Documentación Desafío 3

Parte I

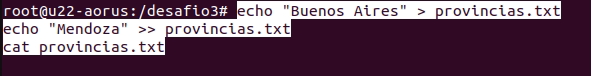
Para el primer ejercicio crearemos un directorio donde poder trabajar con los ficheros y datos que se crearan en los mismo.



**Ejercicio 1 y 2:**

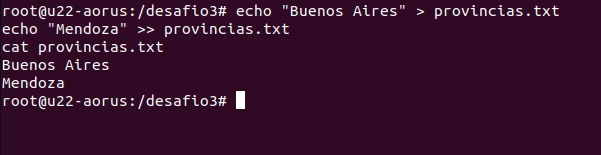
Para este ejercicio tenemos que generar un archivo llamado “provincias.txt” donde el mismo deberá contener como información las provincias “Buenos Aires” y “Mendoza”.

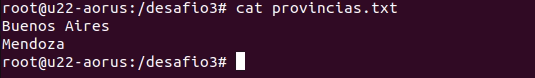
Esto lo realizaremos de la siguiente manera:



En esta parte le estamos indicando que dentro de un archivo provincias.txt se ingresen los datos indicados “Mendoza” y “Buenos Aires”.

Luego de ejecutar el comando en particular nos deberá arrojar lo siguiente, donde tambien podremos verificar el archivo en cuestión creado y con los datos:





**Ejercicio 3:**

Para este punto deberemos listar los archivos dentro del directorio “/dev”, lo realizaremos de la siguiente manera utilizando el comando “ls /dev/tty\*”:





**Ejercicio 4:**

Aca deberemos generar 4 subdirectorios que deberán llamarse “formación” “ventas” “personal” “clientes”, los mismos los generaremos con 1 solo comando de la siguiente manera:

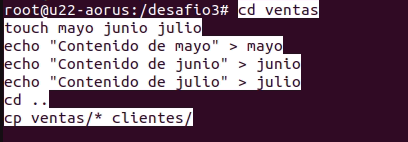
Utilizaremos el comando “mkdir” de modo que quedara asi “mkdir formación ventas personal clientes”





**Ejercicio 5:**

Aca deberemos generar archivos dentro del directorio de ventas “mayo” “junio” “Julio”, esto lo realizaremos de la siguiente manera:





**Ejercicio 6:**

Deberemos realizar una copia en clientes de todos los archivos generados en ventas, para esto lo realizaremos de la siguiente manera:





**Ejercicio 7:**

Ya que copiamos los archivos del directorio, ahora deberemos eliminar el directorio llamado “ventas” junto con todos sus archivos internos, eso lo realizaremos de la siguiente manera con el comando “rm -r ventas”:





**Ejercicio 8:**

Ahora mismo deberemos renombrar nuestro directorio llamado “clientes” a “clientes\_2022” con el siguiente comando “mv clientes clientes\_2022”:





Parte II

**Ejercicio 1:**

Ahora mismo pasaremos a crear grupos de administradores y desarrolladores, a su vez comprobaremos la GID que se les asigna a cada grupo de la siguiente manera:

Crearemos los grupos con los siguientes comandos:  
sudo groupadd administradores

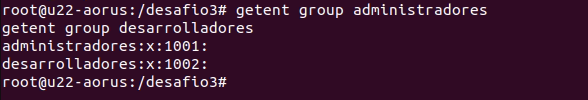
sudo groupadd desarrolladores



Y verificaremos los GID con los siguientes:

getent group administradores

getent group desarrolladores



De esta manera tenemos generados los grupos de permisos solicitados y a la vez podemos verificar que GID poseen cada uno.

**Ejercicio 2:**

Deberemos generar usuarios “web” y “app”, los mismos deben pertenecer únicamente al grupo de “desarrolladores”, esto lo realizaremos de la siguiente manera:

Para generar los usuarios y asignar su respectivo grupo, utilizaremos el siguiente comando:

sudo useradd -m -G desarrolladores web

sudo useradd -m -G desarrolladores app

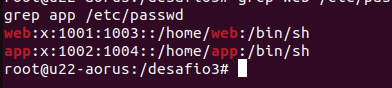


Luego para verificar que los usuarios creados posean el grupo específico asignado utilizaremos los siguientes comandos:

grep web /etc/passwd

grep app /etc/passwd







**Ejercicio 3:**

Ahora deberemos loguearnos como uno de los usuarios que generamos anteriormente “web” y deberemos crear un archivo donde solo el mismo usuario pueda tener permisos de lectura y escritura, la tarea la realizaremos con el siguiente comando:

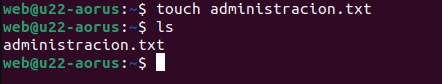
Ingresamos al usuario “web”: su web



Creamos el archivo: touch administración.txt



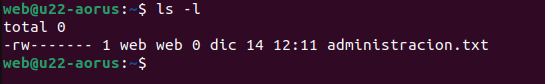
En este caso, como no tendremos permisos de bash, no podremos ejecutar comandos dentro del mismo, pare eso saldremos del usuario y realizaremos la siguiente modificación en el mismo con con comando “usermod –S /bin/bash”, lo que nos permitirá acceder a un entorno bash del usuario y completar la tarea.



Modificamos permisos: chmod 600 administracion.txt



Modificaremos y verificaremos los permisos del archivo



Salimos de la sesión: exit



**Ejercicio 4:**

Ahora realizaremos un directorio compartido dentro del usuario app, donde generaremos 3 archivos, lo realizaremos de la siguiente manera:

Ingresaremos al bash del usuario ”app”: su app

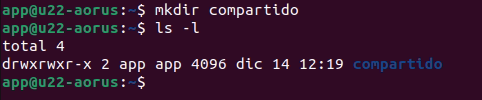


Generaremos el directorio con el que trabajaremos: mkdir compartido

Ingresaremos al directorio home del usuario app



Crearemos el directorio de trabajo

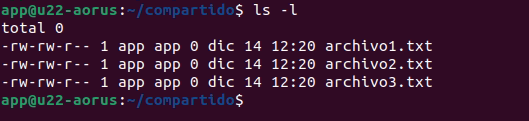


Ingresaremos al directorio creado: cd compartido



Crearemos los archivos solicitados dentro del mismo: touch archivo1.txt archivo2.txt archivo3.txt

Verificamos que los archivos se hayan creado correctamente



Saldremos de la sesión: exit

Salimos de la sesión



**Ejercicio 5:**

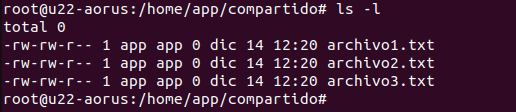
Ingresaremos al directorio compartido del usuario app, y modificaremos el grupo propietario del archivo2.txt de la siguiente manera:



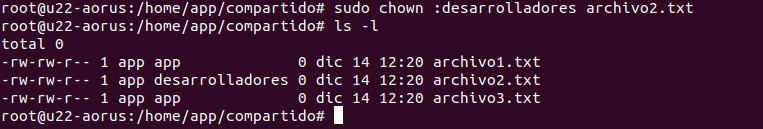
Dentro del home del usuario app, ingresaremos al directorio “compartido”



Dentro del mismo ubicaremos el archivo que necesitamos modificar el grupo de propietarios en este caso es el “archivo2.txt”



Modificaremos el grupo propietario con el siguiente comando “sudo chown :desarrolladores archivo2.txt”, una vez ejecutado el mismo, deberemos tener el archivo en cuestión con el grupo propietario específico.



**Ejercicio 6:**

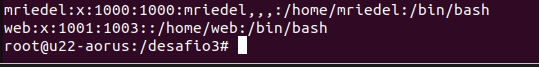
Ahora procederemos a eliminar el usuario app, manteniendo el home del mismo para no perder los archivos anteriormente generados y modificados.

Para realizar el procedimiento lo haremos de la siguiente manera:

Con el comando “sudo userdel app” eliminaremos el usuario



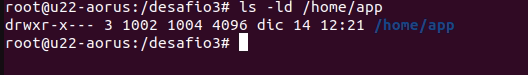
Luego de ejecutar el comando para eliminar el usuario solicitado, verificaremos que el mismo se haya eliminado con “cat /etc/passwd”



Y como se puede observar el usuario app, que se encontraba junto al usuario web, ya no se encuentra disponible.

Una vez eliminado el usuario verificaremos que sucedió con su directorio home, donde el mismo se debería de mantener ya que no le indicamos en el comando de eliminación que elimine tambien su respectiva home:

Lo realizaremos con el siguiente tomando “ls -ld /home/app”



Como podemos verificar el home se mantuvo con los mismos permisos del usuario app.

**Ejercicio 7:**

Para abordar la situación y restringir el acceso no autorizado al archivo “Lista\_Precios”, dentro del directorio home de Steve, se deberían proponer utilizar las siguientes medidas de seguridad:

1. Generar un grupo de permisos específico para acceder al archivo:

Lo realizaremos con el siguiente comando: “sudo groupadd auditoria”



1. Se cambiarían propietario y grupo al archivo de “Lista\_Precios”

Se realizaría con el siguiente comando:   
“sudo chown steve:auditoria /home/steve/Lista\_Precios”





1. Establecer permisos apropiados para el archivo:

Con el comando “sudo chmod 600 /home/steve/Lista\_Precios”

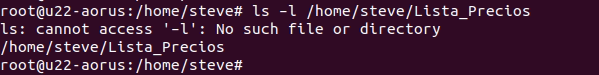


1. Se agregaría los demas usuarios que necesiten editar el archivo:

Con el comando “sudo usermod pepe -G auditoria”



1. Verificaríamos los permisos del archivo con el comando “ls –l /home/steve/Lista\_Precios”



Los cambios realizados anteriormente cumplen las siguientes funciones:

* **Medidas de Seguridad**: Se crea un grupo específico para acceder al archivo, lo que permite un control más preciso sobre quiénes pueden acceder a los datos.
* **Tipo de Usuarios**: Steve es el propietario del archivo, y otros usuarios autorizados pueden ser agregados al grupo si es necesario.
* **Tipo de Permiso**: Se establecen permisos que permiten la lectura y escritura solo al propietario (Steve) y ninguno para otros usuarios.
* **Verificación de Permisos**: Se verifica que los permisos estén configurados correctamente usando ls -l.

Esto asegura que solo Steve y aquellos en el grupo auditoria tengan acceso al archivo "Lista\_Precios". Otros usuarios no tendrán ningún permiso sobre el archivo. Este enfoque mejora significativamente la seguridad del archivo y minimiza el riesgo de acceso no autorizado.