COMANDOS BÁSICOS
Curso de Seguridad Informática (www.solnu.com)
Universitat de Barcelona

Instalación/desinstalación de software

```
apt-get update (actualiza la información de nuestro
servidor de paquetes)
apt-cache search <parámetro> (busca <parámetro> en las
definiciones del los paquetes)
apt-cache show paquete (descripción del paquete)
apt-cache depend paquete (muestra las dependencias)
apt-get install <paquetes> (descarga e instala los
paquetes solicitados)
apt-get remove <paquetes> (desinstala los paquetes
solicitados)
apt-get upgrade (actualiza los paquetes instalados a la
nueva versión)
apt-get clean  (elimina todos los paquetes descargados)
apt-build install paquete (compila el tarball,crea el
paquete deb y lo instala)
```

Instalación/desinstalación de paquetes .DEB

```
dpkg -i paquete - Instalación de paquetes .deb
dpkg -r paquete - Desinstala un paquete.
dpkg --purge paquete - Desinstala además los ficheros
de configuración.
dpkg --force -r paquete - Fuerza la desinstalación.
dpkg -c paquete - Muestra el contenido de un paquete.
dpkg -L paquete - Muestra todos los ficheros.
dpkg -S fichero - Muestra a qué paquete pertenece.
dpkg --get-selections - Listado todos los instalados.
dpkg-reconfigure paquete - Reconfigura paquetes.
```

Consolas virtuales

```
Alt+F1 a Alt+F6 fuera del entorno gráfico
Ctrl+Alt+F1 a Ctrl+Alt+F6 si estamos en entorno gráfico
Alt+F7 volver a las X
```

Búsqueda de ficheros

```
Modo de empleo: find [ruta-de-acceso...] [expresión]
ejemplo: find . -name "*module*"
whereis ejecutable - Busca un ejecutable
type comando       - Muestra la ubicación del comando.
```

Enlaces simbólicos

```
ln [OPCIÓN]... OBJETIVO [NOMBRE_DEL_ENLACE]
ln [OPCIÓN]... OBJETIVO... DIRECTORIO
```

Empaquetar/desempaquetar

```
tar -cf archivo.tar fichero01 fichero02 carpeta01 ...
tar -xvf archivo.tar
tar -zxvf archivo.tar.gz
tar -jxvf archivo.tar.bz2
gzip, bzip2 compresión / gunzip, bunzip2 descompresión
```

Permisos, usuarios, grupos

Valor	Permisos	Valor	permisos
0	---	4	r--
1	--x	5	r-x
2	-w-	6	rw-
3	-wx	7	rwx

Ejemplos:
chmod 755 fichero
chmod u+x fichero
chmod g-r fichero
chmod o+r fichero
chown
chgrp

Creación de nuevos usuarios

```
adduser o useradd  - crea un usuario nuevo.
adduser user group - añade un usuario a un grupo.
deluser            - borra un usuario del sistema.
delgroup group     - elimina un grupo
deluser user group - elimina un usuario de un grupo
```

Comandos básicos

```
ls    -  Muestra el contenido de un directorio
cd    - Cambio de directorio
mkdir - Crea un directorio
rmdir - Borra un directorio
rm    - Borra ficheros
mv    - Mover un archivo
cp    - Copia un archivo
```

Manuales

```
man <PalabraClave> - muestra el man determinado
man -f <PalabraClave> - busca la <palabra clave>
man -k <PalabraClave> - busca en el contenido.
man <sección> <PalabraClave> - llama la sección del man
apropos  palabra_clave - Busca dentro de las man
```

Parada - inicio de sistema

```
halt     - detiene el sistema.
reboot   - reinicia el sistema.
init 0   - Apaga la máquina.
init 1   - Single user
init 6   - Reinicia la máquina.
exit     - Termina la ejecución del programa en curso.
shutdown - permite parar el sistema con muchas opciones
shutdown -t1 -h now - Apaga la máquina.
shutdown -t1 -r now - Reinicia la máquina.
```

Uso de disco / memoria / estado del sistema

```
mount - monta un dispositivo
umount - desmonta un dispositivo
df - Muestra información sobre el sistema de ficheros
du - Muestra un resumen del uso de disco para cada
fichero, recursivamente para directorios
free - Muestra info del estado de la memoria RAM y SWAP
ulimit - permite limitar los recursos o visualizarlos
```

Procesos

```
kill   - Mata un proceso.
ps     - Muestra los procesos que se están ejecutando
en el sistema
pstree - Muestra los procesos que se están ejecutando
en el sistema, en forma de árbol.
top    - Muestra las tareas que se están ejecutando en
el sistema, la memoria, estado de la CPU,...
at [-f script] [tiempo] - Sirve para ejecutar un script
a una hora y/o fecha.
```

Procesos activos

```
fuser -v archivo - Muestra los procesos que están
usando un fichero o directorio.
lsof | less      - Lista los ficheros* abiertos por los
procesos.
lsof -c comando  - Lista los ficheros abiertos por un
proceso.
lsof +D /tmp     - Lista los procesos que están usando
mi directorio.
lsof -i :22022   - Muestra que proceso se encuentra
detrás del puerto 22022
```

Job Control

Ctrl+c	Finaliza una tarea
Ctrl+z	Pausa una tarea
fg n nom	Foreground
bg n nom	Background
&	Pone la instrucción que precede en Background
jobs	Lista las tareas que se están ejecutando
kill	Mata un proceso
Ctrl+S	Para la transferencia de datos a la terminal.
Ctrl+Q	Resume,reinicia la transferencia de datos.
nohup	Mantiene la tarea después de cerrar la shell.

Acceso

```
w       - Muestra quién y que hace en el sistema.
who     - Muestra quién está en el sistema.
last    - Muestra una lista de los últimos usuarios que
han entrado al sistema.
lastlog - Muestra el último acceso de cada usuario de
nuestro sistema.
lastb - Intentos de conexión fallidos (/var/log/btmp).
faillog - Intentos fallidos y define máximo permitido.
fail2ban - Banea las IP con muchos errores de conexión.
```

Envio de mensajes

```
write - envía un mensaje a un usuario determinado.
wall - envía un mensaje a todos los usuarios conectados
mesg - permite enviar mensajes a tu terminal.
talk - permite chatear con otro usuario.
```

Editores y manipulación de texto

```
grep - Busca una cadena de caracteres dentro de un
archivo o varios archivos.
more - Muestra la información ajustándolo al tamaño de
la pantalla.
nano - Editor de texto
vi   - Editor de texto muy común en sistemas unix (ver
apéndice.)
```

Configuración de red

```
ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up
ifconfig eth0 down
ifconfig eth0 hw ether 00:01:02:03:04:05
ifconfig eth0:1 192.168.1.1 netmask 255.255.255.0 up
dhclient eth0
route add default gw 161.116.32.254
route add -net 192.168.2.0/24 gw 192.168.1.254
netstat -nr  - Muestra la tabla de routing.
```

Netstat

```
netstat -napt - Saber qué puertos tiene abiertos.
n - No resuelve las direcciones a sus nombres DNS.
a - Muestra todos las conexiones.
p - Muestra el número y nombre del proceso,dueño de
dicha conexión.
t - sólo muestra conexiones tcp.
```

Envio de mail

```
mailx -s "Asunto" micuenta@demail.org < fichero.txt
echo "cuerpo mail" | mail -s "Asunto" mail@mail.org
uuencode adjunto adjunto|mail -s "Asunto" mail@mail.org
```

Información del sistema

```
lsusb    - listado de dispositivos conectados al usb.
lspci    - listado de dispositivos conectados al pci.
lshw     - listado completo del hardware visible.
hwinfo   - listado completo del hardware visible.
uptime   - tiempo en activo.
hwscan   - escanea el hardware del equipo.
scsiadd  - permite buscar dev scsi en caliente.
```

Dividir ficheros

```
split [OPCIÓN] [FICHERO [PREFIJO]]
split -b50m openbsd-3.9.iso (divide en ficheros de 50M)
cat                         (une varios ficheros)
```

Pantalla de un terminal

```
clear  - limpia la pantalla.
reset  - inicializa la sesión de terminal.
tput   - inicializa la sesión de terminal y mucho más.
```

Entorno

```
history - Listado de comandos usados por el usuario.
fc -l   - Listado de últimos comandos.
profile - Define environment para un usuario o grupo.
locale  - Muestra la zona geográfica configurada.
loadkeys es - Carga el mapa de teclado español.
locale charmap - Muestra el código de caracteres usado.
set - Muestra las variables locales definidas.
env - Muestra las variables de entorno definidas.
export - Muestra las variables de entorno declaradas.
export VARIABLE=valor - Añadimos una variable.
pwd - Muestra el directorio actual.
```

Kernel / Módulos

```
lsmod    - Listado de módulos cargados.
modprobe - Carga el modulo y sus dependencias.
insmod   - Carga el modulo determinado.
rmmod    - Elimina un modulo determinado.
uname -a - Versión del kernel.
modinfo  - Muestra información sobre un módulo.
depmod   - Comprueba las dependencias del módulo.
modconf  - Programa gráfico para listar,cargar y
descargar módulos del kernel.
cat /proc/version - Versión del núcleo y compilador.
cat /proc/modules - Lista los módulos cargados.
```

Tuberías

```
Una tubería hace que la salida de un programa sea la
entrada de otro
(|) Su sintaxis suele ser: comando | comando
```

Conceptos de entrada/salida (I/O)(E/S)

```
stdin  - entrada estandar para datos,el teclado     (0)
stdout - salida estandar para los programas, screen (1)
stderr - salida estandar para los mensajes de error (2)
Redirecciones,un redireccionador redirige la salida de
un comando a un fichero
(<) comando < fichero
(>) Su sintaxix suele ser: comando > fichero
```

Logs

```
/var/log/kern.log  - Mensajes del núcleo.
/var/log/syslog - Registro de mensajes relativos a la
seguridad.
/var/log/debug - Registro de información de depuración
de los programas.
/var/log/messages - Mensajes del sistema de carácter
informativo.
/var/log/user.log - Información del usuario.
/var/log/XFree86.0.log - Información sobre las X
/var/log/Xorg.0.log - Información sobre las X
/var/log/auth.log - Accesos al sistema(incluye los
intentos fallidos).
```

Backup/Restore del MBR

```
dd if=/dev/hda of=mbr.dat count=1 bs=512    - Backup
dd if=mbr of=/dev/hda                       - Restore
```

Máquinas virtuales con XEN

```
xm console <DomId>  - Acceso a consola de la máquina.
xm create [-c] <cfgfile> - Crea una máquina virtual.
xm destroy <DomId>  - Destruye la máquina virtual.
xm list             - Lista información de las MV.
xm pause <DomId>    - Pausa una máquina virtual.
xm reboot <DomId>   - Reinicia una máquina virtual.
xm shutdown <DomId> - Apaga una máquina virtual.
xm top              - Monitoriza el sistema y las MV.
xm unpause <DomId>  - Restaura una máquina pausada.
```

LVM

```
vgdisplay - Muestra los VG's
vgcreate  - Crea un VG
vgremove  - Elimina un VG
vgextend  - Amplia un VG
vgreduce  - Reduce un VG
vgscan    - Busca VG's en los discos del sistema
lvdisplay - Muestra los LV's
lvcreate  - Crea un LV
lvremove  - Elimina un LV
lvextend  - Amplia un LV
lvreduce  - Reduce un LV
Ejemplos:
vgcreate vg_sys /dev/sda1 /dev/sdb1
lvcreate -L5G vg_sys -n xen
lvextend -L +7G /dev/vg_sys/xen
lvremove /dev/vg_sys/xen
```

File System

```
mkfs           - Crea un File System
mkfs.msdos     - Crea un File System DOS
mkfs.reiserfs  - Crea un File System ReiserFS
mkfs.xfs       - Crea un File System XFS
mkfs.ext3      - Crea un File System ext3
mkfs.reiser4   - Crea un File System Reiser4
mkfs.vfat      - Crea un File System VFAT (Windows)
mkfs.jfs       - Crea un File System JFS
mkswap         - Crea una SWAP
swapon         - Activa/desactiva swap
xfs_growfs     - Amplia un FS XFS en caliente
resize2fs      - Amplia un FS ext2/ext3 en offline
ext2resize     - Amplia un FS ext2/ext3 en offline
ext2online     - Amplia un FS ext2/ext3 online
mount -o remount,resize /home - Amplia un FS JFS online
resize_reiserfs -f /dev/myvg/homevol(online)
resize_reiserfs /dev/myvg/homevol
```


Jordi Blasco Pallarès - jordi.blasco@gmail.com