|  |
| --- |
| Cybersecurity |
| 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.
   1. Command to inspect permissions:

|  |
| --- |
| Ls -l etc/shadow |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chmod 600 /etc/shadow |

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

|  |
| --- |
| Ls -l /etc/gshadow |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chmod 600 /etc/gshadow |

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

|  |
| --- |
| Ls -l /etc/group |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chmod 644 /etc/group |

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

|  |
| --- |
| Ls -l /etc/passwd |

* 1. Command to set permissions (if needed):

|  |
| --- |
| sudo chmod 644 /etc/passwd |

### Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin with the useradd command.
   1. 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 |

1. Ensure that only the admin has general sudo access.
   1. 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.
   1. Command to add group:

|  |
| --- |
| Sudo addgroup engineers |

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

|  |
| --- |
| Sudo usermod -aG sudo engineers sam  Sudo usermod -aG sudo engineers joe  Sudo usermod -aG sudo engineers amy  Sudo usermod -aG sudo engineers sara |

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

|  |
| --- |
| Sudo mkdir /home/engineers |

1. Change ownership on the new engineers’ shared folder to the engineers group.
   1. Command to change ownership of engineers’ shared folder to engineers group:

|  |
| --- |
| Sudo chown :engineers /home/engineers |

### Step 4: Lynis Auditing

1. Command to install Lynis:

|  |
| --- |
| Sudo apt install lynis |

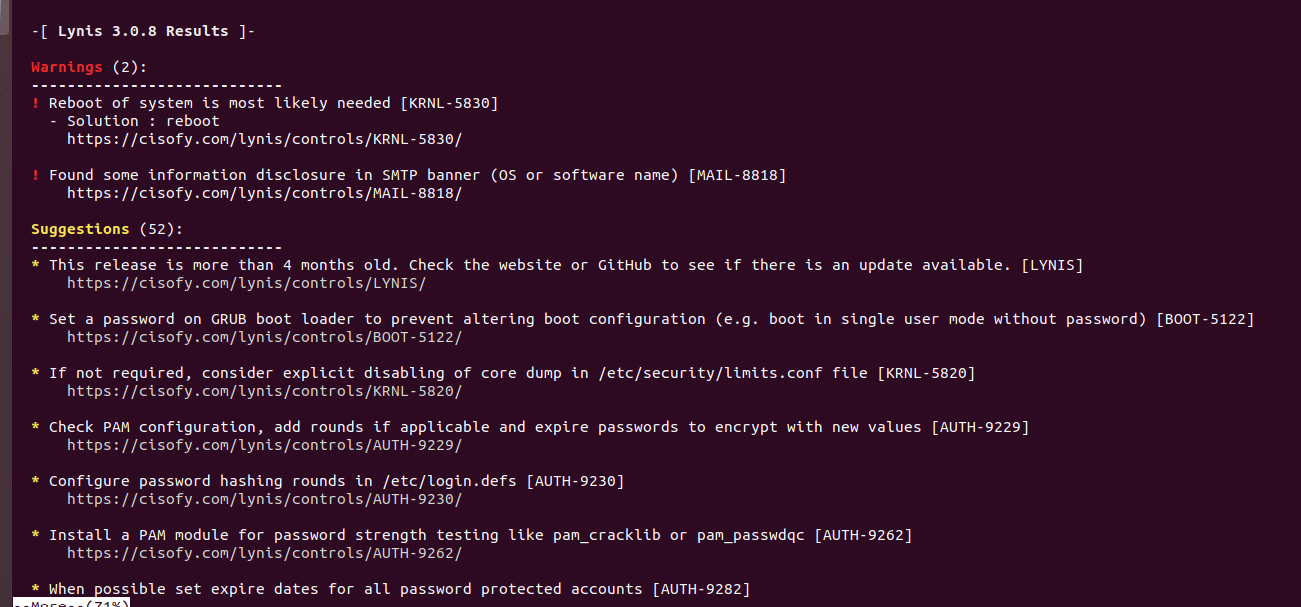
1. Command to view documentation and instructions:

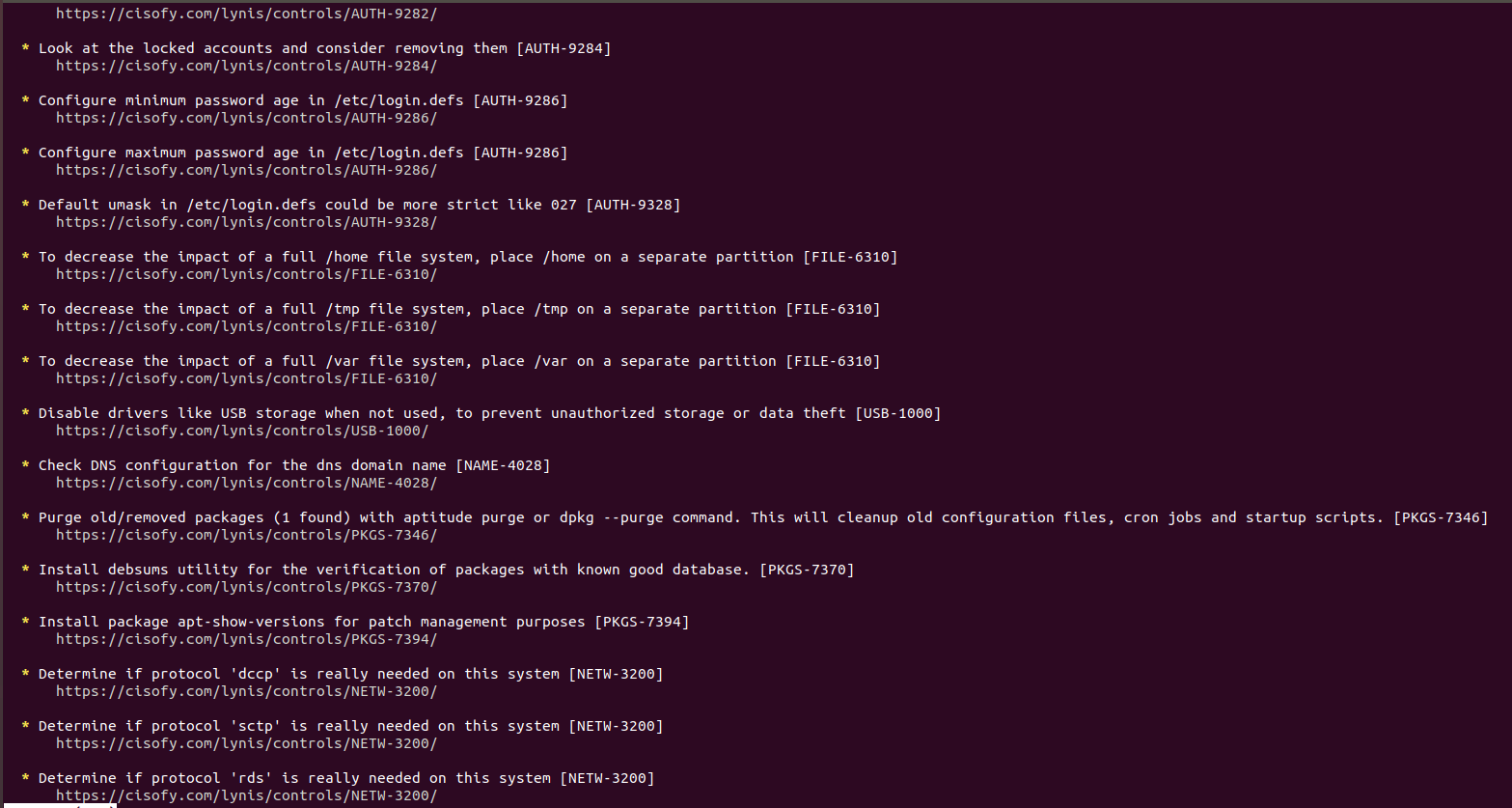
|  |
| --- |
| Man lynis |

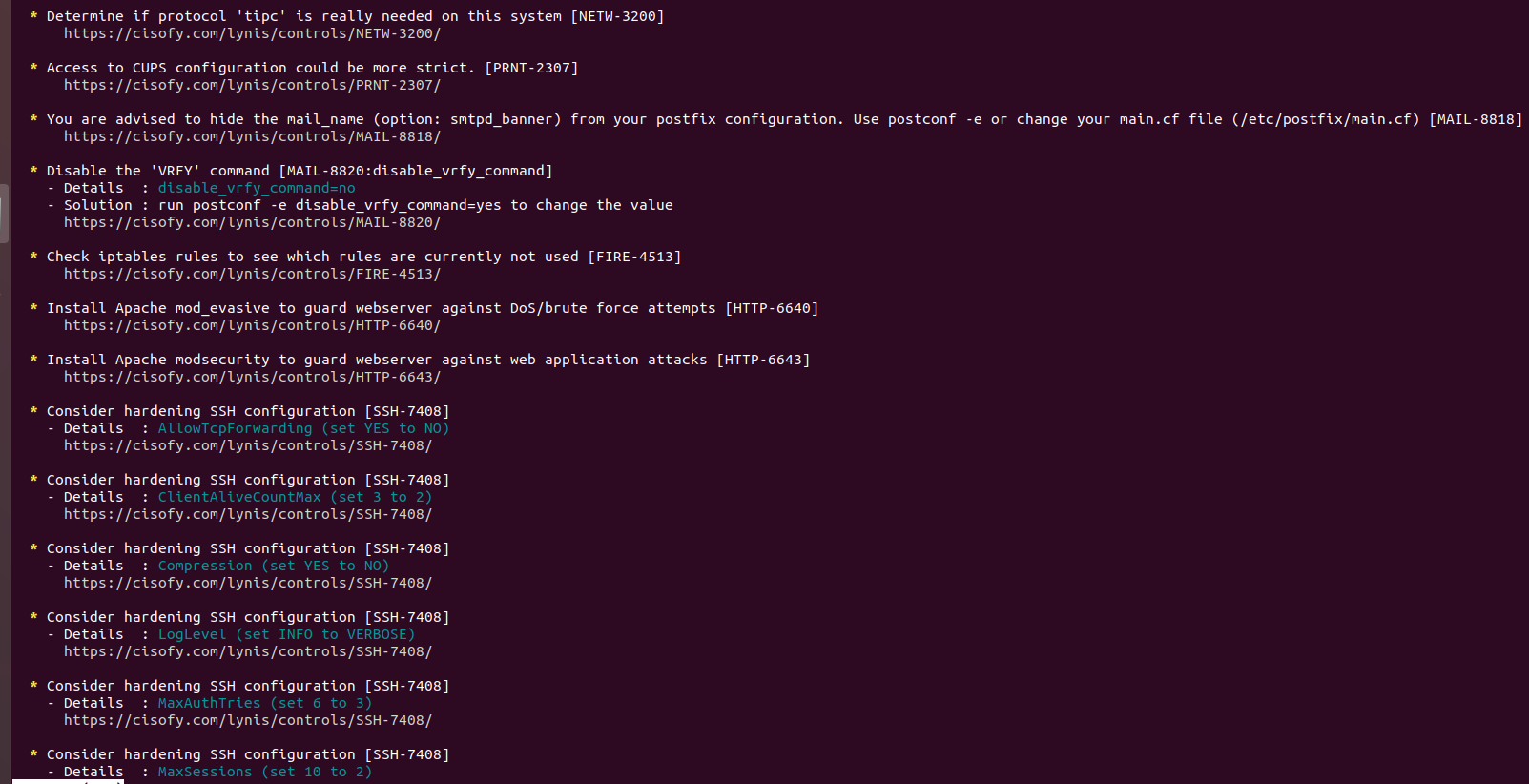
1. Command to run an audit:

|  |
| --- |
| Sudo lynis audit system |

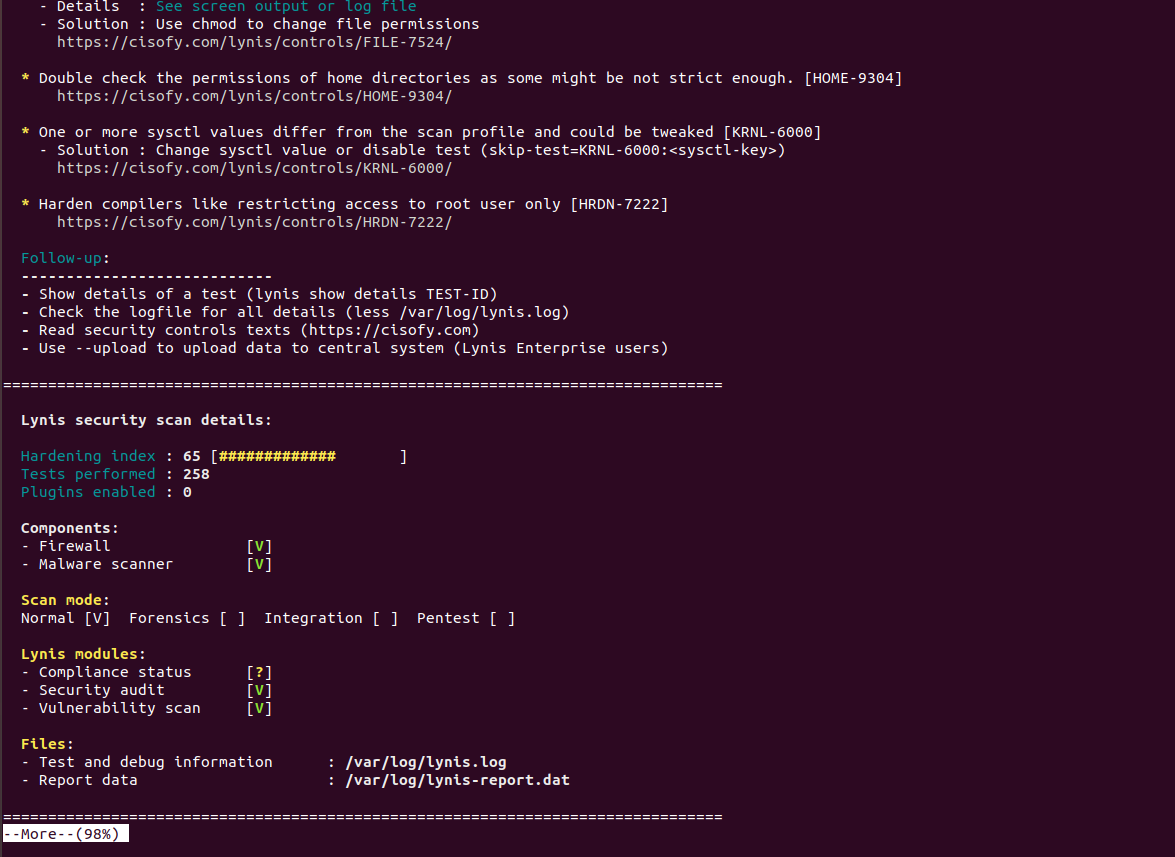
1. Provide a report from the Lynis output with recommendations for hardening the system.
   1. We will need to require a password for all users. Need to change the permissions on /etc/sudoers.d
   2. Check file permissions on printers and spools
   3. Change postfix banner for email.
   4. Check permissions in home directories.

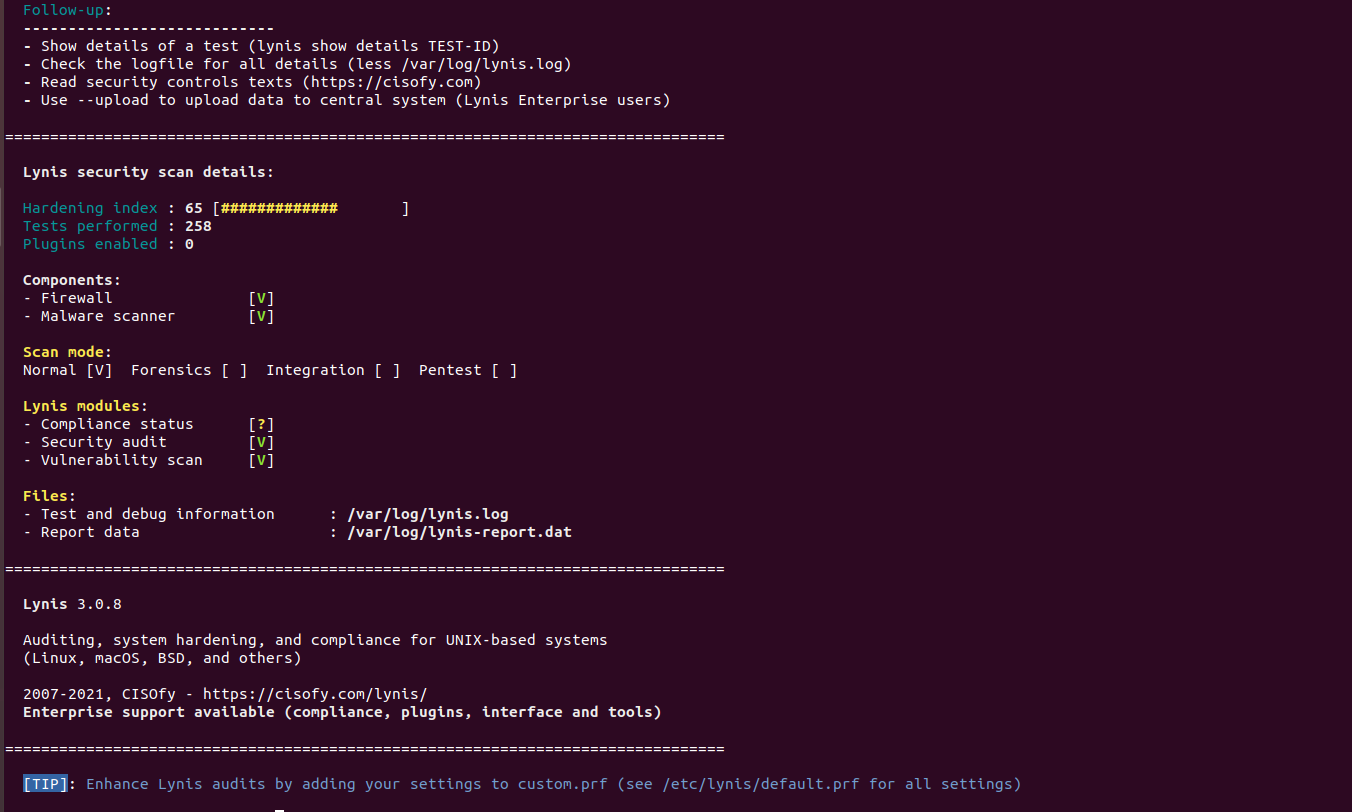






### Bonus



1. Command to install chkrootkit:

|  |
| --- |
| Sudo apt-get install chkrootkit |

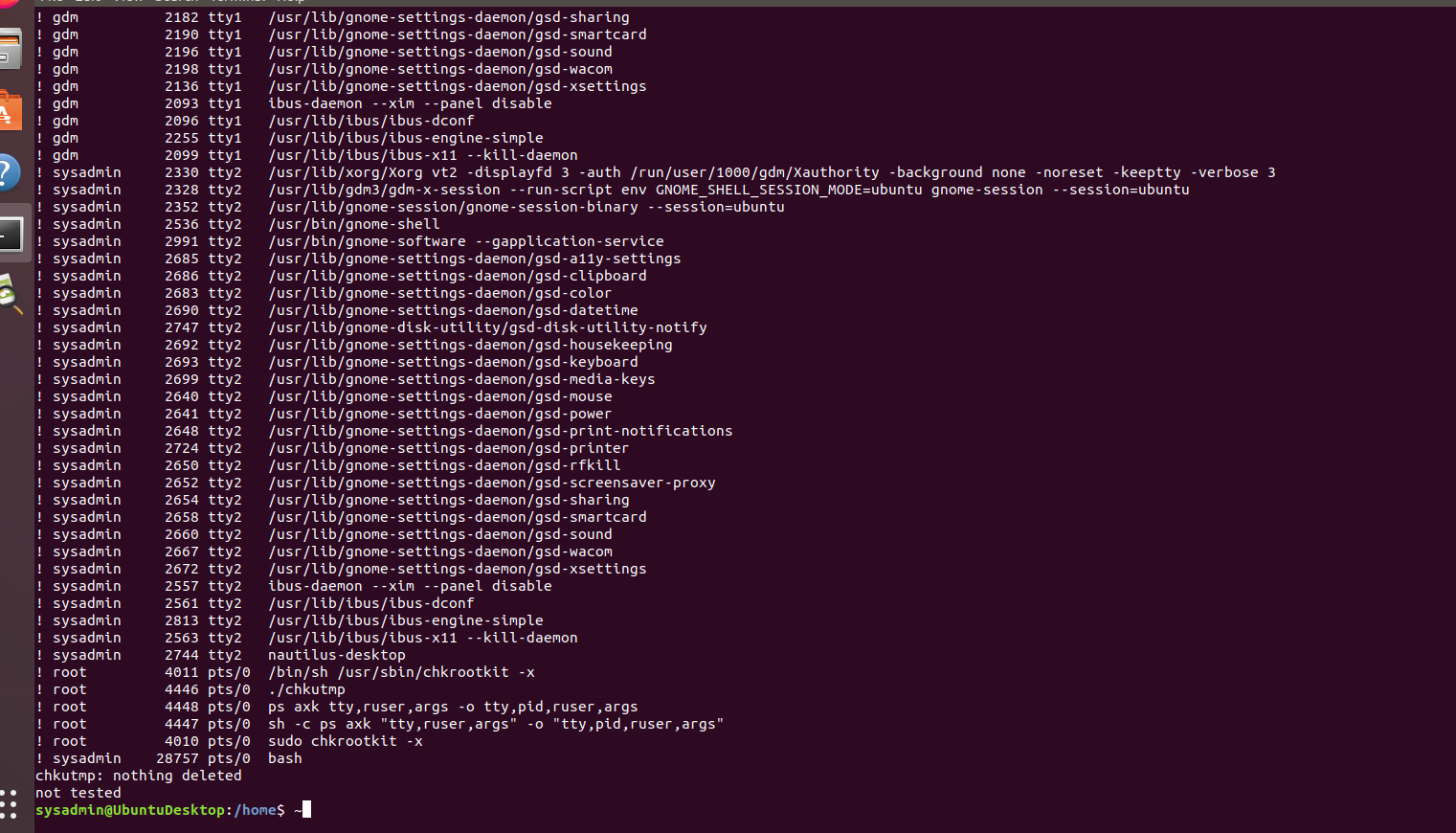
1. Command to view documentation and instructions:

|  |
| --- |
| Man checkrootkit |

1. Command to run expert mode:

|  |
| --- |
| Sudo chkrootkit -x |

1. Provide a report from the chrootkit output with recommendations for hardening the system.
   1. Screenshot of end of sample output:



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.