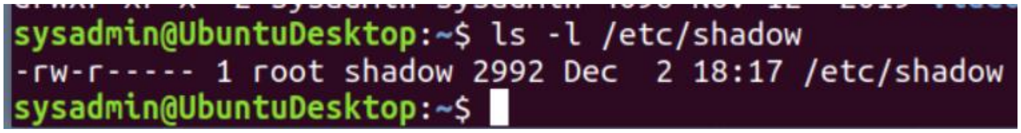
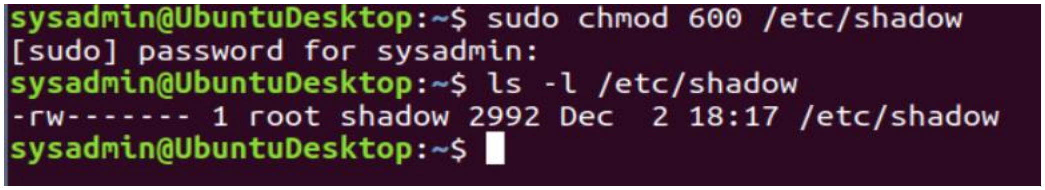
Week 4 _ Linux Systems Administration

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): shows at 640 will change to 600

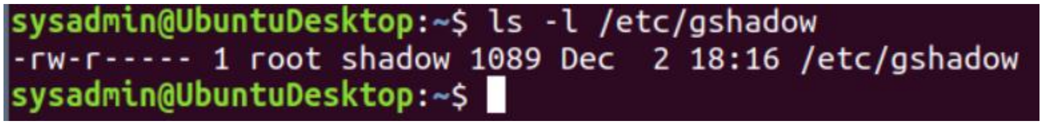


```
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 2992 Dec  2 18:17 /etc/shadow
sysadmin@UbuntuDesktop:~$ 
```



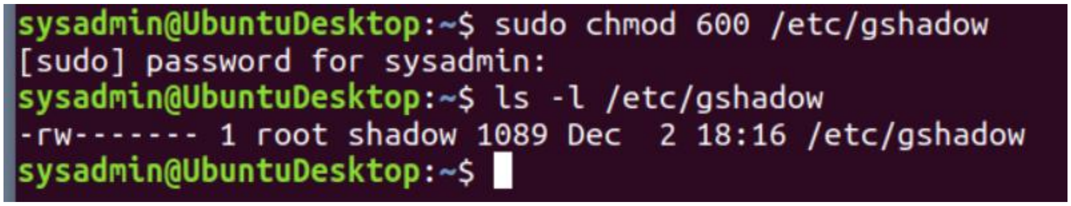
```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/shadow
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw------- 1 root shadow 2992 Dec  2 18:17 /etc/shadow
sysadmin@UbuntuDesktop:~$ 
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access. (640) >(600)
    - Command to inspect permissions: ls -1 /etc/



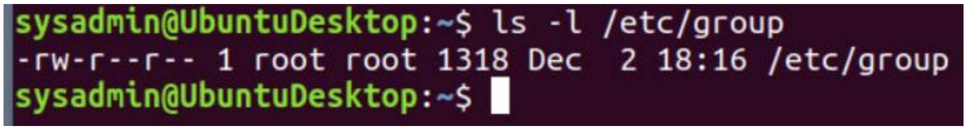
```
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw-r----- 1 root shadow 1089 Dec  2 18:16 /etc/gshadow
sysadmin@UbuntuDesktop:~$ 
```

- Command to set permissions (if needed): sudo chmod 600 /etc/gshadow

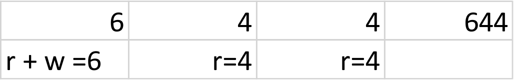


```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/gshadow
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw------- 1 root shadow 1089 Dec  2 18:16 /etc/gshadow
sysadmin@UbuntuDesktop:~$ 
```

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



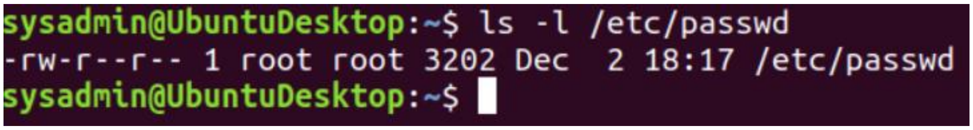
```
sysadmin@UbuntuDesktop:~$ ls -l /etc/group
-rw-r--r-- 1 root root 1318 Dec  2 18:16 /etc/group
sysadmin@UbuntuDesktop:~$ 
```



6	4	4	644
r + w =6	r=4	r=4	

- Command to set permissions (if needed): sudo chmod 644 group -R (not need to change

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

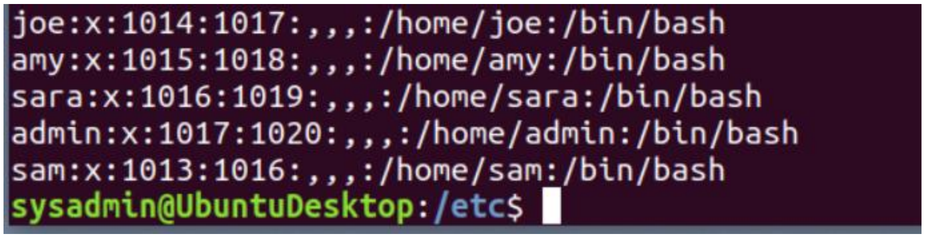


```
sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3202 Dec  2 18:17 /etc/passwd
sysadmin@UbuntuDesktop:~$ 
```

    - Command to set permissions (if needed): no need to modify

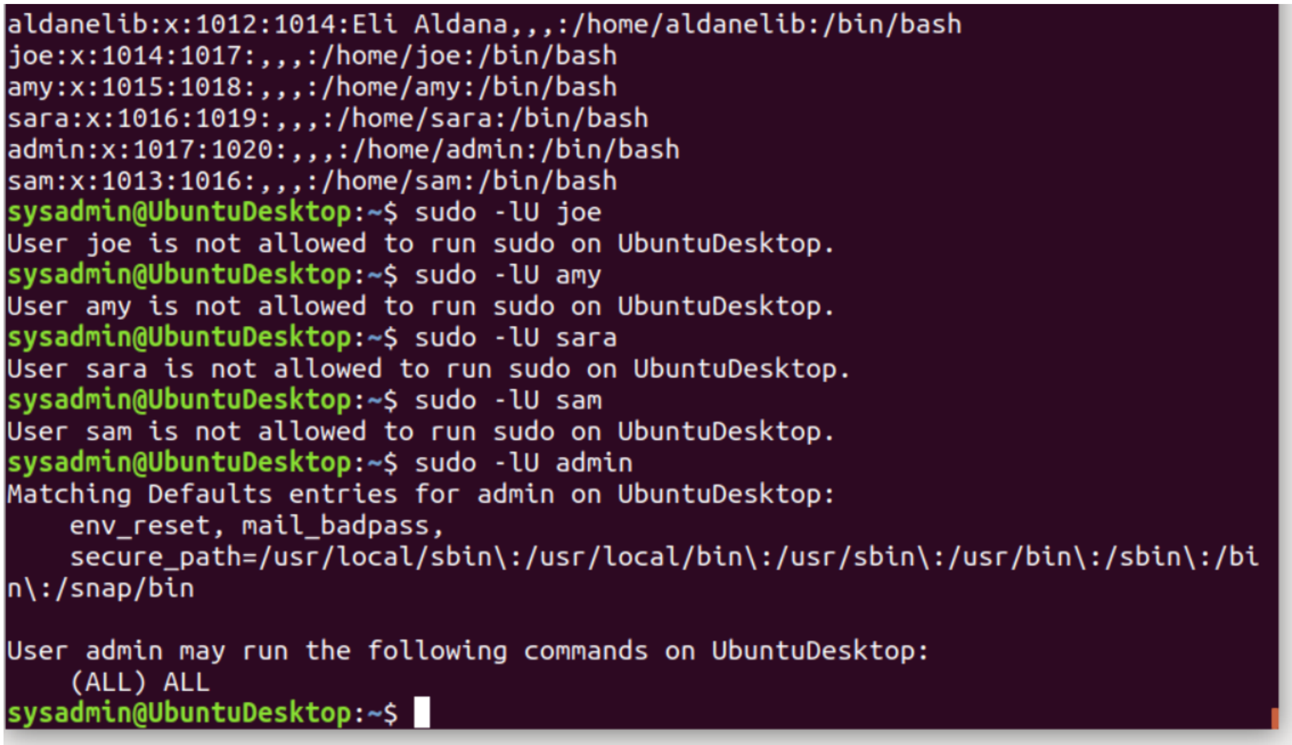
Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin`.



```
joe:x:1014:1017:,,,:/home/joe:/bin/bash
amy:x:1015:1018:,,,:/home/amy:/bin/bash
sara:x:1016:1019:,,,:/home/sara:/bin/bash
admin:x:1017:1020:,,,:/home/admin:/bin/bash
sam:x:1013:1016:,,,:/home/sam:/bin/bash
sysadmin@UbuntuDesktop:/etc$ 
```

    - Command to add each user account (include all five users):
        - sysadmin@UbuntuDesktop:/etc$ sudo adduser sam
        - sysadmin@UbuntuDesktop:/etc$ sudo adduser admin
        - sysadmin@UbuntuDesktop:/etc$ sudo adduser sara
        - sysadmin@UbuntuDesktop:/etc$ sudo adduser amy
        - sysadmin@UbuntuDesktop:/etc$ sudo adduser joe
2. Ensure that only the `admin` has general sudo access.
    - Checked all users – sudo -lU unsername

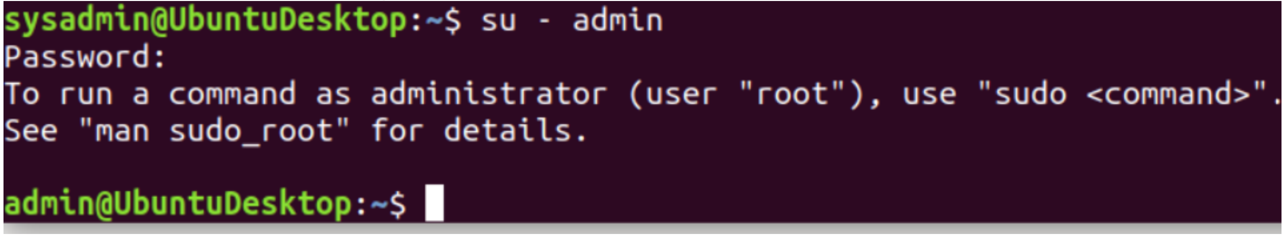


```
aldanelib:x:1012:1014:Eli Aldana,,,:/home/aldanelib:/bin/bash
joe:x:1014:1017:,,,:/home/joe:/bin/bash
amy:x:1015:1018:,,,:/home/amy:/bin/bash
sara:x:1016:1019:,,,:/home/sara:/bin/bash
admin:x:1017:1020:,,,:/home/admin:/bin/bash
sam:x:1013:1016:,,,:/home/sam:/bin/bash
sysadmin@UbuntuDesktop:~$ sudo -lU joe
User joe is not allowed to run sudo on UbuntuDesktop.
sysadmin@UbuntuDesktop:~$ sudo -lU amy
User amy is not allowed to run sudo on UbuntuDesktop.
sysadmin@UbuntuDesktop:~$ sudo -lU sara
User sara is not allowed to run sudo on UbuntuDesktop.
sysadmin@UbuntuDesktop:~$ sudo -lU sam
User sam is not allowed to run sudo on UbuntuDesktop.
sysadmin@UbuntuDesktop:~$ sudo -lU 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\:/bi
n\:/snap/bin

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

-

3. Command to add `admin` to the `sudo` group: sudo usermod -aG sudo admin



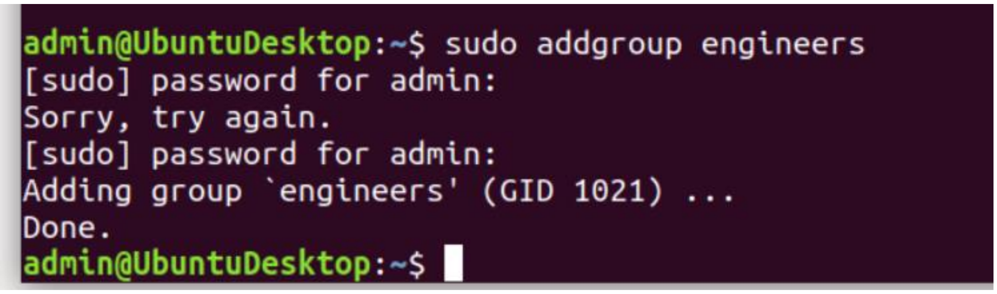
```
sysadmin@UbuntuDesktop:~$ su - admin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@UbuntuDesktop:~$
```

   -

Step 3: Create User Group and Collaborative Folder

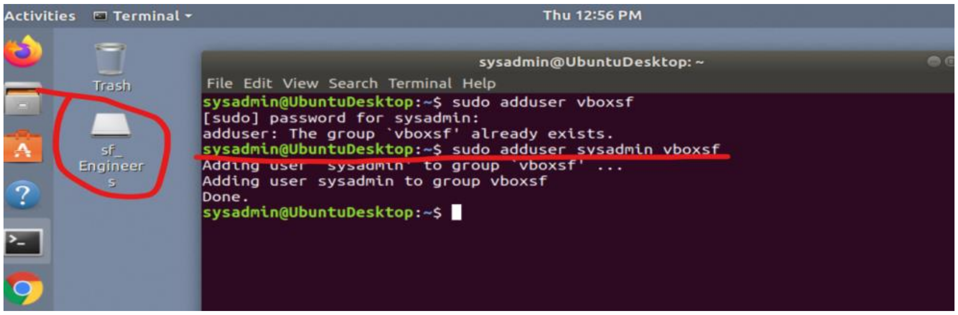
1. Add an `engineers` group to the system.
   - Command to add group: sudo addgroup engineers



```
admin@UbuntuDesktop:~$ sudo addgroup engineers
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Adding group `engineers' (GID 1021) ...
Done.
admin@UbuntuDesktop:~$
```

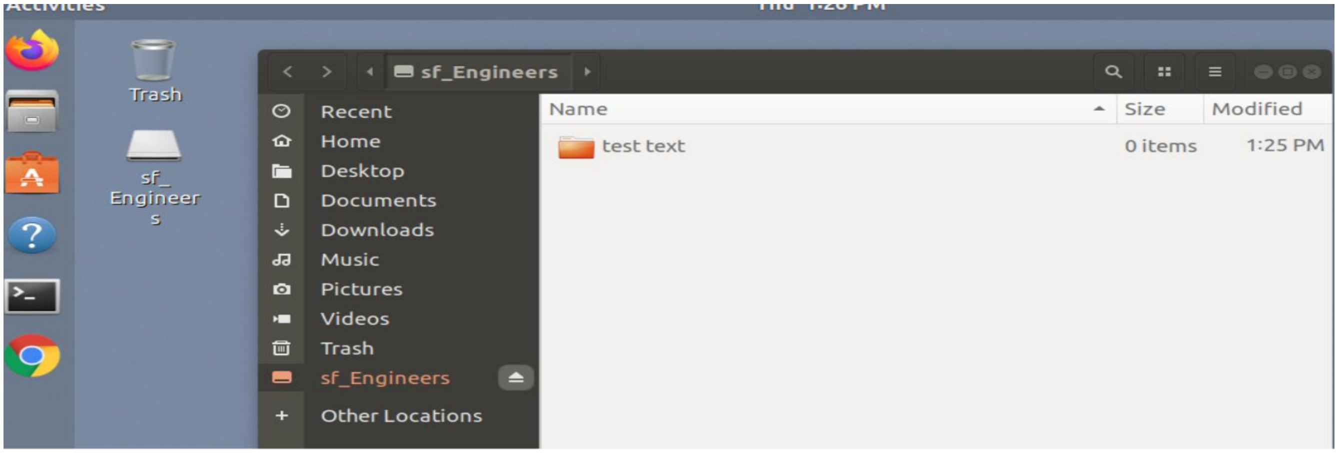
2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
   - Command to add users to `engineers` group (include all four users):
      - sudo adduser sam engineers
      - sudo adduser joe engineers
      - sudo adduser amy engineers
      - sudo adduser sara engineers

3. Create a shared folder for this group at `/home/engineers`.
   - Command to create the shared folder: **sudo adduser sysadmin vboxsf**



Activities
Terminal
Thu 12:56 PM
Trash
sf_
Engineer
s
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
sysadmin@UbuntuDesktop:~$ sudo adduser vboxsf
[sudo] password for sysadmin:
adduser: The group `vboxsf' already exists.
sysadmin@UbuntuDesktop:~$ sudo adduser sysadmin vboxsf
Adding user `sysadmin' to group `vboxsf' ...
Adding user sysadmin to group vboxsf
Done.
sysadmin@UbuntuDesktop:~$
```



Name	Size	Modified
test text	0 items	1:25 PM

4. Change ownership on the new engineers' shared folder to the `engineers` group.

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

   sudo chown sam:engineers

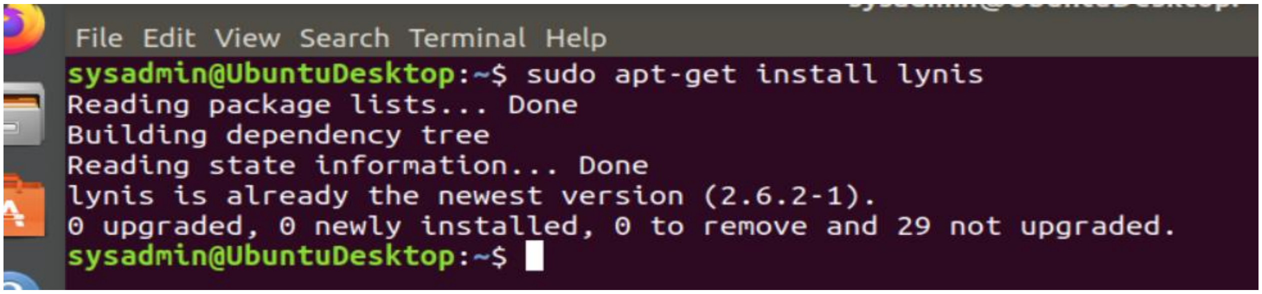
   o sudo chown joe:engineers

   o sudo chown amy:engineers

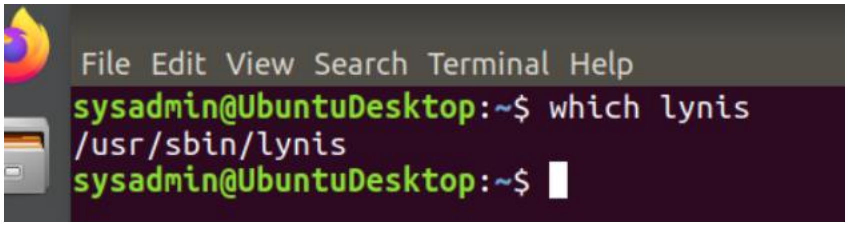
   o sudo chown sara:engineers

Step 4: Lynis Auditing

1. Command to install Lynis:



```
sysadmin@UbuntuDesktop:~$ sudo apt-get install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (2.6.2-1).
0 upgraded, 0 newly installed, 0 to remove and 29 not upgraded.
sysadmin@UbuntuDesktop:~$
```

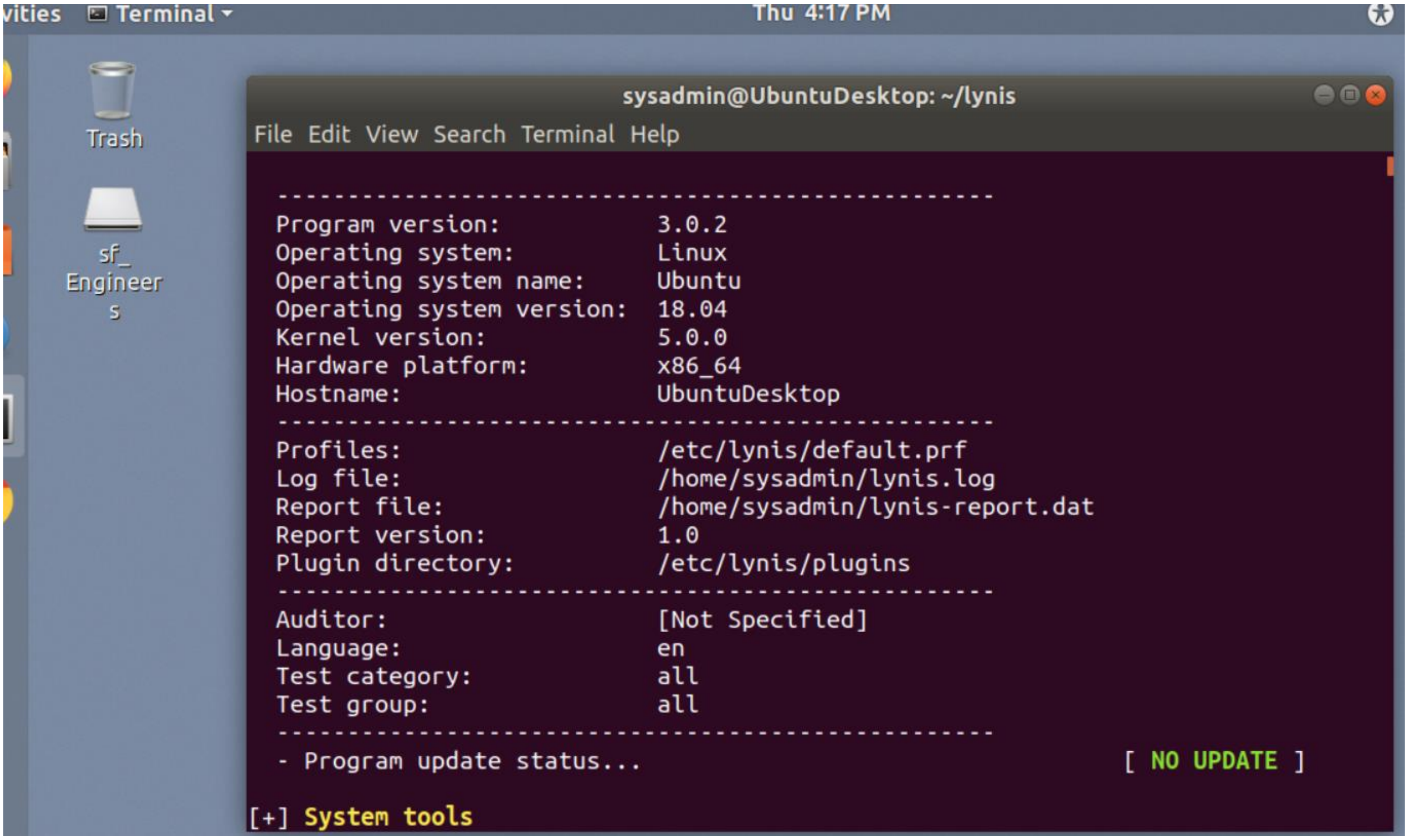


```
sysadmin@UbuntuDesktop:~$ which lynis
/usr/sbin/lynis
sysadmin@UbuntuDesktop:~$
```

2. Command to see documentation and instructions:

    - Command to run an audit: $ lynis audit system

3. Provide a report from the Lynis output on what can be done to harden the system.
    - Screenshot of report output:


vities
Terminal
Thu 4:17 PM
Trash
sf_ Engineers
sysadmin@UbuntuDesktop: ~/lynis
File Edit View Search Terminal Help

```
 ---------------------------------------------------
 Program version:           3.0.2
 Operating system:          Linux
 Operating system name:     Ubuntu
 Operating system version:  18.04
 Kernel version:            5.0.0
 Hardware platform:         x86_64
 Hostname:                  UbuntuDesktop
 ---------------------------------------------------
 Profiles:                  /etc/lynis/default.prf
 Log file:                  /home/sysadmin/lynis.log
 Report file:               /home/sysadmin/lynis-report.dat
 Report version:            1.0
 Plugin directory:          /etc/lynis/plugins
 ---------------------------------------------------
 Auditor:                   [Not Specified]
 Language:                  en
 Test category:             all
 Test group:                all
 ---------------------------------------------------
 - Program update status...                          [ NO UPDATE ]

[+] System tools
```

Bonus

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