-

UD 08.
LINUX: PROTECCIÓN DE RECURSOS

Sistemas Informáticos
DAW CFGS

Borja Salom

b.salomsantamaria@edu.gva.es 2022/2023

Versión:221211.2018

nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos simbolos son:

ÿ Importante

ÿ Atencion

ÿ Interesantes

ÍNDICE DE CONTENIDO

UD08. LINUX: PROTECCIÓN DE RECURSOS

1. USUARIOS

El concepto de usuario en Linux permite entornos de ejecución separados para diferentes propósitos. Dos personas pueden trabajar simultáneamente en el mismo sistema, cada una con un usuario diferente y un directorio de inicio diferente.

También es muy común que muchos servicios internos del sistema tengan su propio usuario para restringir el acceso a ese servicio como mecanismo de seguridad. De esta forma, si un servicio ve comprometida su seguridad por un ataque, el acceso que tenga el usuario de ese servicio servirá de contención del ataque, y no podrá acceder a archivos pertenecientes a otro usuario (persona o servicio). .

> **Daemon** es el término utilizado en Linux para referirse a un proceso de servicio que se ejecuta en segundo plano de forma no interactiva. Por lo general terminan con la letra d, como **httpd** o **ftpd.**

La configuración de usuario en Linux se maneja esencialmente en los siguientes dos archivos.

1.3 Archivo /etc/passwd

Este archivo contiene información sobre las cuentas de usuario y sus características.

Esta es la sintaxis utilizada en cada línea:

- nombre:contraseña:UID:GID:GECOS:directorio:shell

Puedes ver el significado de cada campo con man passwd:

- **nombre:** nombre de usuario
- **contraseña:** La contraseña del usuario en texto sin formato, o un asterisco * o x si encriptado.
- **UID:** Número único de identificación del usuario. Los usuarios pueden cambiar muchos parámetros, incluido su nombre, pero nunca se debe cambiar el UID.
  El UID de Root es 0. Las cuentas de servicio y daemon tienen los números más bajos, mientras que las cuentas de usuario final comienzan en el valor definido en UID_MIN en el archivo /etc/login.defs . • **GID:** Número identificador único de grupo. Varios usuarios pueden tener un mismo grupo, aunque al crear un usuario se crea por defecto un grupo con el mismo nombre salvo que se indique lo contrario. Los datos del grupo aparecen en /etc/group.
- **GECOS:** Campo de comentario que incluye información extra sobre el usuario (nombre real, dirección…) Informalmente se llama información dactilar.
- **Directorio:** directorio de inicio del usuario. Los usuarios finales normalmente se encuentran en

/hogar.

- **Shell:** El shell que el usuario usa por defecto (en muchos casos es /bin/bash). Si el usuario tiene /sbin/nologin o /usr/bin/false, significa que no tiene permiso para iniciar sesión en el sistema, lo cual es común en los demonios como medida de seguridad.

Un ejemplo:

```
root:x:0:0:root:/root:/bin/bash
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usuario:x:1000:1000:usuario,,,:/home/usuario:/bin/bash
```

1.4 Archivo /etc/sombra

Contiene información sobre las contraseñas de los usuarios en /etc/passwd, que almacena de forma cifrada.

- **Nombre:** nombre de usuario
- **contraseña:** Contraseña encriptada. La función hash utilizada para cifrar el La contraseña se indica al principio. • **Lastmod:**

Tiempo transcurrido desde el último cambio de clave. • **Min:** Número

mínimo de días hasta que se pueda volver a cambiar la contraseña. • **Max:** Número máximo de días

hasta que el sistema obliga al usuario a cambiar la contraseña.

- **Advertencia:** Número de días previos al Max en los que se notifica al usuario su cambio obligatorio de contraseña.
- **Inactividad:** número de días entre el vencimiento de la contraseña y la cuenta Bloqueo.
- **Caducidad:** fecha en que se deshabilita la cuenta. Si se deja en blanco, la cuenta nunca caduca
- **Reservado:** Campo reservado para usos futuros.

Sobre el campo de contraseña:

- * se utiliza cuando la cuenta nunca ha tenido una contraseña.
- ! significa que la cuenta ha sido deshabilitada para iniciar sesión con contraseña.

Cuando una cuenta está bloqueada (lock: usermod -l user), la contraseña del usuario no se elimina, ¡pero se agrega un signo de exclamación ! al comienzo del hash de la contraseña para indicar que se ha bloqueado. Desbloquear el usuario (unlock: usermod -u user) elimina el signo de exclamación, dejando el hash como estaba antes.

1.5 Comandos de gestión de usuarios

Shadow Tool Suite es una colección de comandos que le permiten administrar usuarios sin tener que manipular directamente los archivos /etc/passwd y /etc/shadow , lo cual no es recomendable dada la posibilidad de dejar inconsistencias en archivos tan delicados. Algunos de los comandos:

- useradd : crea un usuario.
- userdel : elimina un usuario.
- usermod : realice modificaciones a los datos en /etc/passwd. Tienes una opción para cada uno de los campos, excepto el campo GECOS. Incluye opciones para (des)bloquear un usuario (--lock y --unlock).
- chfn – modifica la información del dedo (GECOS).
- chsh : modifica la shell.
- id : imprime información sobre el usuario y sus grupos. ÿ id -u : imprime el UID

  ÿ id -un: imprime el nombre de usuario
- cambiar: cambiar la edad muestra y modifica todas las fechas de contraseña en /etc/sombra.

También existen los comandos adduser y deluser que son más fáciles de usar y ahorran algo de trabajo, por lo que se usan con más frecuencia en la práctica.

> Utilice el manual de man o las opciones -h o --help para ver todas las opciones que ofrecen estos comandos, ya que pueden variar según las distribuciones.

Para establecer y cambiar una contraseña:

- usermod -p PASSWORD USER guarda la contraseña especificada sin cifrarla (habría que pasarle un hash de la contraseña). No debe usar esta opción.
- passwd USER es el comando utilizado, que le permite ingresar una contraseña de forma segura

Con el comando finger podemos obtener información del GECOS de cualquier usuario:

```
$ finger theuser
Login: theuser                          Name: Juan Pérez
Directory: /home/theuser                Shell: /bin/bash
Office: 101, +34 123 456                Home Phone: +34 983 12 34 56
On since Wed Feb 04 10:26 (EST) on pts/1   3 seconds idle
     (messages off)
No mail.
No Plan.
```

2. GRUPOS

Los grupos le permiten otorgar permisos a un conjunto de usuarios simultáneamente.

En Linux un usuario tiene los siguientes grupos: • **Grupo**

primario: es el que aparece como su GID en /etc/passwd. Sólo puede haber un grupo primario.

• **Grupos secundarios o complementarios:** son los que se gestionan en el fichero /etc/groups, donde se puede añadir un usuario a más grupos.

Además, durante la sesión de usuario se puede cambiar temporalmente el grupo al que pertenece el usuario:

• **Grupo real:** este es su grupo principal que está en /etc/passwd. El grupo al que pertenece un usuario cuando inicia sesión.

• **Grupo efectivo:** mediante el comando newgrp puede cambiar el grupo principal al que pertenece el usuario, y la configuración es efectiva hasta que cierre la sesión o cambie de grupo efectivo nuevamente.

2.3 Archivo /etc/grupo

Este archivo contiene información sobre los grupos del sistema. Su estructura es similar a la de los archivos passwd y shadow , con los siguientes campos:

• **grupo:** nombre del grupo

• **contraseña:** Contraseña que permite a un usuario cambiar de grupo. Si está vacío, no requiere contraseña y una x significa que está administrado por el archivo /etc/gshadow.

• **GID:** Identificador único (numérico) del grupo. • **Miembros:** lista

separada por comas de los nombres de usuario que pertenecen a ese grupo.

De manera similar al archivo /etc/shadow , existe el archivo /etc/gshadow , que almacena las contraseñas de grupo cifradas con un hash y también funciona con el asterisco * y la exclamación . Símbolos.

2.4 Comandos de gestión de grupos

La suite Shadow también incluye los comandos:

• groupadd : agregar un nuevo grupo

• groupdel : eliminar un grupo

• groupmod – Modifica la información en /etc/groups • gpasswd –

Modifica la contraseña del grupo, reflejada en /etc/gshadow

2.5 Modificar grupos de usuarios

Una vez que tenemos un grupo creado, podemos agregarlo como principal o secundario a un usuario mediante el comando usermod, con las siguientes opciones:

```
$ usermod --help
Usage: usermod [options] LOGIN

Options:
  ...
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GRO
UPS
                                mentioned by the -G option without remo
ving
                                him/her from other groups
```

Por lo tanto:

- usermod -g GROUP USER: modificar grupo primario •

usermod -G GROUP USER: reemplazar grupo secundario

- usermod -a -G GRUPO DE USUARIO: Agregar un grupo secundario al usuario

3. PERMISOS SOBRE ARCHIVOS Y DIRECTORIOS

En Linux, cada archivo y directorio tiene permisos para:

- **Usuario:** el sistema de archivos almacena un usuario propietario (UID), junto con los permisos asociados al mismo.
- **Grupo:** también se guarda un GID propietario, con permisos •

Otro: También tiene permisos para los usuarios que no tienen ese UID o GID.

El comando ls -l enumera los archivos y directorios, incluida la información sobre sus permisos, de la siguiente manera:

```
$ ls -l
drwxr-xr-x 6 usuario grupo  4096 Jan  5 17:37 directory
-rw-r--r-- 1 usuario grupo  2048 Jul  6 12:56 file
```

El primer campo indica en la primera letra si es un archivo normal (-), directorio (d) o enlace (l). Después de eso, aparecen los permisos, organizados en escritura, lectura y ejecución para el usuario, grupo y otros.

El permiso de ejecución x en los directorios significa que puede acceder dentro del directorio y enumerar su contenido.

3.3 Modificaciones de permisos

Los permisos de un archivo o directorio se pueden cambiar con el comando: chmod **Modo relativo.** Puedes tratar uno de los campos de forma aislada sin tocar el resto de permisos: Se indica primero a quién se le va a cambiar el permiso (puedes poner varios):

- ÿ tu: usuario
  - ÿ g: grupo
  - ÿ o: otros
  - ÿ a: todo, equivalente a ugo (también se puede dejar en blanco)
- Tipo de operación:
  - ÿ +: agregar permisos
  - ÿ -: eliminar permisos
- Permisos:
  - ÿ r: lectura
  - ÿ w: escribir
  - ÿ x: ejecución

Ejemplos:

- archivo chmod u+x
- archivo chmod go-x
- archivo chmod +x

Modo absoluto. La información completa del permiso se puede reemplazar usando un número de base 8 (octal) de tres dígitos. Los permisos coinciden con los del número en binario.
Lo bueno de trabajar en octal es que cada carácter se puede trabajar de forma independiente.

Ejemplo de permiso 754:

- 7 en binario es 111 ÿ permisos de usuario: rwx
- 5 en binario es 101 ÿ permisos de grupo: rx
- 4 en binario es 100 ÿ permisos de otros: r--

```
$ chmod 754 file
$ ls -l file
-rwxr-xr-- 1 usuario grupo  2048 Jan  6 13:03 file
```

3.4 Mascarilla

La máscara del sistema operativo define los permisos que se asignan de manera predeterminada a los archivos y directorios en el momento en que se crean.

El comando umask sin parámetros imprime el valor que tiene actualmente y se puede manejar en modo simbólico y modo octal:

```
$ umask
0022
$ umask -S
u=rwx,g=rx,o=rx
```

Si se pasa un parámetro al comando, se establece la nueva máscara.

Modo simbólico: Le permite establecer permisos usando las letras u (usuario), g (grupo), o (otro) y a (todos). Se puede hacer en modo relativo usando los símbolos + y -, o en modo absoluto con =, y combinaciones de ambos.

```
$ # Modo relativo
$ umask g-w
$ umask a+x
$ # Modo relatuvo (u,o) y modo absoluto (g)
$ umask u-w,g=r,o+r
```

Modo octal: Permite configurar los permisos de forma numérica, siempre en modo absoluto.

El modo octal se utiliza en función de los permisos máximos, que para directorios es 777 y para archivos 666 (sin ejecución). Los bits de máscara establecidos en 1 deshabilitarán ese permiso al máximo de permisos. Ej: umask = 023

```
Umask      023: 000010011
Directorio 777: 111111111 -> 111101100 = rwxr-xr--
Archivo    666: 110110110 -> 110100100 = rw-r--r--
```

Muchos sistemas tienen la máscara 022, que se configura con: unmak 022

3.5 Cambio de propietario y grupo

Estos dos atributos se pueden modificar con los comandos:

- chown file new_owner: Modifica el propietario (UID asociado).
- archivo chgrp new_group: modifica el grupo (GID asociado).

Con ambos puedes usar la opción -R sobre directorios, para que realice la operación de forma recursiva, es decir, la aplica a todo lo que contiene directamente o en subdirectorios, sub-subdirectorios, etc.