

# Prácticas

## 1. Gestión de los usuarios

Objetivo: crear un usuario y aplicar una política de seguridad.

1. Cree un usuario tom que tenga el UID 1200, el grupo users, el comentario "Cazador de Jerry" y el shell /bin/bash. Por supuesto, cree el usuario con su directorio personal:

```
# useradd -m -u 1200 -g users -c "Cazador de Jerry" tom
```

2. Dé la contraseña "tomcat" a tom. Veamos un truco: puede crear una contraseña sin inserción mediante el comando **passwd** con el parámetro `--stdin`:

```
# echo tomcat | passwd --stdin tom
```

3. Añada un grupo cat con el GID 530:

```
# groupadd -g 530 cat
```

4. Añada a tom en el grupo cat editando el archivo `/etc/group`. Para ello, añada el nombre tom al final de la línea correspondiente.

```
cat:x:530:tom
```

5. Modifique la información de cambio de contraseña de tom con el comando **chage**. No se puede cambiar la contraseña antes de 10 días, y es obligatorio cambiarla cada 50 días.

```
# chage tom
Changing agin information for tom
Minimum Password Age [7] : 10
Maximum Password Age [40] : 50
...
```

6. Suprima al usuario tom. Ejecute luego el comando **pwck**. Rectifique el problema.

```
# userdel tom
# pwck
```

El comando le informa de que el grupo cat contiene un usuario tom que ya no existe. Por lo tanto, debe quitar a tom del grupo cat para conservar la coherencia del sistema.

7. Avise a sus usuarios de que se parará el sistema el 12 de diciembre a las 17:00 por mantenimiento. Puede utilizar el archivo `/etc/issue`, el archivo `/etc/motd` y el archivo `/etc/issue.net` para escribir su texto.

## 2. La impresión

Objetivo: configurar las impresoras e imprimir archivos.

1. Puede elegir entre tres sistemas de impresión: BSD, System V y CUPS. ¿Qué sistema debería utilizar?

CUPS, ya que es compatible con los dos primeros.

2. Conéctese a la interfaz de administración de CUPS mediante un navegador Web: `http://localhost:631`

3. En una de las impresoras configuradas, verifique el estado de las impresiones e imprima una página de prueba.

4. ¿Qué ocurre si intenta imprimir una imagen png así: `lpr archivo.png`?

Funciona perfectamente: el sistema de impresión CUPS dispone de filtros que gestionan la mayoría de los documentos transformándolos en el lenguaje de impresión de la impresora y en particular en PostScript.

5. Anule todas las impresiones en curso:

```
# lprm -
```

### 3. Automatización de tareas

Objetivo: utilizar el crontab.

1. Ejecute el comando **ps -ef** para el usuario root cada 5 minutos y redireccione el resultado en /tmp/ps\_result, sin chafar los antiguos:

```
# crontab -e root
```

Añada la línea siguiente:

```
*/5 * * * * ps -ef >> /tmp/ps_result
```

2. Verifique la lista de las tareas en crontab:

```
# crontab -l
```

3. Espere cinco minutos y verifique el resultado en /tmp.
4. Cron interpreta todos los archivos colocados en **/etc/cron.d** de manera automática. Por lo tanto, resulta inútil modificar el crontab del usuario root si el comando es permanente: añada un archivo **/etc/cron.d/cron\_ps** con la línea anterior dentro.
5. Prohíba al usuario joe utilizar el contrab. Modificar el archivo **/etc/cron.deny** y añada al usuario joe en una nueva línea de este archivo.

## 4. Las trazas del sistema

Objetivo: estudiar las trazas del sistema y la configuración de syslog.

1. Las trazas del inicio del sistema y su principal información son accesibles desde el comando **dmesg**. Aísle la línea que indica los parámetros de boot del núcleo:

```
# dmesg | grep -i command
```

Encontrará esta línea en la configuración de GRUB.

2. El comando **last** devuelve también la fecha de la última parada y el último reinicio del sistema. Recupere la lista de los últimos reboots:

```
# last | grep reboot
```

Aunque esto funcione, lo mejor sigue siendo:

```
# last reboot
```

3. El archivo **/var/log/message** contiene las trazas de los eventos importantes del sistema, incluso los anteriores al boot. Puede haber varios por culpa de logrotate. En el último, ¿cuál es la información relativa a eth0?

```
# dmesg | grep eth0
```

4. Va a colocar todas las trazas correspondientes al núcleo en un archivo llamado kernel.log. Modifique el archivo **/etc/syslog.conf** en consecuencia. Añada la línea:

```
kern.*      /var/log/kernel.log
```

5. Fuerce syslog a reiniciarse y volver a leer su configuración. Si su distribución no propone un método que utilice los servicios, entonces mande la señal SIGHUP al proceso de syslog:

```
# ps -e | grep syslog | awk '{print $1}'  
4577  
# pgrep syslog  
4577  
# kill -HUP 4577
```

## 5. Archivado

Objetivo: aprender a crear y a manejar los archivos de archivos.

1. El comando **gzip** sirve para comprimir un archivo. Sin embargo, su funcionamiento puede sorprender un poco. Cree un archivo de texto ordinario y comprímalo:

```
# gzip fic.txt
```

El archivo resultante es fic.txt.gz. Pero ¿dónde está el archivo de origen? Fue suprimido.

2. Para evitar este problema, tiene una solución: comprimir el archivo y forzar al resultado a pasar por la salida estándar. Redirija la salida a un archivo.

```
# gzip -c fic.txt >fic.txt.gz
```

3. Efectúe una copia de seguridad en un archivo comprimido al formato gzip de su directorio personal. Utilice únicamente el comando **tar** para ello:

```
# tar cvzf home.tgz /home
```

4. Descomprima este archivo en el lugar de su elección, pero esta vez utilizando tar, gzip y una tubería:

```
# gzip -cd home.tgz | tar xvf -
```