

Ingeniería de Servidores (2016-2017)
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

Instalación y configuración de servicios

Manuel Jiménez Molina

3 de febrero de 2017

Índice

1. a) Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes. b) ¿Qué ha de hacer para que yum pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128) c) ¿Cómo añadimos un nuevo repositorio?	8
1.1. a) Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes.	8
1.2. b) ¿Qué ha de hacer para que yum pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128)	9
1.3. c) ¿Cómo añadimos un nuevo repositorio?	11
2. a) Liste los argumentos de apt necesarios para instalar, buscar y eliminar paquetes. b) ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128) c) ¿Cómo añadimos un nuevo repositorio?	12
2.1. a) Liste los argumentos de apt necesarios para instalar, buscar y eliminar paquetes.	12
2.2. b) ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128)	14
2.3. c) ¿Cómo añadimos un nuevo repositorio?	15
3. a) ¿Con qué comando puede abrir/cerrar un puerto usando ufw? Muestre un ejemplo de cómo lo ha hecho b) ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOS? Muestre un ejemplo de cómo lo ha hecho c) Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles	16
3.1. a) ¿Con qué comando puede abrir/cerrar un puerto usando ufw?	16
3.2. b) ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOS? Muestre un ejemplo de cómo lo ha hecho	17
3.3. c) Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles	19
4. ¿Qué diferencia hay entre telnet y ssh?	24
5. a) ¿Para qué sirve la opción -X? b) 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?	24
5.1. a) ¿Para qué sirve la opción -X?	24
5.2. b) 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?	24

6. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña. Pruebe que funciona. (Pistas: ssh-keygen, ssh-copy-id) 33
7. ¿Qué archivo es el que contiene la configuración del servicio ssh? ¿Qué parámetro hay que modificar para evitar que el usuario root acceda? Cambie el puerto por defecto y compruebe que puede acceder. 35
8. Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo. 40
9. ¿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). Compruebe que la instalación ha sido correcta. 41
10. Realice la instalación usando GUI o PowerShell y compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona 48
11. Muestre un ejemplo de uso del comando (p.e. <http://fedoraproject.org/wiki/VMWare>) 54
12. 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 56
13. Instale phpMyAdmin, indique cómo lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs de hasta 25MiB (en vez de los 8 MiB de límite por defecto). Indique cómo ha realizado el proceso y muestre capturas de pantalla. 59
14. Visite al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando qué está realizando. 64
15. a) Ejecute los ejemplos de find, grep b) Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio. c) Muestre un ejemplo de uso para awk 66
 - 15.1. a) Ejecute los ejemplos de find, grep 66
 - 15.2. b) Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio. 67
 - 15.3. c) Muestre un ejemplo de uso para awk 68
16. Escriba el script para cambiar el acceso a ssh usando PHP o Python. 69
17. Abra una consola de Powershell y pruebe a parar un programa en ejecución (p.ej), realice capturas de pantalla y comente lo que muestra. 71

18.Opcional 1: Instale y pruebe terminator y/o tmux. Con screen, pruebe su funcionamiento dejando sesiones ssh abiertas en el servidor y recuperándolas posteriormente.	75
19.Opcional 2: Instale el servicio y pruebe su funcionamiento.	75
20.Opcional 3:Instale el servicio y pruebe su funcionamiento.	78
21.Opcional 4:Realice la instalación de uno de estos dos “web containers” y pruebe su ejecución	80
22.Opcional 5: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/)	80

Índice de figuras

1.1. Uso de yum install	8
1.2. Uso de yum search	8
1.3. Uso de yum remove	9
1.4. Añadiendo el proxy en yum.conf	9
1.5. Parte 1. Probando yum install con proxy cambiado	10
1.6. Parte 2. Probando yum install con proxy cambiado	10
1.7. Parte 3. Probando yum install con proxy cambiado	11
1.8. Uso de yum-config-manager para añadir repositorio	11
1.9. Activación del repositorio con yum-config-manager	11
1.10. Comprobar que un nuevo repositorio se creó en /etc/yum.repos.d/	11
1.11. Ver contenido de kde.repo	12
2.1. Uso de apt install para gedit	13
2.2. Uso de apt search para gedit	13
2.3. Paquetes mostrados por apt search para gedit	13
2.4. Uso de apt remove para borrar el paquete nmap	14
2.5. Creación de archivo apt.conf	14
2.6. Ver contenido apt.conf	14
2.7. Comprobación de no conexión con nuevo proxy	15
2.8. Uso de add-apt-repository	15
2.9. Añadir nuevo repositorio modificando /etc/apt/sources.list	16
3.1. Habilitar puerto 200/tcp con ufw	17
3.2. Deshabilitar puerto 200/tcp con ufw	17
3.3. Abrir puerto no permanente con firewall-cmd	18
3.4. Comprobar puerto no permanente con firewall-cmd	18
3.5. Abrir puerto permanente con firewall-cmd	18
3.6. Comprobar puerto permanente con firewall-cmd	18
3.7. Cerrado y comprobación puerto no permanente con firewall-cmd	19

3.8.	Cerrado y comprobación puerto permanente con firewall-cmd	19
3.9.	Escenario 1, localhost usando nmap	20
3.10.	Escenario 1, desde fuera usando nmap	20
3.11.	Escenario 2, localhost usando nmap	21
3.12.	Escenario 2, desde fuera usando nmap	21
3.13.	Escenario 3, localhost usando nmap	22
3.14.	Escenario 3, desde fuera usando nmap	22
3.15.	Escenario 4, localhost usando nmap	23
3.16.	Escenario 4, desde fuera usando nmap	23
5.1.	Configuración de red para máquina virtual, adaptador 1	25
5.2.	Configuración de red para máquina virtual, adaptador 2	25
5.3.	Habilitar X11 de ssh en fichero sshd_config para permitir gráficos remotos	26
5.4.	Habilitar X11 de ssh en fichero sshd_config para permitir gráficos remotos	27
5.5.	Habilitar X11 de ssh en fichero sshd_config para permitir gráficos remotos	27
5.6.	Redes de la máquina Ubuntu Server	28
5.7.	Activar interfaz eth1	28
5.8.	Configurar interfaz eth1 con dhclient	29
5.9.	Ver contenido de /etc/network/interfaces	29
5.10.	Añadir configuración para interfaz eth1 en /etc/network/interfaces	30
5.11.	Copia del archivo interfaces	30
5.12.	Comprobación de interfaces tras los cambios	31
5.13.	Comprobación de firewall y servicio ssh	31
5.14.	Uso remoto de ssh sin opción -X	32
5.15.	Uso remoto de ssh con opción -X	33
6.1.	Generación de claves con ssh-keygen	34
6.2.	Ver permisos de las claves generadas	34
6.3.	Copiar clave pública a una máquina remota	35
6.4.	Conexión remota por ssh sin introducir contraseña	35
7.1.	Modificando parámetro PermitRootLogin a no en ssh	36
7.2.	Conexion remota por ssh accediendo como root con PermitRootLogin no	37
7.3.	Modificando parámetro PermitRootLogin a yes en ssh	37
7.4.	Conexion remota por ssh accediendo como root con PermitRootLogin yes	38
7.5.	Cambiando puerto por defecto de ssh	39
7.6.	Intentando acceder por el puerto 22 a ssh	39
7.7.	Accediendo a ssh por el puerto 1000	39
8.1.	Ubuntu. Reiniciando servicio con orden service	40
8.2.	Reiniciando servicio buscando servicio en /etc/init.d	40
8.3.	CentOS. Reiniciando servicio con orden service	40
9.1.	Usando tasksel para instalar LAMP	41
9.2.	Establecer contraseña para mysql-server	42
9.3.	Servidor Apache2 funcionando en Ubuntu Server	43
9.4.	Archivo de html por defecto de Apache2	44
9.5.	Archivo de configuración MySQL	45
9.6.	Comprobando funcionamiento MySQL	45

9.7. Archivo de configuración php	46
9.8. Probando php	46
9.9. Servidor Apache en CentOS	47
9.10. MariaDB funcionando en CentOS	47
9.11. php funcionando en CentOS	48
10.1. Windows Server. Agregar roles	49
10.2. Windows Server. Instalar ISS	50
10.3. Windows Server. Resultados de la instalación de ISS	51
10.4. Windows Server. Dirección de la máquina virtual	52
10.5. Windows Server. Dirección de la máquina virtual	53
10.6. Comprobación de ISS en máquina anfitriona	54
11.1. Creando archivo probando-patch.cpp	54
11.2. Creando archivo probando-patch-modificado.cpp	55
11.3. Creando archivo parche.patch	55
11.4. Aplicando parche a probando-patch.cpp	56
12.1. Estableciendo configuración Webmin	57
12.2. Webmin instalado correctamente	57
12.3. Comprobando Webmin remotamente	58
12.4. Iniciando sesión en Webmin remotamente	59
13.1. Instalando phpmyadmin	60
13.2. Instalando phpmyadmin, eligiendo Apache2 como server	60
13.3. Instalando phpmyadmin. No configurar DB con dbconfig-common	61
13.4. Cambiando archivo de configuracion phpmyadmin. Variable post_max_size	61
13.5. Cambiando archivo de configuracion phpmyadmin. Variable upload_max_filesize	62
13.6. Comprobando remotamente phpmyadmin	63
13.7. Iniciando remotamente a phpmyadmin	63
13.8. Comprobando remotamente tamaño de exportación BDs de phpmyadmin	64
14.1. DirectAdmin. Monitorización de servicios	65
14.2. DirectAdmin. Gestión de paquetes de distribuidores	65
14.3. DirectAdmin. Creación de admin	66
15.1. Ejemplo de uso de comando grep	66
15.2. Exportar archivo pdf por ssh	67
15.3. Comprobando exportación por ssh	67
15.4. Ejemplo de uso de comando find	67
15.5. Script creado con sed para cambiar configuración ssh	67
15.6. Ejecutando script que usa comando sed	68
15.7. Comprobando cambios que realizó el script con sed	68
15.8. Ejemplo de uso para awk	68
16.1. Script en php para acceso a ssh	69
16.2. Ejecución de script en php para acceso a ssh	69
16.3. Comprobar cambios en ssh tras ejecutar script en php	70
16.4. Conexión por ssh al puerto 500	70
17.1. Instalando ISE en Windows Server	71
17.2. ISE resultados de la instalación en Windows Server	72

17.3. Abriendo Paint en Windows Server	73
17.4. Viendo procesos activos con PowerShell	74
17.5. Parando proceso activo con PowerShell	75
19.1. Configuración de fail2ban para ssh	76
19.2. Modificando configuración de fail2ban para ssh	77
19.3. Baneo de fail2ban	78
19.4. Conexión ssh tras esperar baneo de fail2ban	78
20.1. Foto 1.Rkhunter analizando sistema	79
20.2. Foto 2.Rkhunter analizando sistema	79
20.3. Resumen del análisis de Rkhunter	80

Índice de tablas

1. a) Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes. b) ¿Qué ha de hacer para que yum pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128) c) ¿Cómo añadimos un nuevo repositorio?
- 1.1. a) Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes.

Viendo el manual de yum[11] podemos ver los siguientes comandos:

- Para instalar: yum install <paquete>

```
root@localhost manolo 2016-11-18 16:40:06
$ sudo yum install elinks
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: sunsite.rediris.es
* extras: centos.uvigo.es
* updates: sunsite.rediris.es
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete elinks.x86_64 0:0.12-0.36.pre6.el7 debe ser instalado
--> Procesando dependencias: libnss_compat_oss1.so.0()(64bit) para el paquete: e
links-0.12-0.36.pre6.el7.x86_64
--> Procesando dependencias: libmozjs185.so.1.0()(64bit) para el paquete: elinks
-0.12-0.36.pre6.el7.x86_64
--> Ejecutando prueba de transacción
--> Paquete js.x86_64 1:1.8.5-19.el7 debe ser instalado
--> Paquete nss_compat_oss1.x86_64 0:0.9.6-8.el7 debe ser instalado
--> Resolución de dependencias finalizada
```

Figura 1.1: Uso de yum install

- Para buscar: yum search <paquete>

```
root@localhost manolo 2016-11-18 16:44:01
$ yum search elinks
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: sunsite.rediris.es
* extras: centos.uvigo.es
* updates: sunsite.rediris.es
===== N/S matched: elinks =====
elinks.x86_64 : A text-mode Web browser

Nombre y resumen que coinciden con y sólo, use "buscar todo" para todo.
root@localhost manolo 2016-11-18 16:44:26
$
```

Figura 1.2: Uso de yum search

- Para eliminar: yum remove | erase <paquete>


```
root@localhost manolo 2016-11-18 16:42:23
$ sudo yum remove elinks
Complementos cargados:fastestmirror, langpacks
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete elinks.x86_64 0:0.12-0.36.pre6.el7 debe ser eliminado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package           Arquitectura  Versión           Repositorio      Tamaño
=====
Eliminando:
elinks             x86_64        0.12-0.36.pre6.el7 @base            2.6 M
=====
Resumen de la transacción
=====
Eliminar 1 Paquete

Tamaño instalado: 2.6 M
¿Está de acuerdo [s/N]:
```

Figura 1.3: Uso de yum remove

1.2. b) ¿Qué ha de hacer para que yum pueda tener acceso a Internet en el PC del aula?(Pistas: archivo de configuración en /etc,proxy: stargate.ugr.es:3128)

Tenemos que cambiar el proxy del archivo /etc/yum.conf[10]. Los pasos serían:

- Modificar el fichero /etc/yum.conf. Añadiremos la línea proxy=http://stargate.ugr.es:3128 :

```
GNU nano 2.3.1          Fichero: /etc/yum.conf

[main]
cachedir=/var/cache/yum/$basearch/$releasever
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=5
bugtracker_url=http://bugs.centos.org/set_project.php?project_id=23&ref=http://$
distroverpkg=centos-release

# This is the default, if you make this bigger yum won't see if the metadata
# is newer on the remote and so you'll "gain" the bandwidth of not having to
# download the new metadata and "pay" for it by yum not having correct
# information.
# It is esp. important, to have correct metadata, for distributions like
# Fedora which don't keep old packages around. If you don't like this checking
# interrupting your command line usage, it's much better to have something
# manually check the metadata once an hour (yum-updatesd will do this).
# metadata_expire=90m

# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d

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

Figura 1.4: Añadiendo el proxy en yum.conf

- Comprobamos que como estoy con mi ordenador local en casa, yum no tendrá acceso a Internet debido a que el proxy indicado no sirve fuera de la red universitaria. Hacemos por ejemplo yum install y comprobamos que no funciona:

```
$ yum install nmap
Complementos cargados:fastestmirror, langpacks
Could not retrieve mirrorlist http://mirrorlist.centos.org/?release=7&arch=x86_64&repo=os&infra=stock error was
14: curl#52 - "Empty reply from server"
http://ftp.cica.es/CentOS/7.2.1511/os/x86_64/repodata/repomd.xml: [Errno 14] curl#52 - "Empty reply from server"
Intentando con otro espejo.
http://centos.mirror.xtratelecom.es/7.2.1511/os/x86_64/repodata/repomd.xml: [Errno 14] curl#52 - "Empty reply from server"
Intentando con otro espejo.
http://centos.uvigo.es/7.2.1511/os/x86_64/repodata/repomd.xml: [Errno 14] curl#52 - "Empty reply from server"
Intentando con otro espejo.
```

Figura 1.5: Parte 1. Probando yum install con proxy cambiado

```
Loading mirror speeds from cached hostfile
* base: centos.uvigo.es
* extras: sunsite.rediris.es
* updates: sunsite.rediris.es
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete nmap.x86_64 2:6.40-7.el7 debe ser instalado
--> Procesando dependencias: nmap-ncat = 2:6.40-7.el7 para el paquete: 2:nmap-6.40-7.el7.x86_64
--> Ejecutando prueba de transacción
--> Paquete nmap-ncat.x86_64 2:6.40-7.el7 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package           Arquitectura  Versión      Repositorio  Tamaño
=====
Instalando:
nmap               x86_64       2:6.40-7.el7 base          4.0 M
Instalando para las dependencias:
nmap-ncat          x86_64       2:6.40-7.el7 base          201 k
=====
Resumen de la transacción
=====
Instalar 1 Paquete (+1 Paquete dependiente)

Tamaño total de la descarga: 4.2 M
Tamaño instalado: 17 M
Is this ok [y/d/N]: y
Downloading packages:
nmap-6.40-7.el7.x86_64.rpm FAILED
http://ftp.cica.es/CentOS/7.2.1511/os/x86_64/Packages/nmap-6.40-7.el7.x86_64.rpm: [Errno 14] curl#52 - "Empty reply from server"
Intentando con otro espejo.
nmap-ncat-6.40-7.el7.x86_64.rpm FAILED
```

Figura 1.6: Parte 2. Probando yum install con proxy cambiado

```

Error downloading packages:
 2:nmap-ncat-6.40-7.el7.x86_64: [Errno 256] No more mirrors to try.
 2:nmap-6.40-7.el7.x86_64: [Errno 256] No more mirrors to try.

root@localhost manolo 2016-11-18 17:01:30

```

Figura 1.7: Parte 3. Probando yum install con proxy cambiado

Podemos ver como finalmente no instala lo que le pedimos (nmap) ya que es incapaz de acceder Internet para detectar los paquetes necesarios. Puesto que desde casa esto funciona, suponemos que en los ordenadores de clase al no tener este proxy no les será posible acceder a Internet.

1.3. c) ¿Cómo añadimos un nuevo repositorio?

Se pueden añadir repositorios de varias formas[16, 14, 15]:

- Mediante el comando `yum-config-manager --add-repo repositoryURL`:
- Añadimos nuevo repositorio con `yum-config-manager`:

```

root@localhost manolo 2016-11-18 17:15:56
$ yum-config-manager --add-repo=http://apt.kde-redhat.org/apt/kde-redhat/fedora/
kde.repo
Complementos cargados:fastestmirror, langpacks
adding repo from: http://apt.kde-redhat.org/apt/kde-redhat/fedora/kde.repo
grabbing file http://apt.kde-redhat.org/apt/kde-redhat/fedora/kde.repo to /etc/y
um.repos.d/kde.repo
kde.repo | 799 B 00:00
repo saved to /etc/yum.repos.d/kde.repo
root@localhost manolo 2016-11-18 17:25:54
$

```

Figura 1.8: Uso de `yum-config-manager` para añadir repositorio

- Activamos el repositorio que acabamos de añadir.

```

root@localhost manolo 2016-11-18 17:30:59
$ yum-config-manager --enable kde.repo
Complementos cargados:fastestmirror, langpacks

```

Figura 1.9: Activación del repositorio con `yum-config-manager`

- Comprobamos que se ha creado correctamente. Para ello el nuevo repositorio tendrá un archivo en `/etc/yum.repos.d/`:

```

root@localhost manolo 2016-11-18 17:27:57
$ ls /etc/yum.repos.d/kde.repo
/etc/yum.repos.d/kde.repo
root@localhost manolo 2016-11-18 17:30:59
$

```

Figura 1.10: Comprobar que un nuevo repositorio se creó en `/etc/yum.repos.d/`

- Comprobar contenido del nuevo repositorio kde.repo:

```
$ cat /etc/yum.repos.d/kde.repo
# kde.repo, v2.1

[kde]
name=kde
mirrorlist=http://apt.kde-redhat.org/apt/kde-redhat/fedora/mirrors-stable
gpgkey=http://apt.kde-redhat.org/apt/kde-redhat/kde-redhat.RPM-GPG-KEY
#gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-kde-redhat
skip_if_unavailable=1
enabled=1

[kde-testing]
name=kde-testing
mirrorlist=http://apt.kde-redhat.org/apt/kde-redhat/fedora/mirrors-testing
gpgkey=http://apt.kde-redhat.org/apt/kde-redhat/kde-redhat.RPM-GPG-KEY
#gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-kde-redhat
skip_if_unavailable=1
enabled=1

[kde-unstable]
name=kde-unstable
mirrorlist=http://apt.kde-redhat.org/apt/kde-redhat/fedora/mirrors-unstable
gpgkey=http://apt.kde-redhat.org/apt/kde-redhat/kde-redhat.RPM-GPG-KEY
#gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-kde-redhat
skip_if_unavailable=1
enabled=0

root@localhost manolo 2016-11-18 17:33:59
```

Figura 1.11: Ver contenido de kde.repo

- Añadir los archivos de definición del repositorio en /etc/yum.repos.d/. Sería incluir el archivo kde.repo de forma manual, con la información que se ve en la figura anterior.
2. a) Liste los argumentos de apt necesarios para instalar, buscar y eliminar paquetes. b) ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy:stargate.ugr.es:3128) c) ¿Cómo añadimos un nuevo repositorio?
 - 2.1. a) Liste los argumentos de apt necesarios para instalar, buscar y eliminar paquetes.

Viendo el manual de Linux[3] podemos saber los argumentos de apt necesarios para:

- Para instalar: apt install <paquete>

```

[manolo@ubuntu ~] 2016-11-18 11:43:25
$ sudo apt install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
nmap ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 41 no actualizados.

```

Figura 2.1: Uso de apt install para gedit

- Para buscar: apt search <paquete>

```

[manolo@ubuntu ~] 2016-11-18 11:49:52
$ sudo apt search gedit_

```

Figura 2.2: Uso de apt search para gedit

```

gigedit/trusty 0.2.0-1 amd64
  Editor de instrumentos para archivos Gigasampler

leafpad/trusty 0.8.18.1-4 amd64
  Editor de texto simple basado en GTK+

libgtk2-sourceview2-perl/trusty 0.10-1build3 amd64
  enhanced source code editor widget

libwin-hivex-perl/trusty 1.3.9-2build1 amd64
  Vínculos Perl para hivex

nautilus-admin/unknown 0.1.2-1~ubuntu14.04.1 all
  Extension for Nautilus to do administrative operations

python-gtkspellcheck/trusty 3.0-1.1 all
  spellchecking library written in Python for Gtk based on Enchant

python-gtkspellcheck-doc/trusty 3.0-1.1 all
  Python GTK Spellcheck common documentation

python3-gtkspellcheck/trusty 3.0-1.1 all
  spellchecking library written in Python for Gtk based on Enchant

rabbitvcs-core/trusty 0.15.2-1 all
  Easy version control

rabbitvcs-gedit/trusty 0.15.2-1 all
  Extensión de Gedit para RabbitVCS

supercollider-gedit/trusty 1:3.6.3~repack-5 all
  SuperCollider mode for Gedit

[manolo@ubuntu ~] 2016-11-18 11:51:37
$ _

```

Figura 2.3: Paquetes mostrados por apt search para gedit

- Para eliminar: apt remove <paquete> o apt-get purge <paquete>

```

[manolo@ubuntu ~] 2016-11-18 12:18:48
$ sudo apt remove nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios
 libblas3 liblinear-tools liblinear1 liblua5.2-0
Use 'apt-get autoremove' to remove them.
Los siguientes paquetes se ELIMINARÁN:
  nmap
0 actualizados, 0 se instalarán, 1 para eliminar y 41 no actualizados.
Se liberarán 17,6 MB después de esta operación.
¿Desea continuar? [Y/n] y
(Leyendo la base de datos ... 76405 ficheros o directorios instalados actualmente.)
Desinstalando nmap (6.40-0.2ubuntu1) ...
Procesando disparadores para man-db (2.6.7.1-1ubuntu1) ...
[manolo@ubuntu ~] 2016-11-18 12:21:30
$

```

Figura 2.4: Uso de apt remove para borrar el paquete nmap

2.2. b) ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula? (Pistas: archivo de configuración en /etc, proxy:stargate.ugr.es:3128)

Siguiendo el manual de apt.conf[1] debemos de:

- Primero tenemos que crear un archivo llamado apt.conf en la ruta /etc/apt.

```

[manolo@ubuntu ~] 2016-11-10 16:23:19
$ sudo touch /etc/apt/apt.conf
[sudo] password for manolo:
[manolo@ubuntu ~] 2016-11-10 16:23:24
$ sudo ls /etc/apt/apt.conf
/etc/apt/apt.conf
[manolo@ubuntu ~] 2016-11-10 16:23:42
$ _

```

Figura 2.5: Creación de archivo apt.conf

- Añadimos dentro del archivo la línea Acquire::http::Proxy "http://stargate.ugr.es:3128"

```

[manolo@ubuntu ~] 2016-11-10 17:33:59
$ cat /etc/apt/apt.conf
Acquire::http::Proxy "http://stargate.ugr.es:3128";
[manolo@ubuntu ~] 2016-11-10 17:34:01
$

```

Figura 2.6: Ver contenido apt.conf

- Comprobamos que ahora no debería dejarnos instalar paquetes, ya que estoy en mi ordenador local. Hacemos apt update y comprobamos su funcionamiento.

```

Err http://es.archive.ubuntu.com trusty/universe Translation-en
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/main Translation-es_ES
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/main Translation-es
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/main Translation-en
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/multiverse Translation-es_ES
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/multiverse Translation-es
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/multiverse Translation-en
Fallo la conexión
Err http://es.archive.ubuntu.com trusty-updates/restricted Translation-es_ES
Fallo la conexión

```

Figura 2.7: Comprobación de no conexión con nuevo proxy

Podemos ver como no permite conectarse al proxy indicado al cambiarlo. En cambio antes si dejaba ir. Como conclusión el añadir un proxy sirve para cambiar el comportamiento a la hora de buscar los paquetes de apt.

2.3. c) ¿Cómo añadimos un nuevo repositorio?

Para añadir repositorios usamos la siguiente orden[2]:

- Usar `add-apt-repository <repositorio>`

```

Imanol@ubuntu ~ 2016-11-18 15:58:07
$ sudo add-apt-repository "deb http://us.archive.ubuntu.com/ubuntu/ saucy universe
Imanol@ubuntu ~ 2016-11-18 15:58:11
$

```

Figura 2.8: Uso de add-apt-repository

- Añadir en el archivo `/etc/apt/sources.list` el repositorio. La orden `add-apt-repository` hace justo esto, de modo que no tengas que buscar el archivo y añadirlo tú.

```
GNU nano 2.2.6 Archivo: /etc/apt/sources.list

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb http://es.archive.ubuntu.com/ubuntu/ trusty-backports main restricted universe
deb-src http://es.archive.ubuntu.com/ubuntu/ trusty-backports main restricted uni

deb http://security.ubuntu.com/ubuntu trusty-security main restricted
deb-src http://security.ubuntu.com/ubuntu trusty-security main restricted
deb http://security.ubuntu.com/ubuntu trusty-security universe
deb-src http://security.ubuntu.com/ubuntu trusty-security universe
deb http://security.ubuntu.com/ubuntu trusty-security multiverse
deb-src http://security.ubuntu.com/ubuntu trusty-security multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu trusty partner
# deb-src http://archive.canonical.com/ubuntu trusty partner

## Uncomment the following two lines to add software from Ubuntu's
## 'extras' repository.
## This software is not part of Ubuntu, but is offered by third-party
## developers who want to ship their latest software.
# deb http://extras.ubuntu.com/ubuntu trusty main
deb http://us.archive.ubuntu.com/ubuntu/ saucy universe multiverse
# deb-src http://us.archive.ubuntu.com/ubuntu/ saucy universe multiverse
# deb-src http://extras.ubuntu.com/ubuntu trusty main

^G Ver ayuda  ^O Guardar  ^R Leer fich.  ^Y Pág. ant.  ^K Cortar Texto
^X Salir      ^J Justificar  ^W Buscar    ^U Pág. sig.  ^U PegarTxt
```

Figura 2.9: Añadir nuevo repositorio modificando /etc/apt/sources.list

Abajo del archivo podemos ver el repositorio añadido "deb http://us.archive.ubuntu.com/ubuntu/saucy universe multiverse"

3. a) ¿Con qué comando puede abrir/cerrar un puerto usando ufw? Muestre un ejemplo de cómo lo ha hecho
- b) ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOS? Muestre un ejemplo de cómo lo ha hecho
- c) Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles

3.1. a) ¿Con qué comando puede abrir/cerrar un puerto usando ufw?

Revisando el manual de ufw[4] podemos ver sus diferentes órdenes, entre ellas se encuentran las necesarias para abrir y cerrar puertos.

- Abrir puertos con ufw allow <puerto>/protopocolo. Por ejemplo: ufw allow 80/tcp
- Cerrar puertos con ufw deny <puerto>/protopocolo. Por ejemplo: ufw deny 80/tcp

Primero vamos a habilitar ufw y abrir el puerto 200 con protocolo tcp. Terminamos comprobando que está habilitado con `ufw status`:

```
Imanol@ubuntu ~ 2016-11-17 17:23:46
$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
Imanol@ubuntu ~ 2016-11-17 17:23:52
$ sudo ufw allow 200/tcp
Regla actualizada
Regla actualizada (v6)
Imanol@ubuntu ~ 2016-11-17 17:23:55
$ sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
2000           DENY       Anywhere
200/tcp        ALLOW      Anywhere
200           DENY       Anywhere
200 (v6)       DENY       Anywhere (v6)
200/tcp (v6)   ALLOW      Anywhere (v6)
200 (v6)       DENY       Anywhere (v6)
Imanol@ubuntu ~ 2016-11-17 17:24:00
```

Figura 3.1: Habilitar puerto 200/tcp con ufw

Finalmente cerramos ese puerto y comprobamos que se ha cerrado bien:

```
Imanol@ubuntu ~ 2016-11-17 17:26:38
$ sudo ufw deny 200/tcp
Regla actualizada
Regla actualizada (v6)
Imanol@ubuntu ~ 2016-11-17 17:26:43
$ sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
2000           DENY       Anywhere
200/tcp        DENY       Anywhere
200           DENY       Anywhere
200 (v6)       DENY       Anywhere (v6)
200/tcp (v6)   DENY       Anywhere (v6)
200 (v6)       DENY       Anywhere (v6)
```

Figura 3.2: Deshabilitar puerto 200/tcp con ufw

3.2. b) ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOS? Muestre un ejemplo de cómo lo ha hecho

Consultando el manual de `firewall-cmd` averiguamos los comandos necesarios para abrir/cerrar puertos[30, 19]:

- Abrir puertos. Se pueden realizar de varios modos si queremos que los cambios permanezcan aunque se reinicie el sistema.
 - Abrir puerto para que siga estando hasta que se reinicie el sistema. Se usa el comando `firewall-cmd --add-port=443/tcp`.

```
manolo@localhost ~ 2016-11-19 14:17:43
$ firewall-cmd --add-port=443/tcp
success
```

Figura 3.3: Abrir puerto no permanente con firewall-cmd

Comprobamos que el puerto ha sido abierto correctamente, para ello usamos el comando **firewall-cmd --list-ports**.

```
manolo@localhost ~ 2016-11-19 14:37:37
$ firewall-cmd --list-ports
443/tcp
```

Figura 3.4: Comprobar puerto no permanente con firewall-cmd

- Abrir puerto para que siga siendo permanente independientemente de los reinicios del sistema. Se usa el comando **firewall-cmd --permanent --add-port=443/tcp**.

```
manolo@localhost ~ 2016-11-19 14:43:12
$ firewall-cmd --permanent --add-port=443/tcp
success
```

Figura 3.5: Abrir puerto permanente con firewall-cmd

Comprobamos que el puerto ha sido abierto correctamente, para ello usamos el comando **firewall-cmd --permanent --list-ports**.

```
manolo@localhost ~ 2016-11-19 14:52:28
$ firewall-cmd --permanent --list-ports
443/tcp
```

Figura 3.6: Comprobar puerto permanente con firewall-cmd

- Cerrar puertos. Se cerrarán y comprobarán con distintos comandos si son permanentes tras el reinicio o no.
 - Cerrar puertos no permanente con el comando **firewall-cmd --remove-port=443/tcp** y su comprobación con el comando **firewall-cmd --list-ports**.

```
$ firewall-cmd --remove-port=443/tcp
Warning: NOT_ENABLED
manolo@localhost ~ 2016-11-19 14:43:00
$ firewall-cmd --list-ports
manolo@localhost ~ 2016-11-19 14:43:12
$
```

Figura 3.7: Cerrado y comprobación puerto no permanente con firewall-cmd

Podemos ver como el puerto ya no se muestra. Ha sido cerrado correctamente.

- Cerrar puertos permanentes con el comando **firewall-cmd --permanent --remove-port=443/tcp** y su comprobación con el comando **firewall-cmd --permanent --list-ports**.

```
manolo@localhost ~ 2016-11-19 14:52:45
$ firewall-cmd --permanent --remove-port=443/tcp
success
manolo@localhost ~ 2016-11-19 14:53:44
$ firewall-cmd --permanent --list-ports
manolo@localhost ~ 2016-11-19 14:53:52
$
```

Figura 3.8: Cerrado y comprobación puerto permanente con firewall-cmd

3.3. c) Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles

Vamos a abrir/cerrar el puerto 22 de ssh en Ubuntu Server que tiene un servicio asociado (demonio sshd) con ufw y comprobamos como se ve ese puerto según las diferentes combinaciones en el interior y exterior (otra máquina, por ejemplo la anfitriona) usando para ello nmap[20]:

- Escenario 1: puerto 22 cerrado (deny) con ufw y servicio de ssh parado.
 - a) desde localhost: cerrado.

```

[manolo@ubuntu ~ 2016-11-19 15:56:24
$sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
200/tcp        ALLOW      Anywhere
22             DENY      Anywhere
200/tcp (v6)   ALLOW      Anywhere (v6)
22 (v6)        DENY      Anywhere (v6)

[manolo@ubuntu ~ 2016-11-19 15:56:27
$sudo service ssh stop
ssh stop/waiting
[manolo@ubuntu ~ 2016-11-19 15:56:36
$nmmap -p 22 localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-19 15:56 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000068s latency).
Other addresses for localhost (not scanned): 127.0.0.1
PORT      STATE      SERVICE
22/tcp    closed    ssh

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
[manolo@ubuntu ~ 2016-11-19 15:56:46
$

```

Figura 3.9: Escenario 1, localhost usando nmap

- b) desde fuera: filtrado.

```

manolo@manolo-K53SC:~$ nmap -p 22 -Pn 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-19 16:01 CET
Nmap scan report for 192.168.56.101
Host is up.
PORT      STATE      SERVICE
22/tcp    filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds

```

Figura 3.10: Escenario 1, desde fuera usando nmap

- Escenario 2: puerto 22 abierto. (allow) con ufw y servicio de ssh parado.
 - a) desde localhost: cerrado.

```

[manolo@ubuntu ~ 2016-11-19 16:05:42
$ sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
200/tcp        ALLOW      Anywhere
22            ALLOW      Anywhere
200/tcp (v6)   ALLOW      Anywhere (v6)
22 (v6)        ALLOW      Anywhere (v6)

[manolo@ubuntu ~ 2016-11-19 16:05:45
$ sudo service ssh stop
ssh stop/waiting
[manolo@ubuntu ~ 2016-11-19 16:05:49
$ nmap -p 22 localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-19 16:06 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000063s latency).
Other addresses for localhost (not scanned): 127.0.0.1
PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

```

Figura 3.11: Escenario 2, localhost usando nmap

- b) desde fuera: cerrado.

```

manolo@manolo-K53SC:~$ nmap -p 22 -Pn 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-19 16:06 CET
Nmap scan report for 192.168.56.101
Host is up (0.00074s latency).
PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

```

Figura 3.12: Escenario 2, desde fuera usando nmap

- Escenario 3: puerto cerrado (deny) con ufw y servicio de ssh escuchando.
 - a) desde localhost: open.

```

[manolo@ubuntu ~ 2016-11-19 16:11:09
$ sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
200/tcp        ALLOW      Anywhere
22             DENY      Anywhere
200/tcp (v6)   ALLOW      Anywhere (v6)
22 (v6)        DENY      Anywhere (v6)

[manolo@ubuntu ~ 2016-11-19 16:11:11
$ sudo service ssh start
ssh start/running, process 2892
[manolo@ubuntu ~ 2016-11-19 16:11:17
$ nmap -p 22 localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-19 16:11 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00072s latency).
Other addresses for localhost (not scanned): 127.0.0.1
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
[manolo@ubuntu ~ 2016-11-19 16:11:27

```

Figura 3.13: Escenario 3, localhost usando nmap

- b) desde fuera: filtrado.

```

manolo@manolo-K53SC:~$ nmap -p 22 -Pn 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-19 16:12 CET
Nmap scan report for 192.168.56.101
Host is up.
PORT      STATE SERVICE
22/tcp    filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds

```

Figura 3.14: Escenario 3, desde fuera usando nmap

- Escenario 4: puerto 22 abierto con ufw y servicio de ssh escuchando.
 - a) desde localhost: open.

```

[manolo@ubuntu ~ 2016-11-19 16:14:14
$sudo ufw status
Estado: activo

Hasta          Acción      Desde
-----
200/tcp        ALLOW      Anywhere
22             ALLOW      Anywhere
200/tcp (v6)   ALLOW      Anywhere (v6)
22 (v6)        ALLOW      Anywhere (v6)

[manolo@ubuntu ~ 2016-11-19 16:14:22
$sudo service ssh start
ssh start/running, process 2977
[manolo@ubuntu ~ 2016-11-19 16:14:28
$nmmap -p 22 localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-19 16:14 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0012s latency).
Other addresses for localhost (not scanned): 127.0.0.1
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

```

Figura 3.15: Escenario 4, localhost usando nmap

- b) desde fuera: open.

```

manolo@manolo-K53SC:~$ nmap -p 22 -Pn 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-19 16:14 CET
Nmap scan report for 192.168.56.101
Host is up (0.00062s latency).
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

```

Figura 3.16: Escenario 4, desde fuera usando nmap

Tras comprobar estos cuatro estados llegamos a las siguientes conclusiones:

- Si te quieres conectar desde fuera, la máquina a la que te conectas tiene que tener su puerto permitido por el firewall y además que un proceso esté escuchando en dicho puerto.
- Si te conectas desde dentro, podrás hacerlo siempre que tengas un proceso escuchando en el puerto deseado. No importa si el puerto en el firewall está abierto o cerrado ya que este solo controla las conexiones entrantes.

4. ¿Qué diferencia hay entre telnet y ssh?

Telnet[6, 31]: Protocolo para conexiones remotas por TCP. No es segura, ya que la información no es cifrada (la envía en texto plano) y terceros pueden obtenerla del tráfico que se transmite. Usa el puerto 23. Para conocer más a fondo este protocolo, podemos ver su RFC[26, 28].

SSH[5, 17]: Protocolo de red que permite transmitir información sobre un canal seguro. Los datos que pasan por el canal va cifrados por lo que se mantiene su seguridad. Proporciona aplicaciones gráficas sobre una red (X11). Comúnmente es usado en lugar de Telnet. Usa el puerto 22. Para conocer más a fondo este protocolo, podemos ver su RFC[27].

Como conclusión, las diferencias son:

- ssh es más seguro que Telnet, ya que Telnet envía información en texto plano y ssh cifrada.
- ssh es más usado que Telnet, debido a su seguridad.
- ssh proporciona interacción de forma gráfica en la red (X11), Telnet no.
- ssh añade más sobrecarga de banda ancha que Telnet, debido a que su información es cifrada y necesita mayor tamaño.
- Telnet usa el puerto 23 y ssh el 22.

5. a) ¿Para qué sirve la opción -X? b) 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?

5.1. a) ¿Para qué sirve la opción -X?

La opción -X sirve para [64, 8, 7] habilitar X11. X11 es un servicio de ventanas que permite interacción de forma gráfica en red. Esto quiere decir que si usamos ssh podemos ejecutar programas que están en una máquina remota sin tener que instalar el programa en local y X11 es quien se encarga de enseñarnos dicha ejecución, ya que proporciona una ventana donde podremos ver dicha ejecución.

5.2. b) 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?

Antes de empezar a ejecutar remotamente, tenemos aseguraremos que Ubuntu Server y nuestra máquina anfitriona Ubuntu Desktop se puedan comunicar correctamente por

ssh. Para ello en VirtualBox configuramos la red de la máquina virtualizada de Ubuntu Server del siguiente modo:

- Se establece un adaptador en modo NAT.

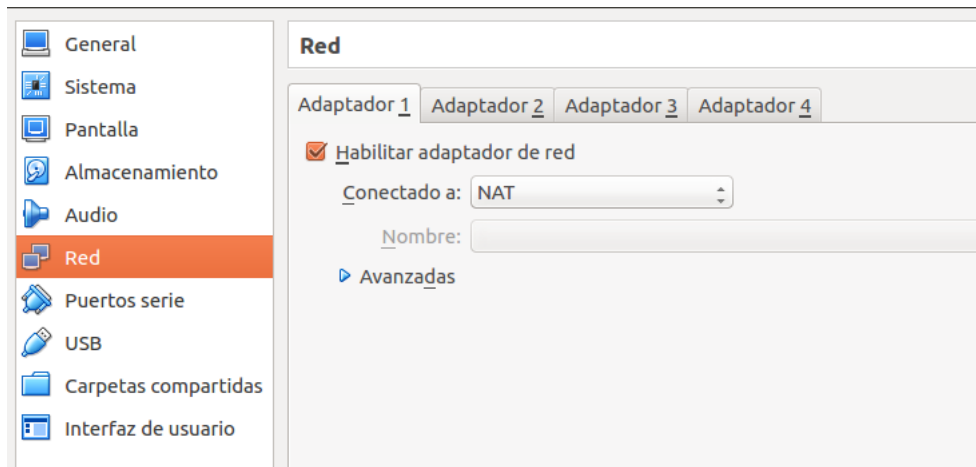


Figura 5.1: Configuración de red para máquina virtual, adaptador 1

- Se crea un segundo adaptador como adaptador-solo-anfitrión.

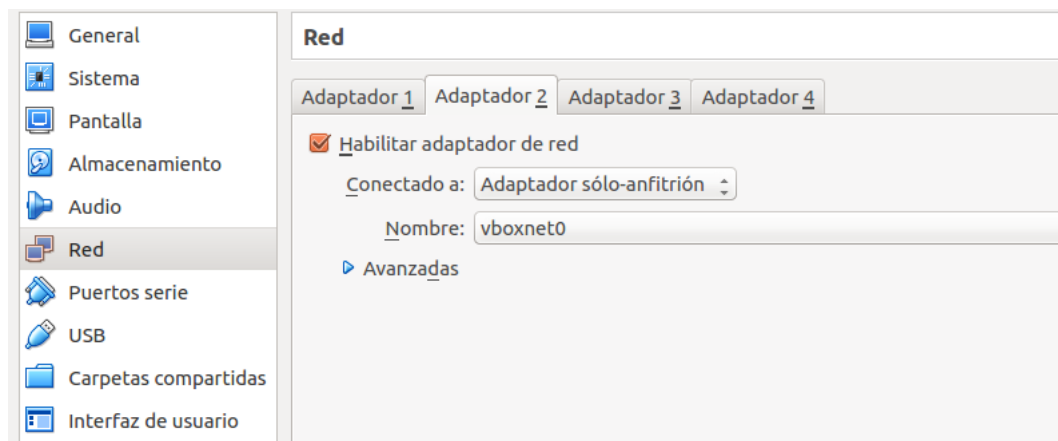


Figura 5.2: Configuración de red para máquina virtual, adaptador 2

Después preparamos el ssh, instalando el openssh-server, para obtener archivos del demonio ssh[13]:

- `sudo apt-get install openssh-server`

Leyendo más documentación sobre ssh, encontramos como ejecutar remotamente desde otra máquina virtual[12, 9]. Iremos paso por paso:

- Nos vamos al archivo de configuración de ssh `/etc/ssh/ssh_config` para habilitar X11. Para ello se establece "ForwardX11 yes".

```
GNU nano 2.2.6 Archivo: /etc/ssh/ssh_config

# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Host *
# ForwardAgent no
# ForwardX11 yes_
# ForwardX11Trusted yes
# RhostsRSAAuthentication no
# RSAAuthentication yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes

^G Ver ayuda  ^O Guardar   ^R Leer fich. ^Y Pág. ant.  ^K Cortar Texto
^X Salir      ^J Justificar ^U Buscar     ^U Pág. sig.  ^U PegarTxt
```

Figura 5.3: Habilitar X11 de ssh en fichero `ssh_config` para permitir gráficos remotos

- Habilitamos X11 también en el archivo `/etc/ssh/sshd_config` estableciendo "X11Forwarding yes":

```
GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no

^G Ver ayuda  ^O Guardar    ^R Leer fich. ^V Pág. ant.  ^K Cortar Texto
^X Salir      ^J Justificar ^W Buscar    ^U Pág. sig.  ^U PegarTxt
```

Figura 5.4: Habilitar X11 de ssh en fichero sshd_config para permitir gráficos remotos

- Reiniciamos el servicio ssh para que los cambios realizados se tengan en cuenta:
 - sudo service ssh restart

```
manolo@ubuntu ~ 2016-11-17 21:15:09
$ sudo service ssh restart
ssh stop/waiting
ssh start/running, process 8960
manolo@ubuntu ~ 2016-11-17 21:18:15
```

Figura 5.5: Habilitar X11 de ssh en fichero sshd_config para permitir gráficos remotos

- Usamos comando `ifconfig[25]` para comprobar las redes que tenemos.

```

[manolo@ubuntu ~] 2016-11-19 19:33:01
$ifconfig
eth0      Link encap:Ethernet direcciónHW 08:00:27:07:54:1a
          Direc. inet:10.0.2.15 Difus.:10.0.2.255 Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe07:541a/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:41 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:48 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:5034 (5.0 KB) TX bytes:4598 (4.5 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1 Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Amfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1
          Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)

```

Figura 5.6: Redes de la máquina Ubuntu Server

- Vemos que no tenemos la interfaz eth1, debemos activarla.

```

[manolo@ubuntu ~] 2016-11-19 19:37:51
$sudo ifconfig eth1 up
[manolo@ubuntu ~] 2016-11-19 19:37:55
$ifconfig
eth0      Link encap:Ethernet direcciónHW 08:00:27:07:54:1a
          Direc. inet:10.0.2.15 Difus.:10.0.2.255 Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe07:541a/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:41 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:48 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:5034 (5.0 KB) TX bytes:4598 (4.5 KB)

eth1      Link encap:Ethernet direcciónHW 08:00:27:29:0e:7d
          Dirección inet6: fe80::a00:27ff:fe29:e7d/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:6 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B) TX bytes:508 (508.0 B)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1 Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Amfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1
          Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)

```

Figura 5.7: Activar interfaz eth1

- eth1 aún no tiene una dirección asociada. Configuramos la interfaz eth1 con el uso de dhclient[24].

```

[manolo@ubuntu ~ 2016-11-19 19:44:56
$ sudo dhclient
[manolo@ubuntu ~ 2016-11-19 19:45:06
$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:07:54:1a
          Direc. inet:10.0.2.15  Difus.:10.0.2.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe07:541a/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:43 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:50 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:6214 (6.2 KB)  TX bytes:5282 (5.2 KB)

eth1      Link encap:Ethernet  direcciónHW 08:00:27:29:0e:7d
          Direc. inet:192.168.56.102  Difus.:192.168.56.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe29:e7d/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:17 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:10 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:5340 (5.3 KB)  TX bytes:1332 (1.3 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1
          Bytes RX:0 (0.0 B)  TX bytes:0 (0.0 B)

```

Figura 5.8: Configurar interfaz eth1 con dhclient

- Configuramos la interfaz[29] para que se quede de forma permanente cada vez que se reinicie en el sistema. Para ello vamos al archivo `/etc/network/interfaces` y añadimos la configuración de eth1 (será la misma que la de eth0).

```

[manolo@ubuntu ~ 2016-11-19 19:46:41
$ sudo less /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

```

Figura 5.9: Ver contenido de `/etc/network/interfaces`

```

GNU nano 2.2.6          Archivo: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

# Configuración de interfaz host-only con eth1
auto eth1
iface eth1 inet dhcp

```

Figura 5.10: Añadir configuración para interfaz eth1 en /etc/network/interfaces

- Realizamos una copia del archivo "interfaces" modificado y lo llamaremos "interfaces.vap". De este modo podemos recurrir a él en caso de pérdida del original.

```

[manolo@ubuntu ~ 2016-11-19 19:58:24]
$ sudo cp /etc/network/interfaces /etc/network/interfaces.vap
[manolo@ubuntu ~ 2016-11-19 19:58:32]
$ ls /etc/network/
if-down.d if-post-down.d if-pre-up.d if-up.d interfaces interfaces.d interfaces.vap run
[manolo@ubuntu ~ 2016-11-19 19:58:44]
$

```

Figura 5.11: Copia del archivo interfaces

- Reiniciamos la máquina "sudo rebootz" comprobamos que las interfaces siguen estando usando ifconfig.

```

[manolo@ubuntu ~] 2016-11-19 20:04:38
$ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:07:54:1a
          Direc. inet:10.0.2.15  Difus.:10.0.2.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe07:541a/64 Alcance:Enlace
          ACTIVO DIFUSION FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:60 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:65 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:6974 (6.9 KB)  TX bytes:6066 (6.0 KB)

eth1      Link encap:Ethernet  direcciónHW 08:00:27:29:0e:7d
          Direc. inet:192.168.56.102 Difus.:192.168.56.255 Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe29:e7d/64 Alcance:Enlace
          ACTIVO DIFUSION FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:5 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:10 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:1945 (1.9 KB)  TX bytes:1332 (1.3 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1
          Bytes RX:0 (0.0 B)  TX bytes:0 (0.0 B)

```

Figura 5.12: Comprobación de interfaces tras los cambios

- Comprobamos que el puerto ssh 22 está abierto por el firewall (ufw allow) y que el servicio ssh está escuchando.

```

[manolo@ubuntu ~] 2016-11-19 20:09:59
$sudo ufw allow 22
Regla actualizada
Regla actualizada (v6)
[manolo@ubuntu ~] 2016-11-19 20:10:14
$sudo ufw status
Estado: activo

Hasta      Acción      Desde
-----
2000       DENY        Anywhere
200        DENY        Anywhere
22         ALLOW       Anywhere
2000 (v6)  DENY        Anywhere (v6)
200 (v6)   DENY        Anywhere (v6)
22 (v6)    ALLOW       Anywhere (v6)

[manolo@ubuntu ~] 2016-11-19 20:10:17
$sudo service ssh status
ssh start/running, process 1867

```

Figura 5.13: Comprobación de firewall y servicio ssh

- Finalmente, ya podemos conectarnos remotamente desde otra máquina. Vamos a comprobar que:
 - Sin la opción -X de ssh no deja ejecutar gedit.

```

manolo@manolo-K53SC:~$ ssh -p 22 192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:IrM07y2HuFb2kbFXZVyCLVz5AzhUyUSGp2KDHLgD5c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
manolo@192.168.56.102's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

System information disabled due to load higher than 1.0

45 packages can be updated.
0 updates are security updates.

New release '16.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

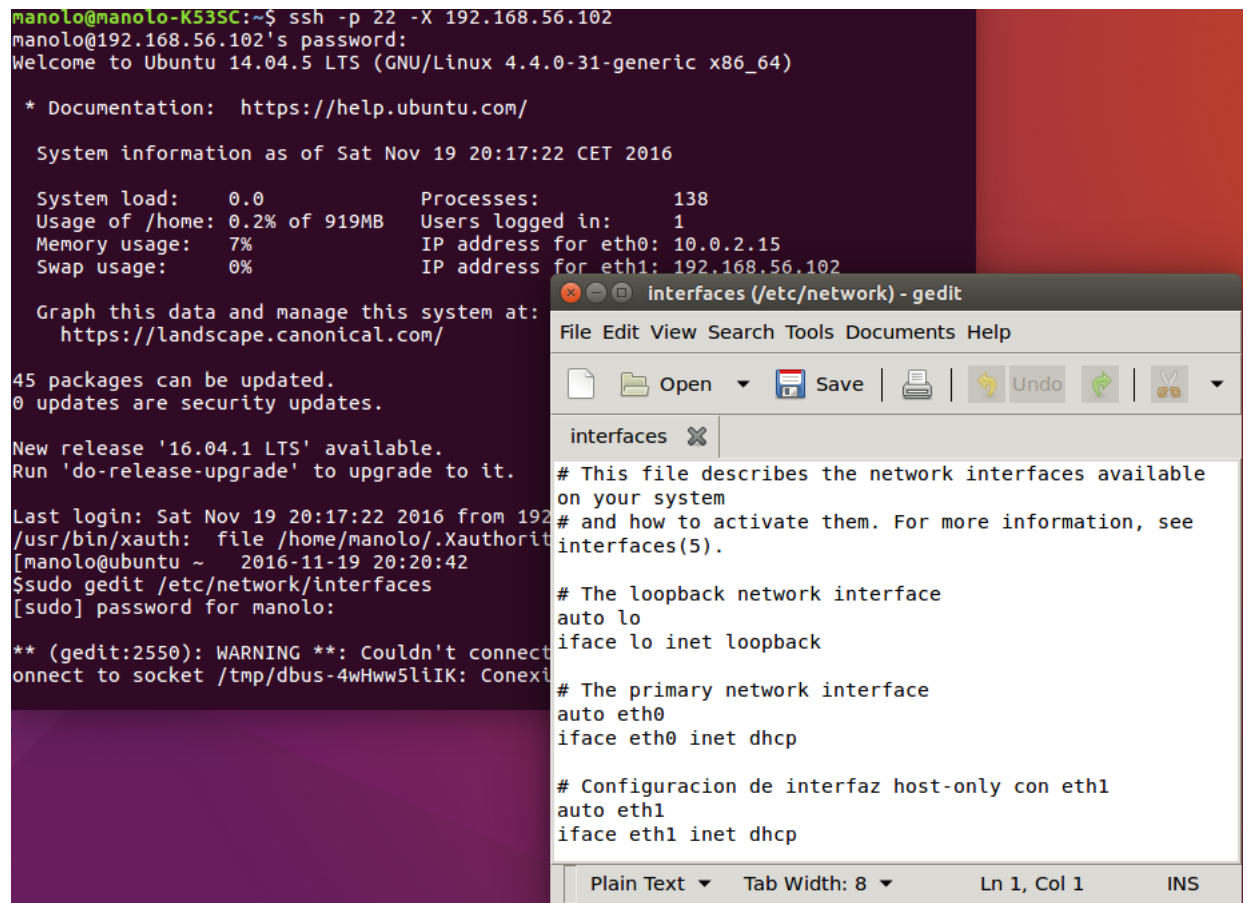
Last login: Sat Nov 19 20:04:37 2016
[manolo@ubuntu ~ 2016-11-19 20:17:22]
$ sudo gedit /etc/network/interfaces
[sudo] password for manolo:
Lo sentimos, vuelva a intentarlo.
[sudo] password for manolo:
error: XDG_RUNTIME_DIR not set in the environment.

(gedit:2471): Gtk-WARNING **: cannot open display:
[manolo@ubuntu ~ 2016-11-19 20:18:07]
$

```

Figura 5.14: Uso remoto de ssh sin opción -X

- Con la opción -X de ssh permite ejecutar gedit.



The screenshot shows a terminal window with an SSH session. The user 'manolo' is connected to a remote host 'manolo-K53SC' via port 22. The terminal displays system information for Ubuntu 14.04.5 LTS, including system load, memory usage, and network interfaces. A gedit window titled 'interfaces (/etc/network) - gedit' is open, showing the contents of the /etc/network/interfaces file. The file contains configuration for the loopback interface 'lo', the primary network interface 'eth0', and a host-only interface 'eth1'.

```
manolo@manolo-K53SC:~$ ssh -p 22 -X 192.168.56.102
manolo@192.168.56.102's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

System information as of Sat Nov 19 20:17:22 CET 2016

System load:      0.0          Processes:        138
Usage of /home:   0.2% of 919MB Users logged in:   1
Memory usage:    7%           IP address for eth0: 10.0.2.15
Swap usage:      0%           IP address for eth1: 192.168.56.102

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

45 packages can be updated.
0 updates are security updates.

New release '16.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 19 20:17:22 2016 from 192.168.56.102
/usr/bin/xauth: file /home/manolo/.Xauthority does not exist
[manolo@ubuntu ~ 2016-11-19 20:20:42]
$ sudo gedit /etc/network/interfaces
[sudo] password for manolo:

** (gedit:2550): WARNING **: Couldn't connect to socket /tmp/dbus-4wHww5liIK: Connection refused

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

# Configuración de interfaz host-only con eth1
auto eth1
iface eth1 inet dhcp
```

Figura 5.15: Uso remoto de ssh con opción -X

6. Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña. Pruebe que funciona. (Pistas: ssh-keygen, ssh-copy-id)

Con las pistas que nos dan, sabemos que ssh-keygen[22] se usa para generación, gestión y conversión de claves de autenticación (clave pública y privada). Por otra parte ssh-copy-id[21] se usa para instalar una clave pública en una máquina remota autorizada.

Indagando un poco más, encontramos en RedHat documentación de sobre "gestión remota con SSH" que hace uso de las órdenes descritas antes. Las desventajas de introducir la contraseña cada vez que nos conectamos remotamente con ssh son las siguientes:

- El proceso inicial de configuración de la conexión podría ser lento.

- ssh no escala bien con un mayor número de máquinas remotas.
- No hay una forma estándar de anular la clave de usuario en todos los hosts o invitados.

Por las desventajas comentadas, no tener que introducir la contraseña en cada conexión ssh remota es bueno. RedHat explica un proceso para acceder de forma remota con ssh sin tener introducir la contraseña (como se ha visto en las imágenes del ejercicio 5). Para ello realiza los siguientes pasos:

- Generación del par de claves ssh. Uso de ssh-keygen. Usaremos encriptación rsa y un tamaño de bits para ella de 2048.

```

[manuelo@ubuntu ~] 2016-11-19 19:02:25
$ sudo ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
28:df:94:be:2c:bd:01:7c:07:33:9c:d3:8e:1b:1e:51 root@ubuntu
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           E           |
|      . +             |
|      0 .             |
|     . . X            |
|    . + S o           |
|    o B =             |
|     . *              |
|     . . O            |
|     . + .            |
+-----+
[manuelo@ubuntu ~] 2016-11-19 19:03:06
$

```

Figura 6.1: Generación de claves con ssh-keygen

- Vamos a ver los permisos de las claves.

```

[manuelo@ubuntu ~] 2016-11-19 19:36:53
$ sudo ls -l /root/.ssh/
total 12
-rw----- 1 root root 1675 nov 19 19:03 id_rsa
-rw-r--r-- 1 root root 393 nov 19 19:03 id_rsa.pub
-rw-r--r-- 1 root root 222 nov 19 19:09 known_hosts
[manuelo@ubuntu ~] 2016-11-19 19:37:10
$

```

Figura 6.2: Ver permisos de las claves generadas

- Copiamos las claves a una máquina remota. Para ello usa ssh-copy-id.

```

[manolo@ubuntu ~] 2016-11-19 19:24:29
$ sudo ssh-copy-id -i /root/.ssh/id_rsa.pub -p 22 manolo@192.168.56.102
/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 prompted now it is to install all the new keys
manolo@192.168.56.102's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p '22' 'manolo@192.168.56.102'"
and check to make sure that only the key(s) you wanted were added.

```

Figura 6.3: Copiar clave pública a una máquina remota

- Ahora ya podemos conectarnos por ssh sin que nos pida la contraseña.

```

[manolo@ubuntu ~] 2016-11-19 19:33:21
$ sudo ssh -p 22 manolo@192.168.56.102
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

System information as of Sat Nov 19 21:26:52 CET 2016

System load:  0.0          Processes:      139
Usage of /home: 0.2% of 919MB  Users logged in: 1
Memory usage:  7%          IP address for eth0: 10.0.2.15
Swap usage:    0%          IP address for eth1: 192.168.56.102

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

45 packages can be updated.
0 updates are security updates.

New release '16.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 19 21:10:28 2016 from 192.168.56.101

```

Figura 6.4: Conexión remota por ssh sin introducir contraseña

NOTA: La secuencia de comandos realizada en este ejercicio está realizada realmente para el usuario root, ya que en cada comando realizamos "sudo". Esto quiere decir que la sesión ssh que se inicia para rootz no para el usuario "manolo".

7. ¿Qué archivo es el que contiene la configuración del servicio ssh? ¿Qué parámetro hay que modificar para evitar que el usuario root acceda? Cambie el puerto por defecto y compruebe que puede acceder.

El archivo que contiene la configuración del servicio ssh es `/etc/ssh/sshd_config`[23].

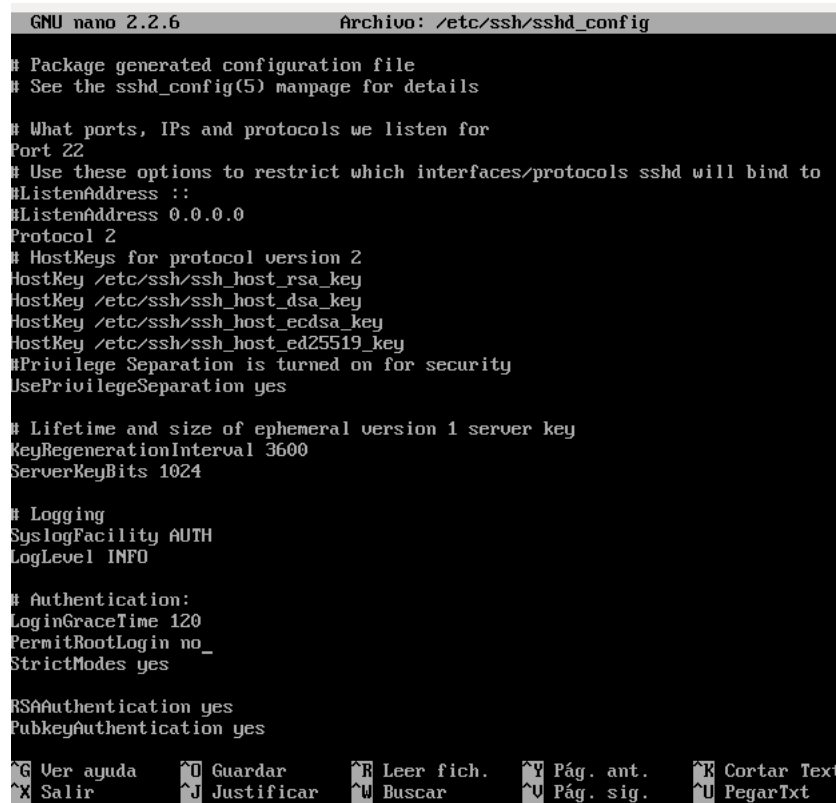
El parámetro para evitar que el usuario root acceda[18] es:

- PermitRootLogin no

Antes que nada, he usado el comando `sudo passwd root` para establecer una contraseña al usuario root (antes no tenía ninguna).

Ahora, vamos a comprobar que no deja acceder como root al poner el parámetro `PermitRootLogin` a no:

- Modificando archivo `sshd_config`:



```
GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no_
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

^G Ver ayuda  ^O Guardar    ^R Leer fich. ^Y Pág. ant.  ^K Cortar Text
^X Salir      ^J Justificar ^W Buscar    ^U Pág. sig.  ^U PegarText
```

Figura 7.1: Modificando parámetro `PermitRootLogin` a no en ssh

- Reiniciamos el servicio ssh:
 - `sudo service ssh restart`
- Intentamos acceder como root remotamente y vemos como no nos deja iniciar sesión con root.

```

manolo@manolo-K53SC:~$ ssh -p 22 root@192.168.56.101
root@192.168.56.101's password:
Permission denied, please try again.
root@192.168.56.101's password:
Permission denied, please try again.
root@192.168.56.101's password:
manolo@manolo-K53SC:~$ date
vie nov 25 17:29:43 CET 2016
manolo@manolo-K53SC:~$

```

Figura 7.2: Conexion remota por ssh accediendo como root con PermitRootLogin no

Para comprobar que realmente termina de funcionar, ponemos PermitRootLogin yes para que ahora sí nos deje acceder como root.

- Modificamos PermitRootLogin yes.

```

GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

^G Ver ayuda  ^O Guardar    ^R Leer fich. ^Y Pág. ant.  ^K Cortar Text
^X Salir      ^J Justificar ^W Buscar    ^U Pág. sig.  ^U PegarText

```

Figura 7.3: Modificando parámetro PermitRootLogin a yes en ssh

- Reiniciamos el servicio ssh:
 - sudo service ssh restart
- Comprobamos que deja acceder remotamente como root.

```
manolo@manolo-K53SC:~$ ssh -p 22 root@192.168.56.101
root@192.168.56.101's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

System information as of Fri Nov 25 13:13:38 CET 2016

System load:   0.16           Processes:      145
Usage of /home: 0.4% of 919MB Users logged in:    0
Memory usage:  12%           IP address for eth0: 10.0.2.15
Swap usage:    0%            IP address for eth1: 192.168.56.101

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

New release '16.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Nov 25 13:13:39 2016 from 192.168.56.1
root@ubuntu:~#
```

Figura 7.4: Conexion remota por ssh accediendo como root con PermitRootLogin yes

El parámetro que hay que cambiar para modificar el puerto[55] por defecto del servicio ssh es:

- Port <numero>

Vamos a cambiar el puerto por defecto para ssh y vamos a comprobar que podemos acceder por ssh.

- Cambiamos el archivo sshd_config y cambiamos por ejemplo el puerto a 1000.

```
GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 1000_
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

[ 88 líneas leídas ]
^G Ver ayuda  ^O Guardar    ^R Leer fich. ^V Pág. ant.  ^X Cortar Texto
^X Salir      ^J Justificar ^W Buscar    ^U Pág. sig.  ^U PegarTxt
```

Figura 7.5: Cambiando puerto por defecto de ssh

- Reiniciamos el servicio ssh para que los cambios sean efectivos:
 - `sudo service ssh restart`
- Comprobamos que no podemos acceder ya remotamente por ssh desde el puerto 22.

```
manolo@manolo-K53SC:~$ ssh -p 22 192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection refused
manolo@manolo-K53SC:~$
```

Figura 7.6: Intentando acceder por el puerto 22 a ssh

- Comprobamos que podemos acceder remotamente por ssh desde el puerto 1000.

```
manolo@manolo-K53SC:~$ ssh -p 22 192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection refused
manolo@manolo-K53SC:~$
```

Figura 7.7: Accediendo a ssh por el puerto 1000

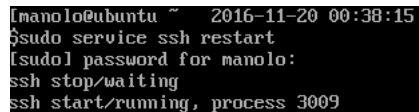
NOTA: en caso de tener el firewall activo, debemos permitir acceso al nuevo puerto asignado para ssh.

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

Sí, es necesario reiniciar el servicio tras realizar cambios en los archivos de configuración asociados a dicho servicio con el fin de que tengan efecto. De este modo leerá los nuevos parámetros. Es necesario reiniciarlo porque el servicio no está leyendo constantemente su configuración.

Los servicios en Ubuntu está en el directorio `/etc/init.d` .Para reiniciar un servicio en Ubuntu usamos la orden[42]:

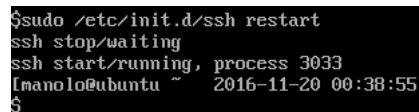
- `service <nombre-servicio>restart`



```
[manolo@ubuntu ~] 2016-11-20 00:38:15
$ sudo service ssh restart
[sudo] password for manolo:
ssh stop/waiting
ssh start/running, process 3009
```

Figura 8.1: Ubuntu. Reiniciando servicio con orden service

- `/etc/init.d/<nombre-servicio>restart`

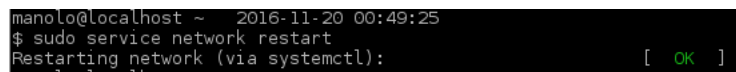


```
$ sudo /etc/init.d/ssh restart
ssh stop/waiting
ssh start/running, process 3033
[manolo@ubuntu ~] 2016-11-20 00:38:55
$
```

Figura 8.2: Reiniciando servicio buscando servicio en `/etc/init.d`

En CentOS[37] se realiza de la misma forma que en Ubuntu:

- `service <nombre-servicio>restart`



```
manolo@localhost ~ 2016-11-20 00:49:25
$ sudo service network restart
Restarting network (via systemctl): [ OK ]
```

Figura 8.3: CentOS. Reiniciando servicio con orden service

9. ¿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). Compruebe que la instalación ha sido correcta.

Para Ubuntu hay varias formas de instalar LAMP[46, 47]:

- De forma manual, es decir, instalando Apache, MySQL (o MariaDB) y PHP (o Python o Perl) de forma separada.
 - `sudo apt install apache2`
 - `sudo apt install mysql-server mysql-client`
 - `sudo apt install php5 php5-mysql libapache2-mod-php5`
- Mediante una interfaz gráfica (Tasksel[38]):
 - `sudo apt install tasksel`. Nos dirá que ya está instalado.
 - `sudo tasksel`. Ejecutamos la interfaz para instalar LAMP.

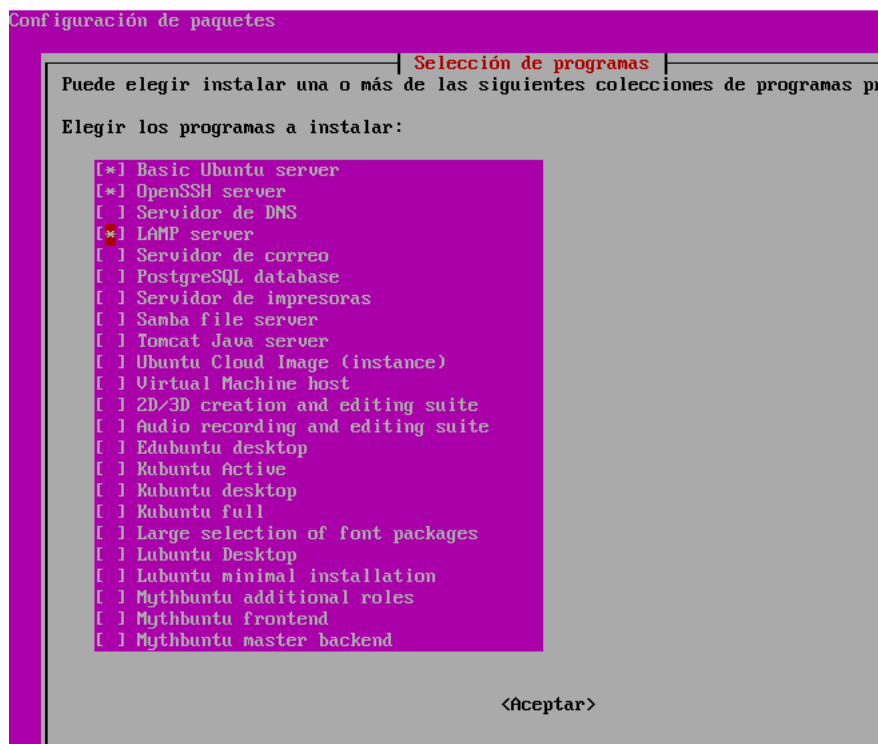


Figura 9.1: Usando tasksel para instalar LAMP

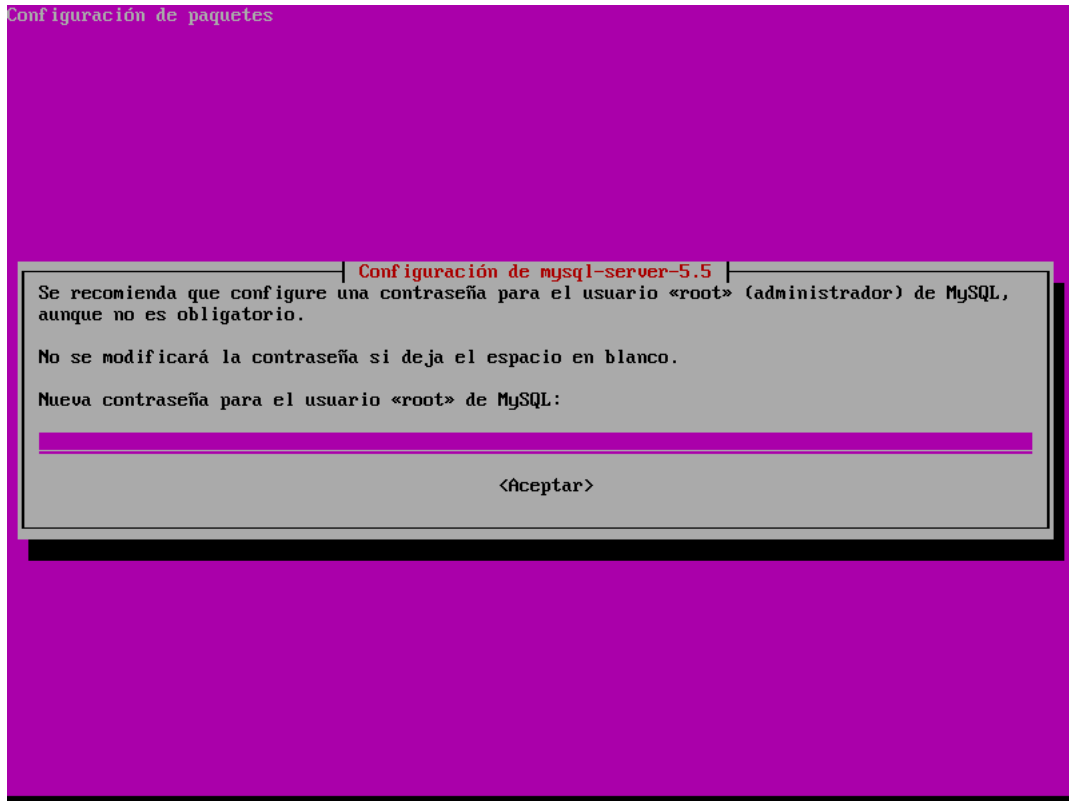


Figura 9.2: Establecer contraseña para mysql-server

- Abrimos para el cortafuegos el puerto 80 (http).
 - `sudo ufw allow 80`
- Restablecemos el servicio apache2.
 - `sudo service apache2 restart`

De cualquiera de los dos modos de instalación, podremos acceder al servidor conectándonos a la dirección de su interfaz de red.

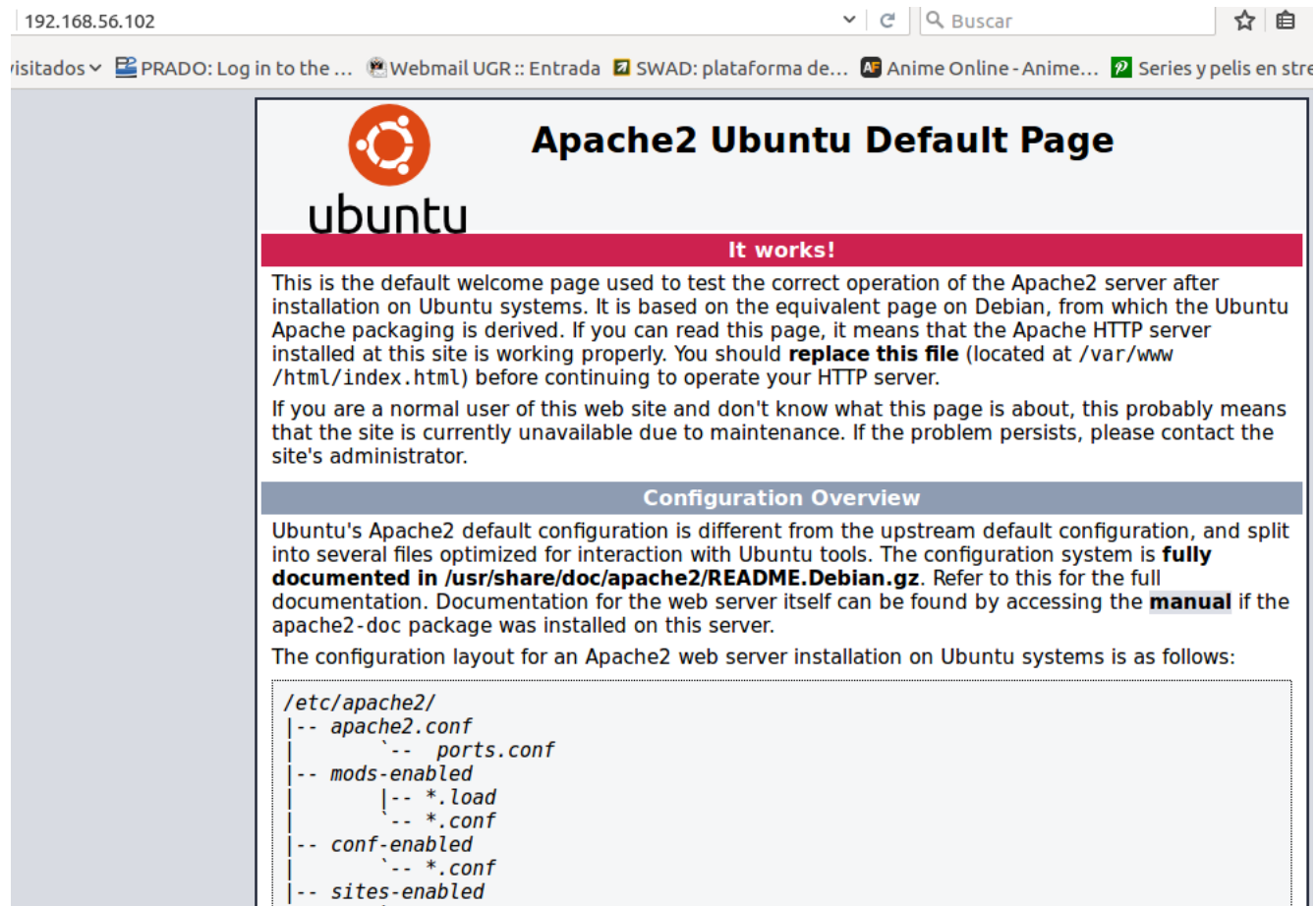


Figura 9.3: Servidor Apache2 funcionando en Ubuntu Server

La documentación de Apache2 nos dice donde están los archivos de configuración. Así mismo, la página por defecto de Apache2 nos da también información sobre sus archivos de configuración.

- Archivo html de Apache: /var/www/html/index.html
- Archivos de configuración: /etc/apache2/

Por ejemplo, aquí vemos el html de la página por defecto de apache2.

```
GNU nano 2.2.6          Archivo: /var/www/html/index.html

<div class="section_header section_header_red">
  <div id="about"></div>
  It works!
</div>
<div class="content_section_text">
  <p>
    This is the default welcome page used to test the correct
    operation of the Apache2 server after installation on Ubuntu systems.
    It is based on the equivalent page on Debian, from which the Ubuntu Apache
    packaging is derived.
    If you can read this page, it means that the Apache HTTP server installed at
    this site is working properly. You should replace this file (located at
    <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
  </p>

  <p>
    If you are a normal user of this web site and don't know what this page is
    about, this probably means that the site is currently unavailable due to
    maintenance.
    If the problem persists, please contact the site's administrator.
  </p>
</div>
<div class="section_header">
  <div id="changes"></div>
  Configuration Overview
</div>
<div class="content_section_text">
  <p>
    Ubuntu's Apache2 default configuration is different from the
    upstream default configuration, and split into several files optimized for
```

Figura 9.4: Archivo de html por defecto de Apache2

La configuración de MySQL[39] se encuentra en el directorio `/etc/mysql`. En especial dentro del archivo `my.cnf`.

```

GNU nano 2.2.6                               Archivo: /etc/mysql/my.cnf
#
# The MySQL database server configuration file.
#
# You can copy this to one of:
# - "/etc/mysql/my.cnf" to set global options,
# - "~/.my.cnf" to set user-specific options.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html
#
# This will be passed to all mysql clients
# It has been reported that passwords should be enclosed with ticks/quotes
# especially if they contain "#" chars...
# Remember to edit /etc/mysql/debian.cnf when changing the socket location.
[client]
port                = 3306
socket              = /var/run/mysql/mysql.sock

# Here is entries for some specific programs
# The following values assume you have at least 32M ram

# This was formally known as [safe_mysqld]. Both versions are currently parsed.
[mysqld_safe]
socket              = /var/run/mysql/mysql.sock
nice                = 0

[mysqld]

```

Figura 9.5: Archivo de configuración MySQL

Comprobamos que MySQL funciona:

```

Imanol@ubuntu ~ 2016-11-20 14:11:04
$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 52
Server version: 5.5.53-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```

Figura 9.6: Comprobando funcionamiento MySQL

En php[34, 41] los archivos de configuración se llaman php.ini. Se encuentran en el directorio /etc/php5/. Por ejemplo la configuración de php para Apache2 se encuentra en /etc/php5/apache2/php.ini.

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

[PHP]

::::::::::::::::::
; About php.ini  ;
::::::::::::::::::
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable. (As of PHP 5.2.0)
; 3. A number of predefined registry keys on Windows (As of PHP 5.2.0)
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (C:\windows or C:\winnt)
; See the PHP docs for more specific information.
; http://php.net/configuration.file

; The syntax of the file is extremely simple.  Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.

; Directives following the section heading [PATH=/www/mysite] only
; apply to PHP files in the /www/mysite directory.  Directives
; following the section heading [HOST=www.example.com] only apply to
; PHP files served from www.example.com.  Directives set in these
; special sections cannot be overridden by user-defined INI files or
; at runtime.  Currently, [PATH=] and [HOST=] sections only work under
```

Figura 9.7: Archivo de configuración php

Vamos a comprobar que php funciona correctamente. Para ello realizamos un ejemplo[33]:

```
[manolo@ubuntu ~] 2016-11-20 14:36:06
$php -a
Interactive mode enabled

php > echo 5+3;
@php > echo "Hola mundo";
Hola mundophp > _
```

Figura 9.8: Probando php

Para CentOS, instalar LAMP se deberá hacer uno por uno:

- Instalamos servidor Apache[35]:
 - `sudo yum install httpd`
 - `sudo service httpd restart`
 - Comprobamos que funciona correctamente:

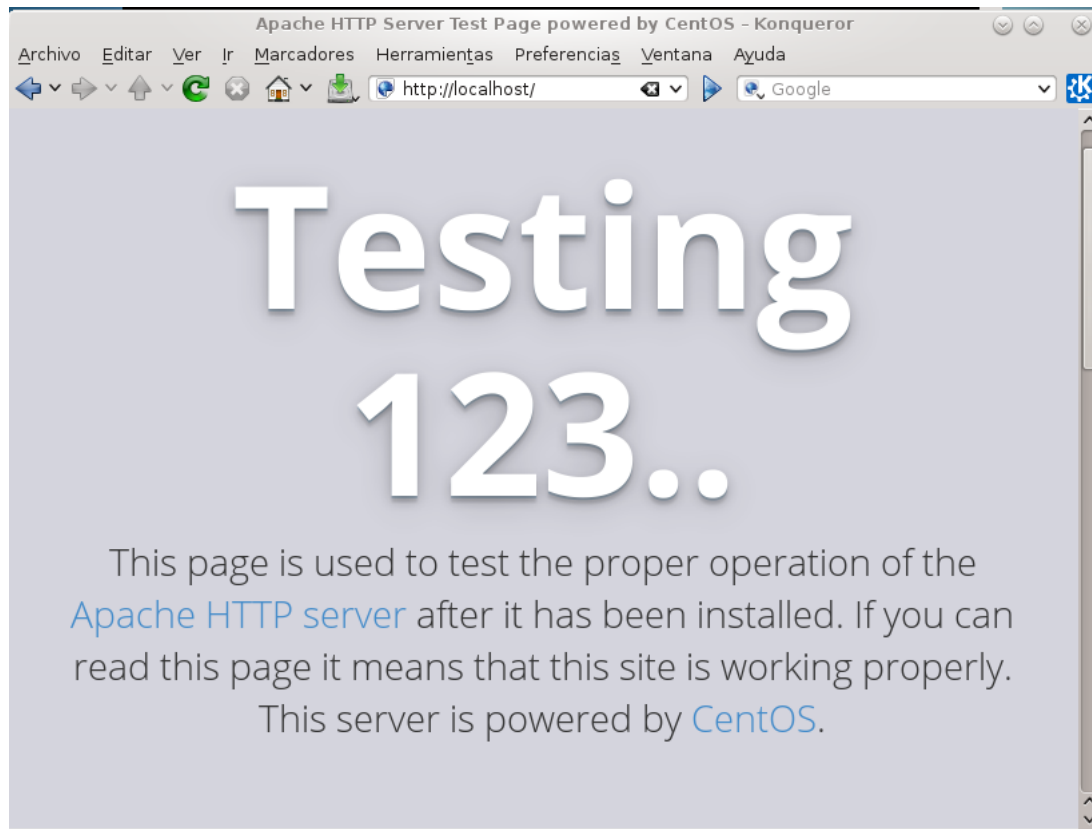


Figura 9.9: Servidor Apache en CentOS

- Instalamos MariaDB (es el MySQL de CentOS)[36, 44]:
 - `sudo yum install mariadb-server`
 - Iniciamos el servicio de MariaDB con:
 - `sudo systemctl start mariadb` o,
 - `sudo /etc/init.d/mysql start`
 - Comprobamos que funciona MariaDB[43]:

```
manolo@localhost ~ 2016-11-20 16:30:11
$ mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
Server version: 5.5.50-MariaDB MariaDB Server

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> █
```

Figura 9.10: MariaDB funcionando en CentOS

- Instalamos php en CentOS.
 - `sudo yum install php php-mysql`
 - `sudo service httpd restart`, para que se efectúen los cambios.
 - `sudo systemctl restart mariadb`, para que se efectúen los cambios.
 - Comprobamos que php funciona:



```
manolo@localhost ~ 2016-11-20 16:54:51
$ php -a
Interactive shell

php > echo "hola mundo";
hola mundophp > █
```

Figura 9.11: php funcionando en CentOS

10. Realice la instalación usando GUI o PowerShell y compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona

Seguimos los pasos indicados:

- En la pantalla de "tareas de configuración inicial" pulsar en agregar roles.

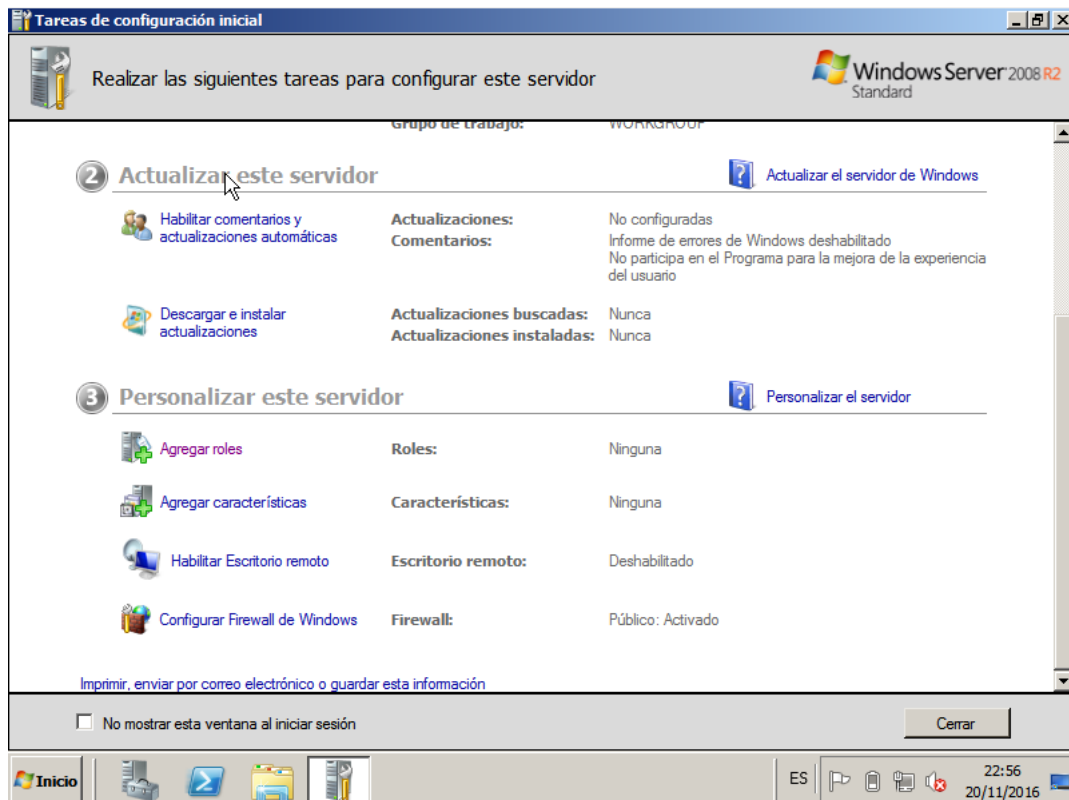


Figura 10.1: Windows Server. Agregar roles

- Dentro del asistente de crear roles, continuar y instalar Servidor Web(IIS).

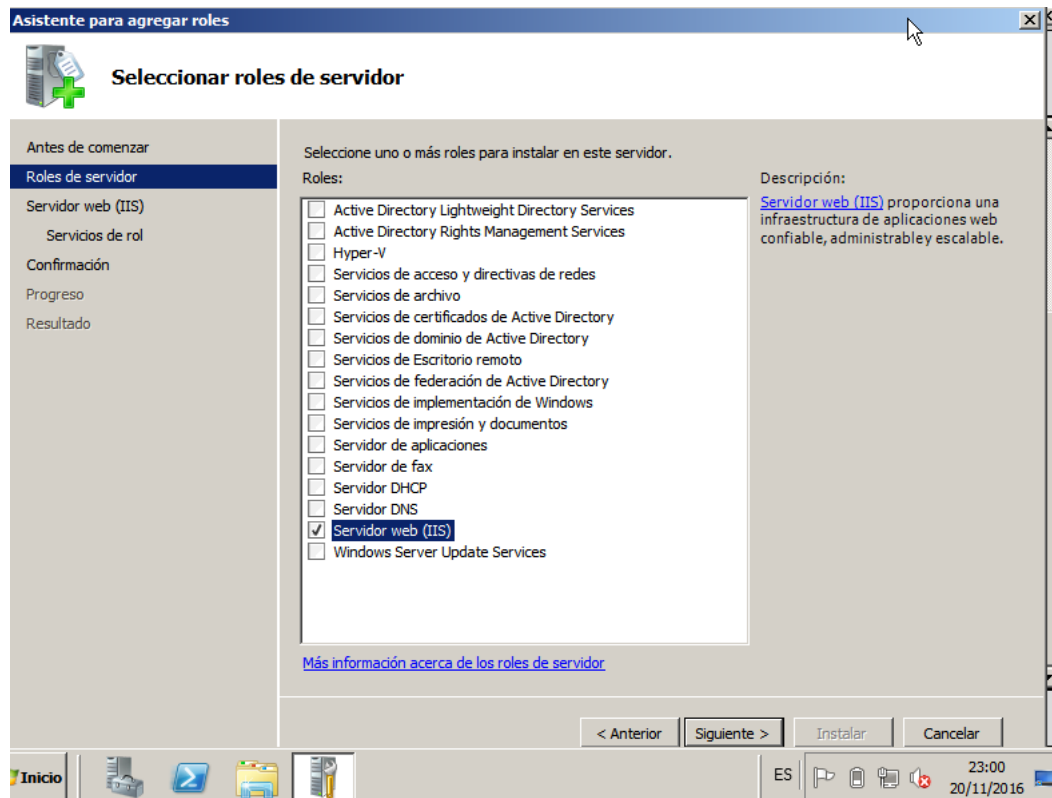


Figura 10.2: Windows Server. Instalar ISS

- Darle a continuar en el asistente y acabar la instalación.

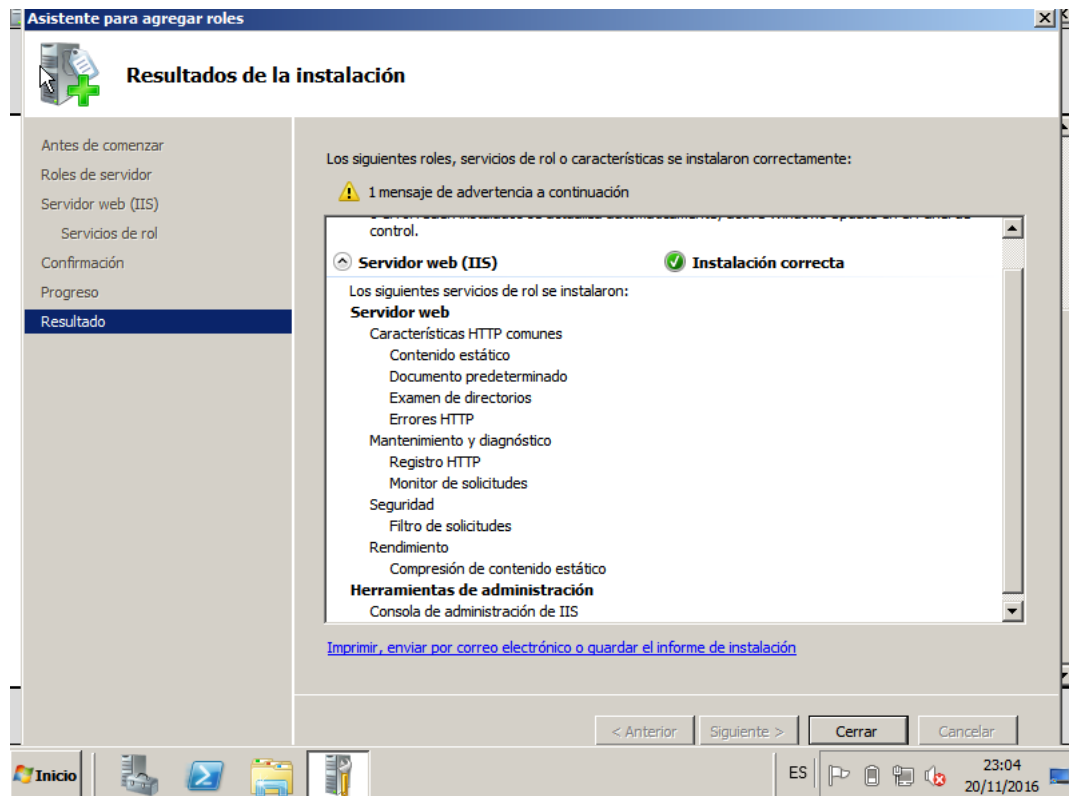


Figura 10.3: Windows Server. Resultados de la instalación de ISS

- Comprobamos que ISS sirve en el localhost de la máquina:

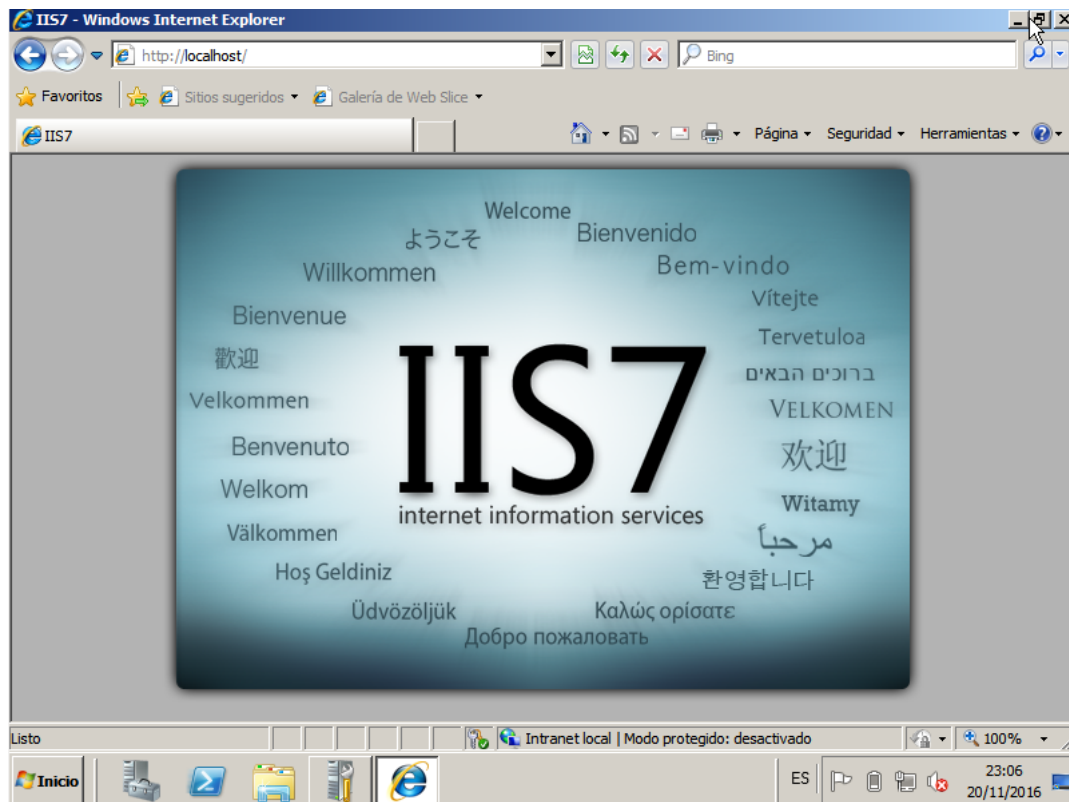


Figura 10.4: Windows Server. Dirección de la máquina virtual

- Ver ip de la máquina usando powerShell (comando `ipconfig[45]`).

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Reservados todos los derechos.

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::7c9f:589b:4bfe:82e5%13
    Dirección IPv4. . . . . : 192.168.56.102
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::11f:b1b2:8ff5:6ab8%11
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de túnel isatap.{38F988B2-9D82-41C1-B229-855E2ED484A3}:

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

Adaptador de túnel isatap.{E3D4FFBA-E473-453C-ADE6-2E6635E29D6A}:

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

PS C:\Users\Administrador>
```

Figura 10.5: Windows Server. Dirección de la máquina virtual

- Comprobar desde la máquina anfitriona que el servidor está correctamente instalado.

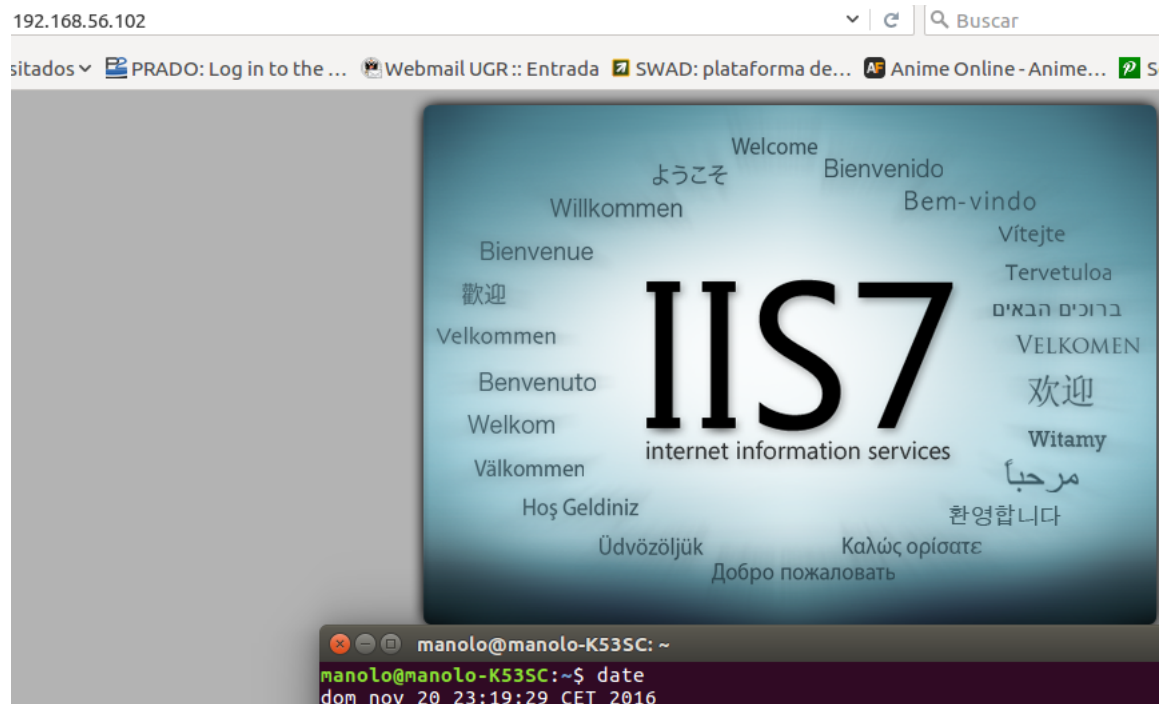


Figura 10.6: Comprobación de ISS en máquina anfitriona

11. Muestre un ejemplo de uso del comando (p.e. <http://fedoraproject.org/wiki/VMWare>)

Encontramos en una página un tutorial para aplicar el comando patch[48]:

- Primero creamos un archivo llamado "probando-patch.cpp"

```
[root@ubuntu tmp 2016-11-24 19:02:07]
$ls
probando-patch.cpp  probando-patch-modificado.cpp
[root@ubuntu tmp 2016-11-24 19:02:13]
$cat probando-patch.cpp
#include <iostream>

using namespace std;

int main()
{
    int a=5;
    cout << "Estamos probando patch" << endl;
    cout << "Numero indicado" << a << endl;
    return 0;
}
[root@ubuntu tmp 2016-11-24 19:02:17]
$
```

Figura 11.1: Creando archivo probando-patch.cpp

- Creamos un segundo archivo modificado sobre el primero y lo llamamos "probando-patch-modificado.cpp".

```
[root@ubuntu tmp 2016-11-24 19:02:41]
$cat probando-patch-modificado.cpp
#include <iostream>

using namespace std;

int main()
{
    int a=5;
    cout << "Estamos probando patch modificandolo" << endl;
    cout << "Numero indicado sumado" << a+1 << endl;
    return 0;
}
[root@ubuntu tmp 2016-11-24 19:02:44]
$-
```

Figura 11.2: Creando archivo probando-patch-modificado.cpp

- Creamos un archivo patch usando el comando diff[32] llamado "parche.patch"

```
[root@ubuntu tmp 2016-11-24 19:13:59]
$diff -u probando-patch.cpp probando-patch-modificado.cpp > parche.patch
[root@ubuntu tmp 2016-11-24 19:15:47]
$cat parche.patch
--- probando-patch.cpp 2016-11-24 19:12:24.352402760 +0100
+++ probando-patch-modificado.cpp 2016-11-24 19:00:53.220402760 +0100
@@ -5,7 +5,7 @@
 int main()
 {
     int a=5;
-    cout << "Estamos probando patch" << endl;
-    cout << "Numero indicado sumado" << a << endl;
+    cout << "Estamos probando patch modificandolo" << endl;
+    cout << "Numero indicado sumado" << a+1 << endl;
     return 0;
 }
[root@ubuntu tmp 2016-11-24 19:15:51]
$
```

Figura 11.3: Creando archivo parche.patch

- Utilizamos el comando patch[40] sobre el archivo "parche.patch" para que se modifique correctamente el archivo creado sin modificar "probando-patch.cpp" para que se actualice a la última versión.

```

[root@ubuntu tmp 2016-11-24 19:02:07]
$ls
probando-patch.cpp  probando-patch-modificado.cpp
[root@ubuntu tmp 2016-11-24 19:02:13]
$cat probando-patch.cpp
#include <iostream>

using namespace std;

int main()
{
    int a=5;
    cout << "Estamos probando patch" << endl;
    cout << "Numero indicado" << a << endl;
    return 0;
}
[root@ubuntu tmp 2016-11-24 19:02:17]
$

```

Figura 11.4: Aplicando parche a probando-patch.cpp

12. 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

Realizaremos la guía de instalación que nos proporciona la página de Webmin[52]:

- Nos vamos al directorio /tmp y descargamos el archivo .gz necesario para instalar webmin.
 - cd /tmp
 - wget http://prdownloads.sourceforge.net/webadmin/webmin-1.820.tar.gz
- Desempaquetamos lo descargado.
 - gunzip webmin-1.820.tar.gz
 - tar xf webmin-1.820.tar
- Ejecutamos el script para webmin y seguimos sus pasos, configurándolo:
 - cd webmin-1.820
 - ./setup.sh /usr/local/webmin . Nos indica la configuración que queremos realizar:
 - Directorio por defecto para archivos de configuración de Webmin. Lo dejamos por defecto en /etc/webmin.
 - Directorio para archivos de log de Webmin. Lo dejamos por defecto en /var/webmin.
 - Ruta para perl. Lo dejamos por defecto /usr/bin/perl.
 - Puerto para el servidor web. Lo dejamos por defecto a 10000.

- Nombre para inicio de sesión. La dejamos por defecto para admin.
- Contraseña para usuario admin. Escribimos la contraseña que queramos.
- Usar SSL. Le indicamos que no.
- Iniciar Webmin cada vez que arranquemos el sistema. Le damos a sí.

```
Installing Webmin from /tmp/webmin-1.820 to /usr/local/webmin ...

*****
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Log file directory [/var/webmin]:

*****
Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.

Full path to perl (default /usr/bin/perl):

Testing Perl ...
Perl seems to be installed ok

*****
Operating system name:   Ubuntu Linux
Operating system version: 14.04.5

*****
Webmin uses its own password protected web server to provide access
to the administration programs. The setup script needs to know :
- What port to run the web server on. There must not be another
  web server already using this port.
- The login name required to access the web server.
- The password required to access the web server.
- If the webserver should use SSL (if your system supports it).
- Whether to start webmin at boot time.

Web server port (default 10000):
Login name (default admin): _
```

Figura 12.1: Estableciendo configuración Webmin

- Finaliza la instalación diciendo que Webmin ha sido instalado satisfactoriamente.

```
Attempting to start Webmin mini web server..
Starting Webmin server in /usr/local/webmin
Pre-loaded WebminCore
..done

*****
Webmin has been installed and started successfully. Use your web
browser to go to

    http://ubuntu:10000/

and login with the name and password you entered previously.
```

Figura 12.2: Webmin instalado correctamente

Una vez configurado e instalado en nuestra máquina virtual de Ubuntu Server, comprobamos que se ha configurado correctamente accediendo al servidor Webmin remotamente desde la máquina anfitriona:

- Si tenemos el firewall activo, debemos habilitar el puerto de Webmin 10000:
 - `sudo ufw enable`
 - `sudo ufw allow 10000`.
- Accedemos a él y comprobamos que funciona.
 - Comprobando que sirve.



Figura 12.3: Comprobando Webmin remotamente

- Entrando el webmin con nuestra cuenta.

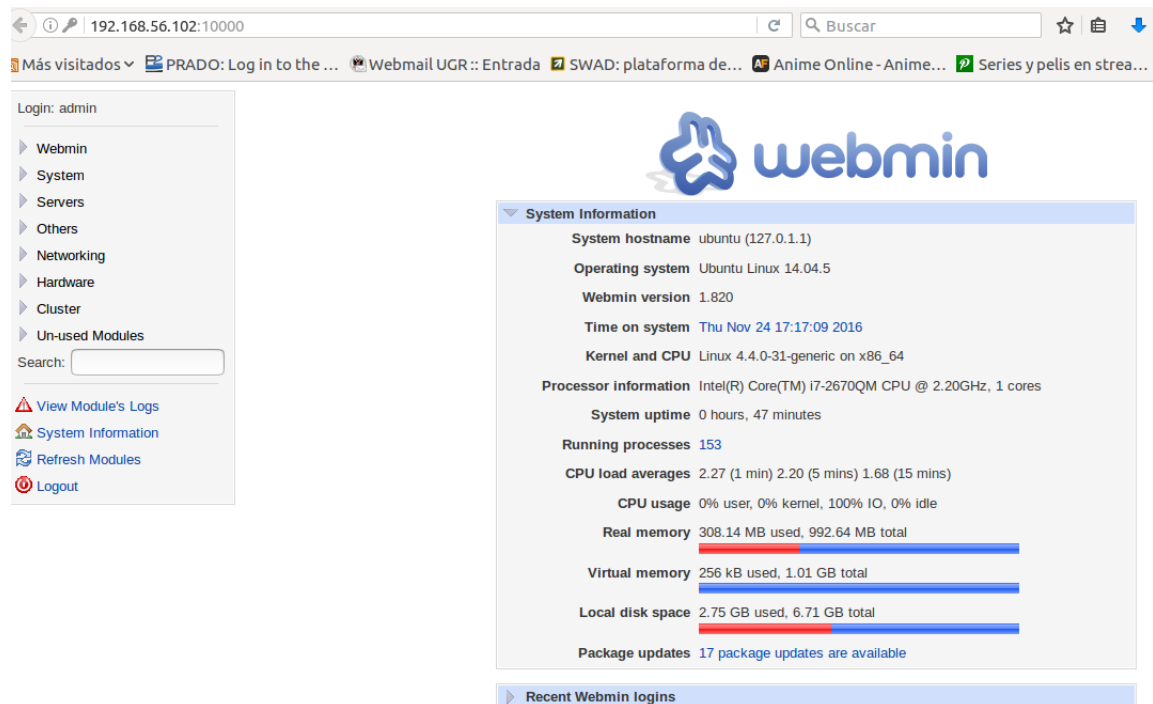


Figura 12.4: Iniciando sesión en Webmin remotamente

13. Instale phpMyAdmin, indique cómo lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs de hasta 25MiB (en vez de los 8 MiB de límite por defecto). Indique cómo ha realizado el proceso y muestre capturas de pantalla.

Realizamos la instalación de phpMyAdmin desde los repositorios de Debian[51]:

- Instalamos con `sudo apt install phpMyAdmin`

```

[nanolo@ubuntu ~] 2016-11-24 20:11:03
$ sudo apt install phpmyadmin
[sudo] password for nanolo:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libblas3 liblinear-tools liblinear1 liblua5.2-0
Use 'apt-get autoremove' to remove them.
Se instalarán los siguientes paquetes extras:
 dbconfig-common javascript-common libjs-codemirror libjs-jquery
 libjs-jquery-cookie libjs-jquery-event-drag libjs-jquery-metadata
 libjs-jquery-mousewheel libjs-jquery-tablesorter libjs-jquery-ui
 libjs-underscore libmcrypt4 php-gettext php5-gd php5-mcrypt webmin
Paquetes sugeridos:
 libjs-jquery-ui-docs libmcrypt-dev mcrypt
Se instalarán los siguientes paquetes NUEVOS:
 dbconfig-common javascript-common libjs-codemirror libjs-jquery
 libjs-jquery-cookie libjs-jquery-event-drag libjs-jquery-metadata
 libjs-jquery-mousewheel libjs-jquery-tablesorter libjs-jquery-ui
 libjs-underscore libmcrypt4 php-gettext php5-gd php5-mcrypt phpmyadmin
Se actualizarán los siguientes paquetes:
 webmin
1 actualizados, 16 se instalarán, 0 para eliminar y 17 no actualizados.
1 no instalados del todo o eliminados.
Se necesita descargar 5.708 kB/20,9 MB de archivos.
Se utilizarán 190 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] ^[[

```

Figura 13.1: Instalando phpmyadmin

- Elegimos Apache2 como servidor para ejecutar phpmyadmin.

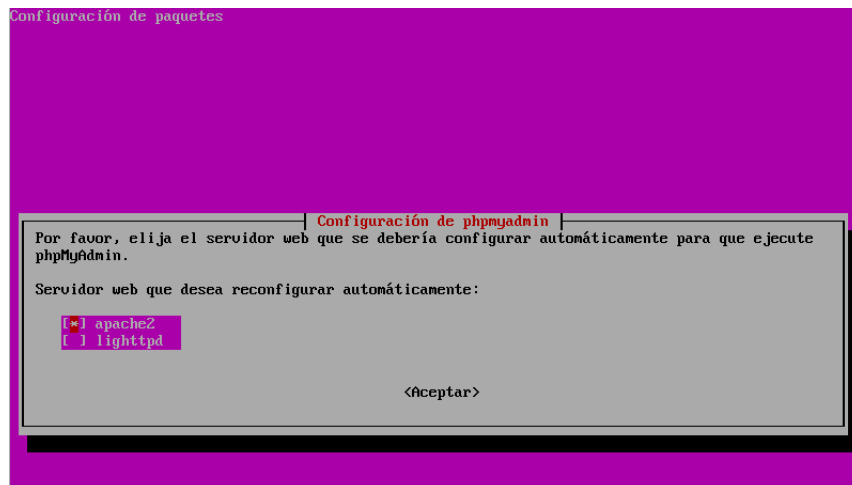


Figura 13.2: Instalando phpmyadmin, eligiendo Apache2 como server

- Ponemos no a configurar la base de datos para phpmyadmin con "dbconfig-common".

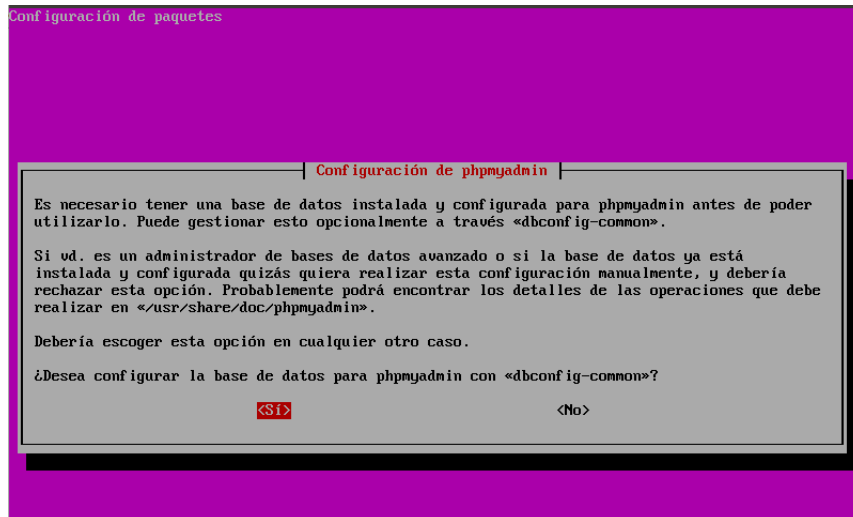


Figura 13.3: Instalando phpmyadmin. No configurar DB con dbconfig-common

- Establecemos la contraseña para phpmyadmin.

Una vez instalado phpMyAdmin, nos vamos a sus archivos de configuración[50, 49] para configurar el tamaño para importar BDs a 25MBs.

- Nos vamos al directorio `/etc/php5/apache2/` y abrimos el archivo `php.ini`.
- Dentro del archivo de configuración debemos cambiar los valores de las variables:
 - `post_max_size = 25M`

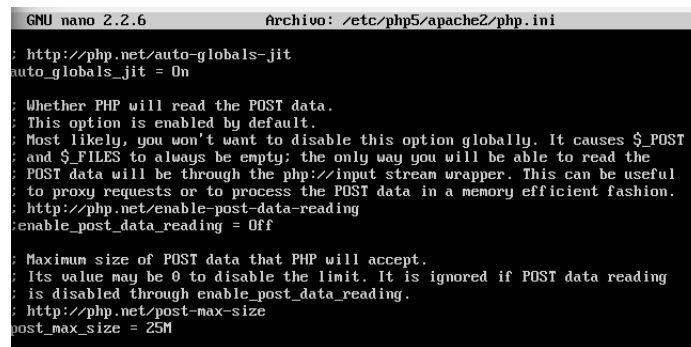


Figura 13.4: Cambiando archivo de configuracion phpmyadmin. Variable `post_max_size`

- `upload_max_filesize = 25M`

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

;::::::::::::::::::
; File Uploads ;
;::::::::::::::::::

; 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 = 25M

; 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

; Whether to allow include/require to open URLs (like http:// or ftp://) as files
; http://php.net/allow-url-include
allow_url_include = Off

^G Ver ayuda  ^O Guardar  ^R Leer fich. ^Y Pág. ant. ^X Cortar Texto
^X Salir      ^J Justificar ^U Buscar    ^U Pág. sig. ^U PegarTxt
```

Figura 13.5: Cambiando archivo de configuracion phpmyadmin. Variable `upload_max_filesize`

- Reiniciamos el servicio apache2.
 - `sudo service apache2 restart`
- Comprobamos remotamente que podemos acceder a phpmyadmin.



Figura 13.6: Comprobando remotamente phpmyadmin

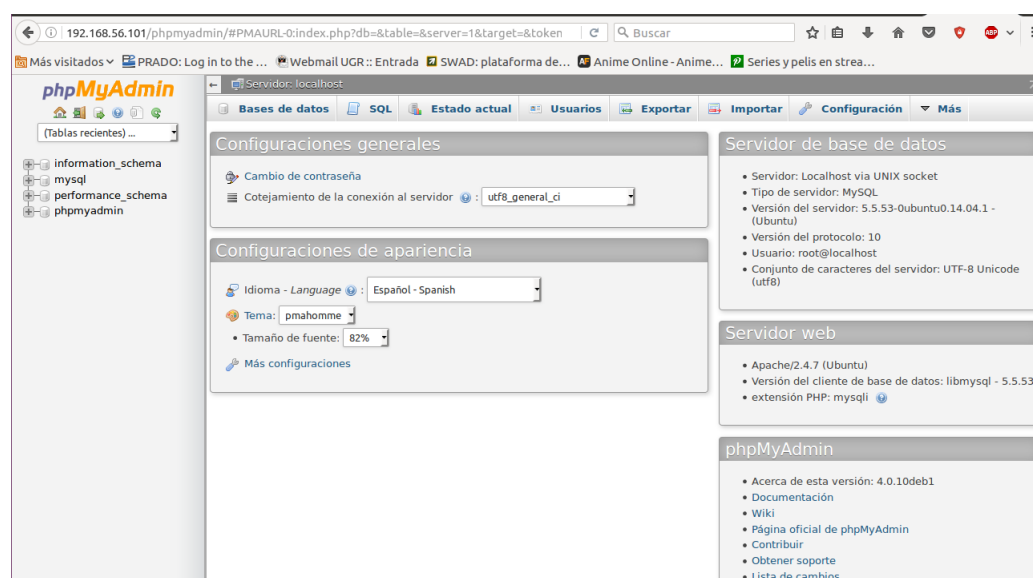


Figura 13.7: Iniciando remotamente a phpmyadmin

- Comprobamos que podemos importar BDs de hasta 25M.

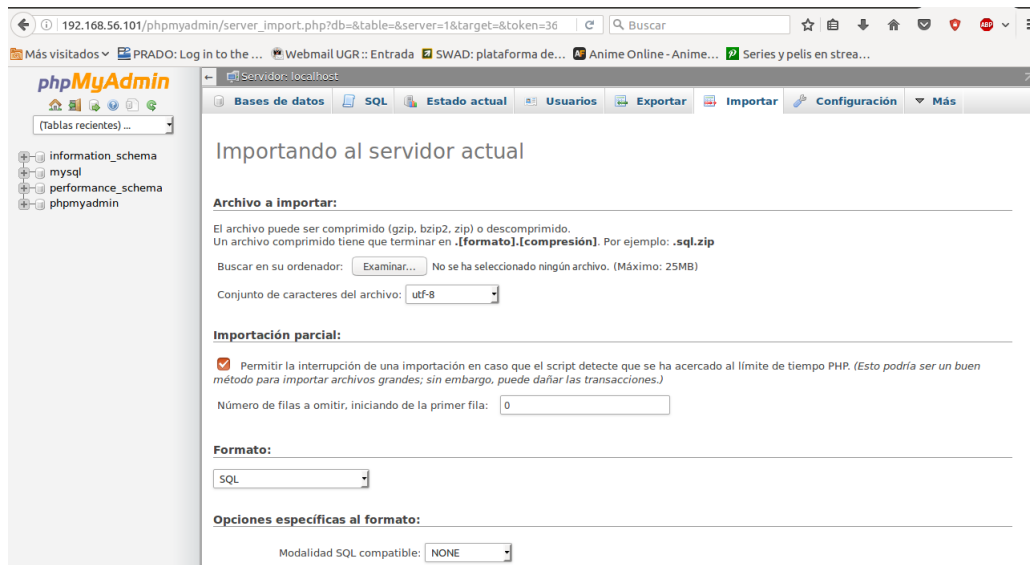


Figura 13.8: Comprobando remotamente tamaño de exportación BDs de phpmyadmin

14. Visite al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando qué está realizando.

He visitado DirectAdmin y tiene diferentes demos las cuales sirven para:

- Usuario: Tienen conocimiento básico.
- Distribuidores: Los que pueden crear cuentas de usuarios.
- Administradores: Conocimiento total sobre los dos anteriores.

Aquí dejo unas imágenes:



Figura 14.1: DirectAdmin. Monitorización de servicios

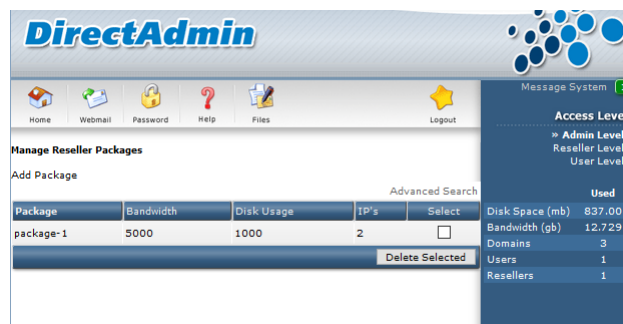


Figura 14.2: DirectAdmin. Gestión de paquetes de distribuidores

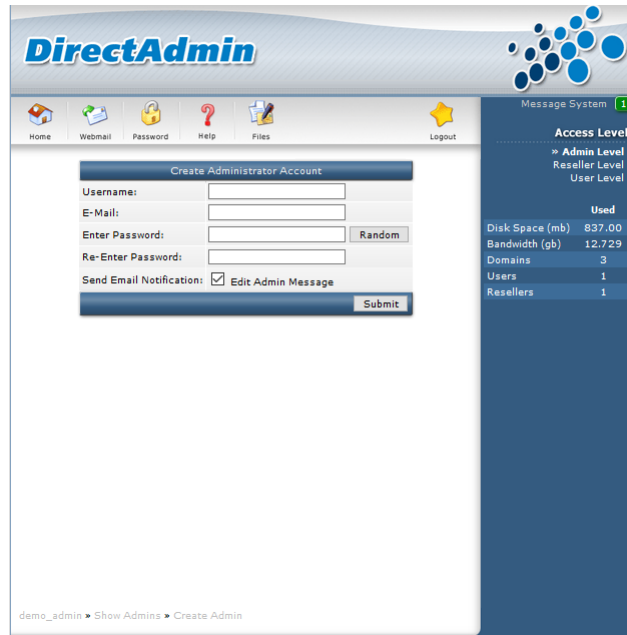


Figura 14.3: DirectAdmin. Creación de admin

15. a) Ejecute los ejemplos de find, grep b) Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio. c) Muestre un ejemplo de uso para awk

15.1. a) Ejecute los ejemplos de find, grep

Vamos a ejecutar los ejemplos que tenemos en el guión, adaptándolos a nosotros. También miramos la documentación sobre ambos comandos para aprender más de ellos.

- Ejemplo de ejecución de grep[56] junto con ps[57].
 - `ps -Af | grep firefox`

```
[manolo@ubuntu ~] 2016-11-25 10:55:10
$ps -Af | grep firefox
manolo 2129 2055 0 10:55 tty1 00:00:00 grep --color=auto firefox
[manolo@ubuntu ~] 2016-11-25 10:55:19
$
```

Figura 15.1: Ejemplo de uso de comando grep

- Ejemplo de ejecución de find.
 - Vamos a exportar remotamente un fichero con extensión pdf a nuestra máquina virtual de Ubuntu Server. Para ello hacemos uso del comando scp[58].

```

manolo@manolo-K53SC:~/Documentos/aas$ scp ISE-P1-InstSOyRAID.pdf manolo
@192.168.56.101:/home/manolo/
manolo@192.168.56.101's password:
Permission denied, please try again.
manolo@192.168.56.101's password:
ISE-P1-InstSOyRAID.pdf          100% 627KB 627.3KB/s   00:00
manolo@manolo-K53SC:~/Documentos/aas$ date
vie nov 25 11:52:39 CET 2016

```

Figura 15.2: Exportar archivo pdf por ssh

- Comprobamos que se ha exportado correctamente.

```

[manolo@ubuntu ~ 2016-11-25 11:47:18
$ls /home/manolo/ISE-P1-InstSOyRAID.pdf
/home/manolo/ISE-P1-InstSOyRAID.pdf
[manolo@ubuntu ~ 2016-11-25 11:47:25
$

```

Figura 15.3: Comprobando exportación por ssh

- Ejecutamos la orden find del ejemplo:

```

[manolo@ubuntu ~ 2016-11-25 12:44:50
$find /home/manolo/ -name '*.pdf' -exec cp {} ~/PDFs \;
cp: «/home/manolo/PDFs/ISE-P2-InstServ.pdf» y «/home/manolo/PDFs/ISE-P2-InstServ.pdf» son el mismo f
ichero
[manolo@ubuntu ~ 2016-11-25 12:45:23
$ls
ISE-P1-InstSOyRAID.pdf ISE-P2-InstServ.pdf PDFs
[manolo@ubuntu ~ 2016-11-25 12:45:34
$cd PDFs/
[manolo@ubuntu PDFs 2016-11-25 12:45:36
$ls
ISE-P1-InstSOyRAID.pdf ISE-P2-InstServ.pdf

```

Figura 15.4: Ejemplo de uso de comando find

15.2. b) Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio.

El script realizado usando sed[59] para cambiar ssh y reiniciar su servicio es el siguiente:

```

[manolo@ubuntu ~ 2016-11-25 20:30:30
$cat ejercicio15.sh
#!/bin/bash

sudo sed -i 's/Port 22/Port 555/' /etc/ssh/sshd_config
sudo service ssh restart

[manolo@ubuntu ~ 2016-11-25 20:30:41
$

```

Figura 15.5: Script creado con sed para cambiar configuración ssh

Al ejecutarlo, me cambiará el puerto 22 que tiene por defecto ssh y me lo establecerá a 555. Después reiniciará el servicio ssh.

```

[manolo@ubuntu ~] 2016-11-25 20:33:23
$ ./ejercicio15.sh
ssh stop/waiting
ssh start/running, process 2461
[manolo@ubuntu ~] 2016-11-25 20:33:25
$ _

```

Figura 15.6: Ejecutando script que usa comando sed

Podemos ver como los cambios se han aplicado correctamente mirando el archivo de configuración de ssh.

```

GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 555
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

```

Figura 15.7: Comprobando cambios que realizó el script con sed

15.3. c) Muestre un ejemplo de uso para awk

Vamos a comprobar utilizando el comando awk[59], el contenido de la variable PermitRootLogin del fichero sshd_config.

```

[manolo@ubuntu PDFs] 2016-11-25 14:11:32
$ awk '/PermitRootLogin/' /etc/ssh/sshd_config
PermitRootLogin no
# the setting of "PermitRootLogin without-password".
[manolo@ubuntu PDFs] 2016-11-25 14:11:38
$

```

Figura 15.8: Ejemplo de uso para awk

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

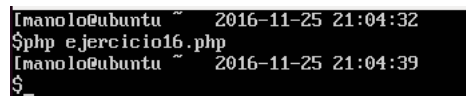
He creado un script en php, que se basa en el uso de exec para ejecutar el un comando[53, 54]. El script es el siguiente:



```
[manolo@ubuntu ~] 2016-11-25 21:03:23
$cat ejercicio16.php
<?php
exec ("sudo sed -i 's/Port 22/Port 500/' /etc/ssh/sshd_config");
exec ("sudo service ssh restart");
?>
[manolo@ubuntu ~] 2016-11-25 21:03:54
$
```

Figura 16.1: Script en php para acceso a ssh

Con este script cambiamos el puerto de ssh a 500. Vamos a ejecutarlo:



```
[manolo@ubuntu ~] 2016-11-25 21:04:32
$php ejercicio16.php
[manolo@ubuntu ~] 2016-11-25 21:04:39
$_
```

Figura 16.2: Ejecución de script en php para acceso a ssh

Una vez ejecutado, comprobamos que el puerto ha sido cambiado en el archivo de configuración de ssh:

```
GNU nano 2.2.6 Archivo: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 500
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

[ 88 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer fich. ^Y Pág. ant. ^K Cortar Texto
^X Salir ^J Justificar ^W Buscar ^U Pág. sig. ^U PegarTxt
```

Figura 16.3: Comprobar cambios en ssh tras ejecutar script en php

Comprobamos que el servicio ssh ha sido reiniciado y que nos podemos conectar remotamente al puerto 500:

```
manolo@manolo-K535C:~$ ssh -p 500 192.168.56.102
manolo@192.168.56.102's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

System information as of Fri Nov 25 21:02:54 CET 2016

System load:  0.13           Processes:    145
Usage of /home: 0.4% of 919MB Users logged in: 1
Memory usage:  12%          IP address for eth0: 10.0.2.15
Swap usage:    0%           IP address for eth1: 192.168.56.102

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

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Nov 25 21:02:54 2016 from 192.168.56.1
[manolo@ubuntu ~    2016-11-25 21:04:58
$
```

Figura 16.4: Conexión por ssh al puerto 500

17. Abra una consola de Powershell y pruebe a parar un programa en ejecución (p.ej), realice capturas de pantalla y comente lo que muestra.

Primero vamos a instalar la funcionalidad ISE(Windows PowerShell Integrated Scripting Environment).

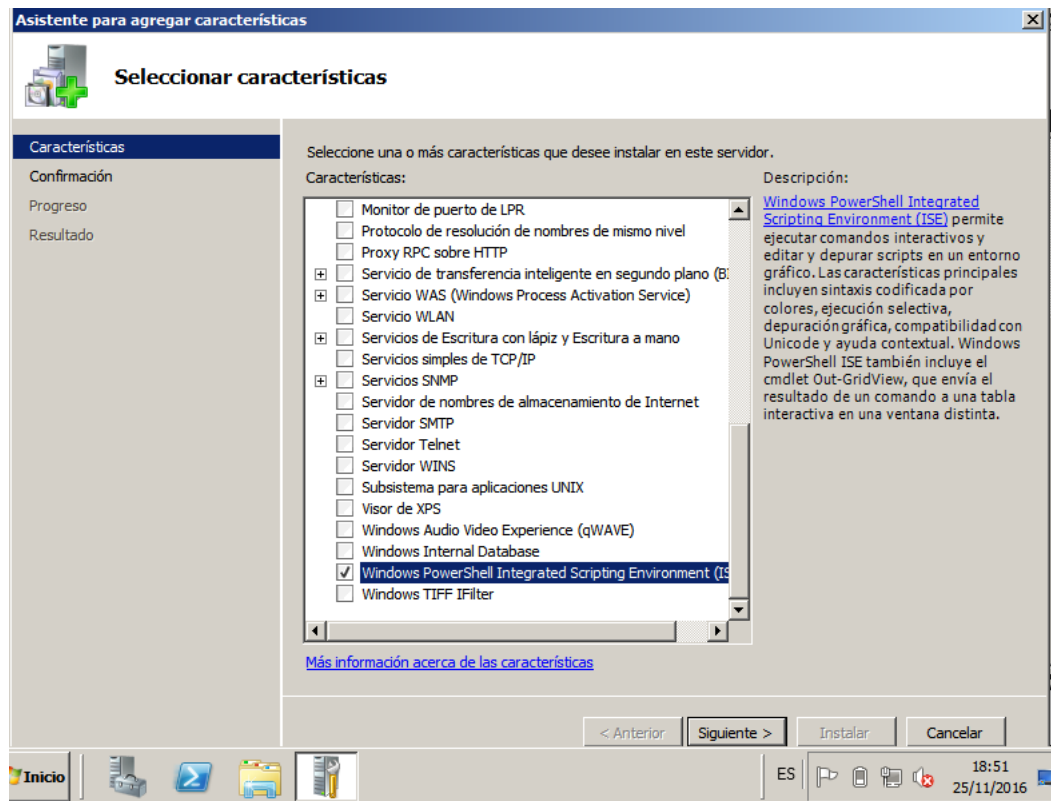


Figura 17.1: Instalando ISE en Windows Server

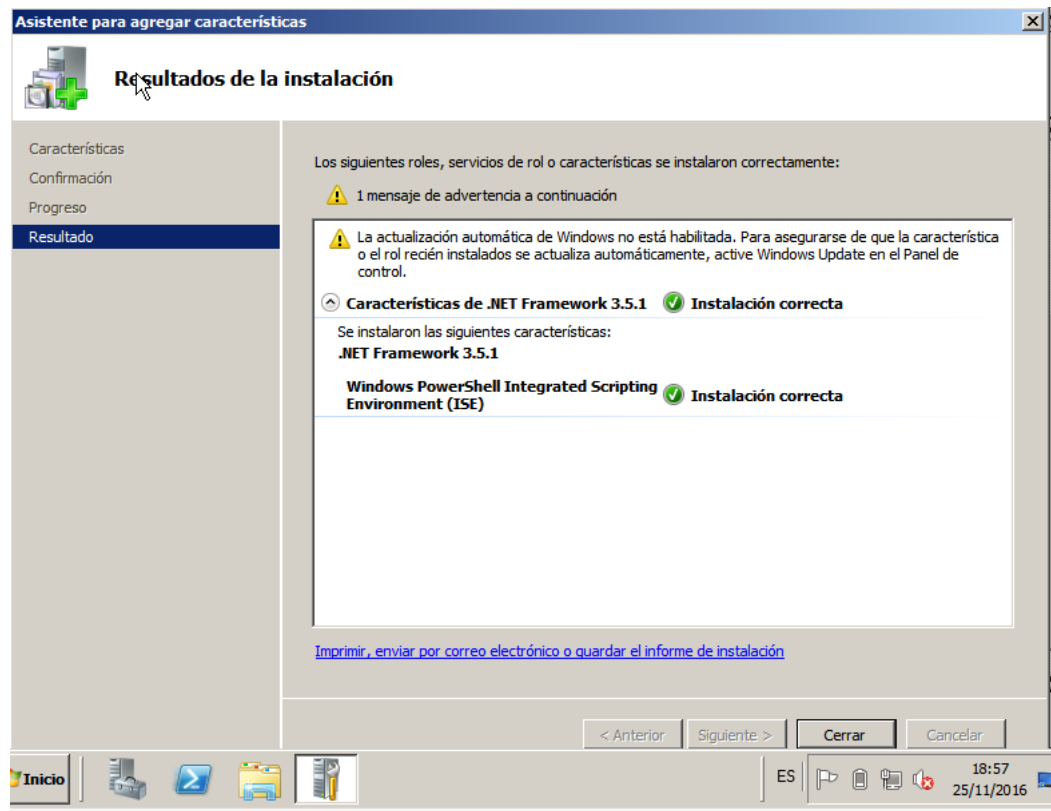


Figura 17.2: ISE resultados de la instalación en Windows Server

Una vez que ya tenemos esa funcionalidad, vamos a abrir un programa, por ejemplo Paint.

PS C:\Users\Adminis\trador> Get-Process

Handles	NPM(K)	PM(K)	WS(K)	UM(K)	CPU(s)	Id	ProcessName
43	6	1956	4964	53	2.58	1688	conhost
387	10	1720	3536	42	0.31	288	csrss
195	11	1784	5480	43	1.81	328	csrss
66	7	1328	4128	49	0.02	380	dwm
542	34	14368	28180	163	1.94	2244	explorer
0	0	0	24	0	0	0	idle
533	19	3528	9808	38	1.02	432	lsass
142	7	2016	3660	18	0.03	440	lsn
460	41	52508	23676	642	7.38	1252	mmc
76	8	2196	5224	36	0.06	1516	mscorsvw
85	10	1900	4912	35	0.09	1556	mscorsvw
144	17	3240	7260	60	0.02	1932	msdtc
116	37	8296	17032	108	0.48	2884	mspaint
625	24	50276	49812	565	2.70	696	powershell
204	12	3472	7260	30	0.52	424	services
29	2	352	1012	5	0.08	212	smss
261	18	5976	10144	73	0.06	496	spoolsv
148	8	6340	11800	37	2.47	1336	sppsvc
46	4	788	2572	13	0.02	228	svchost
346	13	3352	8128	41	0.81	536	svchost
228	15	2820	6332	31	0.36	612	svchost
277	15	8764	11564	44	1.06	700	svchost
795	34	14504	25972	365	1.53	732	svchost
298	17	5056	9360	39	0.31	780	svchost
91	10	4292	8536	36	0.14	820	svchost
268	15	3700	9396	61	0.47	824	svchost
500	30	10436	15044	80	0.83	864	svchost
290	32	9040	11120	48	0.45	992	svchost
128	12	5984	9272	39	0.06	1048	svchost
68	6	1360	4244	29	0.05	1844	svchost
603	0	112	300	3	0.00	4	System
138	11	2672	5944	51	0.00	1792	taskhost
124	10	2264	6768	50	0.27	1964	TrustedInstaller
78	9	1320	4124	43	0.16	336	wininit
99	7	1524	4036	27	0.23	364	winlogon
44	6	864	3180	22	0.00	1080	wlms

Esta copia de windows no es original

Inicio ES 20:06 25/11/2016

Figura 17.4: Viendo procesos activos con PowerShell

Vemos como aparece con nombre de proceso mspaint con id 2884. Vamos a parar ese proceso con el comando Stop-Process -Id 2884.

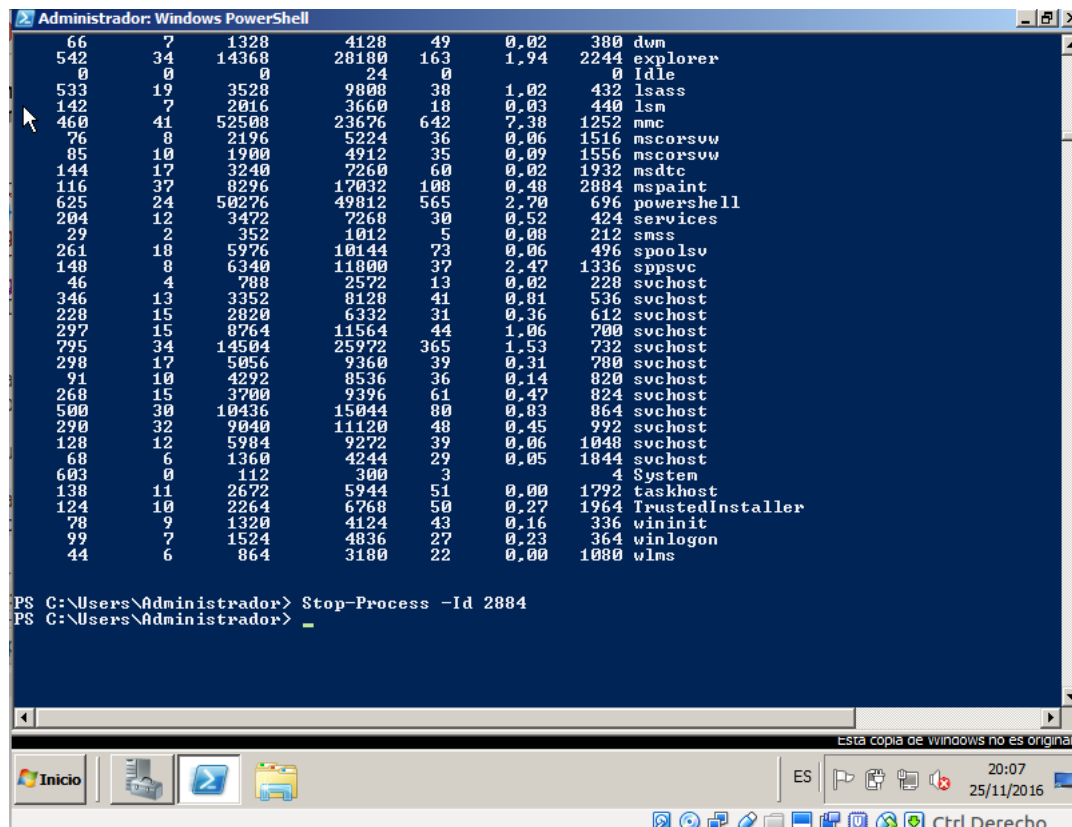


Figura 17.5: Parando proceso activo con PowerShell

Tras ejecutar el comando para pararlo, el programa Paint se cierra.

18. **Opcional 1: Instale y pruebe terminator y/o tmux. Con screen, pruebe su funcionamiento dejando sesiones ssh abiertas en el servidor y recuperándolas posteriormente.**
19. **Opcional 2: Instale el servicio y pruebe su funcionamiento.**

Vamos a realizar una demostración por ssh para probar que nos bloquea la conexión a una dirección dependiendo de lo establecido en la configuración. Antes debemos configurar el firewall (ufw) para permitir conexiones por el puerto 22 (ssh).

Ahora vamos a instalar y probar failban[63, 60]:

- Instalamos fail2ban: `sudo apt-get install fail2ban`.

- La configuración esta en `/etc/fail2ban/jail.conf`. Aquí vemos como está configurado el servicio 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 = 6

[dropbear]
enabled = false
port = ssh
filter = dropbear
logpath = /var/log/auth.log
maxretry = 6

^G Ver ayuda  ^O Guardar  ^R Leer fich. ^Y Pág. ant. ^K Cortar Texto ^C Posición
^X Salir      ^J Justificar ^W Buscar    ^U Pág. sig. ^L PegarTxt    ^T Ortografía
```

Figura 19.1: Configuración de fail2ban para ssh

Podemos ver como tiene varias variables a tener en cuenta, las cuales son:

- enabled: habilitar/ inhabilitar
 - port: puerto del servicio
 - filter: proceso del servicio.
 - logpath: ruta hacia el archivo a escanear
 - maxretry: cantidad máxima de intentos fallidos de autenticación antes de ser bloqueado.
 - findtime: ventana de tiempo en segundos durante el cual se tima en cuenta el parámetro maxretry.
 - bantime: tiempo en segundos que durará el bloqueo de la dirección.
- Modificamos el archivo de configuración de tal modo que:
 - Que con 2 intentos nos bloquee el servicio. Añadimos `maxretry = 2`

- El tiempo que estaremos baneados será de 60 segundos. Añadimos bantime = 60.

```
#
# 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 = 2
findtime = 600
bantime = 60

[dropbear]
enabled = false
port = ssh
filter = dropbear
```

Figura 19.2: Modificando configuración de fail2ban para ssh

- Reiniciamos el servicio fail2ban para guardar cambios: `sudo service fail2ban restart`
- Probamos a conectarnos por ssh desde otra máquina, poniendo contraseñas erróneas. Tras intentarlo 2 veces, vemos como aparece un mensaje de bloqueo o baneo:

```

manolo@manolo-K53SC:~$ ssh manolo@192.168.56.102
manolo@192.168.56.102's password:
Permission denied, please try again.
manolo@192.168.56.102's password:
Permission denied, please try again.
manolo@192.168.56.102's password:
Permission denied (publickey,password).
manolo@manolo-K53SC:~$ ssh manolo@192.168.56.102
manolo@192.168.56.102's password:
Permission denied, please try again.
manolo@192.168.56.102's password:
^C
manolo@manolo-K53SC:~$ ssh manolo@192.168.56.102
ssh: connect to host 192.168.56.102 port 22: Connection refused
manolo@manolo-K53SC:~$ date
vie feb  3 20:59:09 CET 2017
manolo@manolo-K53SC:~$

```

Figura 19.3: Baneo de fail2ban

- Probamos a conectarnos tras 1 minuto, para ver si nos deja. Efectivamente si nos deja.

```

manolo@manolo-K53SC:~$ ssh manolo@192.168.56.102
manolo@192.168.56.102's password:
Permission denied, please try again.
manolo@192.168.56.102's password:

manolo@manolo-K53SC:~$ date
vie feb  3 21:01:18 CET 2017
manolo@manolo-K53SC:~$

```

Figura 19.4: Conexión ssh tras esperar baneo de fail2ban

20. Opcional 3: Instale el servicio y pruebe su funcionamiento.

Vamos a instalar el programa Rkhunter y realizar un análisis de nuestro equipo[61].

- Descargamos el programa de la página oficial[62]
- Lo descomprimos y instalamos. Su archivo de instalación se llama installer.sh. Lo instalamos con la orden: `sudo ./installer.sh --install`
- Miramos el manual de rkhunter (`man rkhunter`).
- Ejecutamos un análisis con la opción `-c` o `--check`: `sudo rkhunter -c`
- Vemos como va analizando el sistema. Analiza comandos del sistema, rootkits (trojanos, gusanos,...), la red, el localhost e incluso versiones de aplicaciones (gnuPG, OpenSSL, PHP, OpenSSH) que fueron en algunas versiones vulnerables.

```

Performing 'strings' command checks
Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables [ None found ]
Checking for preloaded libraries [ None found ]
Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
Checking for prerequisites [ Warning ]
/usr/local/bin/rkhunter [ OK ]
/usr/sbin/adduser [ Warning ]
/usr/sbin/chroot [ OK ]
/usr/sbin/cron [ OK ]
/usr/sbin/groupadd [ OK ]
/usr/sbin/groupdel [ OK ]
/usr/sbin/groupmod [ OK ]
/usr/sbin/grpck [ OK ]
/usr/sbin/nologin [ OK ]
/usr/sbin/pwck [ OK ]
/usr/sbin/rsyslogd [ OK ]
/usr/sbin/sshd [ OK ]
/usr/sbin/tcpd [ OK ]

```

Figura 20.1: Foto 1.Rkhunter analizando sistema

```

Checking for rootkits...

Performing check of known rootkit files and directories
55808 Trojan - Variant A [ Not found ]
ADM Worm [ Not found ]
AjaKit Rootkit [ Not found ]
Adore Rootkit [ Not found ]
aPa Kit [ Not found ]
Apache Worm [ Not found ]
Ambient (ark) Rootkit [ Not found ]
Balaur Rootkit [ Not found ]
BeastKit Rootkit [ Not found ]
beX2 Rootkit [ Not found ]
BOBKit Rootkit [ Not found ]
cb Rootkit [ Not found ]
CiNIK Worm (Slapper.B variant) [ Not found ]
Danny-Boy's Abuse Kit [ Not found ]
Devil RootKit [ Not found ]
Dica-Kit Rootkit [ Not found ]

```

Figura 20.2: Foto 2.Rkhunter analizando sistema

- Al final del análisis nos muestra un resumen. En él nos muestra los archivos comprobados, los archivos sospechosos, los rootkits comprobados y los que podrían ser uno, y las aplicaciones sospechosas.

```

System checks summary
=====

File properties checks...
  Required commands check failed
  Files checked: 145
  Suspect files: 6

Rootkit checks...
  Rootkits checked : 380
  Possible rootkits: 0

Applications checks...
  Applications checked: 4
  Suspect applications: 0

The system checks took: 4 minutes and 25 seconds

All results have been written to the log file: /var/log/rkhunter.log

```

Figura 20.3: Resumen del análisis de Rkhunter

Este programa es útil, ya que informa de posibles rootkits que podrían estar en nuestro sistema y vulnerabilidades que podrían ser explotadas. De hecho cada [warning] puede ser un aspecto de seguridad a mejorar.

21. **Opcional 4: Realice la instalación de uno de estos dos “web containers” y pruebe su ejecución**
22. **Opcional 5: 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/>)**

Referencias

- [1] <http://manpages.ubuntu.com/manpages/wily/en/man5/apt.conf.5.html>, consultado el 10 de Noviembre de 2016.
- [2] <http://manpages.ubuntu.com/manpages/wily/man1/add-apt-repository.1.html>, consultado el 10 de Noviembre de 2016.
- [3] <http://manpages.ubuntu.com/manpages/xenial/man8/apt.8.html>, consultado el 10 de Noviembre de 2016.
- [4] <http://manpages.ubuntu.com/manpages/xenial/man8/ufw.8.html>, consultado el 10 de Noviembre de 2016.
- [5] https://wiki.archlinux.org/index.php/Secure_Shell, consultado el 10 de Noviembre de 2016.

- [6] <https://wiki.archlinux.org/index.php/telnet>, consultado el 10 de Noviembre de 2016.
- [7] <http://man.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man1/ssh.1?query=ssh%26sec=1>, consultado el 17 de Noviembre de 2016.
- [8] <http://mcuser.uv.es/es/art.php?art=ard&pag=rx11.html>, consultado el 17 de Noviembre de 2016.
- [9] <http://mcuser.uv.es/es/art.php?art=ard&pag=rx11.html>, consultado el 17 de Noviembre de 2016.
- [10] <https://linux.die.net/man/5/yum.conf>, consultado el 17 de Noviembre de 2016.
- [11] <https://linux.die.net/man/8/yum>, consultado el 17 de Noviembre de 2016.
- [12] https://wiki.archlinux.org/index.php/Secure_Shell#X11_forwarding, consultado el 17 de Noviembre de 2016.
- [13] <https://www.openssh.com/manual.html>, consultado el 17 de Noviembre de 2016.
- [14] <http://man7.org/linux/man-pages/man1/yum-config-manager.1.html>, consultado el 18 de Noviembre de 2016.
- [15] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Managing_Yum_Repositories.html, consultado el 18 de Noviembre de 2016.
- [16] <https://access.redhat.com/solutions/265523>, consultado el 18 de Noviembre de 2016.
- [17] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Reference_Guide/ch-ssh.html, consultado el 19 de Noviembre de 2016.
- [18] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/V2V_Guide/Preperation_Before_the_P2V_Migration-Enable_Root_Login_over_SSH.html, consultado el 19 de Noviembre de 2016.
- [19] <https://fedoraproject.org/wiki/Firewalld/es>, consultado el 19 de Noviembre de 2016.
- [20] <https://linux.die.net/man/1/nmap>, consultado el 19 de Noviembre de 2016.
- [21] <https://linux.die.net/man/1/ssh-copy-id>, consultado el 19 de Noviembre de 2016.
- [22] <https://linux.die.net/man/1/ssh-keygen>, consultado el 19 de Noviembre de 2016.

- [23] https://linux.die.net/man/5/sshd_config, consultado el 19 de Noviembre de 2016.
- [24] <https://linux.die.net/man/8/dhclient>, consultado el 19 de Noviembre de 2016.
- [25] <https://linux.die.net/man/8/ifconfig>, consultado el 19 de Noviembre de 2016.
- [26] <https://tools.ietf.org/html/rfc318>, consultado el 19 de Noviembre de 2016.
- [27] <https://tools.ietf.org/html/rfc4253>, consultado el 19 de Noviembre de 2016.
- [28] <https://tools.ietf.org/html/rfc854>, consultado el 19 de Noviembre de 2016.
- [29] <https://wiki.debian.org/es/NetworkConfiguration>, consultado el 19 de Noviembre de 2016.
- [30] <http://www.firewalld.org/documentation/man-pages/firewall-cmd.html>, consultado el 19 de Noviembre de 2016.
- [31] <http://www.tldp.org/HOWTO/Text-Terminal-HOWTO-12.html#ss12.5>, consultado el 19 de Noviembre de 2016.
- [32] <http://man7.org/linux/man-pages/man1/diff.1.html>, consultado el 20 de Noviembre de 2016.
- [33] <http://php.net/manual/en/features.commandline.interactive.php>, consultado el 20 de Noviembre de 2016.
- [34] <http://php.net/manual/es/configuration.file.php>, consultado el 20 de Noviembre de 2016.
- [35] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Confined_Services/chap-Managing_Confined_Services-The_Apache_HTTP_Server.html, consultado el 20 de Noviembre de 2016.
- [36] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/chap-Managing_Confined_Services-MariaDB.html, consultado el 20 de Noviembre de 2016.
- [37] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/sect-Managing_Services_with_systemd-Services.html, consultado el 20 de Noviembre de 2016.
- [38] <https://help.ubuntu.com/community/Taskel#Installation>, consultado el 20 de Noviembre de 2016.
- [39] <https://linux.die.net/man/1/mysql>, consultado el 20 de Noviembre de 2016.
- [40] <https://linux.die.net/man/1/patch>, consultado el 20 de Noviembre de 2016.

- [41] <https://linux.die.net/man/1/php>, consultado el 20 de Noviembre de 2016.
- [42] <https://linux.die.net/man/8/service>, consultado el 20 de Noviembre de 2016.
- [43] <https://mariadb.com/kb/en/mariadb/a-mariadb-primer-02-logging-in/>, consultado el 20 de Noviembre de 2016.
- [44] <https://mariadb.com/kb/en/mariadb/yum/>, consultado el 20 de Noviembre de 2016.
- [45] [https://technet.microsoft.com/es-es/library/dd197434\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/dd197434(v=ws.10).aspx), consultado el 20 de Noviembre de 2016.
- [46] <https://wiki.debian.org/es/tasksel>, consultado el 20 de Noviembre de 2016.
- [47] <https://wiki.debian.org/LaMp>, consultado el 20 de Noviembre de 2016.
- [48] <http://www.thegeekstuff.com/2014/12/patch-command-examples/>, consultado el 20 de Noviembre de 2016.
- [49] <http://php.net/manual/es/ini.core.php#ini.enable-post-data-reading>, consultado el 24 de Noviembre de 2016.
- [50] <https://docs.phpmyadmin.net/en/latest/config.html>, consultado el 24 de Noviembre de 2016.
- [51] <https://docs.phpmyadmin.net/en/latest/setup.html#linux-distributions>, consultado el 24 de Noviembre de 2016.
- [52] <http://webmin.com/tgz.html>, consultado el 24 de Noviembre de 2016.
- [53] <http://php.net/manual/es/features.commandline.usage.php>, consultado el 25 de Noviembre de 2016.
- [54] <http://php.net/manual/es/function.exec.php>, consultado el 25 de Noviembre de 2016.
- [55] https://access.redhat.com/documentation/en-US/Red_Hat_Network/5.0.0/html/Reference_Guide/s2-mon-rhnm-d-sshd.html, consultado el 25 de Noviembre de 2016.
- [56] <https://linux.die.net/man/1/grep>, consultado el 25 de Noviembre de 2016.
- [57] <https://linux.die.net/man/1/ps>, consultado el 25 de Noviembre de 2016.
- [58] <https://linux.die.net/man/1/scp>, consultado el 25 de Noviembre de 2016.
- [59] <https://linux.die.net/man/1/sed>, consultado el 25 de Noviembre de 2016.
- [60] <http://codehero.co/como-instalar-y-usar-fail2ban/>, consultado el 3 de Febrero de 2017.

- [61] <http://rkhunter.sourceforge.net/>, consultado el 3 de Febrero de 2017.
- [62] https://sourceforge.net/projects/rkhunter/?source=typ_redirect, consultado el 3 de Febrero de 2017.
- [63] http://www.fail2ban.org/wiki/index.php/Main_Page, consultado el 3 de Febrero de 2017.
- [64] <https://linux.die.net/man/1/ssh>, consultado el 3 de Noviembre de 2016.