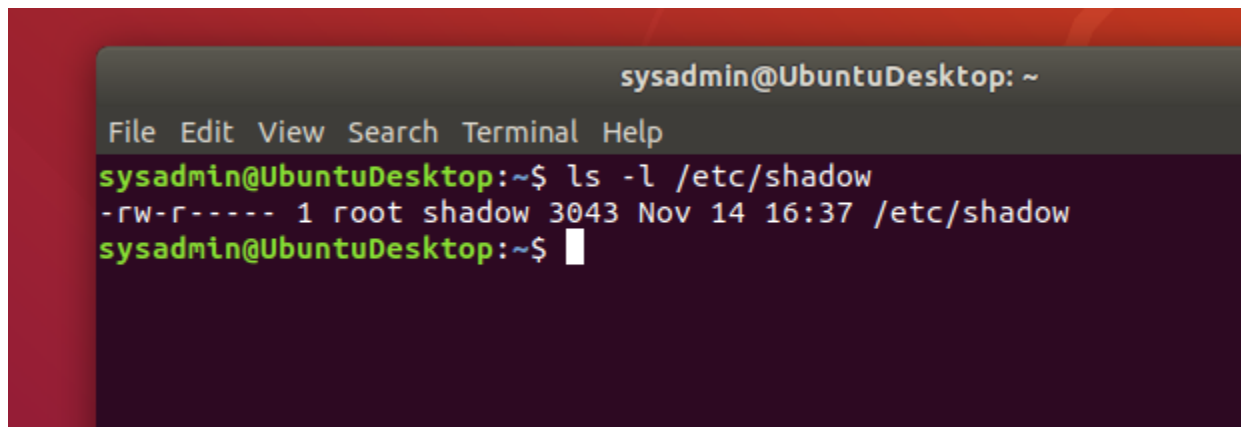


Week 4 Homework: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

- Permissions on /etc/shadow should allow only root read and write access.
- Command to inspect permissions:

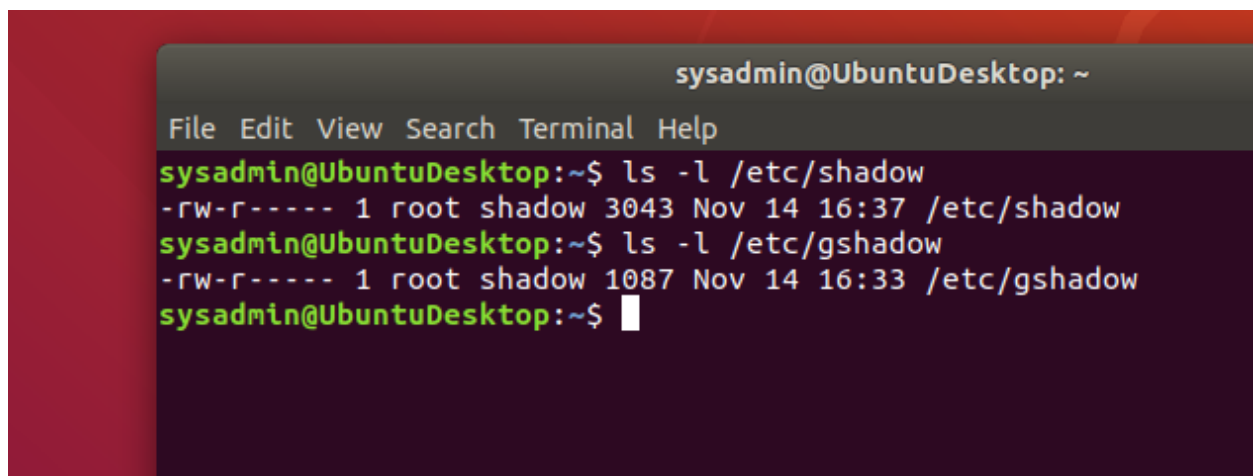


```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow  
-rw-r----- 1 root shadow 3043 Nov 14 16:37 /etc/shadow  
sysadmin@UbuntuDesktop:~$
```

- Command to set permissions (if needed): **Not required as permissions are correct.**

- Permissions on /etc/gshadow should allow only root read and write access.

- Command to inspect permissions:



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow  
-rw-r----- 1 root shadow 3043 Nov 14 16:37 /etc/shadow  
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow  
-rw-r----- 1 root shadow 1087 Nov 14 16:33 /etc/gshadow  
sysadmin@UbuntuDesktop:~$
```

- Command to set permissions (if needed): **Not required as permissions are correct.**

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

- Command to inspect permissions

```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow  
-rw-r----- 1 root shadow 3043 Nov 14 16:37 /etc/shadow  
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow  
-rw-r----- 1 root shadow 1087 Nov 14 16:33 /etc/gshadow  
sysadmin@UbuntuDesktop:~$ ls -l /etc/group  
-rw-r--r-- 1 root root 1318 Nov 14 16:33 /etc/group  
sysadmin@UbuntuDesktop:~$
```

- Command to set permissions (if needed): **Not required as permissions are correct.**

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

- Command to inspect permissions:

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/group  
-rw-r--r-- 1 root root 1318 Nov 14 16:33 /etc/group  
sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd  
-rw-r--r-- 1 root root 3315 Nov 14 16:37 /etc/passwd  
sysadmin@UbuntuDesktop:~$
```

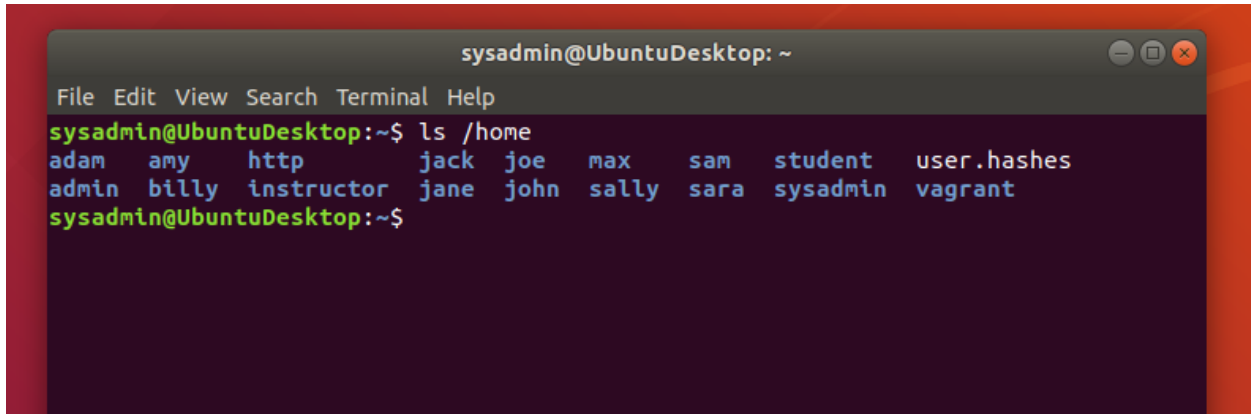
- Command to set permissions (if needed): **Not required as permissions are correct**

Step 2: Create User Accounts

- Add user accounts for sam, joe, amy, sara, and admin.
 - Command to add each user account (include all five users):
 - Add one user:

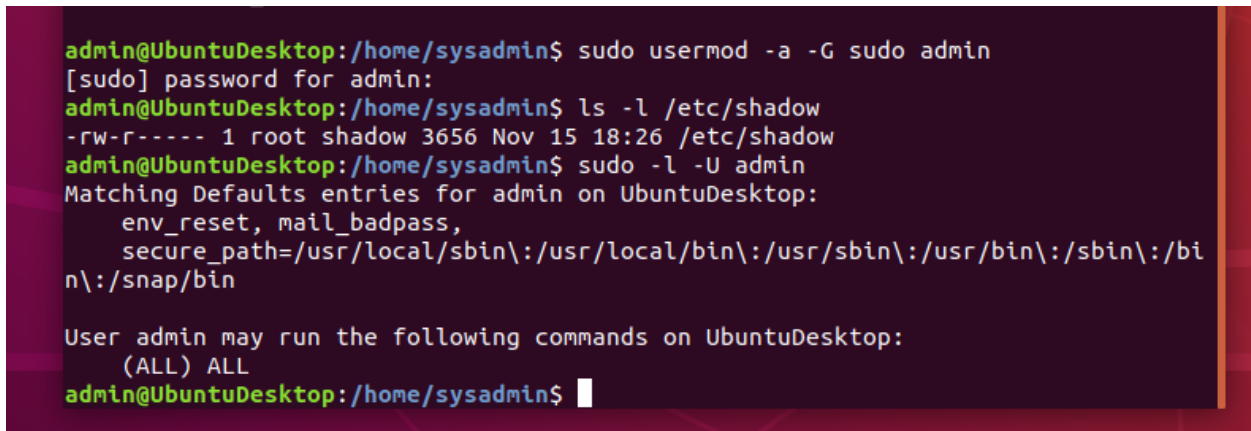
```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
passwd: password updated successfully  
Changing the user information for amy  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
sysadmin@UbuntuDesktop:~$ sudo adduser sara  
Adding user `sara' ...  
Adding new group `sara' (1018) ...  
Adding new user `sara' (1016) with group `sara' ...  
Creating home directory `/home/sara' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Changing the user information for sara  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
sysadmin@UbuntuDesktop:~$ sudo adduser admin  
Adding user `admin' ...  
Adding new group `admin' (1019) ...  
Adding new user `admin' (1017) with group `admin' ...  
Creating home directory `/home/admin' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
Sorry, passwords do not match  
passwd: Authentication token manipulation error  
passwd: password unchanged  
Try again? [y/N]  
Changing the user information for admin  
Enter the new value, or press ENTER for the default  
    Full Name []:  
    Room Number []:  
    Work Phone []:  
    Home Phone []:  
    Other []:  
Is the information correct? [Y/n] y  
sysadmin@UbuntuDesktop:~$
```

- All Users

A terminal window titled 'sysadmin@UbuntuDesktop: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'ls /home' has been executed, displaying a list of files and directories in the /home directory. The output is as follows:

```
sysadmin@UbuntuDesktop:~$ ls /home
adam  amy    http    jack   joe    max    sam    student  user.hashes
admin billy  instructor jane   john   sally  sara   sysadmin  vagrant
sysadmin@UbuntuDesktop:~$
```

- Ensure that only the admin has general sudo access.
 - Command to add admin to the sudo group:

A terminal window showing the process of adding the 'admin' user to the 'sudo' group. The user 'admin' is at the prompt '/home/sysadmin\$'. The command 'sudo usermod -a -G sudo admin' is entered, followed by the password prompt '[sudo] password for admin:'. Then, 'ls -l /etc/shadow' is run, showing permissions for the shadow file. Finally, 'sudo -l -U admin' is run, displaying the matching defaults and the commands that can be run as 'admin'.

```
admin@UbuntuDesktop:/home/sysadmin$ sudo usermod -a -G sudo admin
[sudo] password for admin:
admin@UbuntuDesktop:/home/sysadmin$ ls -l /etc/shadow
-rw-r----- 1 root shadow 3656 Nov 15 18:26 /etc/shadow
admin@UbuntuDesktop:/home/sysadmin$ sudo -l -U admin
Matching Defaults entries for admin on UbuntuDesktop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on UbuntuDesktop:
    (ALL) ALL
admin@UbuntuDesktop:/home/sysadmin$
```

Admin has all access to general sudo access.

Command: sudo usermod -a -G sudo admin

admin@UbuntuDesktop: /home/sysadmin

File Edit View Search Terminal Help

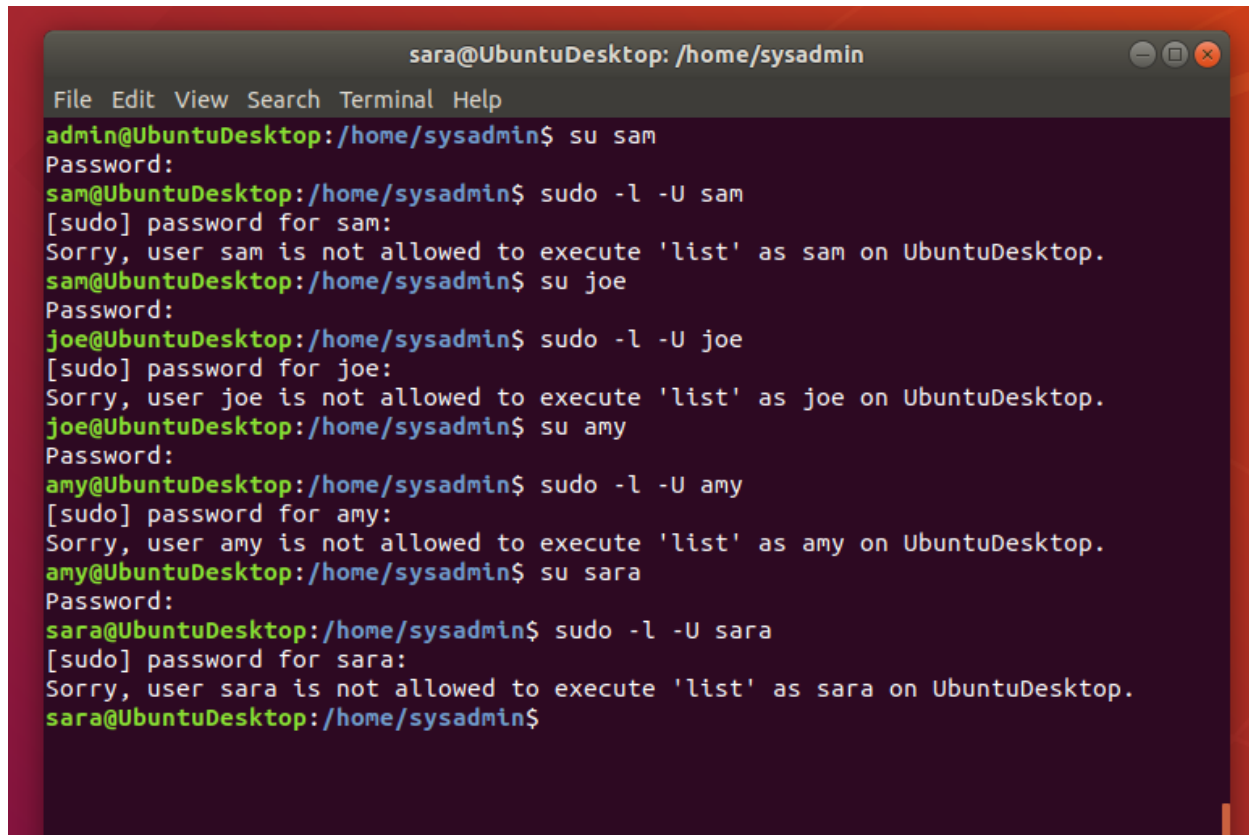
GNU nano 2.9.3

/etc/sudoers.tmp

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:$
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
vagrant ALL=(ALL:ALL) NOPASSWD:ALL
tripwire ALL=NOPASSWD: /usr/sbin/tripwire
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL
#
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
#
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
max     ALL=(ALL:ALL) /usr/bin/less
```

^G Get Help	^O Write Out	^W Where Is	^K Cut Text	^J Justify	^C Cur Pos
^X Exit	^R Read File	^_\ Replace	^U Uncut Text	^T To Spell	^_ Go To Line

Other users not allowed to sudo access

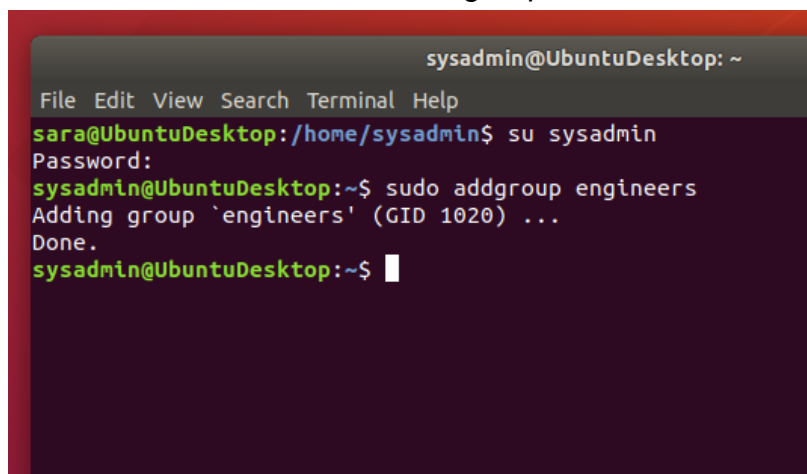


A terminal window titled 'sara@UbuntuDesktop: /home/sysadmin' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a series of commands and their outputs:

```
sara@UbuntuDesktop: /home/sysadmin$ su sam
Password:
sam@UbuntuDesktop: /home/sysadmin$ sudo -l -U sam
[sudo] password for sam:
Sorry, user sam is not allowed to execute 'list' as sam on UbuntuDesktop.
sam@UbuntuDesktop: /home/sysadmin$ su joe
Password:
joe@UbuntuDesktop: /home/sysadmin$ sudo -l -U joe
[sudo] password for joe:
Sorry, user joe is not allowed to execute 'list' as joe on UbuntuDesktop.
joe@UbuntuDesktop: /home/sysadmin$ su amy
Password:
amy@UbuntuDesktop: /home/sysadmin$ sudo -l -U amy
[sudo] password for amy:
Sorry, user amy is not allowed to execute 'list' as amy on UbuntuDesktop.
amy@UbuntuDesktop: /home/sysadmin$ su sara
Password:
sara@UbuntuDesktop: /home/sysadmin$ sudo -l -U sara
[sudo] password for sara:
Sorry, user sara is not allowed to execute 'list' as sara on UbuntuDesktop.
sara@UbuntuDesktop: /home/sysadmin$
```

Step 3: Create User Group and Collaborative Folder

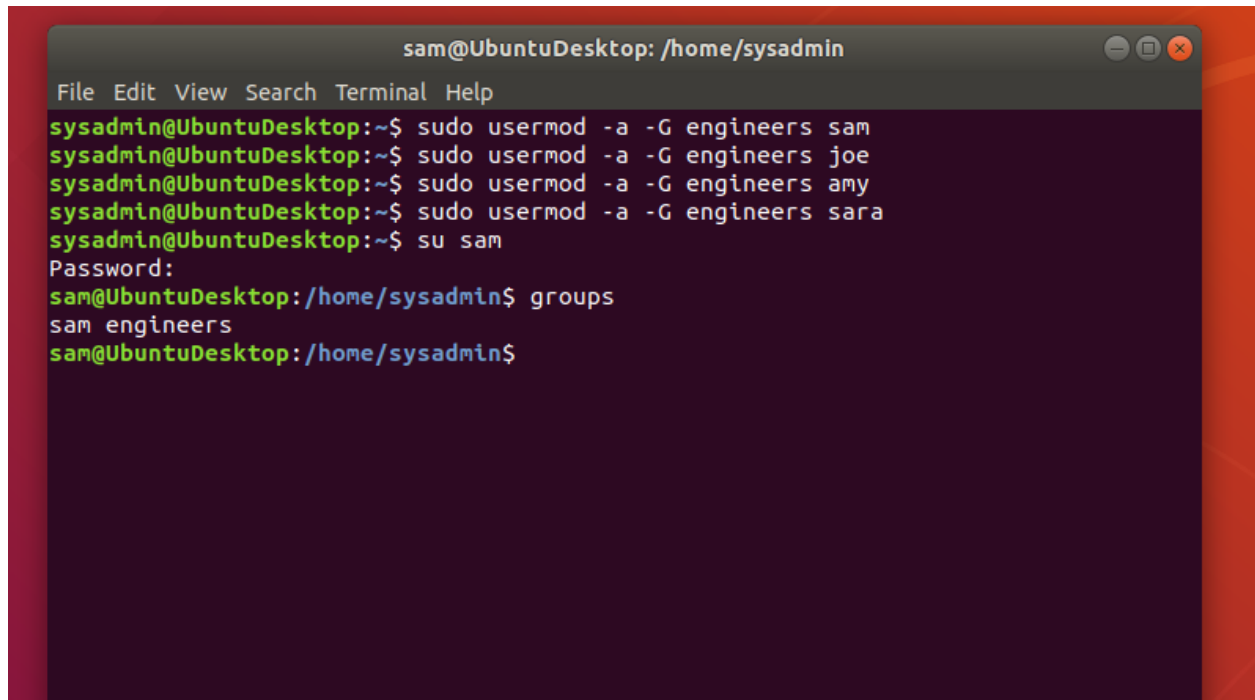
- Add an engineers group to the system.
- Command to add group:



A terminal window titled 'sysadmin@UbuntuDesktop: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and outputs:

```
sysadmin@UbuntuDesktop: ~$ su sysadmin
Password:
sysadmin@UbuntuDesktop: ~$ sudo addgroup engineers
Adding group 'engineers' (GID 1020) ...
Done.
sysadmin@UbuntuDesktop: ~$
```

- Add users sam, joe, amy, and sara to the managed group.
 - Command to add users to engineers group (include all four users)
 - sysadmin@UbuntuDesktop:~\$ sudo usermod -a -G engineers sam
 - sysadmin@UbuntuDesktop:~\$ sudo usermod -a -G engineers joe
 - sysadmin@UbuntuDesktop:~\$ sudo usermod -a -G engineers amy
 - sysadmin@UbuntuDesktop:~\$ sudo usermod -a -G engineers sara
 - sysadmin@UbuntuDesktop:~\$ su sam
 - Password:
 - sam@UbuntuDesktop:/home/sysadmin\$ groups
 - sam engineers



```
sam@UbuntuDesktop: /home/sysadmin
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo usermod -a -G engineers sam
sysadmin@UbuntuDesktop:~$ sudo usermod -a -G engineers joe
sysadmin@UbuntuDesktop:~$ sudo usermod -a -G engineers amy
sysadmin@UbuntuDesktop:~$ sudo usermod -a -G engineers sara
sysadmin@UbuntuDesktop:~$ su sam
Password:
sam@UbuntuDesktop:/home/sysadmin$ groups
sam engineers
sam@UbuntuDesktop:/home/sysadmin$
```

- Create a shared folder for this group at /home/engineers.
- Command to create the shared folder:

```

sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ cd /home
sysadmin@UbuntuDesktop:/home$ ls
adam  amy    http    jack   joe    max    sam    student  user.hashes
admin billy  instructor jane   john  sally  sara  sysadmin vagrant
sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers
sysadmin@UbuntuDesktop:/home$ ls
adam  billy    instructor  joe    sally  student  vagrant
admin engineers jack        john   sam    sysadmin
amy   http     jane        max    sara   user.hashes
sysadmin@UbuntuDesktop:/home$

```

Change ownership of the new engineers' shared folder to the engineers group.

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

sudo chgrp -R engineers /home/engineers/

Or

sudo chown root:engineers /home/engineers/

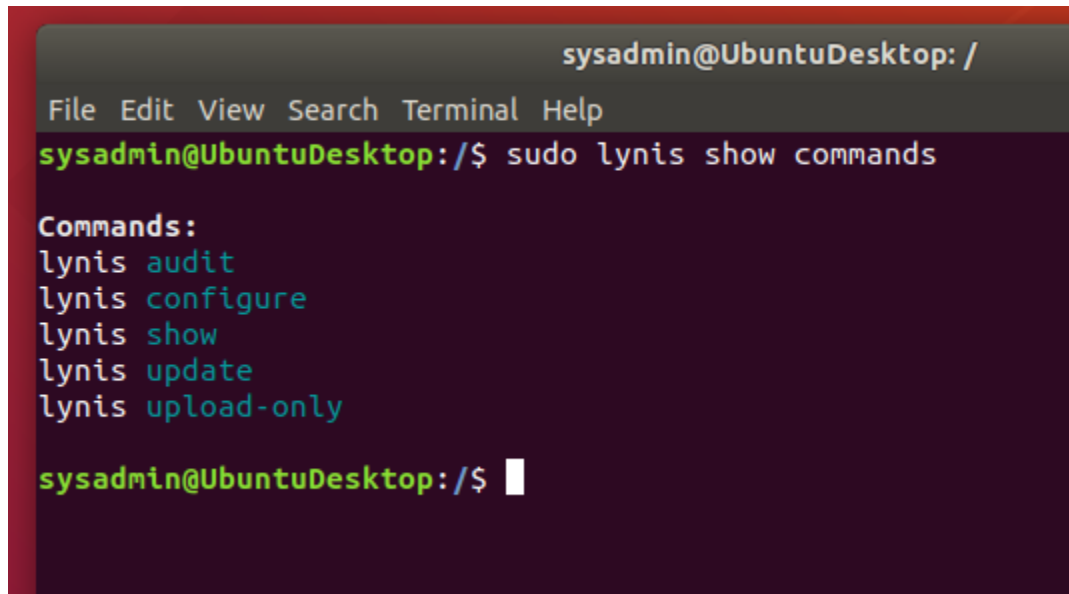
```

sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/home$ sudo chgrp -R engineers /home/engineers/
sysadmin@UbuntuDesktop:/home$ ls -l
total 76
drwxr-xr-x  8 adam      adam      4096 Oct  2 15:09 adam
drwxr-xr-x  8 admin     admin     4096 Nov 15 18:27 admin
drwxr-xr-x  8 amy       amy       4096 Nov 15 18:17 amy
drwxr-xr-x  8 billy    billy    4096 Oct  2 15:09 billy
drwxr-xr-x  2 root     engineers 4096 Nov 15 18:47 engineers
drwxr-xr-x  8 http     http     4096 Oct  2 15:09 http
drwxr-xr-x  8 instructor instructor 4096 Oct  2 14:58 instructor
drwxr-xr-x  8 jack     jack     4096 Oct  2 15:09 jack
drwxr-xr-x  8 jane     jane     4096 Oct  2 15:13 jane
drwxr-xr-x  8 joe      joe      4096 Nov 15 18:16 joe
drwxr-xr-x  8 john     john     4096 Oct  2 15:09 john
drwxr-xr-x  8 max      max      4096 Oct  2 15:09 max
drwxr-xr-x  8 sally    sally    4096 Oct  2 15:09 sally
drwxr-xr-x  9 sam      sam      4096 Nov 15 18:25 sam
drwxr-xr-x  8 sara     sara     4096 Nov 15 18:17 sara
drwxr-xr-x  8 student  student  4096 Oct  2 14:58 student
drwxr-xr-x 17 sysadmin sysadmin 4096 Nov 15 18:09 sysadmin
-rw-r--r--  1 root     root     1594 Oct  2 15:09 user.hashes
drwxr-xr-x 10 vagrant  vagrant  4096 Oct  2 15:27 vagrant

```


Step 4: Lynis Auditing

- Command to install Lynis: **sudo apt install lynis**
- Command to see documentation and instructions

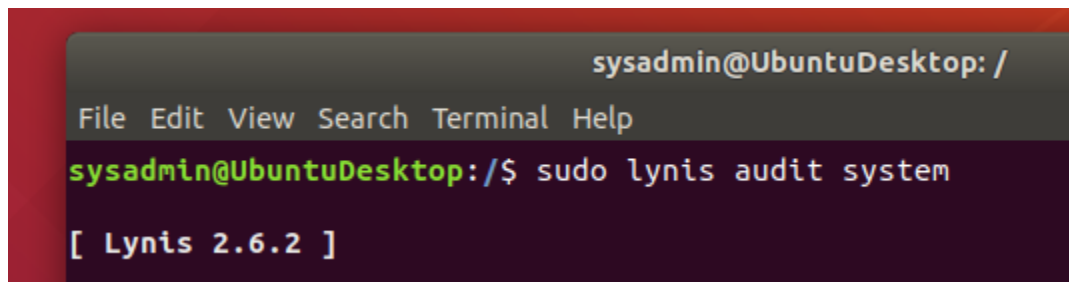
A terminal window titled 'sysadmin@UbuntuDesktop: /' with a menu bar 'File Edit View Search Terminal Help'. The prompt is 'sysadmin@UbuntuDesktop:/\$' and the command 'sudo lynis show commands' has been entered. The output lists the following commands: 'lynis audit', 'lynis configure', 'lynis show', 'lynis update', and 'lynis upload-only'. The prompt is now 'sysadmin@UbuntuDesktop:/\$' with a cursor.

```
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/$ sudo lynis show commands

Commands:
lynis audit
lynis configure
lynis show
lynis update
lynis upload-only

sysadmin@UbuntuDesktop:/$
```

- Command to run an audit:

A terminal window titled 'sysadmin@UbuntuDesktop: /' with a menu bar 'File Edit View Search Terminal Help'. The prompt is 'sysadmin@UbuntuDesktop:/\$' and the command 'sudo lynis audit system' has been entered. The output shows '[Lynis 2.6.2]'.

```
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/$ sudo lynis audit system

[ Lynis 2.6.2 ]
```

- Provide a report from the Lynis output on what can be done to harden the system.
- Screenshot of end of sample output: inside the homework/Lynis folder , here is the link below , 17 images and 1 Report text

[Lynis Screenshot of Report Output Folder](#)
[Lynis Report Text File](#)

what can be done to harden the system:

-Lynis update is available , we can update to a newer version which makes it more secure and gives better results.

Current version is 262

Latest version is 301

- Warning on Linux single user mode authentication, we can make it more secure maybe

-USB ports are enable, maybe we can disable them to make the system more secure

-Found error of vulnerable packages , i think to updating system will solve this problem

-Found a lot of errors on Kernel Hardening, this might be serious and maybe can be fixed with updating the version

And some extra errors at the end

! Version of Lynis is very old and should be updated [LYNIS]

<https://cisofy.com/controls/LYNIS/>

! No password set for single mode [AUTH-9308]

<https://cisofy.com/controls/AUTH-9308/>

! Found one or more vulnerable packages. [PKGS-7392]

<https://cisofy.com/controls/PKGS-7392/>

! Found some information disclosure in SMTP banner (OS or software name)
[MAIL-8818]

<https://cisofy.com/controls/MAIL-8818/>

And lots of suggestions (54) to make the system better.

Bonus

- Command to install chkrootkit:

```
sysadmin@UbuntuDesktop: /
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:/$ chkrootkit

Command 'chkrootkit' not found, but can be installed with:

sudo apt install chkrootkit

sysadmin@UbuntuDesktop:/$ sudo apt install chkrootkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0
 gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
 gir1.2-gudev-1.0 gir1.2-udisks-2.0 gir1.2-unity-5.0 grilo-plugins-0.3-base
 gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-locale1.65.1 libcdr-0.1-1
 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcolamd2
 libdazzle-1.0-0 libe-book-0.1-1 libdataserverui-1.2-2 libeot0
 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14
 libfreerdp-client2-2 libfreerdp2-2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0
 libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1
 liblirc-client0 libmediaart-2.0-0 libmsspub-0.1-1 libodfgen-0.1-1 libqqwing2v5
 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5
 libvncclient1 libwinpr2-2 libxmlsec1 libxmlsec1-nss lp-solve
 media-player-info python3-debconf python3-debian python3-mako
 python3-markupsafe syslinux syslinux-common syslinux-legacy
 update-notifier-common usb-creator-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
 chkrootkit
0 upgraded, 1 newly installed, 0 to remove and 391 not upgraded.
Need to get 318 kB of archives.
After this operation, 1,013 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 chkrootkit
amd64 0.52-1ubuntu0.1 [318 kB]
Fetched 318 kB in 1s (435 kB/s)
Preconfiguring packages ...
Selecting previously unselected package chkrootkit.
(Reading database ... 143525 files and directories currently installed.)
Preparing to unpack .../chkrootkit_0.52-1ubuntu0.1_amd64.deb ...
Unpacking chkrootkit (0.52-1ubuntu0.1) ...
Setting up chkrootkit (0.52-1ubuntu0.1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
sysadmin@UbuntuDesktop:/$
```

- Command to see documentation and instructions:

```
sysadmin@UbuntuDesktop:/$ sudo chkrootkit -h
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
    -h          show this help and exit
    -V          show version information and exit
    -l          show available tests and exit
    -d          debug
    -q          quiet mode
    -x          expert mode
    -e          exclude known false positive files/dirs, quoted,
                space separated, READ WARNING IN README
    -r dir      use dir as the root directory
    -p dir1:dir2:dirN path for the external commands used by chkrootkit
    -n          skip NFS mounted dirs
sysadmin@UbuntuDesktop:/$
```

- Command to run expert mode: **sudo chkrootkit -x**

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
! gdm 2282 tty1 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm 2287 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2293 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2294 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2303 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2237 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2190 tty1 ibus-daemon --xim --panel disable
! gdm 2197 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2356 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2200 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 19231 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/
Xauthority -background none -noreset -keeppty -verbose 3
! sysadmin 19229 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESS
ION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 19250 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 19439 tty2 /usr/bin/gnome-shell
! sysadmin 19886 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 19594 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 19595 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 19592 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 19600 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 19690 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 19601 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 19603 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 19606 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 19552 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 19553 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 19557 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 19638 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 19558 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 19560 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 19564 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 19569 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 19570 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 19573 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 19576 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 19464 tty2 ibus-daemon --xim --panel disable
! sysadmin 19468 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 19757 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 19470 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 19679 tty2 nautilus-desktop
! root 32551 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 547 pts/0 ./chkutmp
! root 551 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 549 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 32550 pts/0 sudo chkrootkit -x
! sysadmin 32540 pts/0 bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:~$
```

sudo chkrootkit -x > /home/sysadmin/report-chkrootkit.txt

```
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -x > /home/sysadmin/report-chkrootkit.txt
/usr/sbin/chkrootkit: 608: /usr/sbin/chkrootkit: exportmode_output: not found
/usr/sbin/chkrootkit: 609: /usr/sbin/chkrootkit: exportmode_output: not found
ls -lsysadmin@UbuntuDesktop:~$ ls -l
total 1144
drwxr-xr-x 3 sysadmin sysadmin 4096 Oct 2 15:22 Cybersecurity-Lesson-Plans
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Desktop
drwxr-xr-x 6 sysadmin sysadmin 4096 Oct 2 15:22 Documents
drwxr-xr-x 2 sysadmin sysadmin 4096 Oct 2 15:23 Downloads
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Music
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Pictures
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Public
drwxr-xr-x 5 sysadmin sysadmin 4096 Oct 2 15:26 python
-rw-rw-r-- 1 sysadmin sysadmin 1127092 Nov 15 19:28 report-chkrootkit.txt
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Templates
drwxr-xr-x 2 sysadmin sysadmin 4096 Nov 12 2019 Videos
sysadmin@UbuntuDesktop:~$
```

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

- Screenshot of end of sample output:

[Chkrootkit Report Text File](#)

what can be done to harden the system: Chkrootkit is a free tool and i think every sysadmin should use it. According to my research on the internet , chkrootkit detects any rootkit infection. There are some important phrases like “infected , Not Infected, Not Found” etc.

```
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -x | grep infected
not infected
not infected
/usr/sbin/chkrootkit: 608: /usr/sbin/chkrootkit: exportmode_output: not found
/usr/sbin/chkrootkit: 609: /usr/sbin/chkrootkit: exportmode_output: not found
not infected
not infected
not infected
! sysadmin      3507 pts/1  grep --color=auto infected
sysadmin@UbuntuDesktop:~$
```