

## 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 useradd sam`  
`sudo useradd joe`

```
sudo useradd amy
sudo useradd sara
sudo useradd 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`
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 -R :engineers /home/engineers
```

### Step 4: Lynis Auditing

1. Command to install Lynis: `sudo apt-get install -y lynis`
2. Command to see documentation and instructions: `man 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:

```
Linux-Module_default_1623800831443_26593 [Running]
Mon 21:15
sysadmin@UbuntuDesktop: /home

File Edit View Search Terminal Help

Suggestions (52):
- Fix all libpam-imapc to set Ssh and Sshpass for PAM sessions [CUST-0286]
  https://your-domain.example.org/controls/CUST-0286/
- Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
  https://your-domain.example.org/controls/CUST-0285/
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
  https://your-domain.example.org/controls/CUST-0810/
- Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
  https://your-domain.example.org/controls/CUST-0811/
- Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
  https://your-domain.example.org/controls/CUST-0830/
- Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]
  https://your-domain.example.org/controls/CUST-0831/
- Install debconf to generate lists of vulnerabilities which affect this installation. [CUST-0870]
  https://your-domain.example.org/controls/CUST-0870/
- Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
  https://your-domain.example.org/controls/CUST-0875/
- Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
  https://ctiofy.com/controls/DEB-0880/
- Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  https://ctiofy.com/controls/BOOT-5122/
- Install a PAM module for password strength testing like pam_cracklib or pam_passwd. [AUTH-9202]
  https://ctiofy.com/controls/AUTH-9202/
- Configure minimum password age in /etc/login.defs [AUTH-9286]
  https://ctiofy.com/controls/AUTH-9286/
- Configure maximum password age in /etc/login.defs [AUTH-9286]
  https://ctiofy.com/controls/AUTH-9286/
- Set password for single user mode to minimize physical access attack surface [AUTH-9300]
  https://ctiofy.com/controls/AUTH-9300/
- Default weak in /etc/login.defs could be more strict like 027 [AUTH-9320]
  https://ctiofy.com/controls/AUTH-9320/
- To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]
  https://ctiofy.com/controls/FILE-6310/
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]
  https://ctiofy.com/controls/FILE-6310/
- To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]
  https://ctiofy.com/controls/FILE-6310/
- Disable drivers like USB sticks when not used, to prevent unauthorized storage or data theft [STRO-1040]
  https://ctiofy.com/controls/STRO-1040/
- Check DNS configuration for the dns domain name [NAME-4020]
  https://ctiofy.com/controls/NAME-4020/
- Purge old/removed packages (if found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7340]
  https://ctiofy.com/controls/PKGS-7340/
- Install debsums utility for the verification of packages with known good database. [PKGS-7370]
  https://ctiofy.com/controls/PKGS-7370/
- Update your system with apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
  https://ctiofy.com/controls/PKGS-7392/
- Install package apt-show-versions for patch management purposes [PKGS-7394]
  https://ctiofy.com/controls/PKGS-7394/
- Consider running ARP monitoring software (arpwatch, arpon) [NETW-3032]
  https://ctiofy.com/controls/NETW-3032/
- Access to CUPS configuration could be more strict. [PRINT-2307]
  https://ctiofy.com/controls/PRINT-2307/
- You are advised to hide the mail name (option: smtp_banner) from your postfix configuration. Use postfix -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8810]
  https://ctiofy.com/controls/MAIL-8810/
- Disable the 'vrfy' command [MAIL-8820:disable_vrfy_command]
  https://ctiofy.com/controls/MAIL-8820/disable_vrfy_command/
- Solution : Run postconf -e disable_vrfy_commands=yes to change the value
  https://ctiofy.com/controls/MAIL-8820/disable_vrfy_commands/
- Check iptables rules to see which rules are currently not used [FIRE-4513]
  https://ctiofy.com/controls/FIRE-4513/
- Install Apache mod_evasive to guard webserver against DOS/brute force attempts [HTTP-6640]
  https://ctiofy.com/controls/HTTP-6640/
- Install Apache mod_security to guard webserver against web application attacks [HTTP-6643]
  https://ctiofy.com/controls/HTTP-6643/

Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls tests (https://ctiofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

Lynis security scan details:
Hardening index : 57 [#####]
Tests performed : 240
Plugins enabled : 1

Components:
Firewall
```

```
Linux-Module_default_1623800831443_26593 [Running]
Mon 21:16
sysadmin@UbuntuDesktop: /home

File Edit View Search Terminal Help

- Install Apache mod_security to guard webserver against web application attacks [HTTP-6643]
  https://ctiofy.com/controls/HTTP-6643/
- Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]
  https://ctiofy.com/controls/HTTP-6710/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o PasswordAuthentication no
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o PermitTTY no
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o X11Forwarding no
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o MaxAuthTries 3
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o MaxSessions 10
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o LogLevel INFO
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o StrictModes 100
  https://ctiofy.com/controls/SSH-7400/
- Consider hardening SSH configuration [SSH-7400]
  Details : ssh -o UsePrivilegeSeparation yes
  https://ctiofy.com/controls/SSH-7400/
- Check what deleted files are still in use and why. [LOGG-2190]
  https://ctiofy.com/controls/LOGG-2190/
- Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7120]
  https://ctiofy.com/controls/BANN-7120/
- Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
  https://ctiofy.com/controls/BANN-7130/
- Enable process accounting [ACCT-9622]
  https://ctiofy.com/controls/ACCT-9622/
- Enable sysstat to collect accounting (no results) [ACCT-9620]
  https://ctiofy.com/controls/ACCT-9620/
- Enable auditd to collect audit information [ACCT-9628]
  https://ctiofy.com/controls/ACCT-9628/
- Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
  https://ctiofy.com/controls/CONT-8104/
- One or more sysctl values differ from the scan profile and could be tweaked [KNLN-6000]
  Solution : Change sysctl value or disable test (skip-test=KNLN-6000=sysctl-key)
  https://ctiofy.com/controls/KNLN-6000/
- Harden compilers like restricting access to root user only [IRON-7222]
  https://ctiofy.com/controls/IRON-7222/

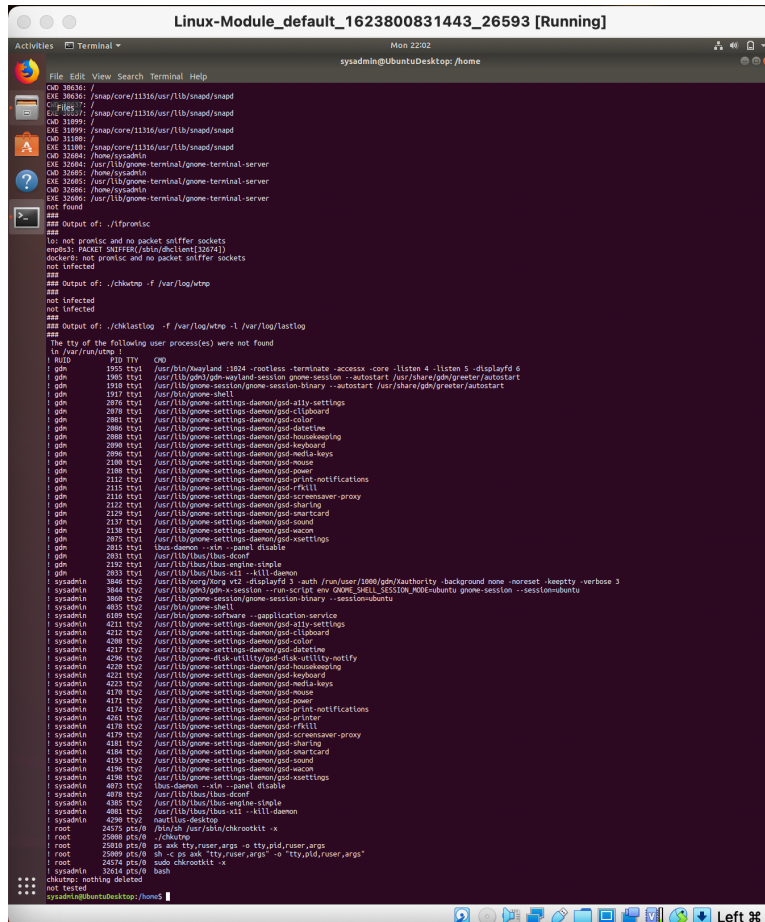
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls tests (https://ctiofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

Lynis security scan details:
Hardening index : 57 [#####]
Tests performed : 240
Plugins enabled : 1

Components:
Firewall
```

## Bonus

1. Command to install chkrootkit: `sudo apt-get install chkrootkit -y`
2. Command to see documentation and instructions: `man chkrootkit`
3. Command to run expert mode: `sudo chkrootkit -x`
4. Provide a report from the chrootkit output on what can be done to harden the system.
  - Screenshot of end of sample output:



```
Linux-Module_default_1623800831443_26593 [Running]
Mon 22:02
sysadmin@UbuntuDesktop:/home

*** Output of: ./ifpromisc
***
lo: not promisc and no packet sniffer sockets
vnet0: PACKET sniffer (driver:ixgbevf)
docker0: not promisc and no packet sniffer sockets
not infected
***

*** Output of: ./chkrootmp -f /var/log/vtmp
***
not infected
not infected
***

*** Output of: ./chkrootlog -f /var/log/vtmp -l /var/log/lastlog
***

The tty of the following user process(es) were not found
in /var/run/vtmp: 1
1 1000 tty /usr/bin/mx4linux -H24 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
1 1000 tty /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
1 1000 tty /usr/lib/gnome-shell
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-ally-settings
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-clipboard
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-color
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-datetime
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-housekeeping
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-keyboard
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-media-keys
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-mouse
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-power
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-print-notifications
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-rxll
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-sharing
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-smartcard
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-sound
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-wacom
1 1000 tty /usr/lib/gnome-settings-daemon/gsd-xsettings
1 1000 tty dbus-daemon -x11 --panel disable
1 1000 tty /usr/lib/ibus/ibus-dconf
1 1000 tty /usr/lib/ibus/ibus-engine-single
1 1000 tty /usr/lib/ibus/ibus-x11 --kill-daemon
1 sysadmin 3844 tty2 /usr/lib/gdm/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
1 sysadmin 3844 tty2 /usr/lib/gdm/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
1 sysadmin 4035 tty2 /usr/bin/gnome-shell
1 sysadmin 4198 tty2 /usr/lib/gnome-software --application-service
1 sysadmin 4211 tty2 /usr/lib/gnome-settings-daemon/gsd-ally-settings
1 sysadmin 4212 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
1 sysadmin 4280 tty2 /usr/lib/gnome-settings-daemon/gsd-color
1 sysadmin 4281 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
1 sysadmin 4286 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
1 sysadmin 4288 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
1 sysadmin 4221 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
1 sysadmin 4222 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
1 sysadmin 4170 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
1 sysadmin 4171 tty2 /usr/lib/gnome-settings-daemon/gsd-power
1 sysadmin 4174 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
1 sysadmin 4201 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
1 sysadmin 4178 tty2 /usr/lib/gnome-settings-daemon/gsd-rxll
1 sysadmin 4179 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
1 sysadmin 4181 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
1 sysadmin 4184 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
1 sysadmin 4185 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
1 sysadmin 4186 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
1 sysadmin 4196 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
1 sysadmin 4073 tty2 dbus-daemon -x11 --panel disable
1 sysadmin 4078 tty2 /usr/lib/ibus/ibus-dconf
1 sysadmin 4385 tty2 /usr/lib/ibus/ibus-engine-single
1 sysadmin 4081 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
1 sysadmin 4290 tty2 nautilus-desktop
1 root 24375 pts/0 /bin/bash /usr/sbin/chkrootkit -x
1 root 25048 pts/0 /usr/bin/chkrootkit
1 root 25048 pts/0 ps aux tty,user,args -s tty,pid,user,args
1 root 25049 pts/0 sh -c ps aux 'tty,user,args' -s 'tty,pid,user,args'
1 root 24374 pts/0 sudo chkrootkit -x
1 sysadmin 3264 pts/0 bash
chkrootkit: nothing deleted
***
not infected
sysadmin@UbuntuDesktop:/home/
```