



# SSH

C.E.S ACADEMIA LOPE DE VEGA

CFGs: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: SERVICIOS EN RED E INTERNET

Prof. Álvaro Márquez

Autor: Rafael Osuna Ventura

## Ejercicio 1.

Instala el servidor y el cliente SSH en Linux y:

```
rafa@rafa-VirtualBox:~$ sudo apt-get install ssh
[sudo] password for rafa:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-server openssh-sftp-server ssh-import-id
Suggested packages:
  ssh-askpass libpam-ssh keychain monkeysphere rssh molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 5 newly installed, 0 to remove and 372 not upgraded.
Need to get 687 kB/1.340 kB of archives.
After this operation, 5.414 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Comprueba que puedes abrir una sesión SSH a invitado@localhost:

```
root@rafa-VirtualBox:/home/rafa# ssh invitado@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Y7YU66X77oVp3B1C760Ngqy0xTASclRKkuxJ0foVJf4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
invitado@localhost's password:
```

Comprueba que algún compañero se puede conectar y abrir una sesión de tu máquina con ssh:

```
root@usuario-VirtualBox:/home/usuario# ssh rafa@192.168.0.104
The authenticity of host '192.168.0.104 (192.168.0.104)' can't be established.
ECDSA key fingerprint is 9b:25:4b:38:c6:3b:63:71:e5:f9:e8:47:46:da:52:74.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.104' (ECDSA) to the list of known hosts.
rafa@192.168.0.104's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.10.0-40-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

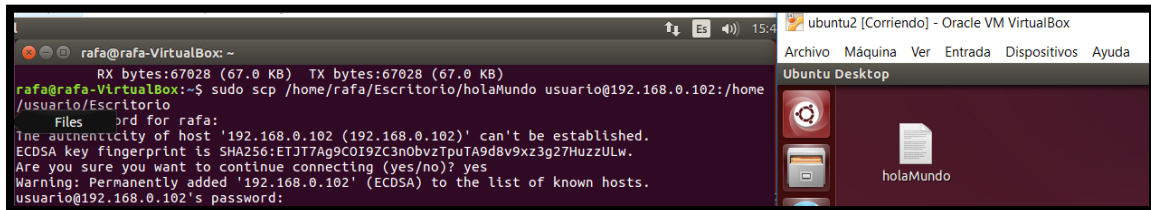
373 packages can be updated.
148 updates are security updates.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

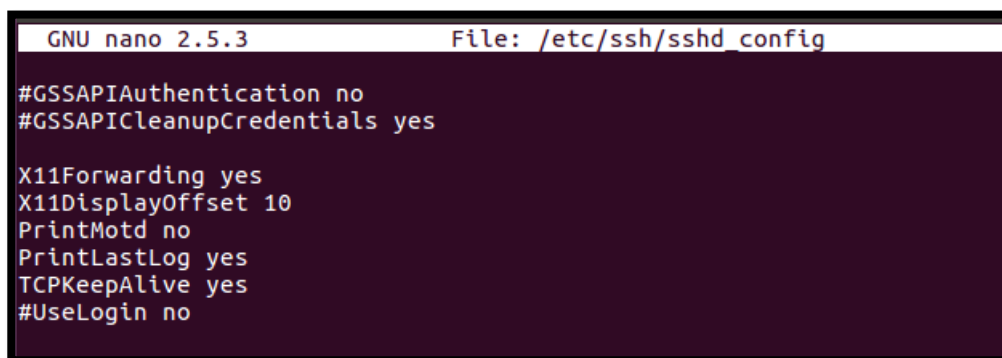
rafa@rafa-VirtualBox:~$
```

Haz la copia de algún pequeño archivo a través de scp hacia la máquina de algún compañero:



```
rafa@rafa-VirtualBox: ~  
RX bytes:67028 (67.0 KB) TX bytes:67028 (67.0 KB)  
rafa@rafa-VirtualBox:~$ sudo scp /home/rafa/Escritorio/holaMundo usuario@192.168.0.102:/home  
/usuario/Escritorio  
Files      ord for rafa:  
The authenticity of host '192.168.0.102 (192.168.0.102)' can't be established.  
ECDSA key fingerprint is SHA256:ETJT7Ag9COI9ZC3n0bvzTpuTA9d8v9xz3g27HuzzULw.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.0.102' (ECDSA) to the list of known hosts.  
usuario@192.168.0.102's password:
```

Habilita en la configuración de tu servidor le redirección X ( /etc/ssh/sshd\_config ) y comprueba que se pueden ejecutar aplicaciones gráficas ( por ejemplo gedit ) en una sesión remota de SSH:

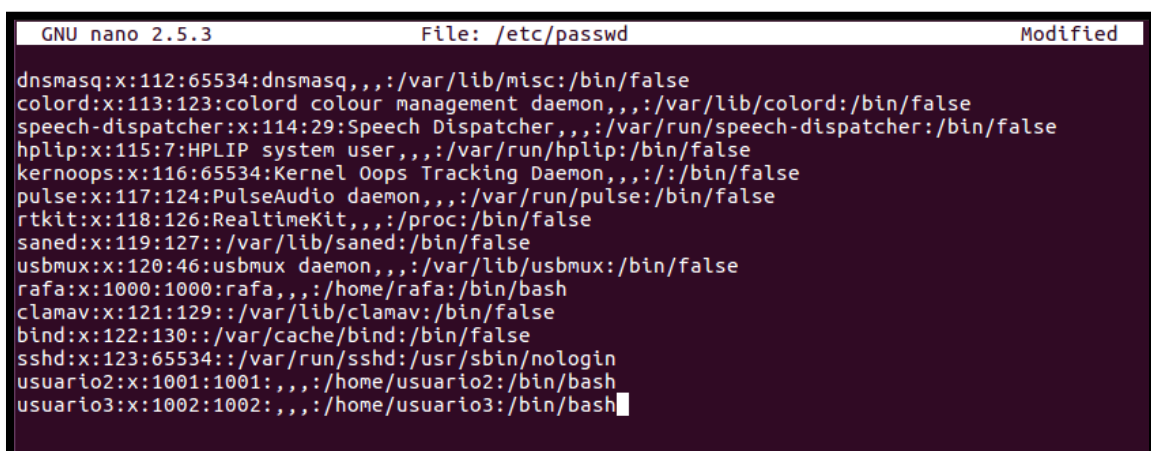


```
GNU nano 2.5.3      File: /etc/ssh/sshd config  
  
#GSSAPIAuthentication no  
#GSSAPICleanupCredentials yes  
  
X11Forwarding yes  
X11DisplayOffset 10  
PrintMotd no  
PrintLastLog yes  
TCPKeepAlive yes  
#UseLogin no
```

## Ejercicio 2.

Sobre el servidor anterior configura las siguientes opciones

1. Arrancar el servidor SSH en la máquina y comprobar que podemos acceder con cualquier usuario desde cualquier equipo.



```
GNU nano 2.5.3      File: /etc/passwd      Modified  
  
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false  
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false  
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false  
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false  
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false  
saned:x:119:127:/:/var/lib/saned:/bin/false  
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false  
rafa:x:1000:1000:rafa,,,:/home/rafa:/bin/bash  
clamav:x:121:129:/:/var/lib/clamav:/bin/false  
bind:x:122:130:/:/var/cache/bind:/bin/false  
sshd:x:123:65534:/:/var/run/ssh:/usr/sbin/nologin  
usuario2:x:1001:1001:/:/home/usuario2:/bin/bash  
usuario3:x:1002:1002:/:/home/usuario3:/bin/bash
```

2. Configurar el servicio SSH para que no admita hacer login como root. Como vemos en el lado izquierdo hemos habilitado para que el usuario root pueda entrar desde otra máquina diferente:

```
GNU nano 2.5.3 File: /etc/passwd Modified
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127:/:/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
rafa:x:1000:1000:rafa,,,:/home/rafa:/bin/bash
clamav:x:121:129:/:/var/lib/clamav:/bin/false
bind:x:122:130:/:/var/cache/bind:/bin/false
sshd:x:123:65534:/:/var/run/sshd:/usr/sbin/nologin
usuario2:x:1001:1001:,,,:/home/usuario2:/bin/bash
usuario3:x:1002:1002:,,,:/home/usuario3:/bin/bash
```

3. El servicio SSH por defecto escucha en el puerto 22. Modifícalo para que arranque en el puerto 10022 (u otro) y averigua cuál sería el comando utilizado para poder acceder al servidor.

```
GNU nano 2.5.3 File: /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 10022
```

4. Cambia los protocolos SSH en cliente y servidor y comprueba si se permite la conexión. Por ejemplo, que el cliente use solo la versión 1 del protocolo y el servidor la 2:

```
GNU nano 2.5.3 File: /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 10022
# Use these options to restrict which interfaces/protocols listen
#ListenAddress ::
#ListenAddress 0.0.0.0
#Protocol 2
# HostKeys for protocol version 2
```

5. Por defecto, al autenticarnos correctamente en el servidor SSH, éste nos muestra la fecha y hora de la última vez que nos conectamos. Encuentra la opción que se encarga de modificar este aspecto:

```
GNU nano 2.5.3 File: /etc/ssh/sshd_config

#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog no
TCPKeepAlive yes
#UseLogin no
```

6. Configura el servidor SSH para que solo permita la autenticación de los usuarios que nosotros indiquemos. 7. Configura el servidor SSH de forma adecuada para que acepte la redirección X11, de tal forma que se puedan ejecutar aplicaciones gráficas de forma remota. Haz pruebas y comprueba su funcionamiento.

```
GNU nano 2.5.3 File: /etc/ssh/sshd_config

#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

AllowUsers usuario02
X11Forwarding yes
X11DisplayOffset 10
```