Manejo de Archivos

ls - listar directorio
ls -al - listado con formato y mostrando ocultos
cd *dir* - cambiar a directorio "dir"
cd ~ cambiar a directorio home
pwd - muestra el directorio actual
mkdir *dir* - crear el directorio "dir"
rm *archivo* - borrar archivo
rm -r *dir* - borrar directorio "dir"
rm -f *archivo* - forzar el borrar archivo
rm -rf *dir* - forzar borrar directorio de forma recursiva
cp *archivo1 archivo2* - copiar *archivo1 a archivo2*
cp -r *dir1 dir2* - copiar *dir1 a dir2*; Creando *dir2 si no existe*
mv *archivo1 archivo2* - renombrar o mover *archivo1* a *archivo2*. Si el *archivo2* es un directorio, mueve *archivo1* al contenido de ese directorio
ln -s *archivo link* - crea un enlace simbólico de link a *archivo*
touch archivo - crea o actualiza un archivo
cat > archivo - coloca la salida estándar en *archivo*
more archivo - muestra el contenido de un archivo
head archivo - muestra las primeras 10 líneas de un archivo
tail archivo - muestra las últimas 10 líneas de un archivo
tail -f *file* - muestra las últimas 10 líneas de en tiempo real

Gestión de procesos

ps - muestra los procesos activos actualmente
top - muestra todos los procesos
kill *pid* - mata un proceso indicando el *pid*
killall *proc* - mata un proceso llamado *proc*
bg - lista los procesos detenidos o trabajando en fondo; puede resumir procesos
fg - trae el proceso más reciente al frente
fg *n* - trae N procesos al frente

Permisología

chmod *octal archivo* - cambia los permisos del *archivo* con *octal*, que pueden ser identificados por separado el usuario, grupo o mundo añadiendo:
* 4 - leer (r)
* 2 - escribir (w)
* 1 - ejecutar (x)

Ejemplos:
chmod 777 - leer, escribir, y ejecutar para todos
chmod 755 - rwx para el dueño, rx para el grupo y mundo
Para más opciones, observa: **man chmod**.

Uso de SSH

ssh *usuario@host* - conecta a *usuario* en *host*
ssh -p *puerto user@host* - conecta a el *host* en el *puerto* con el usuario *user*
ssh-copy-id *user@host* - añade tu llave a el *host* para activar el inicio de sesión sin clave

Búsquedas

grep *patrón archivos* - busca en los archivos por el *patrón*
grep -r patrón *dir* - busca recursivamente el *patrón* en los directorios.
comando | grep *patrón* - busca por el *patrón en la salida del comando*
locate *archivo* - encuentra todas las instancias del archivo

Información del Sistema

date - muestra la hora y fecha actual
cal - muestra el calendario del mes
uptime - muestra el tiempo en ejecución del sistema
w - muestra quién está conectado
whoami - muestra como quién está conectado
uname -a - muestra información del kernel
cat /proc/cpuinfo - información del cpu
cat /proc/meminfo - información de la memoria
man *comando* - muestra el manual para el *comando*
df - muestra el uso de disco
du - muestra el uso de disco del directorio
free - muestra la memoria ram y swap libre
whereis app - muestra las posibles ubicaciones de *app*
which *app* - muestra cual *app* corre por defecto

Compresión

tar cf *file.tar archivos* - crear un archivo tar llamado *file.tar* que contiene *archivos*
tar xf *file.tar* - extrae los contenidos de *file.tar*
tar czf *file.tar.gz files* - crea un tar comprimido con Gzip
tar xzf *file.tar.gz* - extrae un tar que usa Gzip
tar cjf *file.tar.bz2* - crea un tar comprimido con Bzip2
tar xjf *file.tar.bz2* - extrae un tar que usa Bzip2
gzip *file* - comprime *file y lo renombra a file.gz*
gzip -d *file.gz* - descomprime *file.gz* de vuelta a *file*

Redes

P*ing *host - ejecuta ping a *host y muestra los resultados*
whois *dominio* - obtiene la info whois de un dominio
dig *dominio* - obtiene la info DNS de un dominio
dig -x *host* - busca el reverso DNS del *host*
wget archivo - descarga un archivo
wget -c archivo - continua una descarga pausada

Instalando Software

Instalando desde las fuentes (normalmente un tar.gz):
./configure
make
make install
Con sistemas de paquetes
dpkg -i *pkg.deb* - instala un paquete (Debian)
rpm -Uvh *pkg.rpm* - instala un paquete (RPM)

Atajos de teclado

Ctrl+C - detiene el comando actual
Ctrl+Z - pausa el comando actual, lo resumes con **fg** al frente o **bg** en el fondo
Ctrl+D - sierra la sesión, similar a **exit**
Ctrl+W - borra una palabra de la linea actual
Ctrl+U - borra toda la línea
Ctrl+R - repite el último comando
exit - sale de la sesión actual

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

Modo Insert	
i	insert
I	insert al principio de la linea
O	insert linea arriba
o	insert linea abajo
a	insert +1 final de linea
A	insert al final de la linea

Modo comandos	
dd	corta/borra
3dd	corta/borra 3 líneas
yy	copia linea
2yy	copia 2 lineas
p	pega
P	pega en la linea de arriba
2p	pega 2 veces
u	Undo (deshacer)
ctrl r	Redo (rehacer)
guu	convierte la línea a minúscula
gUU	convierte la línea a mayúscula

Selección	
v	modo visual (lo seleccionado se puedo copiar, borrar, etc)
ctrl v	Selección en bloque visual (Se pueden seleccionar columnas)

Movimiento	
h	izquierda
l	derecha
j	abajo
k	arriba
:10	posiciona el cursor en la linea 10

Grabar	
ZZ	graba y sale
:x	graba y sale
:w	graba
:w!	fuerza la grabación
:w archivo	graba "guardar como"
:q	sale si no hubo modificaciones
:wq	graba y sale
:q!	sale sin grabar

Otros en Modo Edición	
ctrl n	autocompleta palabra o muestra lista para completar

Otros	
ctrl g	información de línea
zf	Al marcar un texto con v, pulsar zf se compacta
zd	Descompacta las líneas compactadas con zf
:sort	ordena el texto seleccionado
:set number	pone numero de linea
:split archivo	divide la pantalla (ctrl ww para pasar)
:set number	numeros de linea
>>	tabula
:set si	smart indent (tabula automaticamente al abrir y cerrar {})
:set ts=2	Visualiza TAB como 2 posiciones
:h acción	Ayuda sobre una acción (Ej :h undo)
:%s/viejo/nuevo/g	Reemplaza "viejo" por "nuevo", todas las coincidencias
/patron	Busca la palabra "patron" (n para siguiente N para el anterior)

VIM

Cursor movement

h - move left
j - move down
k - move up
l - move right
w - jump by start of words (punctuation considered words)
W - jump by words (spaces separate words)
e - jump to end of words (punctuation considered words)
E - jump to end of words (no punctuation)
b - jump backward by words (punctuation considered words)
B - jump backward by words (no punctuation)
0 - (zero) start of line
^ - first non-blank character of line
$ - end of line
G - Go To command (prefix with number - 5G goes to line 5)
Note: Prefix a cursor movement command with a number to repeat it. For example, 4j moves down 4 lines.

Insert Mode - Inserting/Appending text

i - start insert mode at cursor
I - insert at the beginning of the line
a - append after the cursor
A - append at the end of the line
o - open (append) blank line below current line
(no need to press return)
O - open blank line above current line
ea - append at end of word
Esc - exit insert mode

Editing

r - replace a single character (does not use insert mode)
J - join line below to the current one
cc - change (replace) an entire line
cw - change (replace) to the end of word
c$ - change (replace) to the end of line
s - delete character at cursor and subsitute text
S - delete line at cursor and substitute text (same as cc)
xp - transpose two letters (delete and paste, technically)
u - undo
. - repeat last command

Marking text (visual mode)

v - start visual mode, mark lines, then do command (such as y-yank)
V - start Linewise visual mode
o - move to other end of marked area
Ctrl+v - start visual block mode
O - move to Other corner of block
aw - mark a word
ab - a () block (with braces)
aB - a {} block (with brackets)
ib - inner () block
iB - inner {} block
Esc - exit visual mode

Visual commands

> - shift right
< - shift left
y - yank (copy) marked text
d - delete marked text
~ - switch case

Cut and Paste

yy - yank (copy) a line
2yy - yank 2 lines
yw - yank word
y$ - yank to end of line
p - put (paste) the clipboard after cursor
P - put (paste) before cursor
dd - delete (cut) a line
dw - delete (cut) the current word
x - delete (cut) current character

Exiting

:w - write (save) the file, but don't exit
:wq - write (save) and quit
:q - quit (fails if anything has changed)
:q! - quit and throw away changes

Search/Replace

/pattern - search for pattern
?pattern - search backward for pattern
n - repeat search in same direction
N - repeat search in opposite direction
:%s/old/new/g - replace all old with new throughout file
:%s/old/new/gc - replace all old with new throughout file with confirmations

Working with multiple files

:e filename - Edit a file in a new buffer
:bnext (or :bn) - go to next buffer
:bprev (of :bp) - go to previous buffer
:bd - delete a buffer (close a file)
:sp filename - Open a file in a new buffer and split window
ctrl+ws - Split windows
ctrl+ww - switch between windows
ctrl+wq - Quit a window
ctrl+wv - Split windows vertically