2021

Práctica Tema 8

FRANCISCO JAVIER LÓPEZ CALDERÓN

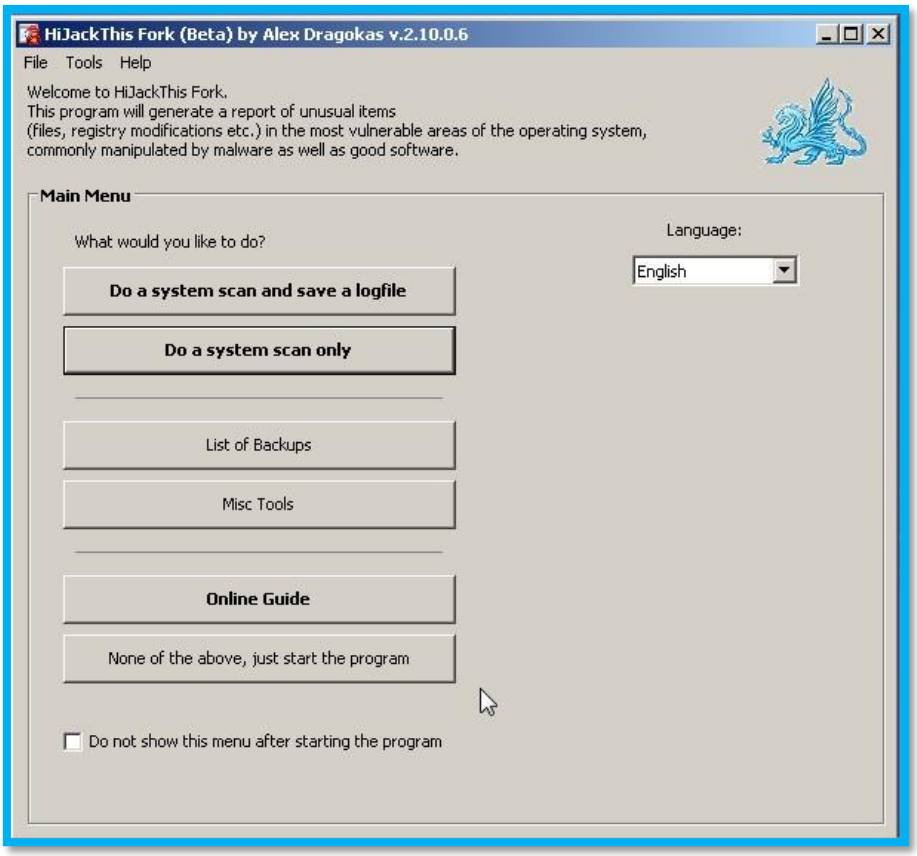
PRACTICAS UT_8.

1. PRACTICA guiada. Una vez probadas las opciones que se muestran a continuación, realizar una descripción del funcionamiento más detallada del programa. CASO PRÁCTICO 1 DEL LIBRO.

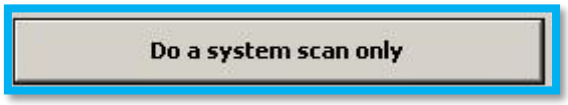
Descargar programa Hijackthis :

http://www.infospyware.com/antispyware/hijackthis/

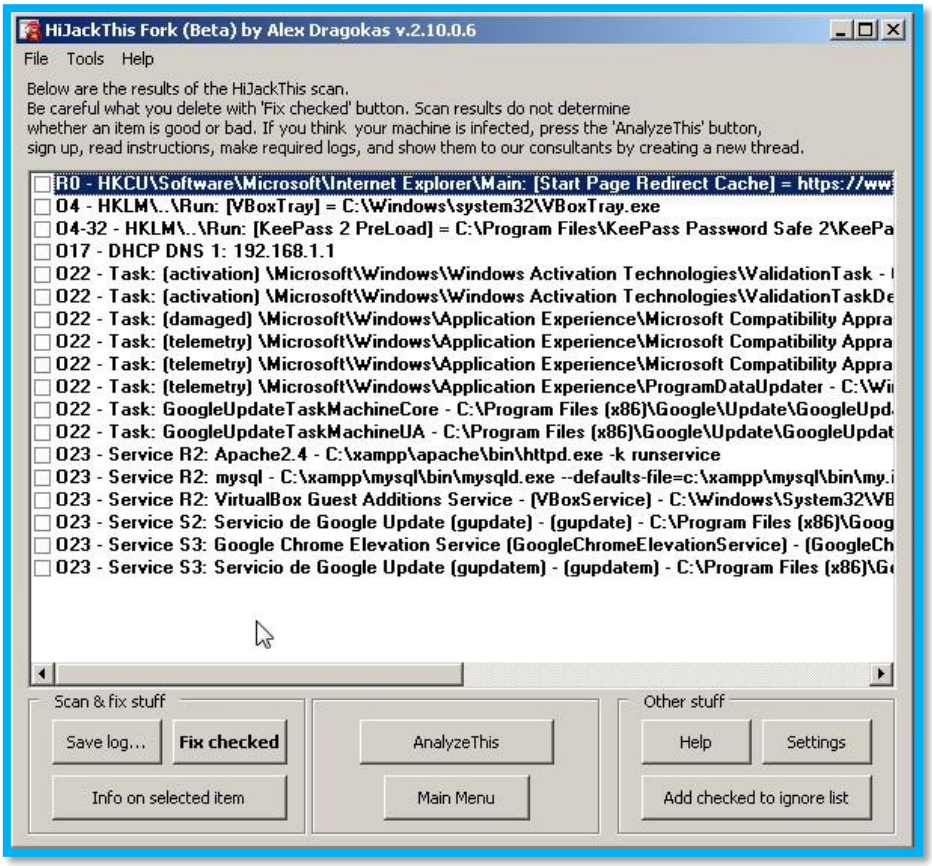
Este programa cuenta con un foro de ayuda, donde si subimos el log proporcionado por la herramienta, informará de cuáles son las referencias de los elementos causantes de los problemas de nuestro equipo y como eliminarlas, en ocasiones utilizando herramientas adicionales.
La instalación es rápida y aparecerá el menú siguiente:



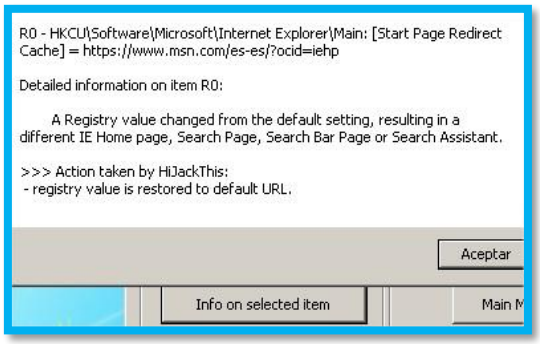
Elegimos la 2ª opción “do a system scan only”.



De forma inmediata se generará un registro como el de la siguiente pantalla.

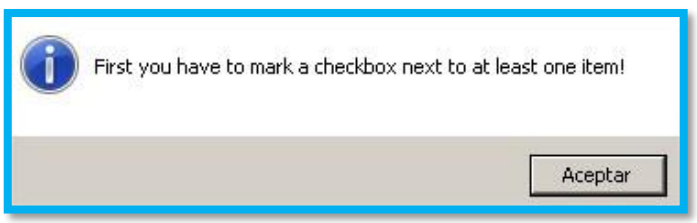


Cuando empezamos a trabajar con esta herramienta, el problema reside en detectar qué entradas son las que hay que corregir.
Para hacernos una idea de qué nos indica cada una podemos seleccionarla y pulsar **"Info on selected Item…"**
Nos mostrará una ventana similar a la siguiente donde se indica que la entrada R1 corresponde a las páginas de inicio y el asistente de busqueda del IE.



Lo más aconsejable es consultar el foro de ayuda. Las entradas que nos indican que debemos corregir son las que aparecen seleccionadas.

Si pulsamos FixChecked es para limpiar el equipo y aceptamos que los registros se borren permanentemente. Así nuestro equipo quedará libre de malware.

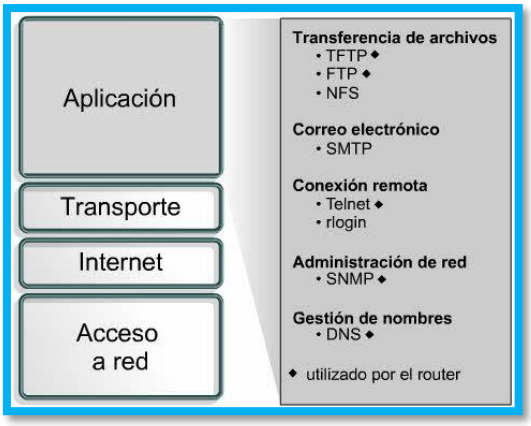


2. SERVICIO SSH

Explicación del servicio para entender las prácticas

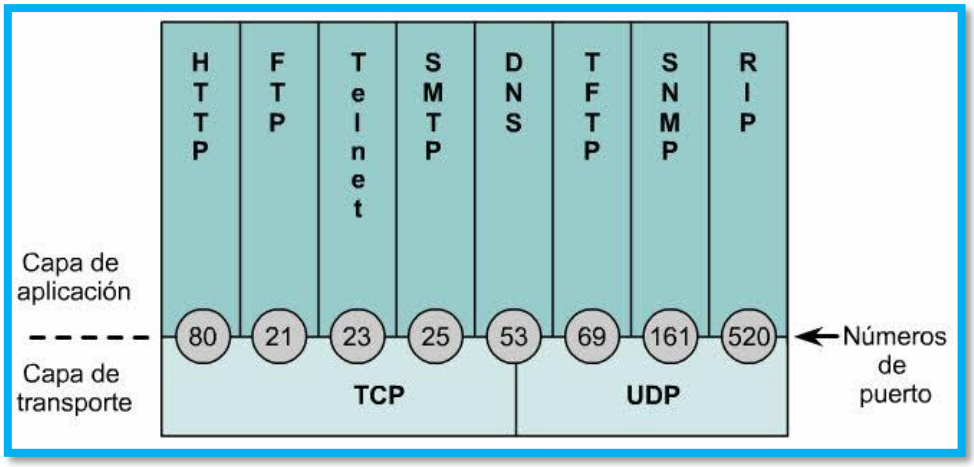
Ubicación dentro de la arquitectura TCP/IP

- En primer lugar, hay que saber en qué capa se encuentra este servicio/aplicación/protocolo dentro de la arquitectura TCP/IP. Se trata de un protocolo en la capa de aplicación, el nivel más cercano al usuario dentro de la arquitectura TCP/IP, justamente encima de la capa de transporte.



- En segundo lugar, en un entorno TCP/IP, para implementar o crear los servicios de una capa, se utilizan los servicios y protocolos de la capa inmediatamente inferior. La capa de transporte está debajo de la capa de aplicación y presta sus servicios y protocolos para que se puedan crear los servicios y protocolos de la capa de aplicación. Los protocolos utilizados en la capa de transporte TCP/IP son TCP (Transport Control Protocol / Protocolo de Control de Transporte) y UDP (User Datagram Protocol / Protocolo de Datagrama de Usuario). El servicio Ssh utiliza por defecto TCP.

- En tercer lugar, para que la capa de Transporte pueda identificar la aplicación / servicio que le está enviando los datos (en este caso Ssh), utiliza un número que llamamos puerto. Los puertos o sockets en una máquina no son más que una forma de identificar a una aplicación de red que se está ejecutando en dicha máquina. Por defecto, las aplicaciones servidoras más típicas en entornos TCP/IP, se ejecutan o, dicho de otra forma, escuchan un protocolo concreto (TCP o UDP) y un puerto concreto. El número de puerto por defecto utilizado por el Servidor Ssh es el 22.



- En cuarto lugar, hay que recordar que las aplicaciones de red diseñadas para entornos TCP/IP tienen siempre un software cliente y un software servidor.

    - Los puertos “bien-conocidos” son siempre para identificar el software servidor. El servidor generalmente está siempre a la espera (escuchando) de recibir peticiones de los clientes. Siempre escucha en un puerto concreto para que los clientes sepan a qué puerto enviar las peticiones.
    - Los clientes envían peticiones utilizando en su máquina el primer puerto libre por encima del 1.203.

Descripción del servicio Ssh

SSH (Secure SHell) **es el nombre de un protocolo de red, que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella.**

SSH trabaja de forma similar a como se hace con Telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión. Sólo sirve para acceder en modo Terminal, es decir, sin gráficos, pero a diferencia de Telnet, proporciona alguna utilidad más como la transferencia de ficheros.

PRACTICA: descargar los programas propuestos a continuación y sobre una red con maquinas virtuales probar los siguientes apartados:

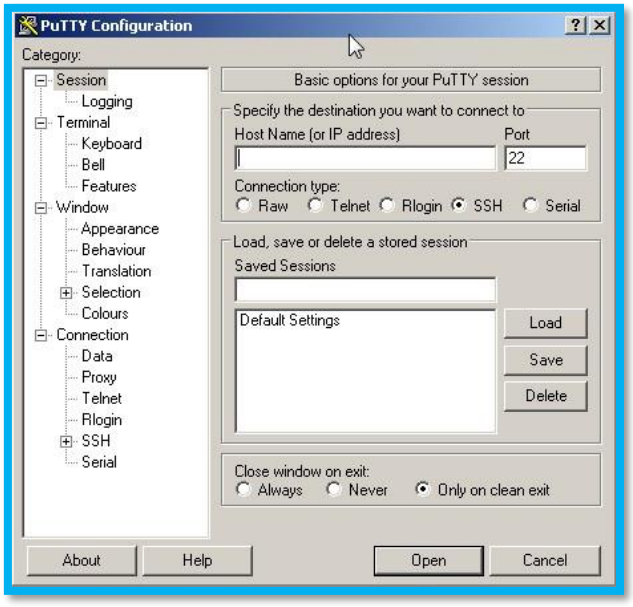
Objetivo:

- Instalar los programas y probar la conexión. El cliente debe instalarse en una máquina virtual y el servidor en otra. Investigar acerca de la generación de claves privadas y publicas con freesshd y utilizar putty con estas claves para poder conectarse vía remota. Se puede usar un programa para generar claves y poder copiarlas en una carpeta donde se guarden las claves para que desde putty puedan ser usadas. (puttygen.exe permite generar claves, entre otros)

Ssh: Software Cliente y su utilización

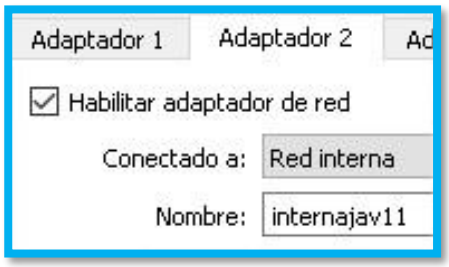
Existen muchas versiones gratuitas tanto para los equipos Windows w7 como Linux y otros. “Putty”: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

La versión de Windows es simplemente un ejecutable putty.exe que al ser ejecutado muestra:

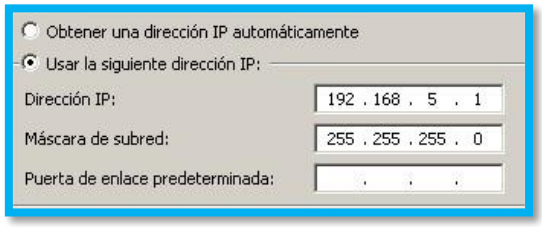


1. **Creamos una red con dos MV en W10**

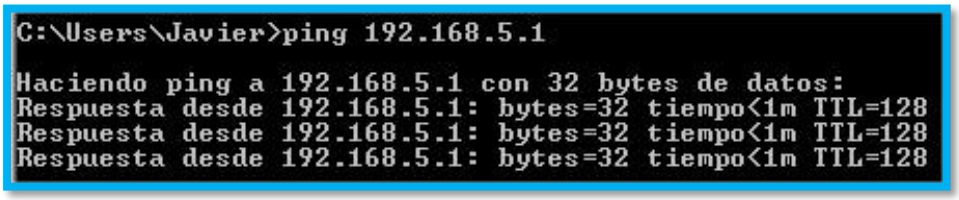
Se utilizarán dos máquinas de Windows 7, cada una de ellas tendrá 2 adaptadores de red, uno para tener conexión a Internet, otra Interna para realizar la práctica con las direcciones requeridas.



- **Una la llamaremos w10-1 con una IP: 192.168.5.1**
- **Otra la llamaremos w10-2 con una IP: 192.168.5.3**

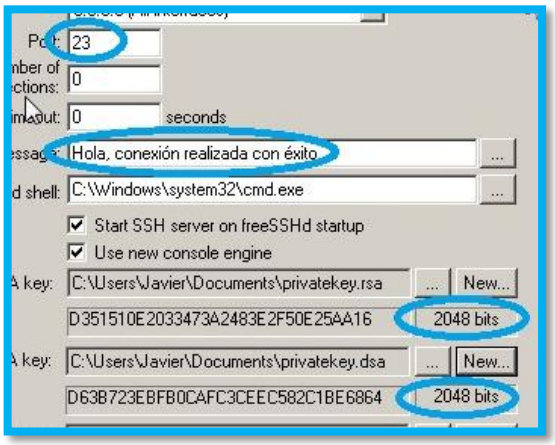


- **Comprobad que la red funciona correctamente y hay conexión entre ambas máquinas.**

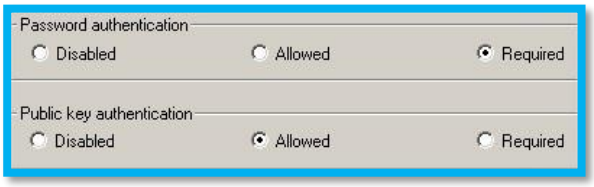


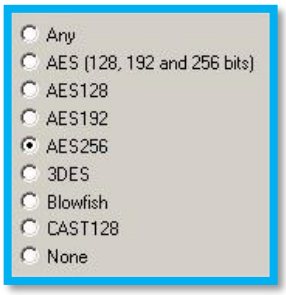
- **Desactivamos el cortafuegos de ambas máquinas.**

- **Instalamos FREESSHD en w10-1 y lo configuramos.**



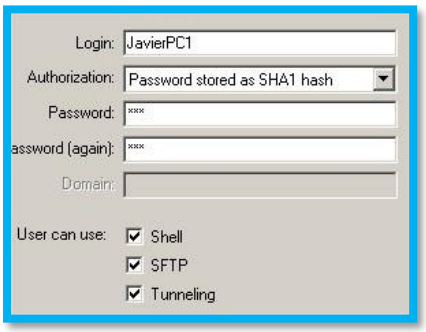
Se utilizará el puerto 23, ya que el puerto 22 nos da un error, tendrá un mensaje de bienvenida y se utilizará el cifrado más seguro (2048b)





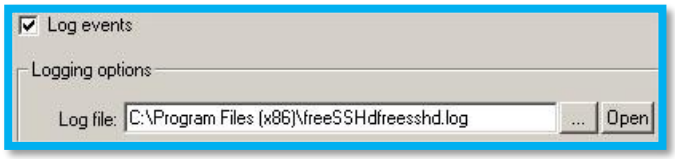
Se utilizará la encriptación "*AES256*"

Se utilizará como ruta para el cliente, el escritorio



Crearemos el usuario "*JavierPC1*" con contraseña "123"

Activaremos el log para almacenar información sobre el SSH



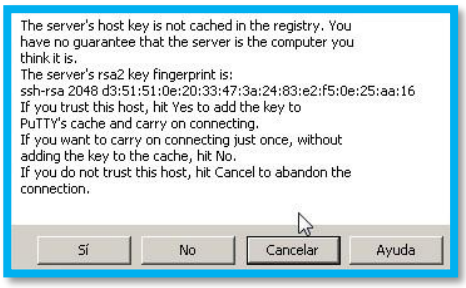
Finalmente, activaremos el servidor SSH:

- **Instalamos Putty en w10-2 y lo configuramos.**

Teniendo el servidor SSH activo en la máquina (Windows 7-1) accederemos a la máquina cliente, (Windows 7 – 2)

En host name y port, colocaremos la dirección IP del servidor SSH y su puerto.

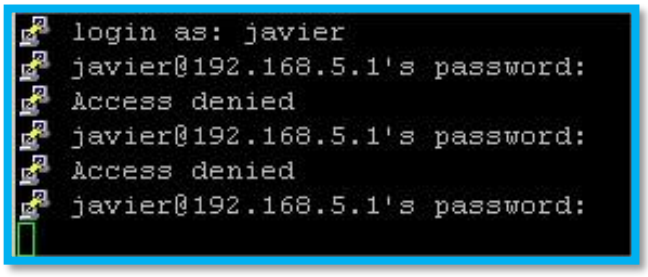
Una vez introduzcamos la información y le demos a "*ok*", nos aparecerá un aviso de seguridad, hacemos click en "*sí*"



A pesar de seguir los pasos (incluido vídeo tutorial) nos aparece un error que al parecer no tiene solución en Windows 7, en el caso de utilizar un servidor Linux podría accederse sin problema.

Dicho error sucede al introducir el usuario, este nos muestra "*acceso denegado*" no tiene solución al menos, en Windows 7. (Se ha probado distintas soluciones, como desactivar "attempt GSAPI" que a varios usuarios ha podido solucionar o crear otros usuarios, sin solución)

Sin embargo, podemos comprobar que "funciona" ya que el servidor SSH es capaz de detectar el usuario, aunque este no se conecte.



3. EJEMPLO CREACIÓN DE UNA RED PRIVADA VIRTUAL. CASO PRÁCTICO 3 DEL LIBRO

Realizar la practica guiada propuesta a continuación o configurar una VPN explicada correctamente. Una vez probados todas las opciones propuestas, realizar una VPN con tres máquina virtuales que se encuentren en distintas redes o no se encuentren conectadas entre ellas.

Buscar videos o tutoriales para crear una VPN con w10

Adjuntar documentacion y url

Ejemplo creación de una red privada virtual

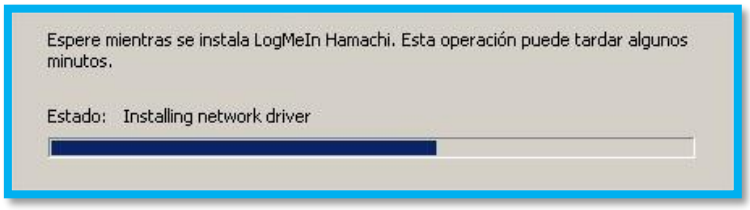
Construir una VLAN con dos ordenadores con conexión a Internet (por ejemplo 2 MV W10)

A .Descargar software Hamachi.

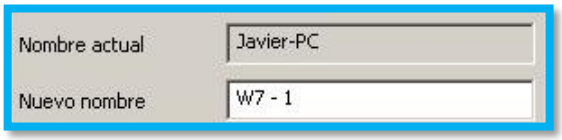
https://www.vpn.net/

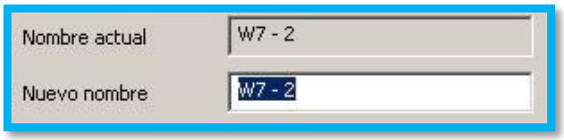
1. Instalar el programa. Durante la instalación nos avisa de que va a instalar un driver de red.

Para poder crear redes, deberemos crear y utilizar cuentas Hamachi.



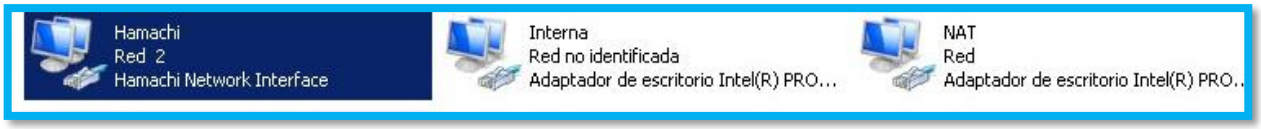
2. Una vez instalado aparece la ventana principal de la herramienta. Pulsamos en el botón inicial para crear nuestra identidad en la red. En W7/w10 nos llamaremos **W7-1/w10-1**





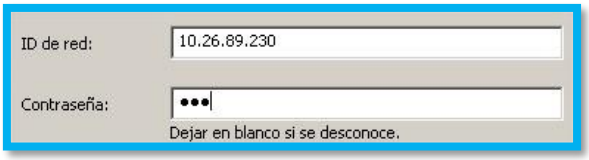
3. Hacemos lo mismo en W7-2/w10-2, esta vez con la identificación **de profesor**. Completando este paso, la ventana principal nos informa de nuestra IP en la red Hamchi. Utilizaremos esa IP para comunicarnos con los otros componentes de la VPN.

4. Si vamos a conexión de red, veremos la nueva interfaz de red llamado Hamachi.

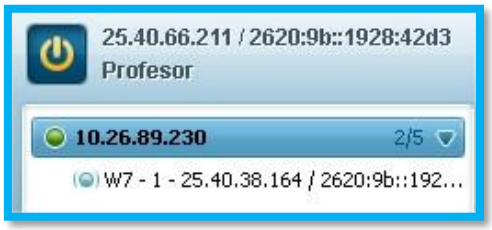


5. Para conectar los dos equipos debemos crear una red en uno y asociarse a esa red en el otro. En el ordenador del profesor pulsamos el botón crear una nueva red. Nos pedirá un nombre y una contraseña.

6. Si el nombre de la red no coincide con ningún nombre de red de otros usuarios de Hamachi, la red está creada. Vamos a W7-1 y pulsamos en unirse a una red existente. Introducimos el nombre y la contraseña



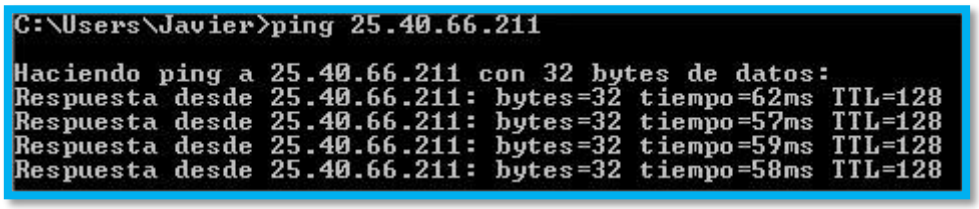
7. En la ventana principal de W7-1 aparece que estamos conectados a esa red, donde está el equipo llamado profesor.



8. En la ventana de W7-2 aparece el nuevo miembro de la red con su IP.

9. Para comprobar la conectividad podemos entrar en W7-1, hacer ping a la IP de W7-2.

Podemos comprobar su buen funcionamiento



4. PRACTICA. Para ver los servicios instalados en el sistema accedemos a ver servicios locales

4.1 Acceder a los servicios de W7/w10 y describe buscando información de los servicios que arranca automaticamente w7/w10. Probar a arrancar y detener servicios sobre una máquina virtual. UTILIZAR EL BUSCADOR DE WINDOWS PARA VER LOS SERVICIOS

En Ubuntu el manejo de servicios se llama demonios. Accedemos a los servicios desde:

Sistema/administración/servicios.

Desde la linea de comandos podemos arrancar y parar los servicios con los siguientes comandos:

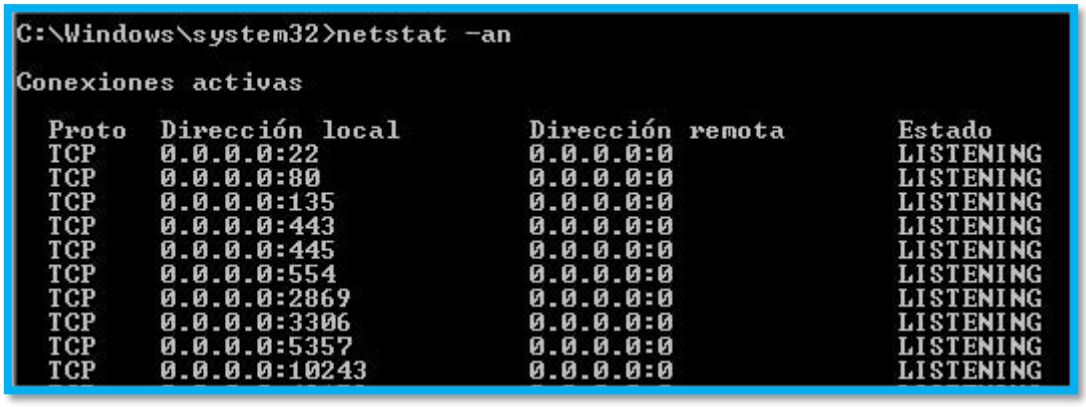
- **Start:** arranca servicio.
- **Stop:** para el servicio
- **Restart:** reinicia el servicio
- **Status:** nos informa del estado del servicio.

Los servicios instalados en el sistema se encuentran en la **carpeta /etc/init.d**

Podemos acceder a los servicios en Windows, desde su buscador, introduciendo: "services.msc"

4.2 PRACTICA

- En W7/W10 para saber quien está conectado. Abrimos el navegador y nos conectamos a alguna web. Sin cerrar el navegador, abrimos el cmd con privilegios(sobre el icono simbolo del sistema y elegir ejecutar como administrador) lanzamos el comando **netstat –an**



- Hay una fila por cada conexión, la primera columna es el protocolo (TCP, UDP). La segunda es la dirección y puerto de nuestra máquina que está conectado con la dirección y puerto de la otra máquina(tercera columna). La cuarta columna es el estado de la conexión: LISTENING significa que el puerto está abierto, está esperando una conexión; y ESTABLISHED, que se ha hecho la conexión. En nuestro ejemplo vemos que hay conexiones establecidas con un servidor web(puerto 80) y que tenemos abiertos varios puertos.

```
TCP    10.0.2.15:49574        193.146.123.113:80     ESTABLISHED
TCP    10.0.2.15:49575        193.146.123.113:80     CLOSE_WAIT
```

- Si ejecutamos **netstat –abn** aparece una quinta columna con el ejecutable de nuestra máquina que está detrás de esta conexión. Podemos confirmar que la conexión al puerto 80 la ha hecho un navegador y que los servicios de disco en red los lleva el **svchost.exe.**

```
[chrome.exe]
 TCP    10.0.2.15:49574
[chrome.exe]
 TCP    10.0.2.15:49575
[chrome.exe]
```

5. PRACTICA de simulación .

Podemos encontrar simuladores en esta o página: http://www.tp-link.es/emulators.html
Intentad configurar algún cortafuegos accediendo a la página indicada.

6. PRACTICA:

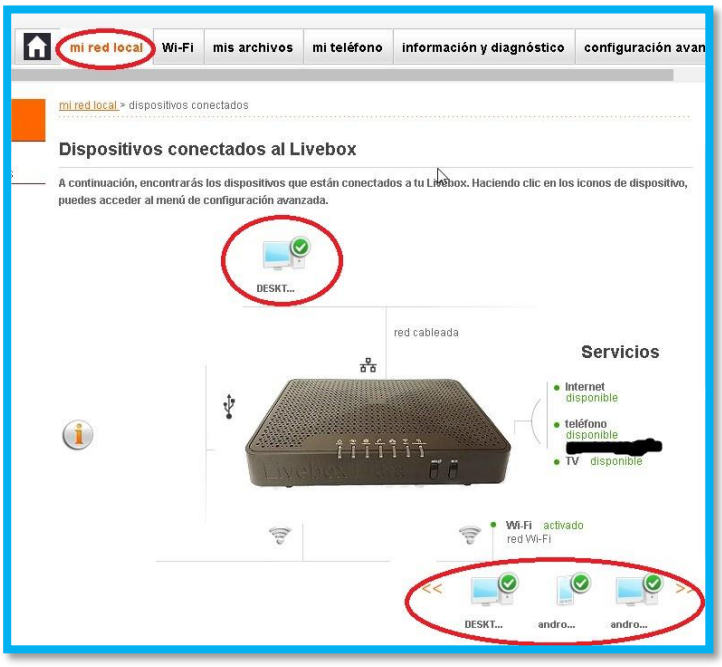
Describe graficamente explicando cada una de las pantallas la configuración de un punto de acceso inalambrico (o router ADSL o FIBRA Wi-Fi). Explica como configurar las medidas de seguridad a tomar para que sea más segura la red domestica.

Muestro la página principal del router, en ella nos muestra información útil como:

Equipos conectados.

Estado de la red.

Etc.



Es posible administrar las redes creadas y su funcionamiento, en mi caso, he creado una red secundaria específicamente para equipos que utilizan 5G.

Es muy recomendable el uso de varias redes ya que al usar todos los equipos en una misma red puede llegar a colapsar la red wifi (no la velocidad de Internet) si no su ancho de banda en la señal wifi

Normalmente, para poder acceder a estas opciones en el router, se utiliza la dirección “192.168.1.1” pero, esto puede llegar a variar, una opción para comprobar cuál es la dirección de nuestro router es ver el manual que viene junto a él o en Internet, buscar el nombre exacto del router.

Otra funcionalidad útil de los router es el poder administrar las direcciones IP a través del DHCP, seleccionar su rango, exclusiones, etc.