Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Step 1: Access the template

Access the template (File permissions in Linux)

Step 2: Access supporting materials

The following supporting materials will help you complete this activity.

The **Instructions for including Linux commands** document provides instructions and best practices for including samples of Linux commands in your portfolio activity.

Navigate to the supporting material (Instructions for including Linux commands)

The **Current file permissions** document demonstrates how the file structure is built for this portfolio activity. The file permissions for each file or directory are also provided.

Navigate to the supporting material (Current file permissions)

Note: It is recommended that you use the **Manage authorization** lab to complete this portfolio activity. If you're revisiting the lab, using the **Current file permissions** document is optional because this file structure has already been created for you.

Step 3: Identify the type of attack causing this network interruption

In the **Manage authorization** lab, check the permissions set for files and subdirectories in the `projects` directory. Make sure you display all permissions, including hidden files. Or, use the content of the **Current file permissions** document to determine the current permissions.

Describe the command you can use to check permissions in the Check file and directory details section of the **File permissions in Linux** template. From the lab, take a screenshot of the Linux command you used. Or, type this command directly into the template.

Then, use either the output of this command in the lab or the content or the **Current file permissions** document to indicate the current permissions. If using the **Current file permissions** document, write these in the 10-character string that would be part of the command's output.

Step 4: Explain how the attack is causing the website to malfunction

Choose one example from the output in the previous step. In the **Describe the permissions string** section of the **File permissions in Linux** template, write a short description that explains the 10-character string in the example. You should describe what the 10-character string is for and what each character represents.

.

Step 5: Change file permissions

The organization does not allow others to have write access to any files. Based on the permissions established in Step 3, identify which file needs to have its permissions modified. Use a Linux command to modify these permissions.

Describe the command you used and its output in the **Change file permissions** section of the **File permissions in Linux** template. In the **Manage authorization** lab, take a screenshot of the Linux command you used. Or, type this command directly into the template.

Step 6: Change file permissions on a hidden file

The research team has archived `.project_x.txt`, which is why it's a hidden file. This file should not have write permissions for anyone, but the user and group should be able to read the file. Use a Linux command to assign `.project_x.txt` the appropriate authorization.

Describe the command you used and its output in the **Change file permissions** on a hidden file section of the **File permissions in Linux** template. In the **Manage**

authorization lab, take a screenshot of the Linux command you used. Or, type this command directly into the template.

Step 7: Change directory permissions

The files and directories in the projects directory belong to the **`researcher2`** user. Only **`researcher2`** should be allowed to access the **`drafts`** directory and its contents. Use a Linux command to modify the permissions accordingly.

Describe the command you used and its output in the **Change directory permissions** section of the **File permissions in Linux** template. In the **Manage authorization** lab, take a screenshot of the Linux command you used. Or, type this command directly into the template.

Step 8: Finalize your document

To finalize the document and make its purpose clear to potential employers, be sure to complete the **Project description** and **Summary** sections of the **File permissions in Linux** template.

In the Project description section, give a general overview of the scenario and what you accomplish through Linux. Write two to four sentences.
In the Summary section, provide a short summary of the previous tasks and connect them to the scenario. Write approximately two to four sentences.

What to Include in Your Response

Be sure to include the following in your completed activity:

- Screenshots of your commands or typed versions of the commands
- Explanations of your commands
- A project description at the beginning
- A summary at the end
- Details on using **`chmod`** to update file permissions
- Details on checking file permissions with **`ls -la`**
- Details on interpreting the 10-character string that represents file permissions
- Details on hidden files and directories

Step 9: Assess your activity

The following is a self-assessment for your Use Linux commands to manage file permissions portfolio activity. You will use these statements to review your own work.

The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your Use of Linux commands to manage file permissions portfolio activity.