

# Hacker Highschool

## SECURITY AWARENESS FOR TEENS



## LECCIÓN 2

# NOCIONES DE COMANDOS DE WINDOWS Y LINUX



## “License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at [www.hackerhighschool.org/license](http://www.hackerhighschool.org/license).

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

## Información sobre la “Licencia de Uso”

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto “Hacker Highschool” son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección “LICENSE” de la página web del proyecto “Hacker Highschool” en [www.hackerhighschool.org/license](http://www.hackerhighschool.org/license).

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto.

El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a esponsorizarlo a través de la compra de una licencia, una donación o una esponsorización.

All works copyright ISECOM, 2004.



## Índice

"License for Use" Information.....	2
Información sobre la "Licencia de Uso".....	2
Contribuciones.....	4
2.1. Objetivos.....	5
2.2. Requerimientos y escenario.....	6
2.2.1 Requerimientos.....	6
2.2.2 Escenario.....	6
2.3. Sistema Operativo: WINDOWS.....	7
2.3.1 ¿Cómo abrir una ventana de MS-Dos?.....	7
2.4. Sistema operativo: LINUX.....	12
2.4.1 ¿Cómo abrir una ventana de consola?.....	12
2.4.2 Comandos básicos.....	13
2.4.3 Herramientas de red.....	15
2.5. Ejercicios Prácticos.....	17
2.5.1 Ejercicio 1.....	17
2.5.2 Ejercicio 2.....	17
2.5.3 Ejercicio 3.....	18
Glosario.....	19



## Contribuciones

Daniel Fernández Bleda, Internet Security Auditors

Jairo Hernández, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM



**Universitat Ramon Llull**





## 2.1. Objetivos

En esta lección introductoria se pretende dar a conocer los comandos básicos de Windows y de Linux, para que el alumno se familiarice con ellos y que le servirán para resolver los problemas planteados en el resto de lecciones.

Al término de la lección el alumno tendrá conocimientos de los comandos:

- generales de Windows y Linux.
- básicos sobre redes:
  - ping
  - tracert
  - netstat
  - ipconfig
  - route

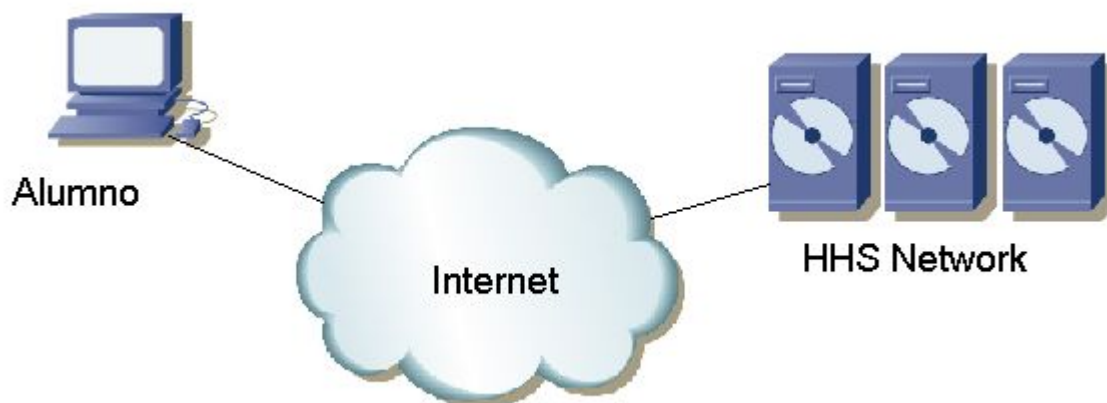
## 2.2. Requerimientos y escenario

### 2.2.1 Requerimientos

Para la presente lección se necesitará:

- Un PC con Windows 98/Me/2000/NT/XP/2003.
- Un PC con Linux Suse/Debian/Knoppix...
- Acceso a Internet.

### 2.2.2 Escenario



Este es el escenario en el que se va a trabajar. Consta de la propia red de ordenadores donde trabajará el alumno, con acceso a Internet, y de la red de servidores de ISECOM destinada al programa Hacker Highschool (HHS), a la cual se accede a través de Internet. Esta es la red contra la que se van a realizar la mayoría de las pruebas.

Debemos tener presente que el acceso a la red de pruebas de ISECOM está restringido, y que es necesario solicitar acceso a ella mediante el proceso de inscripción en el programa: [www.hackerhighschool.org](http://www.hackerhighschool.org).

## 2.3. Sistema Operativo: WINDOWS



Para la mayoría de herramientas referentes al estudio de redes, se utilizan los propios comandos del sistema operativo windows. Es por ello que se va a explicar cómo abrir una ventana de comandos si se está utilizando Windows como sistema operativo.

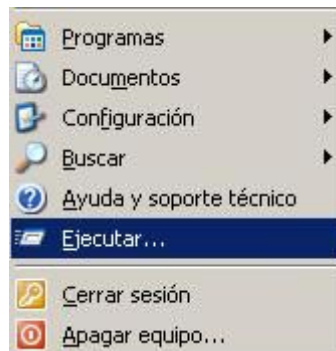
### 2.3.1 ¿Cómo abrir una ventana de MS-Dos?

Para acceder a editar los siguientes comandos, se debe abrir una ventana de comandos. El procedimiento será el mismo para cualquier Windows que se tenga:

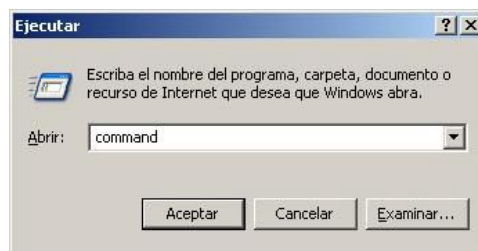
1.- Ir al botón de Inicio.



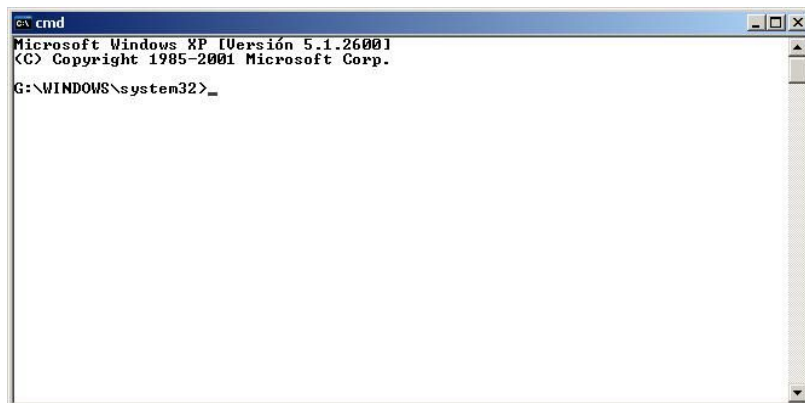
2.- Escoger la opción Ejecutar.



3.- Escribir "**command**" si se está utilizando Windows 95/98 o bien "**cmd**" para el resto de Windows, y pulsar **Aceptar**.



4.- Aparecerá una ventana similar a la siguiente:



5.- Ahora ya se pueden probar los comandos y herramientas que se listan a continuación.

### 2.3.2 Comandos básicos

<b>Date</b>	Muestra o establece la fecha del sistema
<b>Time</b>	Muestra o establece la hora del sistema
<b>Ver</b>	Muestra la versión de MS-DOS que se está utilizando
<b>Dir</b>	Muestra la lista de subdirectorios y ficheros de un directorio o carpeta
<b>Cls</b>	Borra la pantalla
<b>mkdir &lt;directorio&gt;</b>	Crea un directorio o carpeta. Por ejemplo:
<b>md &lt;directorio&gt;</b>	<code>md utilidades</code>
<b>chdir &lt;directorio&gt;</b>	Muestra el nombre o cambia el directorio actual. Por ejemplo:
<b>cd &lt;directorio&gt;</b>	<code>cd utilidades</code>
<b>Rmdir &lt;directorio&gt;</b>	Borra un directorio o carpeta. Por ejemplo:
<b>rd &lt;directorio&gt;</b>	<code>rd utilidades</code>
<b>tree &lt;ruta&gt;</b>	Muestra de forma gráfica-texto la estructura de carpetas de una unidad o ruta. Por ejemplo:
	<code>tree c:\utilidades</code>
<b>Chkdsk</b>	Comprueba un disco y muestra un informe de estado
<b>Mem</b>	Muestra la cantidad de memoria usada y libre en el sistema
<b>rename &lt;origen&gt; &lt;destino&gt;</b>	Cambia el nombre de uno o más ficheros. Por ejemplo:
<b>Ren &lt;origen&gt; &lt;destino&gt;</b>	<code>ren nombreantiguo nombrenuevo</code>



<b>copy</b> <origen> <destino>	Copia uno o más ficheros en otra localización. Por ejemplo: <pre>copy c:\util\fichero.txt c:\temporal</pre>
<b>move</b> <origen> <destino>	Cambia el nombre a ficheros y directorios. Por ejemplo: <pre>move c:\utilidades c:\herramientas</pre>
<b>type</b> <fichero>	Muestra el contenido de un fichero de texto. Por ejemplo: <pre>type c:\utilidades\mifichero.txt</pre>
<b>More</b> <fichero>	Muestra la información pantalla a pantalla. Por ejemplo: <pre>More c:\utilidades\mifichero.txt</pre>
<b>delete</b> <fichero> <b>del</b> <fichero>	Elimina uno o más ficheros. Por ejemplo: <pre>del c:\utilidades\mifichero.txt</pre>

*Nota: Las palabras entre corchetes < > no son comandos, sino que deben substituirse por los valores deseados. Hay comandos que pueden emplearse utilizando su forma larga o corta, por ejemplo, "delete" y "del" son el mismo comando.*

### 2.3.3. Herramientas de red

<b>ping</b> <máquina>	<p>El comando ping permite enviar "sondas" ICMP (Internet Control Message Protocol) a otra computadora, con el objetivo de saber si ésta es alcanzable a través de la red. Además muestra un resumen estadístico acerca del porcentaje de sondas que no han tenido respuesta y del tiempo de respuesta. Se puede utilizar el nombre de la máquina o directamente su dirección IP en Internet.</p> <p>Por ejemplo:</p> <pre>ping www.google.com ping 193.145.85.2</pre> <p>Algunas opciones son:</p> <ul style="list-style-type: none"> <li><b>-n &lt;N&gt;</b> : envía N paquetes</li> <li><b>-t</b> : envía de manera indefinida los paquetes.</li> </ul> <p>Para cancelar ésta y otras opciones: CTRL+C.          Para ver más opciones: ping /h</p>
-----------------------	--



<b>tracert</b> <máquina>	<p>El comando tracert es la abreviatura de <b>trace route</b>, el cual nos permite saber la ruta que siguen los paquetes desde el origen, es decir, nuestra máquina, hasta la máquina destino. También se pueden visualizar los tiempos de cada salto. Como máximo, se listarán 30 saltos. Es interesante observar que se obtienen los nombres de las máquinas por las cuales viajan los paquetes.</p> <p>Por ejemplo:</p> <pre>tracert <a href="http://www.google.com">www.google.com</a> tracert 193.145.85.2</pre> <p>Algunas opciones:</p> <ul style="list-style-type: none"> <li>-h &lt;N&gt; : para especificar N saltos como máximo.</li> <li>-d : no muestra en nombre de las máquinas.</li> </ul> <p>Para ver más opciones: <code>tracert</code></p>
<b>ipconfig</b>	<p>El comando ipconfig muestra información sobre las interfaces de red activas en el ordenador.</p> <p>Por ejemplo:</p> <pre>ipconfig</pre> <p>Algunas opciones:</p> <ul style="list-style-type: none"> <li>/all : muestra más detalles</li> <li>/renew : activa las direcciones IP del adaptador cuando se usa configuración automática con DHCP.</li> <li>/release : desactiva las direcciones IP del adaptador cuando se usa configuración automática con DHCP.</li> </ul> <p>Para ver más opciones: <b>ipconfig /?</b></p>
<b>route</b>	<p>El comando route sirve para definir rutas estáticas, borrar rutas o simplemente ver el estado de las rutas.</p> <p>Algunas opciones:</p> <ul style="list-style-type: none"> <li><b>Print</b> : muestra la lista de rutas.</li> <li><b>Delete</b> : borra una ruta.</li> <li><b>Add</b> : añade una ruta.</li> </ul> <p>Por ejemplo:</p> <pre>route print</pre> <p>Para ver más opciones: <b>route /?</b></p>

**netstat**

Muestra gran cantidad de información sobre el estado de la red y conexiones de red establecidas con máquinas remotas.

Algunas opciones:

- a** Muestra todas las conexiones y puertos escucha.
- e** Muestra estadísticas Ethernet.

Por ejemplo:

```
netstat  
netstat -an
```

Para ver más opciones: **netstat /?**



## 2.4. Sistema operativo: LINUX



Por el mismo motivo que sobre un Windows se ha necesitado abrir una ventana de MS-Dos, si se utiliza LINUX, la gran mayoría de comandos igualmente se ejecutan desde una ventana que emula como si se estuviera trabajando desde una consola. Es por este motivo que se va a proceder a explicar cómo abrir una ventana de consola en LINUX.

### 2.4.1 ¿Cómo abrir una ventana de consola?

Para acceder a editar los siguientes comandos, se debe abrir una pantalla de consola:

1. - Ir al botón de K



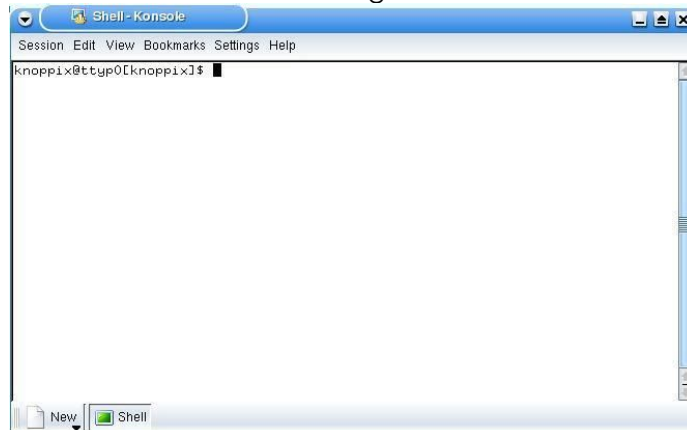
2. - Escoger la opción Run Command:



3. - Escribir "konsole".



4. - Debería salir una ventana similar a la siguiente:



5. - Ahora ya se pueden probar los comandos y herramientas que se listan a continuación.

## 2.4.2 Comandos básicos

<b>pwd</b>	Muestra el nombre del directorio actual.
<b>hostname</b>	Muestra el nombre de la máquina local (en la que estamos trabajando)
<b>finger &lt;usuario&gt;</b>	Muestra información sobre el usuario <usuario>  Por ejemplo: <pre>finger root</pre>
<b>ls</b>	Lista el contenido de directorios  Por ejemplo: <pre>ls -la</pre>

<b>cd</b> <directorio>	<p>Cambia al directorio &lt;directorio&gt;.</p> <p>Ejemplo 1:</p> <p>Si nuestro login es "milogin", el comando</p> <pre>\$cd</pre> <p>cambia al directorio /home/mylogin</p> <p>Ejemplo 2:</p> <pre>\$cd -</pre> <p>Cambia al último directorio visitado.</p> <p>Ejemplo 3:</p> <pre>\$cd /tmp</pre> <p>Cambia al directorio "tmp"</p>
<b>cp</b> <origen> <destino>	<p>Copia ficheros. Copia el fichero "origen" en "destino".</p> <p>Por ejemplo:</p> <pre>cp /etc/passwd /tmp</pre>
<b>rm</b> <fichero>	<p>Borra ficheros. Sólo el propietario del fichero (o root) puede borrarlo.</p> <p>Por ejemplo:</p> <pre>rm mifichero</pre>
<b>mv</b> <origen> <destino>	<p>Mueve o renombra ficheros y directorios</p> <p>Por ejemplo:</p> <pre>mv nombreantiguo nombrenuevo</pre>
<b>mkdir</b> <directorio>	<p>Crea un directorio con nombre "directorio"</p> <p>Por ejemplo:</p> <pre>mkdir midirectorio</pre>
<b>rmdir</b> <directorio>	<p>Borra el directorio "directorio" si se encuentra vacío</p> <p>Por ejemplo:</p> <pre>rmdir midirectorio</pre>
<b>man</b> <comando>	<p>Muestra las páginas del manual on-line</p> <p>Por ejemplo:</p> <pre>man ls</pre>

*Nota: Las palabras entre corchetes < > no son comandos, sino que deben sustituirse por los valores deseados.*



## 2.4.3 Herramientas de red

<b>ping</b> <máquina>	<p>El comando ping permite enviar "sondas" ICMP (Internet Control Message Protocol) a otra computadora, con el objetivo de saber si ésta es alcanzable a través de la red. Además muestra un resumen estadístico acerca del porcentaje de sondas que no han tenido respuesta y del tiempo de respuesta. Se puede utilizar el nombre de la máquina o directamente su dirección IP en Internet.</p> <p>Por ejemplo:</p> <pre>ping <a href="http://www.google.com">www.google.com</a> ping 193.145.85.2</pre> <p>Para ver más opciones: <code>man ping</code></p>
<b>tracert</b> <máquina>	<p>El comando tracert indica la ruta que siguen los paquetes desde el origen, es decir, nuestra máquina, hasta la máquina destino llamada &lt;máquina&gt;. Por ejemplo:</p> <pre>tracert <a href="http://www.google.com">www.google.com</a></pre> <p>Para ver más opciones: <code>man tracert</code></p>
<b>ifconfig</b>	<p>El comando ifconfig muestra información sobre las interfaces activas (ethernet, ppp, etc.).</p> <p>Por ejemplo:</p> <pre>ifconfig</pre> <p>Para ver más opciones: <code>man ifconfig</code></p>
<b>route</b>	<p>El comando route sirve para definir rutas estáticas, borrar rutas o simplemente ver el estado de las rutas.</p> <p>Algunas opciones:</p> <ul style="list-style-type: none"> <li>print: muestra la lista de rutas.</li> <li>delete: borra una ruta.</li> <li>add: añade una ruta.</li> </ul> <p>Por ejemplo:</p> <pre>route</pre> <p>Para ver más opciones: <code>man route</code></p>

**netstat**

Muestra gran cantidad de información sobre el estado de la red y de las conexiones TCP/IP establecidas.

Por ejemplo:

```
netstat
netstat -an
```

Para ver más opciones: `man netstat`





## 2.5. Ejercicios Prácticos

### 2.5.1 Ejercicio 1

Para profundizar sobre los conocimientos adquiridos de Windows.

- Accede a una ventana de MS-DOS
- Identifica la versión de MS-DOS que estás utilizando. ¿Qué versión has detectado? ¿Qué comando has utilizado?
- Identifica la fecha y hora del sistema. Comprueba que sean correctas; sino, modificalas para que lo sean. ¿Qué comandos has utilizado?
- Identifica todos los directorios y ficheros que se encuentran en "c:\". ¿Qué comando has utilizado y cuál ha sido la salida de este comando?
- Crea el directorio c:\hhs\tema0. Copia en este directorio todos los ficheros con la extensión .sys que se encuentren en c:\. ¿Qué ficheros has encontrado? ¿Qué comandos has utilizado?
- Identifica la dirección IP de tu máquina. ¿Qué comando has utilizado? ¿Qué dirección IP tienes?
- Traza la ruta hasta alguna máquina del dominio de ISECOM (Por Ejemplo 193.145.85.201). Identifica las direcciones IPs de los equipos intermedios.

### 2.5.2 Ejercicio 2

Para profundizar sobre los conocimientos adquiridos de Linux.

- Identifica el propietario del fichero "/etc/passwd". ¿Qué comandos has utilizado?
- Crea el directorio "trabajo" en nuestro directorio (por ejemplo, si nuestro login es "milogin", crear el directorio en "/home/milogin"), y copia el fichero "passwd" en el directorio "trabajo" que acabamos de crear. Identifica el propietario del fichero "passwd" que se ha copiado.
- Crea el directorio ".oculto" en el directorio "trabajo". Lista el contenido de nuestro directorio. ¿Cómo podríamos listar el contenido de nuestro directorio de forma que pudiéramos visualizar el directorio ".oculto"?
- Identifica el nombre y la dirección IP de tu máquina. ¿Qué comandos has utilizado? ¿Qué dirección IP tienes?
- Recuerda el escenario de la práctica (apartado 0.1.2) y traza la ruta hasta alguna máquina del dominio de ISECOM (Por Ejemplo 193.145.85.202). Identifica las direcciones IP de los equipos intermedios.





### 2.5.3 Ejercicio 3

Completa la siguiente tabla con los paralelismos entre Windows y Linux. Por ejemplo:

En Linux: comando `--help` es lo mismo que en Windows comando `/h`.

En linux: `cp` (copiar) es lo mismo que en Windows `copy`.

	
comand o -- help	comando /h
cp	copy del
mv	
more	
	print deltree
ls	
cd	
	md
	rd
route	
	tracert
Ping	
	ipconfig



## Glosario

### Dirección IP (IP address):

Es la dirección que identifica a cualquier máquina en Internet. El formato son 4 números, con valores entre 0 y 255, separados por puntos.

Por ejemplo, 10.160.10.240.

### Dominio (Domain):

Es un nombre que identifica una o más direcciones IP. Por ejemplo, el dominio Microsoft.com representa cerca de una docena de direcciones IP. Los nombres de dominio se usan en URLs para identificar determinadas páginas Web. Por ejemplo, en la URL <http://www.pcwebopedia.com/index.html>, el nombre de dominio es pcwebopedia.com.

Cada nombre de dominio tiene un sufijo que indica a qué nivel de dominio superior (TLD, Top Level Domain) pertenece. Este número de sufijos es limitado. Por ejemplo:

- gov – Agencias gubernamentales
- edu – Instituciones Educativas
- org – Organizaciones (no lucrativas)
- com – Negocios comerciales
- net – Organizaciones de Red
- es – España
- ... etc ...

Como Internet está basada en direcciones IP, y no nombres de dominio, cada servidor Web necesita un sistema de nombres de dominio (DNS, Domain Name System) que traduzca los nombres de dominio a direcciones IP.

### MS-DOS (Microsoft Disk Operating System)

El MS-DOS es un sistema operativo. Su objetivo es facilitar la comunicación entre el usuario y el ordenador, y utilizar eficientemente los recursos disponibles, por ejemplo el uso de memoria y CPU.

### Router (encaminador, direccionador, enrutador)

Dispositivo que distribuye tráfico entre redes. Un router está conectado como mínimo a dos redes, generalmente dos LANs (Local Area Network) o WANs (Wide Area Networks) o una LAN y la red del ISP (Internet Service Provider). Los routers se localizan en la pasarela, el lugar donde dos o más redes se conectan.

Los routers usan tablas de encaminamiento para determinar el mejor camino donde dirigir los paquetes IP.



### Sistema Operativo (Operating System – OS):

Un sistema operativo es un programa especial que se ejecuta en un ordenador tras ser encendido y cuya función es gestionar el resto de programas, o aplicaciones, que en él se ejecutarán, como, por ejemplo, un procesador de texto o una hoja de cálculo, o la impresión de un texto en una impresora o una conexión a Internet. El sistema operativo también es responsable de detectar dispositivos hardware y establecer la comunicación entre el usuario y el hardware (teclado, ratón, monitor, etc). Ejemplos de sistemas operativos son: Windows, Linux, UNIX, etc.