Tutoriales y Manuales

Recopilación de **Tutoriales y Manuales** ordenados por categorías
Descargas Cursos, Tutoriales y Manuales, Libros PDF

Entradas Mensuales

▼ 2022 (Total: 537)
► julio (Total: 45)
► junio (Total: 67)
► mayo (Total: 90)
► abril (Total: 69)
► marzo (Total: 103)
▼ febrero (Total: 75)
Lapsus$ filtra un torrent con casi 19GB de informa...
Grupo sudamericano Lapsus hackea nVidia y roba 1TB...
El ejército de Ucrania pide a los ciudadanos que t...
Elon Musk activa servicio internet por satélite co...
La restauración de fábrica de Windows 11 deja arc...
Google está modificando por primera vez su página ...
Algunos SSD NVMe pueden perder datos cuando se va ...
Rusia ataca de nuevo con malware destructivo (Herm...
La descarga de una película pirata con malware pro...
Eurolink: 6 mil millones de € de la Unión Europea ...
Alternativas a los sistemas operativos Windows, Ma...
Arrancar en modo seguro en Windows 11
Sistemas vulnerables para practicar legalmente ata...
Linux es más rápido que Apple o Microsoft en corre...
Windows 11 dejará de admitir los cifrados inseguro...
Xenomorph es un nuevo malware para Android capaz d...
Google Drive bloquea por error archivos .DS__Store...
NAS ASUSTOR afectado por ataques del ransomware De...

Ficheros /etc/passwd /etc/shadow y /etc/group en GNU/Linux

viernes, 18 de febrero de 2022 | Publicado por el-brujo

Es un archivo que almacena información esencial que se requiere durante el inicio de sesión en sistemas Gnu/Linux. Dicho de otra manera, ahí se va a almacenar información relativa a las cuentas de usuarios. El archivo guarda texto sin formato, el cual va a proporcionar información útil para cada cuenta de usuario.

El archivo **/etc/passwd** almacena información esencial, que se requiere durante el inicio de sesión en linux. En otras palabras, almacena información de la cuenta del usuario. /etc/passwd es un archivo de texto sin formato. Contiene una lista de las cuentas del sistema, que proporciona información útil para cada cuenta, como ID de usuario, ID de grupo, directorio de inicio, shell y más.

El archivo */etc/passwd* debe tener permiso de lectura general, ya que muchas utilidades lo usan para asignar un ID a los nombres de usuario. **El acceso de escritura a este fichero está limitado a la cuenta de superuser/root**. El archivo es propiedad de root y tiene como permisos 644. Lo que viene a significar que solo puede ser modificado por root o usuarios con privilegios de sudo.

Un rápido vistazo al archivo /etc/passwd

El nombre del archivo se origina en una de sus funciones iniciales. Este contenía los datos utilizados para verificar las contraseñas de las cuentas de los usuarios. Sin embargo, en los sistemas Unix modernos, **la información de la contraseña se suele almacenar en un archivo diferente**, utilizando contraseñas ocultas u otras implementaciones de bases de datos.

Se puede decir que el archivo */etc/passwd* **es una base de datos basada en texto sin formato, la cual contiene información sobre todas las cuentas de usuarios que se encuentran el sistema**. Como decíamos, es propiedad de root, y aun que solo es modificable por root o usuarios con privilegios de sudo, también es legible por los demás usuarios del sistema.

¿Qué es el archivo /etc/passwd?

Una característica a destacar, es que se trata de un archivo simple de texto ASCII. Este **es un archivo de configuración que contiene detalles relativos a las cuentas de usuarios**. Identificar a los usuarios de forma única es esencial y necesario en el momento del inicio de sesión, y ahí es justo dónde los sistemas Gnu/Linux utilizan */etc/passwd*.

> **/etc/passwd** Información de configuración sobre las cuentas de usuario del sistema.
> **/etc/shadow** Contraseñas de las cuentas de usuario
> **/etc/group** Información sobre los grupos del sistema.

En este archivo de texto sin formato **encontraremos una lista de las cuentas del sistema, guardando de cada cuenta información útil como ID de usuario, ID de grupo, directorio de inicio, shell y más**. Además, este debe tener permiso de lectura general, pues muchas utilidades de comandos lo utilizan para asignar un ID de usuario a los nombres de usuario.

Aun que es posible agregar y administrar usuarios directamente en este archivo, no es recomendable hacerlo, ya que esta acción puede añadir errores, lo cual sería un problema. En lugar de hacerlo así, lo suyo es utilizar los comandos disponibles para la administración de usuarios.

¿Cuál es el uso de este archivo?

Existen varios esquemas de autenticación diferentes que se pueden usar en sistemas Gnu/Linux. **El esquema estándar más utilizado es realizar la autenticación en los archivos */etc/passwd* y */etc/shadow***. En el archivo */etc/passwd* se almacena la lista de usuarios del sistema junto con información importante sobre estos. Gracias a este archivo el sistema puede identificar a los usuarios de forma única, pues esto es esencial y necesario en el momento de iniciar la sesión correspondiente de forma correcta.

El contenido del fichero */etc/passwd* determina quien puede acceder al sistema de manera legitima y que puede hacer una vez dentro. Es por esto que este archivo quizás pueda ser considerado como la primera linea de defensa del sistema para evitar los accesos no deseados. Por este motivo, es importante mantenerlo libre de errores y fallos.

Formato del archivo /etc /passwd

En el contenido de este archivo, nos vamos a encontrar el nombre de usuario, el nombre real, la información de identificación y la información básica de la cuenta de cada usuario. Como decíamos, **este es un archivo de texto con una entrada por línea, y cada una de estas líneas representa una cuenta de usuario**.

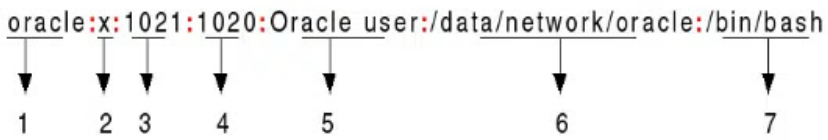
Para **ver su contenido**, los usuarios podemos utilizar un editor de texto o un comando como el siguiente:

```
cat /etc/passwd
```

- Instalar un firmware no oficial en un router neutro
- Vulnerabilidad de validación de entrada datos numé...
- Unredacter es una herramienta gratuita para recupe...
- Deja sin Internet a todo un barrio para evitar que...
- Aceptar Cookies automáticamente y evitar mensajes ...
- EE.UU. dice que Rusos atacaron contratistas americ...
- Introducción al Sandbox de Privacidad de Android
- Ficheros /etc/passwd /etc/shadow y /etc/group en G...
- Google presenta Chrome OS Flex, un nuevo sistema o...
- Envían 1TB en 1 segundo a 1 kilómetro de distancia...
- ¿Qué es el SIM Swapping? Así pueden hackear tus cu...
- El 74% del dinero robado en ataques de ransomware ...
- Actualizaciones de seguridad importantes de Apple ...
- Cibertataques en Ucrania: Agencias militares y ban...
- pfSense distro basada en FreeBSD monitoriza y admi...
- Nueva versión distro Hacking: Kali Linux 2022.1
- Administrar y crear servicios con systemd en Linux
- Un bug de Zoom para MacOS Monterey dejaba encendid...
- Android 13 permite ejecutar Windows 10, 11 y distr...
- Windows añade protecciones para evitar la extracci...
- Telefónica, Vodafone y Orange dicen que las empres...
- Detenidos en Madrid por fraude zapatillas falsific...
- Intel estrena con el kernel 5.18 funciones de pago...
- Google paga 8.7 millones de dólares en recompensas...
- AMD rompe su récord de cuota de mercado como fabri...
- Empiezan a vender "Air Tags" silenciados para espi...
- Mejora la temperatura de tu SSD con un disipador d...
- Malware Qbot necesita sólo 30 minutos para robar d...
- La Policía Nacional desarticula una organización c...
- SpaceX pierde 40 de los 49 nuevos satélites instal...
- Plugins y addons (scripts) para el firmware router...
- EE. UU. incauta 3.600 millones de dólares robados ...

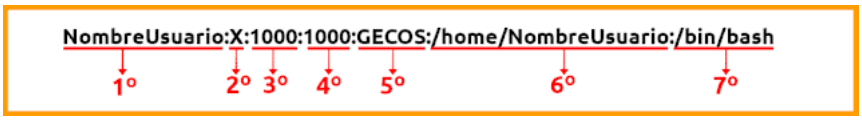
Cada línea del archivo *`/etc/passwd`* va a contener siete campos separados por puntos (:). Normalmente, la primera línea describen al usuario root, seguido del sistema y las cuentas de usuario normales. Las nuevas entradas se van añadiendo al final.

/etc/passwd contiene una entrada por línea para cada usuario (cuenta de usuario) del sistema. Todos los campos están separados por un (:). Total de siete campos de la siguiente manera. En general, la entrada del archivo /etc/passwd tiene el siguiente aspecto:



Valores del archivo /etc/passwd

A continuación vamos a ver qué significa cada uno de los valores que nos vamos a encontrar en cada una de las líneas del fichero */etc/passwd*:



1. **Nombre de usuario**→ Este **s**e utiliza cuando el usuario inicia sesión. Debe tener entre 1 y 32 caracteres de longitud.
2. **Contraseña**→ El carácter x nos va a indicar que la contraseña cifrada se almacena en el archivo */etc/shadow*.
3. **ID de usuario (*UID*)**→ A cada usuario se le asigna un ID de usuario (*UID*) unívoco en el sistema. El UID 0 está reservado para root y los UID 1-99 están reservados para otras cuentas predefinidas. El sistema va a reservar otros UID del 100 al 999 para cuentas/grupos administrativos y del sistema.
4. **ID de grupo (*GID*)**→ Este es el ID del grupo principal al que pertenece el usuario (*almacenado en el archivo /etc/group*).
5. **Información del de usuario (*GECOS*)**→ Aquí encontraremos el campo de comentario. En este se permite añadir información adicional sobre los usuarios, como son el nombre completo, el número de teléfono, etc.
6. **Directorio de inicio**→ Aquí nos encontraremos con la ruta absoluta al directorio "home" del usuario. Si este directorio no existe, el directorio de usuarios se convierte en /.
7. **Shell**→ Esta es la ruta absoluta del shell (*/bin/bash*). Aun que podría no ser un shell como tal. Si el shell se establece en */sbin/nologin* y el usuario intenta iniciar sesión en el sistema Gnu/Linux directamente, el shell */sbin/nologin* va a cerrar la conexión.

Como hemos dicho líneas más arriba, a excepción de la contraseña, **con cualquier editor de textos como «vim» o «gedit» y privilegios de «root» podremos cambiar el comportamiento y configuración de todos los usuarios almacenados en «/etc/passwd»**. Aunque también es necesario insistir en que, modificar este archivo no se debe hacer salvo un caso excepcional (*y sabiendo lo que se hace*), pues si se corrompe o borramos algo en un despiste, nos podemos encontrarnos ante una catástrofe, pues en este archivo se encuentra la raíz básica de todos los permisos que usamos y usaremos en el sistema.

A. Permiso del archivo /etc/passwd

Porque `/etc/passwd` El archivo es muy importante para los sistemas Linux, su permiso predeterminado es `644` para evitar modificaciones erróneas, de modo que cualquier usuario solo pueda leer el archivo y solo el usuario root pueda editarlo. Puede el permiso de la siguiente manera

```
# ls -l /etc/passwd

-rw-r--r-- 1 root root 1501 May 11 16:58 /etc/passwd
```

B. Cómo funciona el comando passwd

Es posible cambiar su propia contraseña o la contraseña asignada a un usuario con `/usr/bin/passwd` mando. Puede obtener el permiso de este comando a continuación:

```
ls -l /usr/bin/passwd

-rwsr-xr-x. 1 root root 27832 Jun 10 2014 /usr/bin/passwd
```

Puede ver que el usuario y el propietario del grupo son root con permisos de lectura y ejecución también para los demás usuarios. Aunque es propiedad de root, puede ver el **Bit SETUID** representado por el `s` permiso que permite a los usuarios ejecutar un programa como si fueran el usuario propietario del programa (root en nuestro caso). Es por eso que puede usar este comando para cambiar su contraseña incluso si no es un usuario root.

Para cambiar su propia contraseña, simplemente ingrese el comando passwd sin opción

```
$ passwd

Changing password for user papso.

Changing password for papso.

(current) UNIX password:

New password:
```

- Microsoft deshabilita temporalmente los instalador...
- Multadas con casi 6 millones de € varias operadora...
- Ciberataque a Vodafone Portugal deja sin servicio ...
- NVIDIA abandona finalmente de forma oficial sus pl...
- La UE invertirá 43.000 millones de euros para dupl...
- Google afirma que la verificación en 2 pasos ha co...
- Microsoft deshabilitará por defecto las macros en ...
- Países Bajos multa a Apple con 5 millones € por la...
- El nuevo super yate de Jeff Bezos es tan grande qu...
- Una filtración de datos expone las identificacione...
- Meta amenaza con cerrar Facebook e Instagram en Eu...
- Microsoft detectó 35.700 millones de intentos de a...
- The Wall Street Journal hackeado por China
- Facebook pierde usuarios por primera vez en su his...
- El nuevo estándar WiFi 802.11bf permitirá detectar...
- Mozilla refuerza la privacidad Firefox combinando ...
- Monitorizar el rendimiento de contenedores Docker ...
- Raspberry Pi OS ya está disponible en 64 bits de f...
- VLC denuncia que hay personas domiciliando sus rec...
- Estándar Encrypted Client Hello (ECH) permitirá me...
- Roban 320 millones dólares de Ethereum a la plataf...
- Comando Robocopy: herramienta copia de seguridad d...
- Publicado exploit para nueva vulnerabilidad local ...
- Microsoft explica el motivo porque algunos usuario...
- La huella digital de tu GPU también sirve para ras...

► enero (Total: 88)
► 2021 (Total: 730)
► 2020 (Total: 212)
► 2019 (Total: 102)
► 2018 (Total: 150)
► 2017 (Total: 231)
► 2016 (Total: 266)
► 2015 (Total: 445)
► 2014 (Total: 185)
► 2013 (Total: 100)
► 2012 (Total: 8)
► 2011 (Total: 7)
► 2010 (Total: 15)

Síguenos en:

Ten en cuenta que, si puede cambiar su propia contraseña sin privilegios de root, no puede cambiar la contraseña de un usuario sin ella.

```
$ passwd patrick

passwd: Only root can specify a user name.
```

Contraseñas se almacenan en el archivo /etc/shadow

Las contraseñas cifradas no se almacenan en el archivo /etc/passwd. Se almacena en el archivo /etc/shadow. En los viejos tiempos no había un gran problema con este permiso de lectura general. Todos podían leer las contraseñas cifradas, pero el hardware era demasiado lento para descifrar una contraseña bien elegida y, además, la suposición básica solía ser la de una comunidad de usuarios amigable.

Casi todos los sistemas operativos modernos de línea Linux/UNIX utilizan algún tipo de conjunto de contraseñas ocultas, donde /etc/passwd tiene asteriscos (*) en lugar de contraseñas cifradas, y las contraseñas cifradas están en /etc/shadow, que el superusuario puede leer solamente.

Fichero /etc/shadow

El fichero /etc/shadow almacena las contraseñas de las cuentas de usuario. Se utiliza este fichero por seguridad. `/etc/shadow` es un archivo de texto que contiene información sobre las contraseñas de los usuarios del sistema. Es propiedad del usuario root y del grupo oculto y tiene 640 permisos.

Esto es debido a que es necesario que cualquier usuario pueda leer información de cuentas de usuario, que se almaenan en /etc/passwd. Si las contraseñas se almacenaran en el fichero /etc/passwd, cualquier usuario del sistema tendría acceso a las contraseñas (cifradas).

La solución, guardar las contraseñas en un fichero al que solo puede acceder el usuario root.

```
javier@smr01Profesor:~$ cat /etc/shadow
cat: /etc/shadow: Permiso denegado
javier@smr01Profesor:~$ sudo cat /etc/shadow
```

...

```
pepito:$1$GeYcB$uo.yrKAWYXffHcQqkn.a1.:14715:0:99999:7:::
pepita:$1$b9lwK1t0$7CguRqM2yin72JKKRC/n70:14715:0:99999:7:::
maria:$1$Rxr4IClP$ruhdnFzF40gDLtTPZFe5F.:14718:0:99999:7:::
ramon:$1$on5bv0Gu$qWLrJ7Fp8Y/Umazwe8Ifo/:14718:0:99999:7:::
```

Si queremos obtener información sobre lo que almacena /etc/shadow, consultamos su página de manual.

Contraseñas Cifradas

Contraseña: Es su contraseña cifrada. La contraseña debe tener un mínimo de 8 a 12 caracteres, incluidos caracteres especiales, dígitos, minúsculas alfabéticas y más. Por lo general, el formato de la contraseña se establece en idsalt$hashed. El $id es el algoritmo utilizado en GNU/Linux de la siguiente manera:

1 – MD5
$2a$ – Blowfish
$2y$ – Eksblowfish
5 – SHA-256
6 – SHA-512

1: MD5
2a: Blowfish
2y: Eksblowfish
5: SHA-256
6: SHA-512

El formato básico del fichero es el siguiente:

Nombre de usuario	(Obligatorio) Identifica al usuario para el que se almacena la contraseña.
Contraseña cifrada	Contraseña cifrada del usuario.
Información de edad	El resto de campos almacena información para gestionar la caducidad de las contraseñas.

Fichero /etc/group

Se trata del fichero donde se guarda información de los grupos a los que pertecen los usuarios del sistema. En cada línea se almacena información de un grupo. Los campos son los siguientes:

Nombre grupo	identifica al grupo.
Contraseña	No se suele utilizar.
GID	Identificador numérico del grupo
Lista de miembros	Nombres de usuarios separados por coma que pertenecen al grupo.

Comandos comunes que usan archivos /etc/passwd

Aquí hay una lista de comandos:

passwd command
su command
sulogin command
getent command
login command
pwck command
pwunconv command
chpasswd command
chsh command
chfn command
useradd command
userdel command

Suponemos que se ha creado, pero podemos comprobarlo de varias formas. La más directa sería con el comando **id** seguido del nombre del usuario recién creado.

```
id
```

```
alumno@jpedrerom:~$ id alfonsomg
uid=1003(alfonsomg) gid=1004(alfonsomg) grupos=1004(alfonsomg)
```

Fuentes:
https://ubunlog.com/etc-passwd/
https://www.linuxenespañol.com/ayuda/etc-passwd-descripcion-de-funcionamiento-y-formato/

Entradas relacionadas:

Programas gratuitos para hacer copias de seguridad en Windows

Herramientas Recuperación y Copia de Seguridad de Windows 10

Comparativa de Google: Usuarios expertos en seguridad Vs Usuarios normales y corrient...

Datos personales de clientes de Movistar y O2 expuestos en un acceso a sus sistemas

La gran mayoría de los usuarios ignora las alertas de seguridad en Internet

El CCN-CERT actualiza la guía para defenderse del ransomware

Etiquetas: ETC , gnu/linux , group , grupo , id , passwd , shadow , user , users , usuarios

0 comentarios :

PUBLICAR UN COMENTARIO

Los comentarios pueden ser revisados en cualquier momento por los moderadores.

Serán publicados aquellos que cumplan las siguientes condiciones:
- Comentario acorde al contenido del post.
- Prohibido mensajes de tipo SPAM.
- Evite incluir links innecesarios en su comentario.
- Contenidos ofensivos, amenazas e insultos no serán permitidos.

Debe saber que los comentarios de los lectores no reflejan necesariamente la opinión del STAFF.

Escribe tu comentario

Entrada más reciente Inicio Entrada antigua