| 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 shadow  Because the owner is already root, we do not need to change the owner. |
| --- |

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 gshadow  Because the owner is already root, we do not need to change the owner. |
| --- |

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 group  Because the owner is already root, we do not need to change the owner. |
| --- |

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  Because the owner is already root, we do not need to change the owner. |
| --- |

### **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 engineers sam  sudo usermod -aG engineers joe  sudo usermod -aG engineers amy  sudo usermod -aG 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 engineers |
| --- |

### Step 4: Lynis Auditing

1. Command to install Lynis:

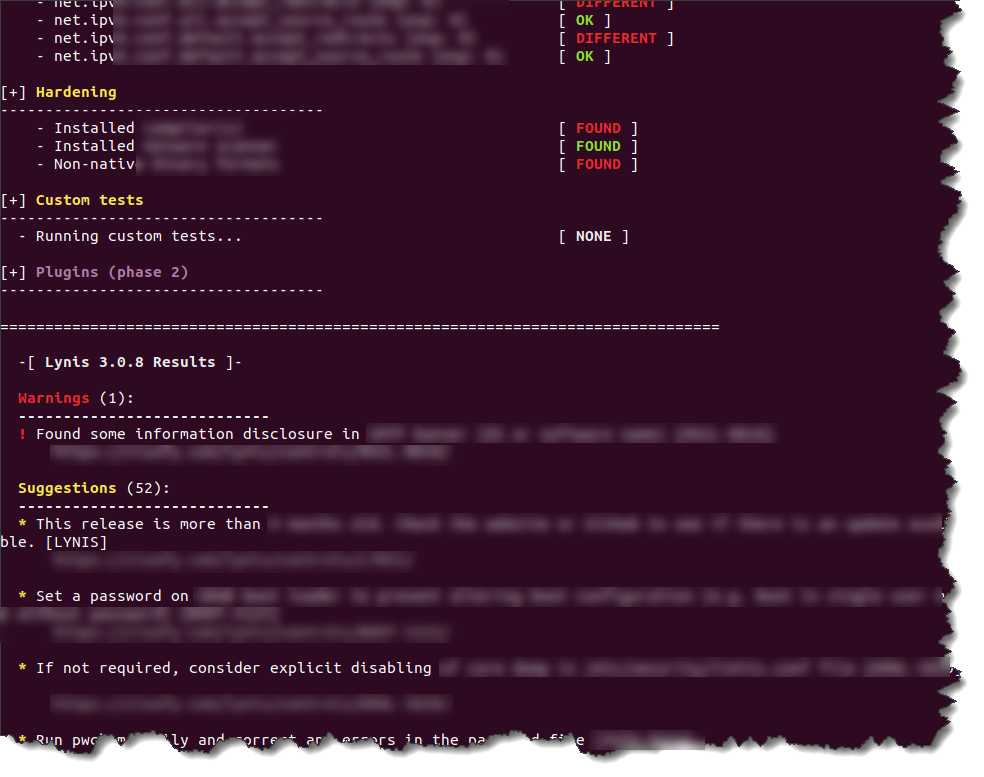
| sudo apt install lynis |
| --- |

1. Command to view documentation and instructions:

| man lynis – this will give you a complete and full manual entry for lynis  lynis --help – this will give you an abbreviated help document for the program |
| --- |

1. Command to run an audit:

| lynis audit <type>  Recommended for the first time running the Lynis to run the following:  lynis audit system (which is also the most common type of audit). |
| --- |

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

### Bonus

1. Command to install chkrootkit:

| sudo apt install chkrootkit |
| --- |

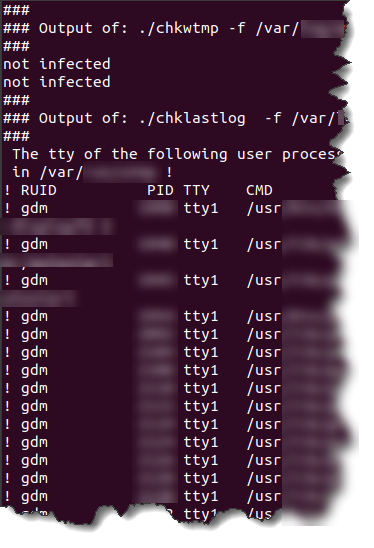
1. Command to view documentation and instructions:

| man chkrootkit – this will give you a complete and full manual entry for lynis  chkrootkit --help – this will give you an abbreviated help document for the program |
| --- |

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.