

Tarea Administracion : Tema 4 Gestión de Usuario

En esta Tarea De Administración se han encargado los siguientes aspectos:

- Configurar una imagen virtual para crear 4 usuarios de prueba (prueba1, prueba2, ..., prueba4). Deshabilitar el acceso al sistema para todos los usuarios salvo prueba4. Usar un mecanismo distinto de inhabilitación de acceso para cada usuario.
- Cambiar la clave de prueba4 “a mano”, editando el fichero /etc/passwd y /etc/shadow.
- Añadir todos los usuarios de prueba al grupo “pruebaGrupo”. Establecer que, en la carpeta / home/pruebaGrupo, los usuarios de este grupo puedan escribir y leer cualquier fichero, pero no puedan borrar ficheros de otros usuarios.
- Establecer que, para todos los usuarios que pueden loguearse en el sistema, las contraseñas tengan un tiempo de vida máximo de 10 días, de forma que se reciba una advertencia dos días antes de que caduque la contraseña. Probar a forzar el cambio de contraseña del usuario prueba4 y comentar cuál es el mensaje de advertencia recibido.
- Crear un usuario con una cuenta restrictiva a la que solo se le permita ejecutar un script que consulte el espacio libre en la partición raíz y el número de i-nodos libres, generando una salida como la siguiente: El espacio libre es “X” El número de i-nodos libres es “X”

→ Parte 1:

Como se nos ha pedido debemos crear 4 usuarios de prueba los cuales crearemos mediante el comando “**adduser**” o mediante el comando “**useradd**” con el flag “-m” para que nos cree el home del usuario(en este caso no nos solicita los datos del usuario , ni nos crea el Shell del usuario) . Para que **useradd** nos cree el shell del usuario debemos de escribirlo de la siguiente manera: (3)

Código para insertar en el terminal:

```
sudo adduser prueba1
sudo adduser prueba2
(3) sudo useradd prueba3 -m -s $SHELL
sudo adduser prueba4
```

En el caso de usar “**adduser**” nos solicitará los siguientes campos :

```
Cambiando la información de usuario para prueba1
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] S
```

Posteriormente debemos de inhabilitar el acceso, tenemos dos métodos posibles:

→ ***usermod -L user*** (deshabilitar el usuario mediante usermod)

◆ Para habilitar de nuevo el usuario debemos poner

• ***usermod -U user***

→ ***passwd -l user*** (deshabilitar el usuario mediante passwd)

◆ Para habilitar de nuevo el usuario debemos poner

• ***passwd -u user***

El resultado quedará reflejado en el fichero /etc/shadow .

La diferencia que podemos ver de una cuenta deshabilitada y otra habilitada es :

Si la cuenta está deshabilitada, la cadena de la contraseña empieza por el carácter : !

Código para insertar en el terminal:

sudo usermod -L prueba1

sudo passwd -l prueba2

sudo passwd -l prueba3

→ **Parte 2:**

Para cambiar la clave del usuario prueba4 utilizaremos el comando “passwd” el cual se utiliza de la siguiente manera:

passwd user

Código para insertar en el terminal:

sudo usermod prueba4

Posteriormente el sistema solicitará la nueva contraseña, todos los cambios quedarán reflejados en el fichero shadow.

→ **Parte 3:**

Para añadir los usuarios de prueba al grupo “**pruebaGrupo**”, en primer lugar debemos de crear el grupo, mediante el comando “**addgroup**”

Código para insertar en el terminal:

sudo addgroup pruebaGrupo

Nota : Nos saldrá un mensaje de error por lo cual deberemos de usar el siguiente flag --force-badname. El motivo por el cual nos da el error es que no se aceptan mayúsculas.

```
chrisle@debian:~$ sudo addgroup pruebaGrupo
addgroup: Introduzca un nombre de usuario que se ajuste a la expresión regular
configurada en la variable de configuración NAME_REGEX. Utilice la opción
«--force-badname» para relajar esta comprobación o reconfigure NAME_REGEX.
```

Posteriormente creamos la carpeta /home/pruebaGrupo y asignamos a dicha carpeta el grupo pruebaGrupo, mediante el comando

Código para insertar en el terminal:

sudo chgrp -R pruebaGrupo /home/pruebaGrupo

sudo chmod g+s pruebaGrupo //Cambiamos los permisos

Como queremos que los ficheros solamente puedan ser borrados por el propietario de dicho fichero deberemos de usar el permiso especial t.

Para ello realizaremos :

```
sudo chmod g+t pruebaGrupo
```

Como queremos que los ficheros solamente puedan ser borrados por el propietario de dicho fichero deberemos de usar el permiso especial t.

Para ello realizaremos : `sudo chmod g+t pruebaGrupo`

Asignamos el grupo a los usuarios de prueba

```
sudo usermod -G pruebaGrupo prueba1
```

```
sudo usermod -G pruebaGrupo prueba2
```

```
sudo usermod -G pruebaGrupo prueba3
```

```
sudo usermod -G pruebaGrupo prueba4
```

Para modificar los permisos de los ficheros podemos aplicar una máscara en el directorio o modificar la máscara propia de cada usuario.

→ Parte 4:

Para establecer restricciones en las contraseñas de los usuarios que tengan permisos de login. Utilizaremos el comando chage que posee las siguientes posibilidades:

- *chage -d ult día usuario* ⇒ último cambio de password.
- *chage -m min días usuario* ⇒ nº de días que han de pasar para poder cambiar la contraseña.
- *chage -M max días usuario* ⇒ nº de días máximo que puede estar con la misma contraseña sin cambiarla.
- *chage -W warn días usuario* ⇒ establece un aviso de que la contraseña expira un número de días antes de que expire, indicando que tiene que cambiarla.
- *chage -I inac días usuario* ⇒ nº de días después de que la contraseña expire que la cuenta se deshabilitará de forma automática si la contraseña no ha sido cambiada.
- chage -E exp días usuario* ⇒ fecha en la que la cuenta expira y se deshabilita de forma automática.

Código para insertar en el terminal:

Para limitar la contraseña seguiremos los siguientes pasos:

```
sudo chage -M 10 -W 2 prueba1
```

```
sudo chage -M 10 -W 2 prueba2
```

```
sudo chage -M 10 -W 2 prueba3
```

```
sudo chage -M 10 -W 2 prueba4
```

Comprobación de restricciones en las contraseñas

Para ello lo que realizaremos será modificar la fecha para así comprobar los mensajes al encontrarse en la fecha límite y posterior de la fecha límite.

Esto lo realizaremos mediante el comando :

```
date --set "año-mes-día"
```

➔ **Parte 5:**

Para esto lo que haremos será crear un fichero "script.sh" , con el siguiente contenido:

```
#!/bin/bash  
df
```

Posteriormente le cambiamos los permisos del fichero.

```
chmod u+x script.sh
```

Ya solamente haría falta iniciar sesión con la cuenta que hayamos modificado.