Portfolio Activity: Use Linux commands to manage file permissions

To pass this course item, you must complete the activity and receive at least 80%, or 7 out of 8 points, on the questions that follow. Once you have completed the activity and questions, review the feedback provided. You can learn more about graded and practice items in the course overview.

Activity Overview

In this activity, you will create a new portfolio document to demonstrate your experience using Linux commands to manage file permissions. You can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. To review the importance of building a professional portfolio and options for creating your portfolio, read Create a cybersecurity portfolio.
To create your portfolio document, you will review a scenario and follow a series of steps. This scenario is connected to the lab you have just completed about how to examine and manage file permissions. You will explain the commands you used in that lab, and this will help you prepare for future job interviews and other steps in the hiring process.
Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the scenario below. Then, complete the step-by-step instructions.
You are a security professional at a large organization. You mainly work with their research team. Part of your job is to ensure users on this team are authorized with the appropriate permissions. This helps keep the system secure.
Your task is to examine existing permissions on the file system. You'll need to determine if the permissions match the authorization that should be given. If they do not match, you'll need to modify the permissions to authorize the appropriate users and remove any unauthorized access.
Note: This scenario involves investigating and updating the same file permissions as the ones in the Manage authorization lab. You can revisit the lab to get screenshots to include in your portfolio document. If you choose, it's also possible to complete this activity without revisiting the lab by typing your commands in the template.

Step-By-Step Instructions

Follow the instructions to complete each step of the activity. Then, answer the 8 questions at the end of the activity before going to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the following link and select *Use Template*. (In this step, you will just open the template. More instructions for how to use the template will be included in later steps.)
Link to template: File permissions in Linux
OR
If you don't have a Google account, you can download the template directly from the following attachment.

File permissions in Linux
DOCX File

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.
To use the supporting materials for this course item, click the links.
The Instructions for including Linux commands document provides instructions and best practices for including samples of Linux commands in your portfolio activity.
Link to 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.
Link to 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.
OR
If you don't have a Google account, you can download the supporting materials directly from the following attachments.
Instructions for including Linux commands
DOCX File
Current file permissions
DOCX File

Step 3: Check file and directory details

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 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: Describe the permissions string

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 other 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