

EJERCICIOS TEMA 1

1. ¿Qué son las notificaciones CERT?

a) Notificaciones periódicas relativas a problemas de seguridad

b) Un tipo de ataque contra la seguridad del sistema.

c) Petición de certificado digital que los usuarios del sistema realizan al administrador.

2. El soporte a usuarios es una tarea básica del Administrador de Sistemas:

a) Verdadero

b) Falso

3. ¿Qué aspectos cubre la seguridad informática en una organización?

a) Protección física de las instalaciones que alojan el Sistema Informático

b) Protección software del Sistema Informático

c) Protección física de las instalaciones y protección software del Sistema Informático

4. Obtenga información acerca de SNORT.

SNORT es un sniffer de paquetes y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos (IDS).

5. ¿A qué hace referencia “la catedral y el bazar”?

La catedral y el bazar es un ensayo sobre el software de código abierto, escrito por Eric S. Raymond. En él se analizan dos modelos de producción software: la catedral, que representa el modelo de desarrollo más hermético y vertical (software propietario), y el bazar, que representa los proyectos de software libre que se potencian con el trabajo comunitario a través de Internet con el código abierto.

EJERCICIOS TEMA 3

Ejercicio 1

Suponiendo la siguiente salida:

```
/etc/rc0.d/:
K74bluetooth  README                      S20sendsigs  S31umountnfs.sh
S35networking S60umountroot K80openvpn    S10unattended-upgrades
S30urandom    S32rpcbind      S40umountfs  S90halt

/etc/rc1.d/:
K15pulseaudio K20acpi-support K20kerneloops K20saned K74bluetooth
K80openvpn    K81rpcbind  README  S30killprocs S70dns-clean S70pppd-dns
S90single

/etc/rc2.d/:
README      S20kerneloops      S20sysstat      S24prueba
S50pulseaudio S50saned      S70pppd-dns S90binfmt-support S99grub-common
S99rc.local S16openvpn S20speech-dispatcher S25bluetooth S50rsync
S70dns-clean S75sudo      S99acpi-support S99ondemand S99rc.local

/etc/rc6.d/:
K74bluetooth  README                      S20sendsigs  S31umountnfs.sh
S35networking S60umountroot K80openvpn    S10unattended-upgrades
S30urandom    S32rpcbind      S40umountfs  S90reboot

/etc/rcS.d/:
README S13pcmciautils S25brlTTY S37apparmor S43rpcbind S55urandom
S70x11-common
```

Se pide:

1. Diferencias entre el apagado y reinicio de la máquina. Comentar un ejemplo de un script que tuviese que ejecutarse al parar y no al reiniciar la máquina.

En el apagado el sistema se deja consistente, por ejemplo se vacía la caché, y se envía una señal de apagado que hace que el PC deje de consumir energía y responder mientras que el reinicio consiste en una señal de apagado seguida por otra de inicio.



Podemos mencionar como ejemplo de script que se ejecuta al parar y no al reiniciar que el apagado (nivel 0) tiene el fichero S90halt que asumo que parará el sistema y el reinicio (nivel 6) tiene el fichero S90reboot que será para reiniciar el sistema. En ambos casos es el fichero que se ejecuta el último, ya que es el mayor de los ficheros 'S'.

2.¿Qué diferencias observas entre los niveles de tipo-monousuario?

El nivel rc1 tiene ficheros de tipo K para parar detener procesos, como K15pulseaudio o K20saned, o matar demonios mientras que el nivel rcS no. Además, el nivel rc1 ejecuta el demonio S90single y el nivel rcS no.

3.Indique qué se activa antes en el nivel 2, el soporte ACPI o el soporte para el bluetooth.

Se activa antes el soporte para bluetooth, ya que éste es S25 y el soporte ACPI es S99, y los ficheros S se ejecutan de menor a mayor según el número que siga a la 'S'.

4.Si ejecutamos las siguientes órdenes como administrador:

```
> echo "echo \"HOLA\$1\" > /tmp/p1" > /etc/rc2.d/S24prueba
> mv /etc/rc2.d/S24prueba /etc/rc2.d/S71prueba
> cp /etc/rc2.d/S71prueba /etc/rc4.d/K00prueba
> chmod u+x /etc/rc2.d/S71prueba /etc/rc4.d/K00prueba
> telinit 4
> telinit 2
```

Indique el contenido del fichero /tmp/p1:

- Después de ejecutar la orden "telinit 4"

El fichero tendrá:

HOLA stop → esto es porque rc ejecuta los ficheros K con el parámetro stop y los S con start.

- Después de ejecutar la orden "telinit 2"
 - Antes de que se ejecute el script S70dns-clean

HOLA stop → esto es porque el script que sobrescribirá el fichero p1 es el S71prueba, por lo que aún no se habrá ejecutado y contendrá lo que tenía antes.

- Antes de que se ejecute el script S75sudo

HOLA start → ya sí se ha ejecutado S71prueba y se ha sobrescrito el fichero.

5.¿Cómo eliminaría el servicio openvpn a todos los niveles?

```
rm /etc/rc?.d/*openvpn
```

Ejercicio 2

¿Qué sucedería si el sector MBR de un disco duro queda dañado (por ejemplo, en una caída)? ¿Cómo podríamos repararlo?

Pasaría que ya no se cargaría el sistema operativo, ya que el MBR es el encargado de cargar el núcleo del S.O. y pasarle el control para que termine de iniciar el sistema.

Para repararlo debemos usar `sudo grub-install /dev/sda`, pero deberíamos hacerlo desde otro sistema o con un USB booteable ya que el problema es que no tenemos MBR y no podemos cargar ningún sistema.

Ejercicio 3

Comenta el significado de las siguientes líneas de un fichero de configuración:

```
menuentry 'Debian GNU/Linux, con Linux 3.16.0-4-amd64' --class debian
--class gnu-linux --class gnu --class os {
    insmod part_msdos
    insmod ext2
    set root='hd0,msdos1'
    search --no-floppy --fs-uuid --set=root bf8474c5-958e-4cca-a568-
4828b2310fda
    echo      'Cargando Linux 3.16.0-4-amd64...'
    linux    /boot/vmlinuz-3.16.0-4-amd64 root=UUID=bf8474c5-958e-4cca-
a568-4828b2310fda ro initrd=/install/gtk/initrd.gz quiet
    echo      'Cargando imagen de memoria inicial...'
    initrd   /boot/initrd.img-3.16.0-4-amd64
}
```

Se están definiendo las entradas de un menú en la directiva `menuentry`. Dicho menú se llamará 'Debian GNU/Linux, con Linux 3.16.0-4-amd64' y se definen las entradas del menú con la opción `--class`. En la entrada `os` se definen los comandos que están entre `{ }`, entre los cuales podemos ver algunos `echo` y el proceso `initrd`.

¿Qué fichero modificaría para eliminar la opción 'quiet' de todas las entradas linux?

El fichero `/etc/default/grub` y haría un `ctrl + F` por 'quiet' para cambiarlo.

NOTA: la opción debe ser algo parecido a `GRUB_CMDLINE_LINUX_DEFAULT`



Ejercicio 4

Interprete el siguiente código:

```
# tty1 - getty
#
# This service maintains a getty on tty1 from the point the system is
# started until it is shut down again.
start on stopped rc RUNLEVEL=[2345]
stop on runlevel [!2345]

respawn
exec /sbin/getty -8 38400 tty1
```

Es un fichero de configuración de evento (.conf) en el que podemos ver bajo qué condiciones se lanzará, establecido en la directiva start on ... , y bajo qué condiciones parará, en la directiva stop on ... → parará cuando no esté en los niveles 2,3,4 o 5. Además, se le indica que se active de nuevo cada vez que se pare, directiva respawn, y que ejecute el programa getty de la carpeta /sbin con los comandos que aparecen a continuación.

¿Qué sucedería si elimina el 2 en RUNLEVEL=[2345]?

Significa que el nivel 2 no tendría tty.

Ejercicio 5

¿Por qué no deberíamos apagar el sistema utilizando directamente el botón de POWER del ordenador?

Porque puede que haya procesos que se estén ejecutando y que un corte de energía los interrumpa, dejándolos a la mitad. Además puede que haya ficheros abiertos y que no se cerraría correctamente.



¿Qué alternativas conoce?

De forma gráfica podríamos darle a Apagar, en el menú. Y por terminal podríamos usar un halt o telinit 0.

Ejercicio 6

Indique la secuencia de pasos que necesita para cambiar los parámetros de configuración de GRUB.

Debemos editar el fichero /etc/default/grub y luego debemos hacer un update-grub bajo superusuario.

Ejercicio 7

¿Qué tendríamos que hacer si queremos que el script deliver_pizza.sh que está en el HOME de root se ejecutase siempre en el nivel de ejecución 4?

Debemos hacer un enlace simbólico en el nivel rc4. Esto se hace del siguiente modo:

```
> ln -s /root/deliver_pizza.sh /etc/rc4.d/S99deliver_pizza
```

NOTA: es importante que sea un -s, ya que ln solo crea enlaces físicos.



EJERCICIOS TEMA 4

Ejercicio 1

Comenta distintas formas de imposibilitar el acceso al sistema por parte de un usuario.

1. Podemos establecer `/sbin/nologin` o `/bin/false` como su intérprete shell por defecto (último campo del fichero `/etc/passwd`).
2. Podemos borrar el usuario con `deluser <nombre_usuario>`.
3. Podemos cambiarle la contraseña para que no pueda acceder a su cuenta.
4. Podemos inhabilitarle la cuenta poniendo `“!!”` o `“*”` en el campo de la contraseña en el archivo `/etc/passwd`.
5. Podemos caducarle la cuenta desde el archivo `/etc/shadow`.

Ejercicio 2

¿Cómo se determina el grupo primario de un usuario?

Podemos saber cuál es el grupo primario del usuario X si miramos la 4ª columna de dicho usuario en el archivo `/etc/passwd`.

¿Cómo lo cambiaría?

Podemos editar dicho fichero directamente o usar el comando `usermod`.

Ejercicio 3

Explica las diferencias que supondría utilizar las siguientes máscaras: 077, 027, 022 y 755.

	Ficheros	Directorios
Permisos base	666	777
077	600	700
027	640	750
022	644	755
755	022	022



¿Cómo modificarías los valores del umask por defecto de un usuario?

Durante una sesión vale con ejecutar el comando `umask XXX` donde XXX es la nueva máscara que queremos usar. Si lo queremos hacer permanente debemos modificar el archivo `/$HOME/.bashrc` o similar (puede cambiar el nombre de un S.O. a otro).

¿Y de todos los usuarios?

En caso de querer un cambio global debemos editar el archivo `/etc/profile`

NOTA: los archivos `.bashrc` o `.bash_profile` ejecutan todo lo de `/etc/profile` al comienzo. Dicho archivo es global mientras que los otros son personales.

¿Habría alguna forma de forzarles a mantenerlos?

No, ya que siempre se puede ejecutar `umask`, a no ser que restringamos la ejecución de dicho comando.

Ejercicio 4

¿Es cierto que el administrador del sistema puede modificar el password de un usuario?

Sí, con `passwd <usuario>` puede modificar la contraseña.

¿Puede ejecutar algún programa que le permita leerla?

No, ya que las contraseñas están cifradas. Como mucho puede ver el resumen.

Ejercicio 5

Imagina la siguiente salida:

```
pagutierrez@pagutierrez--TOSHIBA:~/tmp$ ls -la
total 8
-rw-rw-r-- 1 root      profesores  0 2012-03-19 18:30 prueba
pagutierrez@pagutierrez--TOSHIBA:~/tmp$ newgrp profesores
Contraseña:
pagutierrez@pagutierrez--TOSHIBA:~/tmp$
```

¿Qué salida producirían los siguientes comandos?

1. `chmod o+w prueba`

Le añade permisos de escritura a los demás usuarios.



2. echo "HOLA" >> prueba

Guardaría en el archivo prueba "HOLA" ya que dicho archivo pertenece al grupo de profesores y con el comando newgrp hemos cambiado a ese grupo.

3. cat prueba

Produciría la lectura por consola del archivo prueba, porque al tener permisos de lectura para el grupo es una operación permitida.

Ejercicio 6

Comente el contenido del siguiente fichero:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:38:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
saned:x:112:121::/home/saned:/bin/false
pagutierrez:x:1000:1000:Pedro A. Gutiérrez,,,:/home/pagutierrez:/bin/bash
```

¿Con qué usuarios podría logearse en el sistema a través del administrador (el comando sudo su usuario tendría sentido?)

Con todos salvo con syslog y saned, debido a que tienen como shell /bin/false, es decir, se les ha limitado la cuenta.

¿Qué usuarios tienen una carpeta personal?

Todos salvo nobody.

¿Detecta alguna inconsistencia?

Hay dos usuarios con el mismo UID (list y irc tienen el UID 38).



Ejercicio 7

Explique por qué no produce ninguna salida el siguiente listado:

```
pedroa@pagutierrezLaptop:~$ ls /etc/skel/  
pedroa@pagutierrezLaptop:~$
```

No produce ninguna salida porque los ficheros de esa carpeta están ocultos (empiezan por un .), para obtener una salida ha de usarse `ls -a`.

¿Qué ficheros hubiese esperado obtener?

Aquellos que se copian al \$HOME de un usuario cuando se añade al sistema, como el `.profile`, `.bashrc` o `.bash_logout`.



EJERCICIOS TEMA 5

Ejercicio 1

¿Cómo podríamos listar el PID de todos los procesos en ejecución utilizando ls?

Con el comando ps -A. También podemos hacer un ls /proc/.






Ejercicio 2

Explicar cada una de las cifras que aparecen en la siguiente salida:

```
pagutierrez@TOSHIBA:~$ free
```

	total	used	free	shared	buffers	cached
Mem:	1012004	924100	87904	0	13292	142316
-/+ buffers/cache:		768492	243512			
Swap:	1000444	508868	491576			

El comando free muestra la cantidad de memoria libre y usada que tiene el sistema. Por una parte muestra la memoria física, la swap y la memoria caché y de buffer consumida por el kernel.

-  La columna total es el espacio total.
-  La columna used es el espacio usado del total.
-  La columna free es el espacio que queda libre.
-  La columna buffers es el espacio usado en buffers por el kernel.
-  La columna cached es el espacio usado en caché por el kernel.

Ejercicio 3

¿Qué diferencia existe entre hibernar un equipo y suspender un equipo? ¿En qué sentido influye en la memoria del sistema?

El modo suspensión detiene todas las operaciones de todos los procesos y salva el estado del sistema en la RAM. Este modo no vuelca a memoria de intercambio. El ordenador pasa a un modo de bajo consumo en el que el sistema aún necesita energía.



El modo hibernación traslada todos los datos de la memoria a la memoria de intercambio (por tanto, la memoria swap debe ser tan grande como la RAM) y además este modo apaga la máquina. En este estado no necesita energía alguna. Al encender de nuevo el equipo el kernel recarga el contenido de la memoria desde la swap.

Ejercicio 4

¿Para qué sirven los comandos vmstat e iostat? ¿Para qué tareas los utilizaría en su labor como administrador de sistemas?

El comando vmstat sirve para el control y la gestión de los procesos y memoria consumida, es decir, sirve para monitorizar la actividad de la CPU y de la memoria.

El comando iostat sirve para ver estadísticas sobre la CPU y los dispositivos particiones, es decir, sirve para el control de dispositivos de entrada/salida.

El primero, vmstat, lo usaría si algún usuario tuviese demasiado procesos activos para ver la carga del sistema o para monitorizar el uso de memoria. El segundo, iostat, lo usaría si hubiese algún problema con el acceso a disco desde los dispositivos o particiones de E/S.

Ejercicio 5

¿Para qué sirven los comandos df y du? Ponga ejemplos de situaciones en que debería utilizar dichos comandos.

El comando df sirve para ver la capacidad, el espacio libre y el punto de montaje de cada uno de los sistemas de ficheros del equipo mientras que el comando du sirve para mostrar el espacio usado por cada subdirectorío del directorio actual, es decir, ambos sirven para la monitorización del espacio en disco mediante df y du.

El comando df lo utilizaría si quisiese montar un nuevo sistema de ficheros, para comprobar que todo fuese correcto. El comando du lo utilizaría para localizar qué carpeta en concreto es la que ocupa mucho espacio en un sistema saturado para notificarle al usuario propietario que la borrarse o hiciese algo con ella o actuar yo en consecuencia.

Ejercicio 6

¿Qué debería hacer si un proceso consume demasiada CPU del sistema que está administrando? ¿Qué comandos debería utilizar para pararlo temporalmente, reiniciarlo e investigar más sobre el mismo?

Antes de matar el proceso directamente y cortar el problema de raíz, deberíamos estudiar qué hace porque puede que no sea malicioso y sea parte de algún script para un equipo de investigación, por ejemplo. Lo primero que deberíamos hacer antes de nada es suspenderlo



con STOP, aplicarle un renice para darle menos prioridad (por ejemplo un 15) y estudiarlo con strace. Aquí tenemos dos opciones, podemos hacer que continúe y estudiarlo con strace -p <pid> o lanzarlo de nuevo con strace <proceso>. Tras ver qué hace y sopesar la situación se puede hablar con el dueño y reanudarlo con CONT o matarlo directamente.

Para parar un proceso podemos hacer kill -STOP <pid> o kill -SIGSTOP <pid>. Haciendo renice 15 <pid> le damos la nueva prioridad. Para estudiarlo con strace -p <pid> o un strace <proceso> y para hacer que continúe kill -SIGCONT <pid> o kill -CONT <pid>.

NOTA: esto pone en los apuntes, copiao' tal cual:

comando: > top → para localizar el proceso (PID)

pausarlo: > kill -s STOP <PID>

cambiar prioridad: renice 14 <PID>

reiniciar: > kill -s CONT <PID>

Para investigar usamos: strace -p <PID> → miramos las llamadas al sistema

Ejercicio 7

Relacione el UID de un fichero con el UID real de un proceso y el UID efectivo de un proceso. Comente al menos dos motivos por los que el UID de un proceso es necesario en un sistema GNU/Linux.

El UID de un fichero es el identificador de usuario del propietario del fichero, mientras que es UID real del proceso es el UID del usuario real, el que lo ejecutó, y el UID efectivo es el UID bajo el cual se ejecutan las órdenes (es donde se reflejan los cambios de dominio).

El UID es necesario porque:

- Así podemos saber qué usuario es el responsable de lanzar el proceso y actuar en consecuencia si es malicioso.
- Podemos bloquear todos los procesos de un usuario por su UID.

Ejercicio 8

Un memory leak es un consumo incremental sin fin de memoria por parte de un proceso. ¿Cómo encontraría este tipo de procesos en un sistema GNU/Linux?

Podemos ejecutar el comando top y ver cómo va incrementando el consumo por parte del proceso en tiempo real.

NOTA: en los apuntes pone, copiao' tal cual:



usamos top ordenado por memoria

Ejercicio 9

¿Para qué sirve el comando killall? ¿Qué señal envían por defecto los comandos kill y killall (número y nemónico)?

killall <comando> : permite mandar una señal a todos los procesos que estén ejecutando dicho comando.

Tanto kill como killall mandan por defecto la señal SIGTERM, que es la 15.

Ejercicio 10

Especifica el contenido de dos entradas para el fichero crontab:

- **La primera debe imprimir el espacio libre en las particiones del sistema cada hora. La información se volcará al fichero /var/log/reportEspacia.log**

0 0-23/1 * * * \$HOME/espacioLibreParticiones → el fichero espacioLibreParticiones contiene las instrucciones necesarias para imprimir el espacio libre en las particiones.

- **La segunda debe imprimir el listado de todos los procesos, incluyendo el nombre de usuario, a las 9:00h, a las 12:00h y a las 15:00 los viernes. La información se volcará /var/log/reportProcesos.log**

0 9,12,15 * * * 5 \$HOME/listadoProcesos → el fichero listadoProcesos contiene las instrucciones para imprimir todos los procesos incluyendo el nombre de usuario.

EJERCICIO TEMAS 7

Ejercicio 1

¿Con qué se corresponde la siguiente salida? ¿Cómo puede obtenerse en un sistema GNU/Linux?

```
/dev/sda5 /      ext4 rw 0 0
```

```
/dev/sda6 /home ext4 rw 0 0
```

Es la información de todos los sistemas de ficheros a montar, o ya montados, y las zonas de intercambio a activar. Indica el fichero especial de bloques, el punto de montaje, el tipo, las opciones del fichero, etc

Se puede obtener haciendo `cat /etc/fstab`.

¿Cómo podría indicar un dispositivo si solo conoce su UUID o su etiqueta?

Se podría indicar usando `LABEL=<etiqueta>`

Ejercicio 2

Suponiendo el siguiente contenido para el fichero `/etc/fstab`:

<code>LABEL=/</code>	<code>/</code>	<code>ext3</code>	<code>defaults,usrquota</code>	<code>0 1</code>
<code>/dev/sda3</code>	<code>/windows</code>	<code>vfat</code>	<code>defaults</code>	<code>0 0</code>
<code>/dev/dvd</code>	<code>/media/dvd</code>	<code>iso9660</code>	<code>noauto,owner,ro</code>	<code>0 0</code>
<code>/dev/fd0</code>	<code>/media/floppy</code>	<code>vfat</code>	<code>noauto,uid=500</code>	<code>0 0</code>
<code>/dev/sda4</code>	<code>/otrolinux</code>	<code>ext3</code>	<code>rw,auto</code>	<code>0 2</code>
<code>/dev/sda2</code>	<code>swap</code>	<code>swap</code>	<code>defaults</code>	<code>0 0</code>

¿Qué puntos de montaje tendría algún contenido tras iniciar el sistema?

La raíz (`/`), `/dev/sda3`, `/dev/sda4` y `/dev/sda2` ya que como opciones tienen `auto` o `defaults` (que incluye `auto`) y se montan al arrancar el sistema.



Ejercicio 3

Establezca que los permisos por defecto para archivos sean 601 para la partición /dev/sda4 del ejercicio anterior. Suponiendo que la partición ya esté montada, ¿cómo haría efectivos los permisos de manera inmediatamente?

Para establecer los permisos en 601 hay que poner en la parte de opciones: umask=<máscara que hace los permisos 601> → en este caso no se puede llegar al permiso 601 porque umask trabaja sobre los permisos base, que son 666 así que no podemos conseguir 601, lo máximo que podemos conseguir es 600 (con la máscara 077).

Para hacerlo efectivo deberíamos montar de nuevo la partición con el comando mount.

Ejercicio 4

¿Cómo sabría el número de bloques libres de la partición /dev/sda3?

Usando el comando df: df /dev/sda3

Ejercicio 5

¿Cuál es la diferencia entre formatear (a bajo nivel) y particionar un disco? ¿Cuál es la diferencia entre formatear (a alto nivel) y particionar un disco? ¿Cuándo se crea el journal?

Formatear a bajo nivel es devolver a estado de fábrica el disco y particionar es crear una división de una unidad física de almacenamiento. Formatear a alto nivel no borra el contenido del disco, sólo borra sus referencias así que el sistema creerá que está “vacío” y lo sobrescribirá.

El journal se crea cuando se quiere tener un registro de las operaciones (ext3 y ext4 tienen journal).



EJERCICIOS TEMA 8

Ejercicio 1

¿Cuál es el propósito de compartir de compartir una impresora Linux utilizando SAMBA?

Compartir las impresoras con Windows, porque SAMBA es una implementación libre del protocolo de ficheros compartidos de Microsoft.

Ejercicio 2

Supón que tenemos la suerte (cada vez más habitual) de que el fabricante de una impresora nos ha proporcionado un fichero PPD denominado newprinter.ppd. ¿Para qué sirve ese fichero? ¿Qué labor administrativa está haciendo el siguiente comando?

Lpadmin -p prueba -E -v parallel:/dev/lp0 -m newprinter.ppd

El fichero ppd es un fichero que sirve para que CUPS sepa como manejar una impresora (driver) ya que contiene las opciones soportadas (formato de papel, duplex, bandejas, contraseña, etc).

La labor administrativa que cumple es añadir una impresora de nombre prueba, instalada en /dev/lp0 y el driver con el que va a funcionar es newprinter.ppd.

Ejercicio 3

¿Qué comando utilizarías para imprimir un fichero a la impresora por defecto desde la línea de comandos? ¿Este comando es exclusivo de CUPS? ¿Cómo harías para saber las impresoras que hay en un sistema CUPS?

Utilizaría lp o lpr, que no es exclusivo de CUPS. Para saber las impresoras que hay en un sistema CUPS utilizaría `cat /etc/cups/printers.conf`.



EJERCICIOS TEMA 9

Ejercicio 1

¿Cómo podrías utilizar el comando tar para crear una copia incremental de su directorio home con dos niveles (0 y 1)?

Con la opción -incremental ó -G, tar permite crear un backup incremental y saber qué archivos del total están presentes en dicho backup.

El fichero cambios.snar es un archivo con metadatos de las diferencias para los siguientes backups.

Copia nivel 0:

```
tar -cvzf backup/backup_nivel0.tgz -g backup/cambios.snar /home
```

Copia nivel 1:

```
tar -cvzf backup/backup_nivel1.tgz -g backup/cambios.snar /home
```

Ejercicio 2

Proporciona un comando que realizase una copia de seguridad de su directorio home (nivel 0) en el primer dispositivo de cinta conectado al sistema. Elije el comportamiento más adecuado (rewinding o non-rewinding).

```
Dump 0 -u -f /dev/nst0 /home
```



Ejercicio 3

Crea un fichero crontab que realice las siguientes copias de seguridad de /dev/sda1, regularmente, sobre el primer dispositivo de cinta:

- a. Una copia de nivel 0 una vez al mes.
- b. Una copia de nivel 2 una vez a la semana.
- c. Una copia de nivel 5 cada día que no se haya producido ni una de nivel 0 ni una de nivel 2.

En el peor escenario, ¿cuántos comandos de restauración tendrías que aplicar para recuperar un fichero del que se realizó copia con esta configuración?.

```
@monthly dum 0 -u -f /dev/nst0 /dev/sda1
```

```
@weekly dum 2 -u -f /dev/nst0 /dev/sda1
```

```
0 0 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
2,3,4,5,6,7 * dum 5 -u -f /dev/nst0 /dev/sda1
```

En el peor de los casos se deberá realizar una restauración completa con el comando:

Restore -r -f /dev/nst0

Ejercicio 4

Realiza una copia de seguridad de tu directorio \$HOME en la carpeta /var/tmp utilizando el comando tar. Comprime el fichero con el algoritmo gzip. Haz un fichero que, al descomprimirlo, genere la misma estructura de directorios original. ¿Qué opción utilizarías para extraerlo preservando los permisos?.

Tar ppz /var/tmp \$HOME

Opción:

- p (minúscula) → conserva los permisos de los ficheros
- P (mayúscula) → guarda los ficheros con su ruta absoluta
- z → comprime mediante gzip



Ejercicio 5

Comenta al menos tres directrices generales a tener en cuenta cuando se realizan copias de seguridad de los archivos.

Cuando se realiza una copia de seguridad se debe tener en cuenta:

- Guardar la copia de seguridad en un disco conectado a la máquina no es seguro, por eso se recomienda utilizar cintas magnéticas.
- El nivel de la copia de seguridad, ya que una copia de seguridad completa (nivel 0) contiene muchos archivos, por lo que lo ideal es una completa un día concreto y el resto programar copias incrementales de niveles 1, 2, 3, etc.
- Realizar las copias cuando la carga del sistema sea baja, por ejemplo, de madrugada cuando hay menos usuario usando el sistema.

Ejercicio 6

Supón que en una empresa la sensibilidad de los datos es muy alta y no hay restricciones de espacio en el dispositivo para hacer las copias. ¿Qué tipo de copia de seguridad crees que sería la más adecuada?. ¿Qué sistema instaurarías si el espacio fuese limitado? Suponiendo que la mayoría de los cambios en el disco se producen de lunes a viernes y que el domingo el sistema está ocioso, ¿cómo organizarías las copias de seguridad en este segundo caso?.

Esta pregunta es más subjetiva, luego os recomiendo pensad vuestra propia respuesta en base al contenido del temario y lo aprendido en los ejercicios anteriores.