Practica 9 Linux - Administración de usuarios.

GNU/Linux es un sistema operativo multiusuario. Esto significa que permite a varios usuarios utilizar el sistema simultáneamente, a través de la línea de comandos o con conexiones remotas. GNU/Linux controla el acceso al equipo y a sus recursos a través de las cuentas de usuarios y grupos. En los sistemas GNU/Linux existen tres tipos de usuarios:

Tipos de usuarios:

 Root. Es el usuario más importante ya que es el administrador y dueño del sistema. Se aconseja utilizar la cuenta de *root* para las tareas específicas de administración y el resto del tiempo utilizar una cuenta de usuario normal.

 Usuarios normales. Son los usuarios que pueden iniciar sesión en el sistema y tienen una funcionalidad limitada, tanto en los comandos que pueden ejecutar, como a los ficheros a los que tienen acceso.

 Usuarios asociados a servicios. Este tipo de usuarios no pueden iniciar sesión en el sistema. Su utilización es muy útil ya que permiten establecer los privilegios que tiene un determinado servicio. Por ejemplo, el servidor de páginas Web tiene asociado un usuario para poder especificar a qué ficheros tiene acceso; y por lo tanto que ficheros son visibles a través de Internet.

Todos los usuarios del sistema tienen un identificador de usuario (UID) y un identificador de grupo (GID). El administrador del sistema *root* tiene los identificadores de usuario y grupo 0:0 y los demás usuarios tienen un valor mayor que 0. Existen varias formas de administrar el sistema, que van variando dependiendo de su facilidad o control sobre el sistema.

Básicamente, puede administrar el sistema a través de tres formas diferentes:

 Interfaces gráficas. Existen diferentes interfaces gráficas que permiten administrar el sistema de una forma fácil y sencilla. Puede utilizar la interfaz de administración de x-Windows o utilizar la web de administración (webmin). Este método es el más sencillo, pero es el que menos control proporciona sobre el sistema.

 Terminal del sistema. Una de las ventajas de los sistemas GNU/Linux es que puedes administrarlo totalmente a través del intérprete de comandos o terminal del sistema. Una de las grandes ventajas de utilizar el terminal del sistema es que permite una gran flexibilidad a la hora de interactuar con el sistema, pudiendo crear pequeños programas (scripts) para simplificar la administración del sistema.

 Ficheros de configuración. Por último, la modificación directa de los ficheros de configuración es el método que permite tener un mayor control del

sistema. Como desventaja hay que destacar que para administrar el sistema de esta forma hay que conocer muy bien el sistema.

No se puede decir que un método sea el mejor, ya que el uso de un método u otro depende siempre de la tarea que desees realizar y de tus conocimientos. Lo mejor, como siempre, es conocer los tres métodos y utilizar el mejor en cada momento.

Intérprete de comandos.

La gestión de usuarios y grupos se puede realizar directamente a través del intérprete de comandos. En la siguiente tabla se muestran los comandos más importantes para la gestión de usuarios y grupos.

Comando	Descripción
Usuarios	
adduser <usuario>	Permite dar de alta a un usuario. Cuando das de alta un usuario el sistema solicita sus datos como nombre completo, dirección, contraseña, etcétera.
addgroup	Permite dar de alta un usuario dentro de un grupo.
chage	Permite establecer los periodos de vigencia de las contraseñas.
id	Muestra el usuario que se está utilizando.
passwd	Permite cambiar la contraseña de un usuario. Si ejecutas passwd cambias la contraseña del usuario actual y si ejecutas passwd nombre_usuario cambia la contraseña del usuario indicado.
su	Permite cambiar de usuario.
sudo	Permite ejecutar un comando como root.
userdel <usuario>	Permite borrar un usuario.
usermod	Permite modificar las propiedades de un usuario.
Grupos	
groups	Muestra los grupos a los que pertenece el usuario.
groupadd	Permite dar de alta a un grupo.
groupdel	Permite borrar un grupo de usuarios.
groupmod	Permite modificar las propiedades de un grupo.
Manipulación del fichero /etc/shadow	
pwconv	Crea y actualiza el fichero /etc/shadow.
pwunconv	Desactiva el fichero /etc/shadow.

Ficheros utilizados.

Siempre resulta muy útil conocer el funcionamiento interno del sistema operativo para poder tener un mayor control de las operaciones que realiza. Para conocer el funcionamiento interno debes conocer dos tipos de ficheros:

aquellos ficheros que se utilizan para guardar la información de los usuarios y grupos, y los ficheros con los valores predeterminados que utiliza el sistema. La información de las cuentas de usuario y grupos se encuentran en los siguientes ficheros:

 /etc/passwd**.** En este fichero se encuentra un listado de las cuentas de usuario que están dados de alta en el sistema.

 /etc/shadow**.** En este fichero se encuentran cifradas las contraseñas y sus periodos de vigencia.

 /etc/group**.** Listado de grupos activos en el sistema y usuarios que pertenecen a dichos grupos.

En el fichero /etc/passwd se almacenan los datos de las cuentas de los usuarios. A continuación se muestra el fragmento de código de un usuario:

javier:x:1000:1000::/home/javier:/bin/bash

Como puede ver en el ejemplo anterior, para cada usuario se almacena la siguiente información:

Login:x:UID:GID:Descripción:Directorio de trabajo: Shell del usuario

Es recomendable asignar a los servicios del sistema el shell /bin/false para que no puedan iniciar sesión en el sistema.

Por motivos de seguridad, las contraseñas de los usuarios se almacenan en el fichero /etc/shadow y no en el fichero /etc/passwd.

Por ejemplo, para el usuario anterior en el fichero /etc/passwd en vez de almacenar la contraseña se guarda el carácter “x“ y en el fichero /etc/shadow se almacena la contraseña cifrada.

El fichero /etc/group almacena los datos de los grupos que han sido dados de alta en el sistema. A continuación se muestra un fragmento del fichero: root:x:0:root,javier javier:x:1000: Para cada grupo el sistema almacena el nombre del grupo, el identificador de grupo (GID) y los usuarios que pertenecen al grupo. En el ejemplo anterior se puede ver como los usuarios root y javier pertenecen al grupo root. Al dar de alta un usuario si no especifica ningún parámetro el sistema utiliza los valores por defecto. El sistema guarda los valores por defecto en los siguientes ficheros:

 /etc/default/useradd. Permite establecer el shell que se va utilizar por defecto, el directorio home que van a tener los usuarios, etcétera.

 /etc/login.defs. Entre las opciones más importantes permite establecer los datos de expiración de las contraseñas, longitud mínima de las contraseñas, UID y GID mínimos y máximos, etcétera.

1.3.- Configuración con asistentes.

La administración de los usuarios del sistema se puede realizar gráficamente con la herramienta Usuarios y grupos en xWindows o a través de webmin.

Inicia la aplicación Usuarios y grupos que se encuentra en el submenú Administración dentro de sistema. Aparece la ventana Gestor de usuarios donde puedes realizar la administración de los usuarios del sistema de una forma fácil y sencilla. Para añadir un nuevo usuario pulsa el botón Añadir, introduce el nombre de usuario, pulsa Aceptar y posteriormente introduce la contraseña del usuario.

Otra forma de administrar los usuarios del sistema es utilizar Webmin.

Recuerda que Webmin es una herramienta de configuración de sistemas accesible vía web para GNU/Linux y otros sistemas Unix. Para ello puedes acceder con un navegador a webmin (https://127.0.0.1:10000). Una vez dentro en la página principal dentro de menú System accedes a Users and groups.

Practica

1. Crea los grupos smr1 y smr2

2. . Crea los usuarios pedro y pablo. Estos usuarios deben pertenecer únicamente al grupo smr1.

3. . Crea los usuarios alba y nerea. Estos usuarios deben pertenecer únicamente al grupo smr2.

4. Accede como usuario pedro

5. Crea un fichero con nombre topsecret.txt al que únicamente él tenga acceso, tanto de lectura como de escritura.

6. . Crea otro fichero, también como usuario pedro, con nombre ventas_trimestre.txt al que tengan acceso, tanto para leer como para escribir todos los usuarios que pertenezcan al mismo grupo. Comprueba como usuario pablo que puedes modificar el fichero.

7. . Como usuario alba, crea un fichero con nombre empleados.txt al que pueda acceder cualquier usuario para leer su contenido, y cualquier usuario del mismo grupo para leer o escribir.

8. . Copia el fichero empleados.txt al directorio de trabajo de alumno. Cambia el propietario y el grupo al que pertenece el fichero, ahora debe ser alumno.

9. . Como usuario pablo, copia un programa del directorio /usr/bin al directorio de trabajo con un nombre diferente. Por ejemplo kalarm se puede copiar como alarma. Mira los permisos de este programa. Comprueba que se puede ejecutar.

10. . Cambia los permisos de alarma de tal forma que sólo lo pueda ejecutar el propietario del archivo.

11. .Crea el usuario modesto, perteneciente a oficina2. Dentro de su directorio de trabajo, crea un directorio de nombre compartido_con_todos.

12. .Dentro de ese directorio, edita con el OpenOffice los ficheros telefono_contactos, gastos_marzo y sueldos. Inserta varias entradas en cada uno de los ficheros.

13. .Da permiso de lectura a la carpeta compartido_con_todos y a todos los ficheros que contenga para todos los usuarios.

14. .Restringe el acceso de escritura sobre el fichero telefono_contactos para que sólo lo puedan modificar los usuarios del grupo al que pertenece su propietario.

15. .Cambia los permisos de gastos_marzo para que sólo pueda modificarlo su propietario y leerlo cualquiera del mismo grupo.

16. .Cambia los permisos de sueldos para que sólo su dueño tenga acceso a él, tanto para lectura como para escritura.

17. .Si un usuario tiene permiso de lectura sobre un fichero pero ese fichero se encuentra dentro de un directorio sobre el que no tiene permiso de lectura, ¿podrá leer el fichero?, haz la prueba. Nota: Cada vez que se utilice el comando chmod, una o varias veces en un ejercicio, se deben especificar los parámetros en forma de literales y en forma numérica. Por ejemplo, si escribimos chmod a+r fichero, chmod g+w fichero, chmod ow fichero, chmod ax fichero; debemos indicar también que utilizando el formato numérico tendríamos chmod 664 fichero.