ADMINISTRACIÓN DE SEGURIDAD

1 OBJETIVO:

Comprender y manejar la seguridad en Linux con el objetivo de administrar los usuarios y el acceso a los recursos por parte de estos.

Es parte de este objetivo la creación de usuarios y grupos y la lectura de los permisos de cada archivo o directorio, teniendo en cuenta quien accede al mismo y con que permisos lo hace

2 USUARIOS

Entre otras cualidades Linux es reconocido por su seguridad, y un punto crítico en este tema es la definición de usuarios.

De forma predeterminada al instalar el sistema queda declarado un usuario llamado "**root**". Este usuario o mejor dicho "Súper Usuario" tiene derechos plenos, y es quién puede realizar todas las tareas administrativas, accediendo a áreas críticas del sistema sin restricción alguna. Es por esto, entre otros motivos, por lo cual dentro de un entorno Linux es altamente recomendado no ingresar al sistema como "root" salvo que la tarea a desarrollar así lo requiera.

Una de las primeras tareas administrativas a realizar entonces consistirá en el alta de usuarios, grupos, y las asignaciones de permisos para los mismos.

Debemos tener muy presente que Linux es CASE SENSITIVE, es decir que distingue entre mayúsculas y minúsculas, lo cual es muy importante tener en cuenta tanto al momento de seleccionar un nombre como una contraseña. Por otro lado existe una convención, que se arrastra de Unix, por la cuál no se recomienda utilizar mayúsculas en los nombres de usuarios.

3 PERMISOS

En el capítulo anterior hemos tenido un primer acercamiento a la línea de comandos, viendo algunas órdenes básicas para poder movernos a través de la estructura de directorios de LINUX. Este es el momento de comenzar con la administración de la seguridad del sistema. Como punto de partida debemos saber que dentro de un sistema UNIX, cada archivo o directorio tiene una serie de permisos establecidos y que los mismos, se definen a tres niveles: Propietario, Grupo, y otros.

Pasemos entonces a explicar en que consisten cada uno de estos grupos:

- **Usuario Propietario**: También llamado *owner* en inglés, es el usuario que ha creado el archivo. Se lo identifica con la letra **u** (de **U**ser).
- **Grupo Propietario**: Es el grupo de usuarios al que se le define como propietario del archivo o directorio. Su identificación se realiza con la letra **g**. (de **G**roup)
- **Otros**: o *others*, o sea todos los demás usuarios del sistema que nos son ni el usuario ni el grupo propietario, a los que se identifica mediante la letra **o** (**O** de **O**thers).

Los permisos que se pueden establecer sobre un archivo o directorio son los siguientes:

- **r**: ***r****ead* (lectura). El usuario que tenga este permiso podrá si es un directorio, listar los recursos almacenados en él, y si es cualquier otro tipo de archivo podrá leer su contenido.

- **w**: ***w****rite* (escritura). Todo usuario que posea este permiso para un archivo podrá modificarlo. Si se posee para un directorio se podrán crear y borrar archivos en su interior.

- **x:** *execute* (ejecución). Este permiso para el caso de los archivos permitirá ejecutarlos desde la línea de comandos y para los directorios, el usuario que lo posea tendrá acceso para realizar el resto de las funciones permitidas mediante los otros permisos (lectura y/o escritura).

Para determinar los permisos finales siempre se deben tener en cuenta los siguientes aspectos:

- La prioridad en la aplicación de permisos es: **U**suario, **G**rupo, **O**tros, siendo esto determinante al momento de calcular los permisos efectivos.

- Para poder realizar operaciones sobre cualquier directorio (leer o escribir) será necesario siempre, tener otorgado además el permiso de ejecución.

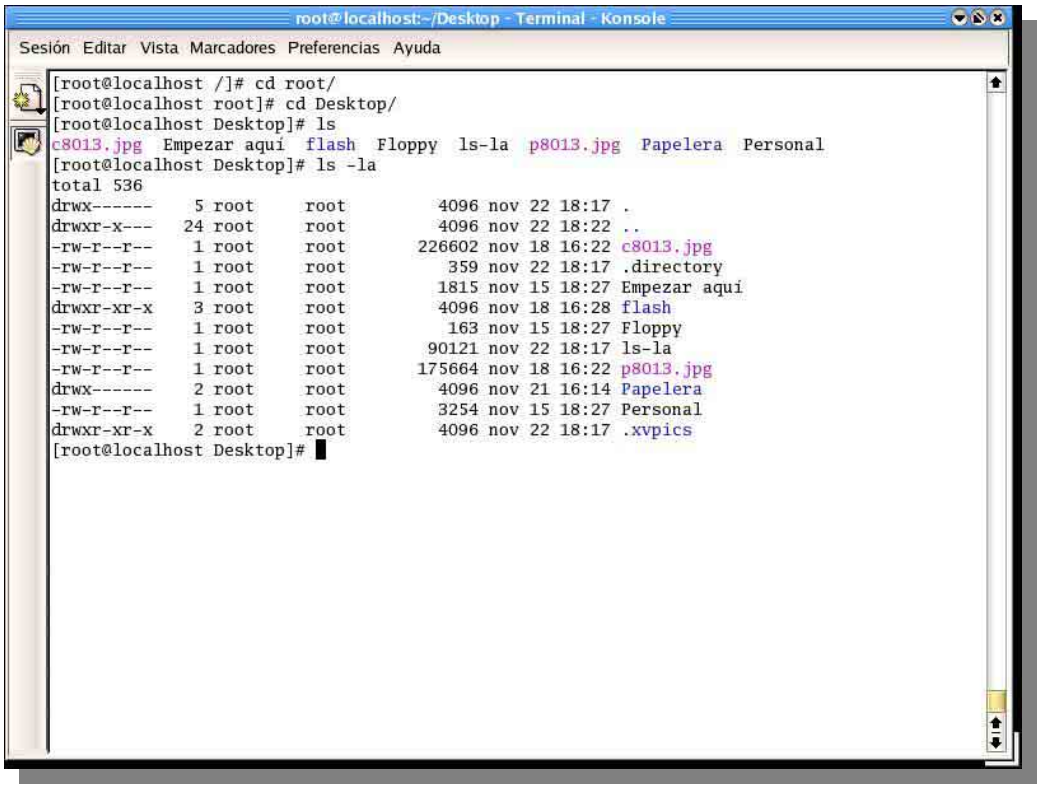
- Para acceder a un recurso de cualquier forma (ejecución, lectura o escritura) se deben tener permisos de ejecución para todos los directorios que contienen al recurso directa e indirectamente.

3.1 LECTURA DE PERMISOS

Para clarificar este tema vamos a usar la figura siguiente, en la cual es posible observar el contenido de un directorio, luego de ejecutar el comando ***ls –la*** (recordemos que el modificador **l** muestra información detallada del contenido de un directorio y **a**, permite visualizar a los archivos ocultos).

En primer lugar la expresión *total*, refiere al número de bloques de disco ocupados por los archivos del directorio listado (en este caso 536 bloques).

Los campos que aparecen de izquierda a derecha son los siguientes:



- El primer carácter es el modo del archivo, siendo este una **d** si se trata de un directorio, un guión **"-"** si se trata de un archivo estándar o una **b** o una **c**, si se trata de archivos de dispositivo (modo **b**loque o **c**arácter).
- Los siguientes nueve caracteres refieren a los permisos del archivo o directorio anteriormente citados (ugo), de modo que los tres primeros hacen alusión a los permisos del usuario propietario (u)**,** los tres siguientes a los permisos del grupo al que pertenece (g) y los últimos tres a los permisos declarados para el resto de los usuarios (o). A modo de ejemplo podemos visualizar que el archivo ***p8013.jpg***, tiene definidos permisos ***rw*** (lectura y escritura) para el propietario, y de solo lectura ***r*** tanto para el grupo al cual pertenece el *owner* como para los demás usuarios.
- La primera columna, contiene un número (**1** en el caso de nuestro archivo p8013.jpg) que refiere al número de links o enlaces que existen a este archivo en diferentes lugares del sistema de archivos. En el caso de los directorios, el número hace referencia a los subdirectorios que contiene ese directorio.
- La siguiente indica el propietario (*owner*) del archivo o directorio (root).

- La tercera muestra el nombre del grupo que incluye al *owner* (root).
- La cuarta columna muestra el tamaño del archivo.
- Luego viene información de fecha y hora de modificación.
- Por último, en la sexta columna figura el nombre del archivo o directorio.

4 COMANDOS RELACIONADOS

- ***adduser***

Este comando permite agregar un nuevo usuario al sistema.

Sintaxis:

adduser -[OPCIONES] NOMBRE_USUARIO

Opciones:

```
-d    (home dir)
```

Se utiliza para establecer el directorio de trabajo del usuario. Es conveniente, a fin de tener un sistema bien organizado, que este se localice dentro del directorio /home.

```
-e    (expire date)
```

Se utiliza para establecer la fecha de expiración de una cuenta de usuario. Esta debe ingresarse en el siguiente formato: AAAA-MM-DD.

```
-g    (initial group)
```

Indica el GID (group ID), esto es el grupo al que ese usuario pertenece. Esto es importante porque en Linux un grupo de usuarios puede compartir una serie de archivos y directorios. El número ha de ser el mismo para todos los que formen el grupo. Así, el grupo de los que formen el grupo 100 será uno, el 101 será otro, el 102 otro, etc. (TODOS los USUARIOS, deberían estar bajo el mismo grupo, "users", que suele ser el grupo 100). Los archivos que identifican a los grupos están en: /etc/group.

Se utiliza para establecer grupos adicionales a los que pertenecerá el usuario. Estos deben separarse utilizando una coma y sin espacios. Esto es muy conveniente cuando se desea que el usuario tenga acceso a determinados recursos del sistema, como acceso a la unidad de disquetes, administración de cuentas, etc. Nota: los grupos asignados deben existir.

```
-u [uid]
```

Se utiliza para establecer el UID, es decir la ID del usuario, que debe ser único. De forma predeterminada se establece como UID el número mínimo mayor a 99 y mayor que el de otro usuario existente. Cuando se crea una cuenta de usuario por primera vez, generalmente se asignará 500 como UID del usuario. Los UID entre 0

y 99 son reservados para las cuentas de los servicios del sistema. Los usuarios se almacenan en el archivo /etc/passwd.

Una vez generado el usuario será necesario asignarle una contraseña mediante el uso del comando *passwd*, que pasaremos a explicar a continuación.

- ***passwd***:

Como hemos dicho mediante el uso del comando, se le asigna una contraseña a un usuario. Una vez ingresado el comando, el sistema requerirá que se proceda a teclear la nueva contraseña para el usuario y que la repitamos para confirmar. Por seguridad el sistema no mostrará los caracteres tecleados, por lo que debe hacerse con cuidado. Este procedimiento también puede utilizarse para cambiar una contraseña existente.

Sintaxis:

passwd [NOMBRE_USUARIO]

- ***groupadd***

Se utiliza para crear nuevos grupos en el sistema. El archivo que contiene la base de datos de los grupos es /etc/group.

Sintaxis:

groupadd -[OPCIONES] NOMBRE_GRUPO

Opciones:

-g [gid] ID para el grupo, el cual debe ser único y mayor que 499.

-f Aborta la operación y muestra un error si el grupo ya existe. (El grupo no es alterado.) Si se especifica -g y -f, pero el grupo ya existe, la opción -g es ignorada

4.1 ARCHIVOS DE CONFIGURACION IMPORTANTES

- **/etc/passwd**

Archivo que contiene la base de datos de los usuarios del sistema. Dentro del mismo nos encontramos con 7 campos separados por ":", en donde se especifica:

[login]:[password]:[número_de_usuario]:[número_grupo]:[info_usuario]:[directorio_home]:[shell]

Si en el lugar de la contraseña nos encontramos con la letra "x", significa que la información relativa a la misma está almacenada por motivos de seguridad, en forma encriptada en otro archivo de configuración ubicado en */etc* llamado *shadow*.

Veamos como ejemplo una línea del archivo *passwd*:

ita:x:500:500::/home/ita:/bin/bash

Si utilizamos la estructura anteriormente citada podemos obtener la siguiente información:

Nombre login:	ita
Password :	no hay información
UID:	500
GID:	500
Información del usuario:	no hay
Directorio Home:	/home/ita
Shell:	/bin/bash

Como vemos la información de la contraseña no está almacenada aquí, hecho que es reconocible por la aparición de la letra "x" en el lugar de la misma.

Shell se refiere al intérprete de comandos del usuario, que será el que use inmediatamente después de entrar en el sistema. De forma predeterminada es /bin/bash.

- **/etc/group**

Este archivo es el que contiene la base de datos de los grupos existentes en el sistema. Su estructura es similar a la de *passwd*. Por lo tanto en cada línea del archivo, nos encontraremos con los siguientes campos:

[nombre_grupo]:[password]:[GID]:[lista_usuarios]

Nombre_grupo: De forma predeterminada, con los comandos habituales se crea un grupo con el mismo nombre que el usuario creado, aunque pueden existir otros grupos con nombres específicos.

Password: Se usa para dar a una serie de individuos un mismo directorio con una cuenta común.

GID : (Group ID) Número de Identificación en el Sistema del grupo.

Lista_usuarios: son los usuarios que pertenecen al grupo, separados por comas.

- **/etc/shadow**

La función de este archivo es almacenar las contraseñas de los usuarios definidos en /etc/password en forma encriptada. La particularidad de este archivo es que tiene restringidos los permisos y no es accesible por los usuarios normales, de modo que no puedan acceder a la información de los usuarios.

La estructura de cada entrada del archivo es la siguiente:

[Usuario]:[password]:[días del último cambio]:[días antes del cambio]:[Días después del cambio]:[tiempo de aviso]:[días antes de la inhabilitación]:[periodo que lleva caducado]

Usuario: Nombre del usuario

Password : Este es el password cifrado.

Días del último cambio: Tiempo transcurrido desde el último cambio de password, pero contado en días a partir del 1 de enero de 1970, comienzo de la era UNIX.

Días antes del cambio: Periodo (en días) para que el password deba ser cambiado.

Días después del cambio: Días transcurridos luego de ser cambiado.

Tiempo de aviso: Periodo en el que el sistema tiene que avisar de la necesidad del cambio.

Días antes de la Inhabilitación: Días antes de la inhabilitación de la cuenta.

Periodo que lleva caducado: Días desde que la cuenta está deshabilitada.

NOTAS

CUESTIONARIO CAPITULO 32

1.- ¿Que comando utilizaría para listar el contenido de una carpeta y observar los premisos establecidos a sus archivos y Directorios?

2.- ¿Cuál es el resultado de escribir el comando adduser –d /home/Sergio sergio?

3.- ¿Cuál es el objetivo de archivo shadow ubicado en /etc?

4.- ¿Cuál es el resultado de escribir groupadd admin?

5.- ¿En la lectura de permisos que es U G O y cual es su significado?