IES Gonzalo Nazareno

- ***Creación de usuario y aplicación de política de seguridad.-***

-IMPLANTACION DE SISTEMAS OPERATIVOS-

1/3/2022 ***Jose Antonio Canalo Gonzalez***

Indice

INTRODUCCION

Creación de usuario y aplicación de política de seguridad.

1) Crea dos usuarios de nombre externo1 y externo2, que tengan el UID 1200 y UID 1201 respectivamente, tengan como comentario Becarios. Además tendrán como shell /bin/bash, y sus propios directorios personales. Ambos deben pertenecer al grupo externos de GID 1300.
2) Cuando el usuario intenta acceder al sistema, ¿qué es lo que ocurre?, indica los procedimientos que seguirías como administrador para investigar y solventar el problema.
3) Añade un grupo con el nombre itinerantes con GID 1400.
4) Añade a externo1 en el grupo itinerantes editando el fichero /etc/group.
5) Modifica la información de cambio de contraseña de externo1. No se puede cambiar la contraseña antes de 10 días, y es obligatorio cambiar la contraseña cada 30 días. Indica las diferentes métodos que puedes emplear.
6) ¿Qué realizan los comandos pwck y grpck? . ¿Para que lo emplearías?.
7) Crea las carpetas externos e itinerantes. Dichas carpetas pertenecerán a root, y al grupo de su nombre. En las carpetas externos e itinerantes, todos los miembros pertenecientes a un grupo, podrán acceder y escribir en su carpeta, es decir grupo externos en carpeta externos, todo objeto creado por un usuario debe pertenecer al grupo. Crea la carpeta publica, en ellas podrán acceder y escribir todo usuario del sistema pero no podrán borrar objetos que no les pertenezcan.
8) Pon una contraseña al grupo itinerantes. La contraseña será: itinerantes.
9) Cómo podría acceder el usuario externo2 a la carpeta de itinerantes?.

10) Analiza las funciones que realizan los ficheros en conexiones **no ssh**:
    /etc/issue
    /etc/issue.net
    /etc/motd
    Pon ejemplos de aplicación.

11) Avisa a los usuarios de que se parará el sistema el 19 de febrero a las 15:00 por mantenimiento. Comenta el procedimiento que has seguido.
12) ¿Cómo configurarías mensaje personalizados de inicio para un usuario concreto?.
13) En el supuesto de acceder a la terminal vía **ssh**, ¿cómo lo configurarías?. Modificación de `/etc/ssh/sshd_config`

EJERCICIO 1Crea dos usuarios de nombre externo1 y externo2, que tengan el UID 1200 y UID 1201 respectivamente, tengan como comentario Becarios. Además tendrán como shell /bin/bash, y sus propios directorios personales. Ambos deben pertenecer al grupo externos de GID 1300.

Creamos el grupo necesario con groudpadd y luego creamos los usuarios necesarios y lo agregamos con useradd

```
jose@debian:~$ su -
Contraseña:
root@debian:~# groudpadd -g 1300 externo
-bash: groudpadd: orden no encontrada
root@debian:~# groupadd -g 1300 externo
root@debian:~# useradd externo1 -u 1200 -g 1300 -m -s /bin/bash
root@debian:~# useradd externo1 -u 1201 -g 1300 -m -s /bin/bash
useradd: el usuario «externo1» ya existe
root@debian:~# useradd externo2 -u 1201 -g 1300 -m -s /bin/bash
root@debian:~#
```

EJERCICIO 2 Cuando el usuario intenta acceder al sistema, ¿qué es lo que ocurre?, indica los procedimientos que seguirías como administrador para investigar y solventar el problema.

Pues no podriamos entrar porque los usuarios no tienen contraseña entoces deberiamos de cambiarla con el comando passwd, gracias a esto podriamos usar dichos usuarios.

EJERCICIO 3 Añade un grupo con el nombre itinerantes con GID 1400.

Usamos comando groupadd -g 1400 Itinerantes

```
root@debian:~# groupadd -g 1400 Itinerantes
root@debian:~# less /etc/group
root@debian:~#
```

EJERCICIO 4 Añade a externo1 en el grupo itinerantes editando el fichero /etc/group.

Con la ayuda de nano abrimos el repositorio /etc/group, y añadimos el usuario Externo1.

```
systemd-coredump:x:999:
externo:x:1300:
Itinerantes:x:1400:externo1:
```

EJERCICIO 5 Modifica la información de cambio de contraseña de externo1. No se puede cambiar la contraseña antes de 10 días, y es obligatorio cambiar la contraseña cada 30 días. Indica las diferentes métodos que puedes emplear.

Para la configuración de este ejercicio usaremos el comando llamado chage. Lo usaremos con unas funciones determinadas para su configuración.
El comando en cuestión es chage Externo1 -m 10 -M 30 donde -m(es para asignar los dias minimos entre cambios de contraseña) y -M(es para asignar los dias máximos de cambios de contraseña).
Tras ese comando podremos ver que al realizar el comando con -l nos aparecera la información referente a la cue ta indicada que en este caso es Externo 1.

```
root@debian:~# passwd -S externo1
externo1 L 03/01/2022 0 99999 7 -1
root@debian:~# passwd -n10 -x 30 externo1
passwd: información de caducidad de la contraseña cambiada.
root@debian:~# passwd -S externo1
externo1 L 03/01/2022 10 30 7 -1
root@debian:~#
```

EJERCICIO 6 Qué realizan los comandos pwck y grpck? . ¿Para que lo emplearías?.

A veces creamos, borramos o modificamos usuarios de forma manual, tocando los archivos ***/etc/passwd y /etc/shadow***. Ésto, a veces, genera problemas de sincronización entre ambos archivos.
Para comprobar si tenemos problemas en éstos archivos no tenemos más que ejecutar el comando pwck sin parámetros.

pwck chequeará dichos archivos y nos informará si hay problemas en ellos. Por supuesto, nos dará algún warning, informándonos de que hay cuentas sin directorio home, como por ejemplo, las de sistema (que no deben tenerlo).
Una vez comprobados los problemas, ya podremos solucionarlos.
Una opción interesante de pwck, para cuando tenemos ambos archivos un poco desordenados es -s. Si ejecutamos:
pwck -s
Nos ordenarla las entradas de ambos archivos por uid.
Otro comando muy útil cuando tenemos problemas con los archivos de usuarios es pwconv.
grpck
verifica la integridad de la información de autenticación del sistema.
El ***grpck*** verifica la integridad de la información de grupos.
Comprueba que todas las entradas del archivo /etc/group y /etc/gshadow tienen el formato adecuado y contiene datos válidos.
Tendremos que eliminar las entradas que estén mal formateadas o tienen errores.
Se realizan comprobaciones para verificar que cada entrada tiene:
· El número correcto de campos
· Un nombre de grupo único y válido
· Un identificador de grupo válido (/etc/group solamente)
· Una lista válida de los usuarios y administradores
· Una entrada correspondiente en el archivo /etc/gshadow (respectivamente /etc/group para los controles gshadow)

EJERCICIO 7 Crea las carpetas externos e itinerantes. Dichas carpetas pertenecerán a root, y al grupo de su nombre. En las carpetas externos e itinerantes, todos los miembros pertenecientes a un grupo, podrán acceder y escribir en su carpeta, es decir grupo externos en carpeta externos, todo objeto creado por un usuario debe pertenecer al grupo. Crea la carpeta publica, en ellas podrán acceder y escribir todo usuario del sistema pero no podrán borrar objetos que no les pertenezcan.

Para este ejercicio utilizaremos a los comandos ***mkdir, chown, chmod*** y al concepto conocido como sticky bit:
Con ls -ld podemos ver como todos los permisos y grupos se han aplicado correctamente a las carpetas correspondientes.

```
root@debian:~# mkdir /{Externos,Itinerantes,Publica}
```

```
root@debian:~# chown :externo /Externos/
root@debian:~# chown :Itinerantes /Itinerantes/
root@debian:~# chmod 1774 /Externos/
root@debian:~# chmod 1774 /Itinerantes/
root@debian:~# chmod g+s /{Externos,Itinerantes}
root@debian:~# chmod 1777 /Publica/
root@debian:~#
```

```
root@debian:~# ls -ld /{Externos,Itinerantes,Publica}
drwxrwsr-T 2 root externo     4096 mar  1 19:24 /Externos
drwxrwsr-T 2 root Itinerantes 4096 mar  1 19:24 /Itinerantes
drwxrwxrwt 2 root root        4096 mar  1 19:24 /Publica
root@debian:~#
```

EJERCICIO 8 Pon una contraseña al grupo itinerantes. La contraseña será: itinerantes.

Ahora deberemos poner la contraseña al un grupo y esto se realiza con el comando

gpasswd:

```
root@debian:~# gpasswd Itinerantes
Cambiando la contraseña para el grupo Itinerantes
Nueva contraseña:
Vuelva a introducir la nueva contraseña:
root@debian:~#
```

EJERCICIO 9 Cómo podría acceder el usuario externo2 a la carpeta de itinerantes?.

entrarmos en Externo2 debemos hacer que el usuario Externo2
adquiera el grupo Itinerantes y para ello vamos a utilizar el comando newgrp:

```
root@debian:/# passwd externo2
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
root@debian:/# su externo2
externo2@debian:/$
```

```
externo2@debian:/$ newgrp Itinerantes
Contraseña:
externo2@debian:/$ touch /Itinerantes/test.txt
externo2@debian:/$ tree /Itinerantes/test -ugp
```

EJERCICIO 10 Analiza las funciones que realizan los ficheros en conexiones no ssh:

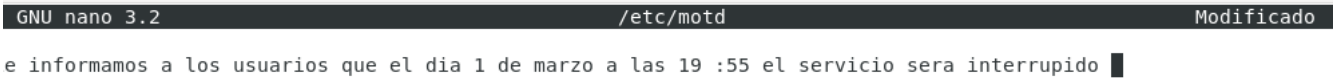
/etc/issue
/etc/issue.net
/etc/motd

Pon ejemplos de aplicación.

El fichero /etc/issue es un fichero de texto plano que también aceptará algunas secuencias de Escape (ver más abajo) para insertar información sobre el sistema. Además existe el fichero issue.net que puede usarse cuando se ingresa en el sistema remotamente. /etc/issue.net se muestra solo en conexiones remotas y /etc/motd se utiliza también para mostrar información pero lo hace después del login, no antes, esta característica hace que en sistemas con interfaz gráfica normalmente el usuario no vea dicho mensaje.

EJERCICIO 11avisa a los usuarios de que se parará el sistema el 19 de febrero a las 15:00 por mantenimiento. Comenta el procedimiento que has seguido.

Para este ejercicio modificaremos el repositorio /etc/motd en el cual pondremos el mensaje



EJERCICIO 12 ¿Cómo configurarías mensaje personalizados de inicio para un usuario concreto?.

Una forma sencilla para un usuario concreto sería configurar un echo en su archivo .bashrc al final de la línea que se encargaria de mostrar el mensaje.

EJERCICIO 13 n el supuesto de acceder a la terminal vía ssh, ¿cómo lo configurarías?. Modificación de `/etc/ssh/sshd_config`

```
root@debian:/# nano etc/ssh/ssh_config
```

Para este ejercicio y para solucionar el problema de que en ssh no mostraría por defecto el mensaje del archivo antes modificado en /etc/motd es editar el archivo /etc/ssh/sshd_config, buscar la linea en la que ponga PrintLastLog, descomentarla y darle el valor “no” en vez de “yes”.
Tras esto ya podriamos ver el mensaje perfectamente.

CONCLUSION

La verdad que fue una practica muy entretenida mas de lo que parece, espero que me pueda valer para el dia de mañana

BIOGRAFÍA O FUENTES UTILIZADAS

https://en.wikipedia.org/wiki/Motd_(Unix)
https://puerto53.com/linux/administracion-de-permisos-en-archivos-y-directorios-de-linux/
https://man7.org/linux/man-pages/man8/pwck.8.html
https://man7.org/linux/man-pages/man8/grpck.8.html
https://es.wikipedia.org/wiki/Identificador_de_grupo