| 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:

| A computer screen with text and numbers  Description automatically generated |
| --- |

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

| A screenshot of a computer  Description automatically generated |
| --- |

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

| A computer screen shot of a program  Description automatically generated |
| --- |

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

| A computer screen with text on it  Description automatically generated |
| --- |

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

| A screenshot of a computer  Description automatically generated |
| --- |

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

| No need to set permissions because the group file already has permissions that allow only ‘root’ read and write access and allow everyone else read access only. |
| --- |

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

| A screenshot of a computer  Description automatically generated |
| --- |

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

| No need to set permissions because the passwd file already has permissions that allow only ‘root’ read and write access and allow everyone else read access only. |
| --- |

### Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin1 with the useradd command.
   1. Command to add each user account (include all five users):

| A screenshot of a computer  Description automatically generated  A screenshot of a computer program  Description automatically generated |
| --- |

1. Ensure that only the admin1 has general sudo access.
   1. Command to add admin1 to the sudo group:

| A screenshot of a computer  Description automatically generated |
| --- |

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

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

| A screenshot of a computer  Description automatically generated |
| --- |

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

| A screenshot of a computer  Description automatically generated |
| --- |

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

| A screenshot of a computer  Description automatically generated |
| --- |

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:

| A screenshot of a computer  Description automatically generated |
| --- |

### Step 4: Lynis Auditing

1. Command to install Lynis:

| A screenshot of a computer  Description automatically generated |
| --- |

1. Command to view documentation and instructions:

| A screenshot of a computer  Description automatically generated |
| --- |

1. Command to run an audit:

|  |
| --- |

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

A screenshot of a computer

Description automatically generated

Optional Additional Challenge

1. Command to install chkrootkit:

| A screenshot of a computer  Description automatically generated |
| --- |

1. Command to view documentation and instructions:

| A screenshot of a computer  Description automatically generated |
| --- |

1. Command to run expert mode:

| A screenshot of a computer  Description automatically generated |
| --- |

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

A screenshot of a computer

Description automatically generated

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