



Module 4 Challenge Submission File

Linux Systems Administration

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.

- a. Command to inspect permissions:

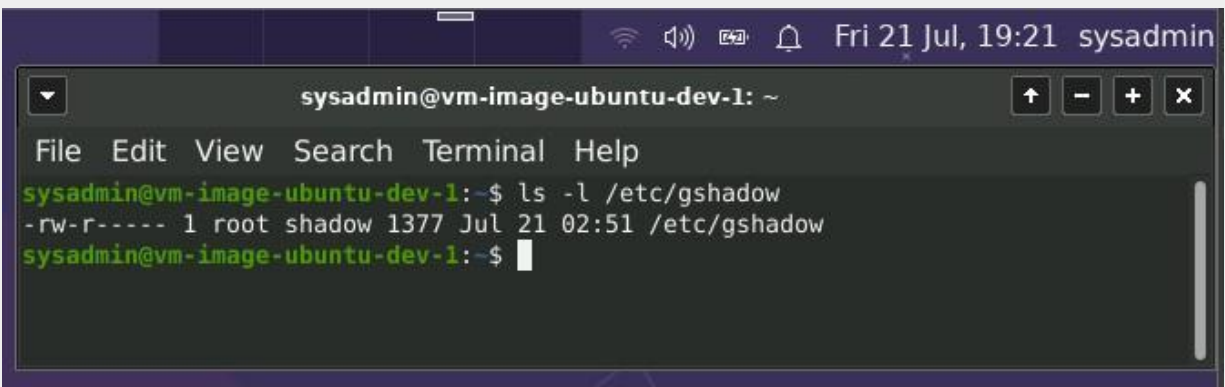
```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/shadow  
-rw-r----- 1 root shadow 3184 Jun 27 21:59 /etc/shadow  
sysadmin@vm-image-ubuntu-dev-1:~$
```

- b. Command to set permissions (if needed):

```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/shadow  
-rw-r----- 1 root shadow 3184 Jun 27 21:59 /etc/shadow  
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chmod 600 /etc/shadow  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/shadow  
-rw----- 1 root shadow 3184 Jun 27 21:59 /etc/shadow  
sysadmin@vm-image-ubuntu-dev-1:~$
```

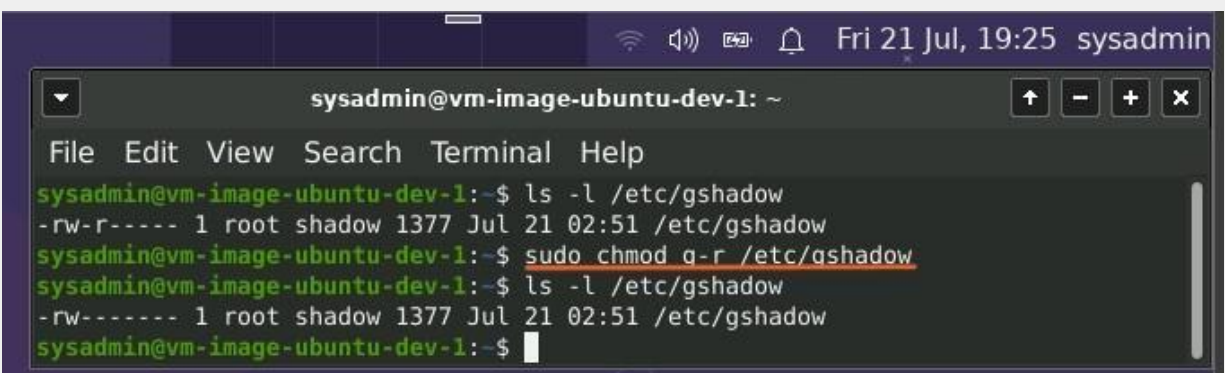
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

a. Command to inspect permissions:



```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/gshadow  
-rw-r----- 1 root shadow 1377 Jul 21 02:51 /etc/gshadow  
sysadmin@vm-image-ubuntu-dev-1:~$
```

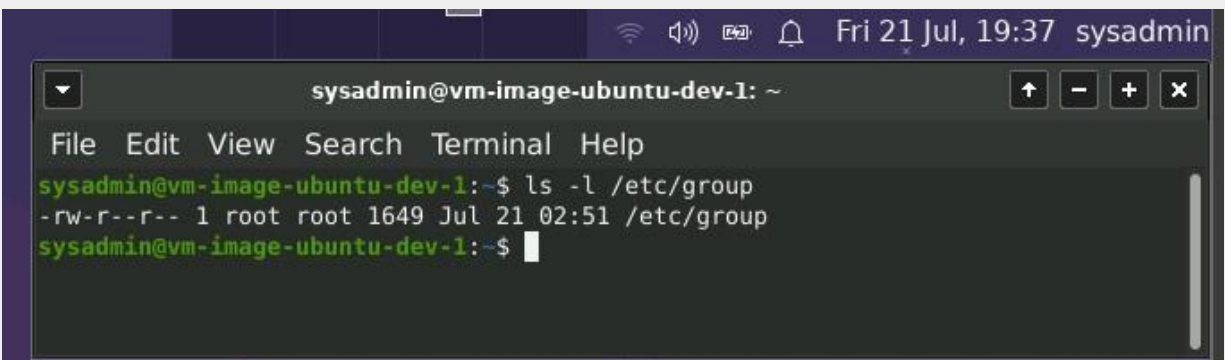
b. Command to set permissions (if needed):



```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/gshadow  
-rw-r----- 1 root shadow 1377 Jul 21 02:51 /etc/gshadow  
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chmod a-r /etc/gshadow  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/gshadow  
-rw----- 1 root shadow 1377 Jul 21 02:51 /etc/gshadow  
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

a. Command to inspect permissions:



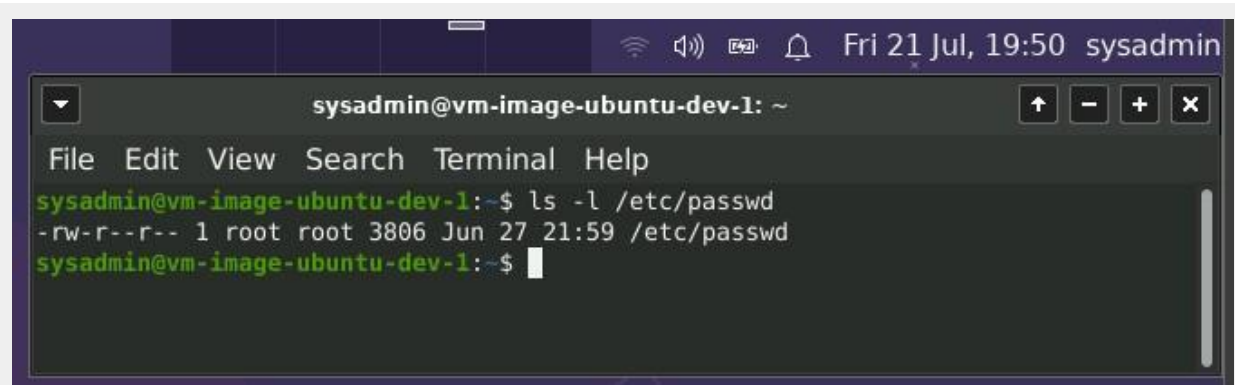
```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/group  
-rw-r--r-- 1 root root 1649 Jul 21 02:51 /etc/group  
sysadmin@vm-image-ubuntu-dev-1:~$
```

b. Command to set permissions (if needed):

No need to set permissions because the group file already has permissions that allow only 'root' read and write access and allow everyone else read access only.

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

a. Command to inspect permissions:



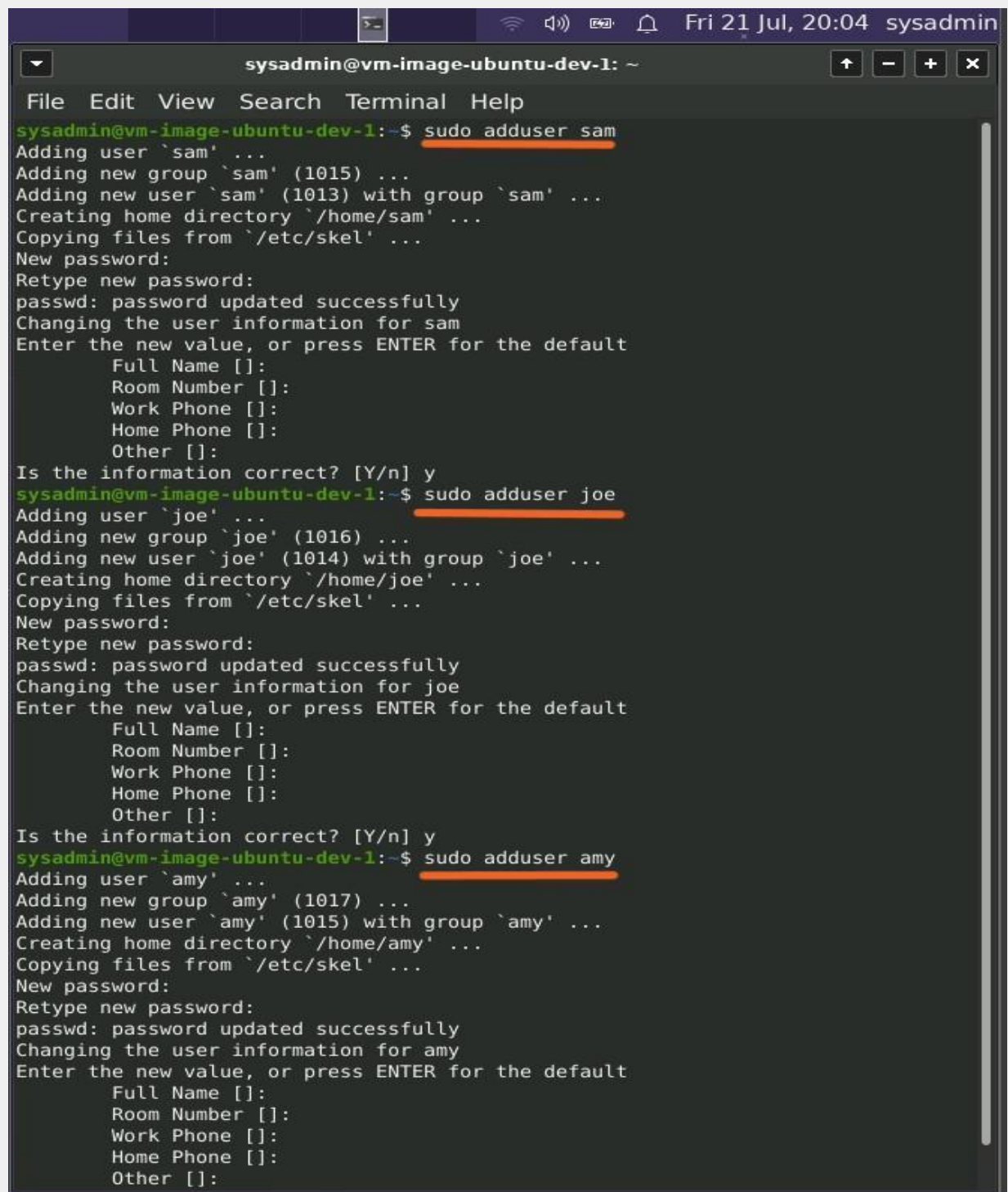
```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /etc/passwd  
-rw-r--r-- 1 root root 3806 Jun 27 21:59 /etc/passwd  
sysadmin@vm-image-ubuntu-dev-1:~$
```

b. Command to set permissions (if needed):

No need to set permissions because the passwd file already has permissions that allow only 'root' read and write access and allow everyone else read access only.

Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin1 with the useradd command.
 - a. Command to add each user account (include all five users):



```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo adduser sam
Adding user `sam' ...
Adding new group `sam' (1015) ...
Adding new user `sam' (1013) with group `sam' ...
Creating home directory `/home/sam' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sam
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@vm-image-ubuntu-dev-1:~$ sudo adduser joe
Adding user `joe' ...
Adding new group `joe' (1016) ...
Adding new user `joe' (1014) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for joe
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@vm-image-ubuntu-dev-1:~$ sudo adduser amy
Adding user `amy' ...
Adding new group `amy' (1017) ...
Adding new user `amy' (1015) with group `amy' ...
Creating home directory `/home/amy' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
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 []:
```

```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ 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' ...
New password:
Retype new 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@vm-image-ubuntu-dev-1:~$ sudo adduser admin1
Adding user `admin1' ...
Adding new group `admin1' (1019) ...
Adding new user `admin1' (1017) with group `admin1' ...
Creating home directory `/home/admin1' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin1
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@vm-image-ubuntu-dev-1:~$
```

2. Ensure that only the `admin1` has general sudo access.

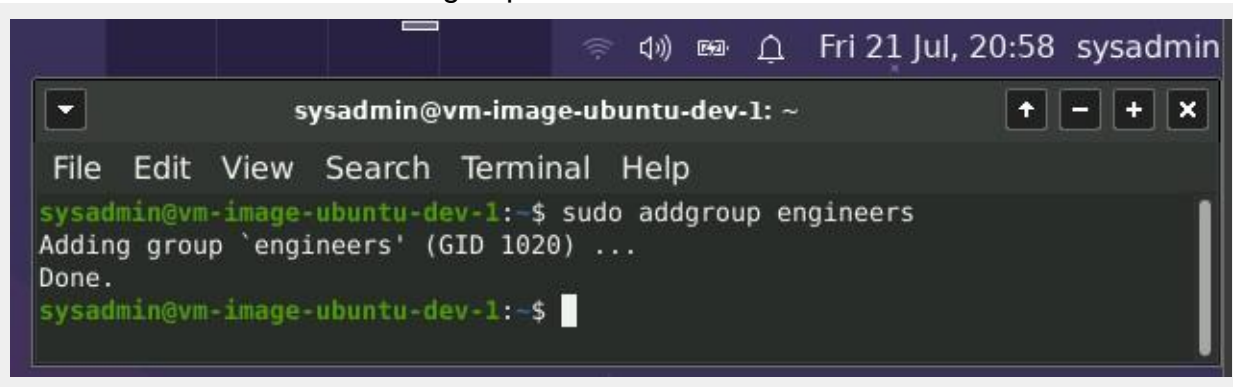
a. Command to add `admin1` to the sudo group:

```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -aG sudo admin1
sysadmin@vm-image-ubuntu-dev-1:~$ groups admin1
admin1 : admin1 sudo
sysadmin@vm-image-ubuntu-dev-1:~$
```


Step 3: Create User Group and Collaborative Folder

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

- a. Command to add group:

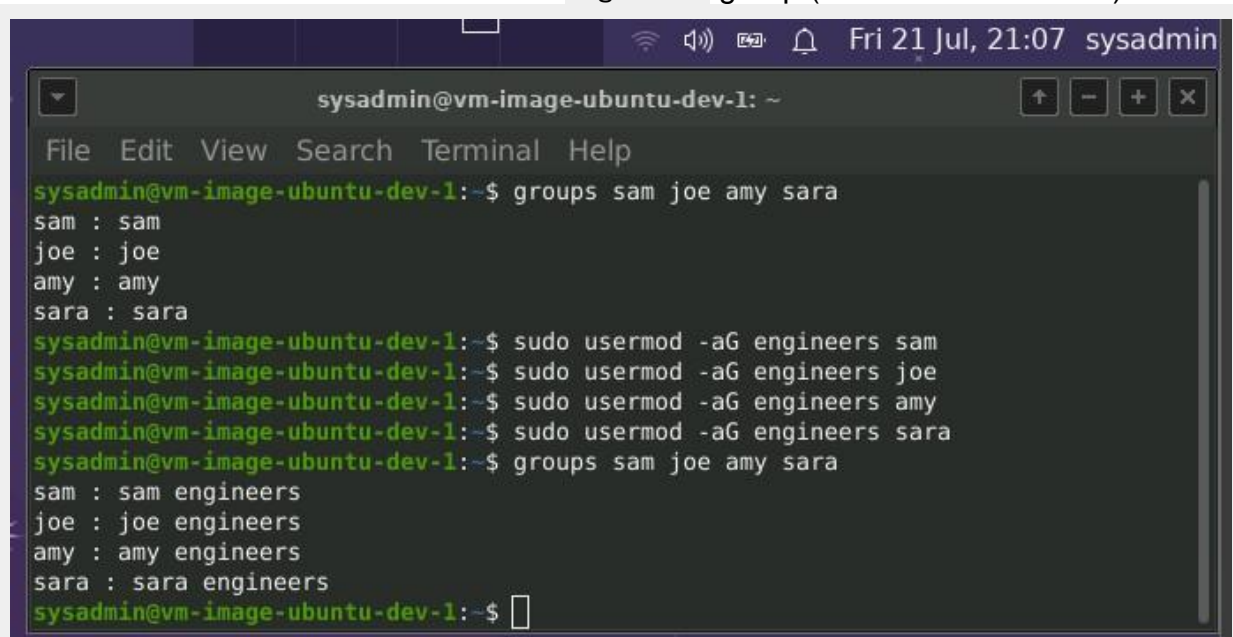


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command `sudo addgroup engineers` being executed. The output is: 'Adding group `engineers` (GID 1020) ... Done.' The prompt returns to `sysadmin@vm-image-ubuntu-dev-1:~$`.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo addgroup engineers
Adding group `engineers` (GID 1020) ...
Done.
sysadmin@vm-image-ubuntu-dev-1:~$
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

- a. Command to add users to `engineers` group (include all four users):

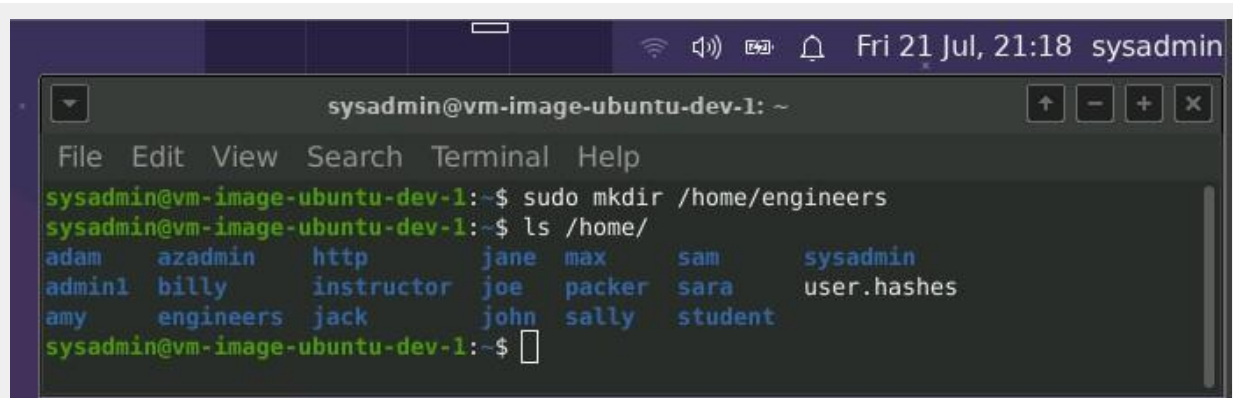


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following sequence of commands and output:
1. `groups sam joe amy sara` outputs: `sam : sam`, `joe : joe`, `amy : amy`, `sara : sara`.
2. `sudo usermod -aG engineers sam`
3. `sudo usermod -aG engineers joe`
4. `sudo usermod -aG engineers amy`
5. `sudo usermod -aG engineers sara`
6. `groups sam joe amy sara` outputs: `sam : sam engineers`, `joe : joe engineers`, `amy : amy engineers`, `sara : sara engineers`.
The prompt returns to `sysadmin@vm-image-ubuntu-dev-1:~$`.

```
sysadmin@vm-image-ubuntu-dev-1:~$ groups sam joe amy sara
sam : sam
joe : joe
amy : amy
sara : sara
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -aG engineers sam
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -aG engineers joe
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -aG engineers amy
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -aG engineers sara
sysadmin@vm-image-ubuntu-dev-1:~$ groups sam joe amy sara
sam : sam engineers
joe : joe engineers
amy : amy engineers
sara : sara engineers
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

a. Command to create the shared folder:

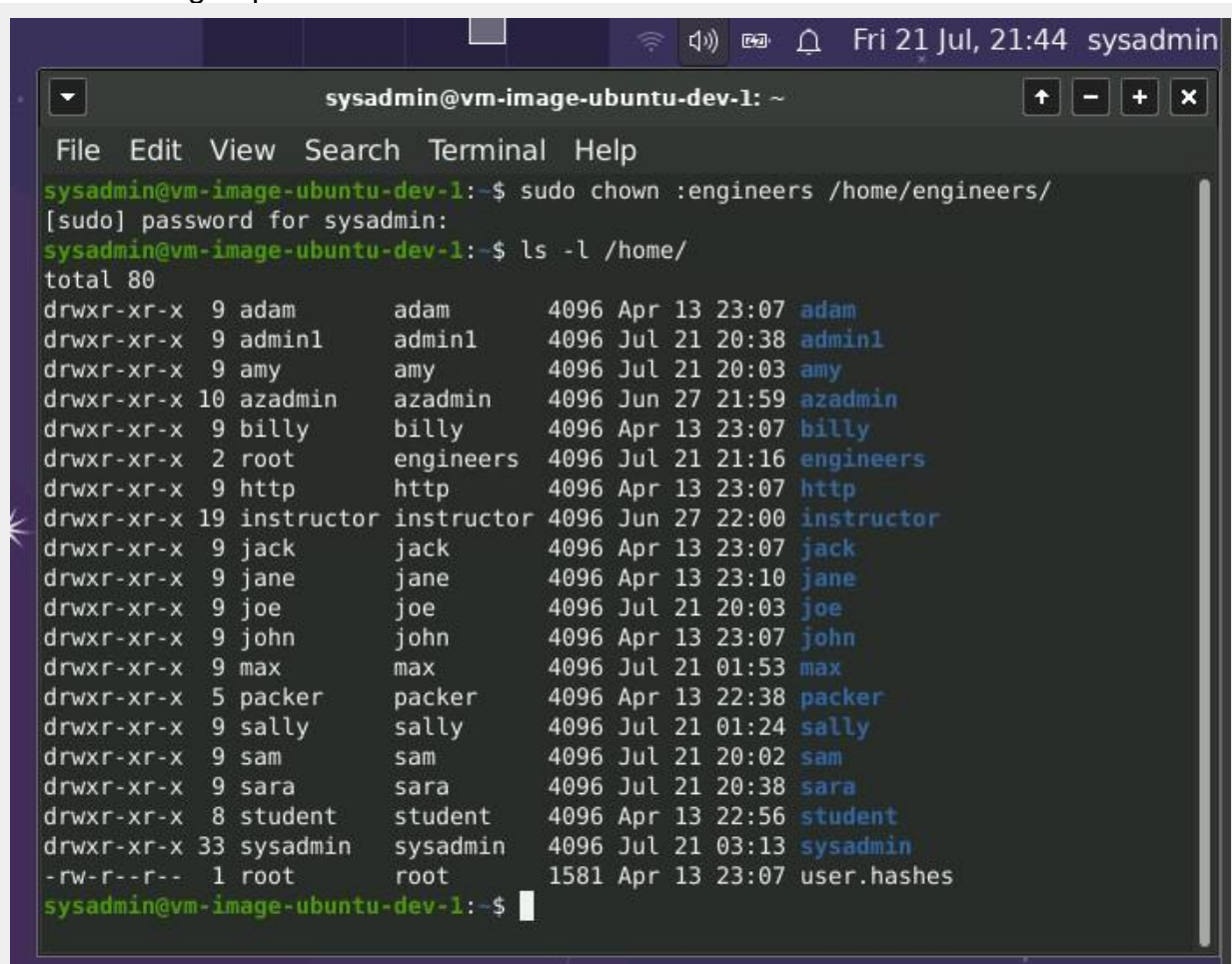


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo mkdir /home/engineers
sysadmin@vm-image-ubuntu-dev-1:~$ ls /home/
adam  azadmin  http  jane  max  sam  sysadmin
admin1 billy    instructor  joe  packer sara  user.hashes
amy   engineers jack  john  sally  student
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

a. Command to change ownership of engineers' shared folder to `engineers` group:

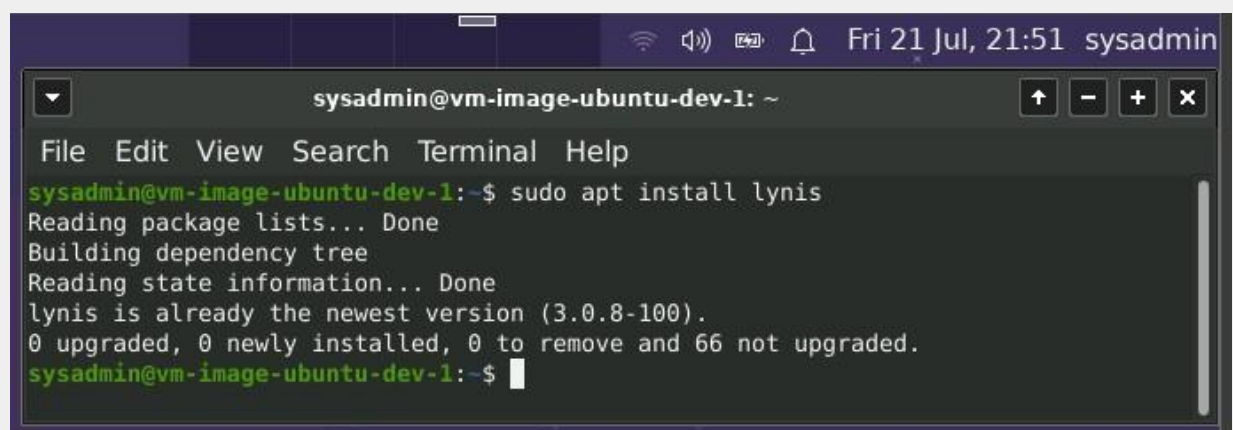


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chown :engineers /home/engineers/
[sudo] password for sysadmin:
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l /home/
total 80
drwxr-xr-x  9 adam      adam      4096 Apr 13 23:07 adam
drwxr-xr-x  9 admin1    admin1    4096 Jul 21 20:38 admin1
drwxr-xr-x  9 amy       amy       4096 Jul 21 20:03 amy
drwxr-xr-x 10 azadmin   azadmin   4096 Jun 27 21:59 azadmin
drwxr-xr-x  9 billy     billy     4096 Apr 13 23:07 billy
drwxr-xr-x  2 root      engineers 4096 Jul 21 21:16 engineers
drwxr-xr-x  9 http      http      4096 Apr 13 23:07 http
drwxr-xr-x 19 instructor instructor 4096 Jun 27 22:00 instructor
drwxr-xr-x  9 jack      jack      4096 Apr 13 23:07 jack
drwxr-xr-x  9 jane      jane      4096 Apr 13 23:10 jane
drwxr-xr-x  9 joe       joe       4096 Jul 21 20:03 joe
drwxr-xr-x  9 john      john      4096 Apr 13 23:07 john
drwxr-xr-x  9 max       max       4096 Jul 21 01:53 max
drwxr-xr-x  5 packer    packer    4096 Apr 13 22:38 packer
drwxr-xr-x  9 sally     sally     4096 Jul 21 01:24 sally
drwxr-xr-x  9 sam       sam       4096 Jul 21 20:02 sam
drwxr-xr-x  9 sara      sara      4096 Jul 21 20:38 sara
drwxr-xr-x  8 student   student   4096 Apr 13 22:56 student
drwxr-xr-x 33 sysadmin  sysadmin 4096 Jul 21 03:13 sysadmin
-rw-r--r--  1 root      root      1581 Apr 13 23:07 user.hashes
sysadmin@vm-image-ubuntu-dev-1:~$
```

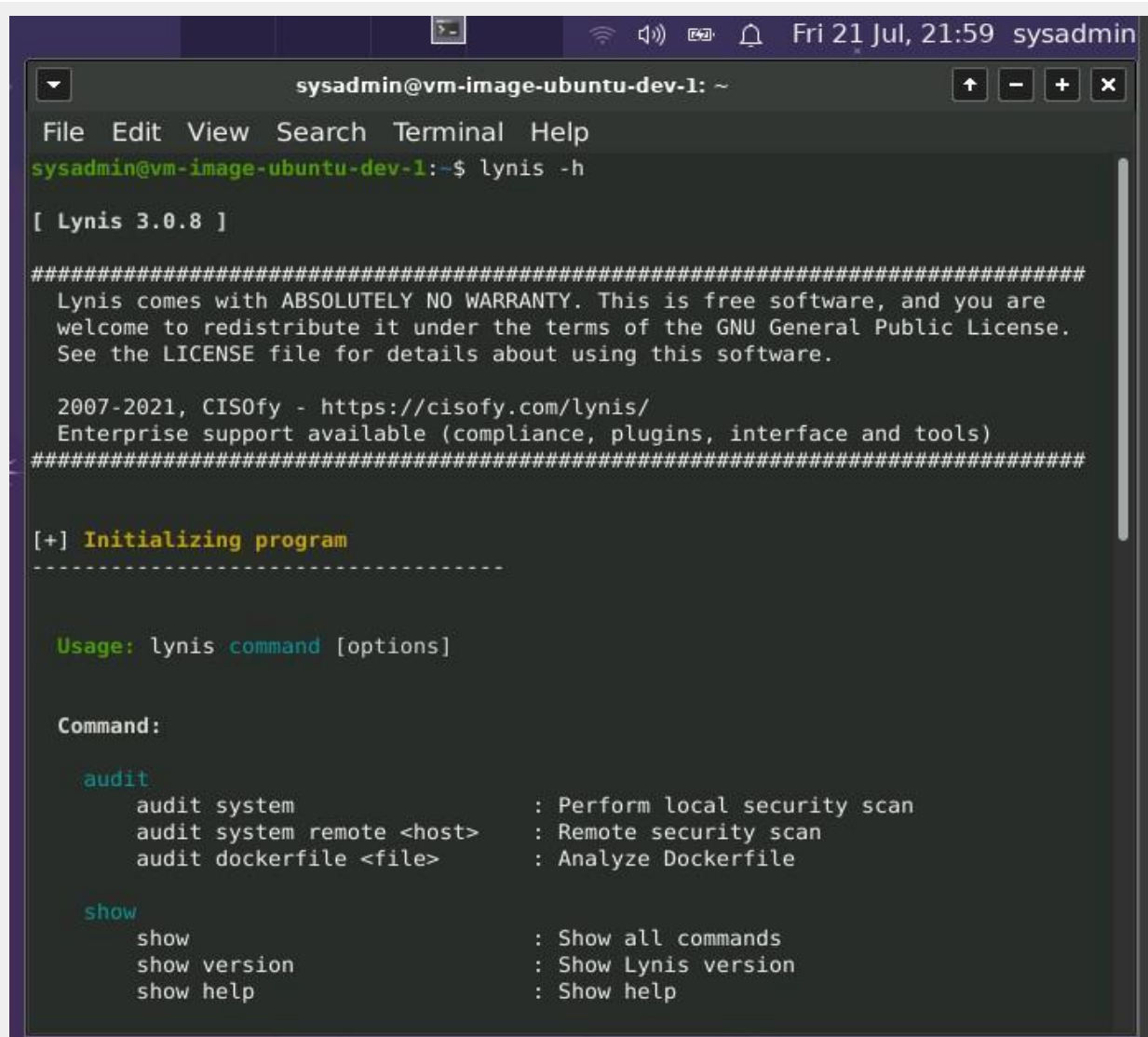
Step 4: Lynis Auditing

1. Command to install Lynis:

A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'sudo apt install lynis' being executed. The output indicates that Lynis is already the newest version (3.0.8-100) and that 66 packages were not upgraded. The prompt returns to the user.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo apt install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (3.0.8-100).
0 upgraded, 0 newly installed, 0 to remove and 66 not upgraded.
sysadmin@vm-image-ubuntu-dev-1:~$
```

2. Command to view documentation and instructions:

A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'lynis -h' being executed. The output displays the Lynis 3.0.8 version, a disclaimer about warranty, contact information for CISofy, and a list of available commands and their descriptions.

```
sysadmin@vm-image-ubuntu-dev-1:~$ lynis -h

[ Lynis 3.0.8 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----

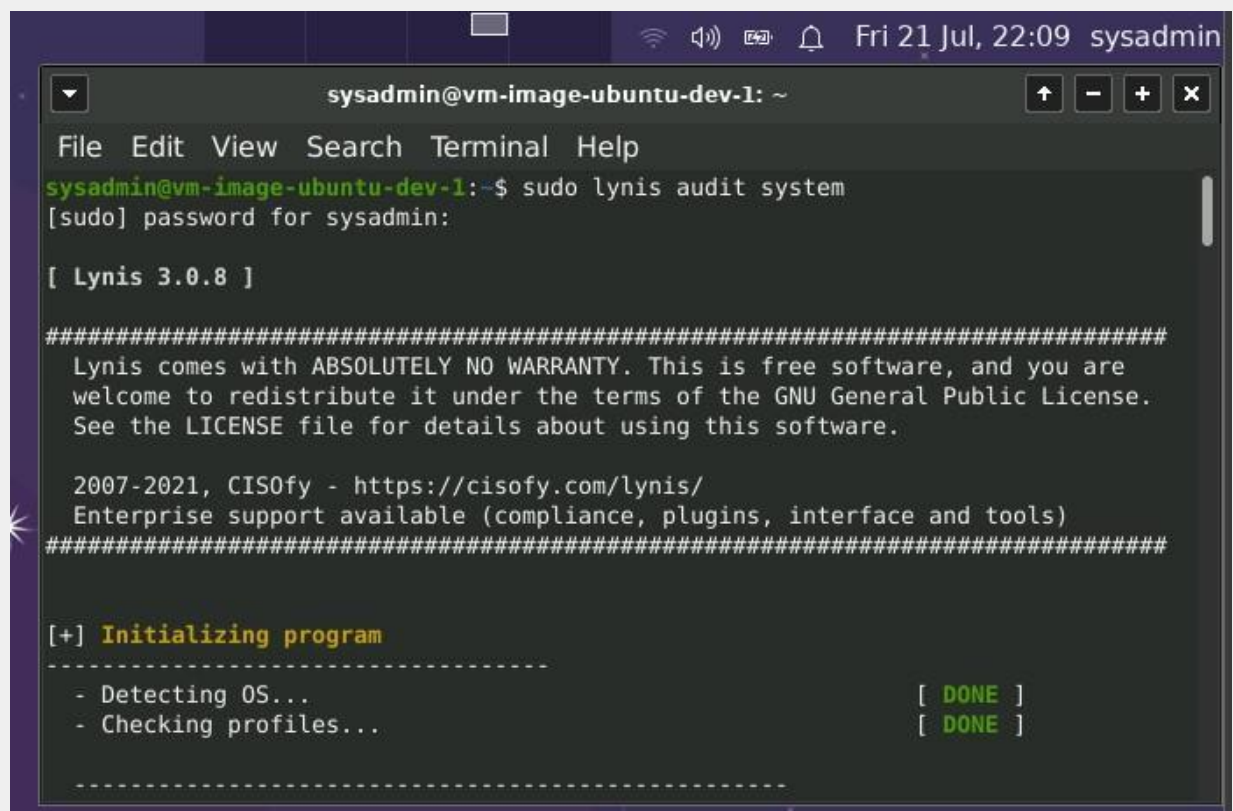
Usage: lynis command [options]

Command:

audit
  audit system          : Perform local security scan
  audit system remote <host> : Remote security scan
  audit dockerfile <file> : Analyze Dockerfile

show
  show          : Show all commands
  show version  : Show Lynis version
  show help     : Show help
```


3. Command to run an audit:



The screenshot shows a terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~'. The user has entered the command 'sudo lynis audit system'. The terminal output shows the Lynis 3.0.8 version, a disclaimer, and the start of the audit process. The audit is currently in the 'Initializing program' phase, with sub-tasks 'Detecting OS...' and 'Checking profiles...' both marked as '[DONE]'.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo lynis audit system
[sudo] password for sysadmin:

[ Lynis 3.0.8 ]

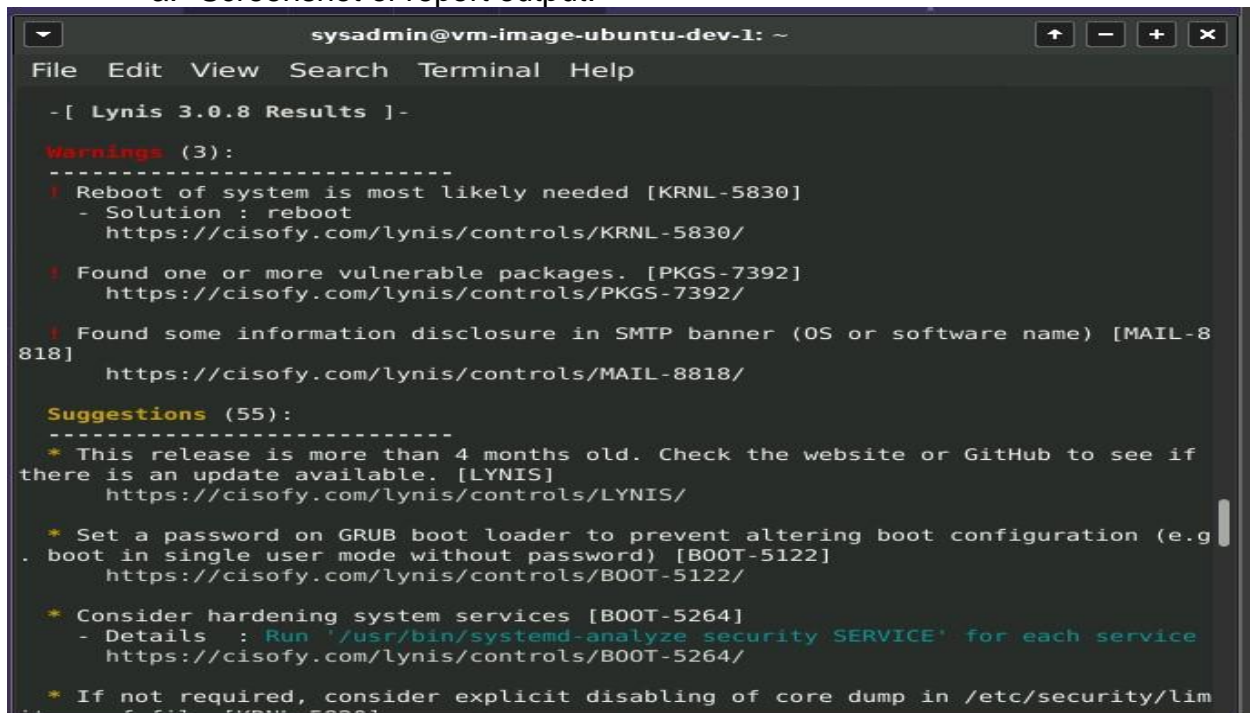
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
-----
```

4. Provide a report from the Lynis output with recommendations for hardening the system.

a. Screenshot of report output:



The screenshot shows the 'Lynis 3.0.8 Results' report. It lists three warnings: a need for a system reboot (KRNL-5830), vulnerable packages (PKGS-7392), and an SMTP banner disclosure (MAIL-8818). It also lists 55 suggestions for hardening, including updating Lynis, setting a GRUB password (B00T-5122), and hardening system services (B00T-5264).

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo lynis audit system
[sudo] password for sysadmin:

[ Lynis 3.0.8 Results ]-

Warnings (3):
-----
! Reboot of system is most likely needed [KRNL-5830]
  - Solution : reboot
    https://cisofy.com/lynis/controls/KRNL-5830/

! Found one or more vulnerable packages. [PKGS-7392]
  https://cisofy.com/lynis/controls/PKGS-7392/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
  https://cisofy.com/lynis/controls/MAIL-8818/

Suggestions (55):
-----
* This release is more than 4 months old. Check the website or GitHub to see if
there is an update available. [LYNIS]
  https://cisofy.com/lynis/controls/LYNIS/

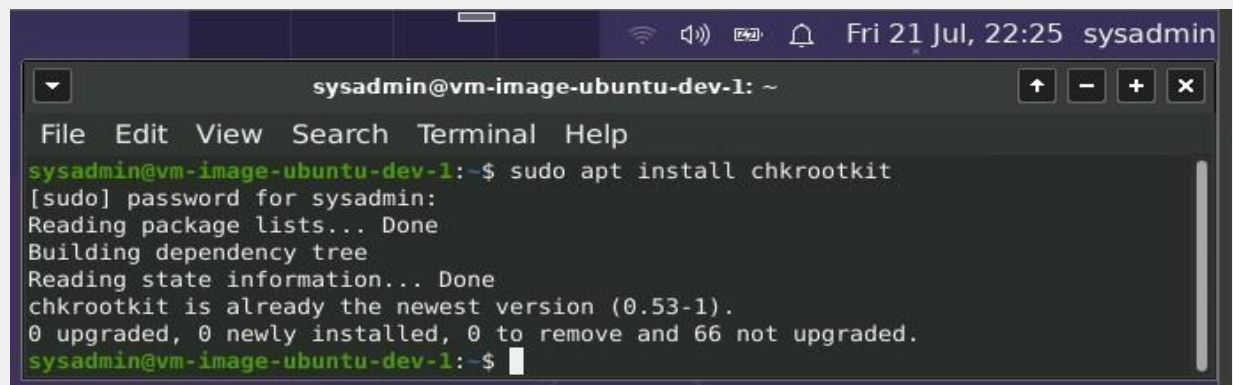
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g.
boot in single user mode without password) [B00T-5122]
  https://cisofy.com/lynis/controls/B00T-5122/

* Consider hardening system services [B00T-5264]
  - Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    https://cisofy.com/lynis/controls/B00T-5264/

* If not required, consider explicit disabling of core dump in /etc/security/lim...
```

Optional Additional Challenge

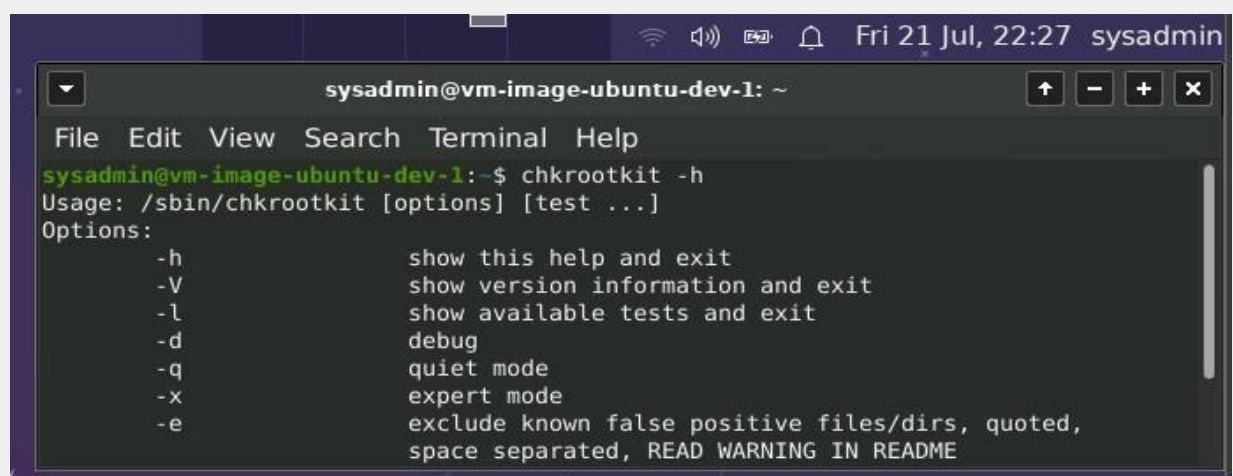
1. Command to install chkrootkit:



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) and system status (Fri 21 Jul, 22:25 sysadmin). The terminal shows the command 'sudo apt install chkrootkit' being executed. The output indicates that chkrootkit is already installed at version 0.53-1 and that no packages need to be upgraded or removed.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo apt install chkrootkit
[sudo] password for sysadmin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
chkrootkit is already the newest version (0.53-1).
0 upgraded, 0 newly installed, 0 to remove and 66 not upgraded.
sysadmin@vm-image-ubuntu-dev-1:~$
```

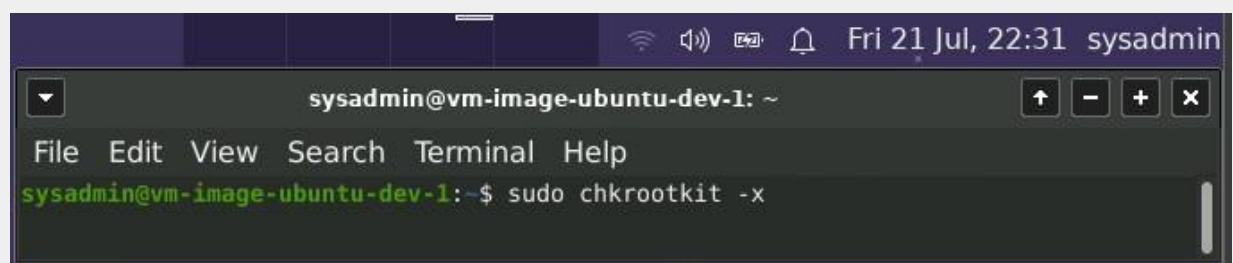
2. Command to view documentation and instructions:



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) and system status (Fri 21 Jul, 22:27 sysadmin). The terminal shows the command 'chkrootkit -h' being executed. The output displays the usage and options for the chkrootkit command.

```
sysadmin@vm-image-ubuntu-dev-1:~$ chkrootkit -h
Usage: /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
```

3. Command to run expert mode:

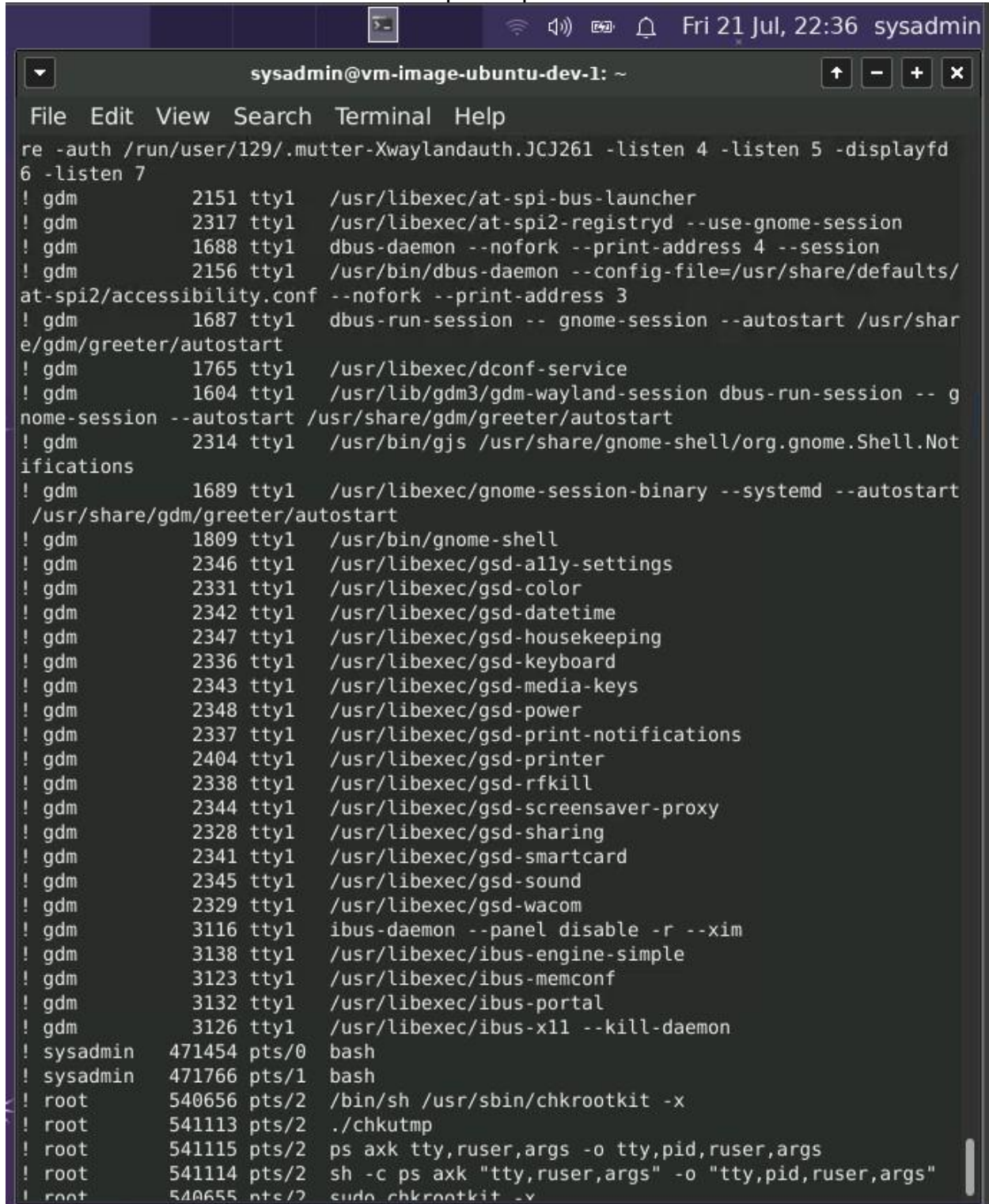


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) and system status (Fri 21 Jul, 22:31 sysadmin). The terminal shows the command 'sudo chkrootkit -x' being executed.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chkrootkit -x
```

4. Provide a report from the chrootkit output with recommendations for hardening the system.

a. Screenshot of end of sample output:



```
re -auth /run/user/129/.mutter-Xwaylandauth.JCJ261 -listen 4 -listen 5 -displayfd
6 -listen 7
! gdm          2151 tty1    /usr/libexec/at-spi-bus-launcher
! gdm          2317 tty1    /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1688 tty1    dbus-daemon --nofork --print-address 4 --session
! gdm          2156 tty1    /usr/bin/dbus-daemon --config-file=/usr/share/defaults/
at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1687 tty1    dbus-run-session -- gnome-session --autostart /usr/shar
e/gdm/greeter/autostart
! gdm          1765 tty1    /usr/libexec/dconf-service
! gdm          1604 tty1    /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- g
nome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2314 tty1    /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Not
ifications
! gdm          1689 tty1    /usr/libexec/gnome-session-binary --systemd --autostart
/usr/share/gdm/greeter/autostart
! gdm          1809 tty1    /usr/bin/gnome-shell
! gdm          2346 tty1    /usr/libexec/gsd-ally-settings
! gdm          2331 tty1    /usr/libexec/gsd-color
! gdm          2342 tty1    /usr/libexec/gsd-datetime
! gdm          2347 tty1    /usr/libexec/gsd-housekeeping
! gdm          2336 tty1    /usr/libexec/gsd-keyboard
! gdm          2343 tty1    /usr/libexec/gsd-media-keys
! gdm          2348 tty1    /usr/libexec/gsd-power
! gdm          2337 tty1    /usr/libexec/gsd-print-notifications
! gdm          2404 tty1    /usr/libexec/gsd-printer
! gdm          2338 tty1    /usr/libexec/gsd-rfkill
! gdm          2344 tty1    /usr/libexec/gsd-screensaver-proxy
! gdm          2328 tty1    /usr/libexec/gsd-sharing
! gdm          2341 tty1    /usr/libexec/gsd-smartcard
! gdm          2345 tty1    /usr/libexec/gsd-sound
! gdm          2329 tty1    /usr/libexec/gsd-wacom
! gdm          3116 tty1    ibus-daemon --panel disable -r --xim
! gdm          3138 tty1    /usr/libexec/ibus-engine-simple
! gdm          3123 tty1    /usr/libexec/ibus-memconf
! gdm          3132 tty1    /usr/libexec/ibus-portal
! gdm          3126 tty1    /usr/libexec/ibus-x11 --kill-daemon
! sysadmin     471454 pts/0    bash
! sysadmin     471766 pts/1    bash
! root         540656 pts/2    /bin/sh /usr/sbin/chkrootkit -x
! root         541113 pts/2    ./chkutmp
! root         541115 pts/2    ps axk tty,ruser,args -o tty,pid,ruser,args
! root         541114 pts/2    sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         540655 pts/2    sudo chkrootkit -x
```