**Activity: Add and manage users with Linux commands**

**Overview:** Authentication is the process of a user proving that they are who they say they are in the system. When managing this, security analysts need to ensure

* not all users get access to the system,
* new users (those who are new to the organization or a group) are added to the system, and
* Current users who change groups or leave the organization are deleted from the system.

**Scenario:** In this scenario, a new employee with the username researcher9 joins an organization. You have to add them to the system and continue to manage their access during their time with the organization.

Here’s how you’ll do this task: **First**, you’ll add a new employee to the system and then to their primary group. **Second**, you’ll make this employee the owner of a file related to a particular project. **Third**, you’ll add the new employee to a supplementary group. **Finally**, you’ll delete the employee from the system.

**Start your lab:** click on “start lab” to start the lab.

**Task 1. Add a new user**

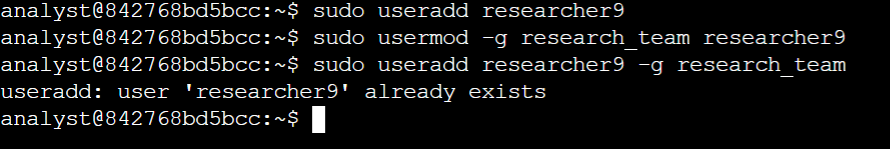
A new employee has joined the Research department. In this task, you must add them to the system. The username assigned to them is researcher9.

1. Write a command to add a user called researcher9 to the system.

**$sudo useradd researcher9**

1. Use the usermod command and -g option to add researcher9 to the research\_team group as their primary group.

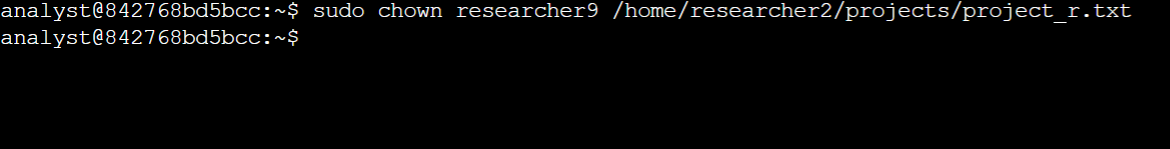
**$sudo usermod –g research –g research\_team researcher9**

**$sudo useradd researcher9 –g research\_team**

**Task 2. Assign file ownership**

The new employee, researcher9, will take responsibility for project\_r. In this task, you must make them the owner of the project\_r.txt file. The project\_r.txt file is located in the /home/researcher2/projects directory, and owned by the researcher2 user.

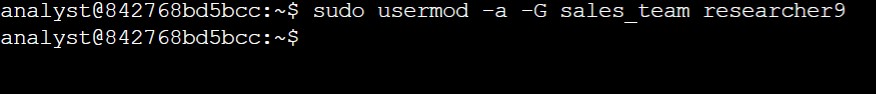
1. Use the chown command to make researcher9 the owner of /home/researcher2/projects/project\_r.txt.

**$sudo chown researcher9 /home/researcher2/projects/project\_r.txt**

**Task 3. Add the user to a secondary group**

A couple of months later, this employee's role at the organization has changed, and they are working in both the Research and the Sales departments. In this task, you must add researcher9 to a secondary group (sales\_team). Their primary group is still research\_team.

1. Use the usermod command with the -a and -G options to add researcher9 to the sales\_team group as a secondary group.

**$sudo usermod –a –G sales\_team researcher9**

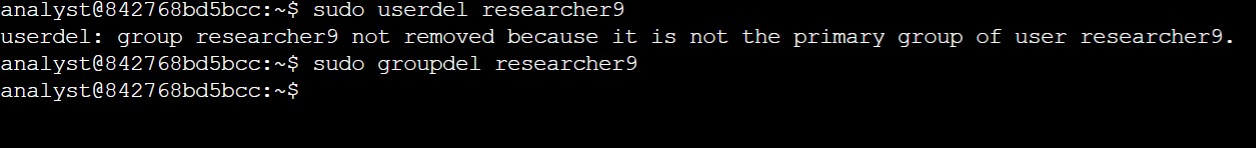
**Task 4. Delete a user**

A year later, researcher9, decided to leave the company. In this task, you must remove them from the system.

1. Run a command to delete researcher9 from the system:

**$sudo userdel researcher9**

1. Run the following command to delete the researcher9 group that is no longer required:

**$sudo groupdel researcher9**

**Conclusion:**

You now have practical experience in using basic Linux Bash shell commands to

* add a new user,
* add a user to a group,
* change user permissions on files, and
* delete a user.