Week 4 Homework Submission File

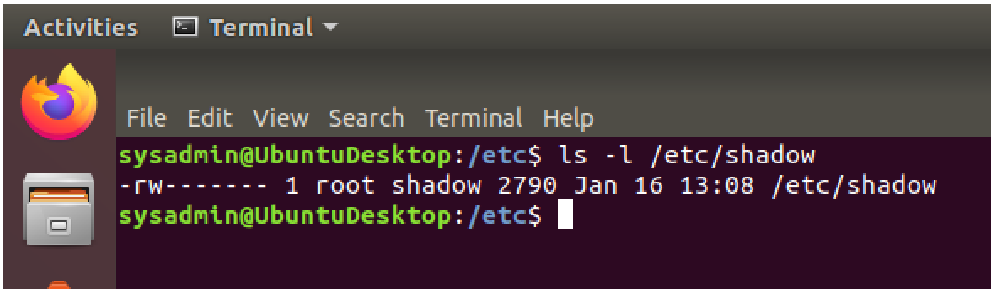
Linux Systems Administration

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

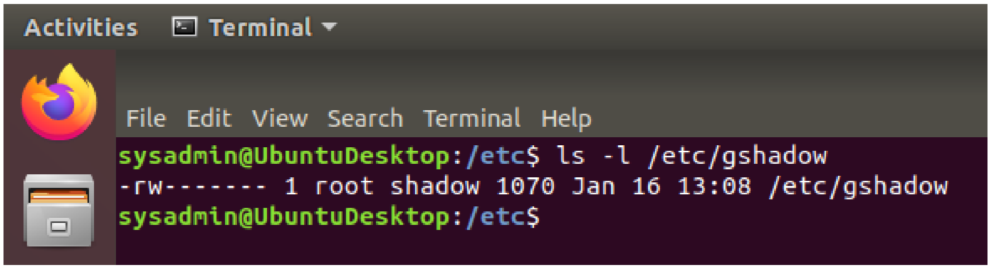


```
sysadmin@UbuntuDesktop:/etc$ ls -l /etc/shadow
-rw------- 1 root shadow 2790 Jan 16 13:08 /etc/shadow
sysadmin@UbuntuDesktop:/etc$
```

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

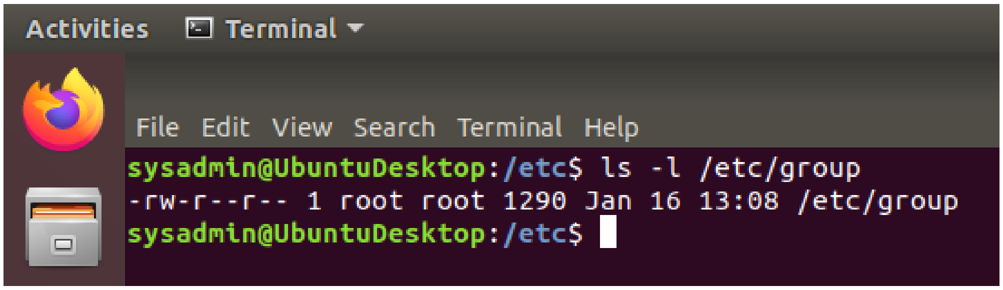


```
sysadmin@UbuntuDesktop:/etc$ ls -l /etc/gshadow
-rw------- 1 root shadow 1070 Jan 16 13:08 /etc/gshadow
sysadmin@UbuntuDesktop:/etc$
```

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

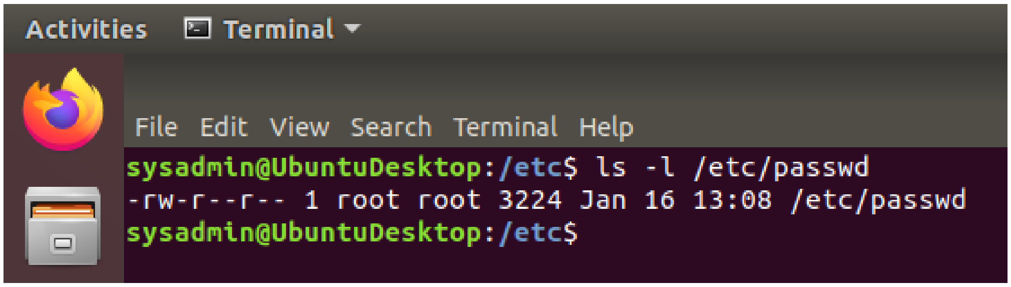


```
sysadmin@UbuntuDesktop:/etc$ ls -l /etc/group
-rw-r--r-- 1 root root 1290 Jan 16 13:08 /etc/group
sysadmin@UbuntuDesktop:/etc$ 
```

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

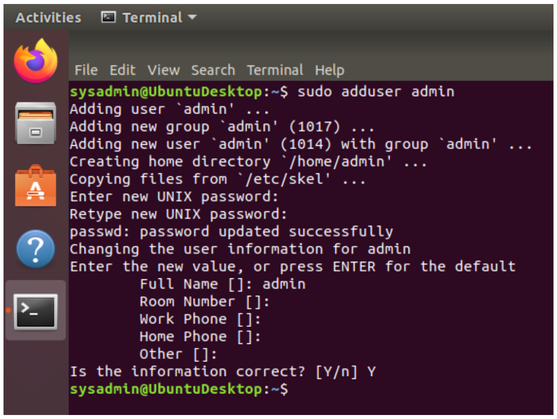


```
sysadmin@UbuntuDesktop:/etc$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3224 Jan 16 13:08 /etc/passwd
sysadmin@UbuntuDesktop:/etc$
```

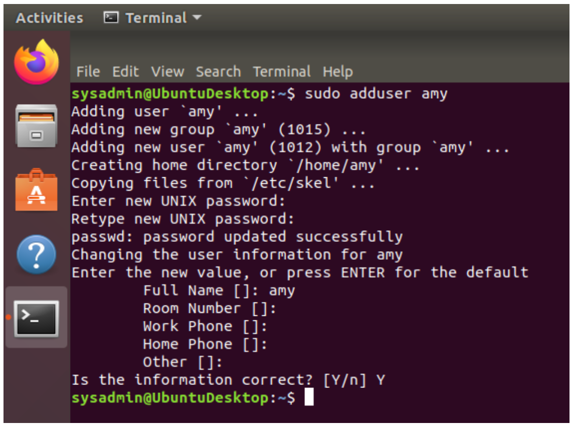
Step 2: Create User Accounts

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

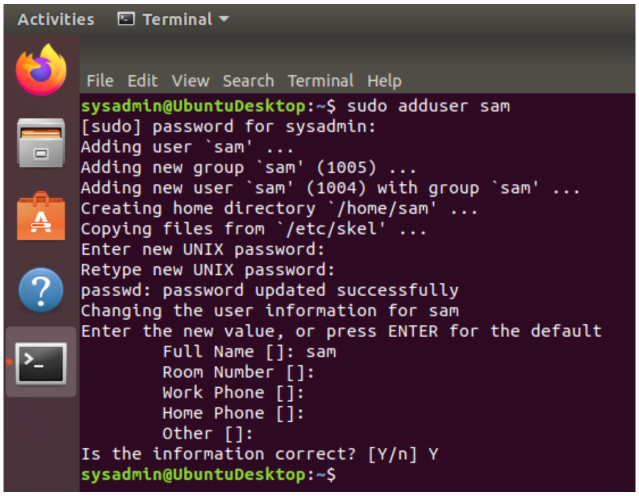
   - Command to add each user account (include all five users):
     - sudo adduser sam
     - sudo adduser joe
     - sudo adduser amy
     - sudo adduser sara
     - sudo adduser admin



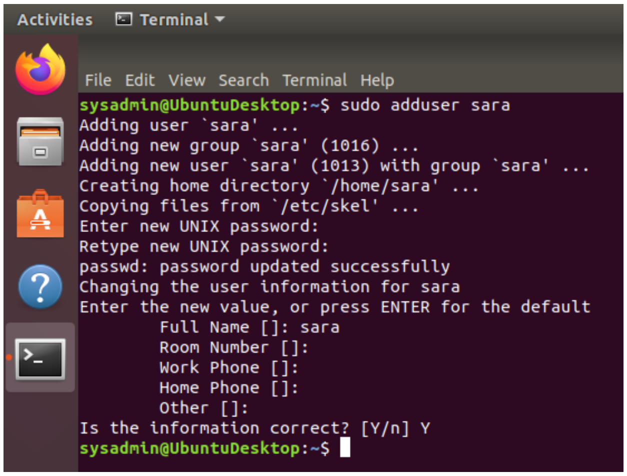
```
sysadmin@UbuntuDesktop:~$ sudo adduser admin
Adding user `admin' ...
Adding new group `admin' (1017) ...
Adding new user `admin' (1014) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
        Full Name []: admin
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sysadmin@UbuntuDesktop:~$
```



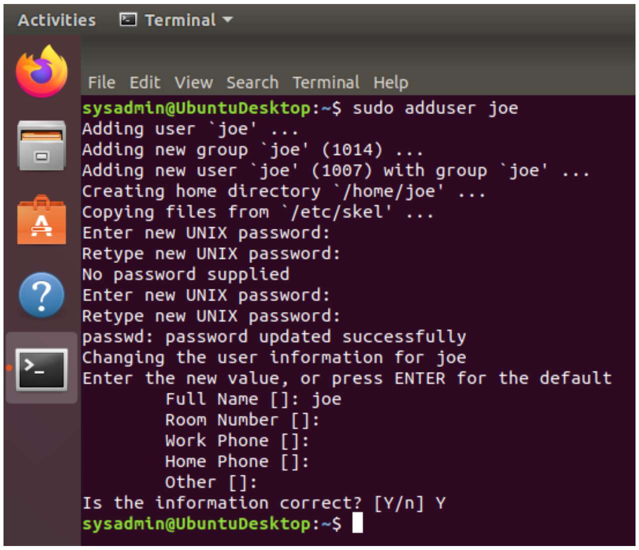
```
sysadmin@UbuntuDesktop:~$ sudo adduser amy
Adding user `amy' ...
Adding new group `amy' (1015) ...
Adding new user `amy' (1012) with group `amy' ...
Creating home directory `/home/amy' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for amy
Enter the new value, or press ENTER for the default
        Full Name []: amy
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sysadmin@UbuntuDesktop:~$ 
```



```
sysadmin@UbuntuDesktop:~$ sudo adduser sam
[sudo] password for sysadmin:
Adding user `sam' ...
Adding new group `sam' (1005) ...
Adding new user `sam' (1004) with group `sam' ...
Creating home directory `/home/sam' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sam
Enter the new value, or press ENTER for the default
        Full Name []: sam
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sysadmin@UbuntuDesktop:~$
```



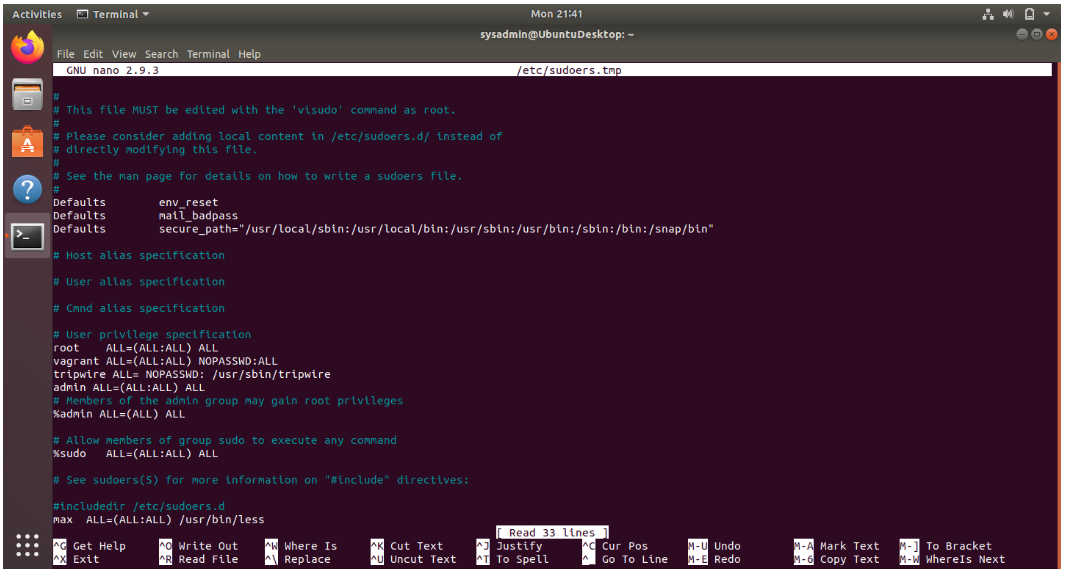
```
sysadmin@UbuntuDesktop:~$ sudo adduser sara
Adding user `sara' ...
Adding new group `sara' (1016) ...
Adding new user `sara' (1013) with group `sara' ...
Creating home directory `/home/sara' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sara
Enter the new value, or press ENTER for the default
        Full Name []: sara
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sysadmin@UbuntuDesktop:~$
```



```
sysadmin@UbuntuDesktop:~$ sudo adduser joe
Adding user `joe' ...
Adding new group `joe' (1014) ...
Adding new user `joe' (1007) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
        Full Name []: joe
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sysadmin@UbuntuDesktop:~$
```

2. Ensure that only the `admin` has general sudo access.

- Command to add `admin` to the `sudo` group: sudo visudo

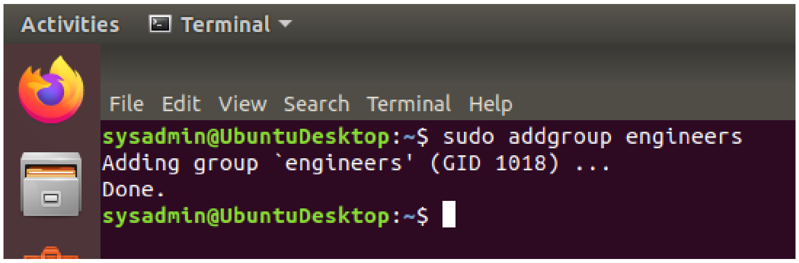

Activities
Terminal
Mon 21:41
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

```
  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:/sbin:/bin:/snap/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
admin ALL=(ALL:ALL) ALL
# 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
                                   [ Read 33 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text  M-W WhereIs Next
```

Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

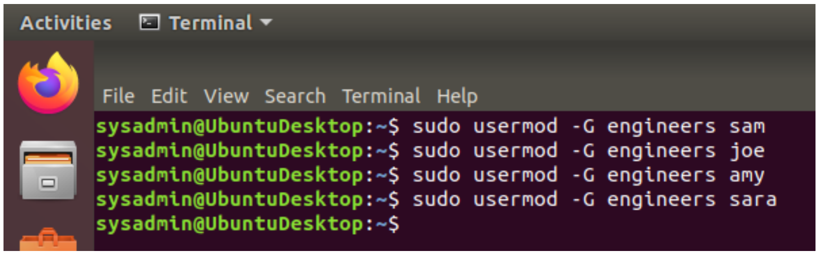
    - Command to add group: sudo addgroup engineers



```
sysadmin@UbuntuDesktop:~$ sudo addgroup engineers
Adding group `engineers' (GID 1018) ...
Done.
sysadmin@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 usermod -G engineers sam
    - sudo usermod -G engineers joe
    - sudo usermod -G engineers amy
    - sudo usermod -G engineers sara



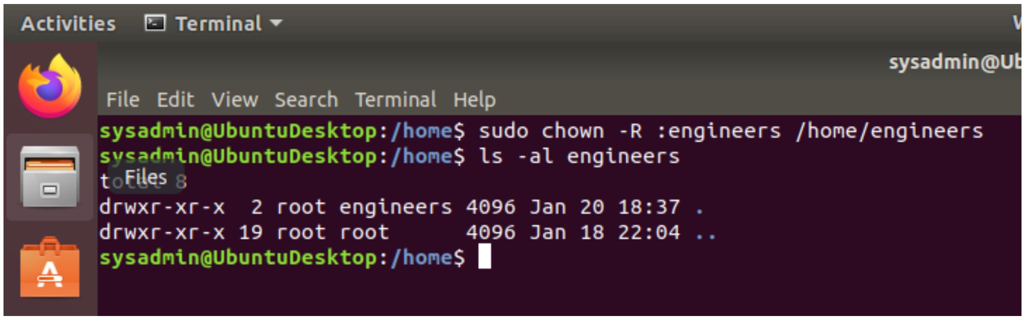
```
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers sam
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers joe
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers amy
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers sara
sysadmin@UbuntuDesktop:~$
```

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

    - Command to create the shared folder: sudo mkdir engineers

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

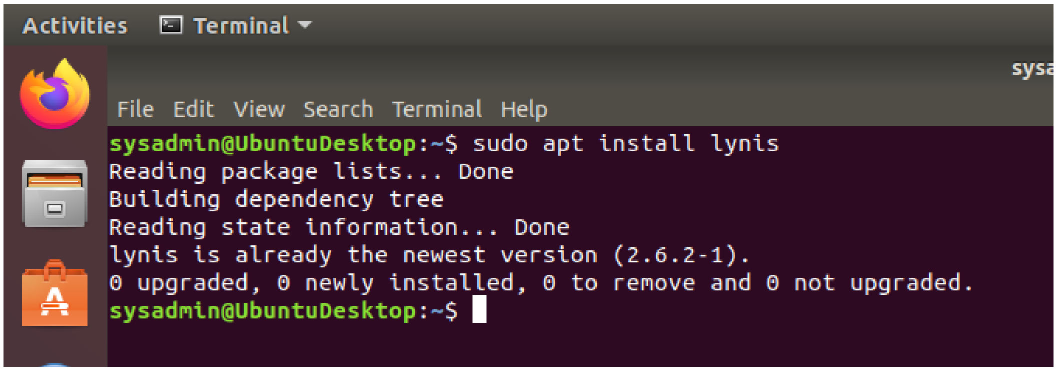
    - Command to change ownership of engineer's shared folder to engineer group: sudo chown -R :engineers /home/engineers



```
sysadmin@UbuntuDesktop:/home$ sudo chown -R :engineers /home/engineers
sysadmin@UbuntuDesktop:/home$ ls -al engineers
total 8
drwxr-xr-x  2 root engineers 4096 Jan 20 18:37 .
drwxr-xr-x 19 root root      4096 Jan 18 22:04 ..
sysadmin@UbuntuDesktop:/home$ 
```

Step 4: Lynis Auditing

1. Command to install Lynis: sudo apt install lynis



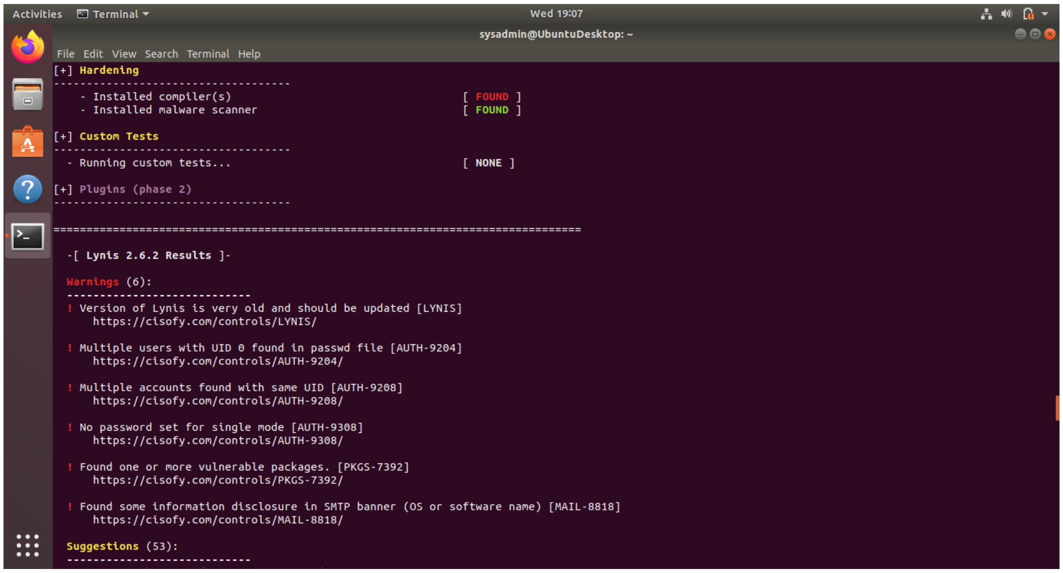
```
sysadmin@UbuntuDesktop:~$ sudo apt install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (2.6.2-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sysadmin@UbuntuDesktop:~$ 
```

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:


Activities
Terminal
Wed 19:07
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

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

[+] Custom Tests
------------------------------------
  - Running custom tests...                               [ NONE ]

[+] Plugins (phase 2)
------------------------------------

================================================================================

  -[ Lynis 2.6.2 Results ]-

  Warnings (6):
  ----------------------------
  ! Version of Lynis is very old and should be updated [LYNIS]
      https://cisofy.com/controls/LYNIS/

  ! Multiple users with UID 0 found in passwd file [AUTH-9204]
      https://cisofy.com/controls/AUTH-9204/

  ! Multiple accounts found with same UID [AUTH-9208]
      https://cisofy.com/controls/AUTH-9208/

  ! 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/

  Suggestions (53):
  ----------------------------
```

Bonus

1. Command to install chkrootkit:

2. Command to see documentation and instructions:

3. Command to run expert mode:

4. Provide a report from the chrootkit output on what can be done to harden the system.
   - Screenshot of end of sample output: