

**Ingeniería de Servidores (2014-2015)**  
GRADO EN INGENIERÍA INFORMÁTICA  
UNIVERSIDAD DE GRANADA

---

## Memoria Práctica 2

---

Antonio Javier Cabrera Gutiérrez

17 de noviembre de 2015

## Índice

1. Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes	5
2. ¿Qué ha de hacer para que yum pueda tener acceso a Internet?¿Cómo añadimos un nuevo repositorio?	5
3. Indique el comando para buscar un paquete en un repositorio y el correspondiente para instalarlo	5
4. Indique que ha modificado para que apt pueda acceder a los servidores de paquetes a traves del proxy. ¿Cómo añadimos un nuevo repositorio?	6
5. ¿Que gestores utilizan OpenSuse?	6
6. ¿Que diferencia hay entre Telnet y SSH?	6
7. ¿Para que sirve la opción -X? Ejecute remotamente, es decir, desde la maquina anfitriona o desde la maquina virtual, el comando gedit en una sesión abierta con ssh. ¿Qué ocurre?	7
8. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña	8
9. ¿Qué archivo es el que contiene la configuración de sshd?¿Qué parámetro hay que modificar para evitar que el usuario root acceda?Cambie el puerto por defecto y compruebe que puede acceder	9
10.Indique si es necesario reiniciar el servicio. ¿Cómo se reinicia un servicio en Ubuntu?¿y en CentOS? Muestre la secuencia de comandos para hacerlo.	10
11.Instale y pruebe terminator. Con screen, pruebe su funcionamiento dejando sesiones ssh abiertas en el servidor y recuperándolas posteriormente	10
12.Instale el servicio y pruebe su funcionamiento	12
13.Muestre los comandos que ha utilizado en Ubuntu Server y en CentOS	13
13.1. CentOS . . . . .	13
13.2. Ubuntu Server . . . . .	17
14.Enumere otros servidores web y las paginas de sus proyectos	17
15.Compruebe que el servicio esta funcionando accediendo a la MV a traves de la anfitriona	18

16. Realice la instalacion de MongoDB en alguna de sus maquinas virtuales. Cree una coleccion de documentos y haga una consulta sobre ellos	18
17. Realice la instalacion de uno de estos dos "web containers" pruebe su ejecucion	20
18. Muestre un ejemplo de uso del comando	22
19. Realice la instalación de esta aplicación y pruebe a modificar algún parámetro de algún servicio. Muestre las capturas de pantalla pertinentes así como el proceso de instalación	22
20. Instale phpMyAdmin, indique como lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs mayores a 8MB (limite por defecto). Indique como ha realizado el proceso y muestre capturas de pantalla	25
21. Visite al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando que esta realizando	27
22. Ejecute los ejemplos de find, grep y escriba el script que haga uso de sed para cambiar la configuracion de ssh y reiniciar el servicio.	28
23. Muestre un ejemplo de uso para awk	29
24. Escriba el script para cambiar el acceso a ssh usando PHP o Python	29
25. Abra una consola de PowerShell y pruebe para un programa en ejecucion, realice capturas de pantalla y comente lo que muestra	30

## Índice de figuras

7.1. ssh -X con gedit . . . . .	7
8.1. 1º Paso . . . . .	8
8.2. 2º Paso . . . . .	8
8.3. Comprobación . . . . .	9
9.1. Cambiamos el puerto . . . . .	9
9.2. Comprobación . . . . .	9
10.1. Reiniciar ssh . . . . .	10
11.1. Lista de ventanas screen . . . . .	10
11.2. Screen 0 . . . . .	11
11.3. Screen 1 . . . . .	11
11.4. Pantalla dividida con screen . . . . .	12
12.1. Configuración de fail2ban . . . . .	12

12.2. Conexión baneada de fail2ban . . . . .	13
12.3. IP baneada por fail2ban . . . . .	13
13.1. Instalar apache . . . . .	14
13.2. Comprobación apache . . . . .	14
13.3. Instalación repositorio mysql . . . . .	15
13.4. Habilitar el repositorio . . . . .	15
13.5. Iniciación del servicio y comprobación del estado . . . . .	16
13.6. Instalación php . . . . .	16
13.7. Reinicio de apache . . . . .	16
13.8. Activación de los servicios después del reiniciar la maquina . . . . .	16
13.9. Comprobación . . . . .	17
15.1. Comprobacion de la conexion FTP . . . . .	18
16.1. Muestra del archivo de personas . . . . .	19
16.2. importar el archivo json . . . . .	19
16.3. Inciar MongoDB . . . . .	19
16.4. Consulta en MongoDB . . . . .	20
17.1. Pagina inicial de apache tomcat . . . . .	20
17.2. Pagina de ejemplos . . . . .	21
17.3. Hola Mundo en apache tomcat . . . . .	21
17.4.Codigo Hola Mundo . . . . .	21
18.1. Proceso de parcheado . . . . .	22
18.2. Resultado del parcheado . . . . .	22
19.1. Pantalla inicial de webmin . . . . .	23
19.2. Pagina principal . . . . .	23
19.3. Configuracion de webmin . . . . .	24
19.4. Configuracion webmin . . . . .	24
19.5. Iniciando tareas CRON . . . . .	25
20.1. Inicio de PHPMyAdmin . . . . .	26
20.2. Fichero ph.init . . . . .	26
21.1. Pagina principal de ispconfig . . . . .	27
21.2. Añadir IP . . . . .	28
21.3. Monitor ispconfig . . . . .	28
23.1. Ejemplo awk . . . . .	29
25.1. Get-Process . . . . .	30
25.2. Notepad sin ejecutar . . . . .	30

## 1. Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes

- Instalar: `yum install paquete`
- Buscar: `yum search paquete`
- Eliminar: `yum remove paquete` <sup>1</sup>

## 2. ¿Qué ha de hacer para que yum pueda tener acceso a Internet? ¿Cómo añadimos un nuevo repositorio?

Se debe de acceder al archivo de configuración de yum en `/etc/yum.conf` y en el parámetro de proxy debemos de poner el servidor como una URL incluyendo el puerto. Además si se requiere un nombre de usuario y una contraseña para acceder al servidor se debe de incluir el parámetro `proxy_username` para el nombre de usuario y el parámetro `proxy_password` para la contraseña. <sup>2</sup>

Para agregar repositorios a yum se puede hacer de dos formas:

La primera forma es accediendo al directorio `/etc/yum.repos.d` donde están localizados los ficheros de repositorio de RedHat. Cada uno de estos ficheros maneja los repositorios. Para agregar un repositorio basta con crear un fichero de ese tipo con la estructura deseada, o si ya esta creado y no es esta activado debemos de activarlo cambiando la variable `enabled` a 1.

La segunda forma es a traves de `yum-config-manager`. En la linea de comando se debe de poner `yum-config-manager --add-repo= url del repositorio`. Una vez agregado debemos de activarlo referenciandolo por su nombre a traves de esta orden: `yum-config-manager --enable "nombre del repositorio"`. <sup>3</sup>

## 3. Indique el comando para buscar un paquete en un repositorio y el correspondiente para instalarlo

Para buscar un paquete se hace a traves de `sudo apt-cache search nombre del paquete`.

Para instalarlo se hace a traves de `sudo apt-get install nombre del paquete`. <sup>4</sup>

---

<sup>1</sup>[http://www.linuxtotal.com.mx/index.php?cont=info\\_admon\\_020](http://www.linuxtotal.com.mx/index.php?cont=info_admon_020)

<sup>2</sup>[https://docs.fedoraproject.org/es-ES/Fedora\\_Core/4/html/Software\\_Management\\_Guide/sn-yum-proxy-server.html](https://docs.fedoraproject.org/es-ES/Fedora_Core/4/html/Software_Management_Guide/sn-yum-proxy-server.html)

<sup>3</sup><http://www.elmundoenbits.com/2011/11/como-agregar-un-repositorio-redhat.html>

<sup>4</sup><http://www.ubuntu-guia.com/2011/01/comando-apt-get-en-ubuntu.html>

#### 4. Indique que ha modificado para que apt pueda acceder a los servidores de paquetes a traves del proxy. ¿Cómo añadimos un nuevo repositorio?

Debemos de entrar en `/etc/apt/apt.conf` o en `/etc/apt.conf.d/`.

Si existe el primer directorio debemos de abrirlo y al final agregar lo siguiente:

```
Acquire{  
http{  
Proxy úrl con su puerto al final;  
}  
}
```

Si no existe el primer directorio y si el segundo entonces debemos de crear un archivo individual para guardar la configuración del proxy y dentro ponemos lo mismo que en el anterior.

Si el proxy tuviese autenticación por medio de usuario y contraseña se debería poner en la dirección url por ejemplo asi:

```
"http://usuarioweb:contraseña@192.168.1.254:3128";  
5
```

Para añadir un repositorio podemos proceder de dos formas:

La primera es añadirlo manualmente, para eso editamos el archivo `sources.list`, la segunda es por medio de apt, escribiendo `sudo add-apt-repository ppa: nombre del repositorio`.<sup>6</sup>

#### 5. ¿Que gestores utilizan OpenSuse?

Entre los gestores de paquetes de OpenSuse tenemos Zypper, YaST y Smart.

Zypper es un gestor de paquetes de linea de comandos<sup>7</sup>

YaST es un gestor de paquetes pero con interfaz grafica.<sup>8</sup>

Por ultimo Smart es un programa reciente cuyo objetivo es crear algoritmo inteligentes y portables para resolver de manera adecuada el problema de la administración de paquetes.<sup>9</sup>

#### 6. ¿Que diferencia hay entre Telnet y SSH?

A simple vista telnet (**T**elecommunication **N**etworking) y SSH (**S**ecure **S**hell) son casi lo mismo.

Por lo general Telnet es el puerto 23 y SSH el puerto 22 y para conectarnos necesitamos un nombre y una contraseña y que la maquina a la cual accedemos acepten estos protocolos.<sup>10</sup>

---

<sup>5</sup><http://tuxjm.net/2009/07/23/como-configurar-y-usar-apt-atras-de-un-proxy-http-en-ubuntu-o-debian>

<sup>6</sup>[http://www.guia-ubuntu.com/index.php/Añadir\\_repositorios\\_externos](http://www.guia-ubuntu.com/index.php/Añadir_repositorios_externos)

<sup>7</sup><https://es.opensuse.org/Zypper>

<sup>8</sup>[https://es.opensuse.org/Archive:YaST\\_Gestión\\_de\\_software](https://es.opensuse.org/Archive:YaST_Gestión_de_software)

<sup>9</sup><https://es.opensuse.org/Archive:Smart>

<sup>10</sup><http://blog.evidaliahost.com/2014/11/21/cual-es-la-diferencia-entre-telnet-y-ssh>

Ahora bien, la diferencia fundamental entre ellos es la seguridad, con Telnet todo lo que hagamos remotamente viajara por la red en forma de texto plano y cualquier tercero que pueda estar espiándonos la red puede saber lo que estamos haciendo. El problema es que cuando se diseño Telnet fue ideado para trabajar en redes privadas y los temas de seguridad no fueron tomados con seria importancia.

En cambio SSH introduce cifrado en sus paquetes cosa que lo hace mas seguro en las redes abiertas, además ssh tiene que utilizar una clave publica para su autenticación, esto por ejemplo telnet no lo hace.

Por ultimo cabe mencionar que SSH ha resuelto el problema del ancho de banda, que era un problema mayor cuando las velocidades de Internet eran muy lentas, esto en la actualidad ya no es muy relevante.<sup>11</sup>

## 7. ¿Para que sirve la opción -X? Ejecute remotamente, es decir, desde la maquina anfitriona o desde la maquina virtual, el comando gedit en una sesión abierta con ssh. ¿Qué ocurre?

Si ponemos ssh -X, hacemos que ssh active el reenvío de X11. Esto permite ejecutar una aplicación X remota y mostrarlo a nivel local. Para el reenvío de X11 tanto el cliente como el servidor deben estar configurados correctamente.<sup>12</sup> Como vemos, al ejecutar la orden gedit, una vez conectados con ssh previamente, nos muestra un gedit con su interfaz gráfica.

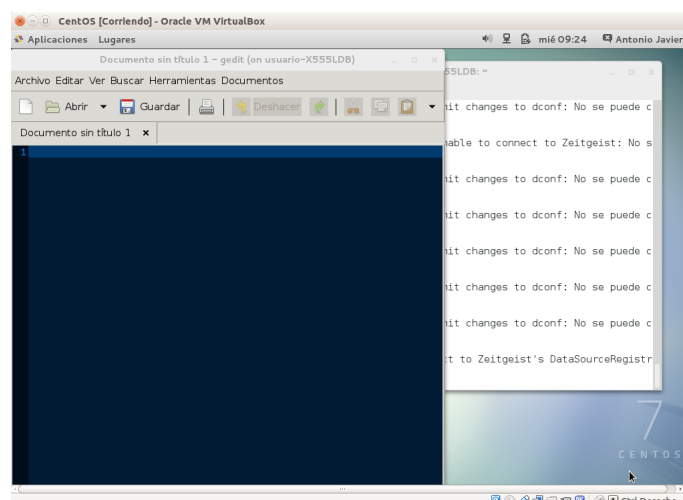


Figura 7.1: ssh -X con gedit

<sup>11</sup><http://www.sivz.com/Diferencia-entre-Telnet-y-SSH-q90231>

<sup>12</sup><http://www.sied.com.ar/2014/02/reenvio-por-x11-a-traves-de-ssh-ejecutar-la-aplicacion-grafica-remota-y-v.html>

## 8. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña

En el primer paso creamos la clave, nos pide el nombre del archivo y una frase de seguridad.

```
usuario@usuario-X555LDB:~/.ssh$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa): miclave
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in miclave.
Your public key has been saved in miclave.pub.
The key fingerprint is:
77:d6:d5:a7:34:79:99:37:e3:6c:4a:fe:d1:d2:4b:16 usuario@usuario-X555LDB
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           .+         |
|          +=*        |
|         oo==       |
|      S . o.oE      |
|       . oo o.o     |
|        o.+o       |
|         +.o        |
|          o         |
+-----+
usuario@usuario-X555LDB:~/.ssh$ ls
authorized_keys  known_hosts  miclave  miclave.pub
```

Figura 8.1: 1º Paso

Ahora las claves generadas las cambiamos al directorio .ssh, con ssh-copy-id copiamos la clave publica al servidor, probamos conectarnos y solo nos pide la frase de seguridad y se conecta.

```
usuario@usuario-X555LDB:~$ ssh-copy-id -t .ssh/miclave.pub ajavier@192.168.56.101
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
ajavier@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'ajavier@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.

usuario@usuario-X555LDB:~$ ssh ajavier@192.168.56.101
Last login: Tue Nov  3 13:47:03 2015 from 192.168.56.1
[ajavier@localhost ~]$ exit
logout
Connection to 192.168.56.101 closed.
```

Figura 8.2: 2º Paso



Para ver las claves autorizadas que acepta el servidor miramos en authorized-keys y nos sale la nuestra.

```
[ajavier@localhost .ssh]$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCM+suoZxhPFne4BNiT6F1by1qG/Wqu9LSyE+vc95jwCt4TnTjnT5SQZN4WntZv5cAZ+4ee5Ch
oKqXqDsrxQ12aaQ4RopV4XVpM/WZipAYkcz/2J7I74lRKsTquJxBkd5H18Gn7q0XMkKGz4u4L7D2zZJVbc1r2XMUdiTB9/LRAxnyWbfekXmz8qKR
+XoDQlQs68emZ74FDfioxx6VHR0+NgRtRWA+NV8HQfGWhJouMk93oTgoDBDj0Q1LaktBLZ4SZgoSaeFf06mhbz9RMuVidS1oVy90AbHnc35/7/aF
CXvtFT3BGBcJxHoqVWvuRctAKYALLL610moDkxEa3AwN usuario@usuario-X555LDB
```

Figura 8.3: Comprobación

Por el ultimo el tema de los permisos es muy importante. Para que funcione, los permisos del HOME deben de ser 700 o 755, no funciona con 770 o similar. Es decir, solo el propietario del HOME puede hacer la conexión. También el HOME/.ssh debe tener permisos 700. Y, por ultimo el fichero authorized\_keys no puede tener permisos de escritura para grupo no para otros. En mi caso lo tengo en -rw———. <sup>13</sup>

## 9. ¿Qué archivo es el que contiene la configuración de sshd? ¿Qué parámetro hay que modificar para evitar que el usuario root acceda? Cambie el puerto por defecto y compruebe que puede acceder

El archivo se llama sshd\_config y se encuentra en /etc/ssh/

El parámetro PermitRootLogin

El puerto por defecto es el 22. cambiemoslo al 69.

```
Port 69
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Figura 9.1: Cambiamos el puerto

```
usuario@usuario-X555LDB:~$ ssh ajavier@192.168.56.101
Last login: Tue Nov 3 14:07:37 2015 from 192.168.56.1
[ajavier@localhost ~]$
```

Figura 9.2: Comprobación

<sup>13</sup><http://blog-alexis.rhcloud.com/2011/06/26/ssh-copy-id-la-vida-un-poco-mas-facil/>

## 10. Indique si es necesario reiniciar el servicio. ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.

Cuando cambiamos el puerto debemos de reiniciar el servicio para ello si utilizamos Ubuntu se hace de la siguiente forma: escribimos `/etc/init.d/ssh restart` o `service sshd restart`, en CentOS también lo podemos hacer con `service sshd restart`.<sup>14</sup>

```
[ajavier@localhost ~]$ sudo service sshd restart
[sudo] password for ajavier:
Redirecting to /bin/systemctl restart  sshd.service
```

Figura 10.1: Reiniciar ssh

## 11. Instale y pruebe terminator. Con screen, pruebe su funcionamiento dejando sesiones ssh abiertas en el servidor y recuperándolas posteriormente

Con screen podemos crear sesiones en la terminal y trabajar con ellas, entonces para crear una sesión ponemos `screen -S` y el nombre, para hacer algo en screen se hace a partir de `CTRL+a`, para crear una ventana usamos `CTRL+a` y soltamos y le damos a la `c`, si le damos a `CTRL+a` y `"` nos sale una lista de las ventanas abiertas.

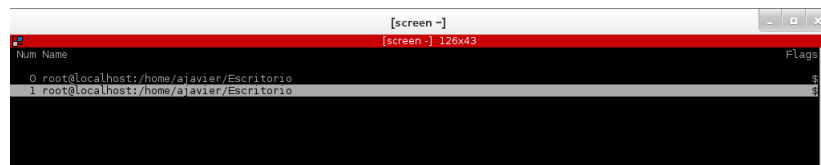


Figura 11.1: Lista de ventanas screen

Se puede ver que tenemos dos. Con `CTRL+a` y `0` se nos pone la ventana 0, y con `CTRL+a` y `1` se nos pone la ventana 1.

<sup>14</sup><https://wiki.centos.org/es/HowTos/Network/SecuringSSH>



Figura 11.2: Screen 0

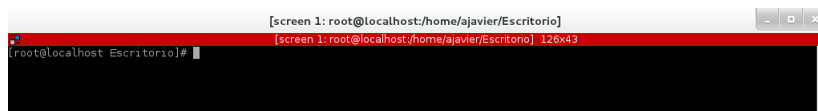
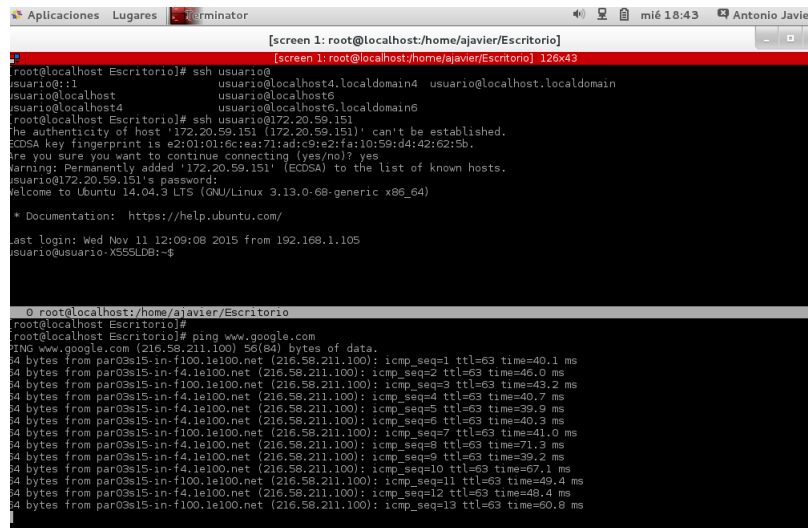


Figura 11.3: Screen 1

Si queremos trabajar con las dos a la vez, usamos CTRL+a y SHIFT+S y nos aparece una pantalla en la que abajo tenemos que poner la ventana que queremos. Si arriba tenemos la 1, abajo ponemos la 0. Nos podemos ir moviendo por ellas a través de CTRL+a y TAB.



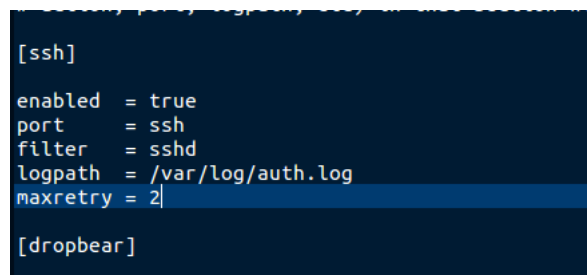
```
[screen 1: root@localhost/home/ajavier/Escritorio] 126x43
root@localhost Escritorio# ssh usuario@172.20.59.151
usuario@172.20.59.151:~$
usuario@172.20.59.151:~$ ping www.google.com
PING www.google.com (216.58.211.100) 56(84) bytes of data:
64 bytes from par03s15-in-f100.1e100.net (216.58.211.100): icmp_seq=1 ttl=63 time=40.1 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=2 ttl=63 time=46.0 ms
64 bytes from par03s15-in-f100.1e100.net (216.58.211.100): icmp_seq=3 ttl=63 time=45.2 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=4 ttl=63 time=40.7 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=5 ttl=63 time=39.9 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=6 ttl=63 time=40.3 ms
64 bytes from par03s15-in-f100.1e100.net (216.58.211.100): icmp_seq=7 ttl=63 time=41.0 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=8 ttl=63 time=71.3 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=9 ttl=63 time=39.2 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=10 ttl=63 time=67.1 ms
64 bytes from par03s15-in-f100.1e100.net (216.58.211.100): icmp_seq=11 ttl=63 time=49.4 ms
64 bytes from par03s15-in-f4.1e100.net (216.58.211.100): icmp_seq=12 ttl=63 time=48.4 ms
64 bytes from par03s15-in-f100.1e100.net (216.58.211.100): icmp_seq=13 ttl=63 time=60.8 ms
```

Figura 11.4: Pantalla dividida con screen

Como se puede ver abajo tenemos una sesión haciendo ping y arriba otra usando ssh.<sup>15</sup>

## 12. Instale el servicio y pruebe su funcionamiento

fail2ban es una herramienta para banear a usuarios que se intenten conectar de forma errónea, yo lo he instalado en ubuntu, para ello hay que escribir `sudo apt-get install fail2ban`. una vez instalado accedemos a su archivo de configuración en `/etc/fail2ban/jail.conf` y donde pone `[ssh]` en el apartado de `maxretry` he puesto 2, osea esto es el numero de intentos de poner bien la contraseña.



```
[ssh]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 2

[dropbear]
```

Figura 12.1: Configuración de fail2ban

Ahora desde ubuntu server he accedido a mi portátil y he escrito dos veces mal la contraseña, a la segunda vez se queda como colgado, si pruebo a conectarme otra vez pasa lo mismo, se queda colgado, utilizando `-v -v -v` como en la imagen de abajo se puede ver se muestra el proceso de conexión que se queda pillado.

<sup>15</sup><https://phenobarbital.wordpress.com/2013/02/18/linux-usando-gnu-screen/>

```

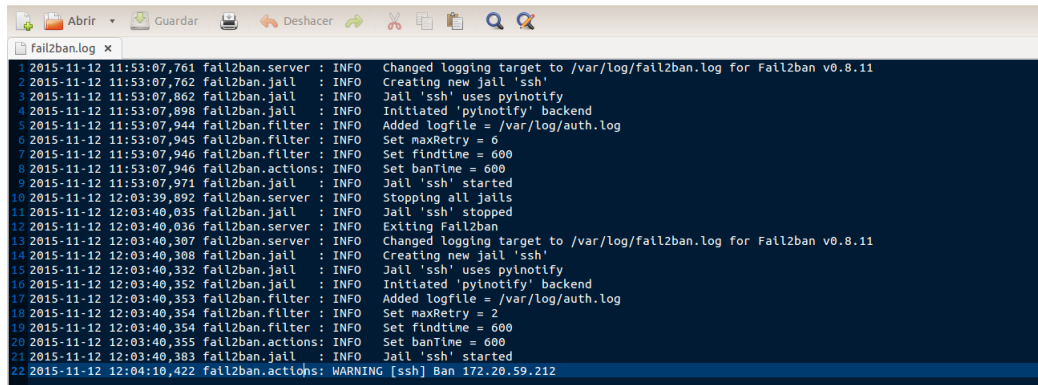
antonio@ubuntu:~$ ssh usuario@172.20.59.212
usuario@172.20.59.212's password:
Permission denied, please try again.
usuario@172.20.59.212's password:

^C
antonio@ubuntu:~$ ssh usuario@172.20.59.212
^C
antonio@ubuntu:~$ ssh usuario@172.20.59.212 -v -v -v
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug2: ssh_connect: needpriv 0
debug1: Connecting to 172.20.59.212 [172.20.59.212] port 22.

```

Figura 12.2: Conexión baneada de fail2ban

Para ver que ocurre nos metemos en el .log de fail2ban, en /var/log/fail2ban.log y vemos que nuestra IP esta baneada



```

1 2015-11-12 11:53:07,761 fail2ban.server : INFO Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.11
2 2015-11-12 11:53:07,762 fail2ban.jail : INFO Creating new jail 'ssh'
3 2015-11-12 11:53:07,862 fail2ban.jail : INFO Jail 'ssh' uses pyinotify
4 2015-11-12 11:53:07,898 fail2ban.jail : INFO Initiated 'pyinotify' backend
5 2015-11-12 11:53:07,944 fail2ban.filter : INFO Added logfile = /var/log/auth.log
6 2015-11-12 11:53:07,945 fail2ban.filter : INFO Set maxRetry = 0
7 2015-11-12 11:53:07,946 fail2ban.filter : INFO Set findtime = 600
8 2015-11-12 11:53:07,946 fail2ban.actions : INFO Set banTime = 600
9 2015-11-12 11:53:07,971 fail2ban.jail : INFO Jail 'ssh' started
10 2015-11-12 12:03:39,892 fail2ban.server : INFO Stopping all jails
11 2015-11-12 12:03:40,035 fail2ban.jail : INFO Jail 'ssh' stopped
12 2015-11-12 12:03:40,036 fail2ban.server : INFO Exiting Fail2ban
13 2015-11-12 12:03:40,367 fail2ban.server : INFO Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.11
14 2015-11-12 12:03:40,368 fail2ban.jail : INFO Creating new jail 'ssh'
15 2015-11-12 12:03:40,392 fail2ban.jail : INFO Jail 'ssh' uses pyinotify
16 2015-11-12 12:03:40,352 fail2ban.jail : INFO Initiated 'pyinotify' backend
17 2015-11-12 12:03:40,353 fail2ban.filter : INFO Added logfile = /var/log/auth.log
18 2015-11-12 12:03:40,354 fail2ban.filter : INFO Set maxRetry = 2
19 2015-11-12 12:03:40,354 fail2ban.filter : INFO Set findtime = 600
20 2015-11-12 12:03:40,355 fail2ban.actions : INFO Set banTime = 600
21 2015-11-12 12:03:40,383 fail2ban.jail : INFO Jail 'ssh' started
22 2015-11-12 12:04:10,422 fail2ban.actions : WARNING [ssh] Ban 172.20.59.212

```

Figura 12.3: IP baneada por fail2ban

En este caso el tiempo de baneo es de 600 segundos, en 600 segundos podre volver a conectarme, pero eso si, poniendo bien la contraseña.

## 13. Muestre los comandos que ha utilizado en Ubuntu Server y en CentOS

### 13.1. CentOS

Primero instalamos Apache: yum install httpd, iniciamos con service httpd start, comprobamos que funciona abriendo nuestro navegador y poniendo localhost. Tarda lo suyo en instalarse.

```
[ajavier@localhost ~]$ sudo yum install httpd
[sudo] password for ajavier:
Complementos cargados:fastestmirror, langpacks
Bloqueo existente en /var/run/yum.pid: otra copia se encuentra en ejecución como
pid 13700.
Another app is currently holding the yum lock; waiting for it to exit...
La otra aplicación es: PackageKit
Memoria : 96 M RSS (811 MB VSZ)
Iniciado: Tue Nov 3 15:55:56 2015 - 02:01 atrás
Estado : Ejecutando. pid: 13700
```

Figura 13.1: Instalar apache

Se puede ver que funciona:

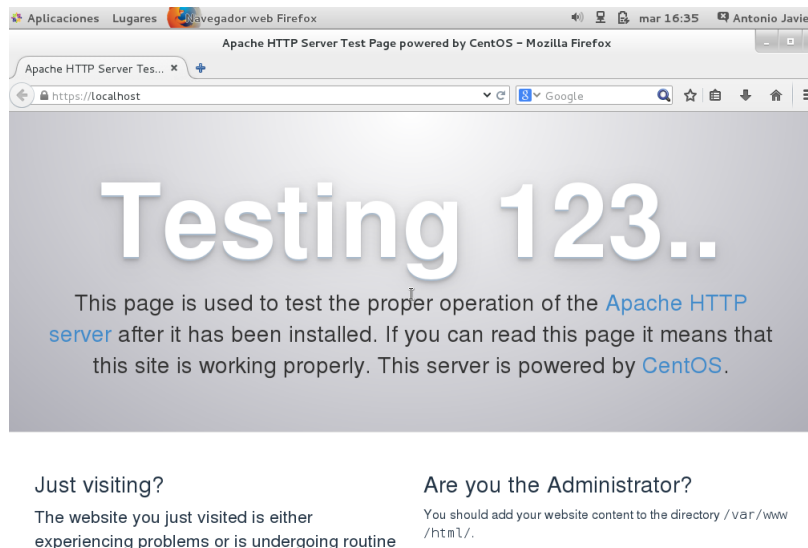


Figura 13.2: Comprobación apache

A continuación instalamos mysql, en este caso al usar CentOS 7 hay que añadir el repositorio

```
[ajavier@localhost ~]$ sudo yum install http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
Complementos cargados:fastestmirror, langpacks
mysql-community-release-el7-5.noarch.rpm | 6.0 kB 00:00
Examinando /var/tmp/yum-root-PRzpo8/mysql-community-release-el7-5.noarch.rpm: mysql-community-release-el7-5.noarch
Marcando /var/tmp/yum-root-PRzpo8/mysql-community-release-el7-5.noarch.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete mysql-community-release.noarch 0:el7-5 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

I

=====
Package Architecture Version Repositorio Tamaño
=====
Instalando:
mysql-community-release
noarch el7-5 /mysql-community-release-el7-5.noarch 4.3 k

Resumen de la transacción
=====
Instalar 1 Paquete
```

Figura 13.3: Instalación repositorio mysql

Procedemos a habilitar el repositorio y a continuación instalamos:

```
[ajavier@localhost ~]$ sudo yum repolist enabled | grep "mysql.*-community.*"
mysql-connectors-community/x86_64 MySQL Connectors Community 17
mysql-tools-community/x86_64 MySQL Tools Community 27
mysql56-community/x86_64 MySQL 5.6 Community Server 184

[ajavier@localhost ~]$ sudo yum install mysql-community-server
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: ftp.cica.es
* extras: ftp.cica.es
* updates: ftp.cica.es
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete mysql-community-server.x86_64 0:5.6.27-2.el7 debe ser instalado
--> Procesando dependencias: mysql-community-common(x86-64) = 5.6.27-2.el7 para el paquete: mysql-community-server-5.6.27-2.el7.x86_64
--> Procesando dependencias: mysql-community-client(x86-64) = 5.6.27-2.el7 para el paquete: mysql-community-server-5.6.27-2.el7.x86_64
--> Ejecutando prueba de transacción
--> Paquete mariadb.x86_64 1:5.5.44-1.el7_1 debe ser obsoleto
--> Paquete mysql-community-client.x86_64 0:5.6.27-2.el7 debe ser obsoleto
--> Procesando dependencias: mysql-community-libs(x86-64) = 5.6.27-2.el7 para el paquete: mysql-community-client-5.6.27-2.el7.x86_64
--> Paquete mysql-community-common.x86_64 0:5.6.27-2.el7 debe ser instalado
--> Ejecutando prueba de transacción
--> Paquete mariadb-libs.x86_64 1:5.5.44-1.el7_1 debe ser obsoleto
--> Paquete mysql-community-libs.x86_64 0:5.6.27-2.el7 debe ser obsoleto
--> Resolución de dependencias finalizada

Dependencias resueltas
```

Figura 13.4: Habilitar el repositorio

Iniciamos el servicio y miramos su estado:

```
[ajavier@localhost ~]$ sudo service mysqld start
Redirecting to /bin/systemctl start mysqld.service
[ajavier@localhost ~]$ sudo systemctl status mysqld
mysqld.service - MySQL Community Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled)
   Active: active (running) since jue 2015-11-05 11:25:57 CET; 2s ago
     Process: 6185 ExecStartPost=/usr/bin/mysql-systemd-start post (code=exited, status=0/SUCCESS)
   Process: 6126 ExecStartPre=/usr/bin/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
    Main PID: 6184 (mysqld_safe)
      CGroup: /system.slice/mysqld.service
              └─6184 /bin/sh /usr/bin/mysqld_safe
                  └─6333 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --...
```

```
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: Support MySQL...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: Note: new de...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: Please make ...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: WARNING: Def...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: This file wi...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: If you do no...
nov 05 11:25:56 localhost.localdomain mysql-systemd-start[6126]: --defaults-f...
nov 05 11:25:56 localhost.localdomain mysqld_safe[6184]: 151105 11:25:56 mysq...
nov 05 11:25:56 localhost.localdomain mysqld_safe[6184]: 151105 11:25:56 mysq...
nov 05 11:25:57 localhost.localdomain systemd[1]: Started MySQL Community Ser...
Hint: Some lines were ellipsized, use -l to show in full.
```

Figura 13.5: Iniciación del servicio y comprobación del estado

A continuación instalamos php:

```
[ajavier@localhost ~]$ sudo yum install -y php php-mysql pgp-gd php-mbstring
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.cica.es
 * extras: ftp.cica.es
 * updates: ftp.cica.es
El paquete php-5.4.16-36.el7_1.x86_64 ya se encuentra instalado con su versión m
ás reciente
No existe disponible ningún paquete pgp-gd.
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete php-mbstring.x86_64 0:5.4.16-36.el7_1 debe ser instalado
--> Paquete php-mysql.x86_64 0:5.4.16-36.el7_1 debe ser instalado
--> Resolución de dependencias finalizada
Dependencias resueltas
```

Package	Arquitectura	Versión	Repositorio	Tamaño
Instalando:				
php-mbstring	x86_64	5.4.16-36.el7_1	updates	503 k
php-mysql	x86_64	5.4.16-36.el7_1	updates	99 k

Figura 13.6: Instalación php

Una vez instalado reiniciamos apache.

```
[ajavier@localhost ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
```

Figura 13.7: Reinicio de apache

Ponemos lo siguiente para que cuando se reinicie la maquina se activen los servicios, utilizamos los siguientes comandos:

```
[ajavier@localhost ~]$ sudo chkconfig httpd on && sudo chkconfig mysqld on
Nota: Reenviando petición a 'systemctl enable httpd.service'.
Nota: Reenviando petición a 'systemctl enable mysqld.service'.
```

Figura 13.8: Activación de los servicios después del reiniciar la maquina

Por ultimo para ver que todo funciona creamos un archivo php llamado phpinfo.php por ejemplo en /www/html y lo abrimos con firefox localhost/phpinfo.php





Figura 13.9: Comprobación

## 13.2. Ubuntu Server

Ahora procedemos a la instalación en ubuntu server Instalamos apache con `sudo apt-get install apache2`.

Procedemos a instalar php con `sudo apt-get install php5 libapache2-mod-php5 php5-cli php5-mysql`.

Por ultimo instalamos mysql `sudo apt-get install mysql-server mysql-client libmysqlclient-dev`<sup>16</sup>

## 14. Enumere otros servidores web y las paginas de sus proyectos

- Cherokee: <http://cherokee-project.com/>
- Lighttpd: <http://www.lighttpd.net/>
- Thttpd: <http://www.acme.com/software/thttpd/>
- jetty: <http://www.eclipse.org/jetty/>

<sup>16</sup><http://blog.desdelinux.net/como-instalar-lamp-en-ubuntu/>

## 15. Compruebe que el servicio esta funcionando accediendo a la MV a traves de la anfitrióna

Se puede ver que la conexión se ha hecho, ya que en sesiones actuales de FTP de Windows nos sale la nuestra, nos pide el usuario y la contraseña como se puede ver en la imagen.

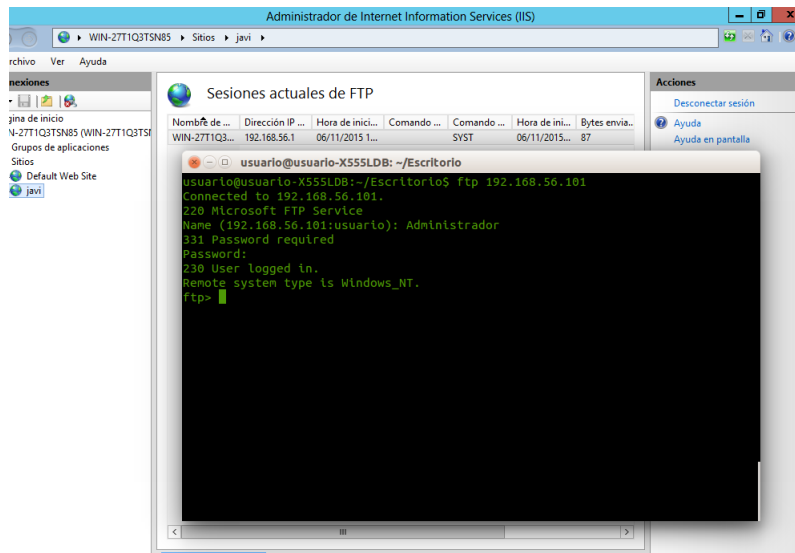


Figura 15.1: Comprobacion de la conexion FTP

## 16. Realice la instalación de MongoDB en alguna de sus máquinas virtuales. Cree una colección de documentos y haga una consulta sobre ellos

He instalado MongoDB en CentOS, para su instalación hay que añadir el repositorio, para esto, hacemos `sudo gedit /etc/yum.repos.d/mongodb.repo` y dentro copiamos lo siguiente

```
[mongodb]
name=MongoDB Repository
baseurl=http://downloads-distro.mongodb.org/repo/redhat/os/x86_64/
gpgcheck=0
enabled=1
```

Hacemos el update e instalamos mongo: `sudo yum -y install mongodb-org mongodb-org-server` Iniciamos el sistema con `systemctl start mongod`<sup>17</sup> Ahora debemos de importar un archivo y crear la base de datos. Yo me he descargado un json de Internet donde hay muchas personas con sus datos.

<sup>17</sup><http://www.liquidweb.com/kb/how-to-install-mongodb-on-centos-7/>

```

17434 {
17435   "isActive": true,
17436   "balance": "$1,125.00",
17437   "picture": "http://placehold.it/32x32",
17438   "age": 40,
17439   "name": "Sophie Gibbs",
17440   "company": "Keytheon",
17441   "phone": "851-419-34828",
17442   "email": "sophie@keytheon.com",
17443   "address": "21804, Carrollton, Lafayette Streets",
17444   "about": "Excepteur occaecat proident sint cupidatat veniam sint laborum do do nostrud irure nisl. Anim tempor elit etusmod
fugiat aliquip ad et tempor mollit cupidatat excepteur. Anim aliqua cupidatat amet deserunt qui magna exercitation reprehenderit aliqua
dolor mollit non pariatur ex. Nostrud reprehenderit enim dolor elit ut quis excepteur ad in nulla incididunt non. Elit enim non elit
dolore incididunt excepteur deserunt labore commodo aliqua.\r\n",
17445   "registered": "1994-12-27T10:45:24 -01:00",
17446   "latitude": -88,
17447   "tags": [
17448     "aliqua",
17449     "non",
17450     "ullamco",
17451     "fugiat",
17452     "laboris",
17453     "nulla",
17454     "occaecat"
17455   ],
17456   "friends": [
17457     {
17458       "id": 1,
17459       "name": "Alexandra Daniels"
17460     },
17461     {
17462       "id": 2,
17463       "name": "Genesis Timmons"
17464     },
17465   ]

```

Figura 16.1: Muestra del archivo de personas

Ahora para incorporarlo a la base datos escribimos los siguiente en la terminal

```

[root@localhost ajavier]# mongoimport --host localhost --port 27017 --db test --
collection people --file /home/ajavier/Descargas/mongodb-consultas.json --jsonAr
ray

```

Figura 16.2: importar el archivo json

Con `--host` le decimos donde esta el archivo con `--port` el puerto, en este caso mongodb usa 27017, que es el de por defecto con `-db` creamos la base de datos que se llama test, con `--collection` creamos la colección que se llamara people y con `--file` ponemos la ruta del archivo.

Iniciamos mongoDB y le indicamos que queremos usar la base de datos test

```

[root@localhost ajavier]# mongo localhost:27017
MongoDB shell version: 2.6.11
connecting to: localhost:27017/test
Server has startup warnings:
2015-11-13T11:06:57.037+0100 [initandlisten] ** WARNING: Readahead for /var/lib/
2015-11-13T11:06:57.037+0100 [initandlisten] ** mongo is set to 4096KB
2015-11-13T11:06:57.037+0100 [initandlisten] ** We suggest setting it t
2015-11-13T11:06:57.037+0100 [initandlisten] ** o 256KB (512 sectors) or less
2015-11-13T11:06:57.037+0100 [initandlisten] ** http://dochub.mongodb.o
rg/core/readahead
> use test
switched to db test
>

```

Figura 16.3: Iniciar MongoDB

Ahora procedemos a hacer una consulta por ejemplo esta:

```
> db.people.find({age:34,isActive:true},{name:1,age:1,isActive:1,_id:0}).pretty
{
  "isActive" : true, "age" : 34, "name" : "Julia Young" }
{
  "isActive" : true, "age" : 34, "name" : "Mackenzie Clapton" }
{
  "isActive" : true, "age" : 34, "name" : "Destiny Calhoun" }
{
  "isActive" : true, "age" : 34, "name" : "Amelia Carroll" }
{
  "isActive" : true, "age" : 34, "name" : "Lauren Hailey" }
{
  "isActive" : true, "age" : 34, "name" : "Molly Chapman" }
{
  "isActive" : true, "age" : 34, "name" : "Leah Timmons" }
>
```

Figura 16.4: Consulta en MongoDB

En esta consulta estamos buscando personas cuya edad sea 34 y sean activas, y filtramos por nombre, edad y si son activas.<sup>18</sup>

## 17. Realice la instalación de uno de estos dos web containers y pruebe su ejecución

Para instalarlo debemos de hacer *sudo yum install tomcat*. Instalamos los paquetes de administrador con *sudo yum install tomcat-webapps tomcat-admin-webapps*. Iniciamos tomcat con *sudo systemctl start tomcat* y accedemos a traves de localhost:8080.<sup>19</sup> Una vez dentro nos aparece esta pantalla

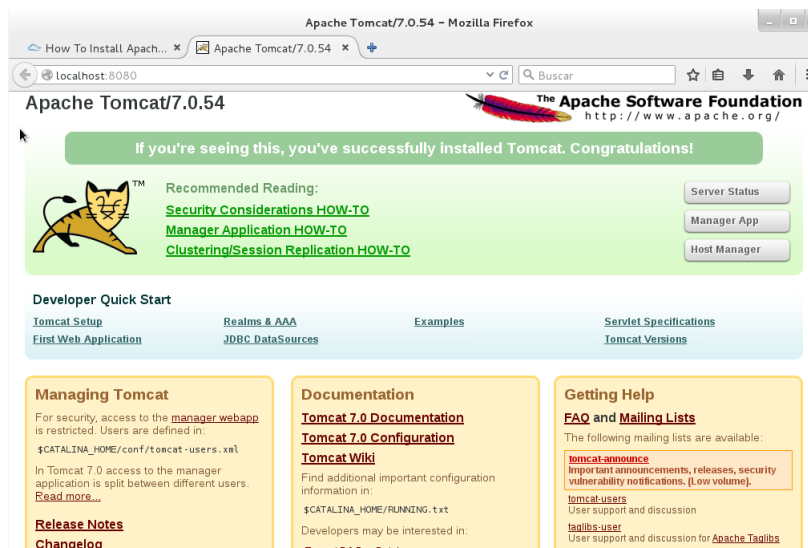


Figura 17.1: Pagina inicial de apache tomcat

Podemos ir probando cosas. Yo he ido al apartado de ejemplos.

<sup>18</sup><http://www.charlascylon.com/post/61794340001/tutorial-mongodb-operaciones-de-consulta>

<sup>19</sup><https://www.digitalocean.com/community/tutorials/how-to-install-apache-tomcat-7-on-centos-7-via-yum>

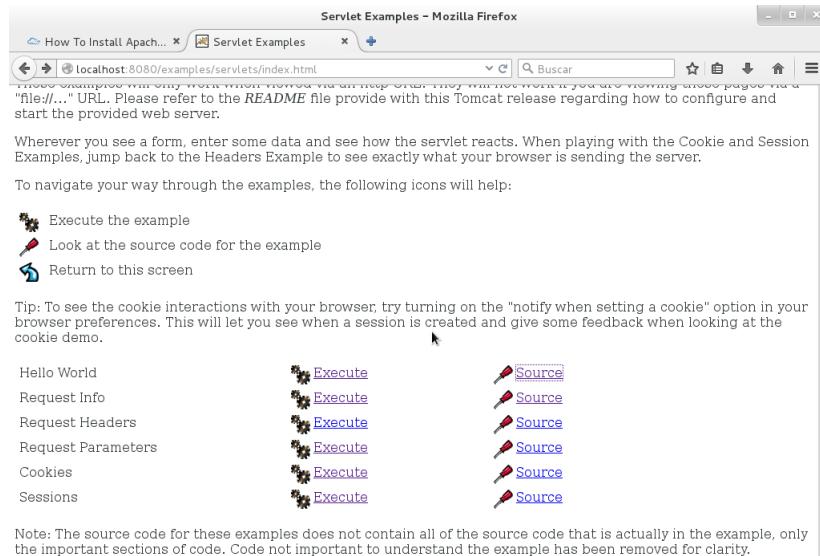


Figura 17.2: Pagina de ejemplos

Ahí le he dado al programa de Hola mundo que muestra hola mundo en la pantalla.

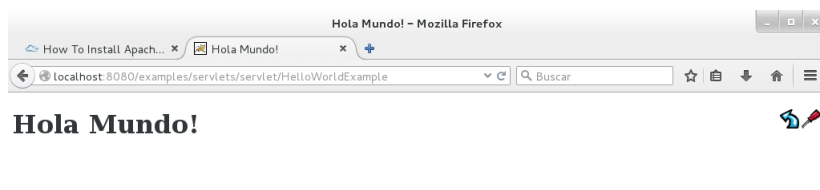


Figura 17.3: Hola Mundo en apache tomcat

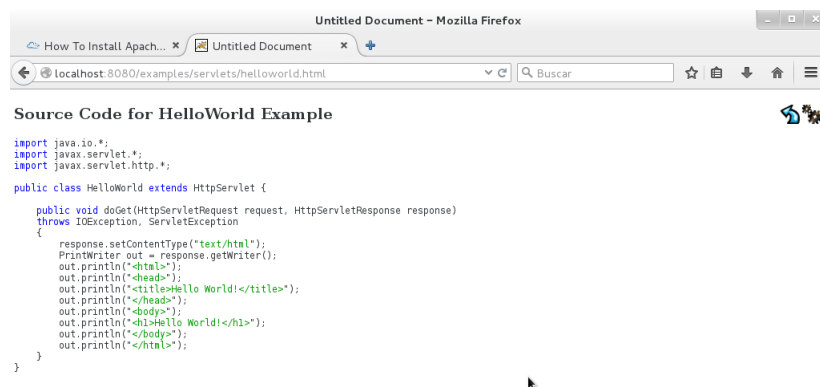


Figura 17.4: Código Hola Mundo

## 18. Muestre un ejemplo de uso del comando

Vamos a hacer un ejemplo. Creamos dos documentos, `viejo.txt` cuyo contenido es "hoy es lunes", y otro fichero donde su contenido es "hoy es martes".

Ahora bien, usando la orden `diff` para crear un fichero con las diferencias que hay entre esos dos ficheros. Ahora creamos un fichero que sera el que parchearemos, en el escribimos, "hoy es lunes me gusta jugar al fútbol, etc."<sup>20</sup> entonces al parchearlo encontrara la frase hoy es lunes y la cambiara por hoy es martes. <sup>20</sup>

```
usuario@usuario-X555LDB:~/Escritorio$ diff -u viejo.txt nuevo.txt > file.patch
usuario@usuario-X555LDB:~/Escritorio$ patch resultado.txt < file.patch
patching file resultado.txt
```

Figura 18.1: Proceso de parcheado

```
usuario@usuario-X555LDB:~/Escritorio$ cat resultado.txt
hoy es martes me gusta el fútbol tengo 22 años soy español
usuario@usuario-X555LDB:~/Escritorio$ █
```

Figura 18.2: Resultado del parcheado

## 19. Realice la instalación de esta aplicación y pruebe a modificar algún parámetro de algún servicio. Muestre las capturas de pantalla pertinentes así como el proceso de instalación

Para instalarlo empezamos abriendo el siguiente archivo: `sudo gedit /etc/yum.repos.d/webmin.repo`. Una vez abierto escribimos lo siguiente:

```
[Webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```

Seguidamente hacemos:

`rpm --import http://www.webmin.com/jcameron-key.asc` Actualizamos los repositorios con `yum check-update`. Instalamos webmin con `sudo yum install webmin -y`. Por ultimo ponemos `sudo chkconfig webmin on` y `sudo service webmin start` para iniciar el servicio. Ahora abrimos el puerto, webmin usa el 10000. `sudo firewall-cmd --add-port=10000/tcp`<sup>21</sup> Se nos abre esta ventana.

<sup>20</sup><http://redes-privadas-virtuales.blogspot.com.es/2010/01/creacion-y-aplicacion-de-parches-con.html>

<sup>21</sup><http://lintut.com/how-to-install-webmin-on-centos-7/>

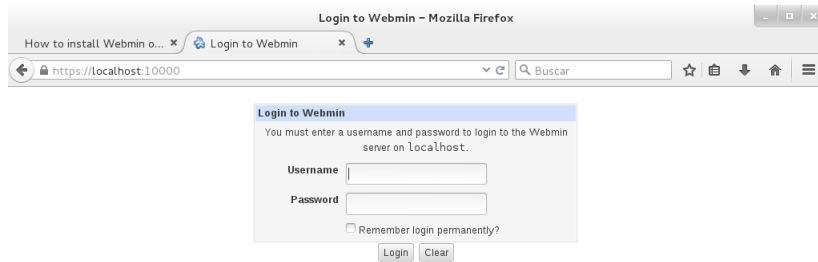


Figura 19.1: Pantalla inicial de webmin

Ponemos ahora el usuario root y la contraseña y entramos a la pagina principal.

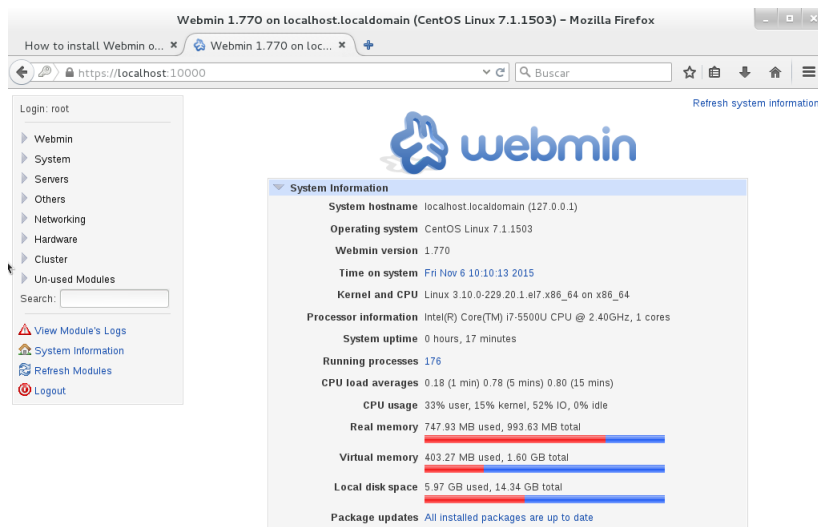


Figura 19.2: Pagina principal

Nos metemos en la pantalla de configuración de webmin.

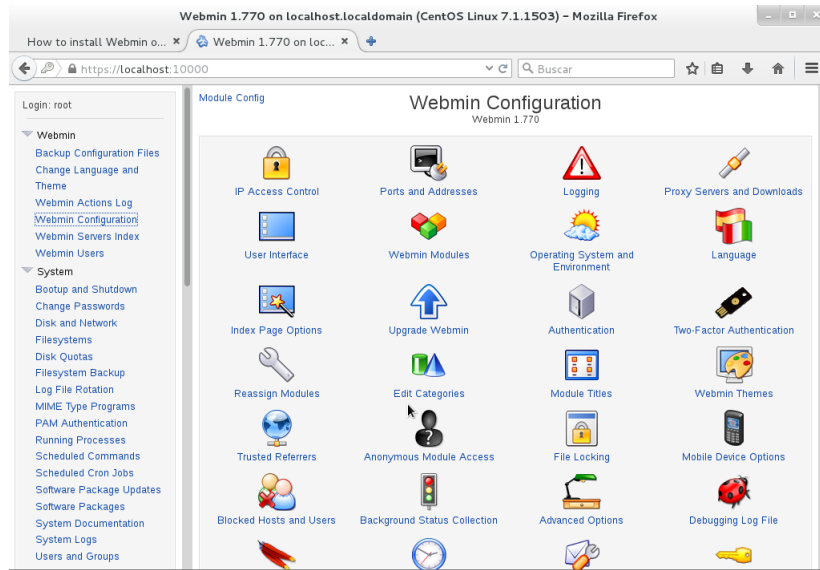


Figura 19.3: Configuración de webmin

Entre otras cosas podemos modificar los puertos, en este caso he cambiado el puerto 10000 por el 6969

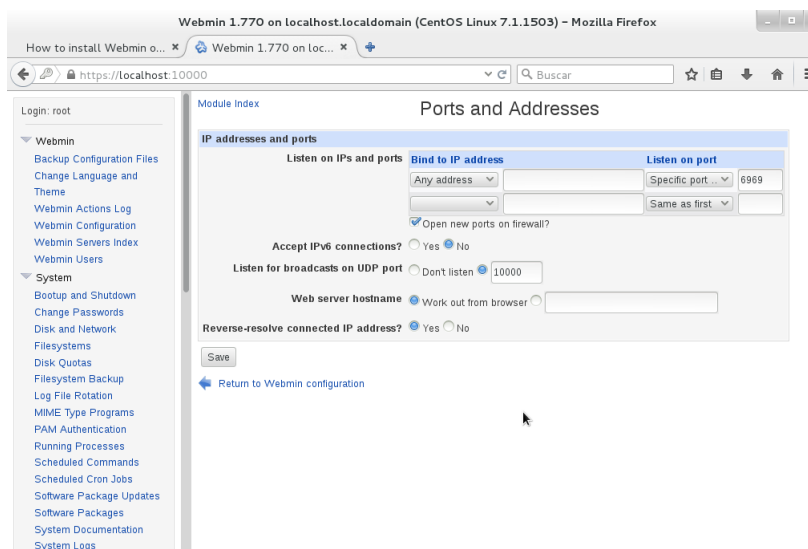


Figura 19.4: Configuración webmin

También hemos programado dos tareas con CRON



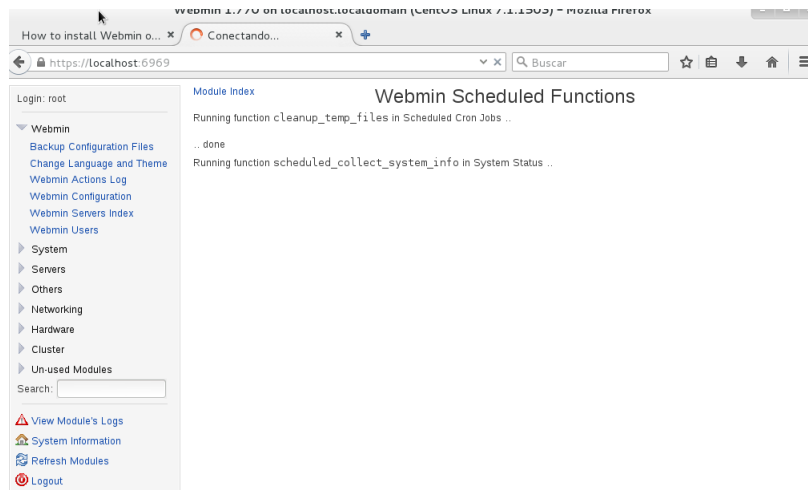


Figura 19.5: Iniciando tareas CRON

## 20. Instale phpMyAdmin, indique como lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs mayores a 8MB (limite por defecto). Indique como ha realizado el proceso y muestre capturas de pantalla

Para instalarlo primero debemos añadir el repositorio con `rpm -iUvh http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm`. Actualizamos con `sudo yum -y update` e instalamos phpmyadmin con `sudo yum -y install phpmyadmin`.

Por ultimo reiniciamos apache. Abrimos phpmyadmin poniendo en el navegador `localhost/phpmyadmin`. Se nos debe de abrir esta pantalla.<sup>22</sup>

<sup>22</sup><http://www.liquidweb.com/kb/how-to-install-and-configure-phpmyadmin-on-centos-7/>

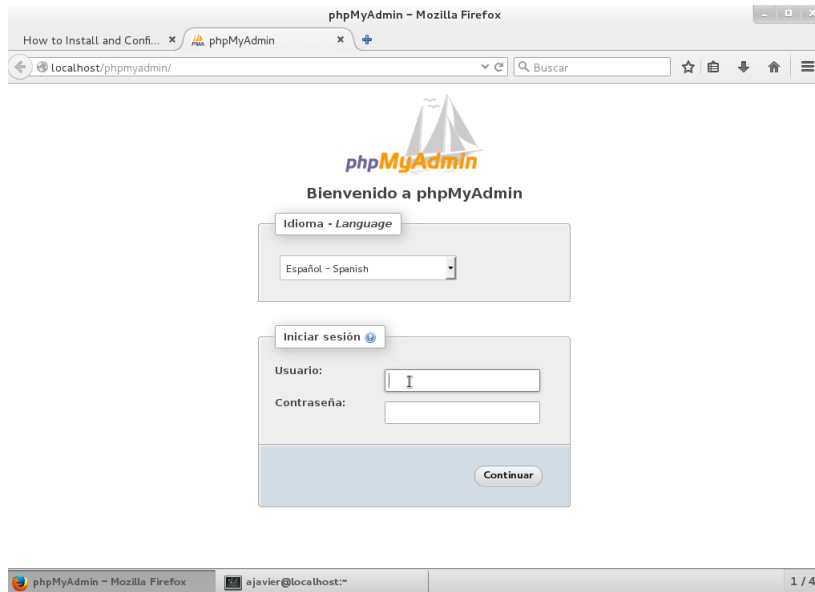


Figura 20.1: Inicio de PHPMyAdmin

Ahora cambiamos el limite por defecto de los 8M. Para ello debemos de acceder al fichero php.ini, y la variable post\_max\_size cambiamos el valor.

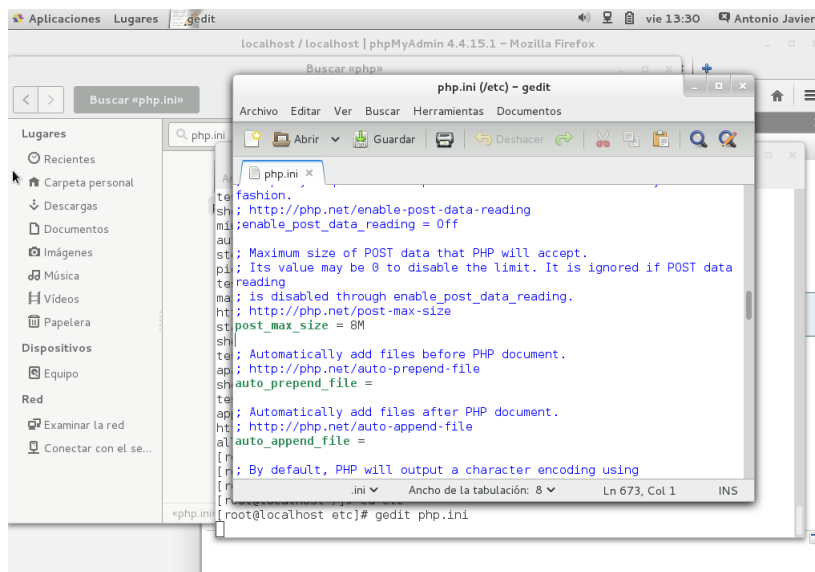


Figura 20.2: Fichero ph.init

## 21. Visite al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando que esta realizando

He probado la demo de ispconfig, ellos te ofrecen una contraseña y un usuario para poder probarla. Una vez dentro nos sale esto:

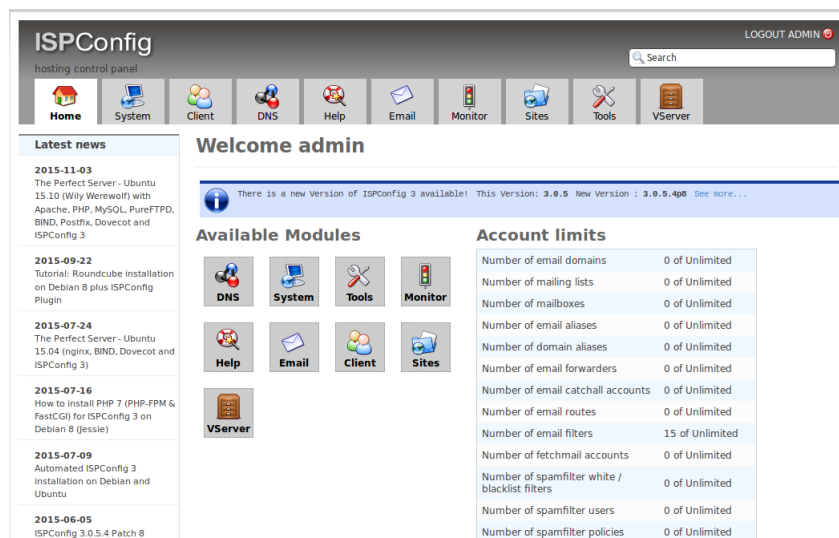


Figura 21.1: Pagina principal de ispconfig

Tambien he añadido una IP

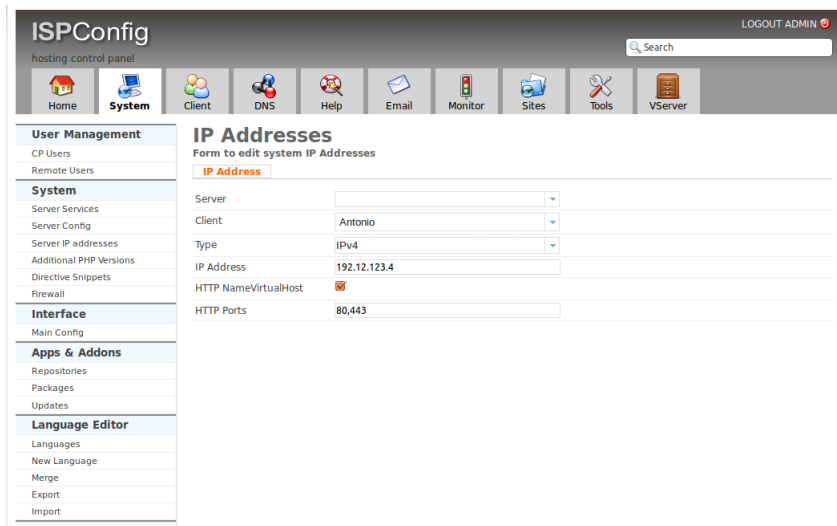


Figura 21.2: Añadir IP

Y por ultimo también he configurado el monitor para que se ejecute cada 5 minutos.

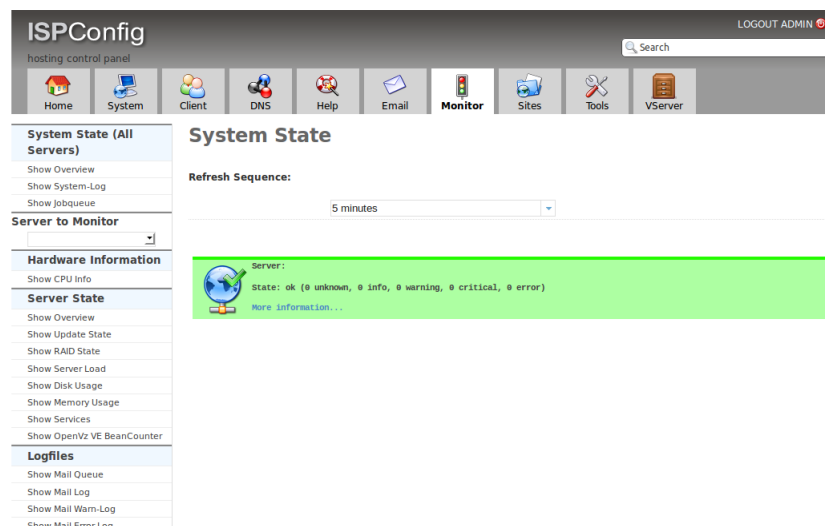


Figura 21.3: Monitor isconfig

22. Ejecute los ejemplos de find, grep y escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio.

```
#!/bin/bash
```

```
sed 's/2m/30s/' /etc/ssh/sshd_config > /etc/ssh/sshd_config2
rm /etc/ssh/sshd_config
mv /etc/ssh/sshd_config2 /etc/ssh/sshd_config
service sshd restart
```

## 23. Muestre un ejemplo de uso para awk

Voy a hacer un ejemplo sencillo, aunque la orden awk tiene mucha potencia a la hora de usarla. El ejemplo es crear un archivo con una serie de palabras y aplicarle awk como se muestra en la captura.



```
usuario@usuario-X555LDB:~/Escritorio$ cat prueba.txt
hola
pedros
papa
mama
pepe
ramon
pedro
ronaldo
roberto
usuario@usuario-X555LDB:~/Escritorio$ awk '/pedro/' prueba.txt
pedro
usuario@usuario-X555LDB:~/Escritorio$ awk '/p/' prueba.txt
papa
pepe
pedro
```

Figura 23.1: Ejemplo awk

En este ejemplo primero busca las palabras que son iguales a pedro y las siguientes las que tienen una p. El primer ejemplo seria parecido al grep.

## 24. Escriba el script para cambiar el acceso a ssh usando PHP o Python

```
import sys
import os
import subprocess
import shutil
fa=open('/etc/ssh/sshd_config', 'r+')
fb=open('/home/ajavier/Escritorio/sshd_config.txt', 'r+')

for line in fa:

    fb.write(line.replace("2m", "30s"))

shutil.copyfile("/home/ajavier/Escritorio/sshd_config.txt", "/etc/ssh/sshd_config")
os.remove('/home/ajavier/Escritorio/sshd_config.txt')
subprocess.call(['service', 'sshd', 'restart'])
```

## 25. Abra una consola de PowerShell y pruebe para un programa en ejecución, realice capturas de pantalla y comente lo que muestra

Abrimos el bloc de notas y la powershell. Ejecutamos Get-Process para ver los procesos abiertos.

```
PS C:\Users\Administrador> Get-Process
```

Handles	NPM(K)	PM(K)	VS(K)	UM(M)	CPU(s)	Id	ProcessName
44	7	1020	7532	60	0.05	1516	conhost
125	9	1168	3320	45	0.06	316	csrss
148	12	1412	11852	54	1.06	380	csrss
190	16	19540	32440	123	0.17	720	dm
854	45	16456	44352	314	1.20	1916	explorer
0	0	0	20	0	0.00	0	Idle
621	19	3680	8116	37	0.20	488	lsass
161	18	2816	7104	62	0.03	1736	msdtc
67	7	1236	6584	89	0.03	1936	notepad
355	25	60860	67016	612	1.00	1772	powershell
214	12	3240	6492	33	0.44	480	services
50	3	304	956	5	0.00	212	smss
328	17	3832	8456	48	0.08	1044	spoolsv
362	34	9572	15400	58	0.19	532	svchost
307	12	2864	7380	38	0.06	592	svchost
286	14	2836	5208	28	0.09	628	svchost
372	15	12288	15268	57	0.21	696	svchost
996	37	12584	23972	143	0.80	764	svchost
281	20	4576	11112	84	0.35	788	svchost
512	31	8552	14160	1127	0.11	892	svchost
103	10	3104	7480	40	0.09	1076	svchost
230	14	3604	8096	44	0.03	1096	svchost
230	18	8424	8936	617	0.11	1124	svchost
140	13	3720	8044	44	0.00	1140	svchost
738	0	120	260	3	1.25	4	System
148	11	1824	5880	82	0.03	1844	taskhostex
0	0	0	3364	43	0.06	300	wininit
133	8	1240	5372	52	0.03	416	winlogon
38	4	512	2484	14	0.00	1164	ulms
260	13	4936	11100	55	0.34	1828	UnitProcSE

```
PS C:\Users\Administrador> _
```

Figura 25.1: Get-Process

Ahora ponemos Stop-Process -Name notepad y paramos el proceso y al volver a ejecutar Get-Process nos sale que ya no esta como es de esperar.

```
PS C:\Users\Administrador> Stop-Process -Name notepad
```

```
PS C:\Users\Administrador> Get-Process
```

Handles	NPM(K)	PM(K)	VS(K)	UM(M)	CPU(s)	Id	ProcessName
44	7	1020	10620	63	0.00	1516	conhost
122	9	1168	3336	45	0.06	316	csrss
133	11	1320	10236	52	1.14	380	csrss
190	16	19536	30908	122	0.20	720	dm
839	44	16076	44224	311	1.25	1916	explorer
0	0	0	20	0	0.00	0	Idle
604	18	2908	8052	37	0.20	488	lsass
158	18	2712	7068	62	0.03	1736	msdtc
394	25	61072	68400	612	1.16	1772	powershell
204	11	3084	6484	31	0.44	480	services
50	3	304	956	5	0.00	212	smss
325	16	2844	8412	48	0.08	1044	spoolsv
356	33	9416	11392	57	0.19	532	svchost
383	12	2084	7532	38	0.06	592	svchost
280	15	2096	5236	28	0.11	628	svchost
364	15	12112	15284	56	0.21	696	svchost
1004	37	11440	23944	143	0.74	764	svchost
371	20	4460	11052	83	0.55	788	svchost
490	30	8500	14100	1127	0.11	892	svchost
103	10	3052	7464	40	0.09	1076	svchost
230	14	3604	8096	44	0.03	1096	svchost
229	18	8372	8924	617	0.11	1124	svchost
140	13	3720	8044	44	0.00	1140	svchost
725	0	120	260	3	1.27	4	System
148	11	1824	5880	82	0.03	1844	taskhostex
70	0	0	3340	43	0.06	300	wininit
133	8	1164	5360	51	0.03	416	winlogon
38	4	512	2484	14	0.00	1164	ulms
119	10	1708	5360	35	0.02	1700	UnitProcSE

```
PS C:\Users\Administrador> _
```

Figura 25.2: Notepad sin ejecutar