

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

Memoria Práctica 2

Ismael Luque Jiménez

4 de noviembre de 2014

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? (Pistas: archivo de configuración en /etc, proxy:stargate.ugr.es:3128) ¿Cómo añadimos un nuevo repositorio? [4, 15] | 5 |
| 3. Indique el comando para buscar un paquete en un repositorio y el correspondiente para instalarlo. | 5 |
| 4. Indiqué qué ha modificado para que apt pueda acceder a los servidores de paquetes a través del proxy. ¿Cómo añadimos un nuevo repositorio? [18] | 5 |
| 5. ¿Qué gestores utiliza OpenSuse? (Pista: http://es.opensuse.org/Gestión_de_paquetes) [10] | 6 |
| 6. ¿Qué diferencia hay entre telnet y ssh? [13, 11] | 6 |
| 7. ¿Para que sirve la opción -X? Ejecute remotamente, es decir, desde la máquina anfitriona (si tiene Linux) o desde la otra máquina virtual, el comando gedit en una sesión abierta con ssh. ¿Qué ocurre? [3] | 6 |
| 8. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña. (Pistas: ssh-keygen, ssh-copy-id). [1] | 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. [2] | 10 |
| 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. [27] | 12 |
| 11. Instale y pruebe terminator. Con screen, pruebe su funcionamiento dejando sesiones ssh abiertas en el servidor y recuperándolas posteriormente. [22] | 12 |
| 12. Instale el servicio fail2ban y pruebe su funcionamiento. [21] | 15 |
| 13. Muestre los comandos que ha utilizado en Ubuntu Server y en CentOS (aunque en este último puede utilizar la GUI, en tal caso, realice capturas de pantalla) [17, 19] | 18 |
| 14. Enumere otros servidores web y las páginas de sus proyectos (mínimo 3 sin considerar Apache, IIS ni nginx). [12] | 21 |

| | |
|--|----|
| 15.¿Cómo comprueba que IIS funciona? Muestre una captura de pantalla. (Pista: su máquina se denomina localhost). | 21 |
| 16.Realice la instalación de uno de estos dos “web containers” y pruebe su ejecución. [14] | 23 |
| 17.Realice la instalación de MongoDB en alguna de sus máquinas virtuales. Cree una colección de documentos y haga una consulta sobre ellos. (http://docs.mongodb.org/manual/introduction.html) [7, 8, 5, 6] | 25 |
| 18.Muestre un ejemplo de uso del comando patch (http://fedoraproject.org/wiki/VMWare) [16] | 28 |
| 19.Realice la instalación de Webmin y pruebe a modificar algún parámetro de algún servicio. Muestre las capturas de pantalla pertinentes así como el proceso de instalación. [20, 28] | 29 |
| 20.Instale phpMyAdmin, indique cómo lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs mayores de 8MB (límite por defecto). Indique cómo ha realizado el proceso y muestre capturas de pantalla. [24, 9] | 36 |
| 21.Visite al menos una de las webs de los software mencionados (DirectAdmin e IspConfig) y pruebe las demos que ofrecen realizando capturas de pantalla y comentando qué está realizando. | 42 |
| 22.Ejecute los ejemplos de find y grep y escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio. [25] | 47 |
| 23.Muestre un ejemplo de uso para awk. [26] | 48 |
| 24.Escriba el script para cambiar el acceso a ssh usando PHP o Python. [23] | 51 |
| 25.Abra una consola de PowerShell y pruebe a parar un programa en ejecución, realice capturas de pantalla y comente lo que muestra. | 52 |

ÍNDICE DE FIGURAS

| | |
|---|----|
| 7.1. Ejecutar Gedit de Forma Remota con SSH | 7 |
| 8.1. Crear Clave RSA sin Contraseña | 8 |
| 8.2. Copiar Clave RSA al Servidor | 9 |
| 9.1. Denegar Acceso a SSH al Usuario Root | 10 |
| 9.2. Cambiar Puerto de Acceso a SSH | 11 |
| 11.1.Ejemplo de Uso de terminator | 12 |
| 11.2.Ejemplo de Uso de screen (1) | 13 |
| 11.3.Ejemplo de Uso de screen (2) | 14 |

| | |
|---|----|
| 11.4. Ejemplo de Uso de screen (3) | 14 |
| 12.1. Cambiar Configuración de fail2ban | 15 |
| 12.2. Configurar fail2ban para SSH | 16 |
| 12.3. Intento de Acceso mediante SSH | 17 |
| 13.1. Acceso Remoto a Apache en Ubuntu | 18 |
| 13.2. Acceso Remoto a Apache en CentOS | 19 |
| 13.3. Script PHP en Servidor Web CentOS | 20 |
| 15.1. Consultar IP en Windows Server | 21 |
| 15.2. Acceso Remoto a IIS en Windows | 22 |
| 16.1. Instalación de Tomcat en Windows | 23 |
| 16.2. Acceso Remoto a Tomcat | 24 |
| 17.1. Añadir Documentos a una Colección en MongoDB | 25 |
| 17.2. Consultar Documentos de una Colección en MongoDB | 26 |
| 17.3. Crear Bases de Datos y Colecciones en MongoDB | 27 |
| 18.1. Ejemplo de Uso de patch | 28 |
| 19.1. Acceso Remoto a Webmin (HTTP) | 29 |
| 19.2. Acceso Remoto a Webmin (HTTPS) [Bloqueado] | 30 |
| 19.3. Acceso Remoto a Webmin (HTTPS) [Desbloqueado] | 31 |
| 19.4. Menú de Configuración de Webmin | 32 |
| 19.5. Configuración del Servidor SSH | 33 |
| 19.6. Opciones del Servidor SSH (Por Defecto) | 34 |
| 19.7. Opciones del Servidor SSH (Cambiadas) | 35 |
| 20.1. Instalación de PHPMyAdmin en Ubuntu | 36 |
| 20.2. Acceso Remoto a PHPMyAdmin | 37 |
| 20.3. Menú de Configuración de PHPMyAdmin | 38 |
| 20.4. Ampliar Límite de Tamaño para Importar Bases de Datos (1) | 39 |
| 20.5. Ampliar Límite de Tamaño para Importar Bases de Datos (2) | 40 |
| 20.6. Ampliar Límite de Tamaño para Importar Bases de Datos (3) | 41 |
| 21.1. Demos Online de DirectAdmin | 42 |
| 21.2. Menú de Configuración de DirectAdmin | 43 |
| 21.3. Añadir Administrador al Sistema en DirectAdmin | 44 |
| 21.4. Listar Usuarios del Sistema en DirectAdmin | 45 |
| 21.5. Consultar Información del Sistema en DirectAdmin | 46 |
| 22.1. Ejemplos de find y grep | 47 |
| 23.1. Fichero de Ejemplo para awk | 48 |
| 23.2. Script awk de Ejemplo | 49 |
| 23.3. Ejecución del Ejemplo awk | 50 |
| 24.1. Script PHP para Acceder a SSH | 51 |
| 25.1. Consultar Procesos en Ejecución con PowerShell | 52 |
| 25.2. Detener Proceso con PowerShell | 53 |
| 25.3. Comprobar Procesos en Ejecución con PowerShell | 54 |

1. LISTE LOS ARGUMENTOS DE YUM NECESARIOS PARA INSTALAR, BUSCAR Y ELIMINAR PAQUETES.

INSTALAR PAQUETES =>yum install PAQUETE

BUSCAR PAQUETES =>yum search NOMBRE_PROGRAMA

ELIMINAR PAQUETES =>yum remove PAQUETE

2. ¿QUÉ HA DE HACER PARA QUE YUM PUEDA TENER ACCESO A INTERNET? (PISTAS: ARCHIVO DE CONFIGURACIÓN EN /ETC, PROXY:STARGATE.UGR.ES:3128) ¿CÓMO AÑADIMOS UN NUEVO REPOSITORIO? [4, 15]

Para configurar yum para que utilice dicho proxy, editamos el archivo /etc/yum.conf para añadir la dirección del proxy y las credenciales de acceso al mismo si son necesarias:

```
proxy=stargate.ugr.es:3128
```

```
proxy\_username=USUARIO
```

```
proxy\_password=CONTRASEÑA
```

Hay varias maneras de añadir un nuevo repositorio: podemos editar el archivo /etc/yum.conf para añadir una nueva sección con dicho repositorio, añadir un archivo .repo al directorio /etc/yum.repos.d/ (ya que yum lee todos los archivos .repo que encuentre en esa carpeta) o añadirlo desde una terminal mediante el comando:

```
yum-config-manager --add-repo URL\_REPOSITORIO
```

.

3. INDIQUE EL COMANDO PARA BUSCAR UN PAQUETE EN UN REPOSITORIO Y EL CORRESPONDIENTE PARA INSTALARLO.

BUSCAR PAQUETES =>apt-cache search NOMBRE_PROGRAMA

INSTALAR PAQUETES =>apt-get install PAQUETE

4. INDIQUE QUÉ HA MODIFICADO PARA QUE APT PUEDA ACCEDER A LOS SERVIDORES DE PAQUETES A TRAVÉS DEL PROXY. ¿CÓMO AÑADIMOS UN NUEVO REPOSITORIO? [18]

Para configurar apt para que utilice dicho proxy, editamos el archivo /etc/apt/apt.conf para añadir la dirección del proxy:

```
Acquire::http::Proxy "http://stargate.ugr.es:3128";
```

5. ¿QUÉ GESTORES UTILIZA OPENSUSE? (PISTA:
HTTP://ES.OPENSUSE.ORG/GESTIÓN_DE_PAQUETES) [10]

OpenSuse utiliza RPM como sistema de empaquetado de su software, mientras que utiliza Libzypp como sistema de gestión de paquetes, el cual se puede manejar tanto con comandos mediante Zypper como gráficamente mediante YaST.

6. ¿QUÉ DIFERENCIA HAY ENTRE TELNET Y SSH? [13, 11]

La principal diferencia entre ssh y telnet es que el primero es un protocolo cifrado y el segundo no.

Mientras que con telnet todas las credenciales de acceso viajan por la red como texto plano (facilitando enormemente el espionaje del tráfico de la red), ssh utiliza técnicas de cifrado que transfieren la información en formato no legible (aunque siguen siendo posibles los ataques por medio de ataques de REPLAY).

7. ¿PARA QUE SIRVE LA OPCIÓN -X? EJECUTE REMOTAMENTE, ES
DECIR, DESDE LA MÁQUINA ANFITRIONA (SI TIENE LINUX) O DESDE
LA OTRA MÁQUINA VIRTUAL, EL COMANDO GEDIT EN UNA SESIÓN
ABIERTA CON SSH. ¿QUÉ OCURRE? [3]

Habilita el forwarding para X11, que es el servidor gráfico por antonomasia en Linux. Esta opción debe usarse con precaución puesto que alguien que pueda modificar los permisos de archivo en el sistema remoto podría acceder al dispositivo X11 y llevar a cabo actividades maliciosas (como los keyloggers).

```
[isma94@localhost ~]$ ssh -X 192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ECDSA key fingerprint is c9:ed:b9:a7:57:8e:6a:0b:72:cb:bb:cb:da:9d:12:63.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.11' (ECDSA) to the list of known hosts.
isma94@192.168.1.11's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

Last login: Sat Nov  1 19:03:37 2014
isma94@ubuntuserver:~$ gedit

(gedit:1752): Gtk-WARNING **: cannot open display:
isma94@ubuntuserver:~$ _
```

Figura 7.1: Ejecutar Gedit de Forma Remota con SSH

No es posible ejecutar gedit puesto que es una aplicación de interfaz gráfica y la máquina virtual no tiene instalado el X Window System.

8. MUESTRE LA SECUENCIA DE COMANDOS Y LAS MODIFICACIONES A LOS ARCHIVOS CORRESPONDIENTES PARA PERMITIR ACCEDER A LA CONSOLA REMOTA SIN INTRODUCIR LA CONTRASEÑA. (PISTAS: SSH-KEYGEN, SSH-COPY-ID). [1]

```
isma94@ubuntuserver:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/isma94/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/isma94/.ssh/id_rsa.
Your public key has been saved in /home/isma94/.ssh/id_rsa.pub.
The key fingerprint is:
e1:36:f7:92:68:46:57:5b:cc:51:e3:65:43:59:38:81 isma94@ubuntuserver
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           .+BB|
|          Eo+++|
|         .+o |
|        . . . o |
|       S o .  |
|      o = o   |
|     + o .   |
|    o .     |
|             |
+-----+
isma94@ubuntuserver:~$ _
```

Figura 8.1: Crear Clave RSA sin Contraseña


```
isma94@ubuntuserver:~$ ssh-copy-id -i .ssh/id_rsa.pub isma94@192.168.1.90
The authenticity of host '192.168.1.90 (192.168.1.90)' can't be established.
ECDSA key fingerprint is 6e:c5:7f:11:15:87:82:e4:6d:2e:6a:60:99:42:79:0a.
Are you sure you want to continue connecting (yes/no)? yes
/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
isma94@192.168.1.90's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'isma94@192.168.1.90'"
and check to make sure that only the key(s) you wanted were added.

isma94@ubuntuserver:~$ ssh isma94@192.168.1.90
Last login: Sat Nov  1 19:00:06 2014
[isma94@localhost ~]$
```

Figura 8.2: Copiar Clave RSA al Servidor

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. [2]

La configuración del demonio de SSH (**sshd**) se encuentra en el archivo `/etc/ssh/sshd_config`.

Para que el usuario root no pueda acceder mediante SSH, debemos cambiar el valor de **PermitRootLogin** de "without-password" a "no".

```
[isma94@localhost ~]$ ssh root@192.168.1.11
root@192.168.1.11's password:
Permission denied, please try again.
root@192.168.1.11's password:
Permission denied, please try again.
root@192.168.1.11's password:
Permission denied (publickey,password).
[isma94@localhost ~]$ ssh isma94@192.168.1.11
isma94@192.168.1.11's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Sat Nov  1 19:59:36 CET 2014

System load:   0.0               Processes:      108
Usage of /home: 0.9% of 451MB    Users logged in: 1
Memory usage:   6%               IP address for eth0: 192.168.1.11
Swap usage:    0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Sat Nov  1 19:59:37 2014 from 192.168.1.11
isma94@ubuntuserver:~$ _
```

Figura 9.1: Denegar Acceso a SSH al Usuario Root

Para cambiar el puerto, cambiamos el valor de **Port** (que por defecto para SSH es el 22) por el puerto que queramos usar. Debemos tener cuidado de que dicho puerto no se encuentre ya en uso por otro servicio, y especificarlo en la petición SSH mediante la opción -p.

```
[isma94@localhost ~]$ ssh isma94@192.168.1.11
ssh: connect to host 192.168.1.11 port 22: Connection refused
[isma94@localhost ~]$ ssh -p 666 isma94@192.168.1.11
isma94@192.168.1.11's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Sat Nov  1 20:41:53 CET 2014

System load:   0.04               Processes:      111
Usage of /home: 0.9% of 451MB     Users logged in: 1
Memory usage:   7%                IP address for eth0: 192.168.1.11
Swap usage:     0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Sat Nov  1 20:41:54 2014 from 192.168.1.90
isma94@ubuntuserver:~$ _
```

Figura 9.2: Cambiar Puerto de Acceso a SSH

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. [27]

Con cada cambio en el archivo de configuración de un servicio, debemos reiniciarlo para que lea y active la nueva configuración.

En ambos sistemas operativos reiniciamos el servicio mediante la orden *service* con la opción *restart*, que ejecuta un script de inicio de los disponibles en */etc/init.d*, pero cada uno utiliza un script distinto para iniciar el servicio SSH.

UBUNTU: `sudo service ssh restart`

CENTOS: `sudo service sshd restart`

11. INSTALE Y PRUEBE TERMINATOR. CON SCREEN, PRUEBE SU FUNCIONAMIENTO DEJANDO SESIONES SSH ABIERTAS EN EL SERVIDOR Y RECUPERÁNDOLAS POSTERIORMENTE. [22]

* **TERMINATOR:** Ejecutamos el programa y dividimos la terminal en 4, dividiéndola primero horizontalmente y dividiendo a su vez cada una de las resultantes verticalmente mediante combinaciones de teclas predefinidas:

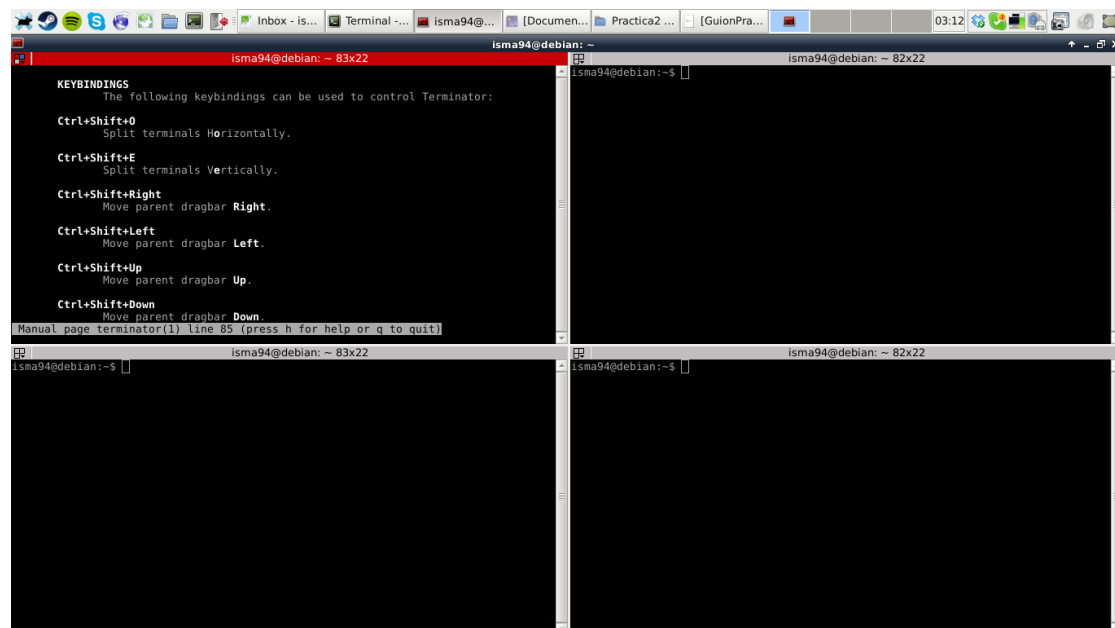
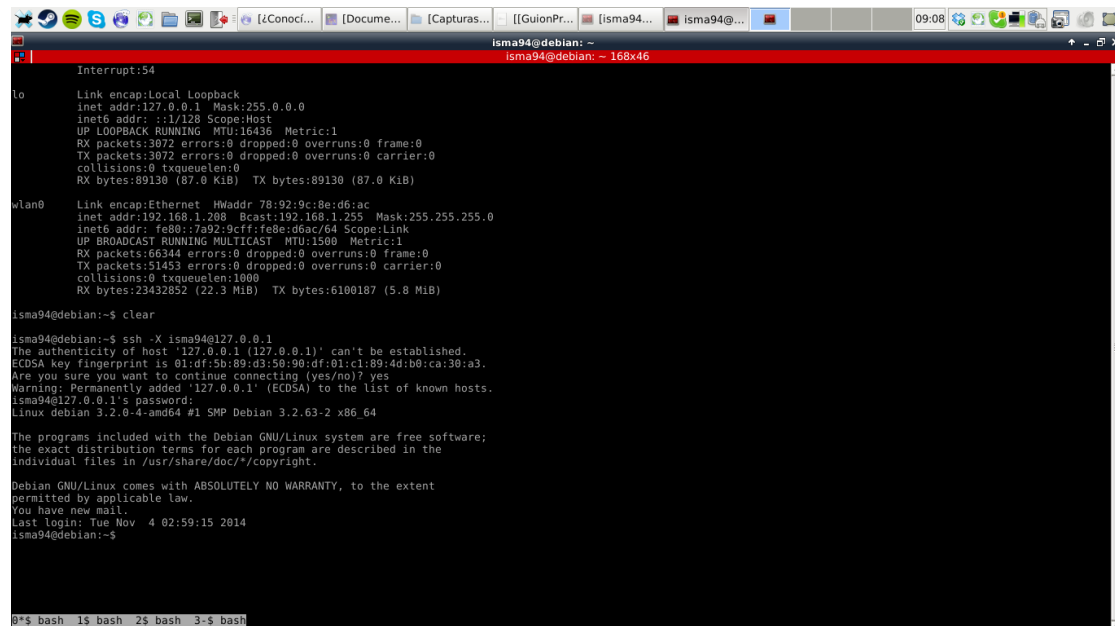


Figura 11.1: Ejemplo de Uso de terminator

* **SCREEN:** Ejecutamos 4 veces el comando screen. Esto creará 4 sesiones de bash simultáneas, en cada una de las cuales podemos iniciar una sesión de ssh totalmente independiente de las demás:



```
Interrupt:54
lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:16436 Metric:1
  RX packets:3072 errors:0 dropped:0 overruns:0 frame:0
  TX packets:3072 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:89130 (87.0 KiB) TX bytes:89130 (87.0 KiB)

wlan0
  Link encap:Ethernet HWaddr 78:92:9c:8e:d6:ac
  inet addr:192.168.1.200 Bcast:192.168.1.255 Mask:255.255.255.0
  inet6 addr: fe80::7a92:9cff:fe8e:d6ac/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:66344 errors:0 dropped:0 overruns:0 frame:0
  TX packets:51453 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:23432852 (22.3 MiB) TX bytes:6100187 (5.8 MiB)

isma94@debian:~$ clear
isma94@debian:~$ ssh -X isma94@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is 01:df:5b:89:0d:50:90:df:01:c1:89:4d:b0:ca:30:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
isma94@127.0.0.1's password:
Linux debian 3.2.0-4-amd64 #1 SMP Debian 3.2.63-2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Tue Nov 4 02:59:15 2014
isma94@debian:~$

0$ bash 1$ bash 2$ bash 3$ bash
```

Figura 11.2: Ejemplo de Uso de screen (1)

Podemos ver las sesiones que tenemos abiertas usando la combinación (Ctrl + a) + w:
Finalmente, podemos renombrar las sesiones para identificarlas usando la combinación (Ctrl + a) + A:

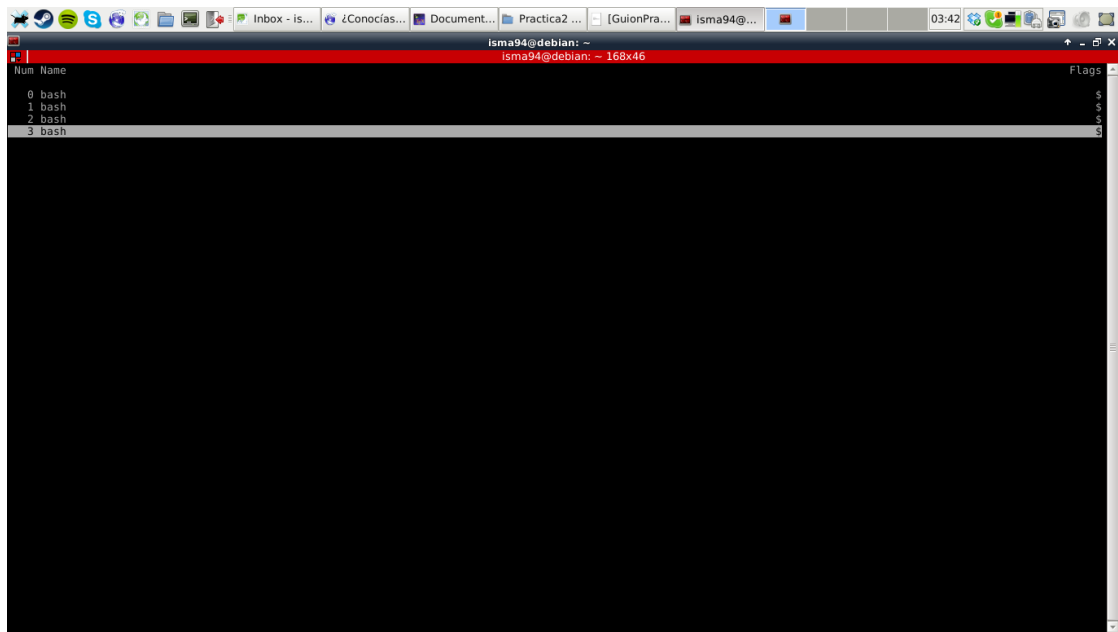


Figura 11.3: Ejemplo de Uso de screen (2)

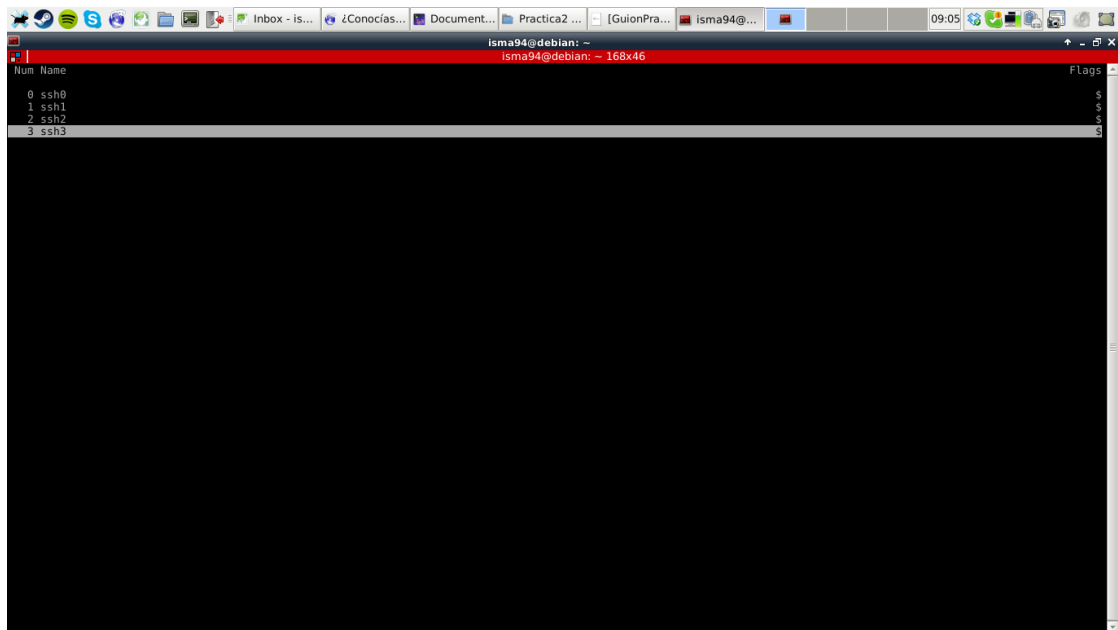


Figura 11.4: Ejemplo de Uso de screen (3)

12. INSTALE EL SERVICIO FAIL2BAN Y PRUEBE SU FUNCIONAMIENTO.

[21]

Este servicio limita los intentos de autenticación mediante fuerza bruta baneando aquellas IP que intenten acceder varias veces con datos erróneos.

Para configurar el servicio, copiamos el archivo de configuración /etc/fail2ban/jail.conf en /etc/fail2ban/jail.local y modificamos éste último:

```
isma94@ubuntuserver:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
isma94@ubuntuserver:~$ sudo service fail2ban restart
 * Restarting authentication failure monitor fail2ban [ OK ]
isma94@ubuntuserver:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            multiport dport
fail2ban-ssh tcp  --  anywhere              anywhere               multiport dport
s ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain fail2ban-ssh (1 references)
target     prot opt source                destination
RETURN    all  --  anywhere              anywhere
isma94@ubuntuserver:~$
```

Figura 12.1: Cambiar Configuración de fail2ban

En este caso, debemos asegurarnos de que se encuentre activo el filtro para SSH:

```
GNU nano 2.2.6      Archivo: /etc/fail2ban/jail.conf

# JAILS
#
# Next jails corresponds to the standard configuration in Fail2ban 0.6 which
# was shipped in Debian. Enable any defined here jail by including
#
# [SECTION_NAME]
# enabled = true
#
# in /etc/fail2ban/jail.local.
#
# Optionally you may override any other parameter (e.g. banaction,
# action, port, logpath, etc) in that section within jail.local

[ssh]

enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3

[dropbear]

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y RePág.    ^K Cortar Tex ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^U Pág. Sig. ^U PegarTxt   ^T Ortografía
```

Figura 12.2: Configurar fail2ban para SSH

Ahora, si una IP alcanza el límite de intentos al acceder por SSH a la máquina virtual, quedará baneada durante 10 minutos:

```
isma94@ubuntu:~$ ssh isma94@192.168.1.11
isma94@192.168.1.11's password:
Permission denied, please try again.
isma94@192.168.1.11's password:
Permission denied, please try again.
isma94@192.168.1.11's password:
Permission denied (publickey,password).
isma94@ubuntu:~$ _
```

Figura 12.3: Intento de Acceso mediante SSH

13. MUESTRE LOS COMANDOS QUE HA UTILIZADO EN UBUNTU SERVER Y EN CENTOS (AUNQUE EN ESTE ÚLTIMO PUEDE UTILIZAR LA GUI, EN TAL CASO, REALICE CAPTURAS DE PANTALLA) [17, 19]

* UBUNTU:

Instalamos el servidor LAMP mediante el comando `tasksel`, que descarga e instala el grupo de tareas completo. En Ubuntu el sistema de gestión de bases de datos por defecto es MySQL.

```
sudo tasksel lamp-server
```

Comprobamos que el servidor web está activo accediendo de forma remota a su IP desde nuestro navegador web:

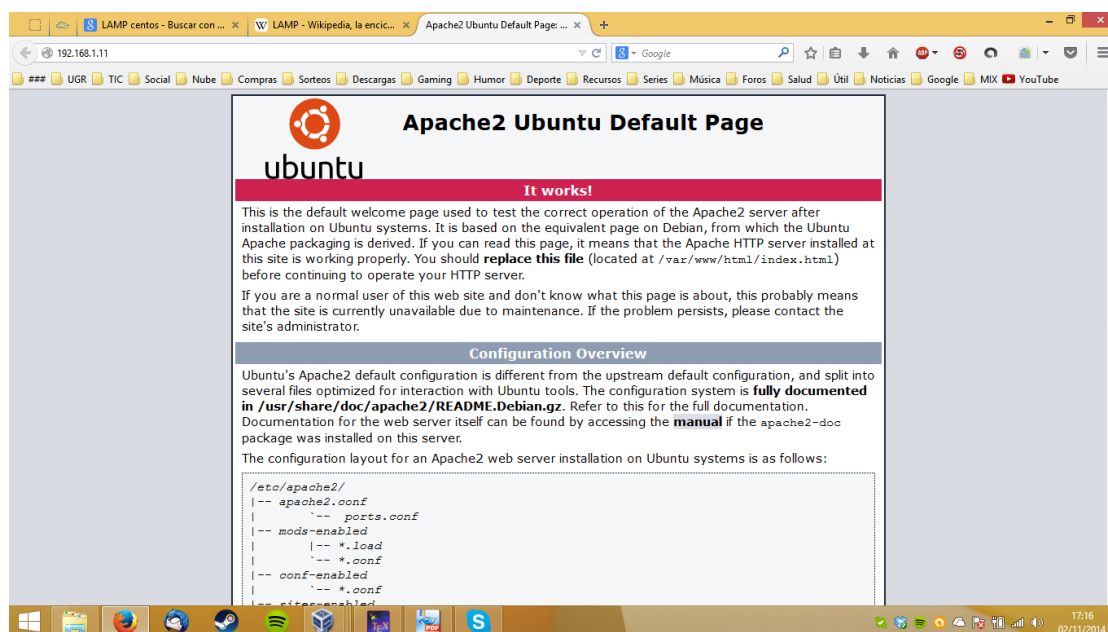


Figura 13.1: Acceso Remoto a Apache en Ubuntu

* CENTOS:

Instalamos y activamos cada componente por separado (Apache + MariaDB + PHP). En CentOS el sistema de gestión de bases de datos por defecto es MariaDB, que funciona igual que MySQL debido a que es una bifurcación del mismo.

1) Apache: Instalamos mediante yum el servidor Apache, iniciamos el servicio y habilitamos su ejecución en el arranque del sistema:

```
sudo yum install httpd
sudo systemctl start httpd.service
sudo systemctl enable httpd.service
```

Comprobamos que el servidor web está activo accediendo de forma remota a su IP desde nuestro navegador web:

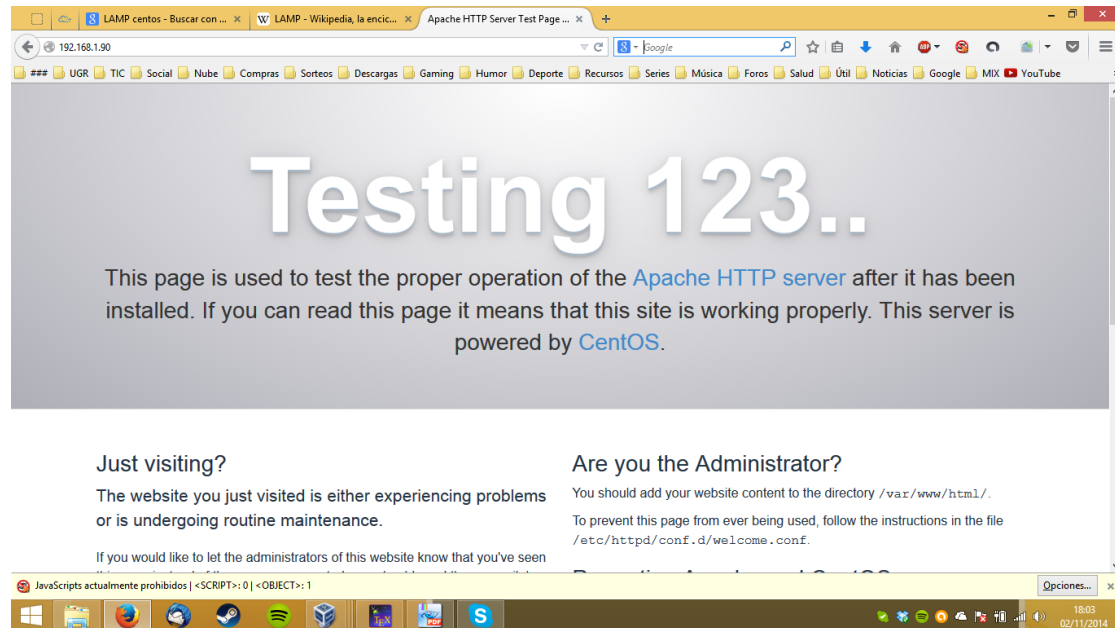


Figura 13.2: Acceso Remoto a Apache en CentOS

2) MariaDB: Instalamos mediante yum el servidor MariaDB, iniciamos el servicio y habilitamos su ejecución en el arranque del sistema:

```
sudo yum install mariadb-server mariadb
sudo systemctl start mariadb
sudo systemctl enable mariadb.service
```

Configuramos el servidor MySQL mediante el comando `mysql_secure_installation`. Como acabamos de instalarlo, no tenemos contraseña para el root, así que introducimos una nueva contraseña cuando nos lo pida. El asistente también nos ofrecerá eliminar los usuarios y las bases de datos de ejemplo, desactivar el login remoto para el root, y cargar automáticamente la nueva configuración.

```
sudo mysql_secure_installation
```

3) PHP: Instalamos la herramienta PHP y reiniciamos el servidor Apache para que comience a trabajar con PHP:

```
sudo yum install php php-mysql
sudo systemctl restart httpd.service
```

Para permitir el tráfico HTTP y HTTPS, utilizamos los siguientes comandos del firewall:

```
sudo firewall-cmd --permanent --zone=public --add-service=http
sudo firewall-cmd --permanent --zone=public --add-service=https
sudo firewall-cmd --reload
```

Para comprobar que PHP está configurado correctamente, creamos un script PHP básico en /var/www/html/info.php con el siguiente código:

```
<?php phpinfo (); ?>
```

Si todo está bien configurado, podremos ejecutar dicho script de forma remota desde nuestro navegador web:

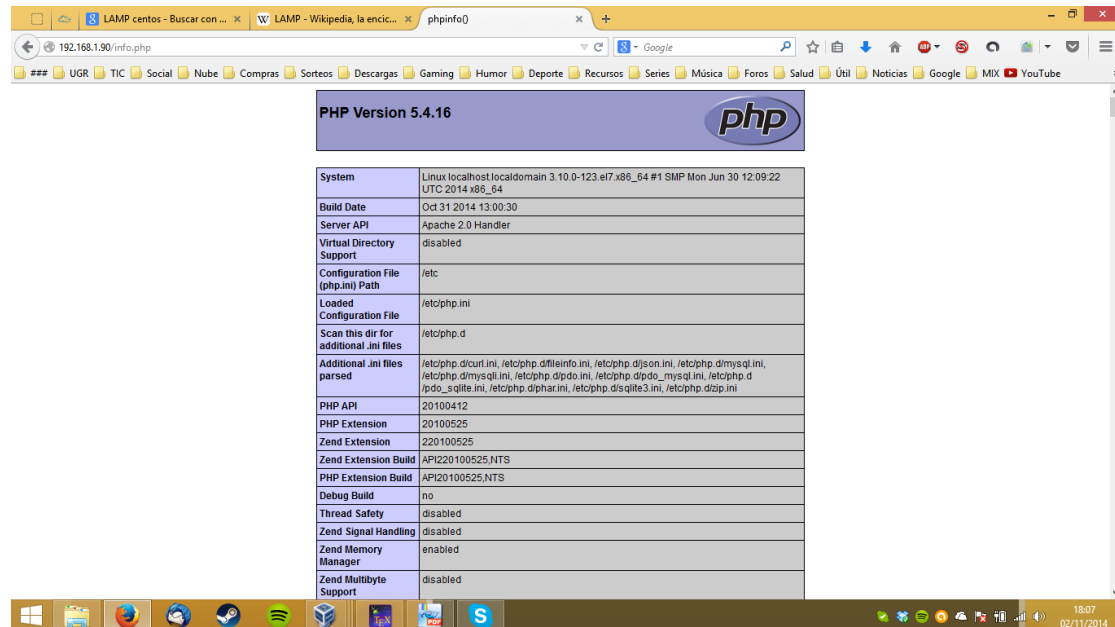


Figura 13.3: Script PHP en Servidor Web CentOS

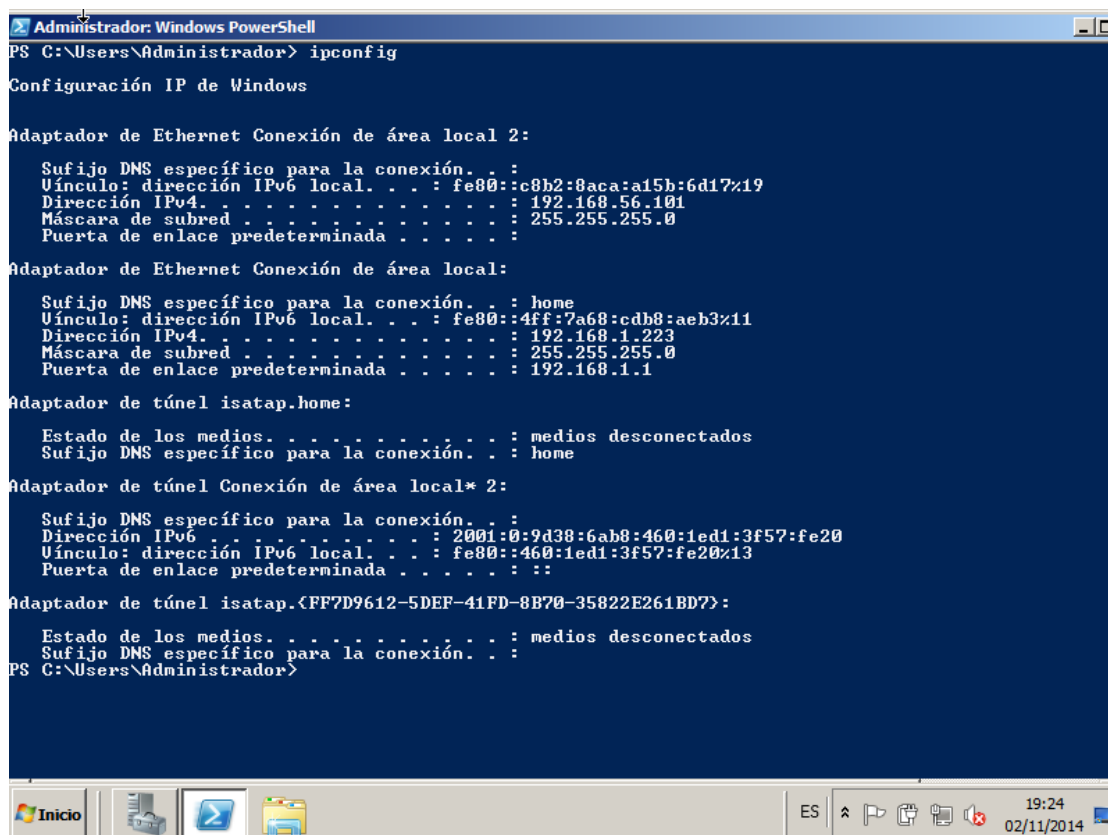
14. ENUMERE OTROS SERVIDORES WEB Y LAS PÁGINAS DE SUS PROYECTOS (MÍNIMO 3 SIN CONSIDERAR APACHE, IIS NI NGINX).

[12]

- **Cherokee:** <http://cherokee-project.com/>
- **Tomcat:** <http://tomcat.apache.org/>
- **Lighttpd:** <http://www.lighttpd.net/>

15. ¿CÓMO COMPRUEBA QUE IIS FUNCIONA? MUESTRE UNA CAPTURA DE PANTALLA. (PISTA: SU MÁQUINA SE DENOMINA LOCALHOST).

Consultamos la IP de la máquina virtual en la que hemos montado el servidor IIS:



```
Administrador: Windows PowerShell
PS C:\Users\Administrador> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 2:

    Sufijo DNS específico para la conexión. . . : 
    Vínculo: dirección IPv6 local. . . : fe80::c8b2:8aca:a15b:6d17%19
    Dirección IPv4. . . . . : 192.168.56.101
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : home
    Vínculo: dirección IPv6 local. . . : fe80::4ff:7a68:cd8b:aeb3%11
    Dirección IPv4. . . . . : 192.168.1.223
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de túnel isatap.home:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : home

Adaptador de túnel Conexión de área local* 2:

    Sufijo DNS específico para la conexión. . . : 
    Dirección IPv6 . . . . . : 2001:0:9d38:6ab8:460:1ed1:3f57:fe20
    Vínculo: dirección IPv6 local. . . : fe80::460:1ed1:3f57:fe20%13
    Puerta de enlace predeterminada . . . . . : 

Adaptador de túnel isatap.{FF7D9612-5DEF-41FD-8B70-35822E261BD7}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : 
PS C:\Users\Administrador>
```

Figura 15.1: Consultar IP en Windows Server

Comprobamos que el servidor web está activo accediendo de forma remota a su IP desde nuestro navegador web:

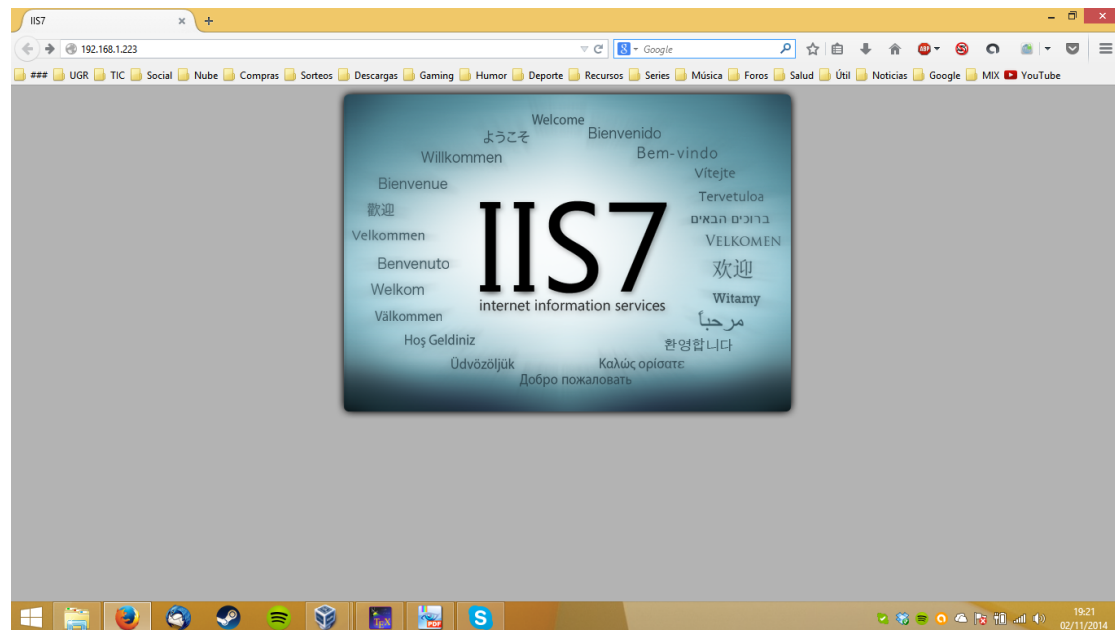


Figura 15.2: Acceso Remoto a IIS en Windows

16. REALICE LA INSTALACIÓN DE UNO DE ESTOS DOS “WEB CONTAINERS” Y PRUEBE SU EJECUCIÓN. [14]

Instalamos el contenedor web Tomcat ejecutando el instalador disponible en su página oficial:

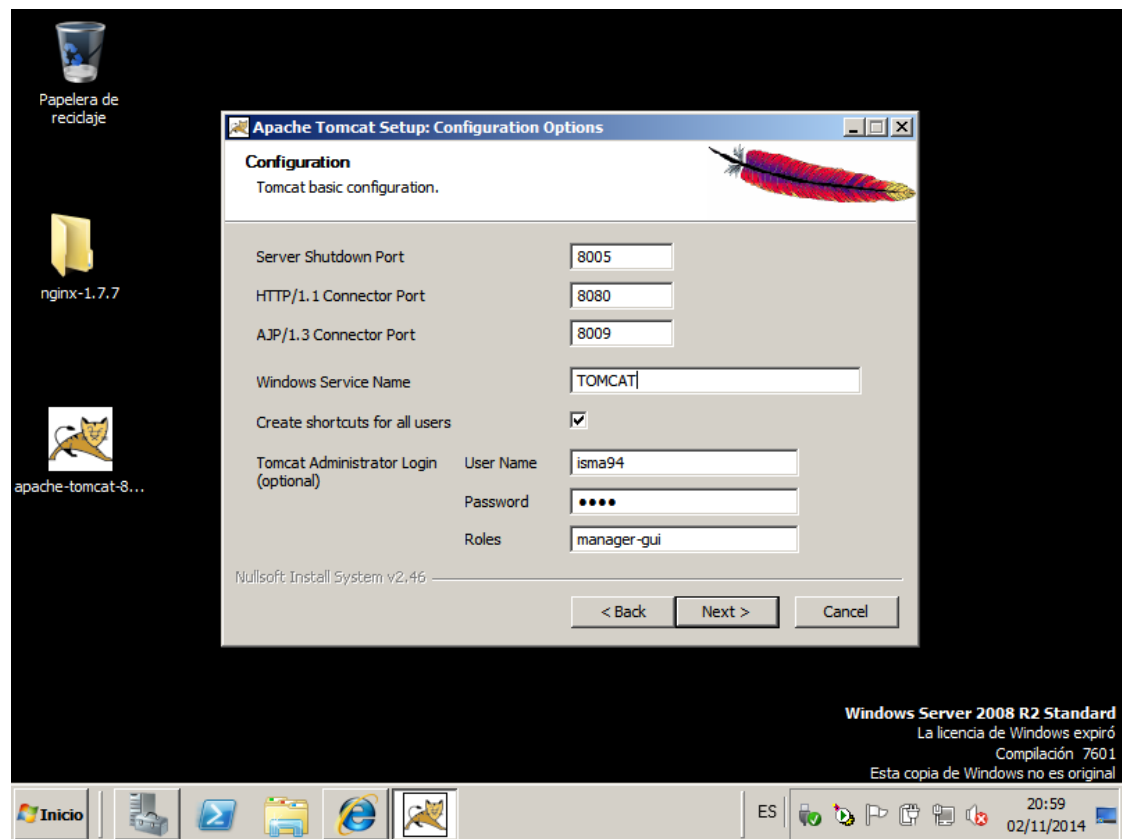


Figura 16.1: Instalación de Tomcat en Windows

Para comprobar su funcionamiento, accedemos de forma remota a la configuración de Tomcat a través del puerto 8080:

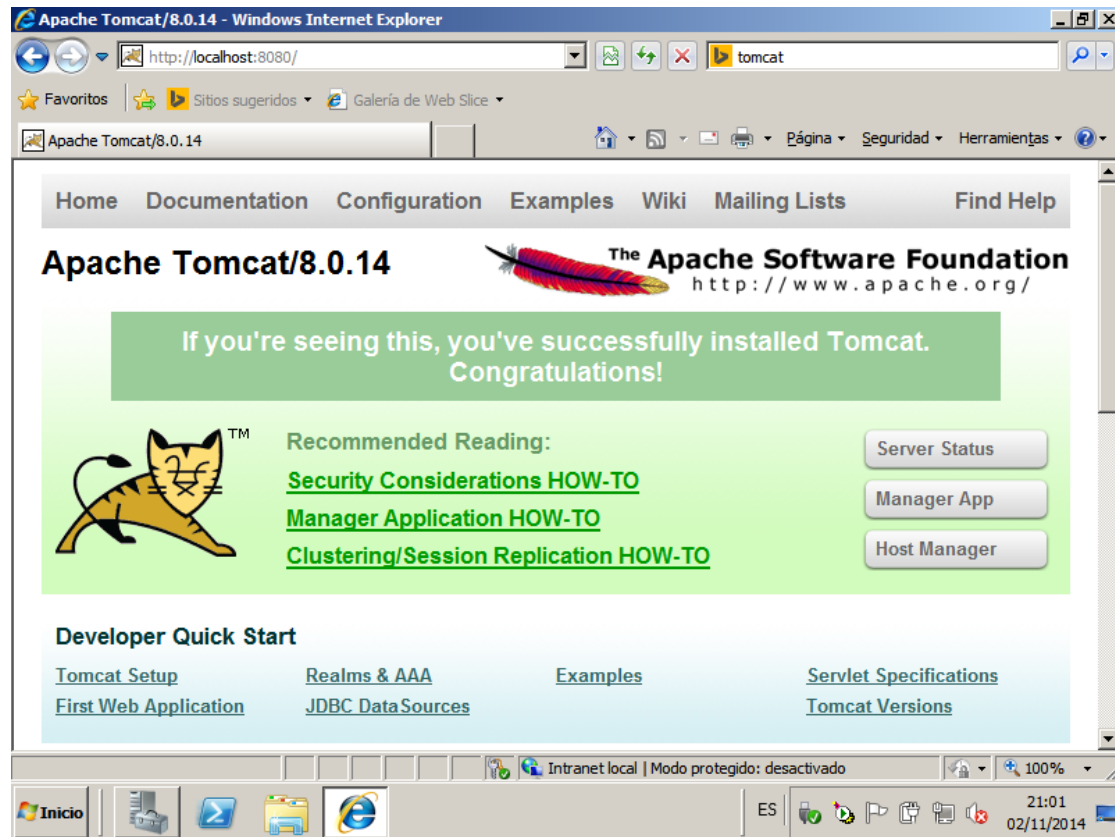


Figura 16.2: Acceso Remoto a Tomcat

17. REALICE LA INSTALACIÓN DE MONGODB EN ALGUNA DE SUS MÁQUINAS VIRTUALES. CREE UNA COLECCIÓN DE DOCUMENTOS Y HAGA UNA CONSULTA SOBRE ELLOS.

([HTTP://DOCS.MONGODB.ORG/MANUAL/INSTALLATION/](http://docs.mongodb.org/manual/installation/))

[7, 8, 5, 6]

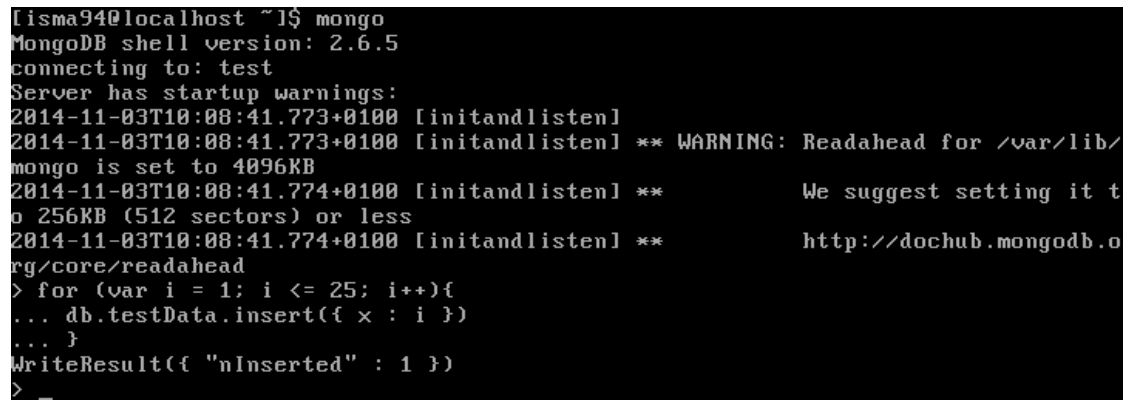
Para instalar el DBMS MongoDB, primero hemos de crear un archivo de repositorio `/etc/yum.repos.d/mongodb.repo` y añadir:

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

Posteriormente, instalamos mediante yum el servidor MongoDB, iniciamos el servicio y habilitamos su ejecución en el arranque del sistema:

```
sudo yum install mongodb-org
sudo service mongod start
sudo chkconfig mongod on
```

Para probar su funcionamiento, añadimos documentos a la colección de prueba "testData" de la base de datos de prueba "test":



```
[isma94@localhost ~]$ mongo
MongoDB shell version: 2.6.5
connecting to: test
Server has startup warnings:
2014-11-03T10:08:41.773+0100 [initandlisten] [initandlisten]
2014-11-03T10:08:41.773+0100 [initandlisten] ** WARNING: Readahead for /var/lib/
mongo is set to 4096KB
2014-11-03T10:08:41.774+0100 [initandlisten] ** We suggest setting it t
o 256KB (512 sectors) or less
2014-11-03T10:08:41.774+0100 [initandlisten] ** http://dochub.mongodb.o
rg/core/readahead
> for (var i = 1; i <= 25; i++){
... db.testData.insert({ x : i })
... }
WriteResult({ "nInserted" : 1 })
> _
```

Figura 17.1: Añadir Documentos a una Colección en MongoDB

Consultamos estos documentos realizando la correspondiente "query.^a la base de datos en uso:

```
... }
WriteResult({ "nInserted" : 1 })
> db.testData.find()
{ "_id" : ObjectId("5457495026418f2e69242e3f"), "x" : 1 }
{ "_id" : ObjectId("5457495026418f2e69242e40"), "x" : 2 }
{ "_id" : ObjectId("5457495026418f2e69242e41"), "x" : 3 }
{ "_id" : ObjectId("5457495026418f2e69242e42"), "x" : 4 }
{ "_id" : ObjectId("5457495026418f2e69242e43"), "x" : 5 }
{ "_id" : ObjectId("5457495026418f2e69242e44"), "x" : 6 }
{ "_id" : ObjectId("5457495026418f2e69242e45"), "x" : 7 }
{ "_id" : ObjectId("5457495026418f2e69242e46"), "x" : 8 }
{ "_id" : ObjectId("5457495026418f2e69242e47"), "x" : 9 }
{ "_id" : ObjectId("5457495026418f2e69242e48"), "x" : 10 }
{ "_id" : ObjectId("5457495026418f2e69242e49"), "x" : 11 }
{ "_id" : ObjectId("5457495026418f2e69242e4a"), "x" : 12 }
{ "_id" : ObjectId("5457495026418f2e69242e4b"), "x" : 13 }
{ "_id" : ObjectId("5457495026418f2e69242e4c"), "x" : 14 }
{ "_id" : ObjectId("5457495026418f2e69242e4d"), "x" : 15 }
{ "_id" : ObjectId("5457495026418f2e69242e4e"), "x" : 16 }
{ "_id" : ObjectId("5457495026418f2e69242e4f"), "x" : 17 }
{ "_id" : ObjectId("5457495026418f2e69242e50"), "x" : 18 }
{ "_id" : ObjectId("5457495126418f2e69242e51"), "x" : 19 }
{ "_id" : ObjectId("5457495126418f2e69242e52"), "x" : 20 }
Type "it" for more
> _
```

Figura 17.2: Consultar Documentos de una Colección en MongoDB

También podemos crear una nueva base de datos y, dentro de ella, una nueva colección en la que crear documentos para después consultarlos:

```
2014-11-03T10:08:41.773+0100 [initandlisten] ** WARNING: Readahead for /var/lib/
mongo is set to 4096KB
2014-11-03T10:08:41.774+0100 [initandlisten] **           We suggest setting it t
o 256KB (512 sectors) or less
2014-11-03T10:08:41.774+0100 [initandlisten] **           http://dochub.mongodb.o
rg/core/readahead
> db
test
> use database
switched to db database
> j = { name : "mongo" }
{ "name" : "mongo" }
> k = { x : 3 }
{ "x" : 3 }
> db.collection.insert(j)
WriteResult({ "nInserted" : 1 })
> db.collection.insert(k)
WriteResult({ "nInserted" : 1 })
> show collections
collection
system.indexes
> db.collection.find()
{ "_id" : ObjectId("54574b01d8f3971224c88867"), "name" : "mongo" }
{ "_id" : ObjectId("54574b05d8f3971224c88868"), "x" : 3 }
>
```

Figura 17.3: Crear Bases de Datos y Colecciones en MongoDB

18. MUESTRE UN EJEMPLO DE USO DEL COMANDO PATCH
([HTTP://FEDORAPROJECT.ORG/WIKI/VMWARE](http://FEDORAPROJECT.ORG/WIKI/VMWARE)) [16]

```
isma94@ubuntuserver:~$ cat viejo.txt
##### VIEJO #####
isma94@ubuntuserver:~$ cat nuevo.txt
##### NUEVO #####
isma94@ubuntuserver:~$ diff -u viejo.txt nuevo.txt > parche.patch
isma94@ubuntuserver:~$ patch < parche.patch
patching file viejo.txt
isma94@ubuntuserver:~$ cat nuevo.txt
##### NUEVO #####
isma94@ubuntuserver:~$ cat viejo.txt
##### NUEVO #####
isma94@ubuntuserver:~$
```

Figura 18.1: Ejemplo de Uso de patch

19. REALICE LA INSTALACIÓN DE WEBMIN Y PRUEBE A MODIFICAR ALGÚN PARÁMETRO DE ALGÚN SERVICIO. MUESTRE LAS CAPTURAS DE PANTALLA PERTINENTES ASÍ COMO EL PROCESO DE INSTALACIÓN. [20, 28]

Para instalar la interfaz Webmin, primero hemos de editar el archivo de repositorios `/etc/apt/sources.list` para añadir:

```
deb http://download.webmin.com/download/repository sarge contrib
```

Posteriormente, añadimos la clave GPG del repositorio, actualizamos paquetes e instalamos Webmin mediante `apt-get`:

```
wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
```

Para comprobar su funcionamiento, accedemos de forma remota a la configuración de Webmin a través del puerto 10000:

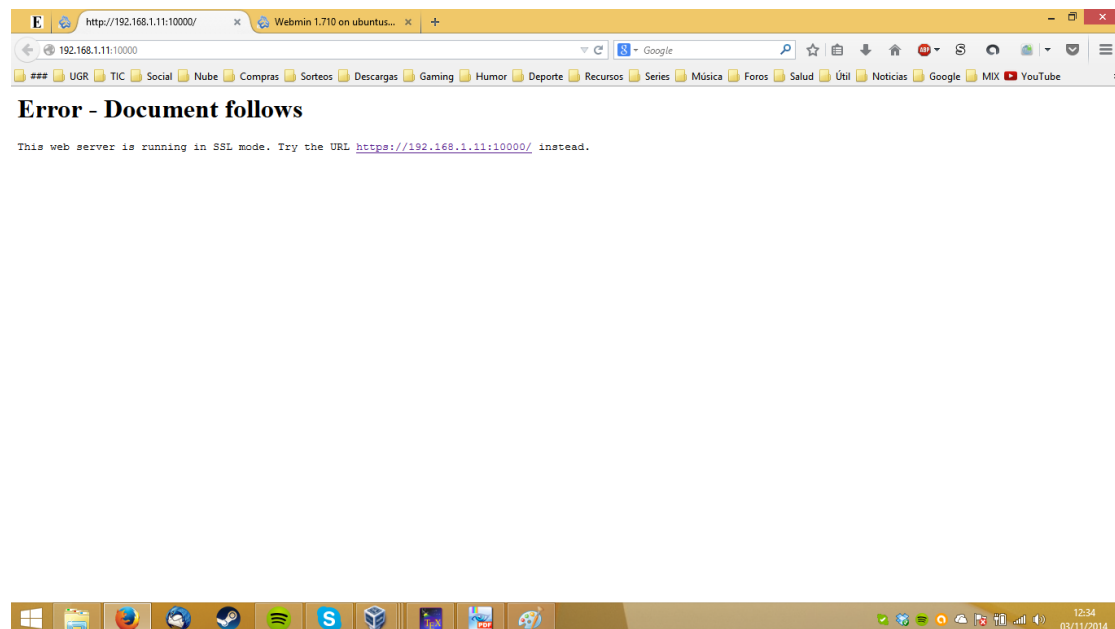


Figura 19.1: Acceso Remoto a Webmin (HTTP)

Puesto que el servidor web se está ejecutando en modo SSL, es necesario utilizar el protocolo HTTPS para poder acceder:

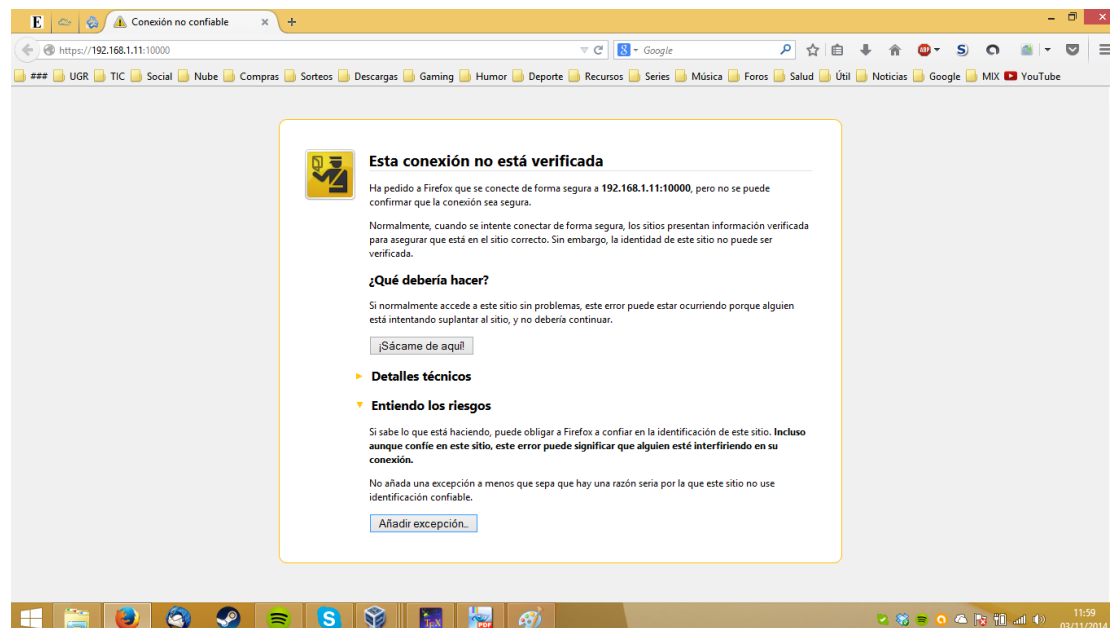


Figura 19.2: Acceso Remoto a Webmin (HTTPS) [Bloqueado]

El navegador bloquea la IP del servidor al no reconocerla como segura. Para solucionarlo, la añadimos a la lista de excepciones:

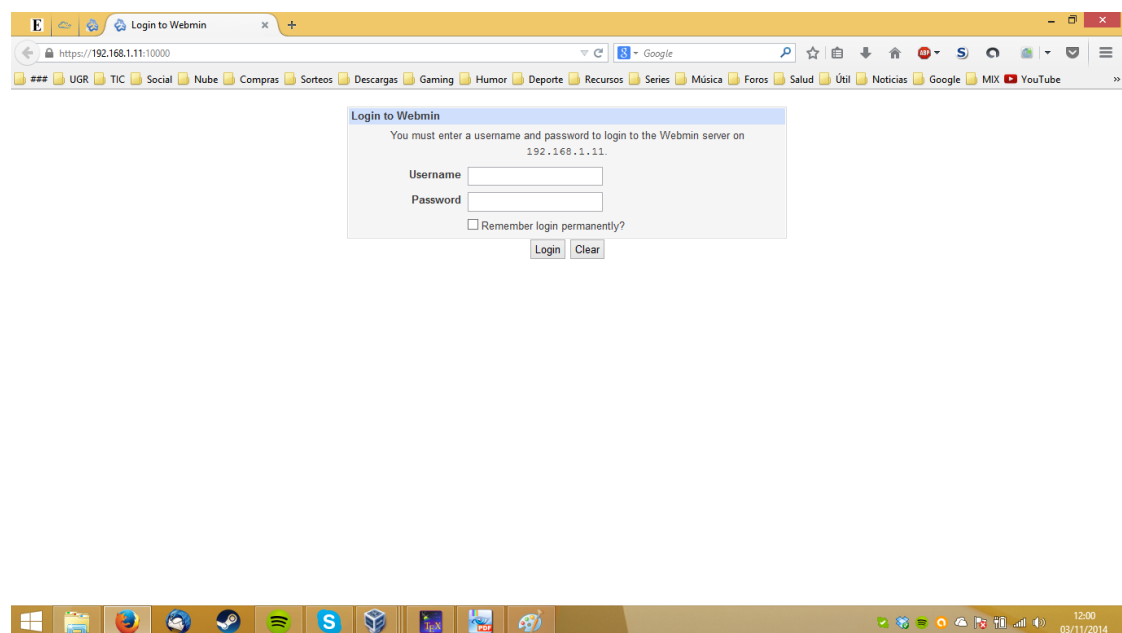


Figura 19.3: Acceso Remoto a Webmin (HTTPS) [Desbloqueado]

Una vez introducidas nuestras credenciales de acceso, accedemos al menú de configuración de Webmin:

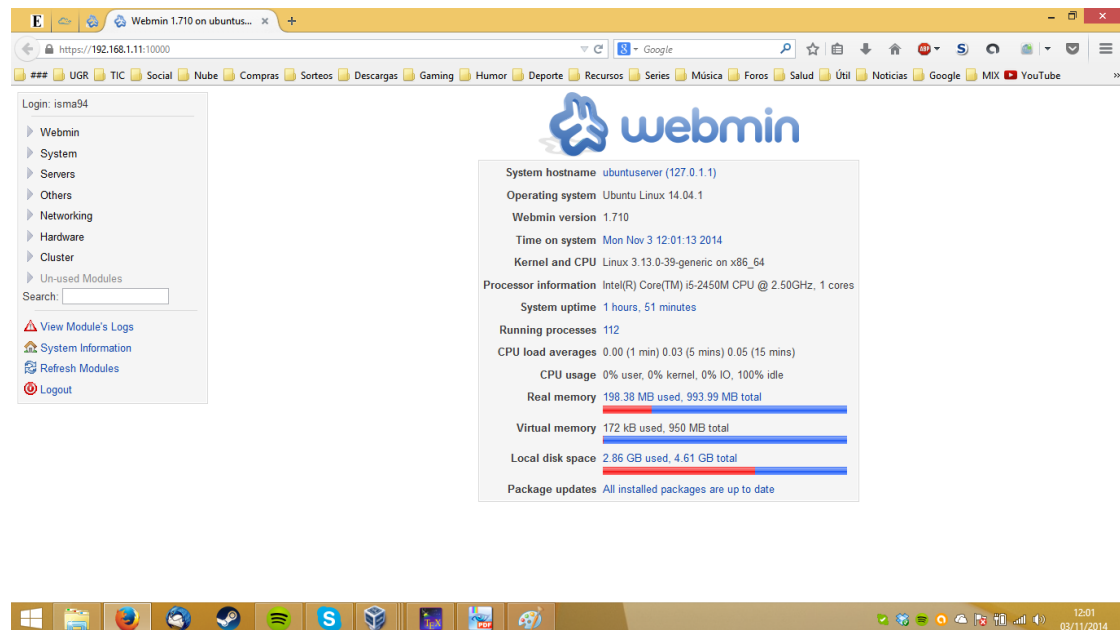


Figura 19.4: Menú de Configuración de Webmin

Para observar el funcionamiento del servicio, una opción sería modificar la configuración de SSH (Server =>SSH Server):

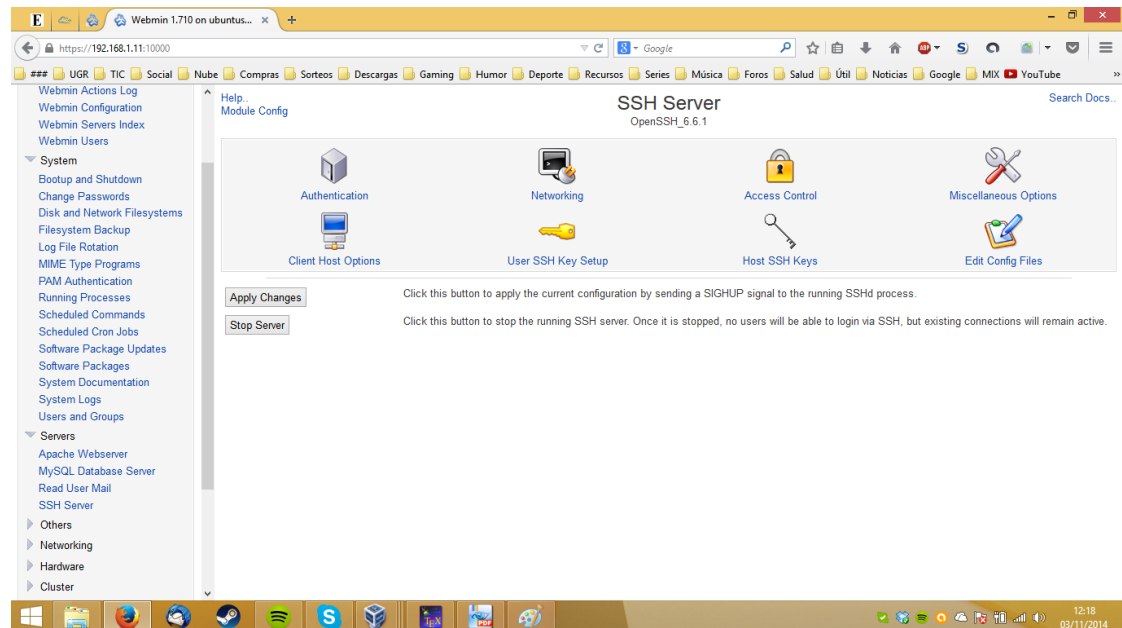


Figura 19.5: Configuración del Servidor SSH

Por ejemplo, podemos modificar las diversas opciones disponibles en el menú Miscellaneous Options:

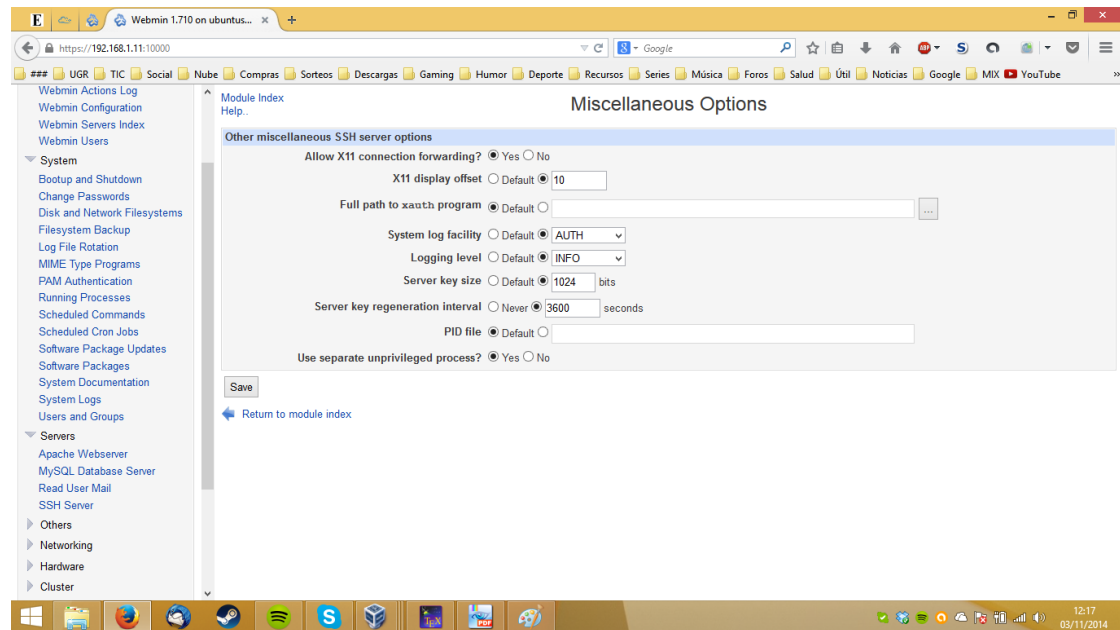


Figura 19.6: Opciones del Servidor SSH (Por Defecto)

Ponemos todos los parámetros en su valor por defecto, guardamos los cambios (Save) y aplicamos la nueva configuración (Apply Changes):

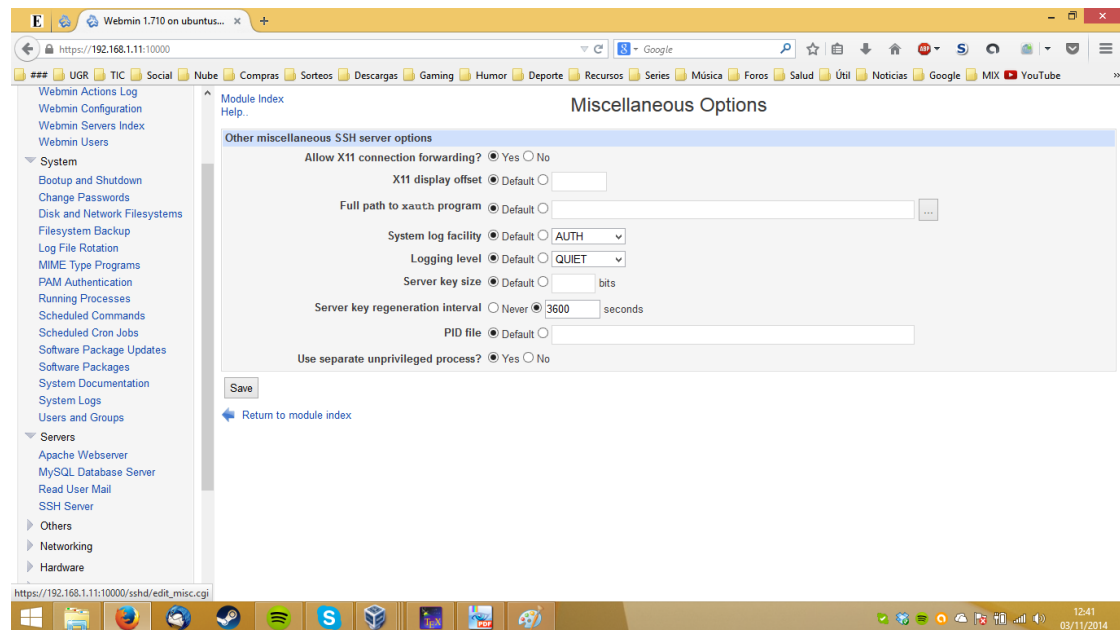


Figura 19.7: Opciones del Servidor SSH (Cambiadas)

20. INSTALE PHPMYADMIN, INDIQUE CÓMO LO HA REALIZADO Y MUESTRE ALGUNAS CAPTURAS DE PANTALLA. CONFIGURE PHP PARA PODER IMPORTAR BDS MAYORES DE 8MB (LÍMITE POR DEFECTO). INDIQUE CÓMO HA REALIZADO EL PROCESO Y MUESTRE CAPTURAS DE PANTALLA. [24, 9]

Primero, instalamos el servicio PHPMyAdmin mediante apt-get y configuramos nuestras contraseñas de acceso:



Figura 20.1: Instalación de PHPMyAdmin en Ubuntu

Para comprobar su funcionamiento, accedemos de forma remota a la configuración de PHPMyAdmin consultando la dirección [IP]/phpmyadmin:

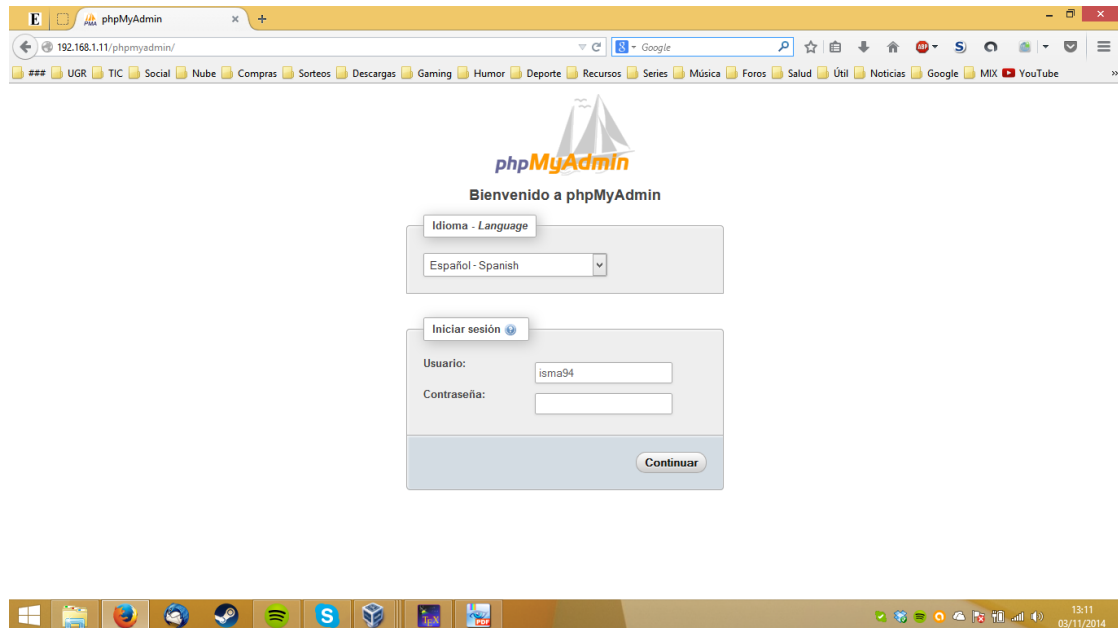


Figura 20.2: Acceso Remoto a PHPMyAdmin

Una vez introducidas nuestras credenciales de acceso, accedemos al menú de configuración de PHPMyAdmin:

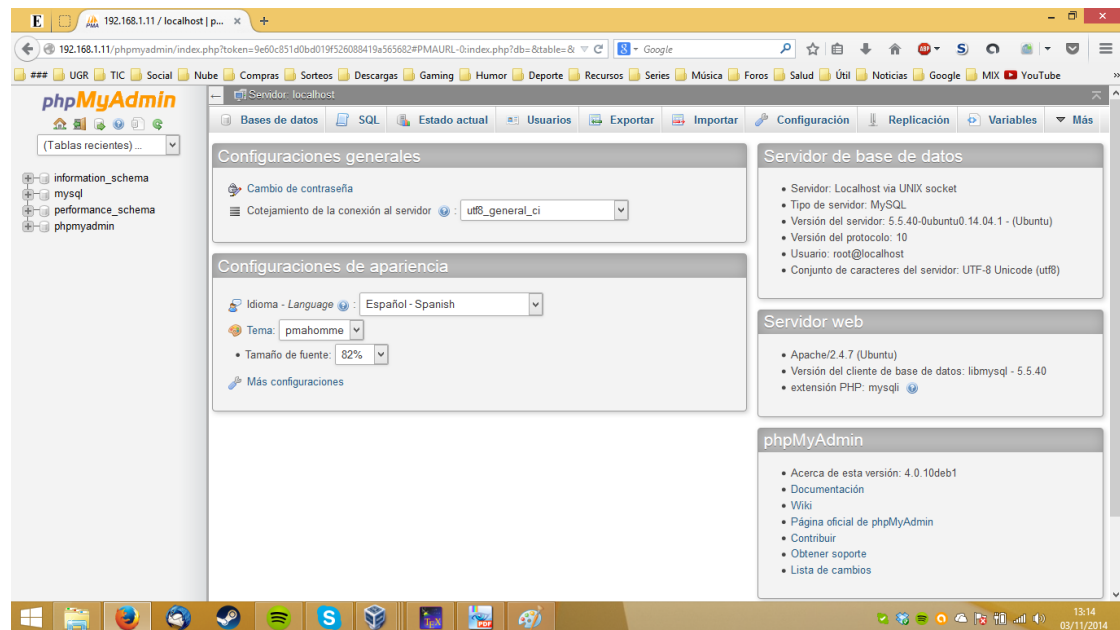


Figura 20.3: Menú de Configuración de PHPMyAdmin

Para ampliar el límite de tamaño al importar bases de datos, debemos editar el archivo de configuración /etc/php5/apache2/php.ini.

La variable post_max_size define el tamaño máximo permitido para subida de datos. Para poder importar ficheros grandes, debemos aumentar este valor, que además debe ser mayor que upload_max_filesize y menor que memory_limit para que funcione correctamente.

```
GNU nano 2.2.6      Archivo: /etc/php5/apache2/php.ini      Modificado

; This option is enabled by default.
; Most likely, you won't want to disable this option globally. It causes $_POST
; and $_FILES to always be empty; the only way you will be able to read the
; POST data will be through the php://input stream wrapper. This can be useful
; to proxy requests or to process the POST data in a memory efficient fashion.
; http://php.net/enable-post-data-reading
enable_post_data_reading = On

; Maximum size of POST data that PHP will accept.
; Its value may be 0 to disable the limit. It is ignored if POST data reading
; is disabled through enable_post_data_reading.
; http://php.net/post-max-size
post_max_size = 40MB_

; Automatically add files before PHP document.
; http://php.net/auto-prepend-file
auto_prepend_file =

; Automatically add files after PHP document.
; http://php.net/auto-append-file
auto_append_file =

; By default, PHP will output a character encoding using
; the Content-type: header. To disable sending of the charset, simply
; set it to be empty.

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y RePág.   ^K Cortar Tex ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^U Pág. Sig. ^U PegarTxt   ^T Ortografía
```

Figura 20.4: Ampliar Límite de Tamaño para Importar Bases de Datos (1)

```
GNU nano 2.2.6      Archivo: /etc/php5/apache2/php.ini      Modificado

;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
; http://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; http://php.net/upload-tmp-dir
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
upload_max_filesize = 20M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y RePág.    ^K Cortar Tex ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág. Sig. ^U PegarTxt   ^T Ortografía
```

Figura 20.5: Ampliar Límite de Tamaño para Importar Bases de Datos (2)


```
GNU nano 2.2.6      Archivo: /etc/php5/apache2/php.ini      Modificado

; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)
; http://php.net/max-input-time
max_input_time = 60

; Maximum input variable nesting level
; http://php.net/max-input-nesting-level
;max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
; max_input_vars = 1000

; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 200M_

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; This directive informs PHP of which errors, warnings and notices you would li$
; it to take action for. The recommended way of setting values for this
; directive is through the use of the error level constants and bitwise
; operators. The error level constants are below here for convenience as well as
; some common settings and their meanings.

[ Búsqueda recomenzada ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía
```

Figura 20.6: Ampliar Límite de Tamaño para Importar Bases de Datos (3)

21. VISITE AL MENOS UNA DE LAS WEBS DE LOS SOFTWARE MENCIONADOS (DIRECTADMIN E ISPCONFIG) Y PRUEBE LAS DEMOS QUE OFRECEN REALIZANDO CAPTURAS DE PANTALLA Y COMENTANDO QUÉ ESTÁ REALIZANDO.

Visitamos la demo online de DirectAdmin (<http://www.directadmin.com/demo.html>):

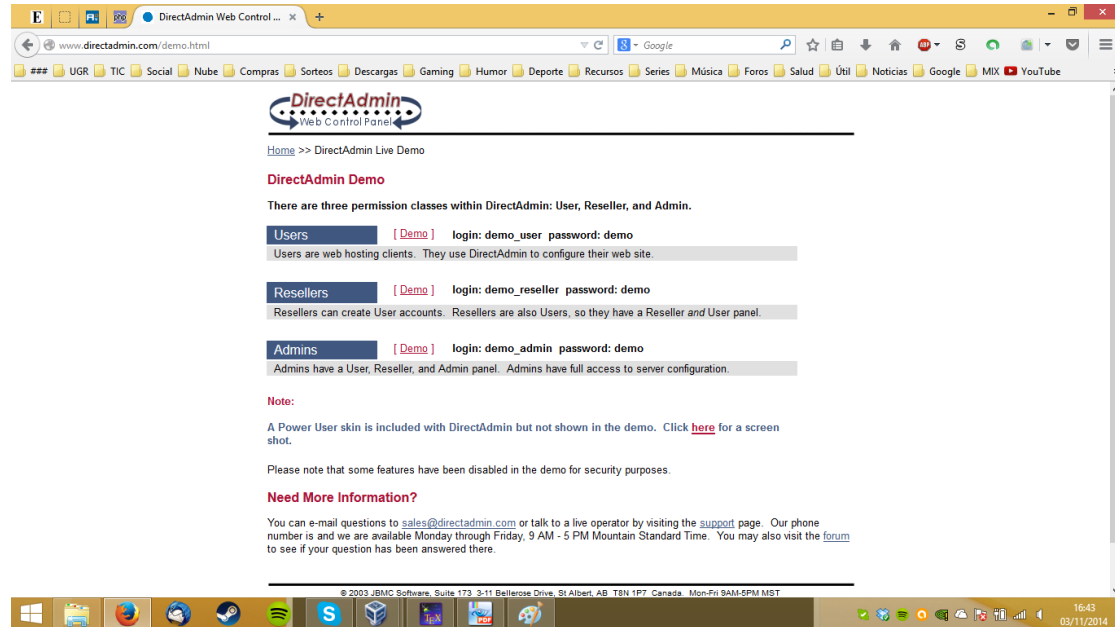


Figura 21.1: Demos Online de DirectAdmin

Para poder observar las opciones de configuración, accedemos a la demo de administrador (<https://www.directadmin.com:2222/>):

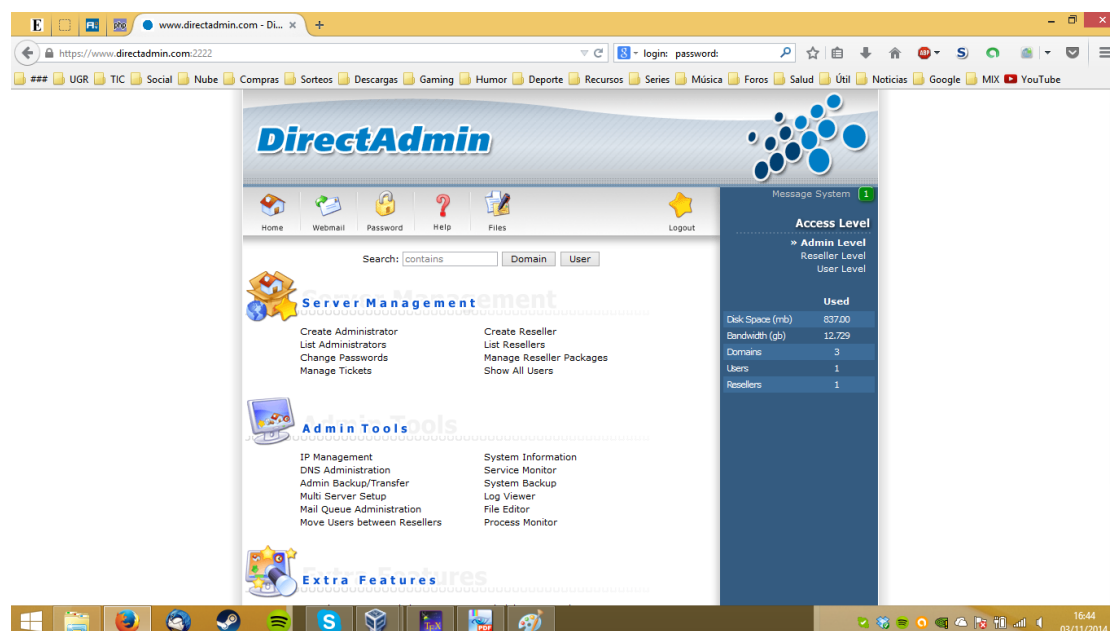


Figura 21.2: Menú de Configuración de DirectAdmin

Para observar el funcionamiento del servicio, podemos realizar diversas acciones, por ejemplo:

- Añadir una cuenta de administrador al sistema:

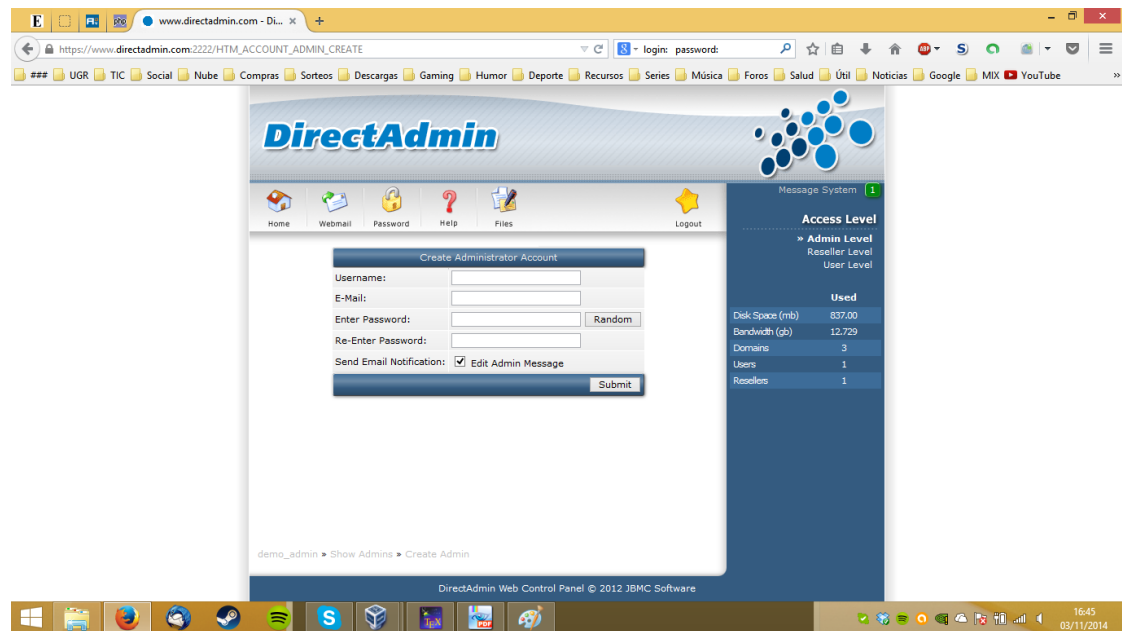


Figura 21.3: Añadir Administrador al Sistema en DirectAdmin

- Listar todos los usuarios del sistema:

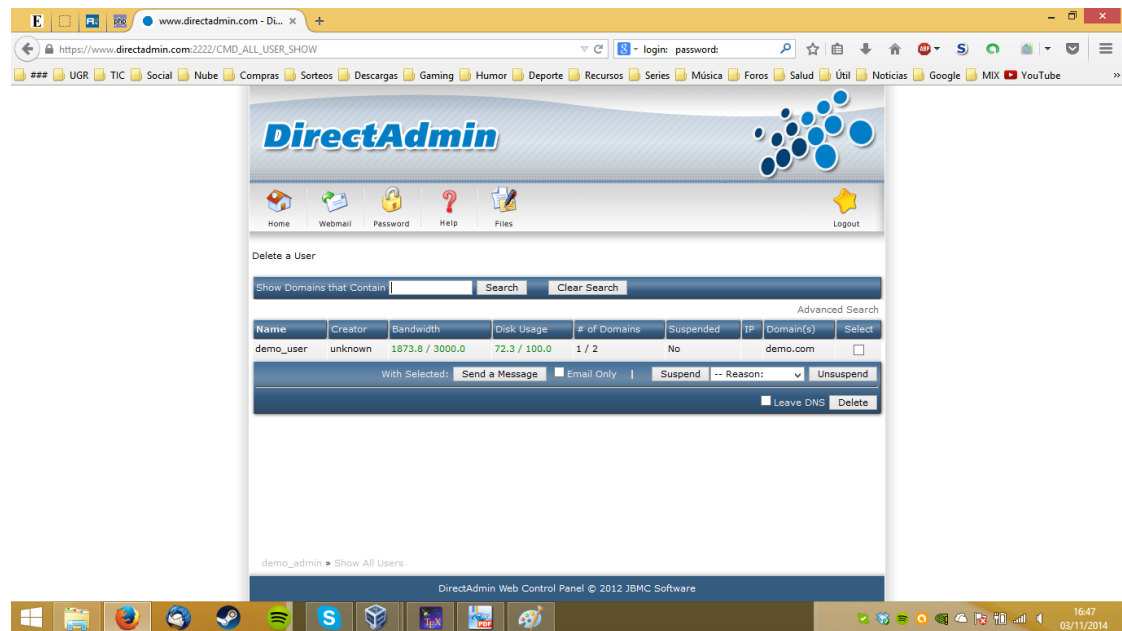


Figura 21.4: Listar Usuarios del Sistema en DirectAdmin

- Consultar la información del sistema:

The screenshot shows the DirectAdmin web interface in a browser window. The URL is https://www.directadmin.com:2222/CMD_SYSTEM_INFO. The interface has a top navigation bar with links like Home, Webmail, Password, Help, Files, and Logout. Below this is a table of system information with columns 'Name' and 'Value'. To the right of the table are sections for 'Access Level', 'Your Account', 'Bandwidth', and 'Disk Space'.

| Name | Value |
|-----------------------|-----------------------------------|
| Processor Name | Sperry 8088 |
| Vendor ID | Sperry |
| Processor Speed (MHz) | 4 |
| Total Memory | 640 kB |
| Free Memory | 12 kB |
| Total Swap Memory | 0 kB |
| Free Swap Memory | 0 kB |
| System Uptime | 8822 Days, 4 Hours and 23 Minutes |
| Apache 2.2.29 | Running |
| DirectAdmin 1.46.3 | Running |
| Exim 4.84 | Running |
| MySQL 5.5.39 | Running |
| Named 9.8.2rc1 | Running |
| ProFTPD 1.3.5 | Running |
| sshd | Running |
| dovecot 2.2.13 | Running |
| Php 5.3.29 | Installed |

Access Level
Admin Level
Reseller Level
» User Level

Your Account
Bandwidth
Disk Space

| | Used | Max |
|-----------------|--------|-----------|
| Disk Space (MB) | 72.3 | 100.0 |
| Bandwidth (GB) | 1.8298 | 2.9396 |
| E-Mails | 2 | 5 |
| Rp Accounts | 2 | 5 |
| Databases | 1 | 3 |
| Inodes | 8563 | unlimited |

Figura 21.5: Consultar Información del Sistema en DirectAdmin

Cualquier modificación de estas opciones está deshabilitada en la demo del servicio.

22. EJECUTE LOS EJEMPLOS DE FIND Y GREP Y ESCRIBA EL SCRIPT QUE HAGA USO DE SED PARA CAMBIAR LA CONFIGURACIÓN DE SSH Y REINICIAR EL SERVICIO. [25]

*** EJEMPLOS DE FIND Y GREP:**

```
isma94@ubuntuserver:~$ ps -Af | grep firefox
isma94    4557  1983  0 17:26 tty1      00:00:00 grep --color=auto firefox
isma94@ubuntuserver:~$ ls docs/
prueba.pdf
isma94@ubuntuserver:~$ ls pdfs/
isma94@ubuntuserver:~$ find /home/isma94/docs -name '*.pdf' -exec cp {} ~/pdfs \;
isma94@ubuntuserver:~$ ls docs/
prueba.pdf
isma94@ubuntuserver:~$ ls pdfs/
prueba.pdf
isma94@ubuntuserver:~$
```

Figura 22.1: Ejemplos de find y grep

*** SCRIPT BASH CON USO DE SED:**

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

```
sed -e 's/PermitRootLogin without-password/PermitRootLogin no/'
-e 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config > temp

cat temp > /etc/ssh/sshd_config
```

23. MUESTRE UN EJEMPLO DE USO PARA AWK. [26]

Primero, creamos un archivo de texto con una serie de líneas con diversa cantidad de palabras separadas por espacios:

```
GNU nano 2.2.6 Archivo: prueba Modificado
tomate lechuga pimiento zanahoria pepino
pimiento tomate lechuga pepino patata zanahoria
lechuga pimiento tomate patata zanahoria
zanahoria tomate pimiento patata lechuga berenjena calabaza
kiwi pimiento puerro coliflor cebolla
calabaza berenjena

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^U Pág. Sig. ^U PegarTxt ^T Ortografía
```

Figura 23.1: Fichero de Ejemplo para awk

Posteriormente, creamos un script awk que realice ciertas acciones cada vez que reconozca unos patrones en una línea del fichero:

```
GNU nano 2.2.6      Archivo: script.awk

{ print "LÍNEA", NR, ":"}

NF > 3 { print "Esta línea tiene más de 3 palabras" }
NF < 6 { print "Esta línea tiene menos de 6 palabras" }
$2 == "tomate" { print "Su segunda palabra es 'tomate'" }
$4 == "patata" { print "Su cuarta palabra es 'patata'" }
```

[6 líneas leídas]

| | | | | | |
|--------------------------|---------------------------|--------------------------|--------------------------|---------------------------|---------------------------|
| [^] G Ver ayuda | [^] O Guardar | [^] R Leer Fich | [^] Y RePág. | [^] K Cortar Tex | [^] C Pos actual |
| [^] X Salir | [^] J Justificar | [^] W Buscar | [^] V Pág. Sig. | [^] U PegarTxt | [^] T Ortografía |

Figura 23.2: Script awk de Ejemplo

Finalmente, ejecutamos el script sobre el archivo mediante el comando awk y observamos los resultados:

```
isma94@ubuntuserver:~$ awk -f script.awk prueba
LÍNEA 1 :
Esta línea tiene más de 3 palabras
Esta línea tiene menos de 6 palabras
LÍNEA 2 :
Esta línea tiene más de 3 palabras
Su segunda palabra es 'tomate'
LÍNEA 3 :
Esta línea tiene más de 3 palabras
Esta línea tiene menos de 6 palabras
Su cuarta palabra es 'patata'
LÍNEA 4 :
Esta línea tiene más de 3 palabras
Su segunda palabra es 'tomate'
Su cuarta palabra es 'patata'
LÍNEA 5 :
Esta línea tiene más de 3 palabras
Esta línea tiene menos de 6 palabras
LÍNEA 6 :
Esta línea tiene menos de 6 palabras
isma94@ubuntuserver:~$ _
```

Figura 23.3: Ejecución del Ejemplo awk

24. ESCRIBA EL SCRIPT PARA CAMBIAR EL ACCESO A SSH USANDO PHP O PYTHON. [23]

```
GNU nano 2.2.6      Archivo: script.php

#!/usr/bin/php

<?php

$ssh = ssh2_connect('192.168.1.90', 22);

ssh2_auth_password($ssh, 'isma94', 'asdf');

ssh2_scp_send($ssh, 'prueba', 'prueba', 0644);

?>_

[ 11 líneas leídas ]
^G Ver ayuda  ^O Guardar    ^R Leer Fich  ^Y RePág.     ^K Cortar Tex ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág. Sig.  ^U PegarTxt   ^T Ortografía
```

Figura 24.1: Script PHP para Acceder a SSH

25. ABRA UNA CONSOLA DE POWERSHELL Y PRUEBE A PARAR UN PROGRAMA EN EJECUCIÓN, REALICE CAPTURAS DE PANTALLA Y COMENTE LO QUE MUESTRA.

Primero, abrimos la consola de PowerShell y consultamos los procesos en ejecución con el comando get-process:

| Handles | NPM(K) | PM(K) | WS(K) | VM(K) | CPU(s) | Id | ProcessName |
|---------|--------|--------|-------|-------|--------|------|------------------|
| 39 | 5 | 1804 | 4164 | 43 | 2.25 | 1088 | conhost |
| 49 | 5 | 1024 | 3048 | 43 | 0.00 | 1256 | conhost |
| 364 | 11 | 1672 | 3676 | 43 | 0.17 | 292 | csrss |
| 175 | 10 | 1660 | 4876 | 41 | 0.69 | 332 | csrss |
| 72 | 7 | 1380 | 4312 | 50 | 0.05 | 1588 | dsm |
| 509 | 34 | 13356 | 26268 | 152 | 0.89 | 1544 | explorer |
| 0 | 0 | 0 | 24 | 0 | 0.00 | 0 | idle |
| 139 | 14 | 5956 | 11880 | 64 | 0.17 | 1032 | inetinfo |
| 45 | 7 | 984 | 3416 | 60 | 0.02 | 2008 | jsm |
| 543 | 19 | 3348 | 9392 | 38 | 0.59 | 436 | lsass |
| 142 | 7 | 2144 | 3764 | 18 | 0.03 | 444 | lsm |
| 149 | 17 | 3312 | 7444 | 60 | 0.03 | 688 | msdtc |
| 268 | 40 | 38368 | 32880 | 586 | 2.03 | 1652 | Oobe |
| 457 | 25 | 79624 | 80724 | 570 | 3.48 | 1848 | powershell |
| 212 | 12 | 4360 | 7856 | 32 | 0.61 | 428 | services |
| 29 | 2 | 352 | 1016 | 5 | 0.11 | 212 | smss |
| 264 | 18 | 6016 | 10412 | 73 | 0.03 | 680 | spoolsv |
| 149 | 8 | 2292 | 7960 | 33 | 0.86 | 1660 | sppsv |
| 132 | 13 | 4084 | 8320 | 39 | 0.06 | 492 | svchost |
| 344 | 14 | 3316 | 8252 | 41 | 0.30 | 536 | svchost |
| 242 | 15 | 2680 | 6360 | 30 | 0.11 | 612 | svchost |
| 287 | 15 | 8976 | 11608 | 43 | 0.50 | 700 | svchost |
| 832 | 40 | 21296 | 26712 | 127 | 1.09 | 736 | svchost |
| 275 | 21 | 4972 | 9656 | 41 | 0.20 | 780 | svchost |
| 206 | 15 | 3680 | 9488 | 61 | 0.09 | 828 | svchost |
| 394 | 32 | 12608 | 15004 | 83 | 0.48 | 872 | svchost |
| 297 | 33 | 9272 | 11592 | 48 | 0.45 | 1000 | svchost |
| 96 | 10 | 4356 | 8688 | 38 | 0.09 | 1020 | svchost |
| 46 | 4 | 780 | 2572 | 13 | 0.00 | 1152 | svchost |
| 130 | 13 | 6312 | 9708 | 39 | 0.13 | 1296 | svchost |
| 68 | 6 | 1344 | 4224 | 29 | 0.05 | 1512 | svchost |
| 633 | 0 | 112 | 300 | 3 | 0.00 | 4 | System |
| 139 | 11 | 2764 | 5988 | 52 | 0.05 | 1956 | taskhost |
| 305 | 23 | 156672 | 80044 | 399 | 3.77 | 1232 | TOMCAT |
| 73 | 8 | 1172 | 4052 | 61 | 0.02 | 228 | TOMCATw |
| 124 | 9 | 2000 | 6644 | 50 | 0.17 | 1452 | TrustedInstaller |
| 88 | 9 | 2108 | 6392 | 91 | 0.13 | 1720 | UIODetect |
| 81 | 9 | 1316 | 4124 | 43 | 0.08 | 340 | wininit |
| 93 | 7 | 1448 | 4624 | 27 | 0.11 | 368 | winlogon |
| 44 | 6 | 860 | 3164 | 22 | 0.02 | 1320 | wlm |

Figura 25.1: Consultar Procesos en Ejecución con PowerShell

Posteriormente, usamos el comando stop-process con las opciones pertinentes para detener el proceso de Tomcat:

```

Administrador: Windows PowerShell

236    15    2960    6660    30    0.11    612 svchost
291    15    8480    11048    43    0.58    700 svchost
790    34    13416    24940    109    1.20    736 svchost
272    21    5240    9924    41    0.27    780 svchost
261    15    3884    9788    62    0.16    828 svchost
504    36    13460    16272    89    0.67    872 svchost
295    32    9392    11640    48    0.52    1000 svchost
92     10    4356    8692    38    0.09    1020 svchost
46     4     780     2572    13    0.00    1152 svchost
130    13    6312    9740    39    0.13    1296 svchost
68     6     1344    4224    29    0.05    1512 svchost
620    0     112     300     3     0.00    4 System
141    11    2712    5996    51    0.05    1956 taskhost
324    24    156592    80024    401    2.14    2876 TOMCAT
74     8     1172    4068    61    0.02    228 TOMCATw
88     9     2140    6436    91    0.16    1720 UI0Detect
81     9     1316    4124    43    0.08    340 wininit
93     7     1448    4712    27    0.11    368 winlogon
44     6     860     3164    22    0.02    1320 wlms

PS C:\Users\Administrador> stop-service -name TOMCAT
PS C:\Users\Administrador> stop-service -name TOMCATw
Stop-Service : No se encuentra ningún servicio con el nombre 'TOMCATw'.
En línea: 1 Carácter: 13
+ stop-service <<<< -name TOMCATw
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (TOMCATw:String) [Stop-Service], ServiceCommandException
+ FullyQualifiedErrorId : NoServiceFoundForGivenName,Microsoft.PowerShell.Commands.StopServiceCommand

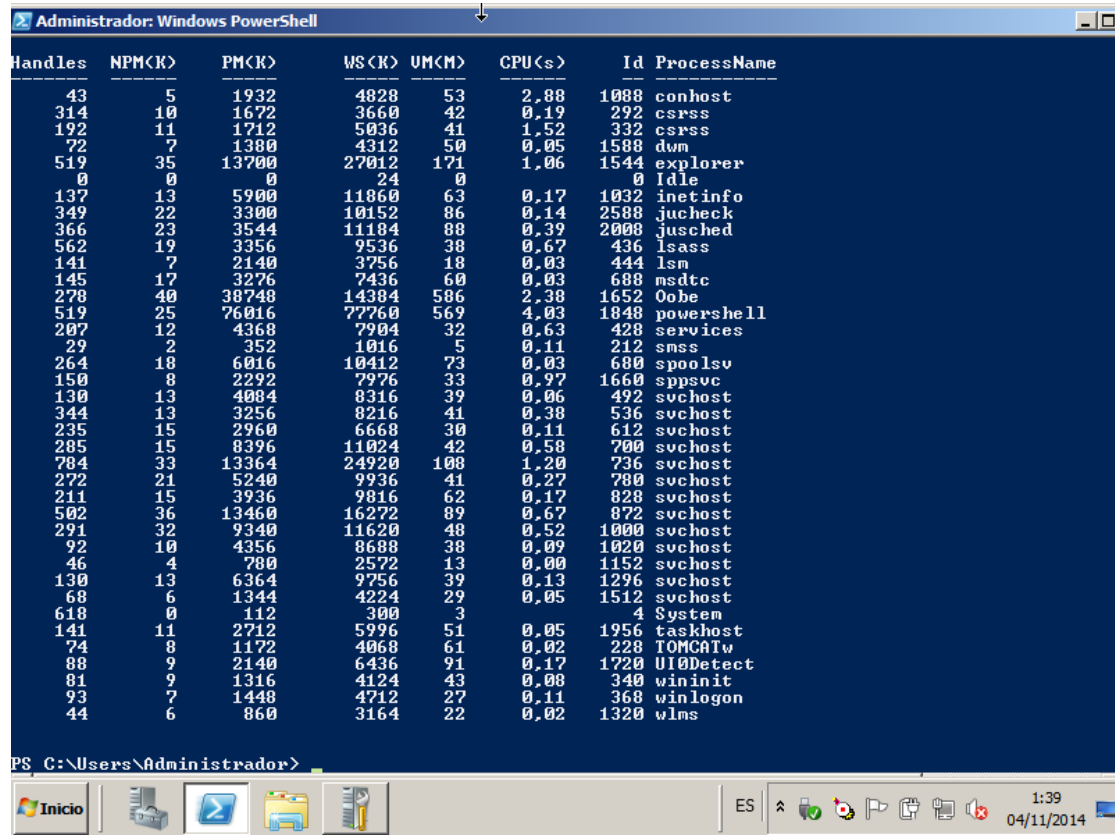
PS C:\Users\Administrador> stop-service -id 2876
Stop-Service : No se encuentra ningún parámetro que coincida con el nombre del parámetro 'id'.
En línea: 1 Carácter: 17
+ stop-service -id <<<< 2876
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Stop-Service], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.StopServiceCommand

PS C:\Users\Administrador> stop-service -id 228
Stop-Service : No se encuentra ningún parámetro que coincida con el nombre del parámetro 'id'.
En línea: 1 Carácter: 17
+ stop-service -id <<<< 228
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Stop-Service], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.StopServiceCommand

PS C:\Users\Administrador>
  
```

Figura 25.2: Detener Proceso con PowerShell

Finalmente, volvemos a consultar la lista de procesos para comprobar que hemos tenido éxito:



| Handles | NPM(K) | PM(K) | WS(K) | VM(M) | CPU(s) | Id | ProcessName |
|---------|--------|-------|-------|-------|--------|------|-------------|
| 43 | 5 | 1932 | 4828 | 53 | 2.88 | 1088 | conhost |
| 314 | 10 | 1672 | 3660 | 42 | 0.19 | 292 | csrss |
| 192 | 11 | 1712 | 5036 | 41 | 1.52 | 332 | csrss |
| 72 | 7 | 1380 | 4312 | 50 | 0.05 | 1588 | dwm |
| 519 | 35 | 13700 | 27012 | 171 | 1.06 | 1544 | explorer |
| 0 | 0 | 0 | 24 | 0 | | 0 | Idle |
| 137 | 13 | 5900 | 11860 | 63 | 0.17 | 1032 | inetinfo |
| 349 | 22 | 3300 | 10152 | 86 | 0.14 | 2588 | jucheck |
| 366 | 23 | 3544 | 11184 | 88 | 0.39 | 2008 | jusched |
| 562 | 19 | 3356 | 9536 | 38 | 0.67 | 436 | lsass |
| 141 | 7 | 2140 | 3756 | 18 | 0.03 | 444 | lsn |
| 145 | 17 | 3276 | 7436 | 60 | 0.03 | 688 | msdtc |
| 278 | 40 | 38748 | 14384 | 586 | 2.38 | 1652 | Oobe |
| 519 | 25 | 76016 | 77760 | 569 | 4.03 | 1848 | powershell |
| 207 | 12 | 4368 | 7904 | 32 | 0.63 | 428 | services |
| 29 | 2 | 352 | 1016 | 5 | 0.11 | 212 | smss |
| 264 | 18 | 6016 | 10412 | 73 | 0.03 | 680 | spoolsv |
| 150 | 8 | 2292 | 7976 | 33 | 0.97 | 1660 | sppsuc |
| 130 | 13 | 4004 | 9316 | 39 | 0.06 | 492 | svchost |
| 344 | 13 | 3256 | 8216 | 41 | 0.38 | 536 | svchost |
| 235 | 15 | 2960 | 6668 | 30 | 0.11 | 612 | svchost |
| 285 | 15 | 8396 | 11024 | 42 | 0.58 | 700 | svchost |
| 784 | 33 | 13364 | 24920 | 108 | 1.20 | 736 | svchost |
| 272 | 21 | 5240 | 9936 | 41 | 0.27 | 780 | svchost |
| 211 | 15 | 3936 | 9816 | 62 | 0.17 | 828 | svchost |
| 502 | 36 | 13460 | 16272 | 89 | 0.67 | 872 | svchost |
| 291 | 32 | 9340 | 11620 | 48 | 0.52 | 1000 | svchost |
| 92 | 10 | 4356 | 8688 | 38 | 0.09 | 1020 | svchost |
| 46 | 4 | 780 | 2572 | 13 | 0.00 | 1152 | svchost |
| 130 | 13 | 6364 | 9756 | 39 | 0.13 | 1296 | svchost |
| 68 | 6 | 1344 | 4224 | 29 | 0.05 | 1512 | svchost |
| 618 | 0 | 112 | 300 | 3 | | 4 | System |
| 141 | 11 | 2712 | 5996 | 51 | 0.05 | 1956 | taskhost |
| 74 | 8 | 1172 | 4068 | 61 | 0.02 | 228 | TOMCATw |
| 88 | 9 | 2140 | 6436 | 91 | 0.17 | 1720 | UI0Detect |
| 81 | 9 | 1316 | 4124 | 43 | 0.08 | 340 | wininit |
| 93 | 7 | 1448 | 4712 | 27 | 0.11 | 368 | winlogon |
| 44 | 6 | 860 | 3164 | 22 | 0.02 | 1320 | wlms |

PS C:\Users\Administrador>

Figura 25.3: Comprobar Procesos en Ejecución con PowerShell

REFERENCIAS

- [1] <http://blog-alexis.rhcloud.com/2011/06/26/ssh-copy-id-la-vida-un-poco-mas-facil/>.
- [2] <http://blog.desdelinux.net/configurar-ssh-por-otro-puerto-y-no-por-el-22/>.
- [3] <http://blog.desdelinux.net/x11-forwarding-a-traves-de-ssh/>.
- [4] http://docs.fedoraproject.org/es-es/fedora_core/4/html/software_management_guide/sn-yum-proxy-server.html.
- [5] <http://docs.mongodb.org/manual/tutorial/generate-test-data/>.
- [6] <http://docs.mongodb.org/manual/tutorial/getting-started/>.
- [7] <http://docs.mongodb.org/manual/tutorial/install-mongodb-on-red-hat-centos-or-fedora-linux/>.
- [8] <http://docs.mongodb.org/manual/tutorial/manage-mongodb-processes/>.
- [9] <http://es1.php.net/manual/es/ini.core.php>.
- [10] <http://es.opensuse.org/gesti>
- [11] http://es.wikipedia.org/wiki/secure_shell.
- [12] http://es.wikipedia.org/wiki/servidor_web.
- [13] <http://es.wikipedia.org/wiki/telnet>.
- [14] <http://kb.sp.parallels.com/es/1569>.
- [15] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sectesting_managing_yum_repositories.html.
- [16] <https://andalinux.wordpress.com/2009/08/24/crear-y-aplicar-parches-patches-en-linux/>.
- [17] <https://help.ubuntu.com/12.04/serverguide/lamp-overview.html>.
- [18] <https://help.ubuntu.com/community/aptget/howto>.
- [19] <https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-centos-7>.
- [20] <https://www.digitalocean.com/community/tutorials/how-to-install-webmin-on-an-ubuntu-cloud-server>.
- [21] <https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-12-04>.

- [22] <http://tuxpepino.wordpress.com/2007/05/24/>
- [23] <http://www.admin-magazine.com/articles/automation-scripting-with-php>.
- [24] http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m5/instalacin_y_configuracin_de_phpmy
- [25] <http://www.lawebdelprogramador.com/temas/sed.php>.
- [26] <http://www.linux-es.org/node/31>.
- [27] <http://www.marlonj.com/blog/2008/12/reiniciar-servicios-en-ubuntu/>.
- [28] <http://www.webmin.com/firewall.html>.