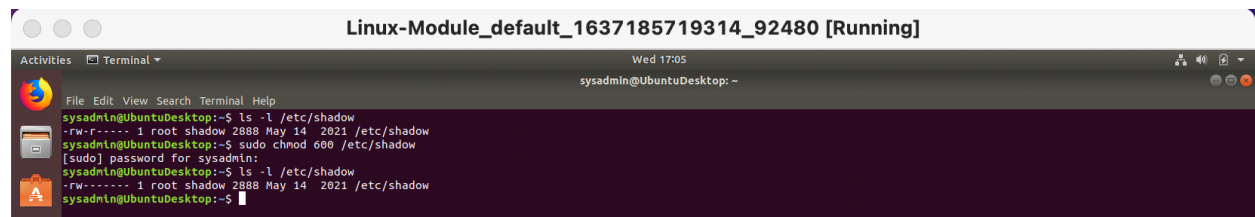


Week 4 Project Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

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

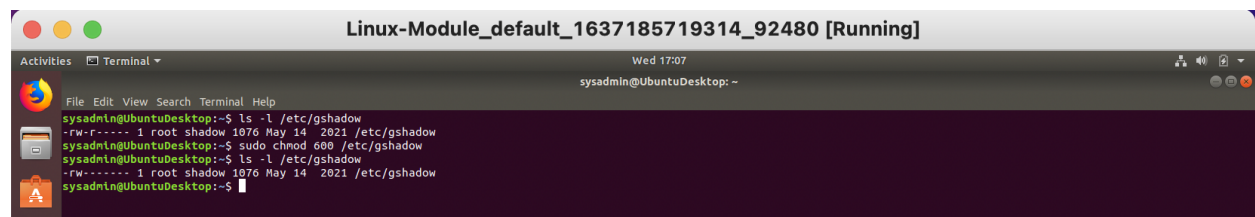
- Command to inspect permissions:
- Command to set permissions (if needed):



```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 2888 May 14 2021 /etc/shadow
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/shadow
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 2888 May 14 2021 /etc/shadow
sysadmin@UbuntuDesktop:~$
```

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

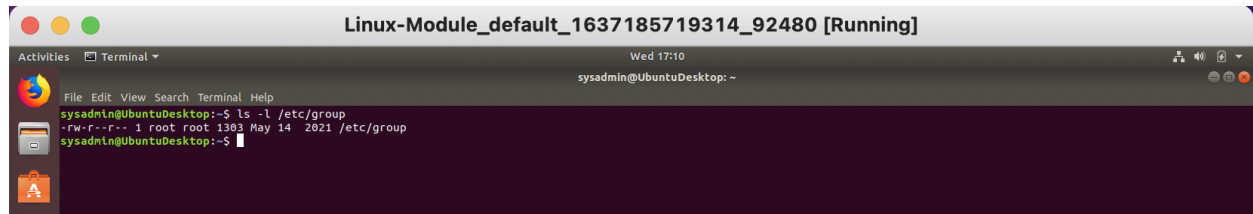
- Command to inspect permissions:
- Command to set permissions (if needed):



```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw-r----- 1 root shadow 1076 May 14 2021 /etc/gshadow
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/gshadow
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw-r----- 1 root shadow 1076 May 14 2021 /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:
- Command to set permissions (if needed): sudo chmod 600 /etc/group

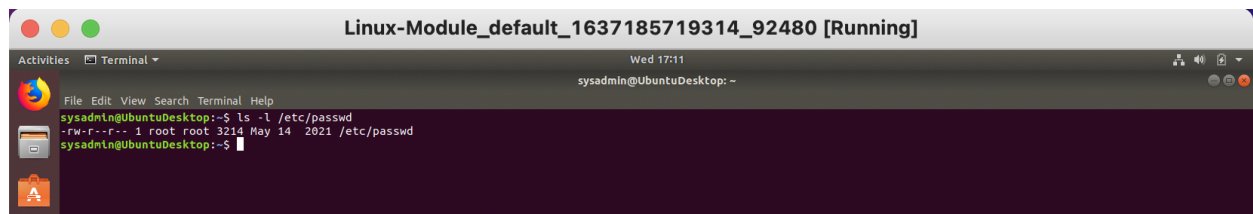


```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ls -l /etc/group
-rw-r--r-- 1 root root 1303 May 14 2021 /etc/group
sysadmin@UbuntuDesktop:~$
```

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

- Command to inspect permissions:
- Command to set permissions (if needed):

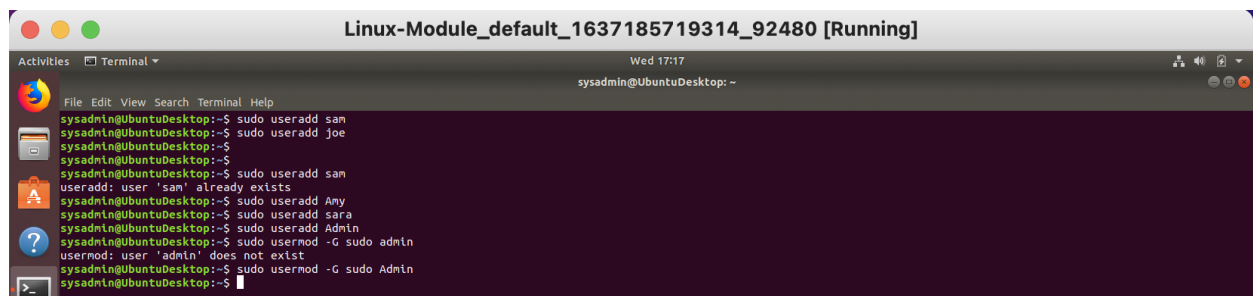
`sudo chmod 600 /etc/passwd`



```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3214 May 14 2021 /etc/passwd
sysadmin@UbuntuDesktop:~$
```

Step 2: Create User Accounts

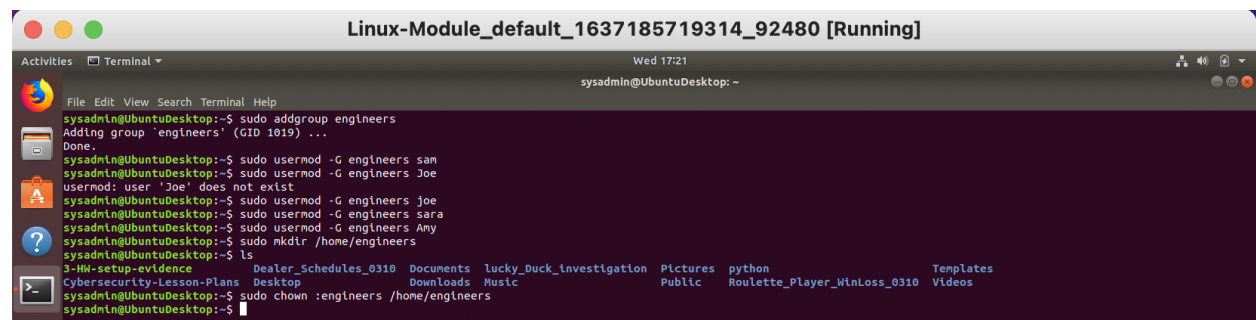
1. Add user accounts for sam, joe, amy, sara, and admin.
 - Command to add each user account (include all five users):
2. Ensure that only the admin has general sudo access.
 - Command to add admin to the sudo group:



```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo useradd sam
sysadmin@UbuntuDesktop:~$ sudo useradd joe
sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$ sudo useradd sam
useradd: user 'sam' already exists
sysadmin@UbuntuDesktop:~$ sudo useradd Amy
sysadmin@UbuntuDesktop:~$ sudo useradd sara
sysadmin@UbuntuDesktop:~$ sudo useradd Admin
sysadmin@UbuntuDesktop:~$ sudo usermod -G sudo admin
usermod: user 'admin' does not exist
sysadmin@UbuntuDesktop:~$ sudo usermod -G sudo Admin
sysadmin@UbuntuDesktop:~$
```

Step 3: Create User Group and Collaborative Folder

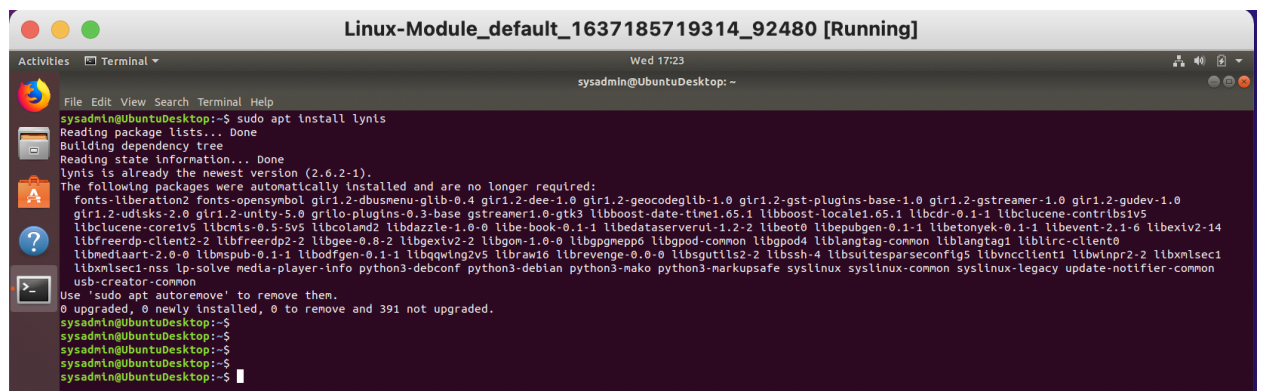
1. Add an engineers group to the system.
 - Command to add group:
2. Add users sam, joe, amy, and sara to the managed group.
 - Command to add users to engineers group (include all four users):
3. Create a shared folder for this group at /home/engineers.
 - Command to create the shared folder:
4. Change ownership on the new engineers' shared folder to the engineers group.
 - Command to change ownership of engineer's shared folder to engineer group:



```
Linux-Module_default_1637185719314_92480 [Running]
Wed 17:21
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo addgroup engineers
Adding group 'engineers' (GID 1019) ...
Done.
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers sam
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers Joe
usermod: user 'Joe' does not exist
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers joe
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers sara
sysadmin@UbuntuDesktop:~$ sudo usermod -G engineers Amy
sysadmin@UbuntuDesktop:~$ sudo mkdir /home/engineers
sysadmin@UbuntuDesktop:~$ ls
Dealer_Schedules_0310 Documents Lucky_Duck_Investigation Pictures python
Cybersecurity-Lesson-Plans Desktop Downloads Music Public Roulette_Player_WinLoss_0310 Templates
sysadmin@UbuntuDesktop:~$ sudo chown :engineers /home/engineers
sysadmin@UbuntuDesktop:~$
```

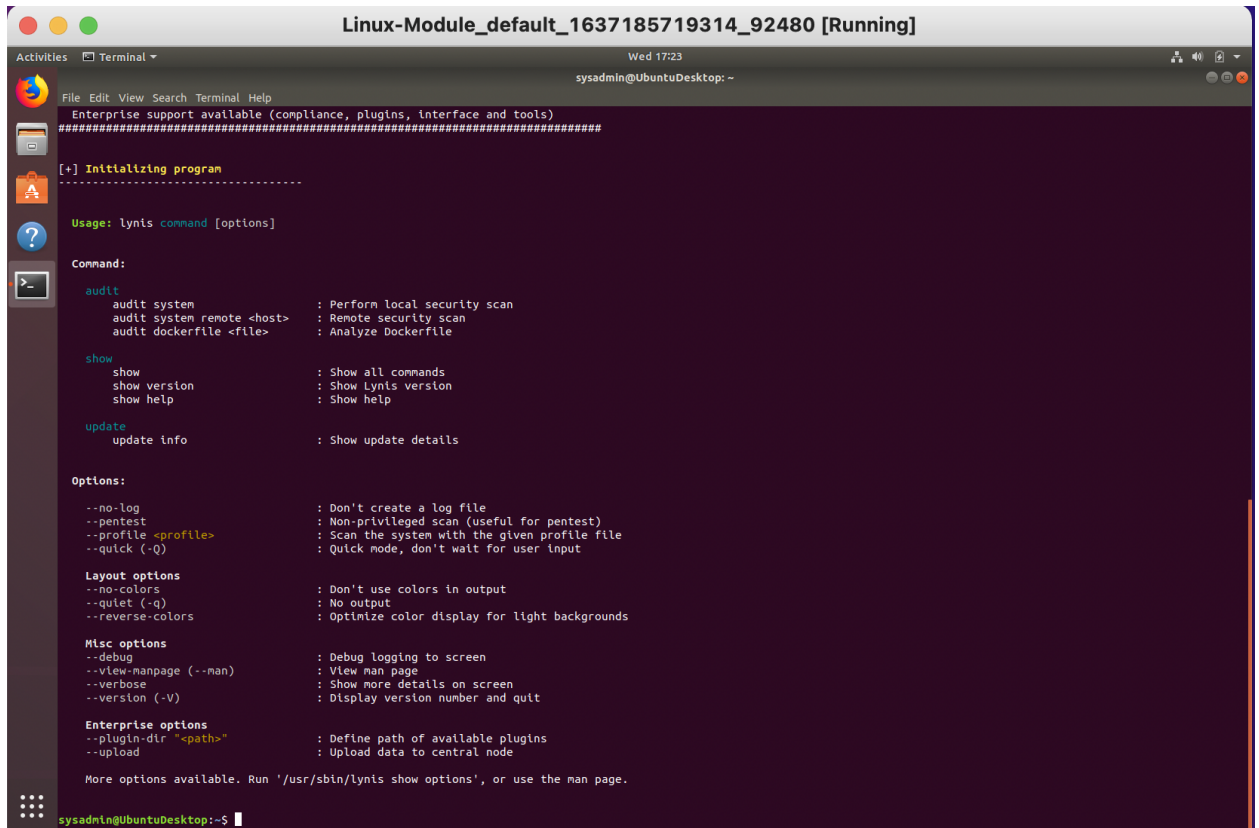
Step 4: Lynis Auditing

1. Command to install Lynis:



```
Linux-Module_default_1637185719314_92480 [Running]
Wed 17:23
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
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).
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 libbdr-0.1-1 libclucene-contribs1v5
 libclucene-core1v5 libcnis-0.5-5v5 libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedatasecserverutil-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 libgpgod-common libgpgod4 liblangtag-common liblangtag1 liblirc-client0
 libmediaart-2.0-0 libnspub-0.1-1 libodfgen-0.1-1 libqgwin2v5 libraw16 librevenge-0.0-0 libsgutls2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxmlsec1
 libxmlsec1-nss lp-solve media-player-info python3-debconf python3-debian python3-nako python3-markupsafe syslinux syslinux-common syslinux-legacy update-notifier-common
 usb-creator-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 391 not upgraded.
sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$
sysadmin@UbuntuDesktop:~$
```

2. Command to see documentation and instructions:



The screenshot shows a terminal window titled "Linux-Module_default_1637185719314_92480 [Running]". The window contains the Lynis help menu, which lists various commands and options. The commands include audit, show, update, and options. The options are categorized into Layout options, Misc options, and Enterprise options. The terminal prompt is "sysadmin@UbuntuDesktop: ~\$".

```
Linux-Module_default_1637185719314_92480 [Running]
Activities Terminal
Wed 17:23
sysadmin@UbuntuDesktop: ~

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

  update
    update info           : Show update details

Options:
  --no-log                : Don't create a log file
  --pentest               : Non-privileged scan (useful for pentest)
  --profile <profile>     : Scan the system with the given profile file
  --quick (-Q)            : Quick mode, don't wait for user input

Layout options
  --no-colors             : Don't use colors in output
  --quiet (-q)            : No output
  --reverse-colors        : Optimize color display for light backgrounds

Misc options
  --debug                 : Debug logging to screen
  --view-manpage (--man)  : View man page
  --verbose               : Show more details on screen
  --version (-V)          : Display version number and quit

Enterprise options
  --plugin-dir <path>    : Define path of available plugins
  --upload                : Upload data to central node

More options available. Run '/usr/sbin/lynis show options', or use the man page.

sysadmin@UbuntuDesktop: ~$
```

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_1637185719314_92480 [Running]
Activities Terminal
File Edit View Search Terminal Help
Wed 17:29
sysadmin@UbuntuDesktop: ~

-----
-[ Lynis 2.6.2 Results ]-
-----
Warnings (4):
-----
! 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/

Suggestions (53):
-----
* Install libpam-tmpdir to set STMP and TMPDIR for PAM sessions [CUST-0280]
https://your-domain.example.org/controls/CUST-0280/

* 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 debsecan 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://cisofy.com/controls/DEB-0880/

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