A continuación se muestran una serie de comandos básicos para el manejo de la terminal de comandos en sistemas Unix. El comando “man” permite obtener información sobre el uso de cualquier comando del sistema.

## COMANDOS PARA EL MANEJO DE FICHEROS:

| COMANDO | UTILIDAD |
|---|---|
| **ls** | Listado de los ficheros y directorios |
| **ls -all** | Muestra todos los atributos y ficheros ocultos |
| **cd [directorio]** | Cambio de directorio en la terminal |
| **pwd** | Muestra el directorio / ruta actual de ejecución |
| **mkdir [directorio]** | Creación de un nuevo directorio |
| **rm [fichero]** | Eliminación de un fichero |
| **rm -R [directorio]** | Eliminación (recursiva) de un directorio |
| **cp [fichero] [salida]** | Creación de una copia (salida) del fichero |
| **cp -r [directorio] [salida]** | Creación de una copia (salida) del directorio |
| **mv [fichero] [salida]** | Permite mover el fichero de ruta y/o nombre |
| **cat [fichero]** | Muestra el contenido del fichero |
| **more [fichero]** | Muestra el contenido del fichero |
| **head -n 100 [fichero]** | Muestra las 100 primeras líneas del fichero |
| **tail -n 100 [fichero]** | Muestra las 100 últimas líneas del fichero |
| **chmod [privilegios] [fichero/directorio]** | Cambiar los privilegios de un fichero o directorio |
| **grep [búsqueda] [fichero]** | Búsqueda de información en un fichero |
| **grep -r [búsqueda] [directorio]** | Búsqueda recursiva de información |
| **cut -d “[carácter]” -f [pos]** | Cortar una cadena mediante un caracter |
| **locate [fichero]** | Búsqueda de un fichero en el sistema |

**Pruebas**:

- Crear un directorio llamado pruebas
- Copiar el archivo /etc/passwd en dicho directorio
- Listar los archivos existentes
- Extraer únicamente las 10 primeras líneas del documento
- Extraer únicamente las 10 últimas líneas del documento
- Cambiar los permisos del fichero a 000
- Probar a leer dicho fichero
- Cambiar los permisos a escritura, lectura y ejecución
- Buscar la palabra “root” dentro del fichero
- Extraer únicamente el directorio del usuario

## COMANDOS PARA EL MANEJO DE PROCESOS:

| COMANDO | UTILIDAD |
|---|---|
| **ps** | Listado de procesos activos del usuario |
| **top** | Listado de todos los procesos activos |

| | |
|---|---|
| **kill -9 [PID]** | Finalización forzada de un proceso en base al PID |
| **killall [proceso]** | Finalización de un determinado proceso |

**Pruebas**:

- Abrir el explorador
- Comprobar cuál es el PID del proceso
- Eliminar el proceso

## COMANDOS PARA OBTENER INFORMACIÓN DEL SISTEMA:

| COMANDO | UTILIDAD |
|---|---|
| **date** | Muestra la fecha actual |
| **uptime** | Tiempo que lleva operativo el sistema |
| **whoami** | Muestra el usuario actual |
| **uname -a** | Muestra la versión exacta del Kernel |
| **man [comando]** | Muestra la ayuda para cualquier comando |
| **whereis [aplicación]** | Indica la ruta donde se encuentra una aplicación |
| **apt-get install [aplicación]** | Instalación de una aplicación de los repositorios |
| **dpkg -i [aplicación]** | Instalación una aplicación (archivo .deb) |

**Pruebas**:

- Obtener cual es la fecha actual
- Buscar donde se encuentra el comando nmap
- Instalar el software terminator de los repositorios

## COMANDOS DE RED:

| COMANDO | UTILIDAD |
|---|---|
| **ping [dominio / IP]** | Identifica si un sistema se encuentra vivo* |
| **whois [dominio / IP]** | Obtención de la información WHOIS del activo |
| **dig [dominio]** | Obtiene la información DNS de un dominio |
| **dig -x [IP]** | Resolución inversa y el nombre del dominio |
| **wget [enlace http]** | Descarga de un determinado enlace HTTP |
| **wget [enlace http] -O [fichero]** | Idéntico al anterior pero se almacena la respuesta en fichero |

**Pruebas**:

- Hacer un ping a Google.es
- Comprobar el whois de la página u-tad.com
- Obtener la dirección IP de u-tad.com
- Realizar una resolución inversa de u-tad.com

- Descargar la página principal de U-tad

## COMANDOS PARA LA GESTION DE SERVICIOS:

| COMANDO | UTILIDAD |
|---|---|
| **service [servicio] start** | Habilita un servicio |
| **service [servicio] stop** | Deshabilita un servicio |
| **service [servicio] status** | Comprueba el estado de un servicio |

**Pruebas**:

- Habilitar el servicio de Apache (apache2)
- Verificar que se ha levantado accediendo a 127.0.0.1 vía web
- Verificar el estado
- Deshabilitar el servicio
- Acceder de nuevo a 127.0.0.1 vía web

## EJEMPLO DE BASH SCRIPTING:

A continuación se muestra un simple ejemplo de bash scripting para obtener todos los dominios a los que redirecciona una web, en este caso cisco.com. Posteriormente se extraen las direcciones IP de dichos dominio y se procede a automatizar todo el proceso.

**Descarga de la página principal y revisión**

```
# wget www.cisco.com
# ls -l index.html
# cat index.html
        --> Podemos ver "<li><a href="http://newsroom.cisco.com/">Newsroom</a></li>"
```

**Identificación de patrón y listado en claro de los dominios**

```
# grep "href=" index.html
# grep "href=" index.html | cut -d "/" -f 3
# grep "href=" index.html | cut -d "/" -f 3 | grep "\."
# grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1
# grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1 | sort -u
# grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1 | sort -u > lista.txt
```

**Automatización para la resolución de los dominios**

```
# for url in $(cat list.txt); do host $url; done
# for url in $(cat list.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort -u
# for url in $(cat list.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort -u >
ips.txt
```

También se podría hacer uso del comando awk (*awk '{print $1 }'*)