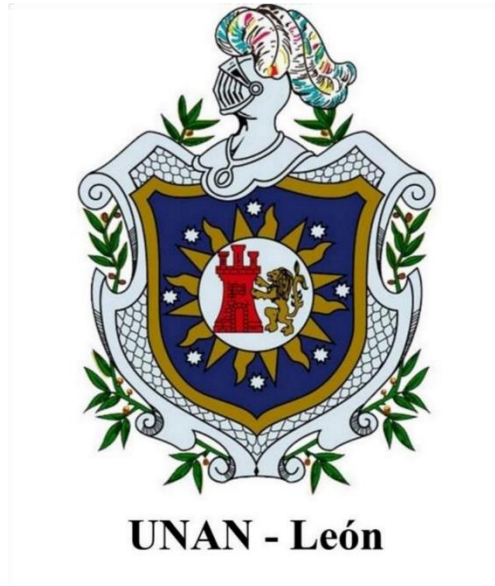


Universidad Nacional Autónoma de Nicaragua
UNAN- León
Facultad de ciencias y tecnologías



COMPONENTE: Administración de sistemas Linux I

CARRERA: ING. EN SISTEMAS DE INFORMACION CON ENFASIS EN
DESARROLLO WEB Y MARKETING DIGITAL.

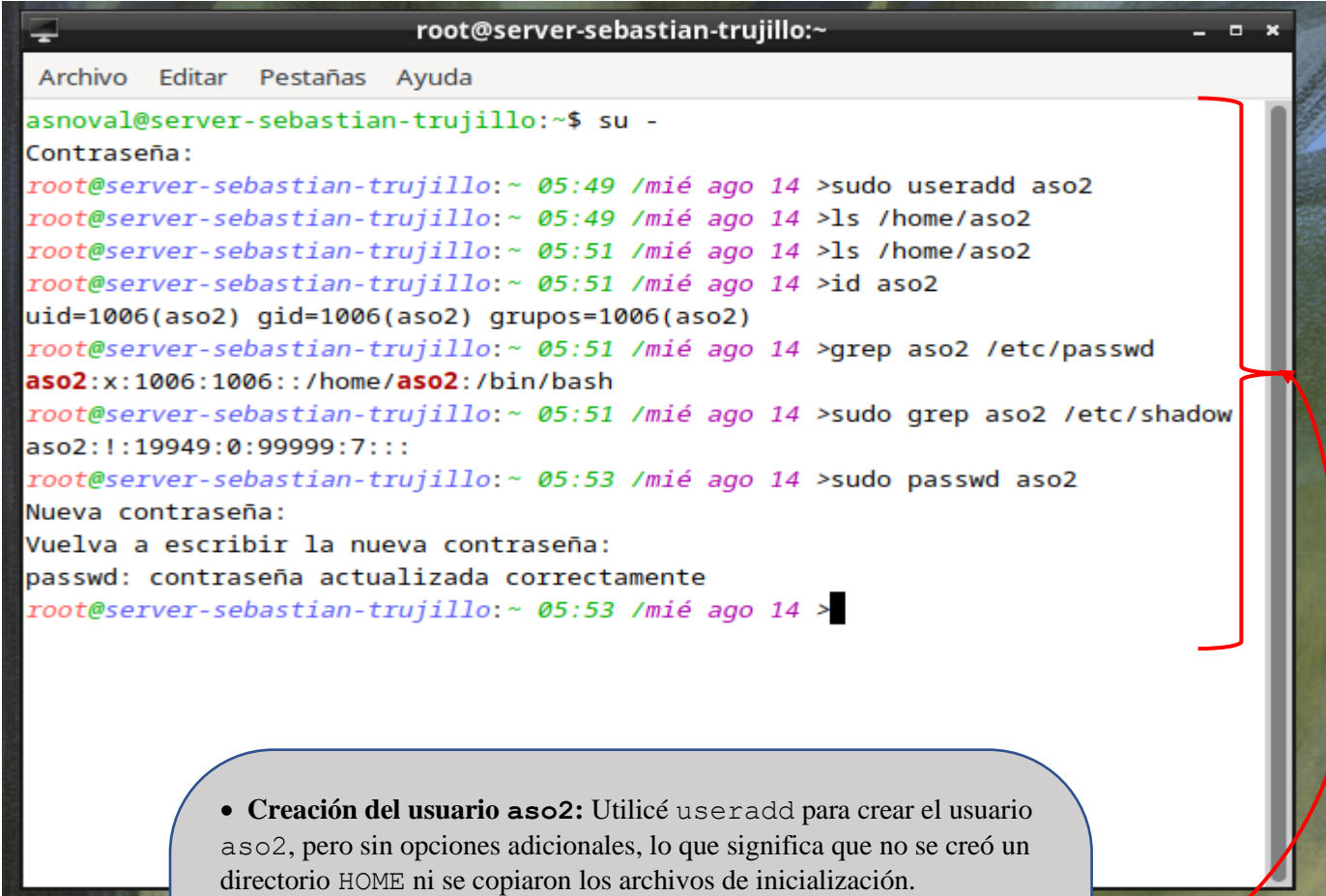
DOCENTE: Rina del Pilar Arauz Altamirano

ESTUDIANTES:

Sebastián Trujillo Zepeda - CARNET: 22-10390-1

Franvir Steven Rivas - CARNET: 22-04782-1

Ejercicio1 y Ejercicio2

A terminal window titled 'root@server-sebastian-trujillo:~' with a menu bar (Archivo, Editar, Pestañas, Ayuda). The terminal shows the following commands and output:

```
asnoval@server-sebastian-trujillo:~$ su -
Contraseña:
root@server-sebastian-trujillo:~ 05:49 /mié ago 14 >sudo useradd aso2
root@server-sebastian-trujillo:~ 05:49 /mié ago 14 >ls /home/aso2
root@server-sebastian-trujillo:~ 05:51 /mié ago 14 >ls /home/aso2
root@server-sebastian-trujillo:~ 05:51 /mié ago 14 >id aso2
uid=1006(aso2) gid=1006(aso2) grupos=1006(aso2)
root@server-sebastian-trujillo:~ 05:51 /mié ago 14 >grep aso2 /etc/passwd
aso2:x:1006:1006:./home/aso2:/bin/bash
root@server-sebastian-trujillo:~ 05:51 /mié ago 14 >sudo grep aso2 /etc/shadow
aso2:!:19949:0:99999:7:::
root@server-sebastian-trujillo:~ 05:53 /mié ago 14 >sudo passwd aso2
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
root@server-sebastian-trujillo:~ 05:53 /mié ago 14 >
```

A red bracket on the right side of the terminal window groups the commands from 'useradd' to 'passwd'. A red arrow points from the bottom of this bracket to the first bullet point in the explanatory text box below.

- **Creación del usuario aso2:** Utilicé `useradd` para crear el usuario `aso2`, pero sin opciones adicionales, lo que significa que no se creó un directorio HOME ni se copiaron los archivos de inicialización.
- **Asignación de grupo primario:** Al usuario `aso2` se le asignó un grupo primario con el mismo nombre (`aso2`).
- **Contraseña:** Luego, usé `passwd` para asignarle una contraseña al usuario, lo que permite que `aso2` inicie sesión con esa contraseña.
- **Verificación en `/etc/passwd` y `/etc/shadow`:** Finalmente, verifiqué que el usuario `aso2` se añadió correctamente a estos archivos de configuración clave del sistema.

Ejercicio 3

```
andres@server-sebastian-trujillo:~  
Archivo Editar Pestañas Ayuda  
root@server-sebastian-trujillo:~ 06:07 /mié ago 14 >cd /etc/skel  
root@server-sebastian-trujillo:/etc/skel 06:07 /mié ago 14 >sudo nano horario  
root@server-sebastian-trujillo:/etc/skel 06:08 /mié ago 14 >sudo useradd -m andres  
root@server-sebastian-trujillo:/etc/skel 06:08 /mié ago 14 >su - andres  
andres@server-sebastian-trujillo:~$ ls -la  
total 16  
drwx----- 3 andres andres 93 ago 14 18:08 .  
drwxr-xr-x. 10 root root 120 ago 14 18:08 ..  
-rw-r--r--. 1 andres andres 18 feb 8 2024 .bash_logout  
-rw-r--r--. 1 andres andres 144 feb 8 2024 .bash_profile  
-rw-r--r--. 1 andres andres 522 feb 8 2024 .bashrc  
-rw-r--r--. 1 andres andres 75 ago 14 18:08 horario  
drwxr-xr-x. 4 andres andres 39 ago 6 19:48 .mozilla  
andres@server-sebastian-trujillo:~$ sudo nano /home/andres/.bashrc  
andres@server-sebastian-trujillo:~$ su -  
Contraseña:  
root@server-sebastian-trujillo:~ 06:10 /mié ago 14 >sudo nano /home/andres/.bashrc  
root@server-sebastian-trujillo:~ 06:11 /mié ago 14 >su - andres  
asnoval ttyl 2024-08-14 17:48 (:0)  
mié 14 ago 2024 18:11:36 CST  
andres@server-sebastian-trujillo:~$
```

1. Crear el archivo "horario":

- Navega a `/etc/skel` y crea el archivo `horario` con el contenido "Las salas de prácticas están abiertas todos los días".

2. Crear un usuario llamado `andres`:

- Utiliza `useradd -m andres` para crear el usuario `andres` y asegurarte de que el archivo `horario` se copie a su directorio `HOME`.

3. Verificar la existencia del archivo "horario":

- Inicia sesión como `andres` y usa `ls -la` para confirmar que el archivo `horario` está en su directorio `HOME`.

4. Configurar la ejecución de `who` y `date` al iniciar sesión:

- Edita el archivo `.bashrc` de `andres` y agrega `who` y `date` al final para que se ejecuten automáticamente al iniciar sesión.

5. Verificar la ejecución de los comandos:

- Inicia sesión nuevamente como `andres` y verifica que los comandos `who` y `date` se ejecutan al inicio de la sesión.

```
done  
fi  
unset rc  
who  
date  
^G Ayuda ^O Guardar  
^Y Salir ^R Leer fich. ^W Reemplazar ^U Pegar
```

Estos pasos configuran tu sistema para que cada nuevo usuario reciba automáticamente un archivo llamado "horario" en su directorio HOME, y específicamente para el usuario andres, configuramos su perfil para que cada vez que inicie sesión, vea quién está conectado y la hora actual. Este proceso utiliza características estándar de Linux como el directorio /etc/skel y el archivo .bashrc para personalizar la experiencia del usuario.

```
root@server-sebastian-trujillo:/etc/skel  
Archivo Editar Pestañas Ayuda  
GNU nano 7.2 horario  
Las salas de practicas están abiertas todos los días  
salon 1 basico unan  
[ 2 líneas leídas ]  
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T E  
^X Salir ^R Leer fich. ^Y Reemplazar ^U Pegar ^J J
```

Ejercicio 4



```
root@server-sebastian-trujillo:~  
Archivo  Editar  Pestañas  Ayuda  
asnoval@server-sebastian-trujillo:~$ su -  
Contraseña:  
root@server-sebastian-trujillo:~ 06:03 /jue ago 15 >sudo userdel aso2  
root@server-sebastian-trujillo:~ 06:03 /jue ago 15 >sudo userdel -r aso2  
userdel: el usuario «aso2» no existe  
root@server-sebastian-trujillo:~ 06:03 /jue ago 15 >
```

4. Borra aso2 con la orden userdel. Responde a las siguientes preguntas:

4.1 Se borra el directorio HOME del usuario?

Cuando utilizas el comando `userdel` sin ninguna opción adicional, **no se borra** automáticamente el directorio `HOME` del usuario. El directorio `/home/aso2` y todos sus archivos permanecen en el sistema.

----R: no se borra

4.2 ¿Qué opción hay que indicar a userdel para que borre el directorio HOME?

Esta opción borra el directorio `HOME` del usuario (en este caso, `/home/aso2`) y su contenido, junto con el usuario en sí.

----R: `sudo userdel -r aso2`

Ejercicio 5

5. En el campo "password" del fichero `/etc/shadow` podemos encontrar diferentes valores que indican distinto comportamiento del sistema o de la cuenta. Responde las siguientes cuestiones

5.1 Si hay una cadena encriptada, es la contraseña, y por tanto significa que:

Si en el campo "password" del archivo `/etc/shadow` hay una cadena encriptada, significa que el usuario tiene una contraseña establecida. Esta contraseña es necesaria para iniciar sesión, y se valida cuando el usuario intenta acceder al sistema el usuario tiene una contraseña establecida y puede iniciar sesión con ella.

5.2 Si encontramos "!!" o "*" significa que:

Si el campo "password" contiene "!!" o "*", significa que la cuenta está bloqueada o que no se ha establecido una contraseña para la cuenta. En este estado, el usuario no puede iniciar sesión utilizando una contraseña la cuenta está bloqueada o no tiene una contraseña establecida.

5.3 ¿Para este último caso, es posible iniciar sesión?

No, no es posible iniciar sesión en una cuenta que tenga "!!" o "*" en el campo "password" de `/etc/shadow`. Estos caracteres indican que la autenticación basada en contraseña está deshabilitada para esa cuenta.

5.4 Una "x" en el campo "password" del fichero `/etc/passwd` significa que:

Una "x" en el campo "password" del archivo `/etc/passwd` indica que la contraseña del usuario no está almacenada en este archivo, sino en el archivo más seguro `/etc/shadow`. Este es el comportamiento estándar en sistemas modernos que utilizan la autenticación en dos archivos separados para mejorar la seguridad.

Ejercicio 6

1- Crear el usuario aso3.

2- Configurar un mínimo de 2 días entre cambios de contraseña.

3- Establecer que la contraseña debe cambiarse cada 60 días como máximo.

```
root@server-sebastian-trujillo:~  
Archivo Editar Pestañas Ayuda  
root@server-sebastian-trujillo:~ 06:18 /jue ago 15 >sudo useradd -m aso3  
root@server-sebastian-trujillo:~ 06:18 /jue ago 15 >sudo chage -m 2 aso3  
root@server-sebastian-trujillo:~ 06:18 /jue ago 15 >sudo chage -M 60 aso3  
root@server-sebastian-trujillo:~ 06:18 /jue ago 15 >sudo chage -W 7 aso3  
root@server-sebastian-trujillo:~ 06:19 /jue ago 15 >sudo chage -I 15 aso3  
root@server-sebastian-trujillo:~ 06:19 /jue ago 15 >sudo chage -E 2024-06-12 aso3  
root@server-sebastian-trujillo:~ 06:19 /jue ago 15 >
```

4- Avisar al usuario 7 días antes de que su contraseña expire.

6- Hacer que la cuenta sea inaccesible a partir del 12 de junio de 2024.

5- Bloquear la cuenta 15 días después de que la contraseña haya expirado.

Ejercicio 7



```
aso3@server-sebastian-trujillo:~  
Archivo Editar Pestañas Ayuda  
aso3@server-sebastian-trujillo:~$ passwd  
Contraseña actual:  
passwd: Error de manipulación del testigo de autenticación  
passwd: no se ha cambiado la contraseña  
aso3@server-sebastian-trujillo:~$
```

Este proceso asegura que el usuario `aso3` se vea obligado a cambiar su contraseña en el próximo inicio de sesión si ha expirado y que respete cualquier restricción de tiempo aplicada.

Configura la fecha de expiración para forzar el cambio de contraseña.

Verifica la configuración para confirmar que la expiración se aplicó correctamente.

Configura las restricciones de tiempo como el mínimo de días entre cambios para que el usuario no pueda cambiar la contraseña antes de ese período.

Prueba el cambio de contraseña para asegurarte de que el sistema aplica las restricciones correctamente.

Debido a que la contraseña ha expirado (según la fecha de caducidad establecida), el sistema debería forzar al usuario a cambiarla. Si también has configurado un mínimo de días entre cambios, el usuario no podrá cambiar la contraseña antes de que haya pasado el período requerido desde el último cambio.

Ejercicio 8

8. Shell restringida

8.1 | Asigna a un usuario dicha shell y comprueba qué acciones puede o no realizar. En la página de manual de bash, en la sección RESTRICTED SHELL, encontraras una descripción detallada de lo que está prohibido para este nuevo tipo de shell. (describe lo que encontró en el man en la sección RESTRICTED SHELL)

```
root@server-sebastian-trujillo: / 07:01 /jue ago 15 > sudo usermod -s /bin/bash aso3
root@server-sebastian-trujillo: / 07:01 /jue ago 15 > su - aso3
aso3@server-sebastian-trujillo: ~$ bash --restricted
aso3@server-sebastian-trujillo: ~$ cd ..
bash: cd: restringido
aso3@server-sebastian-trujillo: ~$ export VAR=value
aso3@server-sebastian-trujillo: ~$ echo "test" > file.txt
bash: file.txt: restringido: no se puede redirigir la salida
aso3@server-sebastian-trujillo: ~$ source script.sh
bash: script.sh: No existe el fichero o el directorio
aso3@server-sebastian-trujillo: ~$ export PATH=/new/path:$PATH
bash: PATH: variable de sólo lectura
aso3@server-sebastian-trujillo: ~$ █
```

Qué es una Shell Restringida

Una shell restringida (en este caso, bash en modo restringido) impone varias limitaciones a los usuarios que la utilizan. Estas restricciones están diseñadas para proporcionar un entorno controlado y seguro, especialmente útil en situaciones donde deseas limitar las acciones que un usuario puede realizar.

Configuración de bash en Modo Restringido

Dado que rbash no está disponible en tu sistema, puedes usar bash en modo restringido. Aquí te explico cómo hacerlo y qué restricciones impone.

1. Verificar la Instalación de bash

Primero, asegúrate de que bash está instalado en tu sistema. Normalmente, bash se encuentra en /bin/bash o /usr/bin/bash. Puedes verificar su ubicación con: `which bash`

2. Cambiar la Shell de un Usuario a bash

Para usar bash como shell restringida, primero cambia la shell del usuario a /bin/bash: `sudo usermod -s /bin/bash aso3`

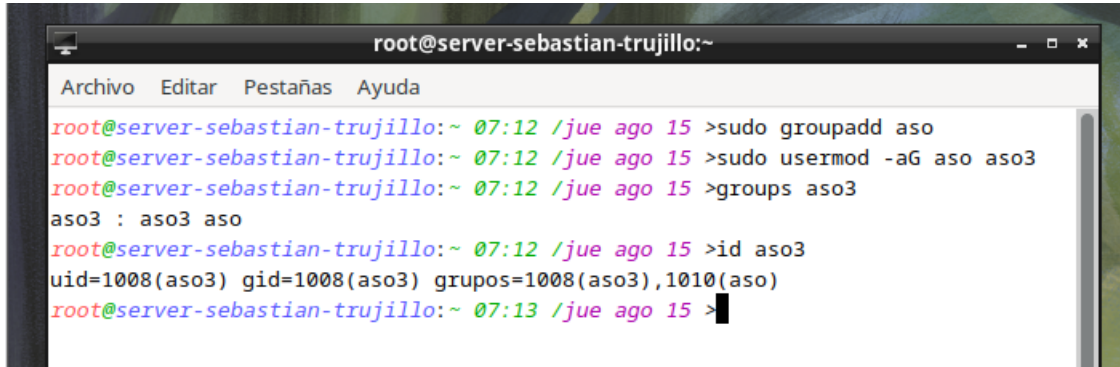
3. Iniciar bash en Modo Restringido

Una vez que hayas cambiado la shell del usuario, inicia sesión como el usuario (aso3) y luego ejecuta bash en modo restringido:

```
su - aso3
```

```
bash --restricted
```


Ejercicio 9



```
root@server-sebastian-trujillo:~
Archivo Editar Pestañas Ayuda
root@server-sebastian-trujillo:~ 07:12 /jue ago 15 >sudo groupadd aso
root@server-sebastian-trujillo:~ 07:12 /jue ago 15 >sudo usermod -aG aso aso3
root@server-sebastian-trujillo:~ 07:12 /jue ago 15 >groups aso3
aso3 : aso3 aso
root@server-sebastian-trujillo:~ 07:12 /jue ago 15 >id aso3
uid=1008(aso3) gid=1008(aso3) grupos=1008(aso3),1010(aso)
root@server-sebastian-trujillo:~ 07:13 /jue ago 15 >
```

Crear el Grupo: Utiliza el comando `groupadd` para crear un nuevo grupo llamado "aso". Esto se hace con una terminal y el comando adecuado para añadir el grupo al sistema.

Añadir el Usuario al Grupo: Después de crear el grupo, usa el comando `usermod` para añadir el usuario `aso3` al grupo "aso". Es importante usar las opciones correctas para añadir al usuario al grupo sin eliminarlo de otros grupos a los que ya pertenece. La opción `-aG` te permite añadir el usuario a un grupo adicional.

Verificar la Pertenencia al Grupo: Para confirmar que el usuario `aso3` ha sido añadido correctamente al grupo "aso", puedes usar uno de los siguientes comandos:

- `groups aso3`: Este comando muestra todos los grupos a los que pertenece el usuario `aso3`, incluyendo el grupo "aso".
- `id aso3`: Este comando muestra información detallada sobre el usuario, incluyendo los grupos a los que pertenece.

Ejercicio 10



```
root@server-sebastian-trujillo:~
Archivo Editar Pestañas Ayuda
root@server-sebastian-trujillo:~ 07:15 /jue ago 15 >sudo groupadd ssoo
root@server-sebastian-trujillo:~ 07:15 /jue ago 15 >sudo usermod -aG ssoo aso3
root@server-sebastian-trujillo:~ 07:15 /jue ago 15 >groups aso3
aso3 : aso3 aso ssoo
root@server-sebastian-trujillo:~ 07:15 /jue ago 15 >id aso3
uid=1008(aso3) gid=1008(aso3) grupos=1008(aso3),1010(aso),1011(ssoo)
root@server-sebastian-trujillo:~ 07:15 /jue ago 15 >
```

Crear el grupo:

Usa `groupadd ssoo` para crear el grupo "ssoo".

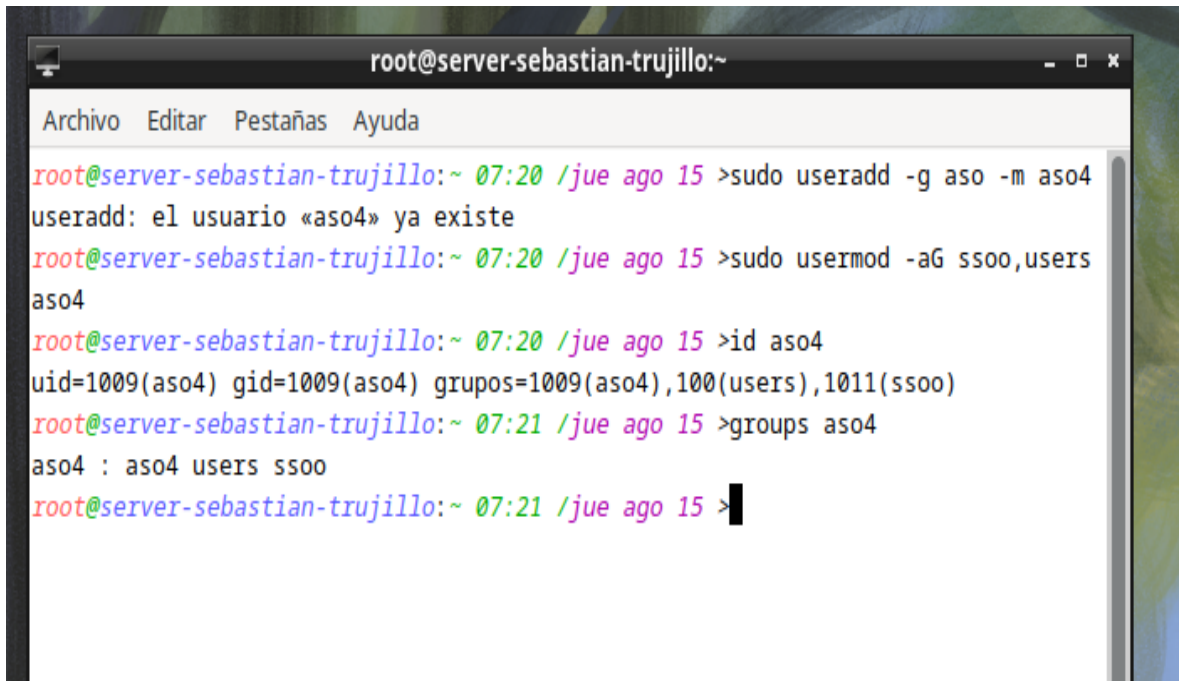
Añadir el usuario al grupo:

Usa `usermod -aG ssoo aso3` para añadir el usuario `aso3` al grupo "ssoo".

Verificar la pertenencia al grupo:

Usa `groups aso3` o `id aso3` para confirmar que `aso3` está en el grupo "ssoo".

Ejercicio 11



```
root@server-sebastian-trujillo:~  
Archivo  Editar  Pestañas  Ayuda  
root@server-sebastian-trujillo:~ 07:20 /jue ago 15 >sudo useradd -g aso -m aso4  
useradd: el usuario «aso4» ya existe  
root@server-sebastian-trujillo:~ 07:20 /jue ago 15 >sudo usermod -aG ss00,users  
aso4  
root@server-sebastian-trujillo:~ 07:20 /jue ago 15 >id aso4  
uid=1009(aso4) gid=1009(aso4) grupos=1009(aso4),100(users),1011(ss00)  
root@server-sebastian-trujillo:~ 07:21 /jue ago 15 >groups aso4  
aso4 : aso4 users ss00  
root@server-sebastian-trujillo:~ 07:21 /jue ago 15 >
```

1. Creación del Usuario con Grupo Primario aso

Cuando usas el comando `useradd`, por defecto se crea un grupo con el mismo nombre que el usuario. Sin embargo, en este caso específico, queremos que el usuario `aso4` tenga como grupo primario un grupo existente llamado `aso` (en lugar de crear un grupo nuevo).

Para hacer esto:

`useradd -g aso -m aso4`: Este comando crea el usuario `aso4` y asigna el grupo `aso` como su grupo primario.

`-g aso`: Asigna el grupo `aso` como el grupo primario del usuario `aso4`.

`-m`: Crea un directorio HOME para el usuario, es decir, un espacio personal donde el usuario puede almacenar sus archivos.

2. Añadir el Usuario a los Grupos Secundarios ss00 y users

Después de crear el usuario, es necesario añadirlo a otros grupos secundarios para que tenga más permisos y acceso a recursos compartidos:

`usermod -aG ss00,users aso4`: Este comando añade el usuario `aso4` a los grupos `ss00` y `users`.

`-aG`: La opción `-aG` (append Group) asegura que el usuario sea añadido a los grupos especificados (`ss00` y `users`) sin ser eliminado de su grupo primario (`aso`).

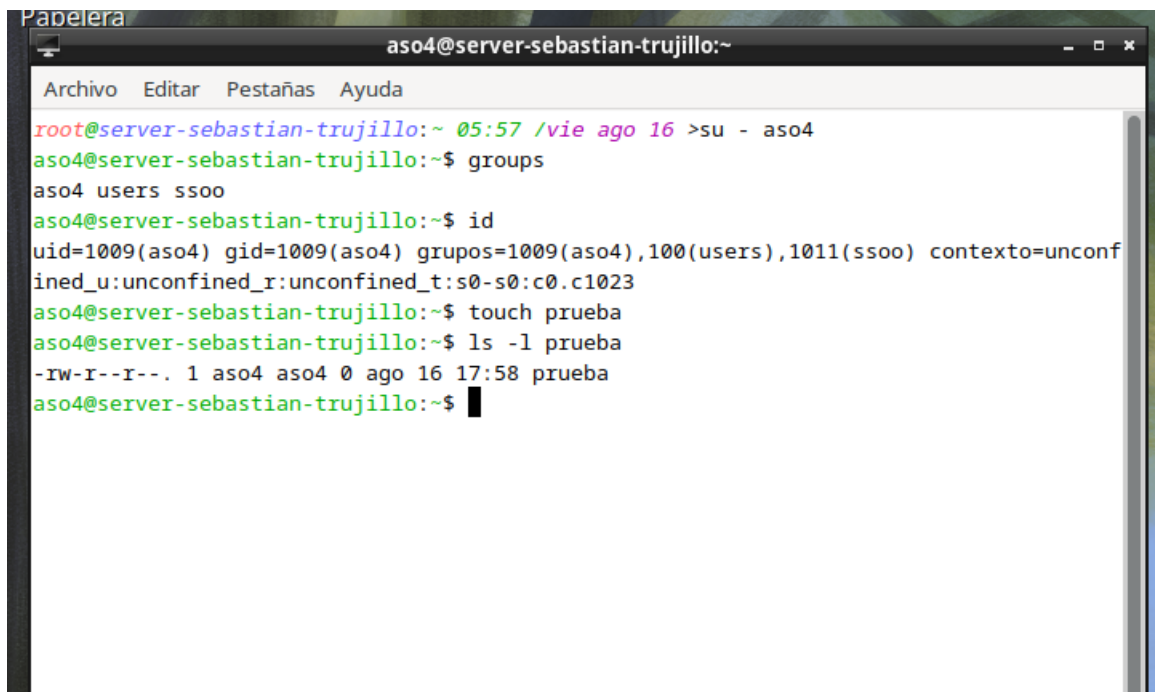
3. Verificación

Finalmente, es importante verificar que el usuario `aso4` se haya creado correctamente y que pertenece a los grupos especificados:

`id aso4`: Este comando muestra toda la información relevante sobre el usuario `aso4`, incluyendo su UID (User ID), grupo primario (GID), y los grupos secundarios a los que pertenece.

`groups aso4`: Este comando lista únicamente los grupos a los que pertenece `aso4`, confirmando que los grupos `aso`, `ss00`, y `users` están asignados correctamente.

Ejercicio 12



```
aso4@server-sebastian-trujillo:~  
Archivo Editar Pestañas Ayuda  
root@server-sebastian-trujillo:~ 05:57 /vie ago 16 >su - aso4  
aso4@server-sebastian-trujillo:~$ groups  
aso4 users ssoo  
aso4@server-sebastian-trujillo:~$ id  
uid=1009(aso4) gid=1009(aso4) grupos=1009(aso4),100(users),1011(ssoo) contexto=unconf  
ined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
aso4@server-sebastian-trujillo:~$ touch prueba  
aso4@server-sebastian-trujillo:~$ ls -l prueba  
-rw-r--r--. 1 aso4 aso4 0 ago 16 17:58 prueba  
aso4@server-sebastian-trujillo:~$
```

1. Inicia sesión como aso4

- Cambia al usuario aso4 usando el comando `su - aso4` para realizar las tareas con su configuración.

2. Verifica el grupo activo del usuario

- Usa `groups` o `id` para comprobar a qué grupos pertenece aso4. El primer grupo que aparece es el grupo activo o primario, que es el grupo asignado a los archivos que cree el usuario.

3. Crea un archivo y verifica su grupo propietario

- Crea un archivo llamado "prueba" con `touch prueba`.
- Verifica con `ls -l prueba` que el grupo propietario del archivo es aso, que es el grupo activo de aso4.