

## ## 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 600 /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 600 /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 644 /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 644 /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 -aG sudo 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 -aG engineers sam`
- `sudo usermod -aG engineers joe`
- `sudo usermod -aG engineers amy`
- `sudo usermod -aG engineers sara`

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

- Command to create the shared folder:

- `sudo mkdir /home/engineers`

- `sudo chmod +s /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 chgrp engineers /home/engineers`

### Step 4: Lynis Auditing

1. Command to install Lynis: `sudo apt-get install lynis -y`
2. Command to see documentation and instructions: `sudo lynis`
3. Command to run an audit: `sudo lynis audit system`

4. Provide a report from the Lynis output on what can be done to harden the system.

- Screenshot of report output:

```
[+] Kernel Hardening
-----
- Comparing sysctl key pairs with scan profile
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ DIFFERENT ]
- kernel.core_uses_pid (exp: 1) [ DIFFERENT ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ DIFFERENT ]
- kernel.kptr_restrict (exp: 2) [ DIFFERENT ]
- kernel.randomize_va_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ DIFFERENT ]
- kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ DIFFERENT ]
- net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
- net.ipv4.tcp_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
- net.ipv6.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]

[+] Hardening
-----
- Installed compiler(s) [ FOUND ]
- Installed malware scanner [ FOUND ]
```

### ### Bonus

1. Command to install chkrootkit: **sudo apt install chkrootkit -y**
2. Command to see documentation and instructions: **sudo chkrootkit -h**
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      2663 tty2    /usr/bin/gnome-shell
! sysadmin      3125 tty2    /usr/bin/gnome-software --gapplication-service
! sysadmin      2828 tty2    /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin      2829 tty2    /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin      2824 tty2    /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin      2836 tty2    /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin      2893 tty2    /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin      2837 tty2    /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin      2838 tty2    /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin      2839 tty2    /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin      2787 tty2    /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin      2788 tty2    /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin      2790 tty2    /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin      2858 tty2    /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin      2791 tty2    /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin      2796 tty2    /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin      2797 tty2    /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin      2800 tty2    /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin      2804 tty2    /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin      2807 tty2    /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin      2812 tty2    /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin      2700 tty2    ibus-daemon --xim --panel disable
! sysadmin      2704 tty2    /usr/lib/ibus/ibus-dconf
! sysadmin      2965 tty2    /usr/lib/ibus/ibus-engine-simple
! sysadmin      2707 tty2    /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin      2889 tty2    nautilus-desktop
! root          27545 pts/0    /bin/sh /usr/sbin/chkrootkit -x
! root          27991 pts/0    ./chkutmp
! root          27993 pts/0    ps axk tty,ruser,args -o tty,pid,ruser,args
! root          27992 pts/0    sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root          27544 pts/0    sudo chkrootkit -x
! sysadmin      27496 pts/0    bash
chkutmp: nothing deleted
not tested
```

---