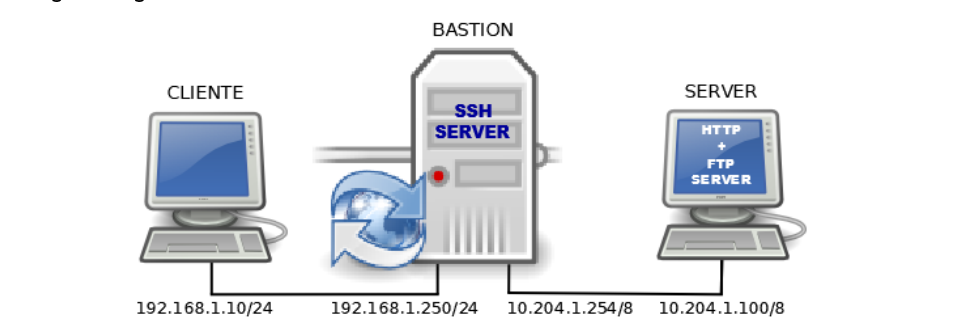
Practica 4 Túneles TCP-IP



Carlos González Martín

2ºB de Grado medio de sistemas microinformáticos y redes

Las Naves Salesianos

Curso 2021-2022

Índice

[1. Que necesitamos 3](#_Toc105495219)

[2. Instalamos los paquetes necesarios 3](#_Toc105495220)

[3. Cambiamos las IP 3](#_Toc105495221)

[4. SSH 6](#_Toc105495222)

[5. FTP 7](#_Toc105495223)

[6. Apache 9](#_Toc105495224)

[7. Túneles SSH 11](#_Toc105495225)

[8. SOCKS 13](#_Toc105495226)

Ilustraciones

[Ilustración 1: Instalando paquetes necesarios 3](#_Toc105495227)

[Ilustración 3: cambiar nombre a la maquina 3](#_Toc105495228)

[Ilustración 4: Cambiando nombre de la maquina en el /etc/hosts 4](#_Toc105495229)

[Ilustración 5: Cambiando ip a bastión 4](#_Toc105495230)

[Ilustración 6: ip ya configurada 5](#_Toc105495231)

[Ilustración 7: maquinas encendidas y con conectividad 5](#_Toc105495232)

[Ilustración 8: Creamos el usuario Batman 6](#_Toc105495233)

[Ilustración 9: Permitimos el acceso a Batman 6](#_Toc105495234)

[Ilustración 10: probamos con usuario para ver si está bien configurado 6](#_Toc105495235)

[Ilustración 11: ssh a bastión con el usuario Batman 6](#_Toc105495236)

[Ilustración 12: Crear el usuario Robin 7](#_Toc105495237)

[Ilustración 13: Creamos en el /etc/shells un directorio de no conexión 7](#_Toc105495238)

[Ilustración 14: comando usermod para que no acceda el usuario Robin 8](#_Toc105495239)

[Ilustración 15: Archivo /etc/passwd 8](#_Toc105495240)

[Ilustración 16: cambiamos el directorio de inicio 9](#_Toc105495241)

[Ilustración 17: Revisamos el directorio de inicio 9](#_Toc105495242)

[Ilustración 18: Servicio apache apagado 9](#_Toc105495243)

[Ilustración 19: Servicio apache en cliente apagado 10](#_Toc105495244)

[Ilustración 20: Búsqueda con Lynx 10](#_Toc105495245)

[Ilustración 21: Búsqueda exitosa de Google con Lynx 10](#_Toc105495246)

[Ilustración 22: Túnel ssh 11](#_Toc105495247)

[Ilustración 23: Nueva terminal y lanzando el comando Lynx 11](#_Toc105495248)

[Ilustración 24: Pagina web del servidor vista en el cliente 12](#_Toc105495249)

[Ilustración 25: Túneles dinámicos 13](#_Toc105495250)

[Ilustración 26: Conexión mediante putty 14](#_Toc105495251)

[Ilustración 27: Socks en FileZilla 14](#_Toc105495252)

[Ilustración 28: Conexión establecida 15](#_Toc105495253)

[Ilustración 30: archivo visualizado en nuestro navegador favorito 15](#_Toc105495254)

# Que necesitamos

Para esta práctica usaremos un debian 11 sin entorno en el que le instalaremos los paquetes y posteriormente configuraremos los servicios

# Instalamos los paquetes necesarios

Instalaremos ftp, ssh, servidor apache y Lynx en la primera máquina y luego clonaremos

con el siguiente comando instalaremos todo:

# apt update ; apt install ssh vsftpd apache2 lynx -y

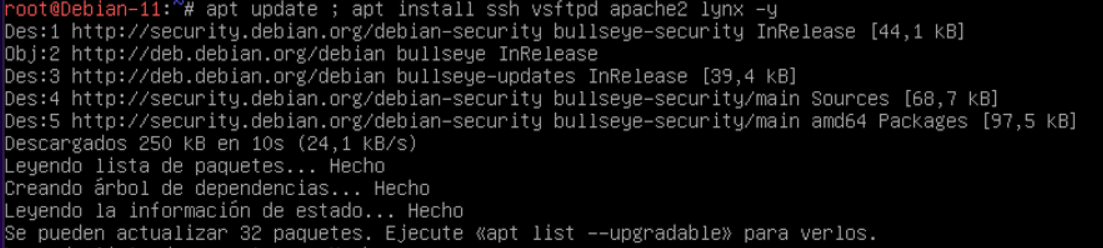


Ilustración : Instalando paquetes necesarios

Una vez instalado los paquetes apagamos la maquina y la clonamos tantas veces como sea necesario en este caso son 3 máquinas cliente, bastión y server.

# Cambiamos las IP

# hostnamectl set-hostname Bastion

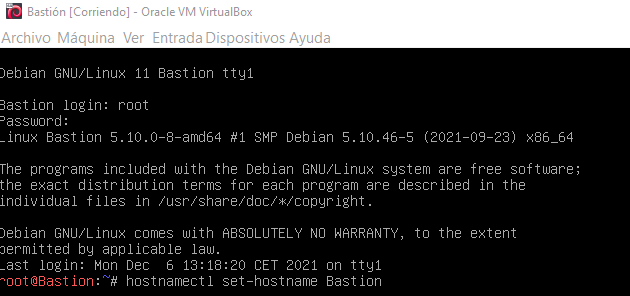


Ilustración 3: cambiar nombre a la maquina

Podemos también cambiarlo en el archivo /etc/hosts y se nos aplica en toda la maquina

# nano /etc/hosts

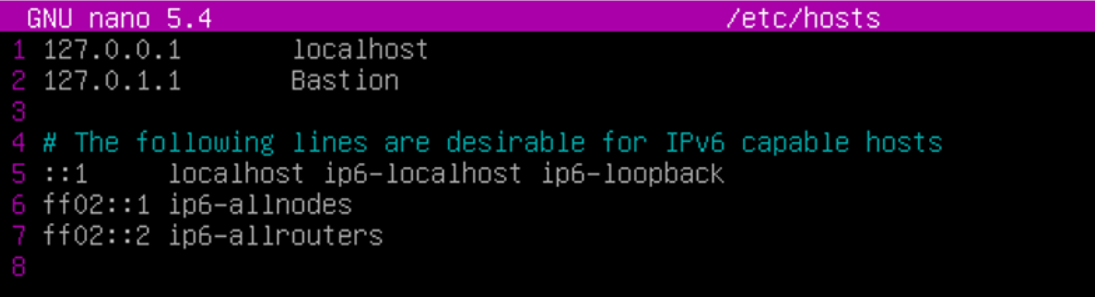


Ilustración 4: Cambiando nombre de la maquina en el /etc/hosts

ahora cambiaremos la ip de la segunda tarjeta de red.

# nano /etc/network/interfaces

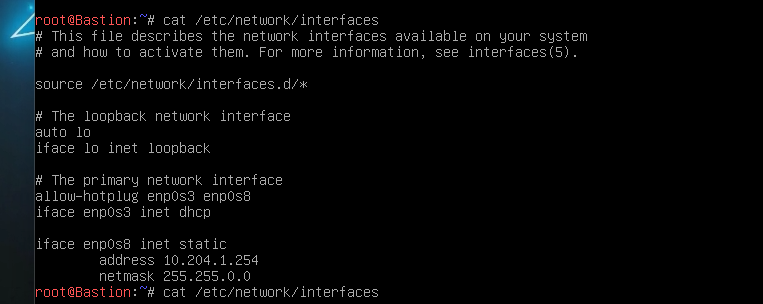


Ilustración 5: Cambiando ip a bastión

Una vez cambiada en el archivo de configuración lo que haremos será aplicar los cambios con el siguiente comando

# service networking restart ; ifup enp0s3 ; ifup enp0s8

# ip -c a

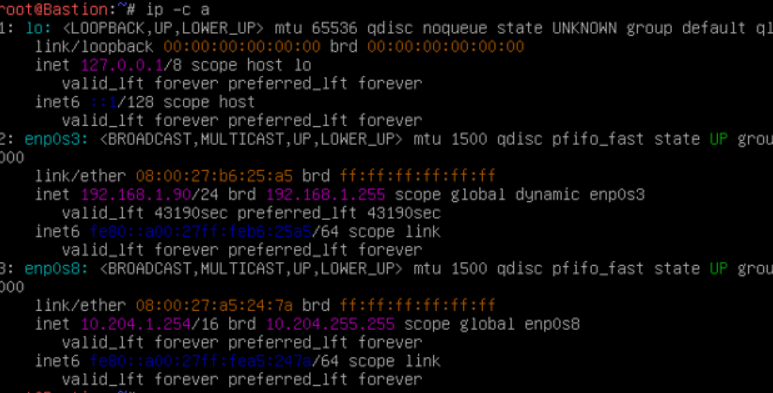


Ilustración 6: ip ya configurada

Vemos que ya se ha cambiado la ip a la máquina, ahora haremos lo mismo a la maquina server, cambiaremos el nombre a la maquina cliente para que sepamos donde estamos

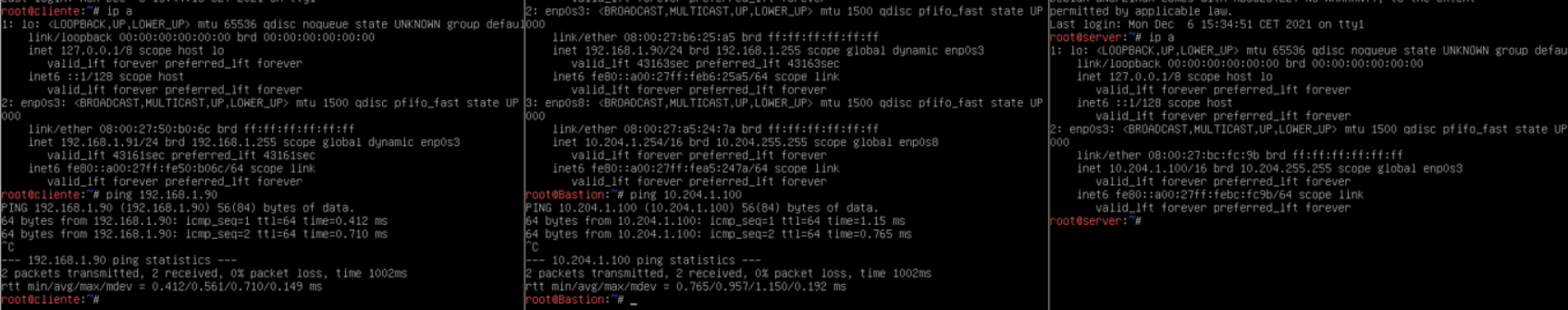


Ilustración 7: maquinas encendidas y con conectividad

una vez que hemos encendido las máquinas y hemos comprobado que tienen conectividad entre ellas configuraremos los servicios en las respectivas maquinas que en este caso es bastión y server.

# SSH

Creamos el usuario Batman con el siguiente comando para que nos podamos conectar por ssh a través de ese usuario

# adduser Batman

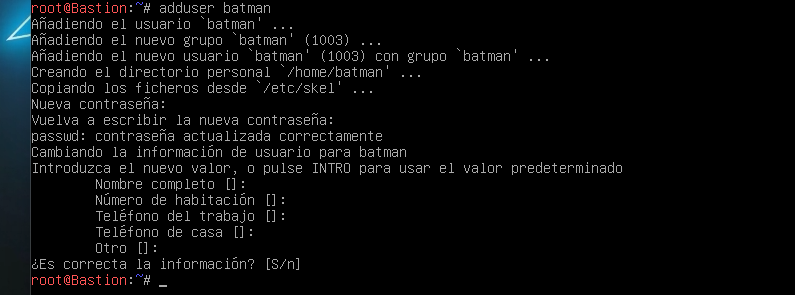


Ilustración 8: Creamos el usuario Batman

Ya que tenemos creado el usuario haremos que ese usuario pueda acceder por ssh, pero el resto no

Ilustración 9: Permitimos el acceso a Batman

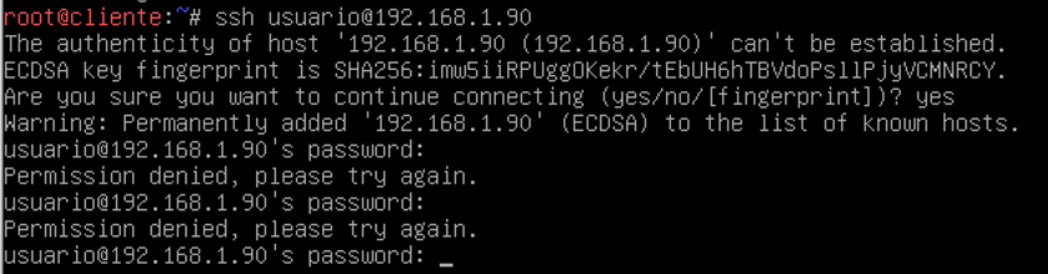


Ilustración 10: probamos con usuario para ver si está bien configurado

Como vemos no nos deja ahora probaremos con el usuario Batman para ver si nos deja

Ilustración 11: ssh a bastión con el usuario Batman

Efectivamente si nos deja conectarnos por ssh a bastión con el usuario Batman.

# FTP

Ahora en la maquina Server crearemos un servicio FTP para la transferencia de archivos

# adduser Robin

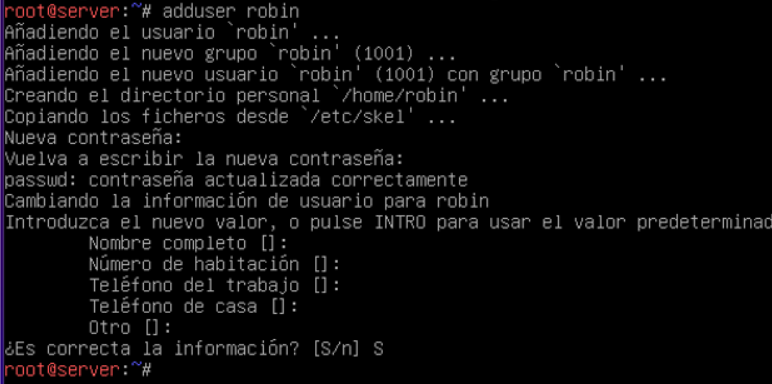


Ilustración 12: Crear el usuario Robin

Creamos el usuario Robin para conectarnos a través de ese usuario.

Para hacer que el usuario Robin se conecte solo por ftp y no por terminal en el servidor añadimos la siguiente línea en el /etc/shells

# nano /etc/shells

/bin/nologin



Ilustración 13: Creamos en el /etc/shells un directorio de no conexión

Una vez creado el directorio para que no se pueda loquear en la maquina mediante la terminal solo por ftp añadiremos esta línea al usuario Robin.

Usaremos el siguiente comando para que funcione correctamente.

# usermod -s /bin/nologin robin

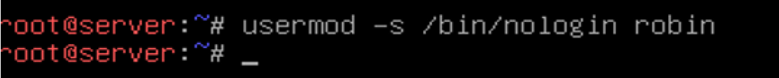


Ilustración 14: comando usermod para que no acceda el usuario Robin

Ahora revisamos en el /etc/passwd si ha cambiado el directorio de conexión no sin antes o reiniciar la maquina o bloquear la maquina con un Exit.

Una vez hecho vemos el archivo passwd

# cat /etc/passwd

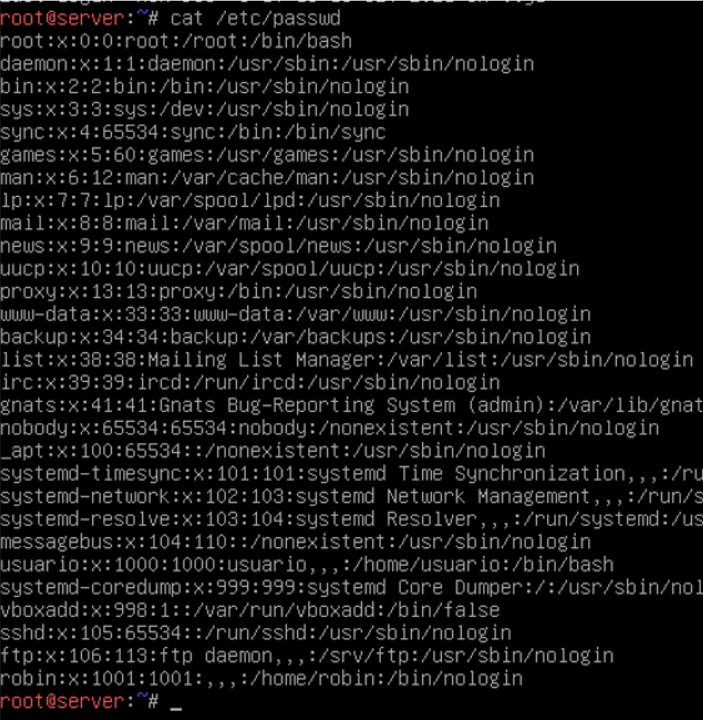


Ilustración 15: Archivo /etc/passwd

y vemos que ha cambiado

Una vez hecho esto cambiamos el directorio de conexión en vez de /home/robin a /var/www/html para eso usamos el siguiente comando

# usermod -d /var/www/html robin



Ilustración 16: cambiamos el directorio de inicio

Revisamos si se ha cambiado con el siguiente comando.

# cat /etc/passwd

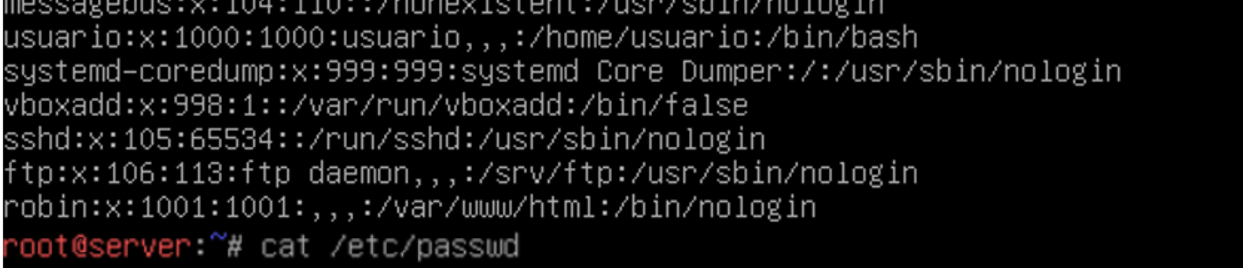


Ilustración 17: Revisamos el directorio de inicio

Teniendo esto hecho podemos pasar al siguiente punto

# Apache

Como he clonado las maquinas tengo que apagar el servicio apache en la maquina cliente y bastión para que no veamos la página de ninguna de estas máquinas solo la de server.

# service apache2 stop

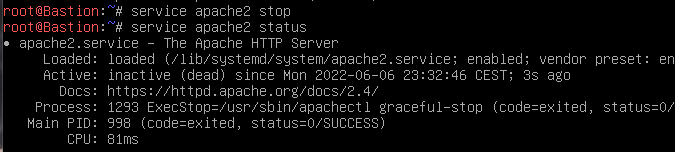


Ilustración 18: Servicio apache apagado

Una vez hecho en bastión haremos lo mismo en el cliente

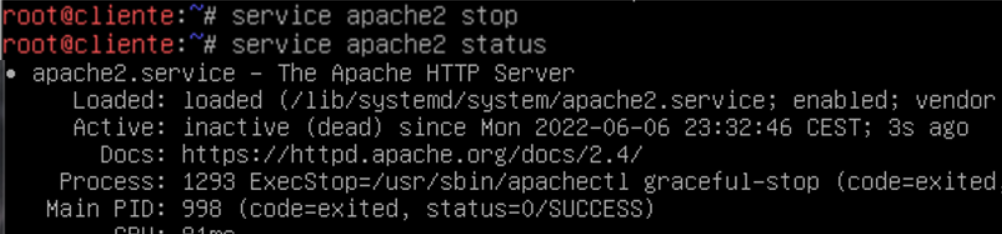


Ilustración 19: Servicio apache en cliente apagado

Ya hecho esto miraremos si funciona el software Lynx en la maquina cliente

# lynx www.google.es

Probamos con la página de Google



Ilustración 20: Búsqueda con Lynx

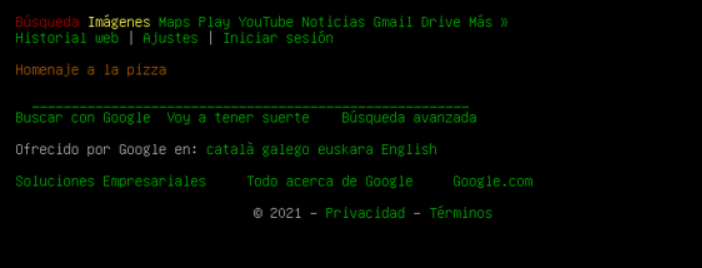


Ilustración 21: Búsqueda exitosa de Google con Lynx

Como teníamos la maquina en modo puente hemos podido visualizar la página de Google

# Túneles SSH

Para hacer los túneles ssh tenemos que saber la ip tanto del bastión como del server

y escribiremos el siguiente comando para hacer correctamente el túnel

# ssh -L 8080:10.204.1.100:80 batman@192.168.1.90



Ilustración 22: Túnel ssh

Una vez creado el túnel iremos a una segunda terminal con la combinación de teclas:

CTRLderecha + F2

Una vez iniciado sesión escribimos el siguiente comando

# lynx localhost:8080



Ilustración 23: Nueva terminal y lanzando el comando Lynx

Una vez hecho esto nos tiene que salir la página web del server

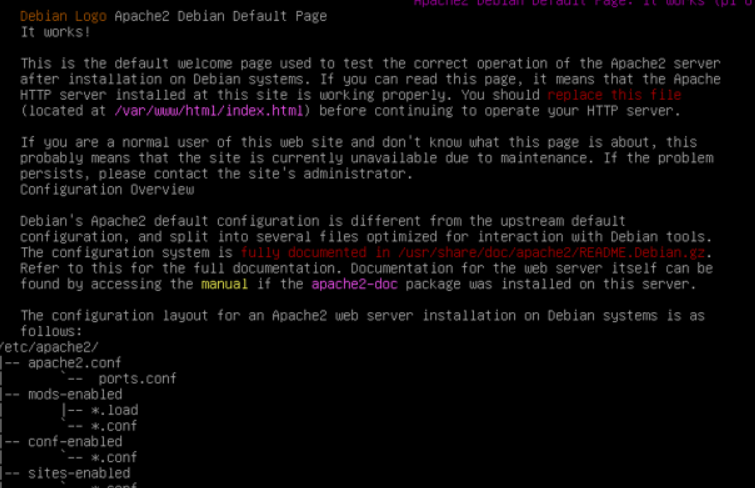


Ilustración 24: Pagina web del servidor vista en el cliente

Ya viendo la página podemos hacer varias cosas como cambiar la página web y verla en el cliente o si hacemos un túnel con nuestro ordenador con Windows por ejemplo lo podemos hacer.

Ya no usaremos más el cliente por lo cual apagaremos la máquina, las demás no ya que las vamos a usar en el siguiente apartado.

# SOCKS

¿Qué es SOCKS?

Socks es un protocolo de internet que permite conexión cliente-servidor para usarlo de manera transparente los servicios de un firewall, y poder conectarse a un servidor de fuera si tienes un firewall en tu salida o al revés para poder conectarte a un servidor que está dentro de un firewall.

Ahora haremos una prueba con las máquinas y con nuestra maquina real

Primero necesitamos putty y filezilla

una vez hecho esto abrimos putty

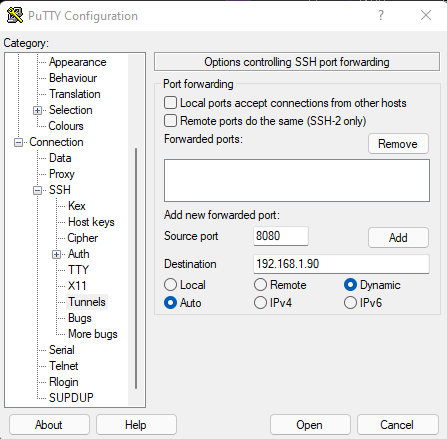


Ilustración : Túneles dinámicos

Nos iremos a SSH, le daremos al + que está a la izquierda y nos vamos a tunnels y escribimos la ip de la maquina y el puerto y luego le damos a ADD

y luego nos vamos a sesión y escribimos la ip de la máquina que es la misma ip del túnel

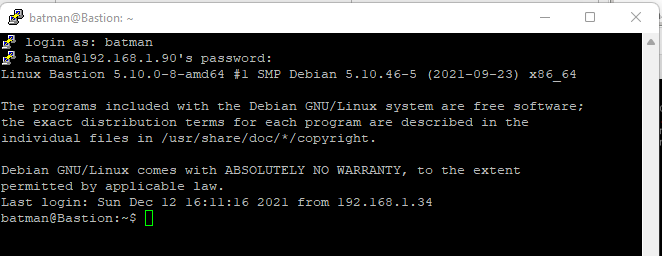


Ilustración : Conexión mediante putty

Ahora en FileZilla nos vamos a edición, opciones y luego a proxy genérico y ponemos la opción a socks 5 y ponemos la ip local que es 127.0.0.1 y el puerto 8080 ya que es el que hemos puesto en el putty

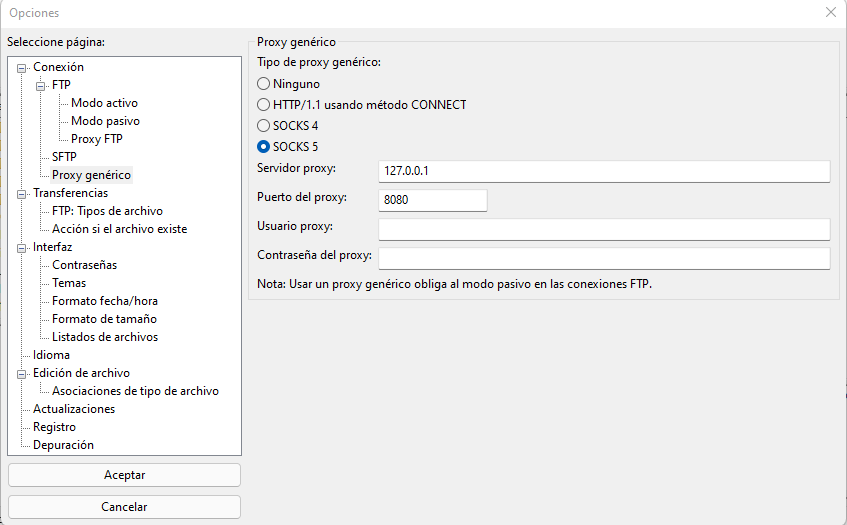


Ilustración : Socks en FileZilla

Luego le damos a aceptar y escribimos la ip de server y luego escribimos el nombre del usuario que en este caso es Robin

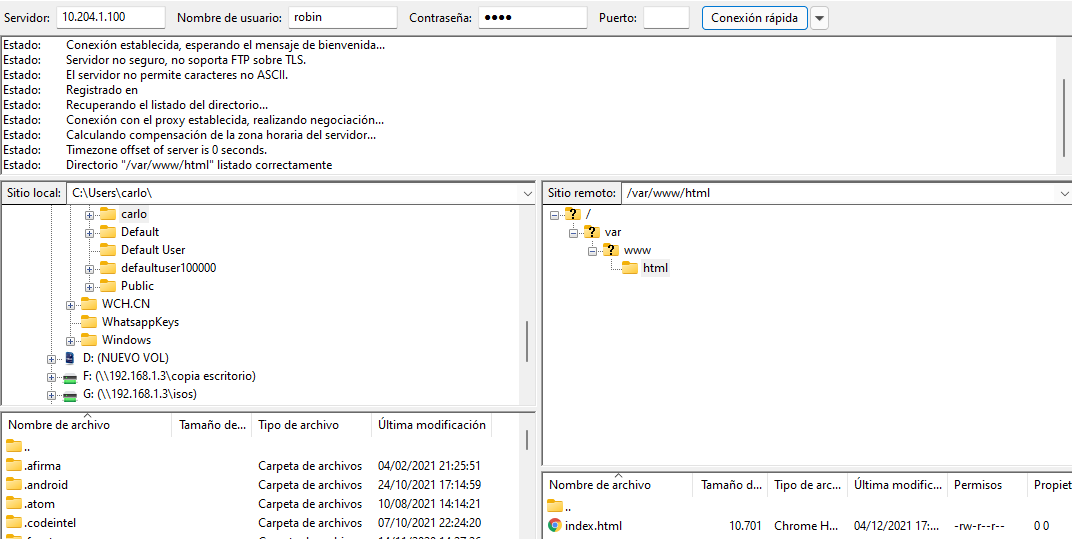


Ilustración : Conexión establecida

Una vez hecho nos copiaremos el archivo al escritorio

Una vez que tenemos el archivo copiado podemos visualizar el archivo con nuestro navegador favorito o podemos escribir la ip pero necesitamos hacer lo mismo en Firefox por ejemplo

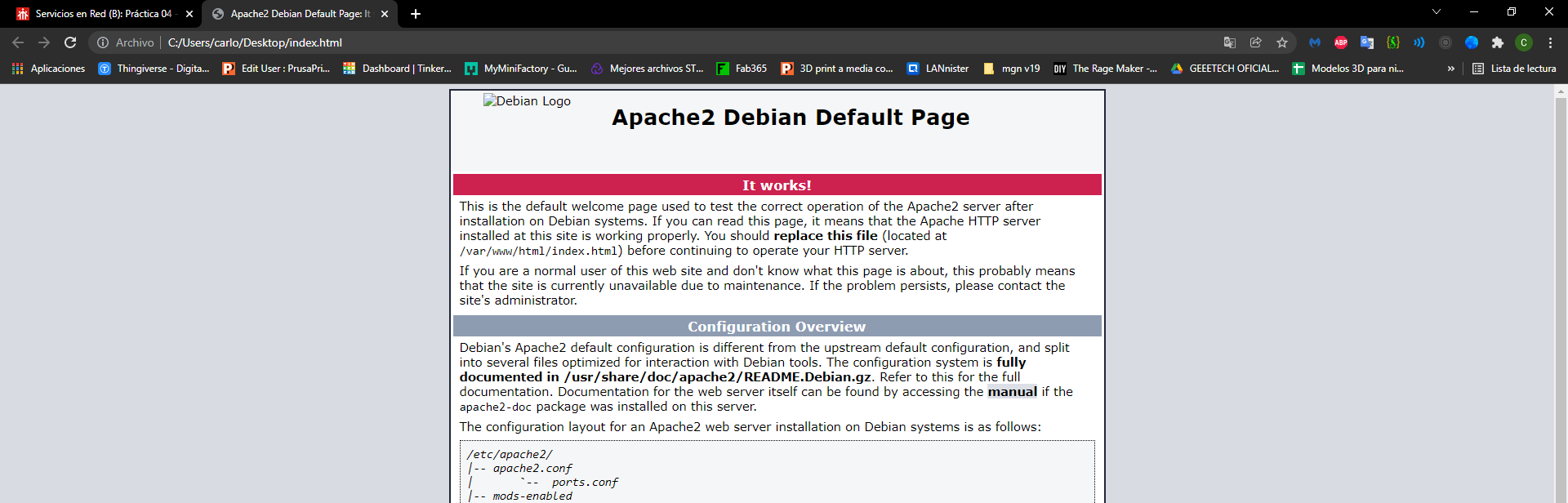


Ilustración : archivo visualizado en nuestro navegador favorito