## **Week 4 Homework Submission File: Linux Systems Administration**

\*\*Note – all commands to run are light blue in sequence

# are explanations of the commands used

### **Step 1: Ensure Permissions on Sensitive Files**

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

**Open Terminal login into sysadmin from ~ navigate to /etc**

**Run the command:**

ls -al /etc/shadow

# -l list files in long format -a shows hidden files

* + Command to set permissions (if needed):

sudo chmod 600 /etc/shadow

#chmod sets file permissions

1. Permissions on /etc/gshadow should allow only root read and write access.  
   * Command to inspect permissions:

ls -al /etc/gshadow

* + Command to set permissions (if needed):

sudo chmod 600 /etc/gshadow

#chmod sets file permissions

1. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions:

ls -al /etc/group

* + Command to set permissions (if needed):

sudo chmod 644 /etc/group

#chmod sets file permissions

1. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions:

ls -al /etc/passwd

* + Command to set permissions (if needed):

sudo chmod 644 /etc/passwd

#chmod sets file permissions

### **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):

**Move to the /home directory and run the following command:**

for u in sam joe amy sara admin; do sudo useradd -m $u; echo "$u:Password" | sudo chpasswd $u; done

Check users are created, run: sudo tail -n5 /etc/shadow /etc/passwd

#for u – creates multiple users with u being the variable

#useradd -m adds a home directory

#echo $u:Password – creates a default user password as “Password”

#chpasswd – command reads a list of user name and password pairs from

standard input and uses this information to update a group of existing

users. Each line is of the format: user\_name:password

1. **Force users to create 16-character passwords incorporating numbers and symbols.**

**From /home directory and run the following command:**

for u in sam joe amy sara admin; do sudo chage -d 0 $u; done

* + Command to edit pwquality.conf file:

**Move to /etc/security run:**

sudo nano /etc/security/pwquality.conf

#navigate down the list to make required changes to pwquality

* + Updates to configuration file:

minclass = 4

minlen = 16

1. **Force passwords to expire every 90 days**.  
   * Command to set each new user's password to expire in 90 days (include all five users):

**From /etc/security run:**

for u in sam joe amy sara admin; do sudo chage -M 90 $u; done

1. **Ensure that only the admin has general sudo access.**

**#Check: sudo visudo for admin access**

* + Command to add admin to the sudo group:

sudo usermod -aG sudo admin

### **Step 3: Create User Group and Collaborative Folder**

1. **Add an engineers group to the system.**
   * Command to add group:

sudo addgroup engineers

1. **Add users sam, joe, amy, and sara to the managed group.**
   * Command to add users to engineers group (include all four users):

for u in sam joe amy sara; do sudo usermod -G engineers $u; done

#check: grep 'engineers' /etc/group

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

sudo mkdir /home/engineers

1. **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 root:engineers engineers

1. **Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory**.  
   * Command to set SGID and sticky bit to shared folder:

sudo chmod g+s,o+t /home/engineers

### **Step 4: Lynis Auditing**

1. Command to install Lynis:

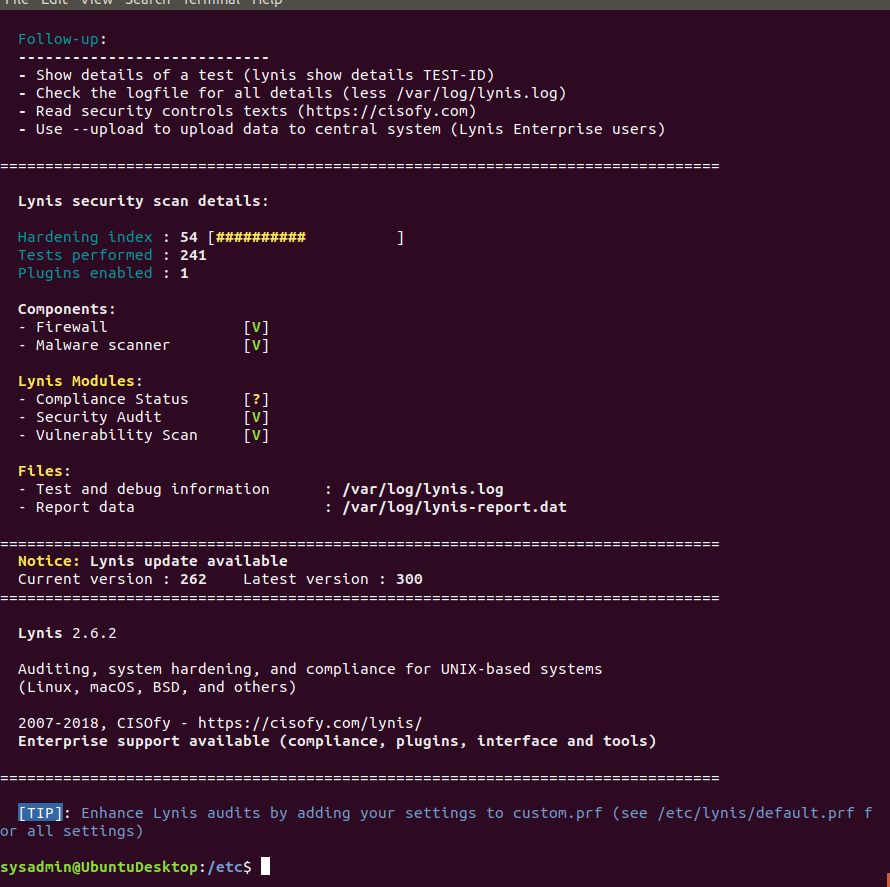
sudo apt -y install lynis

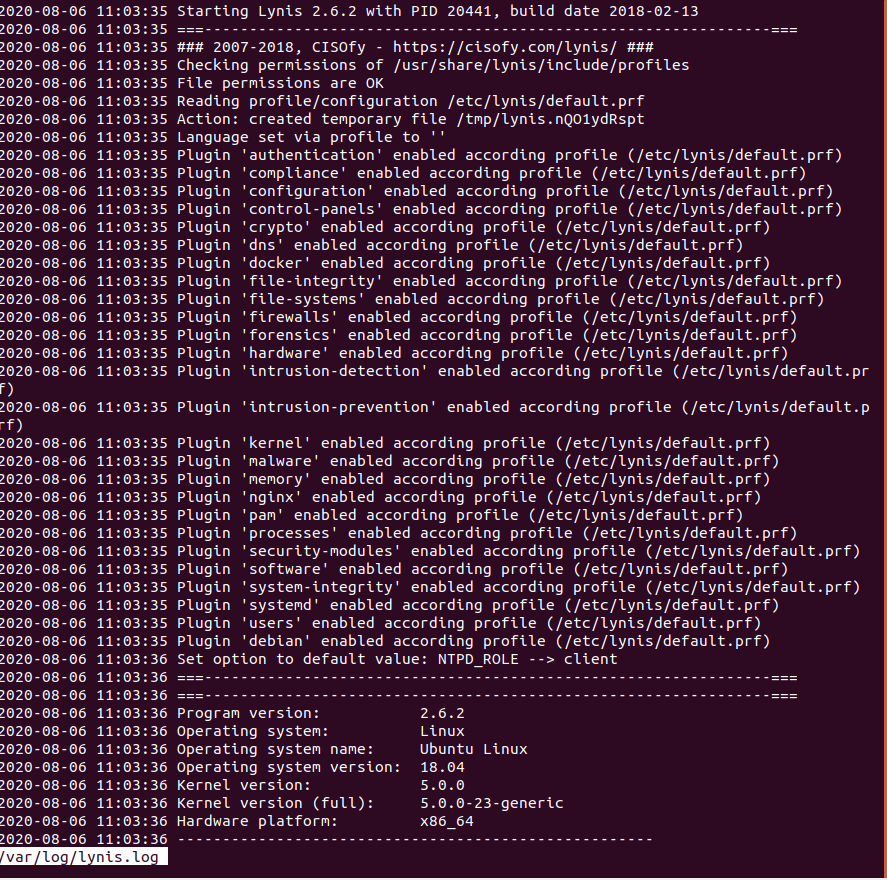
1. Command to see documentation and instructions: man lynis
2. Command to run an audit: sudo lynis audit system
3. Provide a report from the Lynis output on what can be done to harden the system.  
   * Screenshot of report output:

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

-[ Lynis 2.6.2 Results ]-

Warnings (5):





### **Bonus**

1. Command to install chkrootkit: sudo apt -y install chkrootkit
2. Command to see documentation and instructions: man chkrootkit
3. Command to run expert mode:

sudo chkrootkit -x

sudo chkrootkit -q

sudo chkrootkit | grep INFECTED

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

