, sudo adduser admin`
2. **Ensure that only the admin has general sudo access.**

- **Command to add admin to the sudo group:** `sudo usermod -G sudo admin` & verify with `groups admin`.

Step 3: Create User Group and Collaborative Folder

1. **Add an engineers group to the system.**
 - **Command to add group:** `sudo addgroup engineers`
2. **Add users sam, joe, amy, and sara to the managed group.**
 - **Command to add users to engineers group (include all four users):** `sudo usermod -G engineers sam, sudo usermod -G engineers joe, sudo usermod -G engineers amy, sudo usermod -G engineers sara`.
3. **Create a shared folder for this group at /home/engineers.**
 - **Command to create the shared folder:** `mkdir /home/engineers`
4. **Change ownership on the new engineers' shared folder to the engineers group.**
 - **Command to change ownership of engineer's shared folder to engineer group:** `sudo chown :engineers /home/engineers`

Step 4: Lynis Auditing

1. **Command to install Lynis:** `sudo apt install lynis` / `sudo apt upgrade lynis` (if already installed on VM and seeking upgrade to the latest version)
2. **Command to see documentation and instructions:** `man lynis`
3. **Command to run an audit:** `sudo lynis system audit`
4. Provide a report from the Lynis output on what can be done to harden the system.

- Screenshot of report output:

```
* Consider hardening SSH configuration [SSH-7408]
- Details : AllowTcpForwarding (YES --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : ClientAliveCountMax (3 --> 2)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Compression (YES --> (DELAYED|NO))
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : LogLevel (INFO --> VERBOSE)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxAuthTries (6 --> 2)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxSessions (10 --> 2)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : PermitRootLogin (WITHOUT-PASSWORD --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Port (22 --> )
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : TCPKeepAlive (YES --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (YES --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (YES --> NO)
  https://cisofy.com/controls/SSH-7408/
```

Bonus

1. **Command to install chkrootkit:** `sudo apt install chkrootkit / sudo apt upgrade chkrootkit` (if already installed on VM and seeking upgrade to the latest version)
2. **Command to see documentation and instructions:** `man chkrootkit`
3. **Command to run expert mode:** `sudo chkrootkit -x`
4. **Provide a report from the chkrootkit output on what can be done to harden the system.**

- Screenshot of end of sample output:

```
! sysadmin 3179 tty2 /usr/lib/gnome-settings-daemon/gsd-ally-settings
! sysadmin 3180 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 3176 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 3183 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 3264 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 3187 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 3189 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 3193 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 3136 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 3137 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 3141 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 3232 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 3144 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 3147 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 3149 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 3152 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 3160 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 3162 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 3168 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 3050 tty2 ibus-daemon --xim --panel disable
! sysadmin 3054 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 3349 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 3058 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 3263 tty2 nautilus-desktop
! root 4206 pts/1 /bin/sh /usr/sbin/chkrootkit -x
! root 4688 pts/1 ./chkutmp
! root 4690 pts/1 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 4689 pts/1 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 4205 pts/1 sudo chkrootkit -x
! sysadmin 3434 pts/1 bash
..
..
..
sysadmin@UbuntuDesktop:/etc$
```

○