Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

http://www.free-powerpoint-templates-design.com

Usuarios: Linux es un sistema multiusuario, por lo tanto, la tarea de añadir, modificar, eliminar y en general administrar usuarios se con vierte en algo no solo rutinario, sino importante, además de ser un elemento de seguridad que mal administrado o tomado a la ligera, puede convertirse en un enorme hoyo de seguridad. En este ma nua l aprenderás todo lo necesario para administrar completamente tus usuarios en GNU/Linux.

La sintaxis del comando grep al buscar un solo archivo es así:

Tipos de usuarios

Los usuarios en Unix/Linux se identifican por un número único de usuario, User ID, UID. Y pertenecen a un grupo principal de usuario, identificado también por un número único de grupo, Group ID, GID. El usuario puede pertenecer a más grupos además del principal.

Aunque sujeto a cierta polémica, es posible identificar tres tipos de usuarios en Linux:

- Usuario root, También llamado superusuario o administrador.Su UID (User ID) es 0 (cero).

Es la única cuenta de usuario con privilegios sobre todo el sistema.

Acceso total a todos los archivos y directorios con independencia de propietarios y permisos.

Controla la administración de cuentas de usuarios.

Ejecuta tareas de mantenimiento del sistema.

Puede detener el sistema. Instala software en el sistema. Puede modificar o reconfigurar el kernel , controladores.

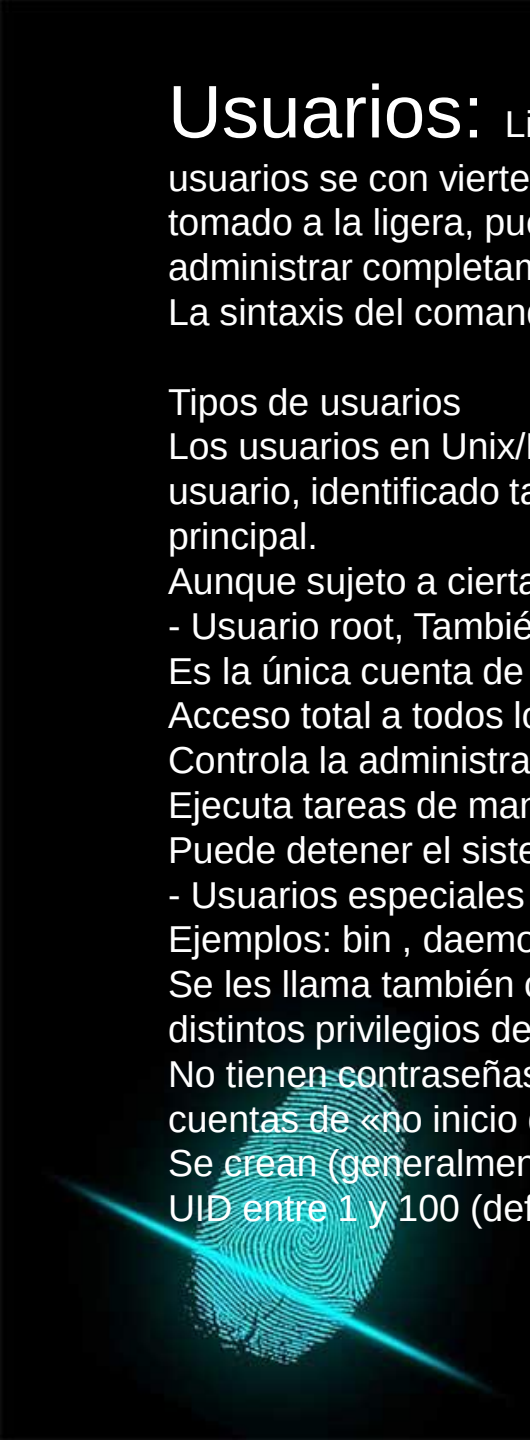
- Usuarios especiales

Ejemplos: bin , daemon , adm , lp , sync , shutdown , mail, operator , squid , apache,

Se les llama también cuentas del sistema. No tiene todos los privilegios del usuario root , pero dependiendo de la cuenta asumen distintos privilegios de root. Lo anterior para proteger al sistema de posibles formas de vulnerar la seguridad.

No tienen contraseñas pues son cuentas que no están diseñadas para iniciar sesiones con ellas. También se les conoce como cuentas de «no inicio de sesión» (nologin)

Se crean (generalmente) automáticamente al momento de la instalación de Linux o de la aplicación. Generalmente se les asigna un UID entre 1 y 100 (definifo en / etc login.defs)



- Usuarios normales
Se usan para usuarios individuales.
Cada usuario dispone de un directorio de trabajo, ubicado generalmente en /home.
Cada usuario puede personalizar su entorno de trabajo.
Tienen solo privilegios completos en su directorio de trabajo o HOME.
Por seguridad, es siempre mejor trabajar como un usuario normal en vez del usuario root , y cuando se requiera hacer uso de comandos solo de root , utilizar el comando
En las distros actuales de Linux se les asigna generalmente un UID superior a 500.

/etc/passwd:

Cualquiera que sea el tipo de usuario, todas las cuentas se encuentran definidas en el archivo de configuración ‘passwd ’, ubicado dentro del directorio /etc. Este archivo es de texto tipo ASCII, se crea al momento de la instalación con el usuario root y las cuentas especiales, más las cuentas de usuarios normales que se hayan indicado al momento de la instalación.
El archivo /etc passwd contiene una línea para cada usuario, similar a las siguientes:
root:x:0:0:root:/root bin bash
pedro:x:501:500:Pedro:/home/pedro:/bin bash
La información de cada usuario está dividida en 7 campos delimitados cada uno por ‘:’ dos puntos.
Campo 1 - Es el nombre del usuario, identificador de inicio de sesión (login). Tiene que ser único
Campo 2 - La ‘x’ indica la contraseña encriptada del usuario, además también indica que se está haciendo uso del archivo / etc shadow , si no se hace uso de este archivo, este campo se vería algo así como: ‘ghy675gjuXCc12r5gt78uuu6R’.
Campo 3 - Número de identificación del usuario (UID). Tiene que ser único. 0 para root , generalmente las cuentas o usuarios especiales se numeran del 1 al 100 y las de usuario normal del 101 en delante, en las distribuciones mas recientes esta numeración comienza a partir del 500.
Campo 4 - Numeración de identificación del grupo (GID). El que aparece es el número de grupo principal del usuario, pero puede pertenecer a otros, esto se configura en /etc/groups
Campo 5 - Comentarios o el nombre completo del usuario.
Campo 6 - Directorio de trabajo (Home) donde se sitúa al usuario después del inicio de sesión.
Campo 7 - Shell que va a utilizar el usuario de forma predeterminada.

/etc/shadow:

Anteriormente (en sistemas Unix) las contraseñas cifradas se almacenaban en el mismo /
etc passwd . El problema es que passwd ’ es un archivo que puede ser leído por cualquier usuario del
sistema, aunque solo puede ser modificado por root . Con cualquier computadora potente de hoy en día, un buen programa de descifrado de contraseñas y paciencia es posible « crackear » contraseñas débiles (por eso la conveniencia de cambiar periódicamente la contraseña de root y de otras cuentas importantes). El archivo ‘ shadow ’, resuelve el problema ya que solo puede ser leido por root . Considérese a shadow ’ como una extensión de passwd ’ ya que no solo almacena la contraseña encriptada, sino que tiene otros campos de control de
El archivo /etc shadow contiene una línea para cada usuario, similar a las siguientes
root:ghy675gjuXCc12r5gt78uuu6R:10568:0:99999:7:7:1::
pedro:rfgf886DG778sDFFDRRu78asd:10568:0:1:9: 1: 1::
La información de cada usuario está dividida en 9 campos delimitados cada uno por ‘:’ dos puntos

Campo 1 - Nombre de la cuenta del usuario.
Campo 2 - Contraseña cifrada o encriptada, un ‘*’ indica cuenta de ‘ nologin
Campo 3 - Días transcurridos desde el 1/ene/1970 hasta la fecha en que la contraseña fue cambiada por última vez.
Campo 4 - Número de días que deben transcurrir hasta que la contraseña se pueda volver a cambiar.
Campo 5 - Número de días tras los cuales hay que cambiar la contraseña. (1 significa nunca). A partir de este dato se obtiene la fecha de expiración de la contraseña.
Campo 6 - Número de días antes de la expiración de la contraseña en que se le avisará al usuario al inicio de la sesión.
Campo 7 - Días después de la expiración en que la contraseña se inhabilitara, si es que no se cambio.
Campo 8 - Fecha de caducidad de la cuenta. Se expresa en días transcurridos desde el 1/Enero/1970 (epoch
Campo 9 - Reservado.

/etc/group:

Este archivo guarda la relación de los grupos a los que pertenecen los usuarios del sistema, contiene una línea para cada usuari o con tres o cuatro campos por usuario:
root:x:0:root
test:x:501:
pedro:x:502:ventas,supervisores,produccion
alumno:x:503:ventas,pedro
El campo 1 indica el usuario.
El campo 2 ‘x’ indica la contraseña del grupo, que no existe, si hubiera se mostraría un ‘hash’ encriptado.
El campo 3 es el Group ID (GID) o identificación del grupo.
El campo 4 es opcional e indica la lista de grupos a los que pertenece el usuario
Actualmente al crear al usuario con useradd se crea también automáticamente su grupo principal de trabajo GID, con el mismo nombre del usuario. Es decir, si se añade el usuario ‘pedro’ también se crea el / etc group el grupo ‘pedro’. Aun así , existen comandos de administración de grupos que se explicarán más adelante

Añadir Usuarios:

Useradd o adduser es el comando que permite añadir nuevos usuarios al sistema desde la línea de comandos. -c añade un comentario al momento de crear al usuario, campo 5 de / etc passwd

useradd juan

Se creará el usuario y su grupo, así como las entradas correspondientes en / etc passwd , etc shadow y / etc group . También se creará el directorio de inicio o de trabajo: /home/juan y los archivos de configuración que van dentro de este directorio y que más adelante se detallan.

Modificar Usuarios con usermod:

Como su nombre lo indica, usermod permite modificar o actualizar un usuario o cuenta ya existente. Sus opciones más comunes o importantes son las siguientes:

-c añade o modifica el comentario, campo 5 de /etc passwd

-d modifica el directorio de trabajo o home del usuario, campo 6 de /etc passwd

-e cambia o establece la fecha de expiración de la cuenta, formato AAAA MM DD, campo 8 de / etc shadow

-g cambia el número de grupo principal del usuario (GID), campo 4 de /etc passwd

-G establece otros grupos a los que puede pertenecer el usuario, separados por comas.

-l cambia el login o nombre del usuario, campo 1 de /etc/passwd y de /etc/shadow

-L bloque la cuenta del usuario, no permitiéndole que ingrese al sistema. No borra ni cambia nada del usuario, solo lo deshabilita.

-s cambia el shell por defecto del usuario cuando ingrese al sistema.

-u cambia el UID del usuario.

-U desbloquea una cuenta previamente bloqueada con la opción L.

Si quiseramos cambiar el nombre de usuario de ‘pedro’ a ‘ peter

#usermod -l peter pedro

Casi seguro también cambiará el nombre del directorio de inicio o HOME en /home, pero si no fuera así, entonces:

#usermod -d /home/peter peter

Otros cambios o modificaciones en la misma cuenta:

#usermod -c "supervisor de area " -s / bin ksh -g 505 peter

Añadir Grupo:

groupadd grupo

Eliminar Grupo:

groupdel grupo

Añadir Usuario dentro de un grupo:

adduser usuario grupo

Eliminar Usuario de un grupo:

deluser usuario grupo

Ver Todos los Grupos del Sistema

cat /etc/group

Cambiar usuario Propietario

chown usuario ruta-fichero

Cambiar grupo propietario

chgrp grupo ruta-archivo

Extructura básica de permisos en archivos:

Hay 3 atributos básicos para archivos simples: lectura, escritura y ejecutar
>> Permiso de lectura (read) -r
Si tienes permiso de lectura de un archivo, puedes ver su contenido.
>> Permiso de escritura (write) -w
Si tienes permiso de escritura de un archivo, puedes modificar el archivo. Puedes agregar, sobrescribir o borrar su contenido
>> Permiso de ejecución (execute) -x
Si el archivo tiene permiso de ejecución, entonces puedes decirle al sistema operativo que lo ejecute como si fuera un programa. Si es un programa llamado « foo » lo podremos ejecutar como cualquier comando.

Usando chmod para cambiar los permisos
chmod change mode) es el comando utilizado para cambiar permisos, se pueden agregar o remover permisos a uno o mas archivos con + (mas) o —(menos)
Si quieres prevenirte de modificar un archivo importante, simplemente quita el permiso de escritura en tu «archivo» con el comando chmod
$chmod -w tuArchivo
si quieres hacer un script ejecutable, escribe
$chmod -rwx archivo
$chmod +rwx archivo
también puedes usar el signo = (igual) para establecer los permisos en una combinación exacta, este comando remueve
Los permisos de escritura y ejecución dejando solo el de lectura
$chmod =r archivos