cONEXIONES REMOTAS

Telnet y SSH

Aarón Cañamero Mochales

Las Naves Salesianos

**Índice:**

[Introducción 1: 2](#_Toc54714303)

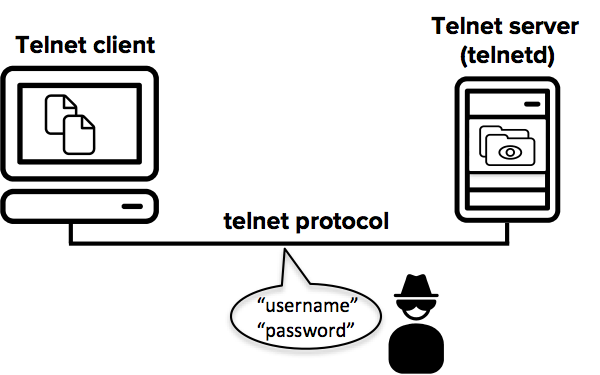
[Desarrollo 1: 3](#_Toc54714304)

[Introducción 2: 13](#_Toc54714305)

[Desarrollo 2: 14](#_Toc54714306)

Introducción 1:

Telnet (Telecommunication Network[1](https://es.wikipedia.org/wiki/Telnet#cite_note-1)​) es el nombre de un [protocolo de red](https://es.wikipedia.org/wiki/Protocolo_de_red) que nos permite acceder a otra máquina para [manejarla remotamente](https://es.wikipedia.org/wiki/Administraci%C3%B3n_remota) como si estuviéramos sentados delante de ella. También es el nombre del [programa informático](https://es.wikipedia.org/wiki/Programa_inform%C3%A1tico) que implementa el [cliente](https://es.wikipedia.org/wiki/Cliente_(inform%C3%A1tica)). Para que la conexión funcione, como en todos los servicios de [Internet](https://es.wikipedia.org/wiki/Internet), la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.



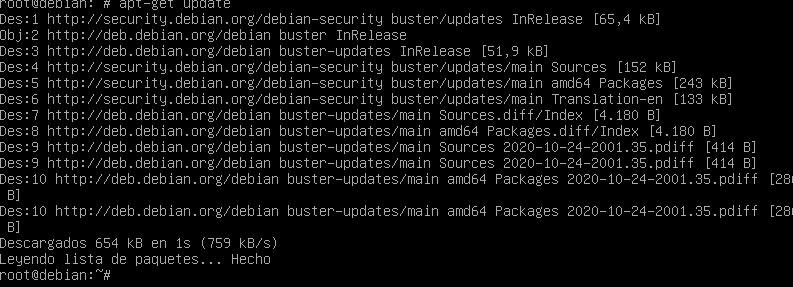
Hoy en día este protocolo también se usa para acceder a los [BBS](https://es.wikipedia.org/wiki/BBS), que inicialmente eran accesibles únicamente con un módem a través de la [línea telefónica](https://es.wikipedia.org/wiki/L%C3%ADnea_telef%C3%B3nica). Para acceder a un [BBS](https://es.wikipedia.org/wiki/BBS) mediante telnet es necesario un [cliente](https://es.wikipedia.org/wiki/Cliente_(inform%C3%A1tica)) que dé soporte a gráficos [ANSI](https://es.wikipedia.org/wiki/ANSI) y protocolos de transferencia de ficheros. Los gráficos [ANSI](https://es.wikipedia.org/wiki/ANSI) son muy usados entre los [BBS](https://es.wikipedia.org/wiki/BBS). Con los [protocolos](https://es.wikipedia.org/wiki/Protocolo_(inform%C3%A1tica)) de transferencia de ficheros (el más común y el que mejor funciona es el [ZModem](https://es.wikipedia.org/w/index.php?title=ZModem&action=edit&redlink=1" \o "ZModem (aún no redactado))) podrás enviar y recibir [ficheros](https://es.wikipedia.org/wiki/Fichero) del [BBS](https://es.wikipedia.org/wiki/BBS), ya sean programas o juegos o ya sea el correo del [BBS](https://es.wikipedia.org/wiki/BBS) ([correo](https://es.wikipedia.org/wiki/Correo) local, de [FidoNet](https://es.wikipedia.org/wiki/FidoNet" \o "FidoNet) u otras [redes](https://es.wikipedia.org/wiki/Red_de_telecomunicaci%C3%B3n)).

Algunos clientes de telnet (que soportan gráficos ANSI y protocolos de transferencias de ficheros como Zmodem y otros) son mTelnet!, NetRunner, [Putty](https://es.wikipedia.org/wiki/Putty" \o "Putty), Zoc, etc..

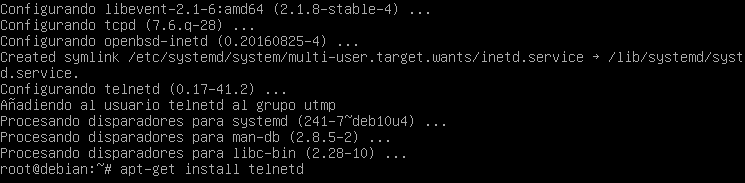
Desarrollo 1:

Instalaremos *Telnet* en la máquina que tenemos montada, en esta práctica utilizaremos una máquina *GNU/Linux* basada en *Debian.*

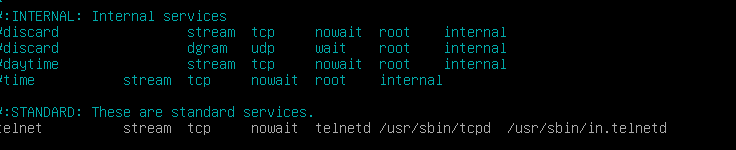
Primero haremos una actualización de todos los paquetes que tenemos en nuestra máquina. Con el comando **APT-GET UPDATE.**



Despues instalaremos el servidor **TELNET**, con el comando **APT-GET INSTALL TELNETD**.

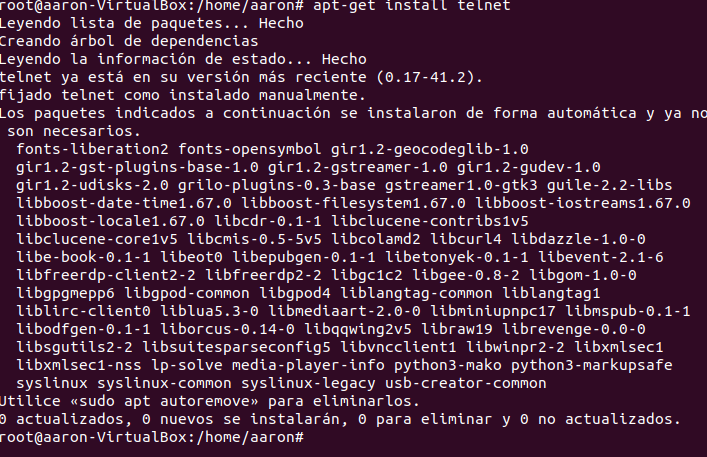


Con el comando **NANO /ETC/INETD.CONF**, podemos comprobar que el servidor de **TELNET** se ha creado correctamente.



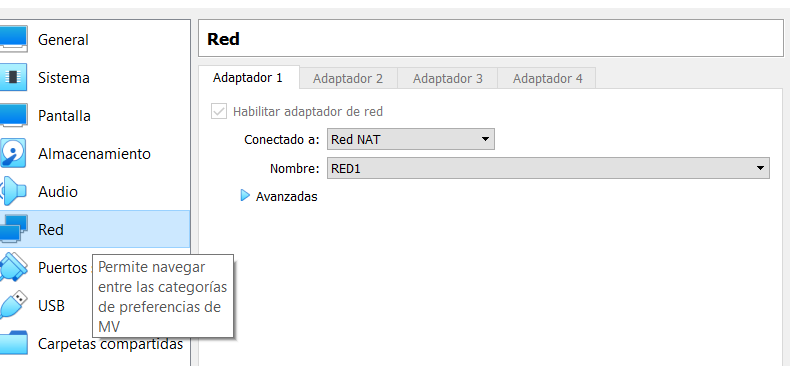
De la misma forma, instalaremos el cliente Telnet en las máquinas que tenemos preparada con Linux Ubuntu.

Instalamos **TELNET** con el comando **APT-GET INSTALL TELNET.**



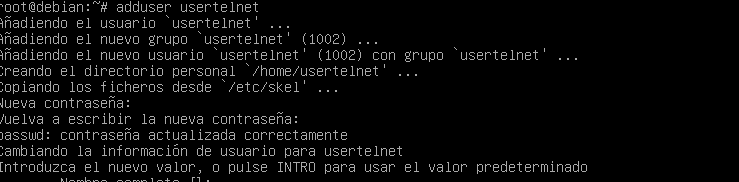
Ambas máquinas estarán conectadas mediante un Red Nat

Lo primero que haremos será apagar la dos maquinas y después añadir las dos a la misma **RED NAT**.

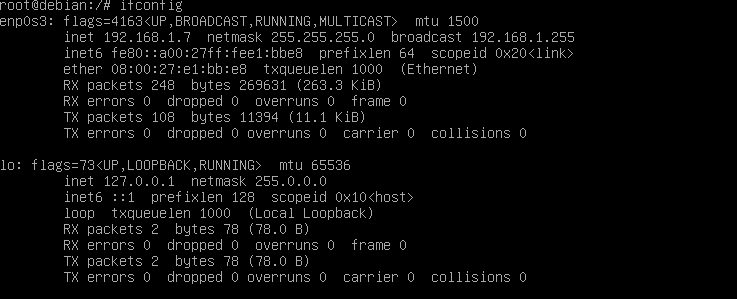


Una vez tenemos las máquinas conectadas en red, probaremos la conexión entre ambas mediante el protocolo telnet, para lo que utilizaremos un usuario creado para la ocasión, que se debe de llama usertelnet, que no debe de tener permisos de administración.

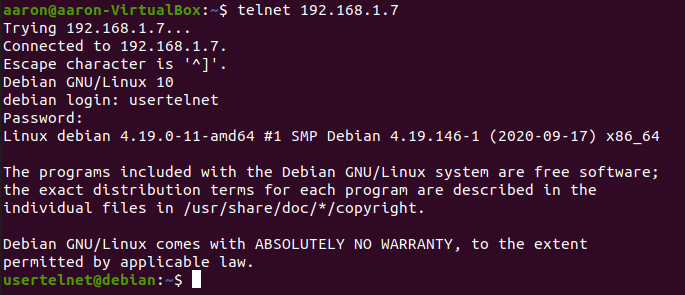
Crearemos en el **SERVIDOR** un **USUARIO** llamado **USERTELNET**. Para ello usaremos el comando **ADDUSER USERTELNET**, este es un Script que hace que nos de unos parámetros paso a paso. Para que no tenga permisos de administración, le damos los predeterminados que tiene un usuario cuando se crea.



Tenemos que mirar que IP tienen nuestro servidor para eso haremos un **IFCONFIG**.

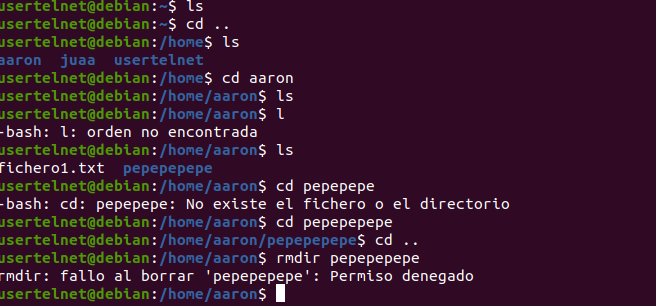


Entramos en el cliente y haremos un **TELNET** al **SERVIDOR**, poniendo la IP del servidor y luego con el usuario y contraseña que queremos entrar.



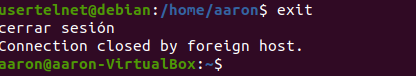
Comprobar que dicho usuario no tiene dichos permisos, por ejemplo, intentando modificar un fichero de un directorio o simplemente accediendo a un directorio al que no pueda acceder.

Aquí podemos comprobar que no podemos, eliminar el archivo de otro usuario, en este caso el usuario **AARON**.

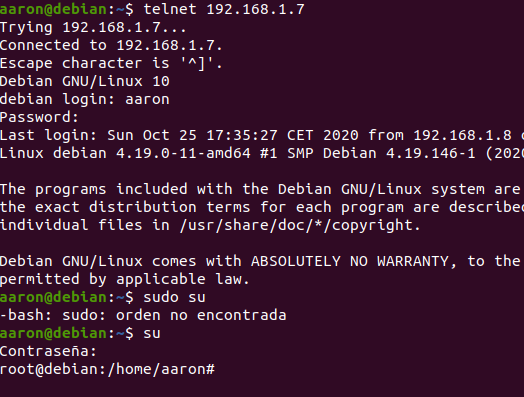


De la misma forma, debemos acceder al servicio con el usuario root e intentaremos realizar las mismas acciones que hemos realizado con el usuario anterior, debemos de comprobar que, en esta ocasión, el usuario puede realizarlas.

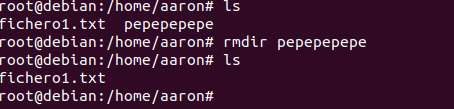
Con el comando **EXIT** salimos de la conexión del **TELNET**.



Despues entramos en una nueva conexión con **ROOT**

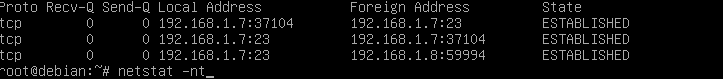


Probamos a eliminar, usamos el comando RMDIR y vemos que podemos hacerlo.



En los momentos de conexión anteriores, debemos de comprobar siempre el estado del puerto utilizado para poner en servicio telnet.

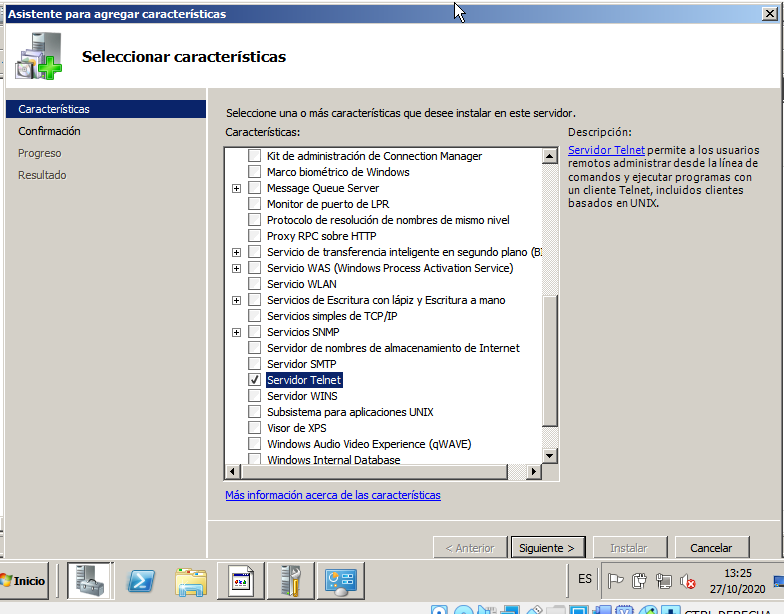
Para comprobarlo ponemos el comando **NETSTAT -NT**.



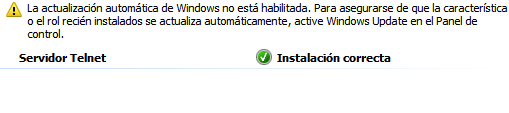
REALIZAR EXACTAMENTE LAS MISMAS TAREAS CON EL SISTEMA OPERATIVO WINDOWS UTILIZANDO PARA ELLO LA MAQUINA CON EL WINDOWS 2008 SERVER Y LA MAQUINA CON EL WINDOWS 7.

Instalaremos *Telnet* en la máquina que tenemos montada con Windows 2008 Server.

Entramos en la selección de características y vamos a activar el servidor telnet.

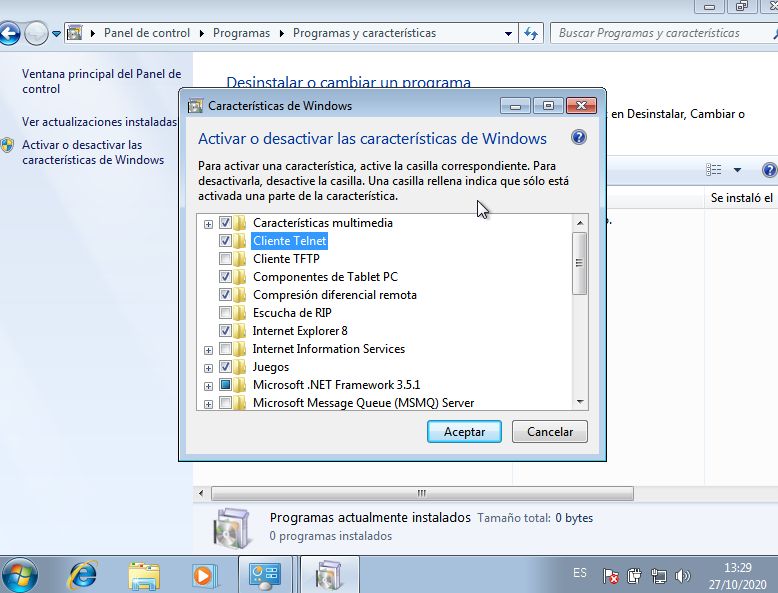


Despues nos saldrá un mensaje como que la instalación ha sido correctamente instalada y a continuación reiniciamos el equipo.

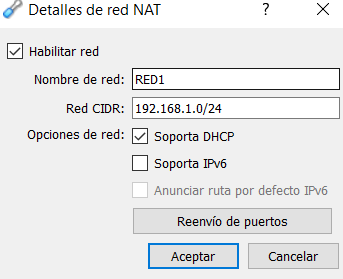


De la misma forma, instalaremos el cliente Telnet en la máquina que tenemos preparada con Windows 7.

Entramos en el panel de control, le damos a programas, despues a características de Windows y activamos la opción de Cliente Telnet.

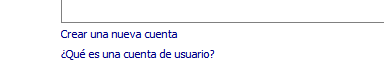


Ambas máquinas estarán conectadas mediante un Red Nat.

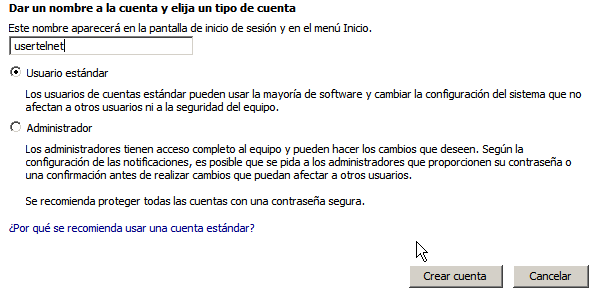


Una vez tenemos las máquinas conectadas en red, probaremos la conexión entre ambas mediante el protocolo telnet, para lo que utilizaremos un usuario creado para la ocasión, que se debe de llama usertelnet, que no debe de tener permisos de administración.

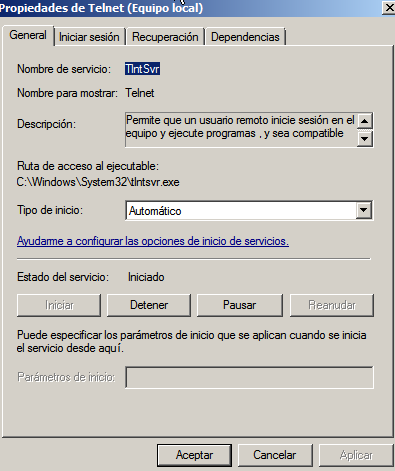
Primero crearemos el usuario **USERTELNET**, en nuestro servidor, para ello nos iremos a crear una nueva cuenta.



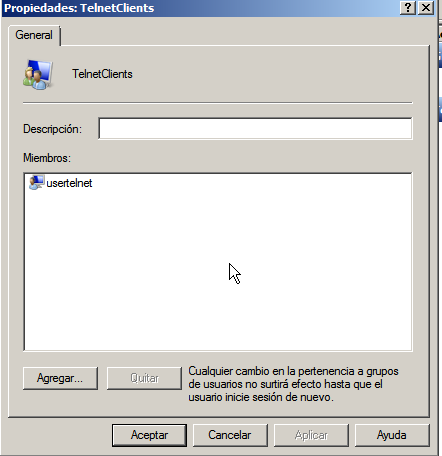
Despues escribimos el nombre del usuario y los permisos que queremos.



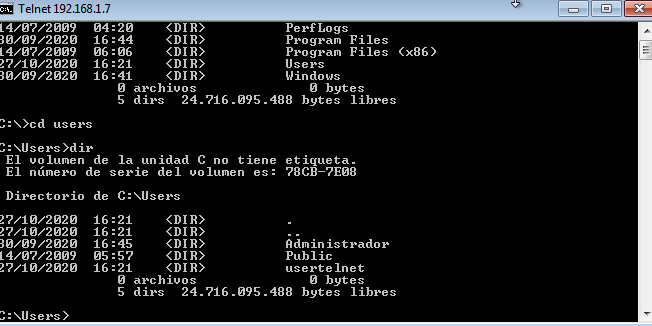
En el servidor tendremos que activar la opción de automático, que por defecto viene desactivado. Esto lo encontraremos en Servicios en la máquina del servidor.



Tendremos que añadir antes el nuevo usuario al grupo al cual pertenece Telnet.



Ahora nos iremos a nuestro cliente e iniciaremos sesión mediante el comando Telnet 192.168.1.7.



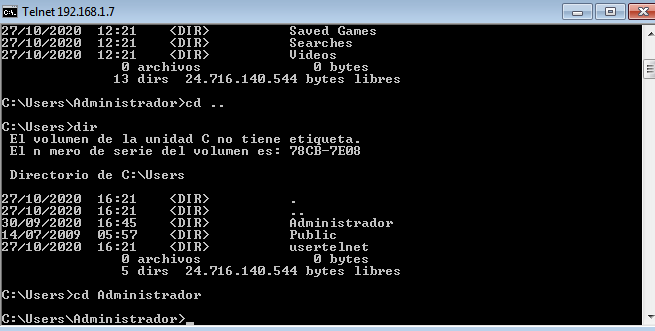
Comprobar que dicho usuario no tiene dichos permisos, por ejemplo, intentando modificar un fichero de un directorio o simplemente accediendo a un directorio al que no pueda acceder.

Intentamos acceder al directorio del **ADMINISTRADOR** y vemos que no podemos acceder, porque no tenemos permisos de administrador y somos un usuario estándar.



De la misma forma, debemos acceder al servicio con el usuario administrador e intentaremos realizar las mismas acciones que hemos realizado con el usuario anterior, debemos de comprobar que, en esta ocasión, el usuario puede realizarlas.

Entrando como **ADMINISTRADOR**, vemos que podemos entrar a la carpeta de administrador, cosa que antes no podíamos.



En los momentos de conexión anteriores, debemos de comprobar siempre el estado del puerto utilizado para poner en servicio telnet.

Una de las formas de comprobar el estado del puerto es escribiendo el comando **TELNET 192.168.1.7 23**, con el puerto al final si se nos conecta es que estamos con el puerto correcto, aunque telnet siempre usa el mismo puerto.



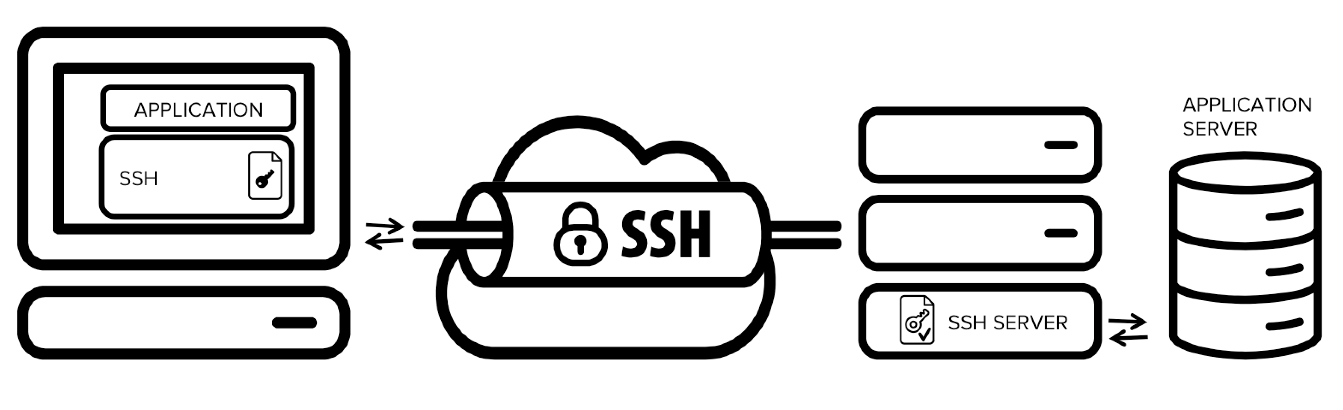
Con **NETSTAT - AN** podemos ver el estado.



Introducción 2:

SSH™ (o *S*ecure *SH*ell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

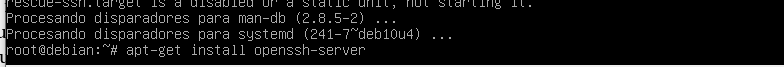
SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como **telnet** o **rsh**. Un programa relacionado, el **scp**, reemplaza otros programas diseñados para copiar archivos entre hosts como **rcp**. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.



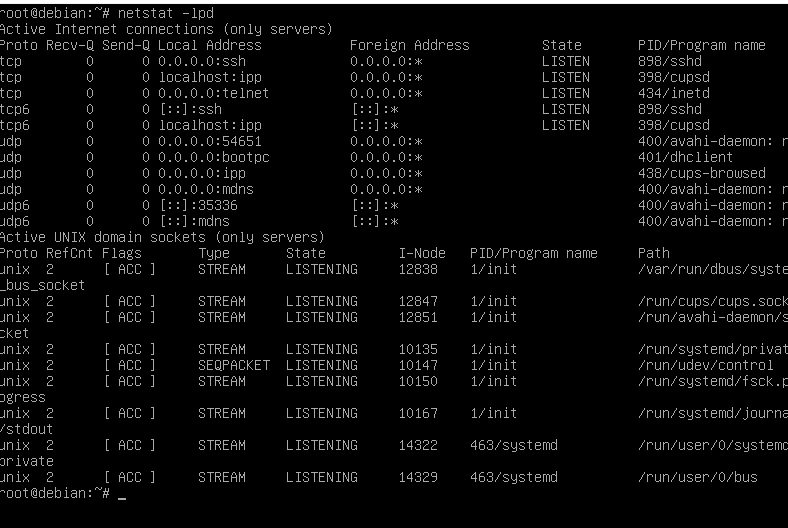
Desarrollo 2:

Instalaremos *SSH* en la máquina que tenemos montada, en esta práctica utilizaremos una máquina *GNU/Linux* basada en *Debian.*

Instalaremos SSH con el comando **APT-GET INSTALL OPENSSH-SERVER**.

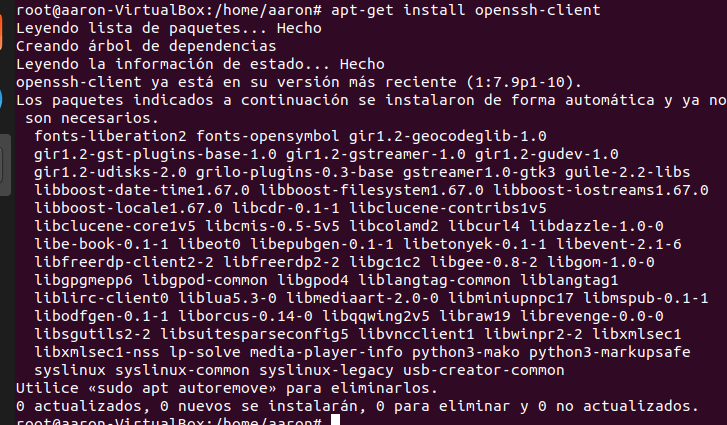


Ahora comprobaremos que lo hemos instalado correctamente. Con el comando **NETSTAT -LPD**, comprobaremos si el servicio esta en escucha o no.



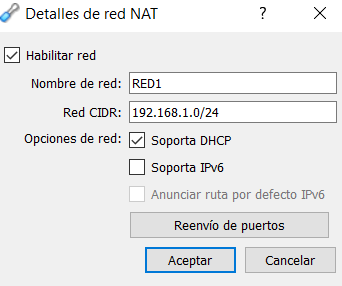
De la misma forma, instalaremos un cliente SSH en la máquina que tenemos preparada con Linux Ubuntu.

Entramos en el cliente y instalamos el cliente de **SSH**, con el comando **APT-GET INSTALL OPENSSH-CLIENT**.



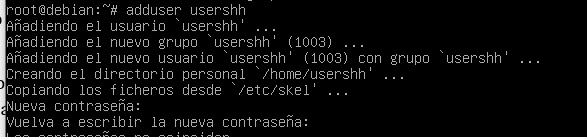
Ambas máquinas estarán conectadas mediante un Red Nat.

Conectamos las dos maquinas a la misma **RED NAT**.

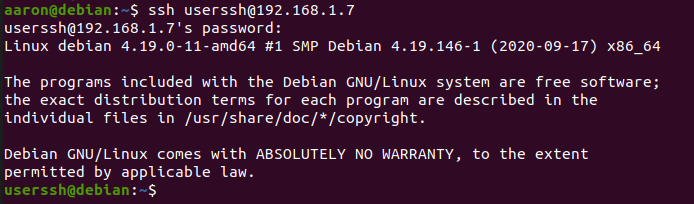


Una vez tenemos las máquinas conectadas en red, probaremos la conexión entre ambas mediante el protocolo SSH, para lo que utilizaremos un usuario creado para la ocasión, que se debe de llama userssh, que no debe de tener permisos de administración.

Creamos el usuario con el comando **ADDUSER USERSSH**.

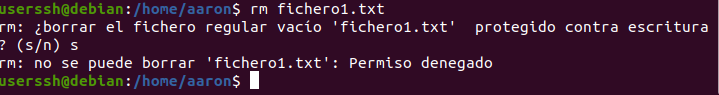


Despues iniciamos sesión con el comando **SSH USERSSH@192.168.1.7**.



Comprobar que dicho usuario no tiene dichos permisos, por ejemplo, intentando modificar un fichero de un directorio o simplemente accediendo a un directorio al que no pueda acceder.

Intentamos eliminar un archivo que no es nuestro y vemos que no podemos hacerlo.

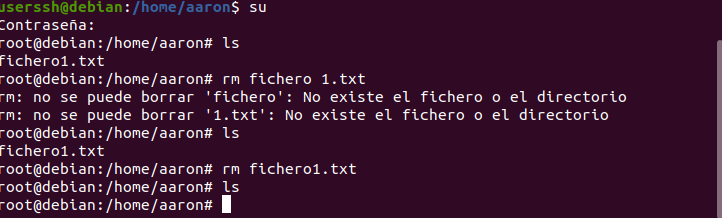


Tambien podemos comprobar que no nos deja crear directorios ni archivos.



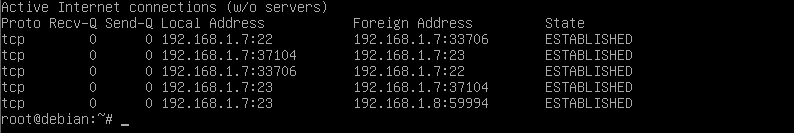
De la misma forma, debemos acceder al servicio con el usuario root e intentaremos realizar las mismas acciones que hemos realizado con el usuario anterior, debemos de comprobar que, en esta ocasión, el usuario puede realizarlas.

Entramos en **ROOT** con el comando **SU** y al intentar borrar o crear un directorio o archivo, vemos que podemos hacerlo, sin ningun tipo de problemas.



En los momentos de conexión anteriores, debemos de comprobar siempre el estado del puerto utilizado para poner en servicio telnet.

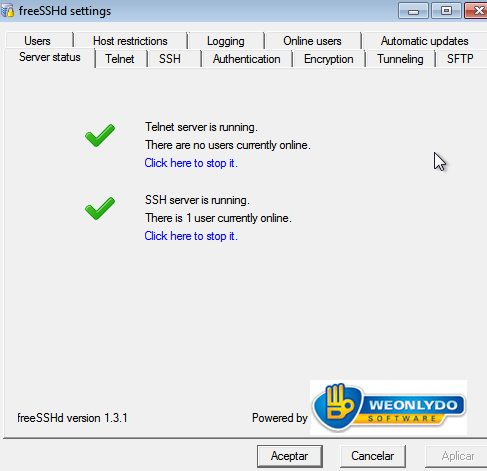
Con el comando **NETSTAT -NT**, podemos comprobar el puerto.



REALIZAR EXACTAMENTE LAS MISMAS TAREAS CON EL SISTEMA OPERATIVO WINDOWS UTILIZANDO PARA ELLO LA MAQUINA CON EL WINDOWS 2008 SERVER Y LA MAQUINA CON EL WINDOWS 7.

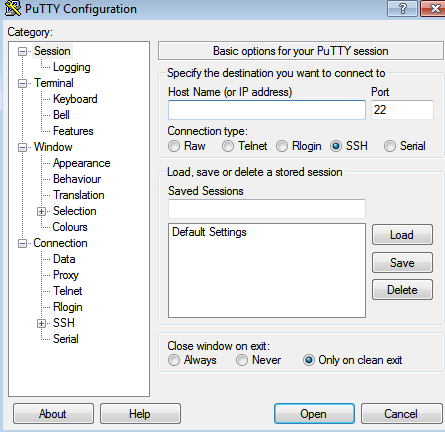
Instalaremos SSH en la máquina que tenemos montada, en esta práctica utilizaremos una máquina Windows 2008 Server.

Para instalarlo nos bajaremos el servicio de SSH y lo configuraremos para que nos de servicio y nos podamos conectar a el.

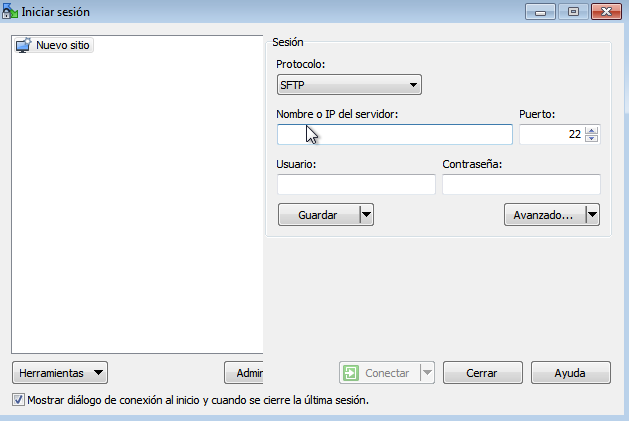


De la misma forma, instalaremos un cliente SSH en la máquina que tenemos preparada con Linux Ubuntu.

En la maquina cliente instalaremos Putty, para poder conectarnos al servidor de ssh. Tambien podemos usar el WinSCP.

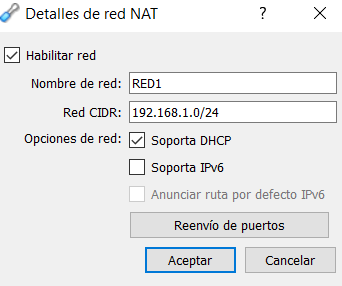


Esto es WinSCp.



Ambas máquinas estarán conectadas mediante un Red Nat.

Uniremos las maquinas a la misma red nat de antes.

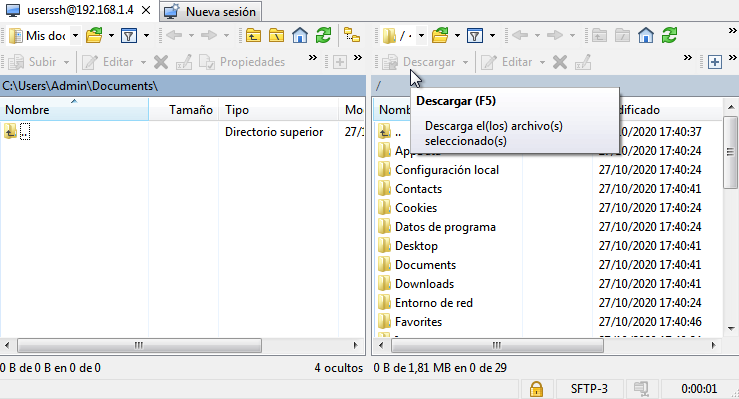


Una vez tenemos las máquinas conectadas en red, probaremos la conexión entre ambas mediante el protocolo SSH, para lo que utilizaremos un usuario creado para la ocasión, que se debe de llama userssh, que no debe de tener permisos de administración.

Creamos el usuario **USERSSH** y despues mediante **WINSCP** entramos en el servidor, ponemos la **IP** el usuario el cual vamos a entrar y su contraseña, tambien tenemos que poner el puerto, que por defecto es el 22.

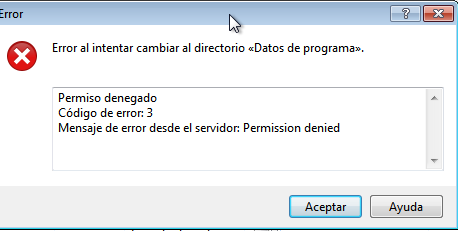


Despues nos conectamos y nos saldrá que estamos en el usuario **USERSSH** y su **IP**.



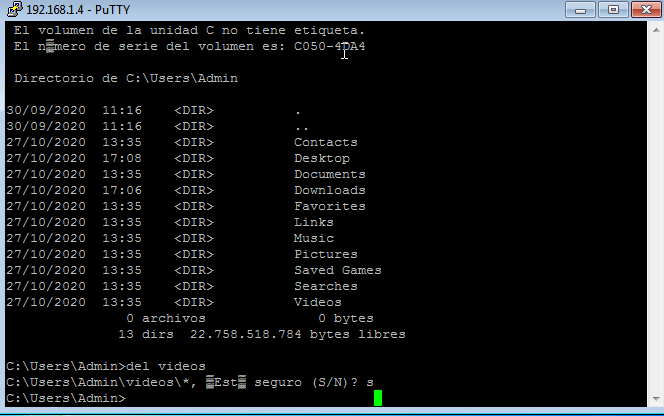
Comprobar que dicho usuario no tiene dichos permisos, por ejemplo, intentando modificar un fichero de un directorio o simplemente accediendo a un directorio al que no pueda acceder.

Al intentar acceder a un archivo o directorio al que no tenemos acceso nos saldrá, permiso denegado.



De la misma forma, debemos acceder al servicio con el usuario administrador e intentaremos realizar las mismas acciones que hemos realizado con el usuario anterior, debemos de comprobar que, en esta ocasión, el usuario puede realizarlas.

Entraremos esta vez desde **PUTTY**, para ver que funciona muy similar, en este caso como **ADMINISTRADOR**, y eliminaremos una carpeta, en este caso vemos que no nos sale permiso denegado.



En los momentos de conexión anteriores, debemos de comprobar siempre el estado del puerto utilizado para poner en servicio ssh.

Con el comando **NETSTAT -ANO | FIND “22”**, podemos ver el puerto 22, si está activo o no.

