|  |
| --- |
|  |
| Manual SSH |
|  |
|  |
| **Álvaro Delgado y Samuel Escudero** |
| **27/11/2015** |

|  |
| --- |
| Manual de SSH completado con las competencias aprendidas en el primer trimestre sobre el funcionamiento del protocolo SSH en el Teide IV. |

Índice

# Ubuntu

[Instalación de servidor SSH](#_Instalación_del_servidor). 2

[Configuración del servidor.](#_Configuración_del_servidor) 3

[Creación clave privada en el servidor](#_Creación_de_la). 4

[Primera conexión](#_Primera_conexión). 5

[Controlar conexiones al servidor](#_Controlar_las_conexiones). 6

[Autenticación con clave pública del cliente](#_Autenticación_con_clave). 7

[Ejecutar aplicaciones gráficas](#_Ejecutar_aplicaciones_gráficas). 9

[Transferencia de archivos sobre SSH](#_Transferencia_de_archivos). 10

[Crear túnel SSH](#_Crear_túnel_SSH). 11

# Windows

[Instalación del cliente SSH](#_Instalación_del_cliente). 12

[Primera conexión](#_Primera_conexión.). 13

[Borrado de las claves públicas de los diferentes servidores](#_Borrado_de_las). 14

[Crear clave privada](#_Autenticación_mediante_clave). 15

[Autenticación mediante clave privada](#_Autenticación_mediante_clave). 16

[Ejecutar aplicaciones gráficas](#_Ejecutar_aplicaciones_gráficas_1). 18

[Transferencia de archivos sobre SSH](#_Transferencia_de_archivos_1). 20

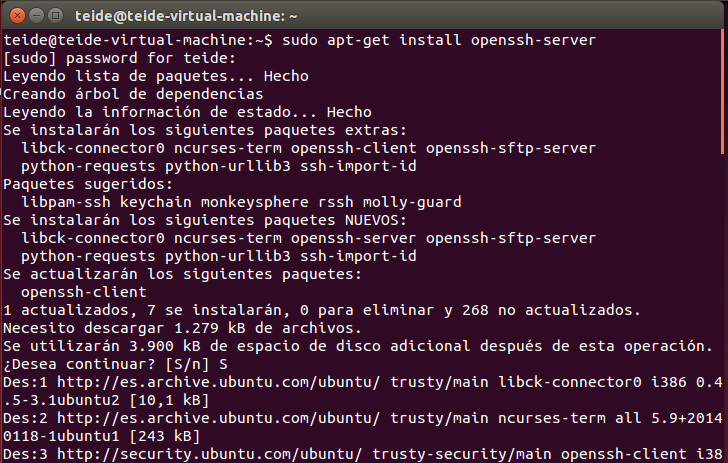
[Crear túnel SSH](#_Crear_túnel_ssh_1). 21

Ubuntu

# Instalación del servidor SSH

Para instalar el servidor SSH en Ubuntu deberemos ejecutar el comando:

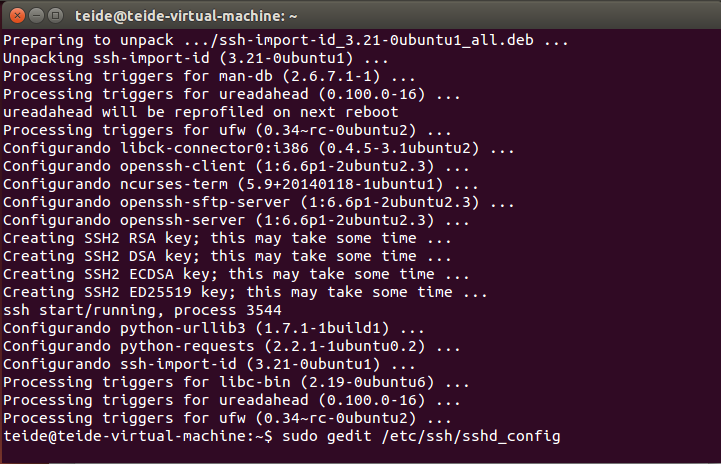
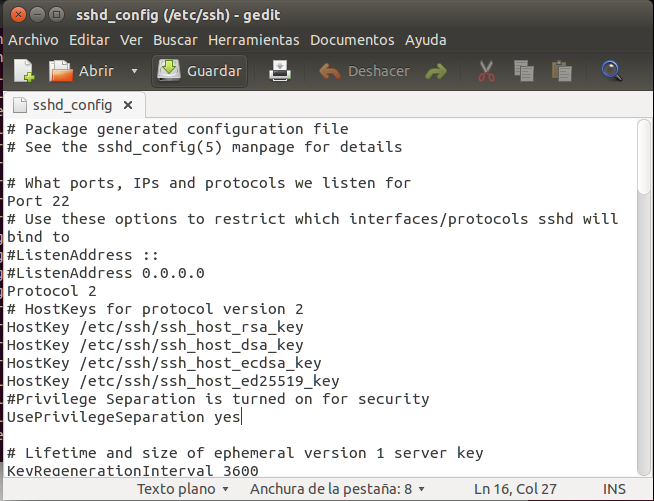
Sudo apt-get install open\_ssh-server



# Configuración del servidor

La configuración se almacena en el fichero sshd\_config, podemos modificarlo con el siguiente commando:

Sudo gedit /etc/ssh/sshd\_config

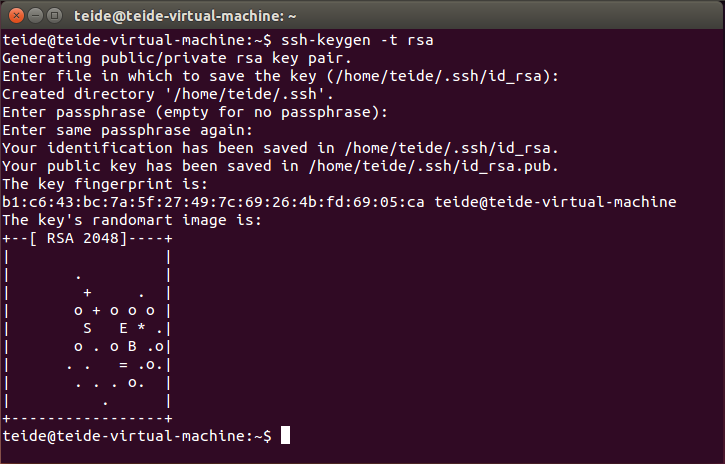
 

# Creación de la clave privada en el servidor

Para generar el par de clave utilizamos el comando:

sudo ssh-keygen -t rsa

Guardara las claves generadas en ~/.ssh/

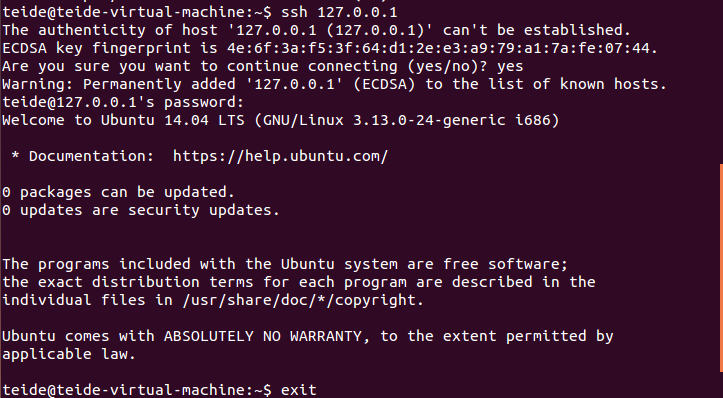


# Primera conexión

Para conectarnos con el cliente ejecutamos el comando:

ssh <ip> -l <usuario>

Nos pedirá la clave y la introducimos.



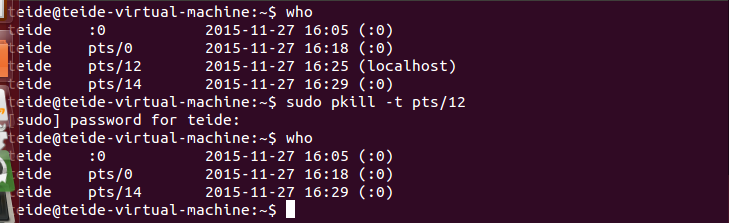
# Controlar las conexiones al servidor

Para ver que usuarios están conectados ejecutamos el comando:

Who

Las conexiones externas serían las pts diferentes de 0, en este caso pts/12 si queremos cerrar esa sesión ejecutamos:

Sudo pkill -t pts/12.



# Autenticación con clave pública del cliente.

Lo primero que debemos hacer es generar el par de claves en el cliente con el comando :

Sudo ssh-keygen -t rsa

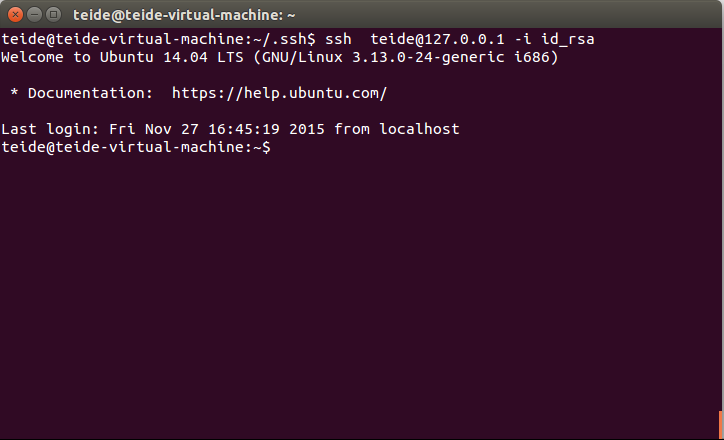
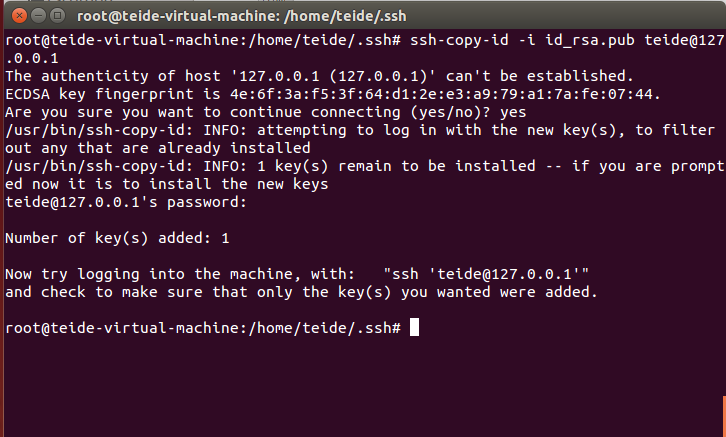
Una vez nos las ha creado las exportamos al servidor mediante el comando:

ssh-copy-ip <clave pública>@<ip\_servidor>

Otra opción es copiarla con un pen drive y copiar su contenido a ~/.ssh/autorithed keys.

Ahora realizamos la conexión:

ssh <usuario>@<servidor> -i <clave\_privada>

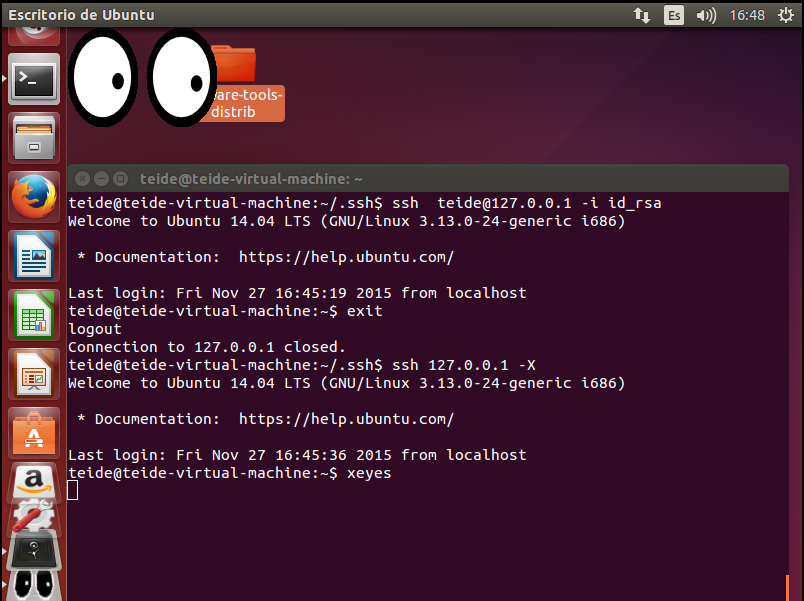


# Ejecutar aplicaciones gráficas

Podemos ejecutar aplicaciones gráficas al conectarnos por ssh usando la variable -X.

ssh <usuario>@<ip\_servidor> -X

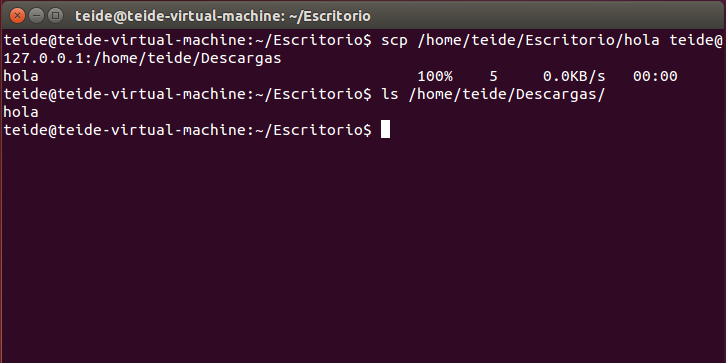
Ejecutamos xeyes



# Transferencia de archivos sobre SSH

Para copiar archivos entre el cliente y el servidor ejecutamos el comando scp:

scp <ruta\_fichero\_local> <usuario>@<ip\_servidor>:<ruta\_destino\_remoto>



# Crear túnel SSH

Podemos crear un túnel ssh mediante el comando:

ssh -L <puerto\_local>:<localhost>:<puerto\_remoto> <usuario>@<ip\_servidor>

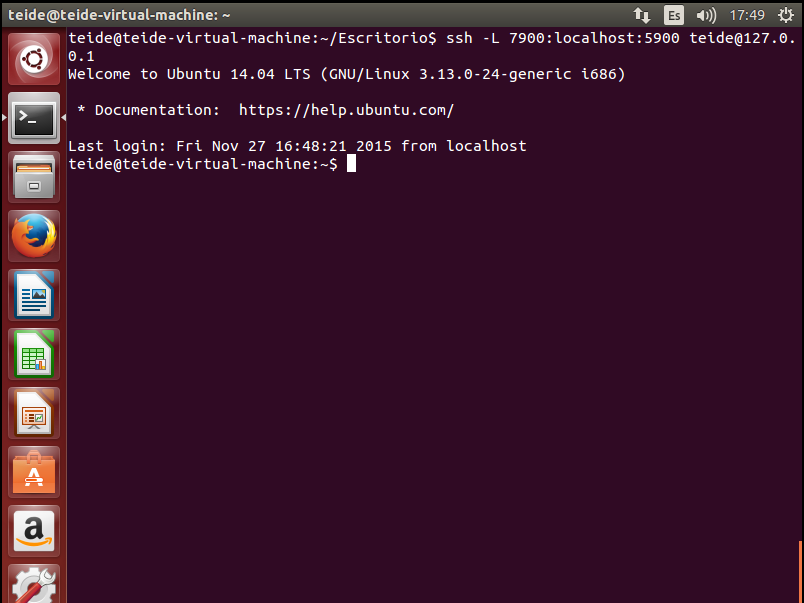
Para usarlo debemos redirigir el tráfico de la aplicación a nuestro puerto local:

Es un comando muy útil dado que nos permite cifrar el tráfico de un puerto ajeno a ssh.

Ejemplo:

ssh -L 7900:interno2:5900 usuario@interno1

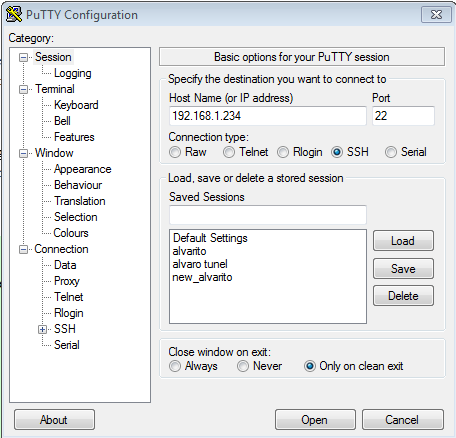
vncviewer localhost::7900



Windows

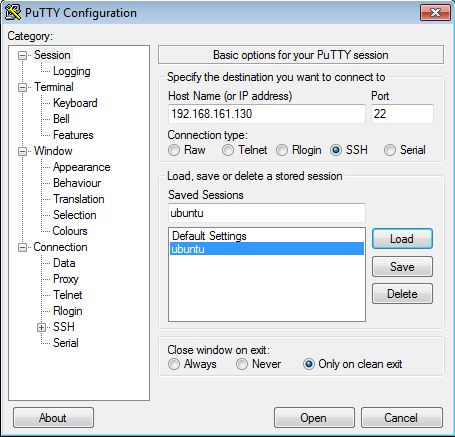
# Instalación del cliente SSH.

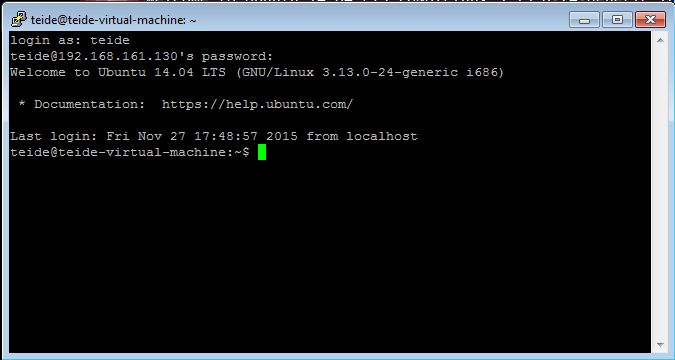
El cliente que usamos en Windows Putty, no necesita instalación, lo ejecutamos veremos la siguiente ventana:



# Primera conexión.

Introducimos la ip del servidor y le damos a conectar:



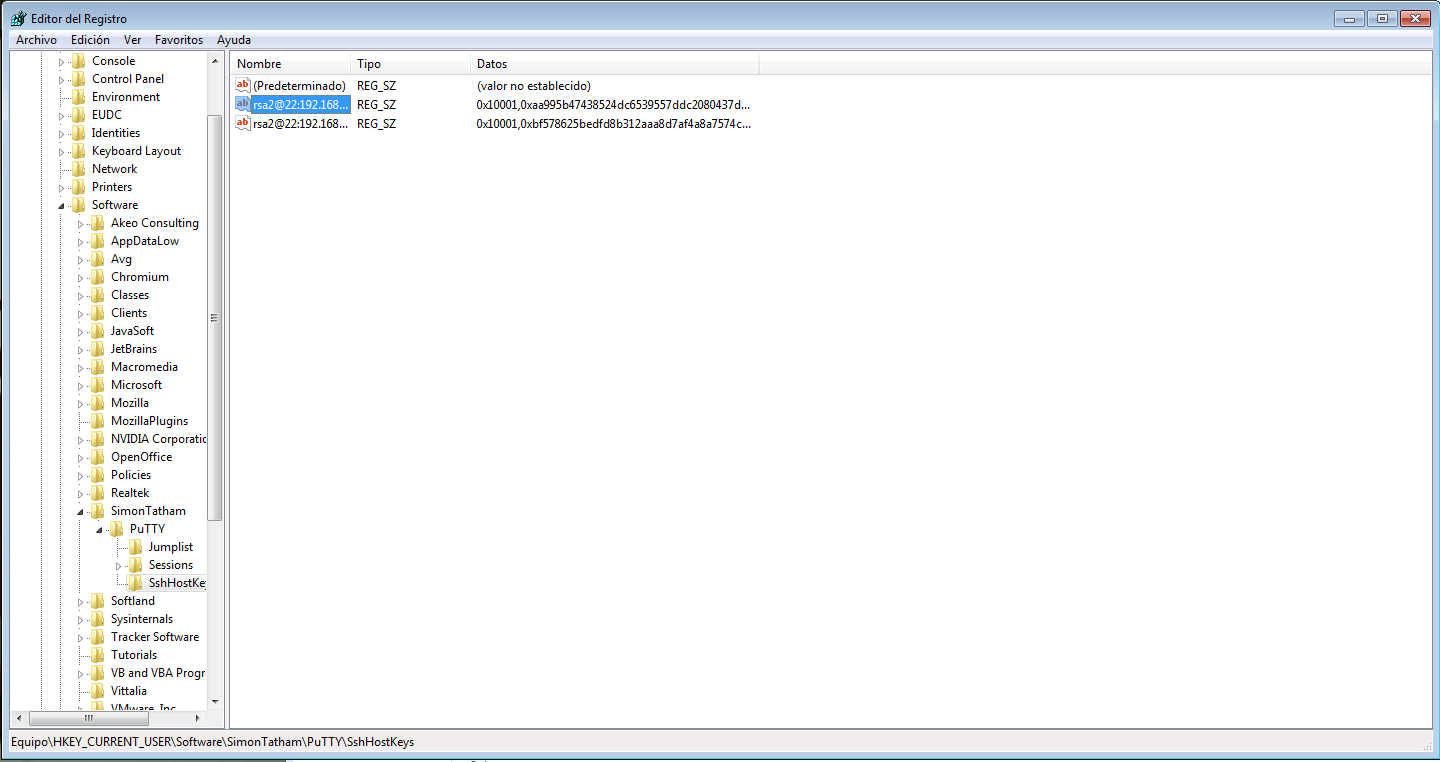


# Borrado de las claves públicas de los diferentes servidores.

Abrimos regedit y seguimos la siguiente ruta:

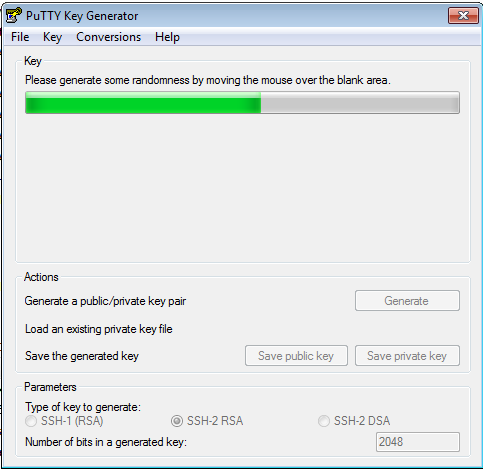
Equipo\HKEY\_CURRENTUSER\Software\SimonThatam\Putty\sshHostKeys

Aquí borramos las rsa2 que queramos.



# Crear clave privada

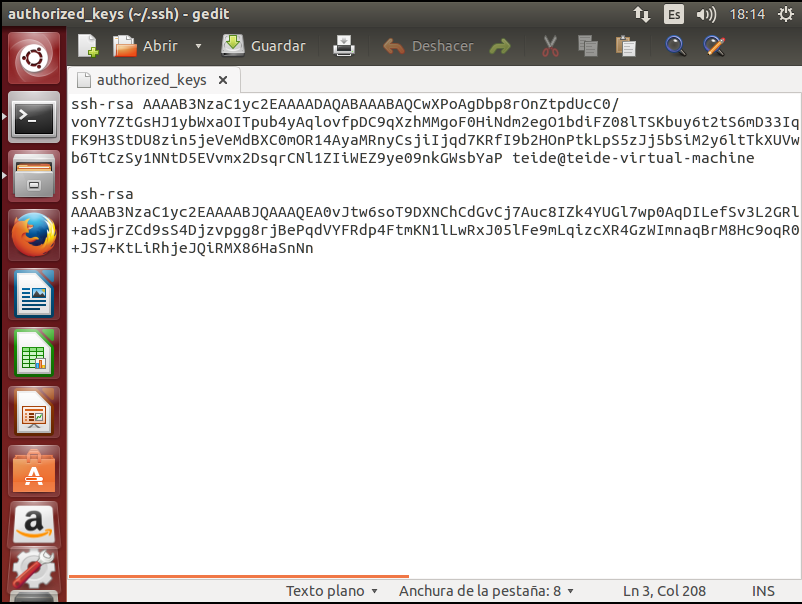
Deberemos descargarnos el PuttyGen y lo ejecutamos.

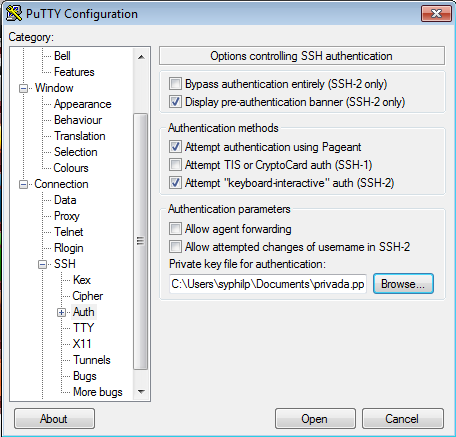


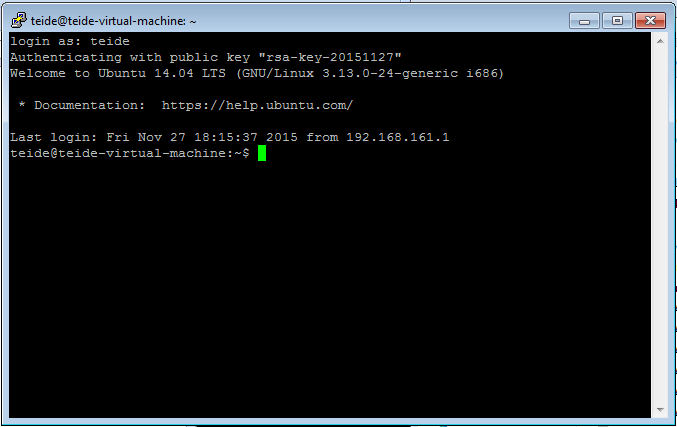


# Autenticación mediante clave privada.

Debes copiar el texto obtenido al crear la clave privada y copiarlo en ~/.ssh/athorized\_keys

Vamos al Putty > ssh >Auth y cargamos nuestra clave privada, le damos a conectar, nos pedirá la passphrase de la clave privada.

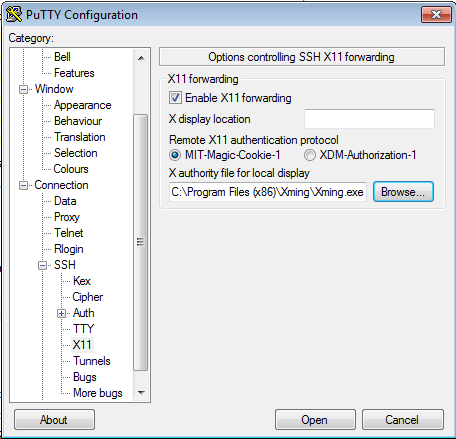


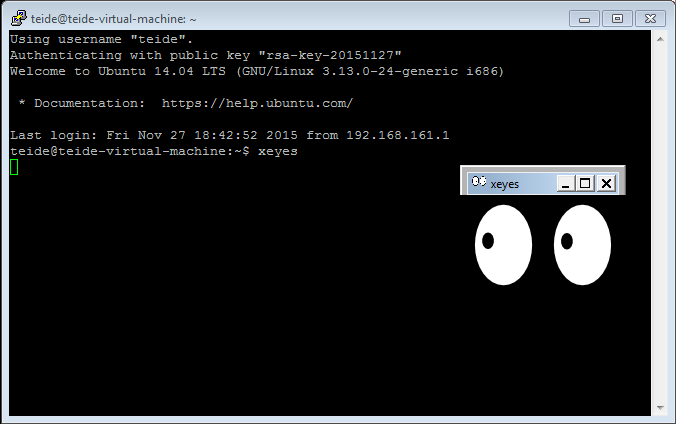


# Ejecutar aplicaciones gráficas

Deberemos instalar el programa xming y ejecutar putty con la opción ssh > x11 > enable x11 activada. Y le damos a conectar.



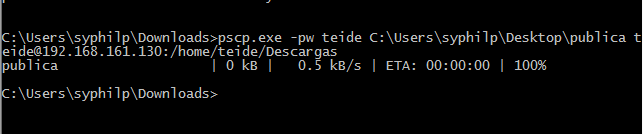




# Transferencia de archivos sobre ssh

Desde cmd ejecutamos el comando:

pscp.exe -pw <usuario> <archivo\_local> <usuario>@<ip\_server>:<archivo\_remoto>



# Crear túnel ssh

En el Putty vamos a SSH > Tunnels. En source port marcamos nuestro puerto local y en Destination ponemos <ip\_remota>:<Puerto\_remoto>. Una vez realicemos la conexión ejecutamos daytime desde cmd usando el puerto local.

