Apuntes de Debian 11

Ip address : te muestra la información del dispositivo, sobre todo las ips.

Ip –c address : Te muestra la información del dispositivo pero con colores

Nano \_\_\_ : editor de texto de un archivo

Para cerrar o abrir los puertos desde un terminal tienes que utilizar el comando ifdown / ifup y después el nombre del puerto comopuede ser enp0s3

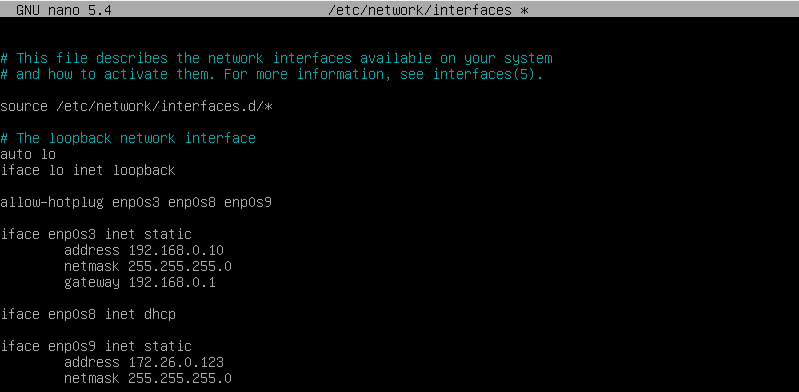
Para reiniciar los servicios en red: service networking restart ; luego tienes que levantar todas las tarjetas que tienes. Service networking restart ; ifup enp0s3

Para apagar la maquina: shutdown –h now

Poner el adaptador 2 con Adaptador puente y el adaptador 3 con red interna

Las direcciones IP de Debian11 tienen que coincidir con las del VirtualBox

Para meter las direcciones IP desde nano se puede meter en /etc/network/interfaces



Después tienes que activarlas con el comando ifup enp0sX

Para ver el nameserver: nano /etc/resolv.conf



Para hacer un archivo inmutable (NADIE lo puede modificar) se pone: chattr +i nombre\_archivo

Para hacer que un archivo solo se le pueda añadir y no se pueda borrar, pero solo se puede añadir texto con las redirecciones de entrada salida (como puede ser echo “XXX” >> Archivo): chattr +a

PREGUNTA EXMANEN: saber que es SSH y telnet

SSH busca que te puedas verificar de alguna forma cuando quieres conectarte con un servidor, como si fuese un lector de huella, también busca que la autentificación sea cifrada, el tráfico de datos enviados y recibidos sean cifrados

Para instalar ssh: apt install ssh

Datos de ssh: service ssh status

Comando: algo que puede identificar o ejecutar un shell

HAY QUE DESCARGAR PuTTY EN UN W7 PARA HACERPRUEBAS

Ventajas del PuTTY:

Desde el putty puedes copiar los textos de tu ordenador, ya que en el debían no puedes porque no puedes instalar las guest\_adittion.

Para meterte a una máquina vitual desde tu Windows: cmd>ssh usuario@ip

Top es un comando en debían para que te muestre la tabla de interprete

Para modificar el servicio ssh: /etc/ssh/sshd\_config

ListenAddress : Limitar las escuchas

Para ver los usuarios: cat /etc/passwd

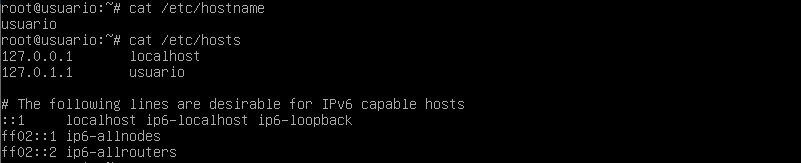
Adduser: crear usuario

Para ver si el servicio ssh está en ejecución: service ssh status

Para que solo se pueda loguear un único usuario AllowuUer nombreUsuario en /etc/ssh/sshd\_config

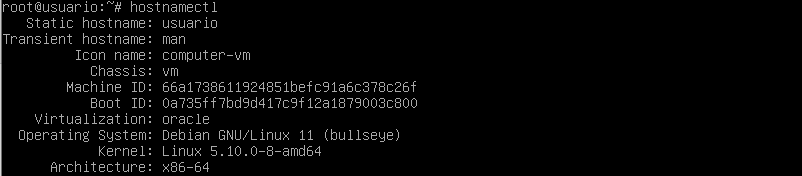
Para que solo se pueda bloquear un único usuario DenyUsers nombreUsuario en /etc/ssh/sshd\_config

Para poder cambiar el nombre de la máquina: Entrar en /etc/hostname y cambiar el nombre y meterte en /etc/hosts y cambiar el nombre y por último reiniciar



El directorio /etc/hosts está en todas las maquinas que sporten TCP/IP

Para ver información de la máquina: hostnamectl



Para cambiar el nombre de la máquina con comando: hostnamectl set-hostname XXX

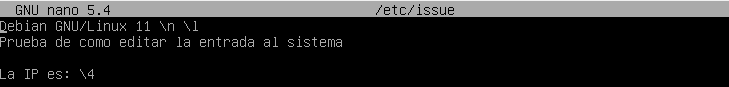


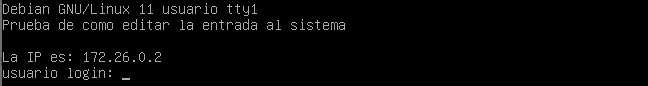
Una vez cambiado el nombre salir con exit y volver a registrase con usuario para poder cambiar la carpeta /etc/hosts

(Windows 10) Para enviar archivos desde un equipo a otro mediante ssh: scp <origen> <destino>

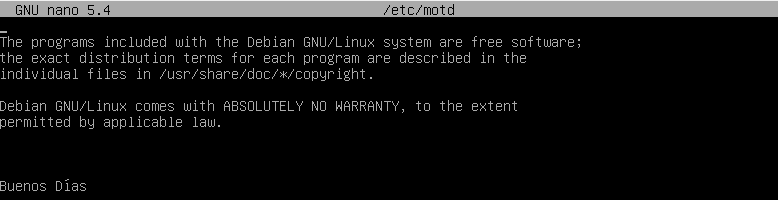
Scp XXX yoda@direcciónIP:/home/yoda/

Como personalizar la entrada al sistema, todos los usuarios lo ven: nano /etc/issue. Si pones \4 puedes poner la dirección IP





Para poner un comentario cuando se loguea un usuario: nano /etc/motd



Para modificar el mensaje de inicio de sesión entrar en. bashrc y modificarlo ahí, pero al final

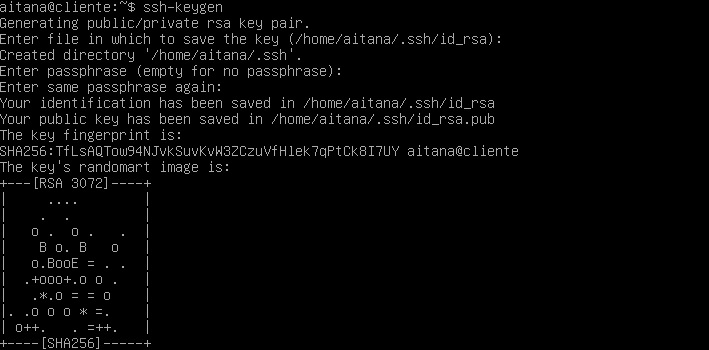
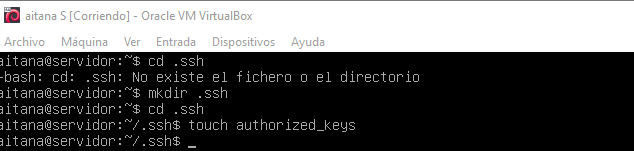
SSH permite encapsular otros protocolos, ya sea por seguridad o privacidad

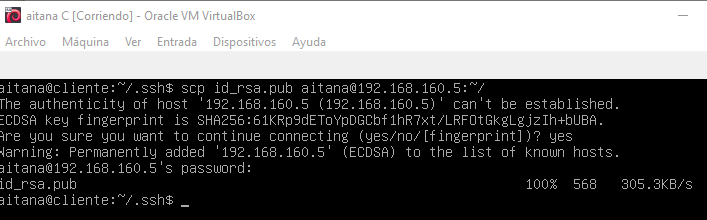
Para ver que conexiones tienes abiertas: netsat, netstat –n para que te salgan las direcciones IP

SSH es el cliente SSHD es el servidor

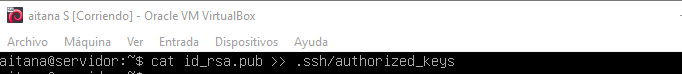
Para conectarte mediante túnel a un ssh desde Windows a debían: ssh –L 8080:172.26.3.171:80 [yoda@172.26.3.171](mailto:yoda@172.26.3.171) , una vez abierto el túnel, iniciar una nueva Shell y conectarte mediante ssh usuario@localhost:2222 que es el puerto que pusimos antes o si no funciona poner ssh –p 2222 usuario@localhost, pero todo esto SIN CERRAR EL TUNEL!!

Como generar las llaves privadas y públicas de ssh, se utiliza el programa ssh-keygen.

1. Generar clave desde el cliente: ssh-keygen y dar intro
2. Para ver la clave tanto publica como privada entrar en el archivo cd .ssh y para ver la clave cat id\_rsa o id\_rsa.pub
3. En el servidor crear un archivo que se llame .ssh y crear el archivo authorized\_keys
4. En el cliente copiarel archivo:



1. En el servidor autorizar la clave publica

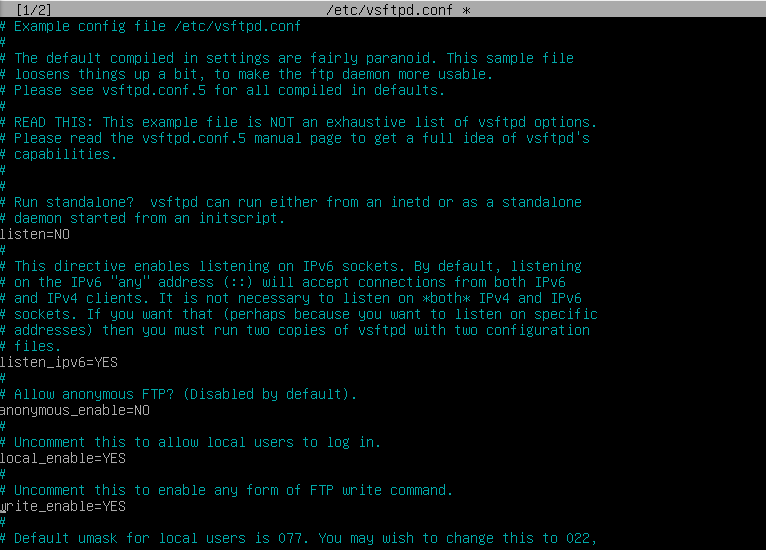


1. Para copiar el archivo de la clave automáticamente: Crear la llave pública y poner el siguiente comando: ssh-copy-id [aitana@0.0.0.0](mailto:aitana@0.0.0.0)

**FTP**

Apt update ; apt install vsftpd -y



Para que puedan subir archivos remotamente: habilitar write\_enable=YES (/etc/vsftpd.conf)

Lo siguiente es hacer service vsftpd restart y volver a conectarte en FileZilla

Con chroot puedes configurar que una carpeta sea el raíz; entrar en /etc/vsftpd.conf y habilitar chroot\_local\_user=YES