Step 1: Ensure/Double Check Permissions on Sensitive Files

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

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

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

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

Step 2: Create User Accounts

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

Command to add each user account (include all five users):

Ensure that only the admin has general sudo access.

-sudo adduser —system—no-create-home Sam

-sudo adduser —system—no-create-home joe

-sudo adduser —system—no-create-home amy

-sudo adduser —system—no-create-home sara

-sudo adduser —system—no-create-home admin

Command to add admin to the sudo group:

-sudo visudo

Step 3: Create User Group and Collaborative Folder

Add an engineers group to the system.

Command to add group:

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

-sudo addgroup engineers

Command to add users to engineers group (include all four users):

-sudo usermod -aG engineers sam

-sudo usermod -aG engineers joe

-sudo usermod -aG engineers amy

-sudo usermod -aG engineers sara

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

Command to create the shared folder:

-sudo mkdir /home/engineers

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 chgrp engineers /home/engineers/

Step 4: Lynis Auditing

Command to install Lynis:

-sudo apt-get install lynis

Command to see documentation and instructions:

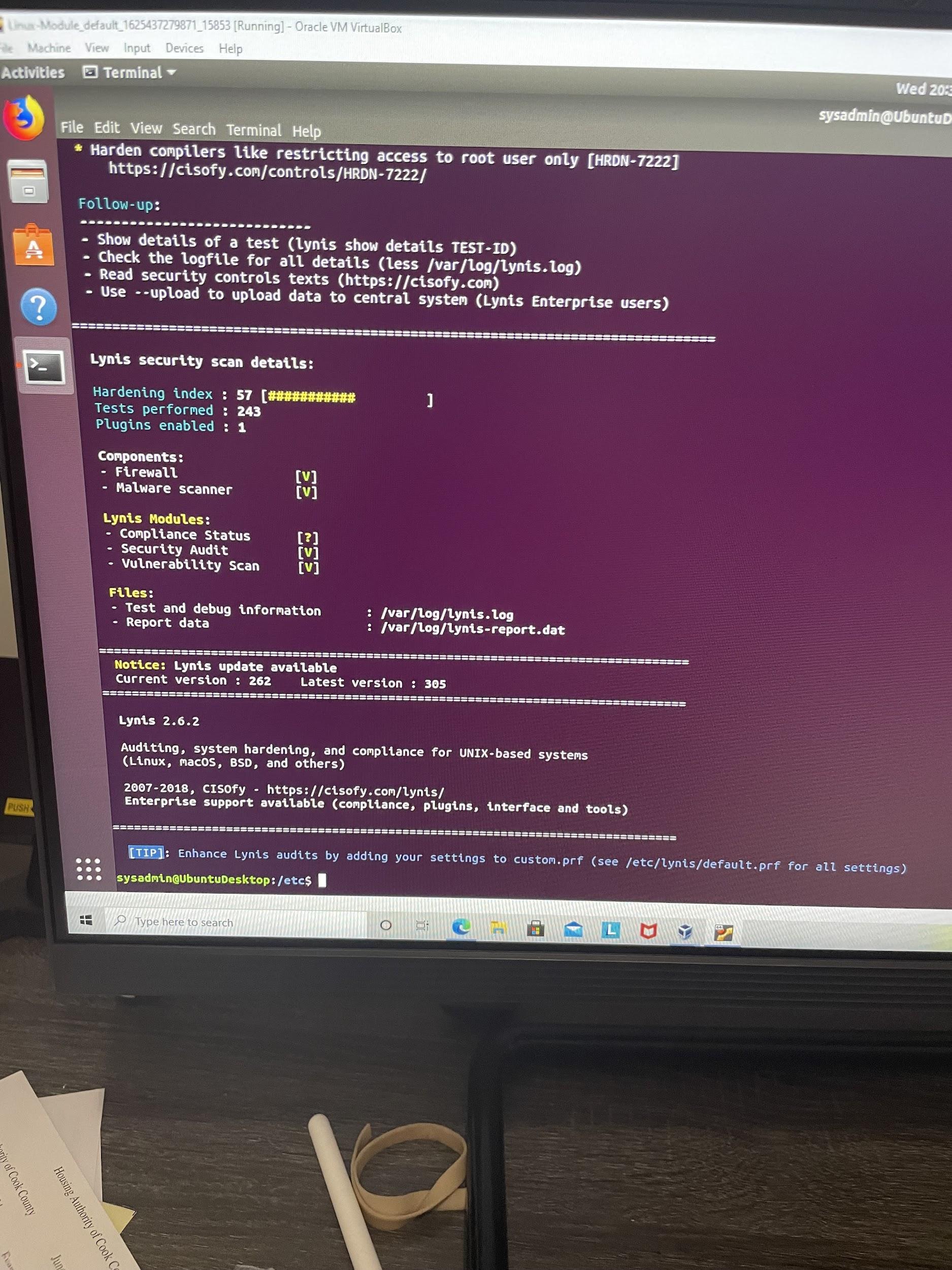
-man lynis

Command to run an audit:

-sudo lynis audit system

Provide a report from the Lynis output on what can be done to harden the system.

Screenshot of report output:



Bonus

Command to install chkrootkit:

-sudo apt install chkrootkit

Command to see documentation and instructions:

-man chkrootkit

Command to run expert mode:

-sudo chkrootkit

Provide a report from the chrootkit output on what can be done to harden the system.

Screenshot of end of sample output:

