Challenge 3: File Permissions, Users, and Groups

Making and overseeing various users and groups is an essential skill for any Linux administrator. Managing multiple accounts can be a difficult task. You may be required to give read, write, or execute privileges to certain files for some accounts, multiple accounts, or no accounts at all.

Step By Step Guide:

- Log in as the root user.
- Open up a terminal and change directories to /etc.
- Inside the etc directory is a file called passwd which holds information about all of the user accounts on your system.
- Display the contents of the passwd file.

- The first field of each line is a user account on the system.
- Some of these are accounts for services that are running while others are for accounts for specific users.
- Use awk to only display a list of the user accounts.

- For our purpose we want to create three new user accounts: test1, test2, and test3.
- Create these users.
- Verify that the three users have been created by displaying the contents of the passwd file.
- Again use awk to only display a list of user accounts. This time redirect the output into a text file which will be stored on the root user's Desktop.

- Inside the etc directory is a file called group which holds information about all of the groups on your system.
- Display the contents of the group file.

- Create a new group called test_group.
- Add user test1 and test2 to the test_group group.
- Display the contents of the group file to verify the results.
- Display the contents of the group file and redirect the output into a text file which will be stored on the root user's Desktop.

- Change directories to the user test1's home directory.
- Change users to become user test1.
- Create a file called file1 and populate it with some text.
- Set the permissions to rw for owner, r for group, and no permissions for all other users.

- Create a file called file2 and populate it with some text.
- Set the permissions to rw for owner and group, and r for all other users.

- Create a file called file3 and populate it with some text.
- Set the permissions to rw for all users.

- Create a file called file4 and populate it with some text.
- Set the permissions to rw for the owner and no permissions for any other user.

- Change back to the root user.
- For each of the created files, change the group to the test_group group previously created.
- For the last created file, file4, change the owner to the test3 user.

- Read and write each file as user test1. Do you get the expected results?
- Read and write each file as user test2. Do you get the expected results?
- Read and write each file as user test3. Do you get the expected results?

- Remove all files.
- Remove the test_group group.
- Remove the users test1, test2, and test3.