Gestión de Usuarios

1. **Creación de usuario "pepe"**:
    - Se utiliza el comando **pw useradd pepe -m -h0** para crear el usuario "pepe" con su directorio personal y sin asignar una contraseña de forma explícita.

      - pw useradd pepe -m -h0

    - Se utiliza **pw usershow pepe** para mostrar la información del usuario "pepe", que incluye su UID, GID, directorio personal y shell predeterminado.

      - pw usershow pepe

    - Se utiliza **pw groupshow pepe** para mostrar la información del grupo de "pepe".

      -pw groupshow pepe

2. **Inicio de sesión y comprobaciones para el usuario "pepe"**:
    - Se inicia sesión mediante SSH con el usuario "pepe".
    - Se utiliza **id** para verificar la identidad del usuario.
    - Se utiliza **pwd** para mostrar el directorio de trabajo actual.
    - Se verifica los permisos del directorio personal de "pepe" con **ls -ld $HOME**.
    - Se crea un archivo de prueba y se verifica con **ls -l**.

      -ssh pepe@localhost

      -id

      -pwd

      --ls -ld $HOME

      -touch prueba1.txt

      -ls -l

3. **Creación de usuarios "luis" y "ana"**:
    - Se utiliza **pw useradd -D -M 700** para establecer el valor predeterminado de los permisos de los directorios creados.

      -pw useradd -D -M 700

    - Se utiliza **pw useradd luis -m -h0 -c 'Luis Carvajal' -s /bin/csh** para crear el usuario "luis" con un shell específico.

      -pw useradd luis -m -h0 -c 'Luis Carvajal' -s /bin/csh

    - Se utiliza **pw useradd ana -m -h0 -c 'Ana García'** para crear el usuario "ana" con una descripción.

-pw useradd ana -m -h0 -c 'Ana García'

4. **Creación del usuario "beatriz" y cambio del shell predeterminado**:
    - Se crea el usuario "beatriz" con un UID específico mediante **pw useradd beatriz -m -h0 -u 20001**.

      -pw useradd beatriz -m -h0 -u 20001

      -ssh beatriz@localhost
    - Se cambia el shell predeterminado a **/usr/local/bin/bash** utilizando **pw useradd -D -s /usr/local/bin/bash**.
    - Se crea el usuario "carlos" con la herramienta **pw useradd carlos -m -h0**.

      -pw useradd -D -s /usr/local/bin/bash

      -pw useradd carlos -m -h0
5. **Bloqueo de la cuenta "ana" y cambio de contraseña para "beatriz"**:
    - Se bloquea la cuenta de "ana" con **pw lock ana**.

      -pw lock ana
    - Se intenta iniciar sesión con "ana" para verificar que está bloqueada.

      -ssh ana@localhost
    - Se desbloquea la cuenta de "ana" con **pw unlock ana**.

      -pw unlock ana
    - Se cambia la contraseña de "beatriz" utilizando **passwd beatriz**.

      -passwd beatriz
6. **Modificación de la descripción para el usuario "ana"**:
    - Se utiliza **pw usermod ana -c 'Ana Jiménez'** para cambiar la descripción del usuario "ana".

      -pw usermod ana -c 'Ana Jiménez'
    - Se utiliza -**finger ana** para verificar el cambio en la descripción.
7. **Cambio del UID para el usuario "ana" y comprobación de los permisos del directorio personal**:
    - Se utiliza **pw usermod ana -u 5000** para cambiar el UID de "ana".

      -pw usermod ana -u 5000

      -ssh ana@localhost

      -id

-ls -ld $HOME

8. **Eliminación de los usuarios "carlos" y "beatriz"**:
    - Se elimina el usuario "carlos" utilizando **pw userdel carlos**.
    - Se elimina el usuario "beatriz" utilizando **rmuser -y beatriz**.
9. **Creación del grupo "amigos" y asignación de usuario "emilio"**:
    - Se crea el grupo "amigos" con **pw groupadd amigos**.
    - Se añade el usuario "emilio" al grupo "amigos" con **pw useradd emilio -m -h0 -G amigos**.
    - Se inicia sesión con "emilio" para verificar la asignación al grupo.

      -ssh emilio@localhost
10. **Añadir usuario "pepe" al grupo "amigos" y verificar los cambios**:
    - Se añade "pepe" al grupo "amigos" con **pw usermod pepe -G amigos**.
    - Se muestra la información del grupo "amigos" con **pw groupshow amigos**.
11. **Añadir usuario "luis" al grupo "amigos" y verificar los cambios**:
    - Se añade "luis" al grupo "amigos" con **pw groupmod amigos -m luis**.
    - Se muestra la información actualizada del grupo "amigos" con **pw groupshow amigos**.
12. **Eliminar usuario "pepe" del grupo "amigos" y verificar los cambios**:
    - Se elimina "pepe" del grupo "amigos" con **pw groupmod amigos -d pepe**.
    - Se muestra la información actualizada del grupo "amigos" con **pw groupshow amigos**.

Supervisión de Usuarios

13.

- who # Muestra quién está conectado al sistema y desde dónde
- w # Proporciona una visión más detallada de los usuarios conectados, incluyendo qué están haciendo
- finger # Muestra información detallada sobre los usuarios conectados, incluyendo su nombre, terminal, hora de inicio de sesión, entre otros detalles
- last # Muestra un historial de las últimas conexiones al sistema, incluyendo la hora de inicio y fin de sesión, así como la duración de la sesión

Estos comandos proporcionarán información valiosa sobre la actividad de los usuarios en el sistema.

Para las Tareas 14 y 15, que involucran la definición de variables de entorno para un usuario específico y para todos los usuarios del sistema, respectivamente, se necesitan modificar ciertos archivos de configuración. Aquí están los pasos:

Tarea 14:

1. Para definir las variables de entorno para un usuario específico (por ejemplo, "usuario"):

Edite el archivo .profile o .bash_profile del usuario en su directorio de inicio

nano ~/.profile # O ~/.bash_profile

2. Agregue las siguientes líneas al archivo con los valores deseados:

bashCopy code

export EDITOR=ee

export PAGER=less

export LESS=-I

export LANG=es_ES.UTF-8

export CLICOLOR

export PATH=$PATH:/usr/local/prog/bin

export PS1='\h:\w \$'

Tarea 15:

1. Para definir las variables de entorno para todos los usuarios del sistema:

Edite el archivo de perfil global del shell correspondiente

nano /etc/profile # Para shell sh/bash

nano /etc/csh.cshrc # Para shell csh/tcsh

Permisos de Ficheros

- **r** (read): Permite la lectura del archivo o directorio. (4)
- **w** (write): Permite la escritura en el archivo o directorio, o bien la creación o eliminación de archivos dentro de un directorio. (2)
- **x** (execute): Permite la ejecución de un archivo (en el caso de un archivo regular) o la búsqueda y acceso a archivos dentro de un directorio (en el caso de un directorio). (1)
- **-** (guion): Indica que el permiso correspondiente está desactivado.

    - **rwxr-xr- -**

1. **rwx**: Permisos del propietario del archivo. (Primer Dígito)
2. **r-x**: Permisos del grupo al que pertenece el archivo. (Segundo Dígito)
3. **r--**: Permisos para otros usuarios del sistema. (Tercer Dígito)

   Cada dígito se descompone en tres bits, que pueden tener un valor de 0 a 7, representando diferentes combinaciones de permisos:

Tarea 16: Comprobar el valor actual de umask y crear un archivo y un directorio.

umask # Comprobar el valor actual de umask

touch archivo.txt # Crear un archivo

mkdir directorio # Crear un directorio

ls -l archivo.txt directorio # Ver los permisos de los archivos creados

Tarea 17: Cambiar el valor de umask y crear más archivos y directorios.

umask 022 # Cambiar el valor de umask

touch archivo2.txt # Crear otro archivo

mkdir directorio2 # Crear otro directorio

ls -l archivo2.txt directorio2 # Ver los permisos de los archivos creados

Tarea 18: Cambiar el valor de umask de manera permanente para un usuario.

Editar el archivo de perfil del usuario correspondiente nano ~/.profile # o ~/.bash_profile # Agregar la línea siguiente (o modificar la existente): umask 022 # Cambiar umask a 022 # Guardar y cerrar el archivo, luego cerrar y volver a abrir la sesión para que los cambios surtan efecto.

Tarea 19: Crear el directorio /home/pruebas y establecer permisos adecuados.

sudo mkdir /home/pruebas # Crear el directorio

sudo chmod 777 /home/pruebas # Establecer permisos para que cualquier usuario pueda acceder

Tarea 20: Crear usuarios y grupos.

sudo pw useradd adan

sudo pw useradd bea

sudo pw useradd carla

sudo pw useradd david

sudo pw groupadd chicos

sudo pw groupadd chicas

sudo pw groupmod chicos -m adan,david

sudo pw groupmod chicas -m bea,carla

Tarea 21: Crear los directorios con los permisos especificados.

cd /home/pruebas

mkdir alfa beta gamma delta

chmod 700 alfa # Permisos solo para el usuario adan

chmod 770 beta # Permisos para bea y el grupo chicas

chmod 770 gamma # Permisos para carla y el grupo chicos

chmod 744 delta # Permisos para david, solo lectura para otros

sudo chown adan:chicos /home/pruebas/alfa

sudo chmod 700 /home/pruebas/alfa

sudo chown bea:chicas /home/pruebas/beta

sudo chmod 770 /home/pruebas/beta

sudo chown carla:chicos /home/pruebas/gamma

sudo chmod 770 /home/pruebas/gamma

sudo chown david /home/pruebas/delta

sudo chmod 744 /home/pruebas/delta

Tareas 22 a 25: Estas tareas requieren interacción manual y observación de los resultados. Puedes utilizar los comandos **su** o **ssh** para iniciar sesión con los usuarios correspondientes y realizar las comprobaciones necesarias. Por ejemplo:

su adan ls -l /home/pruebas/alfa touch /home/pruebas/alfa/archivo_prueba.txt ls -l /home/pruebas/alfa exit # Salir de la sesión de adan

Ejecución de operaciones privilegiadas

Tarea 26:

ls -l /sbin/shutdown

Este comando muestra los permisos del programa **/sbin/shutdown**, lo que nos permite determinar quién puede ejecutarlo y bajo qué condiciones.

-sr-xr-- 2 root operator 15616 Apr 7 2023 /sbin/shutdown

- -r l bit **s** en lugar del bit **x** en el primer conjunto de permisos indica que el bit setuid está activado para el propietario del archivo. Esto significa que cuando un usuario ejecuta este programa, lo ejecuta con los mismos permisos del propietario del archivo, en este caso, **root**.
- El bit **r-x** indica que el grupo al que pertenece el archivo (en este caso, **operator**) tiene permisos de lectura y ejecución, pero no de escritura.
- El bit **r--** indica que otros usuarios fuera del propietario y el grupo solo tienen permisos de lectura, pero no de ejecución ni escritura.

Tarea 27:

su nombre_de_usuario

El comando **su** permite a un usuario cambiar su identidad a otra cuenta de usuario, generalmente a una cuenta con más privilegios, como el superusuario (root).

Tarea 28:

pkg info sudo # Verifica si sudo está instalado

pkg install sudo # Instala sudo si es necesario

El primer comando verifica si **sudo** está instalado en el sistema, mientras que el segundo comando instala **sudo** si no está presente. Luego, para permitir que el usuario **pepe** ejecute cualquier comando con **sudo**, se edita el archivo de configuración de **sudo** utilizando el comando **visudo** y se agrega la línea **pepe ALL=(ALL) ALL**.

Syslog

1. **Facilidades:** Las facilidades son categorías predefinidas que indican la fuente del mensaje. Permiten clasificar los mensajes según su origen. Algunos ejemplos comunes de facilidades son:
    - **auth**: Para mensajes relacionados con autenticación y autorización.
    - **mail**: Para mensajes relacionados con el sistema de correo electrónico.
    - **local0** a **local7**: Reservados para aplicaciones específicas que deseen registrar mensajes.

Estas facilidades proporcionan una manera estructurada de identificar la fuente de los mensajes registrados, lo que facilita la filtración y el análisis posterior.

2. **Prioridades:** Las prioridades son niveles de importancia asignados a los mensajes. Permiten clasificar los mensajes según su gravedad o urgencia. Van desde el nivel más bajo, "debug" (depuración), hasta el nivel más alto, "emergency" (emergencia). La lista completa de prioridades estándar incluye:
    - **debug**: Mensajes de depuración, útiles para desarrolladores.
    - **info**: Mensajes informativos que no indican problemas.
    - **notice**: Mensajes normales pero significativos.
    - **warning**: Mensajes que indican condiciones potencialmente problemáticas.
    - **err**: Mensajes que indican errores no críticos.
    - **crit**: Mensajes que indican errores críticos.
    - **alert**: Mensajes que requieren atención inmediata.
    - **emergency**: Mensajes que indican condiciones de emergencia que requieren acción inmediata.

Al asignar una prioridad a un mensaje, se comunica la importancia relativa del evento registrado, lo que ayuda a los administradores del sistema a priorizar y responder adecuadamente a los problemas.

3. **Acciones:** Las acciones determinan qué se hace con los mensajes registrados. Pueden incluir:
    - **Impresión en la consola**: Los mensajes pueden mostrarse en la consola del sistema para que los usuarios y administradores puedan verlos directamente.
    - **Almacenamiento en archivos de registro específicos**: Los mensajes se pueden escribir en archivos de registro específicos, como **/var/log/messages**, **/var/log/auth.log**, etc.
    - **Envío por correo electrónico**: Los mensajes pueden enviarse por correo electrónico a direcciones de correo electrónico predefinidas.

- **Reenvío a otro servidor syslog**: Los mensajes pueden reenviarse a otro servidor syslog para su procesamiento y almacenamiento centralizados.

Estas acciones permiten a los administradores del sistema configurar syslog para que los mensajes se manejen de la manera más adecuada según las necesidades del entorno y los requisitos de seguimiento y resolución de problemas.

Tarea 31: Para examinar la configuración actual del demonio **syslogd** y ojear el contenido de algunos de los ficheros de **/var/log**, puedes ejecutar los siguientes comandos:

cat /etc/syslog.conf # Examinar la configuración actual de syslogd

cat /var/log/messages # Ojear el contenido del archivo de mensajes generales del sistema

cat /var/log/cron # Ojear el contenido del archivo de registros de cron

cat /var/log/security # Ojear el contenido del archivo de registros de seguridad

Estos comandos te permitirán ver la configuración actual del demonio **syslogd** en el archivo **/etc/syslog.conf** y ojear el contenido de algunos de los archivos de registro en **/var/log**, como **messages**, **cron** o **security**, que son comunes en muchos sistemas Unix y Linux.

Tarea 32: Para registrar todos los mensajes de importancia "warning" o superior generados por la aplicación "acme" en el fichero **/var/log/acme.log**, se pueden añadir las siguientes líneas al fichero de configuración de **syslogd**:

- local4.warning /var/log/acme.log

Esto indicará al demonio **syslogd** que registre todos los mensajes del subsistema **local4** con importancia **warning** o superior en el archivo **/var/log/acme.log**