

Administración de Sistemas Operativos 13/14.

Elías González

Joel Chávez

Administración de Sistemas Operativos 13/14.

Elías González

Joel Chávez

fecha de publicación 19/11/2013

Este documento está construcción. Se irá agregando temario a medida que avance el curso.

Tabla de contenidos

1. A3 SSH	1
0. Introducción.	1
1. Preparativos.	2
Configuracion del Servidor SSH XUbuntu	2
Clientes.	3
2. Instalación Básica	9
3. Personalización del prompt Bash.	12
4. Autenticación mediante claves públicas	13
5. Uso de SSH como túnel para X	14
6. Aplicaciones Windows nativas	14
.....	18
7. Restricciones de uso	18

Lista de figuras

1.1. Usuarios.	2
1.2. IPs Servidor.	3
1.3. Nombre equipo.	3
1.4. IP OpenSuse	4
1.5. Host, dominio	5
1.6. Dns	6
1.7. Putty instalado	7
1.8. IP Win7	8
1.9. Archivo Hosts	8
1.10. Instalar SSH.	9
1.11. Iniciar ssh.	9
1.12. Primera coexion ssh.	10
1.13. Conectado con Putty.	10
1.14. Generar Nuevas Claves.	11
1.15. Reiniciar SSH.	11
1.16. Reconectar con SSH.	12
1.17. Fichero .bashrc.	12
1.18. Ejecutar ssh y ver color del bash	13
1.19. Autenticación	13
1.20. Autenticación	14
1.21. Autenticación	14
1.22. Wine	14
1.23. App con Wine	15
1.24. Probar Wine en server	16
1.25. Probar Wine en cliente	16
1.26. Ccleaner ssh wine	17
1.27. Duda: rm -fr desde cliente en el servidor?	18
1.28. Restricción 7.2	18
1.29. Restricción 7.2	19
1.30. Restricción 7.3	19
1.31. Restricción 7.3	20
1.32. Restricción 7.3	20
1.33. Restricción 7.3	20
1.34. Restricción 7.4	21
1.35. Restricción 7.4	21
1.36. Restricción 7.4	21
1.37. Restricción 7.4	21
1.38. Restricción 7.4	22
1.39. Restricción 7.4	22

Capítulo 1. A3 SSH

Esta práctica constará de los siguientes apartados:

- 0. Introducción.
- 1. Preparativos.
- 2. Instalación básica.
- 3. Personalización del prompt Bash
- 4. Autenticación mediante claves públicas
- 5. Uso de SSH como túnel para X
- 6. Aplicaciones Windows nativas
- 7. Restricciones de uso
- 8. Resumen

0. Introducción.

Para realizar esta práctica vamos a realizar dos esquemas iguales, servidor SSH en XUbuntu con dos clientes (Windows 7 y OpenSuse):

- S1. Servidor SSH XUbuntu.
- C1. OpenSuse.
- C2. Windows 7.

1. Preparativos.

Configuración del Servidor SSH XUbuntu

IP, HOST, Nombres de equipo, usuarios.

Figura 1.1. Usuarios.

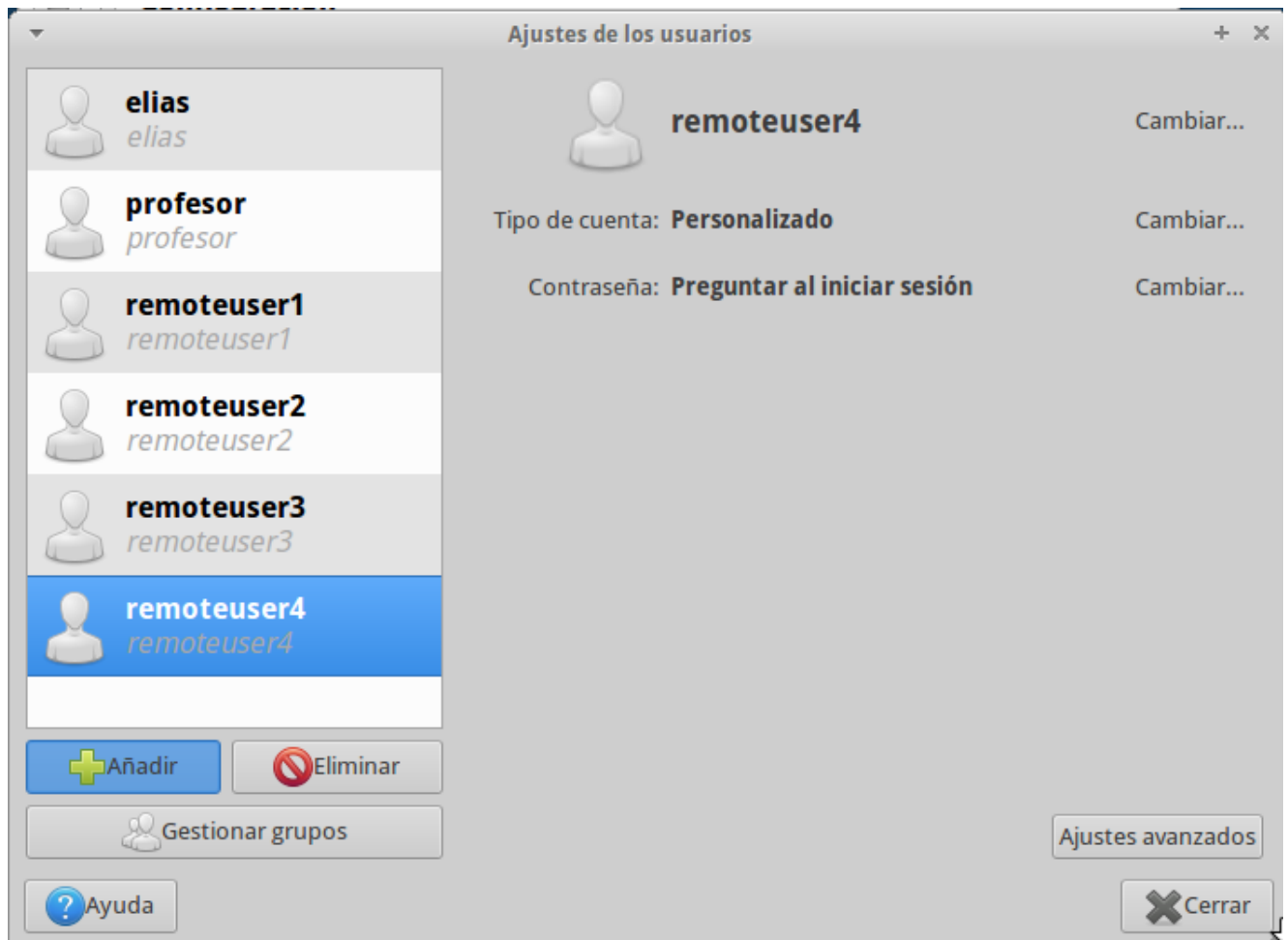


Figura 1.2. IPs Servidor.

```

elias@profesor-VirtualBox:~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:aa:a0:15
          Direc. inet:172.16.109.10  Difus.:172.16.255.255  Másc:255.255.0.0
          Dirección inet6: fe80::a00:27ff:feaa:a015/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:940 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:803 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:701711 (701.7 KB)  TX bytes:95875 (95.8 KB)

eth1      Link encap:Ethernet  direcciónHW 08:00:27:ec:c6:61
          Direc. inet:192.168.1.10  Difus.:192.168.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:feec:c661/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:148 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B)  TX bytes:29257 (29.2 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:256 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:256 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:26945 (26.9 KB)  TX bytes:26945 (26.9 KB)

```

Figura 1.3. Nombre equipo.

```

GNU nano 2.2.6      Archivo: /etc/hosts
127.0.0.1      localhost
127.0.1.1      ssh-server.gonzalez      ssh-server
172.16.109.110 cliente1.suse      ssh-client1
172.16.109.210 cliente2.w7      ssh-client2
172.16.109.11 servidor.joel      sjoel
172.16.109.111 cliente1joel      c1joel
172.16.109.211 cliente2joel      c2joel

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

```

Clientes.

Client1 será OpenSuse y el Client2 Windows 7

Opensuse.

Instalación.

Utilizamos una OVA en la que ya está instalado.

IP, HOST, Nombres de equipo, usuarios.

Figura 1.4. IP OpenSuse

The screenshot shows the 'YaST2 - Ajustes de red' window. The 'Configuración de tarjeta de red' section is active, with the 'Dirección' tab selected. The 'Tipo de Dispositivo' is set to 'Ethernet' and the 'Nombre de Configuración' is 'eth0'. The 'Dirección IP estática asignada' option is selected. The IP address is '172.16.109.111', the subnet mask is '/16', and the host name is 'pc11.aula109'. There are buttons for 'Añadir', 'Editar', and 'Eliminar' for additional IP addresses. At the bottom, there are buttons for 'Ayuda', 'Cancelar', 'Atrás', and 'Siguiente'.

YaST2 - Ajustes de red

Configuración de tarjeta de red

General Dirección Hardware

Tipo de Dispositivo: Ethernet

Nombre de Configuración: eth0

☐ No están Configurados el enlace y la IP(Eslavos asociados) ☐ Use los valores iBFT

☐ Dirección Dinámica: DHCP DHCP versiones 4 y 6(ambas)

☒ Dirección IP estática asignada

Dirección IP: 172.16.109.111 Máscara de Subred: /16 Nombre de host: pc11.aula109

Direcciones Adicionales

Alias	Dirección IP	Máscara de red
-------	--------------	----------------

Añadir Editar Eliminar

Ayuda Cancelar Atrás Siguiente

Figura 1.5. Host, dominio

YaST2 - Ajustes de red

Configuración de Red

Opciones Globales Vista resumen **Nombre de Host/DNS** Encaminamiento

Nombre de Host y Nombre de Dominio

Nombre de <u>h</u> ost	Nombre de <u>D</u> ominio
<input type="text" value="ssh-client"/>	<input type="text" value="chavez"/>

☐ Modificar Nombre de Host mediante DHCP Ningún interfaz con dhcp

☐ Asignar nombre de host a la IP de bucle local

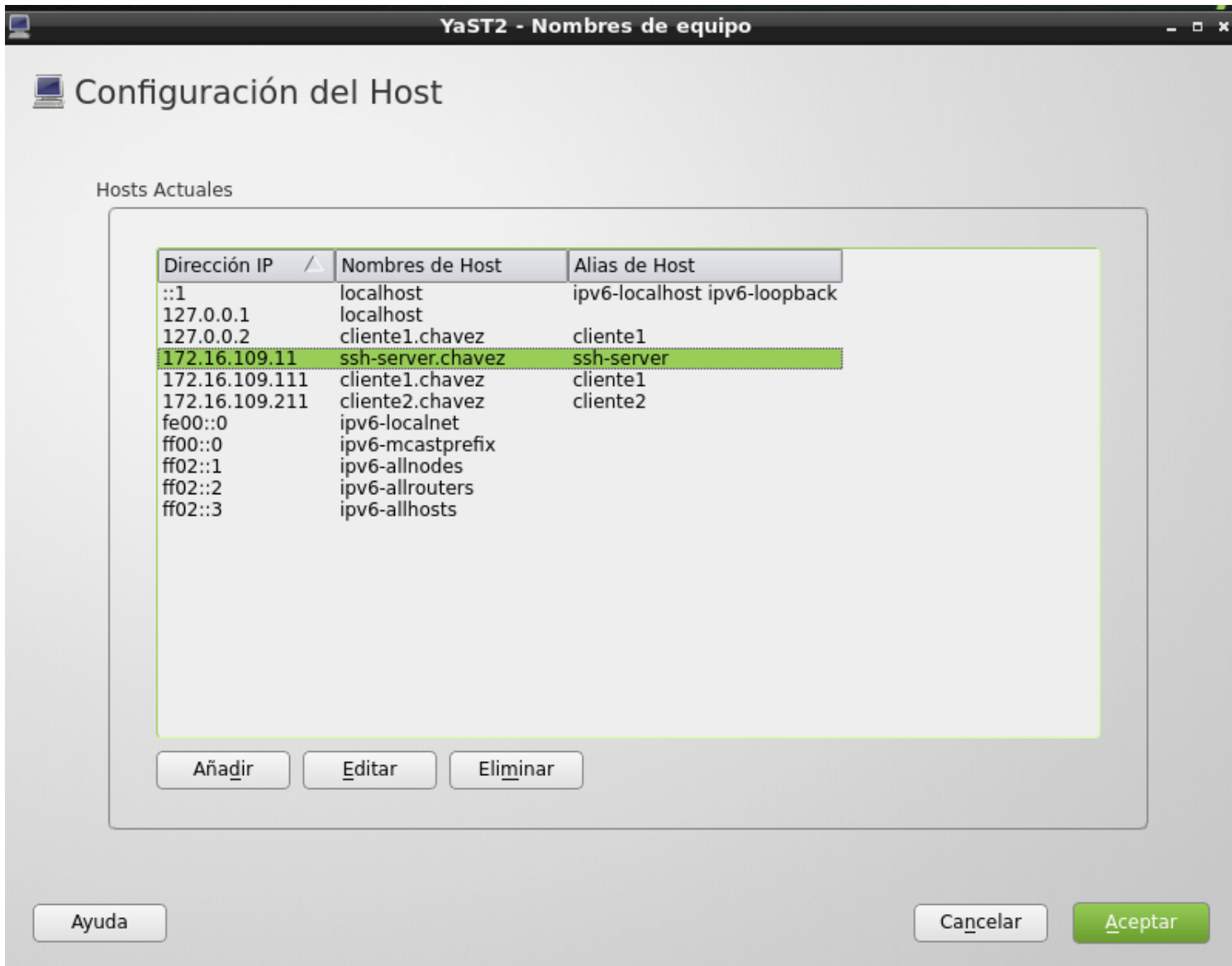
Modificar la configuración del DNS Reglas Personalizadas

Usar Valores Predeterminados

Servidores de Nombres y Lista de Búsqueda de Dominios

Servidor de Nombres <u>1</u>	Búsqueda de Dominio
<input type="text"/>	<input type="text" value="aula109"/>
Servidor de Nombres <u>2</u>	
<input type="text"/>	
Servidor de Nombres <u>3</u>	
<input type="text"/>	

Ayuda Cancelar **Aceptar**

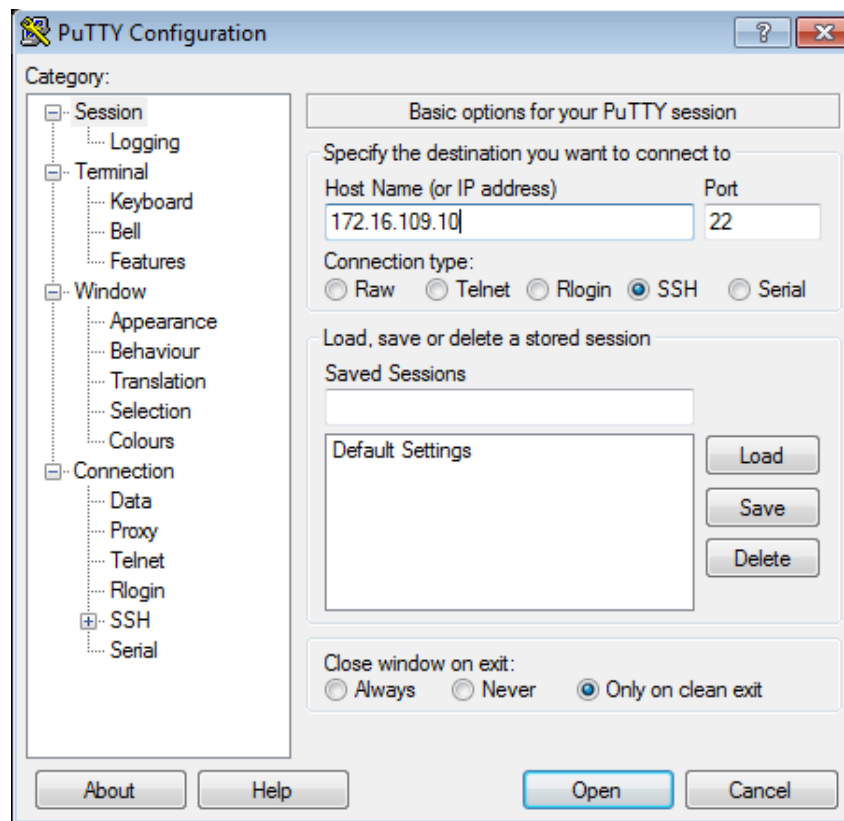
Figura 1.6. Dns

Windows 7

Tendremos que instalar un software para poder utilizar ssh, y modificaremos el archivo C:\Windows\System32\drivers\etc\hosts

Instalación.

Instalaremos el PuTTY

Figura 1.7. Putty instalado

IP, HOST.

Figura 1.8. IP Win7

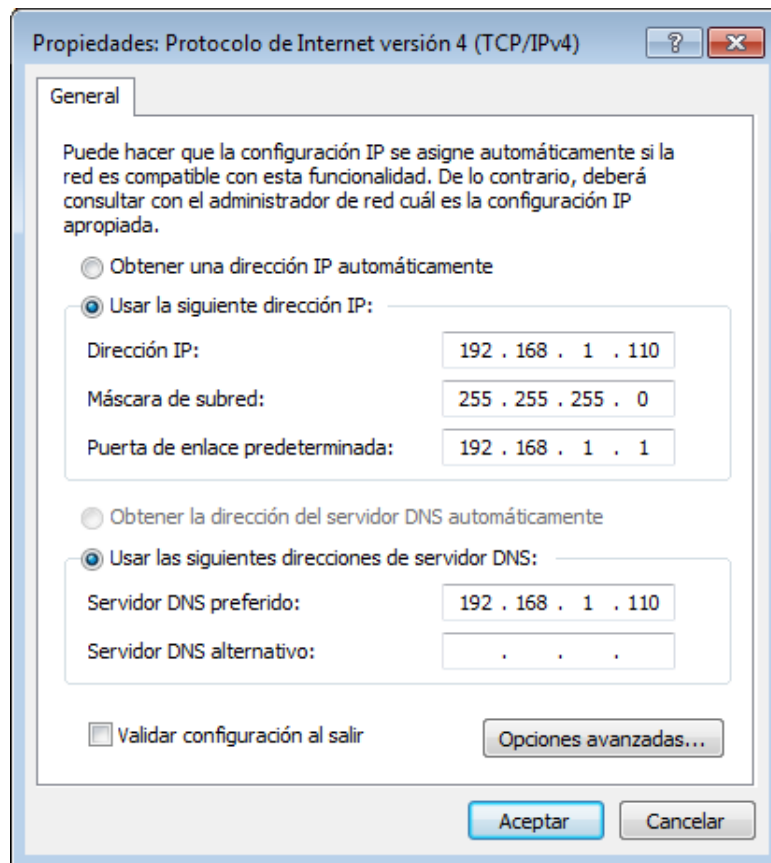
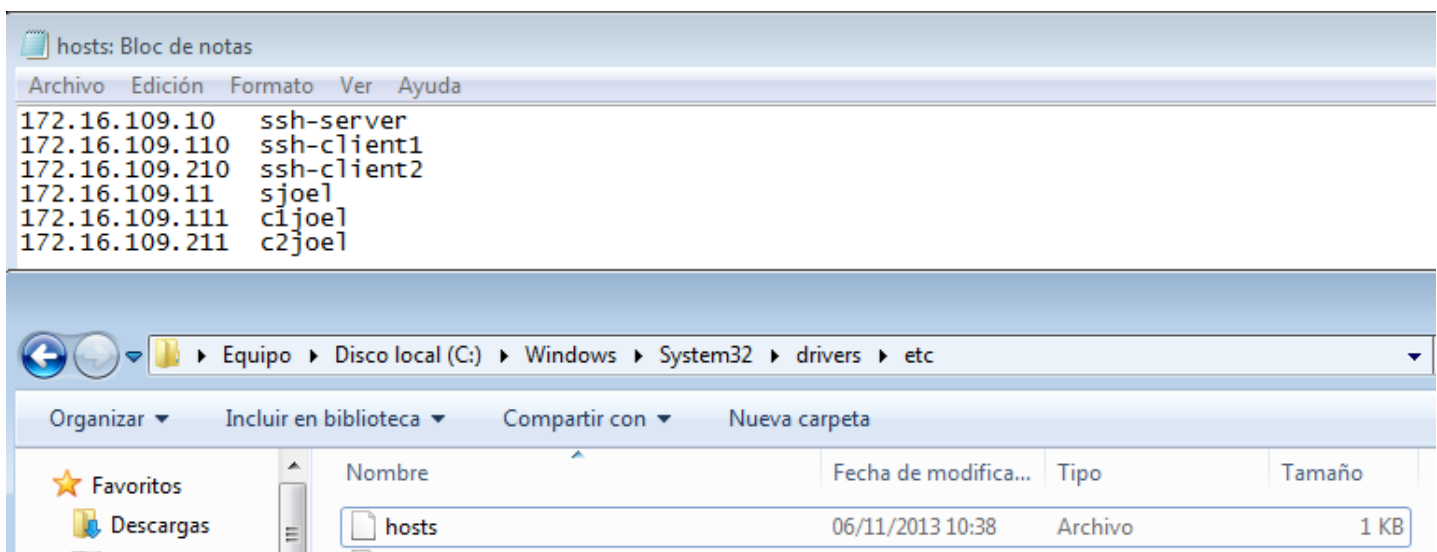


Figura 1.9. Archivo Hosts



2. Instalación Básica

2. Instalación Básica

Instalamos el openssh-server:

Figura 1.10. Instalar SSH.

```
root@profesor-VirtualBox:/home/elias# apt-get install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  ncurses-term python-requests python-urllib3 ssh-import-id
Paquetes sugeridos:
  ssh-askpass rssh molly-guard monkeysphere openssh-blacklist openssh-blacklist-extra
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server python-requests python-urllib3 ssh-import-id
0 actualizados, 5 se instalarán, 0 para eliminar y 150 no actualizados.
Necesito descargar 847 kB de archivos.
Se utilizarán 3.450 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? S
```

Iniciamos el servicio ssh:

Figura 1.11. Iniciar ssh.

```
root@profesor-VirtualBox:/home/elias# /etc/init.d/ssh start
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service ssh start

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the start(8) utility, e.g. start ssh
ssh start/running, process 2780
```

Nos conectamos desde Windows con PuTTY:

Figura 1.12. Primera coexion ssh.

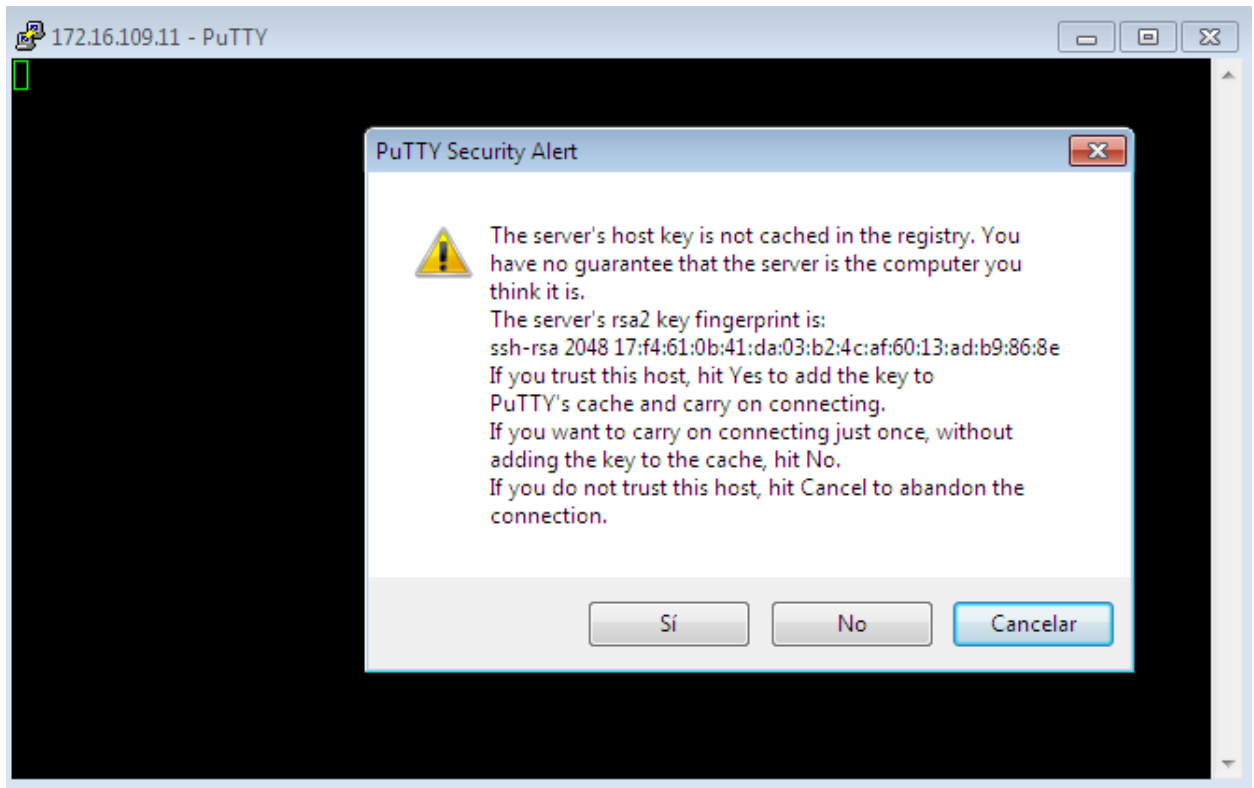
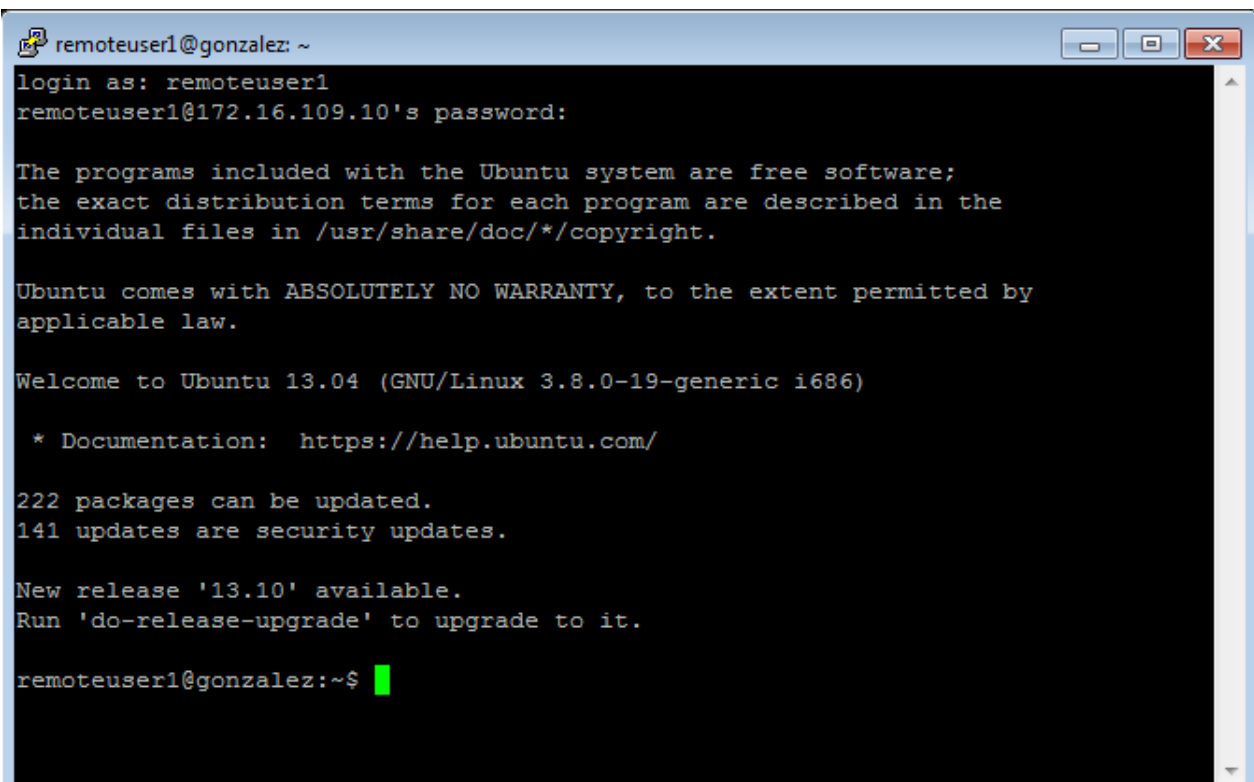


Figura 1.13. Conectado con Putty.



En Windows no encontramos el fichero known_hosts. Crearemos nuevas claves en el servidor con el comando ssh-keygen:

Figura 1.14. Generar Nuevas Claves.

```
root@profesor-VirtualBox:/home/elias# ssh-keygen
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:
a9:64:ff:db:77:8f:d1:27:81:c8:bc:b9:73:87:82:ad root@gonzalez
The key's randomart image is:
+--[ RSA 2048 ]-----+
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
+-----+
  
```

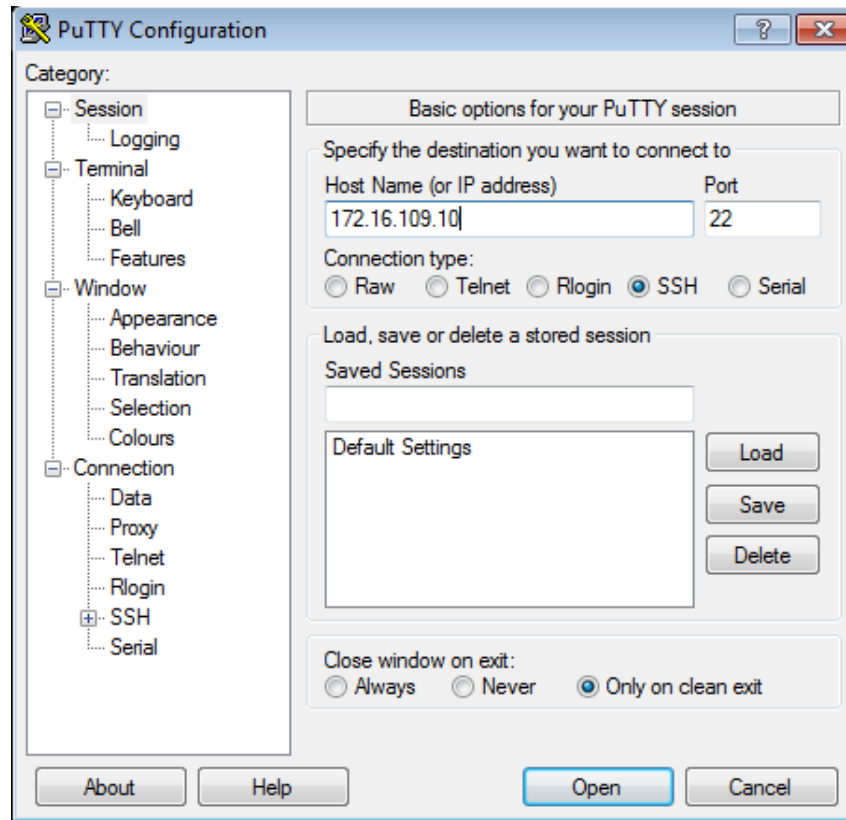
Reiniciamos el servicio:

Figura 1.15. Reiniciar SSH.

```
root@profesor-VirtualBox:/home/elias# /etc/init.d/ssh restart
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service ssh restart

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the stop(8) and then start(8) utilities,
e.g. stop ssh ; start ssh. The restart(8) utility is also available.
ssh stop/waiting
ssh start/running, process 3021
  
```

Volvemos a conectarnos desde los clientes, usando el usuario remoteuser2 y remoteuser1. ¿Qué sucede?:

Figura 1.16. Reconectar con SSH.

3. Personalización del prompt Bash.

En cada usuario hay que modificar el fichero `.bashrc` y agregar unas líneas al final:

Figura 1.17. Fichero `.bashrc`.

```

Terminal - root@profesor-VirtualBox: /home/remotouser1
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
GNU nano 2.2.6          Archivo: .bashrc

#PUNTO 3
#ELIAS Y JOEL
if [-n "$SSH_CLIENT" ]; then text=" ssh"
fi
export PS1='\[\e[0;31m\]\u@h: \w${text}$\[\e[m\]

# ~/.bashrc: executed by bash(1) for non-login shells.

```

Probamos:

Figura 1.18. Ejecutar ssh y ver color del bash

```

asir@pc10:~/proyectos/add1314-elias/actividades$ ssh -p 22 remoteuser1@172.16.109.10
The authenticity of host '172.16.109.10 (172.16.109.10)' can't be established.
ECDSA key fingerprint is ca:a0:d9:04:c7:19:bc:84:52:05:7c:da:9f:66:ba:2c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.109.10' (ECDSA) to the list of known hosts.
remoteuser1@172.16.109.10's password:
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)

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

222 packages can be updated.
141 updates are security updates.

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

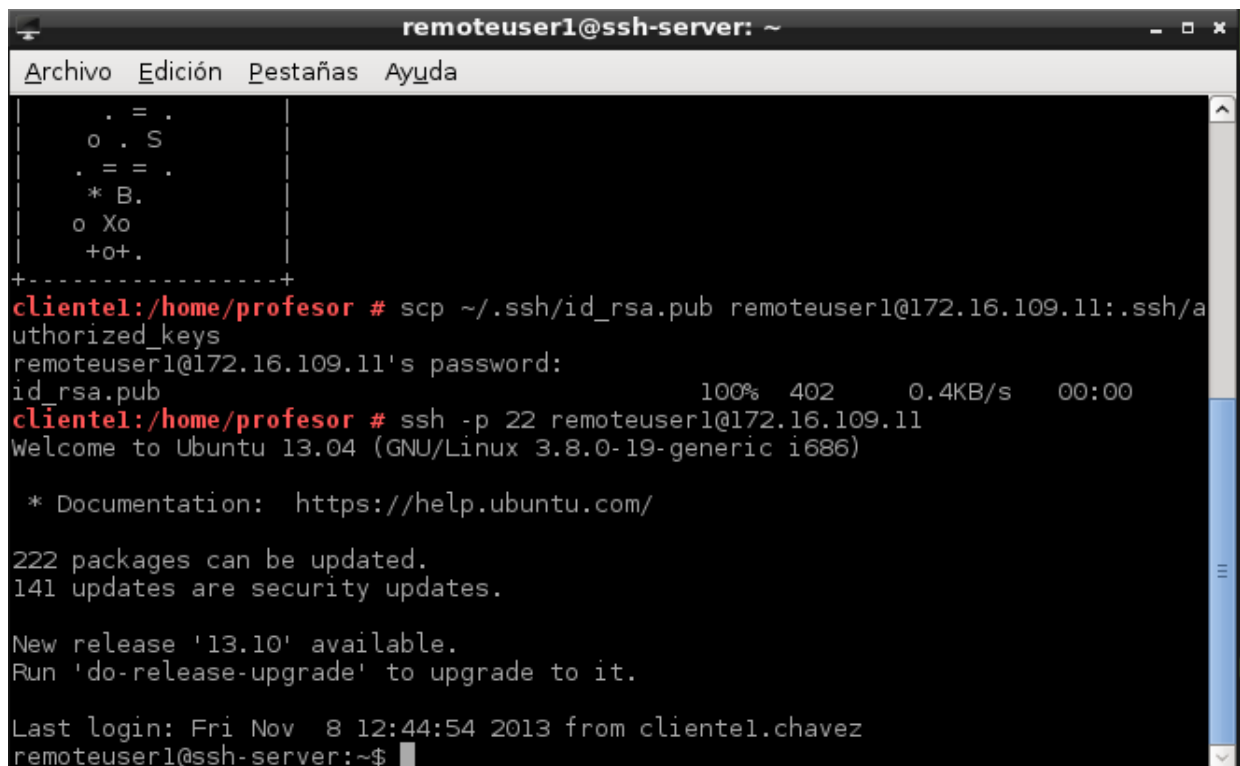
Last login: Wed Nov  6 11:40:08 2013 from cliente1.suse
-bash: /home/remoteuser1/.bashrc: línea 4: error sintáctico cerca del elemento inesperado `fi'

```

Nos ha dado un fallo, lo revisaremos mas adelante.

4. Autenticación mediante claves públicas

Proceso:

Figura 1.19. Autenticación


```

remoteuser1@ssh-server: ~
Archivo  Edición  Pestañas  Ayuda
+-----+
| . = . |
| o . S |
| . = = . |
| * B. |
| o Xo |
| +o+. |
+-----+
cliente1:/home/profesor # scp ~/.ssh/id_rsa.pub remoteuser1@172.16.109.11:~/.ssh/authorized_keys
remoteuser1@172.16.109.11's password:
id_rsa.pub                                100% 402      0.4KB/s   00:00
cliente1:/home/profesor # ssh -p 22 remoteuser1@172.16.109.11
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)

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

222 packages can be updated.
141 updates are security updates.

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Nov  8 12:44:54 2013 from cliente1.chavez
remoteuser1@ssh-server:~$

```

Figura 1.20. Autenticación

```

cliente1:/home/profesor # ssh -p 22 remoteuser1@172.16.109.11
remoteuser1@172.16.109.11's password:
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)

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

222 packages can be updated.
141 updates are security updates.

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov  6 11:37:28 2013 from cliente2.chavez
remoteuser1@ssh-server:~$ █

```

5. Uso de SSH como túnel para X

Proceso:

Figura 1.21. Autenticación

```

cliente1:/home/profesor # ssh -X remoteuser1@172.16.109.11
Warning: No xauth data; using fake authentication data for X11 forwarding.
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)

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

222 packages can be updated.
141 updates are security updates.

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Nov  8 13:10:12 2013 from cliente1.chavez
remoteuser1@ssh-server:~$ geany

```

"ssh -X remoteuser1@ssh-server; geany" no ha ido.

6. Aplicaciones Windows nativas

Instalamos Wine

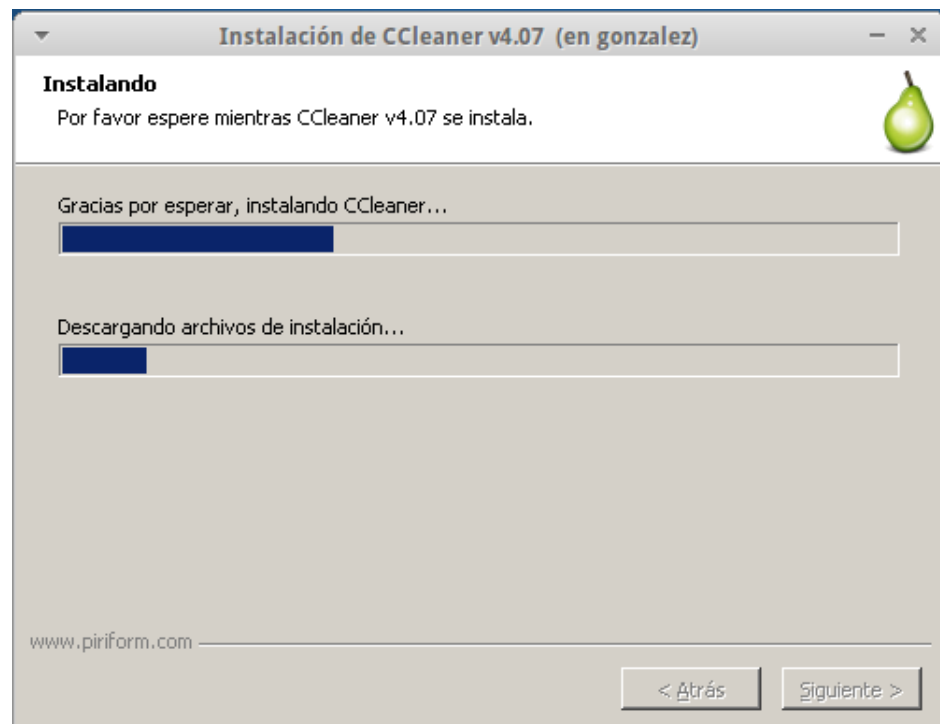
Figura 1.22. Wine

```

root@gonzalez:/home/elias# apt-get install wine
Levendo lista de paquetes... Hecho

```

Instalar aplicación (APP2) de Windows en el servidor SSH usando el emulador Wine. Elegimos el CCleaner porque seguramente al instalar el Wine nos creará una "instalación virtual de windows" con sus registros y archivos temporales que podremos limpiar con el Ccleaner.

Figura 1.23. App con Wine

Comprobar el funcionamiento de APP2 en ssh-server..

Figura 1.26. Ccleaner ssh wine

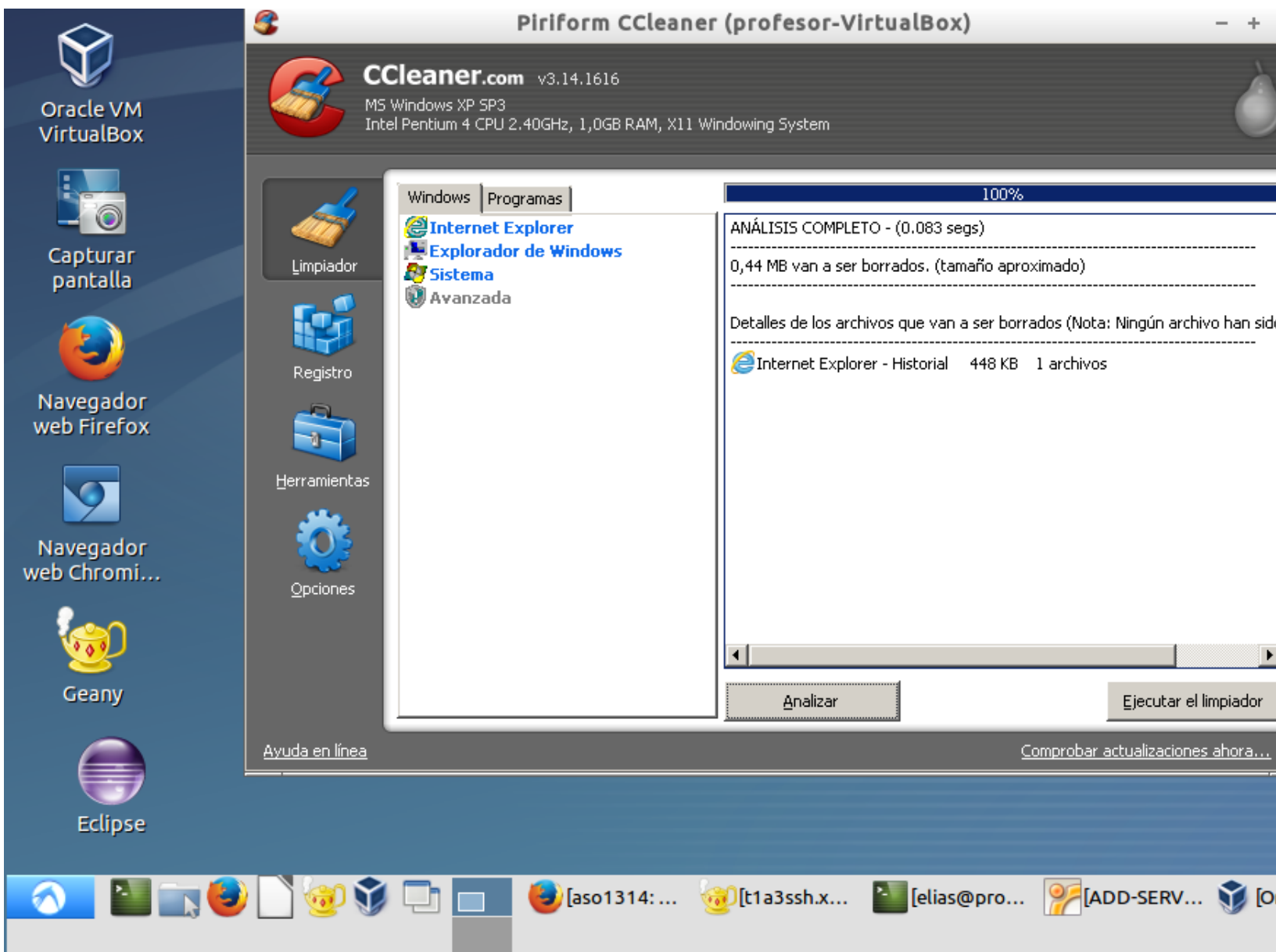
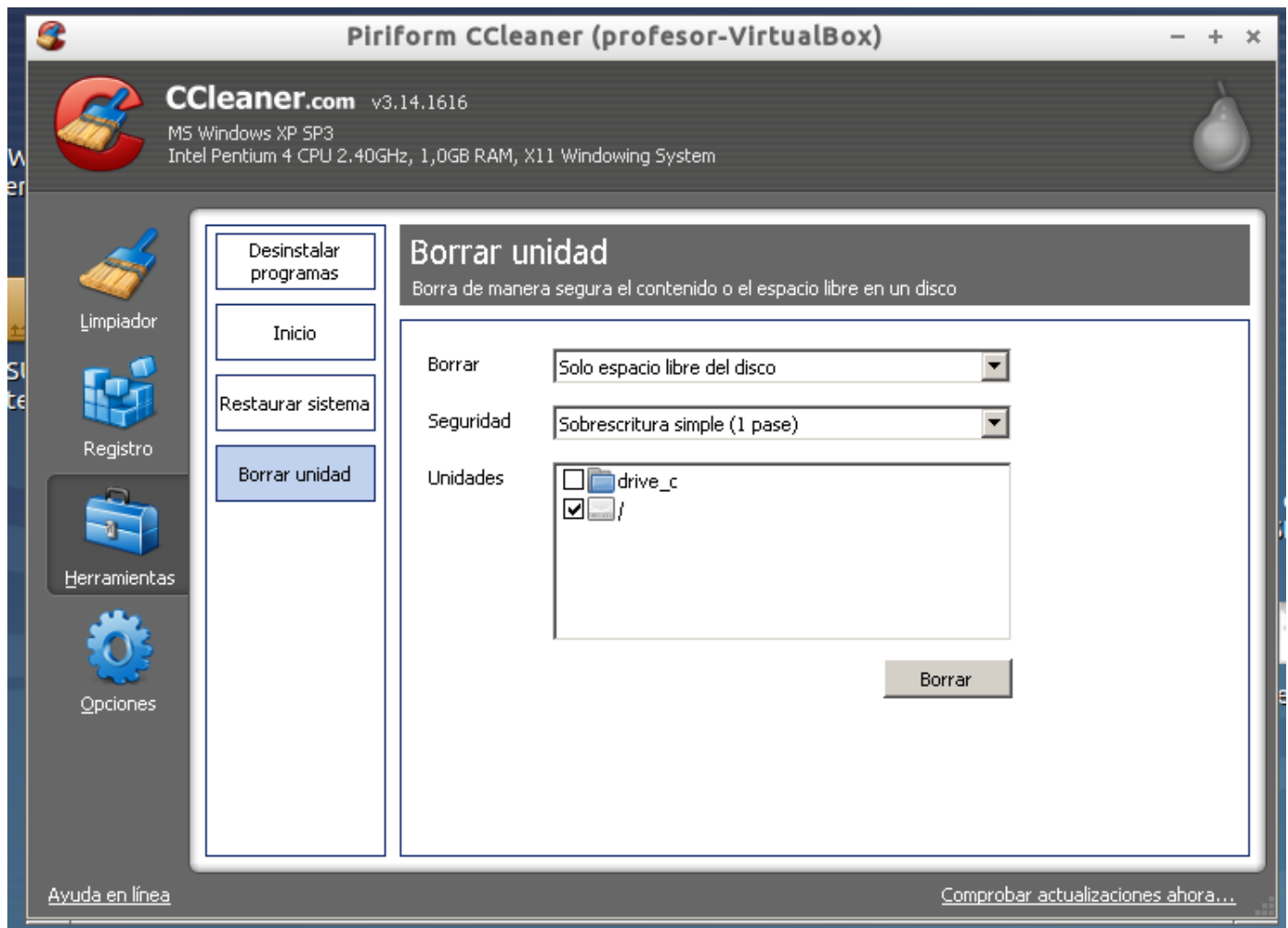


Figura 1.27. Duda: rm -fr desde cliente en el servidor?

7. Restricciones de uso

Vamos a modificar los usuarios del servidor SSH para añadir algunas restricciones de uso del servicio.

7.1 Sin restricción (tipo 1)

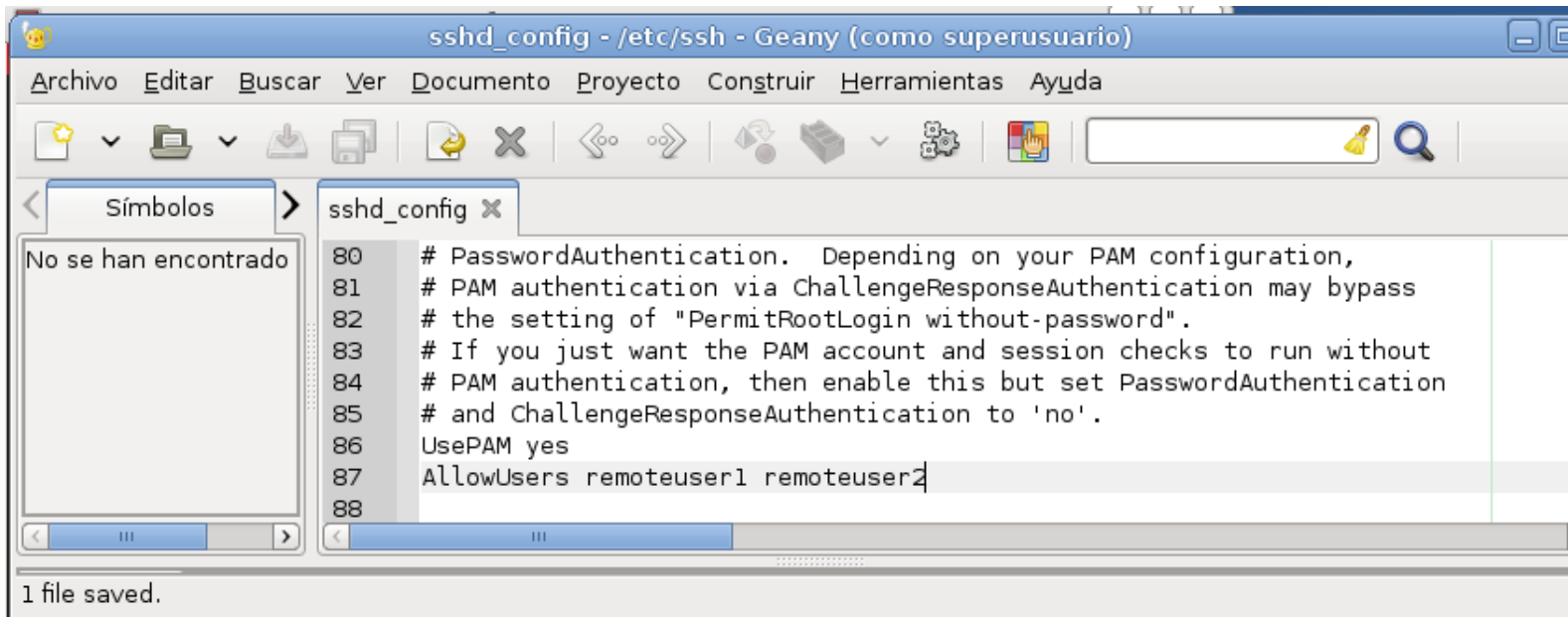
Usuario sin restricciones, el usuario `remoteuser1`, podrá conectarse vía SSH sin restricciones.

Figura 1.28. Restricción 7.2

```
cliente1:/home/profesor # ssh -p 22 ssh-server@172.16.109.11
The authenticity of host '172.16.109.11 (172.16.109.11)' can't be established.
ECDSA key fingerprint is f1:64:88:39:e9:68:cb:85:83:a2:90:a0:df:ed:81:18.
Are you sure you want to continue connecting (yes/no)? █
```

7.2 Restricción total (tipo 2)

Modificamos el archivo `/etc/ssh/sshd_config` añadiendo la denegación, para ello añadiremos una línea al final `"AllowUsers remoteuser1 remoteuser2"` esos serían los permitidos.

Figura 1.29. Restricción 7.2

7.3 Restricción temporal (tipo 3)

Crearemos un script que "bloquee" a los usuarios, irá en `/usr/local/bin/` pero lo lanzaremos manualmente, cuando se lanza la orden de bloquear se modificara el archivo `sshd_config.system` quitando los usuarios que no queremos, y cuando se lanza la orden de permitir se añadirán los usuarios al fichero. (o sustuiremos el fichero completo teniendo dos para cada caso.

Figura 1.30. Restricción 7.3

```
#!/usr/bin/ruby

param=ARGV.first
puts "Ejecutando <#{ $0 }>..."

def show_help
  puts "Forma de uso:"
  puts "** --lock , activar las restricciones SSH"
  puts "** --free , desactivar las restricciones SSH"
end

if param=='--lock' then
  system("sed -e 's/AllowUsers.*/AllowUsers remoteuser1/g' /etc/ssh/sshd_config.tmp > /etc/ssh/sshd_config")
  #system("cp sshd_config.system sshd_config")
  system('service ssh reload')
elsif param=='--free' then
  system("sed -e 's/AllowUsers.*/AllowUsers remoteuser1 remoteuser2 remoteuser3 remoteuser4/g' /etc/ssh/sshd_config.tmp > /etc/ssh/sshd_config")
  #system("cp sshd_config.system sshd_config")
  system('service ssh reload')
else
  show_help
end
```

Figura 1.31. Restricción 7.3

```
AllowUsers remoteuser1  
root@ssh-server:/usr/local/bin# limit-ssh-users.rb --free
```

Figura 1.32. Restricción 7.3

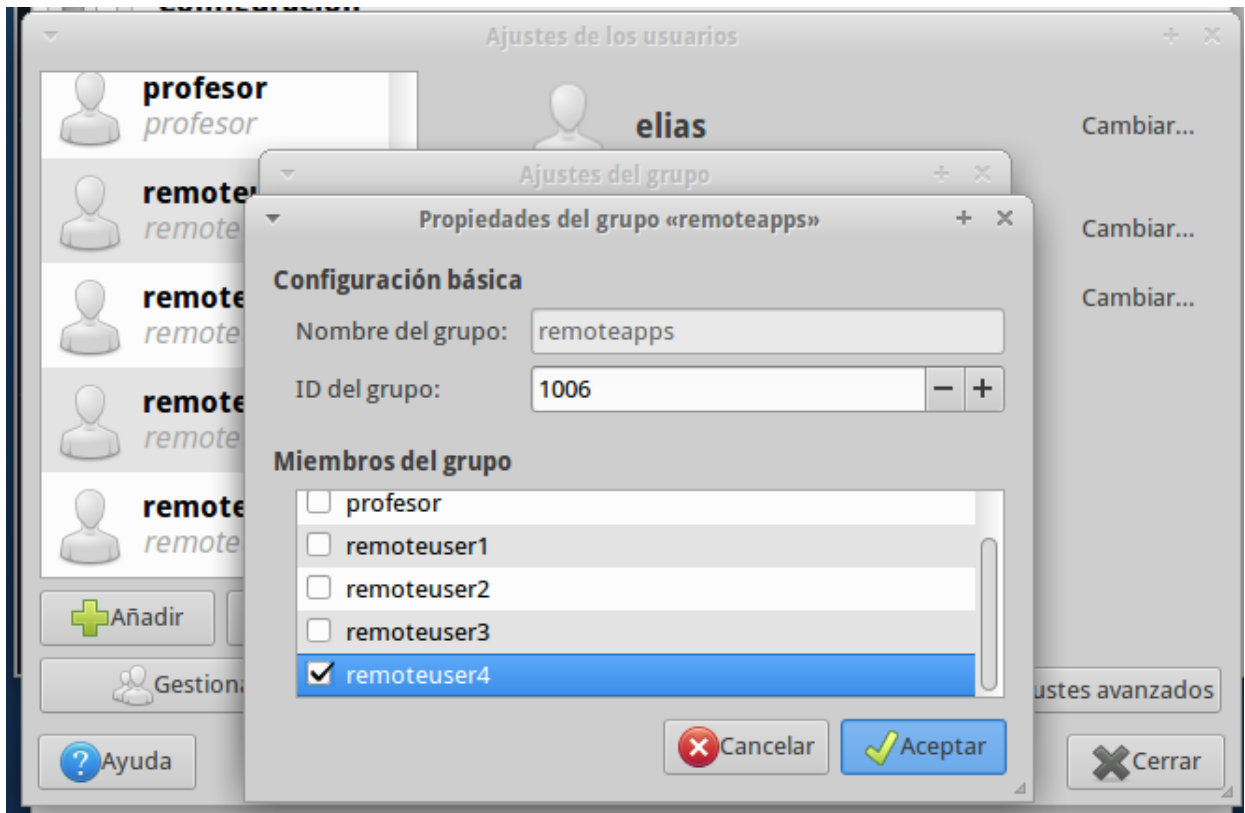
```
# and ChallengeResponseAuthentication to 'no'.  
UsePAM yes  
AllowUsers remoteuser1 remoteuser2 remoteuser3 remoteuser4
```

Figura 1.33. Restricción 7.3

```
cliente1:/home/profesor # ssh -p 22 remoteuser3@172.16.109.11  
remoteuser3@172.16.109.11's password:  
Permission denied, please try again.  
remoteuser3@172.16.109.11's password:  
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)  
  
* Documentation:  https://help.ubuntu.com/  
  
New release '13.10' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Fri Nov 15 13:11:13 2013 from cliente1.chavez  
remoteuser3@ssh-server:~$ ^C  
remoteuser3@ssh-server:~$ exit  
logout  
Connection to 172.16.109.11 closed.  
cliente1:/home/profesor # ssh -p 22 remoteuser3@172.16.109.11  
remoteuser3@172.16.109.11's password:  
Permission denied, please try again.  
remoteuser3@172.16.109.11's password:  
Permission denied, please try again.  
remoteuser3@172.16.109.11's password: █
```

7.4 Restricción sobre aplicaciones (tipo 4)

Vamos a crear una restricción de permisos sobre determinadas aplicaciones. Crear grupo remoteapps (hemos copiado el programa "cat" y le dimos nombre "cat2"):

Figura 1.34. Restricción 7.4

Poner al programa APP1 el grupo propietario a remoteapps:

Figura 1.35. Restricción 7.4

```
root@profesor-VirtualBox:/bin# chown remoteuser4.remoteapps cat2
```

Poner los permisos del ejecutable de APP1 a 750. Para impedir que los que no pertenezcan al grupo puedan ejecutar el programa.

Figura 1.36. Restricción 7.4

```
root@profesor-VirtualBox:/bin# chmod 750 cat2
```

Comprobamos desde servidor con elias y con remoteuser4:

Figura 1.37. Restricción 7.4

```
root@profesor-VirtualBox:/bin# su elias
elias@profesor-VirtualBox:/bin$ cat2 /etc/network/interfaces
bash: /bin/cat2: Permiso denegado
```

Comprobamos desde un cliente:

Figura 1.38. Restricción 7.4

```
remoteuser4@profesor-VirtualBox:~$ cat2 /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
```

Figura 1.39. Restricción 7.4

```
elias@profesor-VirtualBox:~$ cat2 /etc/network/interfaces
-bash: /bin/cat2: Permiso denegado
elias@profesor-VirtualBox:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
```