Add and manage users with Linux

Project description

As a security analyst, I was tasked with reviewing and modifying file permissions for a new user joining the organization. This involves creating the user account, assigning ownership to specific files, modifying group access, and continuing managing their access during their time with the organization. Properly removing the user after they leave the company, all while using safe Linux command practices.

Add a new User

The following Linux command shows and demonstrates how a new user is added to the system.

```
analyst@c56baaddab4c:~$ sudo useradd researcher9
analyst@c56baaddab4c:~$ sudo usermod -g research_team researcher9
analyst@c56baaddab4c:~$
```

I added the new user (researcher9) to the system and also to the (research_team) group as their primary group shown in the second command line. We started the Linux command with (sudo) allowing us temporary elevated permissions to run the command. The (usermod) command modifies existing user accounts, following after is the option (-g) which sets the user's default group/primary group. In this case the primary group is (research_team), which adds the user (researcher9) to the primary group. Once done we will give responsibility for (project_r.txt) to the new employee (researcher9).

Assign File Ownership

We will be assigning responsibility for (project_r.txt) file, to the new employee (researcher9). We will do this with the linux command shown below.

```
analyst@3f04f3929be8:/home$ cd /home/researcher2/projects
analyst@3f04f3929be8:/home/researcher2/projects$ sudo chown researche
r9 project_r.txt
```

The first command used will change directory (cd) to /home/researcher2/projects directory. This is where the project_r.txt file is located due to researcher2 being the current owner. We follow this up with the second command line, using the chown command allows us to assign file

ownership of the “project_r.txt” file to “researcher9”. (sudo) allows us temporary elevated permissions to run the (chown) command following that we select the new user which is (researcher9) then the file we would like the user to have ownership of, which is (project_r.txt).

Add the user to a secondary group

A few months later the organization informed me that the employees (researcher9) role at the organization has changed, and they are working in both the Research and Sales departments. I am tasked with adding (researcher9) to a secondary group (sales_team), their primary group is still (research_team).

```
analyst@a402fd7e0ccb:/home/researcher2/projects$ sudo usermod -a -G s
ales_team researcher9
analyst@a402fd7e0ccb:/home/researcher2/projects$
```

The above Linux command allows me to add a secondary group to the user (researcher9) with the commands showing (sudo) granting us temporary elevated permissions to run (usermod) command which modifies existing user accounts. Following the (usermod) command you also need a (-a) option, which appends the user to an existing group and it’s only used with the (-G) option. The supplemental group is what follows after the (-G), in this case it’s the (sales_team) and the user being added (researcher9).

Delete a user

A year later, researcher9, decided to leave the company. The organization wants the user deleted from our systems to maintain a secure organization. Below I will show the commands to execute the removal of the user from the system.

```
analyst@a402fd7e0ccb:/home/researcher2/projects$ sudo userdel researc
her9
userdel: group researcher9 not removed because it is not the primary
group of user researcher9.
analyst@a402fd7e0ccb:/home/researcher2/projects$ sudo groupdel resear
cher9
analyst@a402fd7e0ccb:/home/researcher2/projects$
```

I ran the Linux command (sudo) which granted us temporary elevated privileges to run the command (userdel) which deletes a user from the system. In this case the user (researcher9) is being deleted. We received a return output command of “userdel: group researcher9 not removed because it is not the primary group of user researcher9” This is expected, because when you create a new “user”, Linux also creates a Group called the “users” name. This is why when using “userdel” it removes the user account, but not delete the group with the same name. This is normal and a safe thing Linux does leaving the group alone just in case it’s being used

elsewhere. This is why the message is expected and not an error. The second command used (groupdel) deletes the group named “researcher9” if it’s not in use anymore.