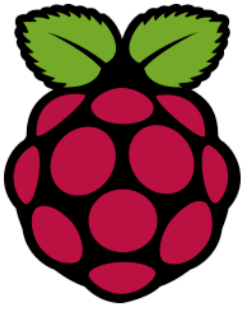
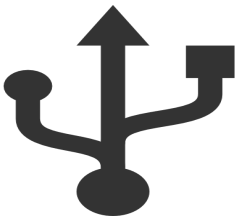
Institut Puig Castellar
Santa Coloma de Gramenet



PUNTO DE ACCESO ANÓNIMO CON USB CIFRADO

CFGS Administración de Sistemas Informáticos y Redes



Benjamín Siles y Abel Gálvez

Curso académico 2 ASIX

23-3-2018

B) GNU Free Documentation License (GNU FDL)

Resumen del proyecto:

Configuración de una raspberry para que actúe como un punto de acceso wifi, en el que los clientes que se conecten tengan acceso a internet de forma anónima. La raspberry será capaz de redirigir el tráfico interno a la red externa de forma anónima.

Configuración de un USB cifrado el cual solo se podrá descifrar a través de la raspberry, además permitirá descargar o subir archivos y documentos para poder compartirlos vía red local.

Abstract:

Configuration of a raspberry to act as a Wi-Fi access point, in which the clients that connect have access to the internet anonymously. The raspberry will be able to redirect internal traffic to the external network anonymously.

Configuration of an encrypted USB which can only be decrypted through the raspberry, in addition to downloading or uploading files and documents in order to share them via local network.

Palabras clave:

Raspberry

Red Anónima

USB

Cifrado

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

Implementación de un USB cifrado, que sea accesible a través de una red local en el mismo momento de enchufarlo sobre la raspberry. Este pendrive permitirá almacenar y compartir la información a través de la raspberry.

Implantación de un punto de acceso a la red Tor a través de un dispositivo Raspberry Pi, los usuarios que se conecten al dispositivo podrán navegar por Internet de forma totalmente anónima. El dispositivo debe estar correctamente ensamblado mediante una carcasa impresa en 3D.

De esta manera los profesores podrían llevar toda la asignatura en un único pendrive y conectarlo en la raspberry donde se tendría un acceso seguro al mismo, además la posibilidad de utilizar la raspberry para navegar de forma segura desde el aula.

Antes de este contexto del trabajo hubo otro el cual se encontrará en el anexo 9.1

1.2 Objetivos del Trabajo

- Creación de un punto de acceso seguro con raspberry pi 3
- Creación de un USB cifrado que la Raspberry diera acceso para poder llegar y descargar los archivos que contendrá.

1.3 Planificación del proyecto y metodología

1.3.1 Fragmentación del Proyecto

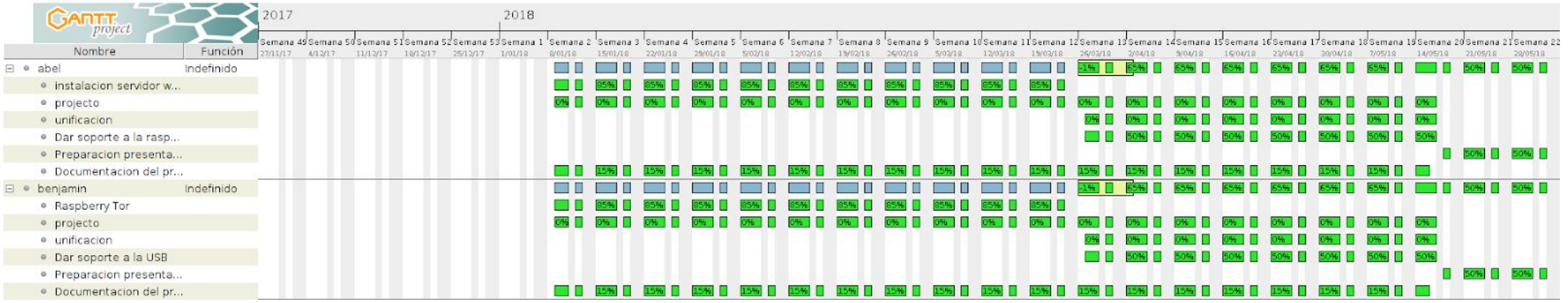
Este proyecto se diferencia en dos partes, esto se hizo así para que cada uno de los integrantes del grupo hiciera el apartado pertinente, para separar la parte de la configuración de la raspberry como el USB WEB Server.

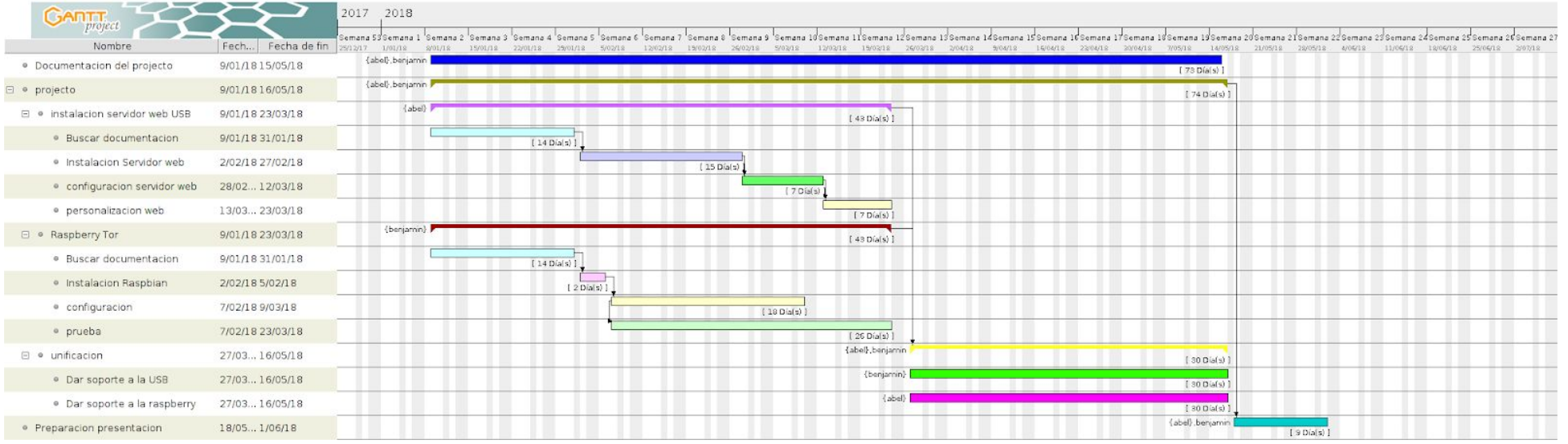
1.3.2 Explicación diferenciación entre versiones

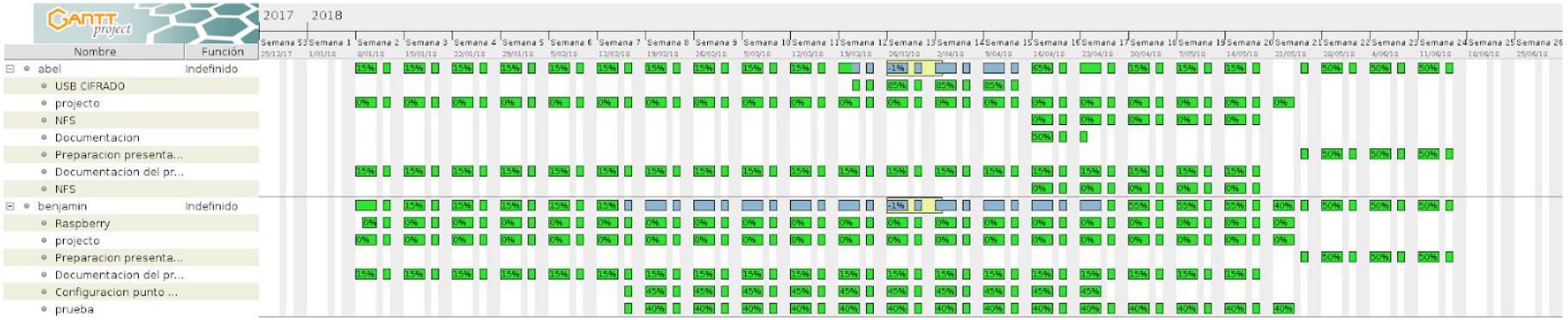
Por desgracia la parte del USB WEB Server no se consiguió finalizar con éxito, siendo así abandonada y sustituida por el apartado USB cifrado, de esta manera ambos integrantes del grupo no se verían afectados por el fallo inesperado del USB WEB Server.

1.3.3 Versiones

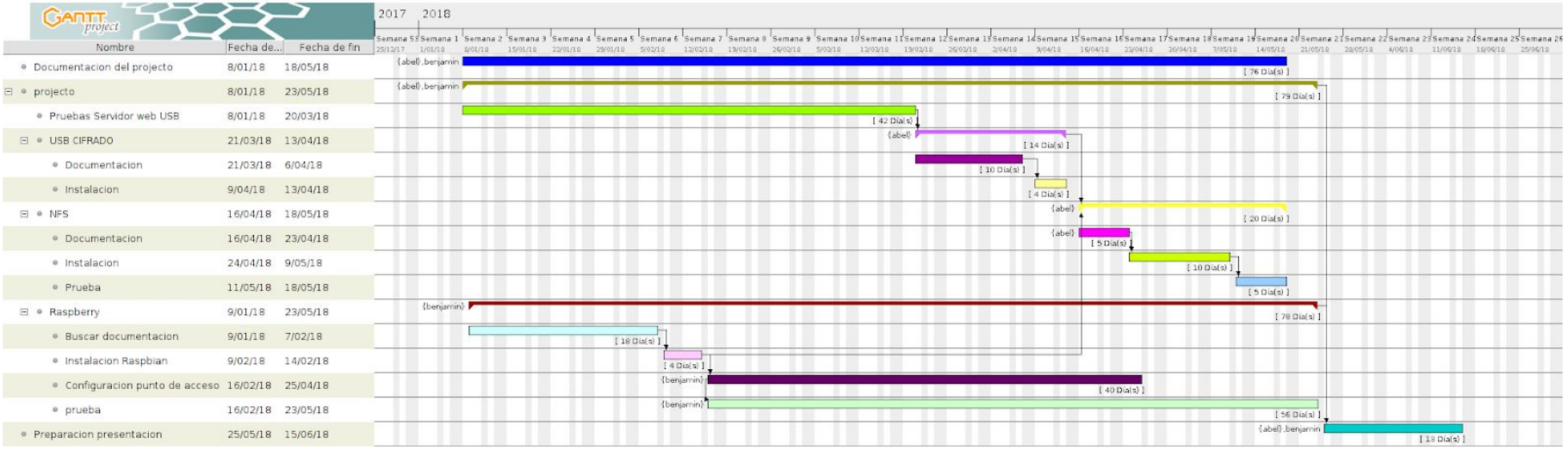
Primera Versión:


GANTT project
2017
2018
Nombre
Función
abel
Indefinido
instalacion servidor w...
projecto
unificacion
Dar soporte a la rasp...
Preparacion presenta...
Documentacion del pr...
benjamin
Indefinido
Raspberry Tor
projecto
unificacion
Dar soporte a la USB
Preparacion presenta...
Documentacion del pr...


GANTT project
2017
2018
Nombre
Fech...
Fecha de fin
Documentacion del projecto 9/01/18 15/05/18
projecto 9/01/18 16/05/18
instalacion servidor web USB 9/01/18 23/03/18
Buscar documentacion 9/01/18 31/01/18
Instalacion Servidor web 2/02/18 27/02/18
configuracion servidor web 28/02... 12/03/18
personalizacion web 13/03... 23/03/18
Raspberry Tor 9/01/18 23/03/18
Buscar documentacion 9/01/18 31/01/18
Instalacion Raspbian 2/02/18 5/02/18
configuracion 7/02/18 9/03/18
prueba 7/02/18 23/03/18
unificacion 27/03... 16/05/18
Dar soporte a la USB 27/03... 16/05/18
Dar soporte a la raspberry 27/03... 16/05/18
Preparacion presentacion 18/05... 1/06/18
{abel},benjamin
[73 Dia(s)]
[74 Dia(s)]
{abel}
[48 Dia(s)]
[14 Dia(s)]
[15 Dia(s)]
[7 Dia(s)]
[7 Dia(s)]
{benjamin}
[48 Dia(s)]
[14 Dia(s)]
[2 Dia(s)]
[10 Dia(s)]
[26 Dia(s)]
{abel},benjamin
[30 Dia(s)]
{benjamin}
[30 Dia(s)]
{abel}
[30 Dia(s)]
{abel},benjamin
[9 Dia(s)]



Segunda Versión:



1.4 Breve sumario de productos obtenidos

- Pendrive 16GB 8€
- Raspberry pi 3 37€
- Ventiladores Raspberry pi 3 8€
- Cargador Raspberry 4€
- Tarjeta SD 16GB 15€
- Carcasa para la Raspberry pi 3 Impresa en 3D.

1.5 Breve descripción de los otros capítulos de la memòria

1.5.1 Punto de Acceso Anónimo

Crear un punto de acceso wifi anónimo con el que poder conectarnos a internet de forma segura.

1.5.2 Servidor Web USB

Creación de un USB con un Servidor Web auto-contenido que permitirá conectarse a él desde cualquier lugar.

ATENCIÓN:

Idea desechada ya que la tecnología actual no permite la creación de un USB con un servidor web que sea compatible con Ubuntu.

1.5.3 USB Cifrado

Creación de un USB cifrado al que sólo se podrá acceder desde la raspberry, con la contraseña adecuada para descifrarlo, para descargar el contenido del mismo.

1.5.4 NFS en Raspberry para el USB Cifrado

Instalación de NFS sobre la raspberry con el sistema Raspbian, para dar acceso sobre el USB a los clientes que deseen descargar o modificar los archivos del mismo directamente desde sus ordenadores clientes.

2. Punto de acceso anónimo

2.1 ¿Qué es una Raspberry?

Una raspberry es un placa de ordenador reducida, desarrollado en Reino Unido por la Fundación Raspberry Pi. Este mini ordenador fue creado para fomentar la enseñanza de la computación en las escuelas.

La raspberry cuenta con diversos modelos:

1. Raspberry Pi 1 Modelo A(2012).

   Fue la primera raspberry en salir. Carecía de puerto Ethernet. Poseía 26 conectores GPIO, salida de vídeo vía HDMI y Video RCA, un conector Jack de 3.5 milímetros, un único conector USB, MicroUSB (De alimentación) y un conector de cámara. Su procesador fue un 'Broadcom BCM2835', Single-Core a 700MHz. También tuvo 256 MB de RAM y una gráfica Broadcom VideoCore IV. Requería de una fuente de alimentación externa.

2. Raspberry Pi 1 Modelo B y B+(2012).

   Una variante del modelo A que trajo consigo diversas mejoras, la inclusión del doble de memoria RAM pasando a 512MB, además un puerto USB más y un conector Ethernet RJ-45.
   Tiempo después se lanzó el Modelo B+, que incluyó 4 puertos USB y pasó de usar una SD a una MicroSD.

3. Raspberry Pi 2 Modelo B(2014).

   Este modelo no incluye el mismo procesador usado en los tres anteriores modelos, el nuevo es la 'Broadcom BCM2836' que pasa de tener 1 núcleo a 4 y de 700MHz a 900MHz.
   La memoria ram pasa a tener 1GB compartida con la gráfica. También incluye 40 pines GPIO, y suprime la conexión RCA.

4. Raspberry Pi 3 Modelo B(2016).

   Este modelo renueva procesador con 4 núcleos y 1,20 GHz y una la inclusión de wifi y Bluetooth 4.1 sin necesidad de adaptadores.

5. Raspberry Pi 3 Modelo B+(2018).

   Este modelo es el más nuevo y incluye una mejora de cpu que pasa de 1.2GHz a 1,4GHz, la conexión wifi pasa a tener doble banda (2,4G y 5G), un nuevo puerto ethernet que pasa a un ancho de banda de 300Mb/s y también cuenta con Bluetooth 4.2 y Bluetooth BLE.

6. Versiones aún más pequeñas que las anteriores.

   a. Raspberry PiZero(2015).

      Este modelo tiene un CPU “Broadcom BCM2835”, que funciona a 1GHz con un solo núcleo. Posee 512MB de RAM, y comparte la gráfica VideoCore IV. Debido a su tamaño sustituye el puerto HDMI por MiniHDMI, manteniendo así las prestaciones. Tampoco usa USB estándar, sino que tiene dos MicroUSB, uno de alimentación y otro de datos. Posee salida RCA, pero en vez de por clavija son solo dos conectores integrados en la placa. Usa MicroSD como sistema de almacenamiento.

   b. Raspberry PiZero W.

      Es la sucesora de la PiZero, la W en su nombre es porque incluye wifi y bluetooth integrados.

A la Raspberry se le puede conectar una pantalla, un teclado y un ratón, pero la micro sd que es donde llevará instalado su sistema es prácticamente obligatoria.

Este mini ordenador tiene muchas utilidades debido a su bajo consumo eléctrico, su tamaño y su precio

2.2 ¿Qué es Hostapd?

El HOSTAPD es un servicio que sirve para convertir un sistema en un punto de acceso utilizando la tarjeta de red wifi para que las máquinas clientes puedan conectarse y dar acceso internet a través de él.

2.3 ¿Qué es un punto de acceso?

Un punto de acceso es una red de área local inalámbrica.

El punto de acceso se conecta a un router, switch o hub por un cable Ethernet o wifi, y a través de una tarjeta inalámbrica proyecta una señal Wi-Fi para que otros dispositivos puedan conectarse a él.

Un punto de acceso se puede utilizar como un repetidor de la red wifi o crear su propia red, si lo usamos como otra red diferente se necesita de un servidor DHCP que otorgará las direcciones IP, el gateway, el servidor DNS entre otros servicios.

2.4 ¿Qué es la navegación anónima?

La navegación anónima sirve para poder navegar por internet sin que se pueda identificar a la persona o dispositivo que accede a cualquier clase de servicio que se encuentra por internet.

Para poder navegar de forma anónima hay muchas maneras de hacerlo, pero las más populares y/o conocidas son TOR e I2P.

TOR e I2P sirven en la práctica para lo mismo navegar de forma anónima, saltarse el bloqueo que los gobiernos aplican a ciertas páginas de internet, etc… La manera de acceder a internet de cada una es diferente.

TOR(Onion):

TOR es un acrónimo formado por las palabras “The Onion Router”, y su traducción vendría a ser enrutamiento de cebolla.

El software TOR es libre y su función es hacer que las comunicaciones entre un cliente y un servidor se hagan mediante lo que se denomina el enrutamiento de cebolla.

Funcionamiento de TOR:

> Tor utiliza el método de enrutamiento de cebolla que le permite cifrar los datos que circulan por Internet en múltiples capas, como una cebolla. A continuación, envía los datos a través de diferentes nodos, cada uno de los cuales se encarga de una capa hasta que el paquete de datos que hemos enviado llega a su destino.

Pero aun asi TOR no es perfecto, porque si se navega por http y no por https la seguridad queda comprometida, porque con TOR se oculta de dónde viene y a dónde va

dirigido el paquete pero no el contenido, de eso se encarga el https.

Si se navega por la red TOR y se loguea en cualquier página, como el correo o el banco no sirve de mucho tener TOR porque de todas maneras se está indicando quién eres, y se puede averiguar desde dónde se navega, por eso es mejor utilizar TOR para cosas concretas como acceder a paginas bloqueadas por el gobierno.

I2P(Garlic):

I2P es una sigla formada por las palabras “Invisible Internet Project”, y su traducción vendría a ser Proyecto de Internet Invisible.

El software I2P es libre y su función es ofrecer una capa de abstracción para las comunicaciones entre distintos ordenadores.

Funcionamiento de I2P:

I2P utiliza túneles de entrada y salida entre el cliente y el servidor. Cada túnel está compuesto por una secuencia de nodos padres, los cuales solo transportan la información en un único sentido (unidireccional).

I2P es compatible con la tecnología P2P, porque en sí utiliza P2P.

2.5 ¿Qué son las iptables?

Las iptables son un comando del sistema linux que permite gestionar su firewall.

El firewall es el que se encarga de bloquear las conexiones entrantes como salientes del sistema.

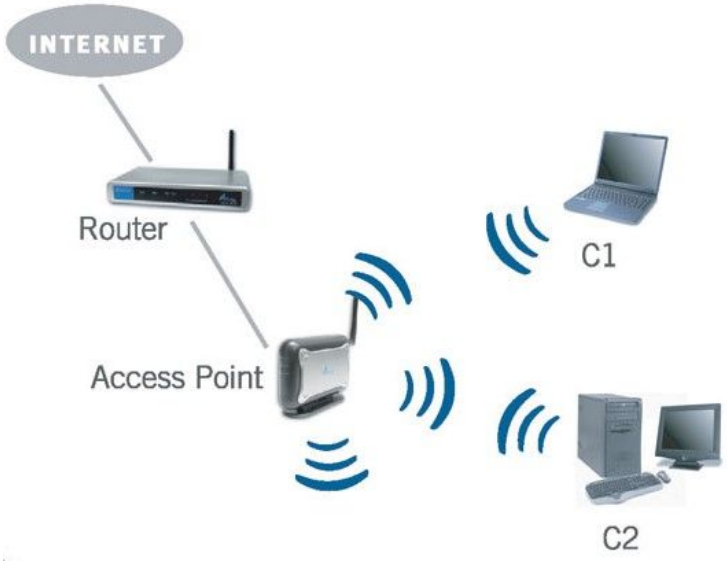
2.6 Creación de un punto de acceso anónimo

Sabiendo ya para qué sirve y que es cada una de las tecnologías anteriores, se puede crear un punto de acceso anónimo que de acceso a internet a los usuarios conectados por wifi.

Para la creación del punto de acceso se utilizará la raspberry pi3/pi3+, dado que estas versiones tienen una tarjeta ethernet y wifi; se usará el wifi para otorgar internet a los usuarios y por la tarjeta ethernet poder salir a internet. De esta manera no se

necesitará un dispositivo específico para otorgar una conexión por wifi.

En el diagrama se puede observar como la raspberry accede a internet, como los clientes se conectan a través de la interfaz wifi a la raspberry y acceden a internet.



Fuente: https://4.bp.blogspot.com/-B27MDtDLtrk/V42vxnfBWzI/AAAAAAAADFA/HEYaeHjggMISGymBe3yO4nrdGDdnaZ6vQCLcB/s1600/ap421w_diagrama.jpg

En la tarjeta SD se instalará el sistema RASPBIAN, que es el sistema linux que se usará para poder configurar e instalar una serie de servicios, además se usará la versión recomendada por que tiene la interfaz gráfica instalación raspbian.

Al tener instalado el sistema RASPBIAN, lo que se debe hacer para obtener una mayor seguridad dentro de la raspberry es cambiar las contraseñas de los usuarios que tiene el sistema por defecto más información.

Para poder manejar el sistema desde otra maquina por si se necesita acceder remotamente, se procede a instalar el servidor SSH que es un servicio con el que se podrá iniciar sesion en la raspberry desde cualquier máquina y poder administrar el estado de la misma raspberry más información.

Ahora la raspberry se encuentra lista para crear el punto de acceso anónimo. Primero se configura la interfaz de red wifi para otorgarle una dirección IP estática, que será la red interna que tendrá el punto de acceso con el que se usará para poder configurar el servidor DHCP y el servicio HOSTAPD más información.

A partir de la dirección IP estática en la tarjeta de red wifi se procederá a configurar e instalar el servicio DHCP para poder otorgar una dirección IP interna, el servidor DNS (Servidor de nombres de dominio), e indicarles la dirección de su puerta de enlace con el que podrán acceder a internet los clientes que se conecten al punto de acceso más información.

Para lograr que se puedan conectar a la raspberry, se procede a instalar y configurar el servicio hostapd, con el que la tarjeta wifi de la raspberry pasará de ser una tarjeta normal de wifi a un punto de acceso, con el que las máquinas que tengan una interfaz wifi puedan acceder a la red más información.

Para lograr que los clientes conectados al punto de acceso puedan navegar de forma anónima, lo que se debería de hacer es instalar y configurar I2P o TOR.

Para averiguar cuál de los dos servicios proporciona un acceso anónimo a la red de forma más segura y rápida, se opta por probar ambos servicios con lo que se empezará a probar el servicio TOR y luego el servicio I2P.

2.6.1 TOR

Para poder comenzar a utilizar la red TOR lo que se debe hacer primero es instalarlo y configurarlo para que los clientes puedan navegar de forma anónima por internet instalación y configuración.

Pero no basta con tener el servicio instalado y configurado lo que se debería hacer ahora es configurar las IPTables. Con las IPTables lo que se hará es redireccionar las conexiones de los clientes y salir a internet a través de la red TOR, con lo que se consigue que los clientes puedan navegar anonimamente por internet IPTables.

Con todo lo anterior configurado lo que toca ahora es comprobar que se puede acceder a internet y que realmente se accede a internet anónimamente pruebas.

En un principio para las pruebas de seguridad se optó en utilizar los programas arachni, ZAP y burp suite, pero a la hora de realizar las pruebas se descartaron más información.

Dato interesante:

La red funciona a partir de organizaciones e individuos que ceden su ancho de banda y poder de procesamiento. Según información que se recuperó

de los documentos de alto secreto filtrados por Edward Snowden en 2013, la Agencia de Seguridad Nacional de Estados Unidos (NSA) habría, supuestamente, conseguido acceder a la información de Tor y así poder descubrir las identidades de los usuarios anónimos que la utilizan.

2.6.2 I2P

Para poder usar el servicio i2p se debe de instalar el programa y configurarlo para dar conexión a los clientes instalación.

A la hora de instalar el programa surgieron diversos problemas de los cuales no se pudo lograr que los clientes puedan acceder a internet, debido a eso y a falta de tiempo se decidió parar y seguir con el servicio TOR más información.

3. Servidor Web USB

Por diferentes inconvenientes con la creación del servidor web en el USB se ha decidido que, en vez de hacer un servidor web se creará un USB cifrado que se desbloquee al conectarlo a la raspberry y esta dará los servicios para poder coger cualquier archivo del USB.

INCONVENIENTES

- XAMPP lite

  Se abandonó ya que no se encontró la manera de hacerlo funcionar en Ubuntu.

- Dokuwiki

  Al conectar el USB tras solucionar todos los problemas que aparecieron, el SO (Sistema Operativo) Ubuntu no reconoció el USB.

- PHP7

  Al cambiar a la versión anterior funcionaba, pero solo al ejecutar el comando "`sudo apt-get install libxml2-dev`".

- XAMPP

  Se descartó porque no se encontraron garantias de éxito suficientes que justificaran el tiempo y esfuerzo necesario.

- Apache, php y MySQL

  Al querer instalar dokuwiki, el navegador web no instalaba dokuwiki.

- Cambio punto de montaje

  Nunca funcionó, el USB no se montaba en la dirección especificada.

Para más información de los problemas acontecidos mirar Anexos 9.2.

4. USB Cifrado

4.1 ¿Qué es el Cifrado?

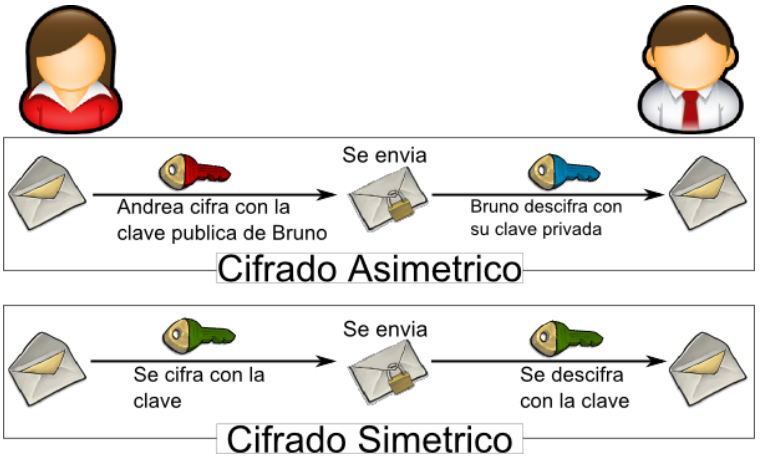
El cifrado es un proceso que utiliza distintos algoritmos con un sistema de claves para transformar un mensaje, archivo, imágenes u otras formas de comunicación, de tal forma que sea incomprensible, o simplemente pase desapercibido a ojos de un tercero que no entre en la comunicación cifrada, ya que dicha persona no tendría las claves necesarias de los algoritmos. Las claves de cifrado y descifrado pueden ser iguales (criptografía simétrica) o distintas (criptografía asimétrica).

4.2 Tipos de cifrado según sus claves

Los tipos de cifrados según sus claves se dividen en dos tipos, simetricos y asimetricos.

Simétricos: Utilizan la misma clave para cifrar y descifrar.

Asimétricos: Utilizan claves distintas para cifrar y descifrar, una clave pública que sirve para cifrar y una clave privada que sirve para descifrar.



Fuente:
https://gilbertsecure.files.wordpress.com/2011/07/seguridad1.jpg

La forma de utilizar un sistema simetrico o asimetrico depende del tipo de tarea a cumplir.

La criptografía asimétrica presenta dos ventajas sobre la criptografía simétrica:

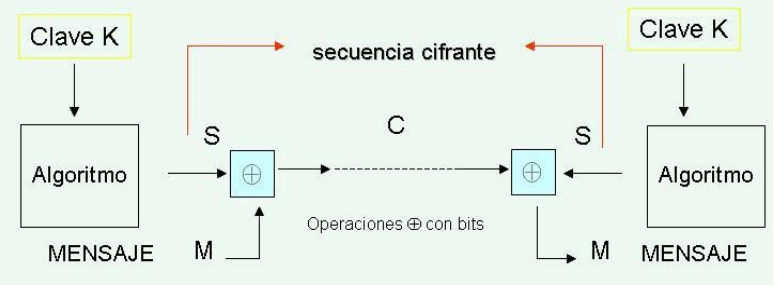
1. Suprime el problema de la transmisión segura de la clave.
2. Permite la firma electrónica.

Sin embargo no reemplaza los sistemas simétricos, ya que los tiempos de cálculo son más cortos con los sistemas simétricos que con los asimétricos.

4.3 Tipos de cifrado según sus algoritmos

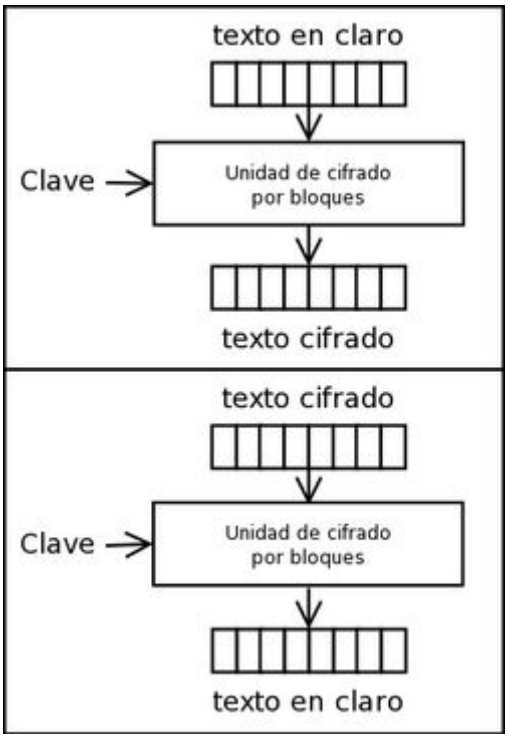
Los tipos de cifrados según sus algoritmos también se dividen en dos tipos.

En flujo: En este tipo los algoritmos se realizan bit a bit. Están basados en la utilización del cifrado simétrico, con claves verdaderamente largas. Estas claves pueden estar predeterminadas o generarse de manera pseudoaleatoria, que genera una secuencia binaria a partir de una clave de inicialización.



Fuente: https://www.researchgate.net/profile/Alejandro_Padron-Godinez/publication/309357528/figure/fig1/AS:423672130347011@1478022715954/Figura-11-Esquema-general-del-Cifrado-de-Flujo-Como-se-menciono-al-inicio-de-esta.jpg

Por bloques: En este tipo de algoritmos se realizan bloque a bloque. Para empezar se descompone el mensaje en bloques de la misma longitud. Tras ello cada bloque se convierte en un bloque del mensaje cifrado mediante una secuencia de operaciones.



Fuente: https://www.krypton.ovh/imgw/Cifrado_por_bloques.png

Este tipo de algoritmos pueden ser tanto de clave simétrica como asimétrica.

4.4 USB Cifrado

USB cifrado con el sistema LUKS.

Este sistema a sido elegido por su capacidad de encriptar el USB al completo, y por su sencilla compatibilidad en raspbian.

Con este sistema solo habrá que conectar el USB a la raspberry pi y escribir la contraseña para desencriptar, además memoriza de forma simple la contraseña, para que sea más sencillo la conectividad con raspbian.

Se encontró un fallo en este proceso ya que el SO Raspbian no aceptaba guardar la contraseña, se consiguió solucionar sin afectar sobremanera el desarrollo del proyecto.

Para ver como configurar el USB con este sistema y la solución que se aplicó mirar Anexo 9.16 y 9.17.

4.5 ¿Qué es LUKS?

LUKS (Linux Unified Key Setup) es una especificación de cifrado de disco creado por Clemens Fruhwirth. Lo bueno de LUKS es que especifica un formato estándar en disco. Esto facilita la compatibilidad y la interoperabilidad entre programas, además también garantiza que puedan implementar gestión de contraseñas en lugar seguro y de manera documentada.

La referencia que acoge LUKS se basa en una versión mejorada de cryptsetup, utilizando dm-crypt como interfaz para el cifrado de disco.

Dato interesante:

En septiembre de 2013, Phoronix publicó una comparativa de rendimiento entre LUKS y eCryptfs: Haciendo uso la versión de Ubuntu 13.10, se obtuvo mejor rendimiento encriptando todo el disco con LUKS, que solo el directorio de datos de usuario con eCryptfs.

4.6 ¿Cómo interviene el cifrado en el proyecto?

El cifrado interviene en el hecho de, si se pierde el pendrive, nadie pueda sustraer la información, ya que en el único lugar en el que podría extraerse sería desde la propia raspberry. Esto no excluye que el pendrive no se pueda descifrar desde otra máquina, cualquier máquina Ubuntu podría servir para descifrarlo siempre que tenga LUKS y la propia contraseña para ello, por eso se aconseja no utilizar la contraseña de este proyecto, ya que es simple y fácil de descifrar.

5. NFS en Raspberry para el USB Cifrado

5.1 ¿Qué es NFS?

NFS o Network File System (Sistema de archivos de red), es un protocolo a nivel de aplicación, según el modelo OSI. Se utiliza para el compartimiento de archivos en un área local de ordenadores. Permite acceder a ficheros remotos, a diferentes tipos de sistemas conectados a una misma red, como si fueran de la misma máquina.

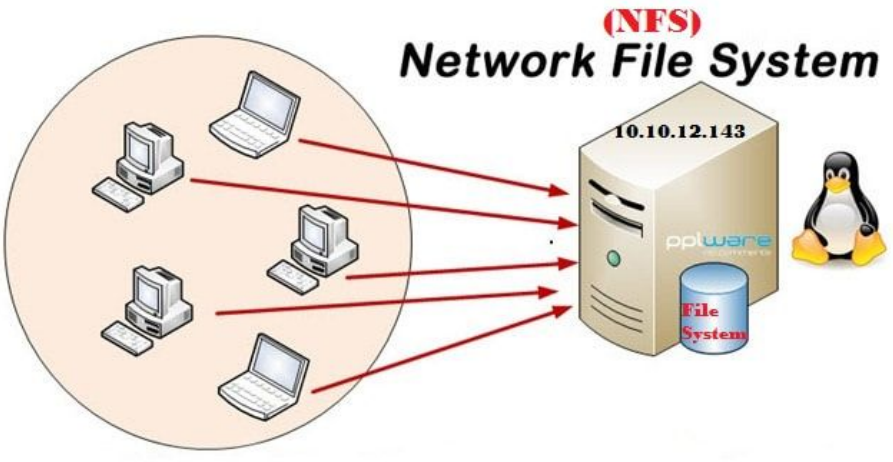
Está dividido en dos partes principales un servidor y uno o varios clientes.

Los clientes acceden de forma remota a los ficheros que se encuentran almacenados en el servidor.

Los ordenadores locales utilizan menos espacio de disco ya que los datos se encuentran centralizados en un servidor, pero pueden ser accedidos y modificados por varios usuarios del área local en el que se encuentra el servidor.

También se pueden compartir a través de la red o dispositivos de almacenamiento como USB, CD-ROM, unidades ZIP entre otros. Esto permite aprovechar el espacio del servidor para otras ocupaciones sin llegar a sobrecargarlo.

Las operaciones sobre los ficheros son síncronas, esto significa que las operaciones realizadas sobre ellos solo retorna cuando el servidor complete la totalidad del trabajo asociado a esa operación. En caso de escritura el servidor escribirá físicamente los datos en disco, y actualizará la estructura de directorios, esto último solo lo hará si es necesario, antes de responder al cliente.



Fuente: https://mundo-hackers.weebly.com/uploads/9/8/5/0/98506118/nfs_orig.jpg

Dato interesante:

Fue desarrollado en 1984 por Sun Microsystems, con el objetivo que fuese independiente de la máquina, esto fue posible gracias a que fue implementado sobre los protocolos XDR y ONC RPC. El protocolo NFS está incluido por defecto en los SO (Sistema Operativo) UNIX y la mayoría de distribuciones de LINUX.

5.2 ¿Cómo interviene NFS sobre el proyecto?

NFS interviene en el proceso de acceder al USB cifrado, ya que se ha procedido a dar acceso desde la Raspberry, instalando NFS (Servidor) en ella, para la descarga de ficheros contenidos en el USB cifrado. La idea principal es que el USB se conecte a la Raspberry, y esta lo descifre y monte con NFS para que los ordenadores clientes puedan acceder con facilidad a los archivos del USB desde su ordenador local utilizando su visualizador de ficheros y carpetas.

Para ver cómo se desarrolló la instalación y configuración de NFS sobre raspbian y un cliente ubuntu mirar Anexo 9.18.

6. Conclusiones

6.1 Conclusiones Punto de Acceso Anónimo

La evidencia que se mostró anteriormente demuestra que tener un punto de acceso anónimo, es que se puede tener varias máquinas a la vez navegando por internet anónimamente y sin necesidad de tener el servicio en cada máquina.

Además de que no solo los delincuentes son los que navegan por la red TOR si no también gente que no desea que terceras personas tengan información sobre ellos, porque a día de hoy la información sobre gustos, las páginas que se navega… debido que estos datos son vendidos al mercado publicitario o utilizados por el gobierno.

Gracias a los servicios como TOR se puede navegar por páginas que los gobiernos desean censurar al público.

6.2 Conclusiones Servidor Web USB

La conclusión final sobre el servidor web USB es la siguiente: la tecnología actual no permite hacer el servidor en un USB de la manera que se quería, ya que la idea era evitar instalaciones en

el ordenador, porque se quería que estuviera sólo en el pendrive. Al final la parte de no querer instalar nada en el ordenador se eliminó para intentar solucionar problemas anteriores, pero al final se llegó a la misma conclusión, no era algo funcional para Ubuntu.

6.3 Conclusiones USB Cifrado

La conclusión final sobre el USB cifrado es la siguiente, es una parte esencial del proyecto que, con los conocimientos adquiridos durante el curso sobre el cifrado, y buscando suficiente información, parece más simple de lo que realmente es. Esto es debido a los tipos de cifrado, ya que aunque en esta memoria se nombren algunos, no se abarcan ni de lejos todos los tipos existentes, y esto ocurre por la facilidad que Ubuntu nos da con su sistema de cifrado para discos y USB; LUKS.

LUKS es un sistema de cifrado simple y fácil de utilizar, pero con un gran potencial para el cifrado, ya que este es capaz de cifrar por completo el disco o USB que se quiera, de esta manera el disco al completo queda con la seguridad de LUKS, y no solo sobre los directorios especificados como podrían hacer otros sistemas de cifrado diferentes.

Gracias a este apartado aprendimos que es el cifrado necesario para lo que se desea utilizarlo en este proyecto, LUKS es la mejor elección de sistema de cifrado que se podría haber elegido.

6.4 Conclusiones NFS en Raspberry para el USB Cifrado

La conclusión sobre el NFS es la siguiente, gracias a NFS podemos compartir, como si se trabajara sólo sobre nuestra propia máquina, archivos de todo tipo simplemente montando el directorio del servidor sobre otro creado en el cliente, de esta manera se facilita el traspaso de archivos entre dos o más personas conectadas de manera local a la raspberry.

Gracias a NFS y al cifrado del USB, podemos compartir de manera segura los archivos en un área local donde la raspberry actuará como servidor de NFS, y los demás ordenadores del área como clientes de la misma.

Ejemplo:

En el caso del instituto: se podría usar para que cada profesor llevase encima un USB con toda la información de la materia, y pedir a los alumnos que se conectaran para descargar esa misma información. Ya que el USB está cifrado, sólo podrían acceder si el profesor se lo permite,

de esta manera se puede evitar la sustracción de información no deseada.

7. Glosario

Raspberry: Placa de ordenador reducida.

Ethernet: Estándar de redes de área local.

GPIO: pin genérico en un chip.

RCA: Conector negro eléctrico común en el mercado audiovisual.

Conector Jack: Conector de audio análogo.

MB: Unidad de información.

RAM: Memoria de trabajo de ordenadores y otros dispositivos.

RJ-45: Conector comúnmente utilizado para conectar redes de ordenadores con cableado.

SD: Dispositivo en formato tarjeta de memoria para dispositivos portátiles.

MicroSD: Formato de tarjeta de memoria flash.

Memoria Flash: Se trata de la tecnología empleada en los dispositivos denominados USB.

MHz: Unidad de medida de la frecuencia.

GHz: Unidad de medida de la frecuencia.

Wi-Fi: Tecnología que permite la interconexión inalámbrica.

Bluetooth: Especificación industrial para Redes Inalámbricas de Área Personal.

MiniHDMI y HDMI: Conector digital de audio y video.

HOSTPAD: Servicio que convierte un sistema en un punto de acceso.

Punto de acceso: Red de área local inalámbrica.

Router: Dispositivo que proporciona conectividad a nivel de red o nivel 3 en el modelo OSI.

Switch: Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace del modelo OSI.

DHCP: Servidor que usa protocolo de red de tipo cliente/servidor.

DNS: Sistema de nomenclatura jerárquica descentralizado para dispositivos conectados a redes IP como internet.

I2P: Software que ofrece una capa de abstracción para comunicaciones entre ordenadores.

Nodos: Punto de intersección.

http: Protocolo de comunicación que permite las transferencias de información en la World Wide Web.

https: Protocolo de aplicación basado en el protocolo http, es la versión segura de http.

TOR: Proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet.

P2P: Red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos.

iptables: Comandos del sistema linux para gestionar firewall.

Firewall: Se encarga de bloquear las conexiones entrantes y salientes del sistema.

Raspbian: Distribución del sistema operativo GNU/Linux y por lo tanto libre basado en Debian Jessie.

Debian Jessie: Comunidad conformada por desarrolladores y usuarios.

SSH: Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera.

ZAP y Burp suite: Herramienta gráfica para probar la seguridad de las aplicaciones WEB.

Edward Snowden: Consultor tecnológico estadounidense.

NSA: Agencia de inteligencia del Gobierno de los Estados Unidos.

MicroUSB y USB: Bus de comunicaciones.

Bus: Sistema digital que transfiere datos entre los componentes de uno o varios ordenadores.

WEB Server: Programa informático que procesa una aplicación que permite mostrar páginas WEB.

XAMPP: Paquete de software libre.

Software: Programa informático.

Software libre: Programa informático que puede ser copiado, estudiado, modificado y utilizado libremente.

Dokuwiki: Software para gestión de webs colaborativas de tipo wiki.

Web Colaborativa: Cualquier persona puede modificar la página web.

SO (Sistema Operativo): Software principal o conjunto de programas de un sistema informático.

Ejemplo: Ubuntu y Windows

PHP: Lenguaje de programación utilizado originalmente para el desarrollo web.

Apache: Servidor web.

MySQL: Sistema de gestión de BBDD (Base de datos) relacional.

BBDD (Base de datos): Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su uso.

Punto de montaje: Carpeta del sistema donde al conectar un USB se pueden ver sus sistema de ficheros (carpetas).

Cifrado: Procedimiento que utiliza un algoritmo con cierta clave para transformar un mensaje.

Algoritmos: Conjunto prescrito de instrucciones o reglas bien definidas.

Claves: Pieza de información que controla la operación de un algoritmo.

Criptografía: Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas.

Criptografía simétrica: Método criptográfico en el que se usa una misma clave para cifrar y descifrar.

Criptografía asimétrica: Método criptográfico en el que se usan dos claves diferentes para cifrar y descifrar.

Firma electrónica: Mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente poder leerlo y saber su dueño.

Cifrado en Flujo: Algoritmo de cifrado que realiza el cifrado incrementalmente.

Cifrado en Bloque: Algoritmo de cifrado que realiza el cifrado en grupos de bits de longitud fija.

Bits: dígito del sistema de numeración binario.

LUKS: Especificación de cifrado de disco.

cryptsetup: Subsistema de cifrado de discos.

dm-crypt: Subsistema de cifrado de discos.

Phoronix: Web tecnológica que ofrece comentarios sobre productos.

eCryptfs: Paquete de software de cifrado de disco para Linux.

NFS (Network File System): Protocolo de nivel de aplicación.

Modelo OSI: Modelo de referencia para los protocolos de la red de arquitectura en capas.

Área Local: Red de ordenadores que abarca un área reducida a una casa, departamento o edificio.

Ficheros remotos: Archivos ubicados en otro ordenador, pero accesibles desde uno propio.

ZIP: Formato de compresión de archivos.

Síncronas: Envío de datos que se da al mismo tiempo que la respuesta.

Directorios: Contenedor virtual en el que se almacena una agrupación de archivos.

Sun Microsystems: Empresa informática.

XDR: Protocolo de prestacion de datos. Permite la prestacion de datos entre máquinas de diferentes arquitecturas y sistemas operativos.

ONC RPC: Protocolo de llamada a procedimiento remoto.

UNIX: Sistema operativo libre.

GNU/LINUX: Sistema operativo libre de tipo UNIX.

Ubuntu: Sistema operativo de código abierto para ordenadores.

Man in the Middle: Es un ataque que consiste en introducirse en la comunicación entre dos equipos.

8. Bibliografía

8.1 USB WebServer

http://ampps.com/wiki/Installing_AMPPS_on_Linux

https://www.redeszone.net/2015/11/01/devd-un-servidor-http-ligero-libre-y-portable-para-windows-linux-y-mac-os-x/

http://www.ampps.com/downloads

https://www.dokuwiki.org/install:dokuwiki_on_a_stick_linux

https://www.dokuwiki.org/install:mongoose

https://www.dokuwiki.org/start?id=es:security

https://www.dokuwiki.org/start?id=install:dokuwiki_on_a_stick_linux

https://ayudawp.com/lleva-tu-wordpress-en-un-pendrive/

https://blog.jblanco.org/apachephpmysql-portable-linux/

https://ceslava.com/blog/como-instalar-wordpress-en-local-paso-a-paso/

http://chicomonte.blogspot.com.es/p/como-crear-un-servidor-web-php-apache.html

https://cjenkins.wordpress.com/2009/03/09/servidor-wamp-portable/

http://conexionesrazonables.blogspot.com.es/2009/11/mowes-servidor-web-para-llevar-en-una.html

https://desarrolloweb.com/articulos/mowes-apache-php-mysql.html

https://es.slideshare.net/LeccionesWeb/xampp-portatil

https://pplware.sapo.pt/microsoft/windows/usbwebserver-8-6-um-autentico-servidor-web-na-penusb/

https://programadorphp.es/wamp-portable

https://softwarerecs.stackexchange.com/questions/10280/portable-lamp-or-xampp-for-linux

https://ubuntuforums.org/showthread.php?t=2299081

http://www.baitic.com/tag/xampp

https://www.linuxtotal.com.mx/?cont=info__tips_018

https://perezneira.wordpress.com/2016/12/01/xampp-cambiar-la-ubicacion-de-htdocs/

8.3 Cifrar USB

https://blog.desdelinux.net/como-encriptar-una-memoria-usb/

https://miguelmenendez.pro/es/articulos/encriptar-cifrar-dispositivo-almacenamiento-usb-linux-unified-key-setup-luks.html

https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)#Tipos_de_cifrado_seg%C3%BAn_sus_propiedades

https://es.wikipedia.org/wiki/LUKS

https://bbs.archlinux.org/viewtopic.php?id=123644

8.4 NFS para USB en Raspberry

https://www.htpcguides.com/configure-nfs-server-and-nfs-client-raspberry-pi/

https://es.wikipedia.org/wiki/Network_File_System

https://www.atareao.es/tutorial/raspberry-pi-primeros-pasos/nfs-en-raspberry/

8.5 Copia de USB a Raspberry

https://www.redeszone.net/2017/03/05/copiar-archivos-pc-raspberry-pi/

https://electrolitoblog.wordpress.com/2012/12/11/montar-pendrive-o-disco-duro-usb-en-raspberry-pi/

8.6 Servidor USB en Raspberry

http://www.bujarra.com/raspberry-como-servidor-de-usb/

8.7 URL Conversor DXF a STL

https://www.ofoct.com/3d-model-file-for-3d-printer-converter/dxf-to-stl.html

http://www.greentoken.de/onlineconv/index.php

8.8 Instalar Raspbian:

https://raspberryparatorpes.net/instalacion/noobs-paso-a-paso-instalar-el-sistema-operativo-en-la-raspberry-pi/

8.9 NOOBS Página oficial

https://www.raspberrypi.org/downloads/noobs/

8.10 Instalar Punto de Acceso Tor:

https://learn.adafruit.com/onion-pi/

https://www.raspberrypizaragoza.es/convierte-tu-raspberry-pi-en-un-punto-de-acceso-wifi/

https://lifehacker.com/how-to-anonymize-your-browsing-with-a-tor-powered-raspb-1793869805

https://geekytheory.com/tutorial-rasbperry-pi-como-crear-un-punto-de-acceso-wifi

https://www.redeszone.net/raspberry-pi/manual-para-configurar-raspberry-pi-como-un-router-wi-fi/

http://www.techradar.com/how-to/computing/how-to-use-a-raspberry-pi-to-browse-anonymously-1305789

http://opensourceforu.com/2016/11/make-tor-proxy-router-raspberry-pi/

https://pimylifeup.com/raspberry-pi-tor-access-point/

https://www.sbprojects.net/projects/raspberrypi/tor.php

https://es.gizmodo.com/como-fabricar-un-router-wifi-de-bolsillo-basado-en-tor-1764726467

https://hackaday.com/2013/06/15/raspberry-pi-tor-proxy-lets-you-take-anonymity-with-you/

8.11 Install OpenVPN:

https://gist.github.com/kremalicious/4c333c8c54fced00ab10c0a892a2304d

8.12 Install Hostapd:

https://frillip.com/using-your-raspberry-pi-3-as-a-wifi-access-point-with-hostapd/

8.13 Mejorar Seguridad Tor:

https://www.redeszone.net/2015/08/15/mejora-la-privacidad-y-el-anonimato-de-la-red-tor-con-astoria/

8.14 Informaciones Tor, I2P y VPN:

http://blog.hostdime.com.co/11-cosas-que-debes-y-no-debes-hacer-con-tor/

https://geekland.eu/diferencias-semejanzas-vpn-y-tor/

https://hipertextual.com/archivo/2013/09/mantener-el-anonimato-en-la-web/

https://es.gizmodo.com/que-es-tor-y-por-que-tu-tambien-deberias-usarlo-1591372289

https://es.slideshare.net/navajanegra_ab/el-lado-oscuro-de-tor-la-deep-web

https://www.genbeta.com/actualidad/i2p-la-nueva-generacion-de-la-deep-web

https://www.redeszone.net/2012/09/07/i2p-red-segura-y-anonima-para-navegar-chatear-y-descargar-archivos/

http://descargar-tor.com/i2p-o-proyecto-de-internet-invisible/

https://es.wikipedia.org/wiki/I2P

https://geti2p.net/es/

https://hacking-etico.com/2014/08/12/anonimato-en-la-red-con-i2p/

https://thehackerway.com/2015/01/27/20-sitios-en-la-web-profunda-de-tor-que-te-podrian-interesar/

https://www.redeszone.net/2016/10/03/comprueba-una-direccion-onion-tor-esta-disponible-la-herramienta-onioff/

8.15 Verificar Seguridad y Más:

https://elbauldelprogramador.com/logrando-el-anonimato-con-tor-parte-2-proxies-y-servidores-de-dns/

https://www.makeuseof.com/tag/duckduckgo-privacy-apps/

https://ipaddress.ip-adress.com/

https://www.quora.com/What-tools-can-be-used-as-an-alternative-of-Burp-Suite

https://www.osi.es/es/actualidad/blog/2016/04/05/navegacion-anonima-es-posible

http://inseguin.blogspot.com.es/2014/01/arachni-framework-una-forma-diferente.html

https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

http://www.arachni-scanner.com/

https://nyx.torproject.org/#home

https://www.redeszone.net/2017/11/18/tor-nyx-monitor/

8.16 Temperatura

https://alteageek.com/2016/04/24/como-medir-la-temperatura-de-nuestra-raspberry/

8.17 lm-sensor

https://www.cyberciti.biz/faq/howto-linux-get-sensors-information/apt-get-install-lm-sensors-ubuntu-debian/

8.18 Lista IP TOR:

https://www.dan.me.uk/torlist/

https://exitlist.torproject.org/exit-addresses

https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1

8.19 Verificar IP Pública

https://www.ipchicken.com/

http://www.see-my-ip.com/

https://bandaancha.eu/mi-ip

https://check.torproject.org/?lang=es

9. Annexos

9.1 Idea Original

Resumen:

Implementación de un servidor web local en un pendrive y un punto de acceso a la red de forma anónima. Configurar una raspberry para que tenga acceso a la red de forma anónima del que el usuario debería poder conectarse a la raspberry por WIFI, y que la raspberry sea capaz de conectarse a la red de forma anónima, en la que todo lo que naveguemos sea totalmente anónimo.

La actividad se centraría en el estudio del software existente y de implementar una solución por algún supuesto de que diera solución a algún problema en las clases que se imparten además la implementación de la red anónima.

Introducción:

Implementación de un servidor auto-contenido en un pendrive, que sea accesibles a través de una red local en el mismo momento de enchufarlo. Este servidor deberá dar acceso a diferentes servicios (web, ftp, wiki ...).
Implantación de un punto de acceso a la red Tor a través de un dispositivo Raspberry Pi, los usuarios que se conecten al dispositivo podrán navegar por Internet de forma totalmente anónima. El dispositivo debe estar correctamente ensamblado mediante una carcasa impresa en 3D.
De esta manera los profesores podrían llevar toda la asignatura en un único pendrive y conectarlo en la raspberry tendríamos un acceso seguro al mismo, además la posibilidad de utilizar la raspberry para navegar de forma segura desde el aula.

Esto fue descartado debido a los problemas explicados en el anexo 9.2

9.2 Problemas de la Creación del USB web server

9.2.1 XAMPP lite

Intentamos crear el USB con XAMPP lite, sólo permitía el correcto funcionamiento en Windows.

Al pinchar el USB en Ubuntu este no lo detectaba y para poder hacerlo funcionar había que instalar XAMPP en la máquina, esto no es lo que buscábamos.

Para este problema decidimos continuar buscando más información al respecto para solucionarlo.

9.2.2 Dokuwiki

Al comenzar la instalación me encontré con varios problemas.

1- Luego me di cuenta que la instalación era para Windows, lo que no me gusta ya que la idea es que funcione multiplataforma y con windows surgen muchos problemas.

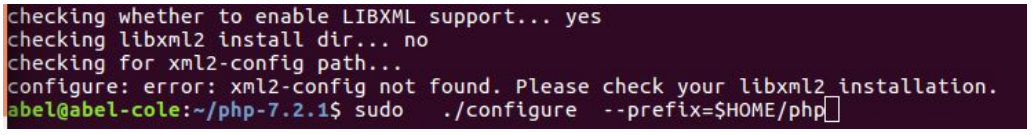
2- Después decidí utilizar una solución hacer una partición en el USB (la cual hicimos con el GParted de Ubuntu) que se debía tener una partición para Windows y otra para Ubuntu, en una partición FAT32 donde estará el DokuWiki_on_a_stick desde Windows y otra en ext3 que servirá para linux.

Después de muchos intentos de instalación y probar el funcionamiento en linux no he encontrado la manera óptima para el correcto funcionamiento en Ubuntu por tanto he decidido buscar otra manera de crear el sitio web en usb.

Me encontré problemas como que el Ubuntu no me detectaba el USB con el DokuWiki

9.2.3 PHP7

Quise instalar php7.2 pero tras varios intentos y búsqueda de información decidí volver a la versión php5.6 que es la que utilizaba el tutorial que estaba siguiendo, pero al querer hacer una actualización del mismo tutorial me encontré con este problema que no me permitía avanzar y no supe solucionar, hasta que probé este comando:



Fuente: Elaboración propia

Al final en la versión php5.6 simplemente añadiendo el siguiente comando se solucionaba el problema:

```
sudo apt-get install libxml2-dev
```

En la versión php7.2 nunca lo probé, he conseguido la instalación correcta del php5.6.

9.2.4 Reintentar con XAMPP

Intenciones
Instalar Ubuntu en pendrive e instalar servidor web para arrancar después desde otro ubuntu donde esté conectado el pendrive.

Pasos

1.- Instalar Ubuntu en USB
2.- Instalar XAMPP en Ubuntu del USB
3.- Conectar USB a otra máquina
4.- Cambiar enlaces simbólicos (de momento de forma manual)
5.- Modificar etiqueta USB
seguir pasos
Desmontar el USB

```
sudo umount /mnt/sdc1
```

cambiar nombre

```
sudo xfs_admin -L WebServer /dev/sdc1
```

6.- Modificar archivo xampp localizado en /media/$USER/WebServer/opt/lampp añadir variable.

```
name=$(who | cut -d" " -f 1)
```

Fuente: Elaboración propia

modificar línea d'aquesta manera.

```
linux|rh9)
        XAMPP_OS="Linux"
        XAMPP_ROOT="/media/$name/WebServer/opt/lampp"
        ;;
```

Fuente: Elaboración Propia

Hemos decidido cambiar porque XAMPP pedía demasiadas chapuzas que acababan en más chapuzas.

9.2.5 APACHE, PHP y MYSQL por separado

Una vez ha sido todo instalado y configurado para su correcto funcionamiento no he conseguido que apache abriera

correctamente el archivo install.php Dokuwiki, ya que después de arreglar el error que me tiraba (404 típico de toda la vida) abría el php correctamente pero no dejaba instalar el DokuWiki.

Por eso he decidido después de mil pruebas e intentos dejar de lado este apartado del proyecto y cambiar a crear un pendrive cifrado que al conectar a la raspberry se descifre y poder acceder a esta información a través de la raspberry.

9.2.6 Cambio punto de montaje USB

El último intento que probé fue instalar el XAMPP en la máquina y tratar de que los archivos se montasen donde el XAMPP se va a buscarlos, pero esto tampoco ha funcionado, a demas que mientras lo hacía me di cuenta de que esto no era lo que queríamos.

Tras varios intentos de experimentación parece que Ubuntu no me permite montar el usb en la carpeta /opt/lampp/apps/

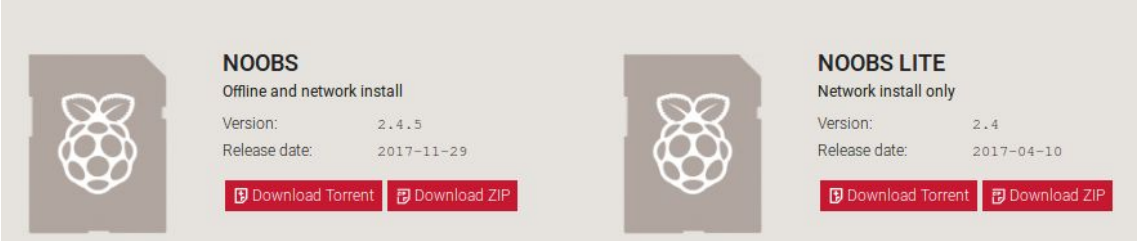
Por lo tanto, hemos vuelto a crear el USB cifrado y por eso vamos a crear un nuevo apartado en la memoria del proyecto que se llamara USB Cifrado.

9.3 Instalación Sistema Raspbian en la Raspberry

NOTA: Las imagenes son de mala calidad por que son fotografías del monitor, porque para obtener imágenes de mayor calidad sería necesario de una capturadora que no se dispone.

El primer paso para instalar el sistema Raspbian en la Raspberry lo que se debe de hacer es dirigirse a la página NOOBS, para descargar el instalador del sistema.

De las dos opciones que ofrece la página web, se opta por descargar el instalador en “.zip”, y elegir por si se opta por hacer la instalación por red o desde la sd (aunque cogerá también de internet pero no tanto).

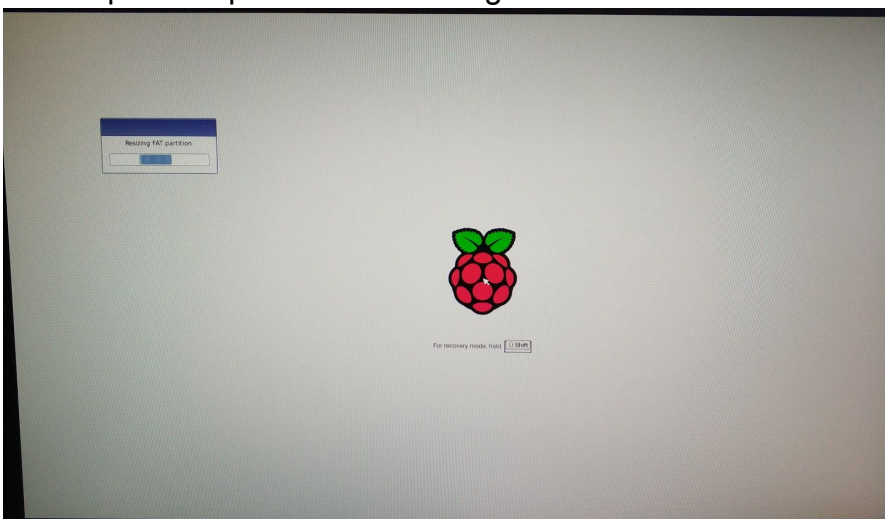


Fuente: https://www.raspberrypi.org/downloads/noobs/

Se crea una carpeta temporal en la que se descomprimira el “.zip” y luego todo el contenido de la carpeta se copiara en la SD que utiliza la raspberry.

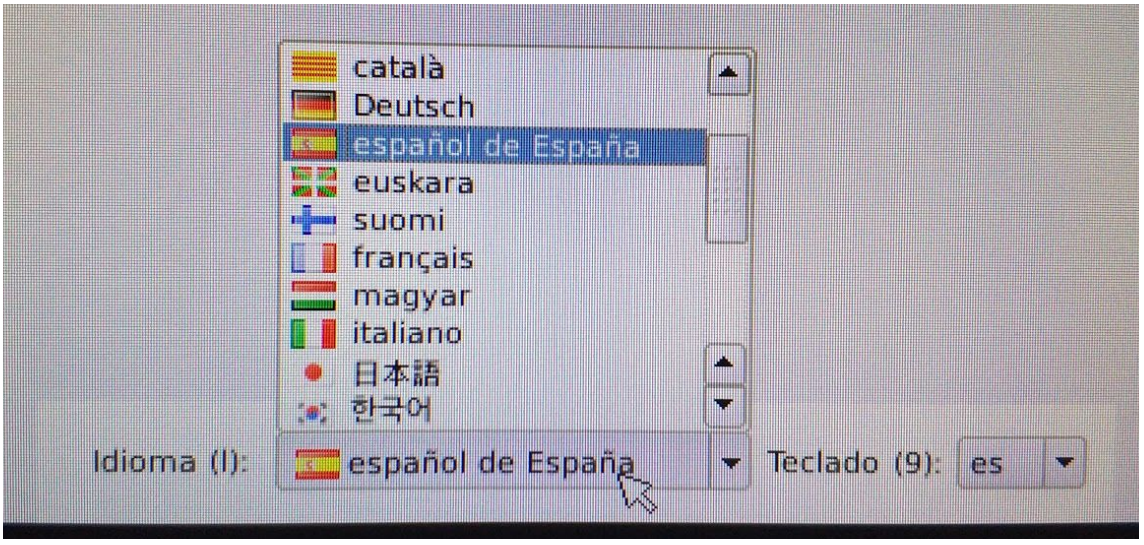
Se conecta en la raspberry todos los periféricos (mouse, monitor, teclado, cable de red, SD), también conectar la fuente de alimentación [mirar si no arranca].

Esperar a que termine de cargar el sistema.



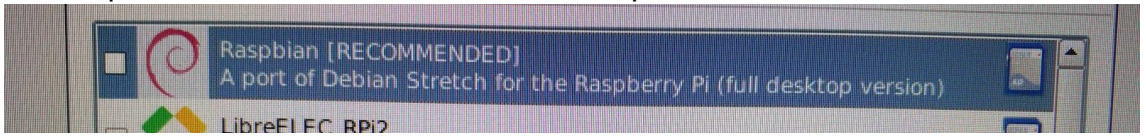
Fuente: Elaboración Propia

El primer paso ha hacer es elegir el idioma del sistema y del teclado.



Fuente: Elaboración Propia

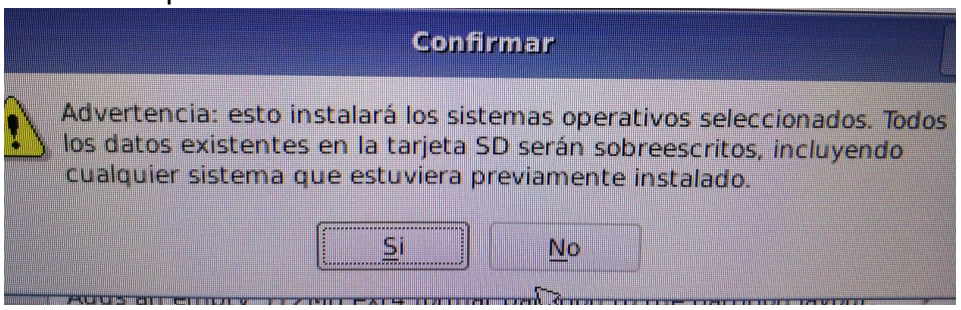
Marcar el cuadrado con una “X” con el sistema que instalaremos, que en este caso será el sistema Raspbian.



Fuente: Elaboración Propia

Para continuar lo que se debe hacer es darle al botón de instalar (Arriba a la izquierda).

A la hora de darle al botón de instalar, aparecerá una ventana donde pregunta si estamos seguros de continuar, le daremos a “SI” para continuar.



Fuente: Elaboración Propia

Ahora comenzará el proceso de instalación con lo que solo queda esperar a que termine.

Una vez haya terminado notificará si la instalación ha sido un éxito, le damos al botón ok con eso estará el sistema instalado y lista para usar.

Para instalar el sistema Raspbian se tuvo en cuenta la pagina [link].

9.4 Configuración IP Estática

Para obtener una dirección IP estática, se modifica el fichero de configuración ->

```
“sudo nano /etc/network/interfaces”
```

Antes de modificar el fichero de configuración, se realizará una copia de seguridad como esta:

```
“sudo cp /etc/network/interfaces
/etc/network/interfaces-old”
```

Se procede a modificar el fichero como la imagen de abajo en el que la red interna del punto de acceso puede cambiar a la que cada uno desee.

```
auto lo
auto eth0
iface lo inet loopback
iface eth0 inet dhcp

auto wlan0
allow-hotplug wlan0

iface wlan0 inet static
        address 192.168.50.1
        netmask 255.255.255.0

up iptables-restore < /etc/iptables.ipv4.nat
```

Fuente: Elaboración Propia

La red interna para este punto de acceso será la 50.

Al terminar de escribir, se guarda y se sale del fichero de configuración:

Para guardar -> “ctrl + o”
Para salir -> “ctrl + x”

Para que la configuración tenga efecto se reiniciará la raspberry o se reiniciará el servicio de red ->

“`sudo reboot`” <- Reiniciar la raspberry
“`sudo service networking restart`” <- Reiniciar servicio

Por último y lo más importante se debería de comprobar que la tarjeta de red tiene la dirección indicada.

“`ip -c a`”

La parte que importa es la de la tarjeta de red wlan0 y en la foto de abajo se puede observar un ejemplo.

```
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether b8:27:eb:05:bb:93 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.1/24 brd 192.168.50.255 scope global wlan0
       valid_lft forever preferred_lft forever
    inet6 fe80::ba27:ebff:fe05:bb93/64 scope link
       valid_lft forever preferred_lft forever
```

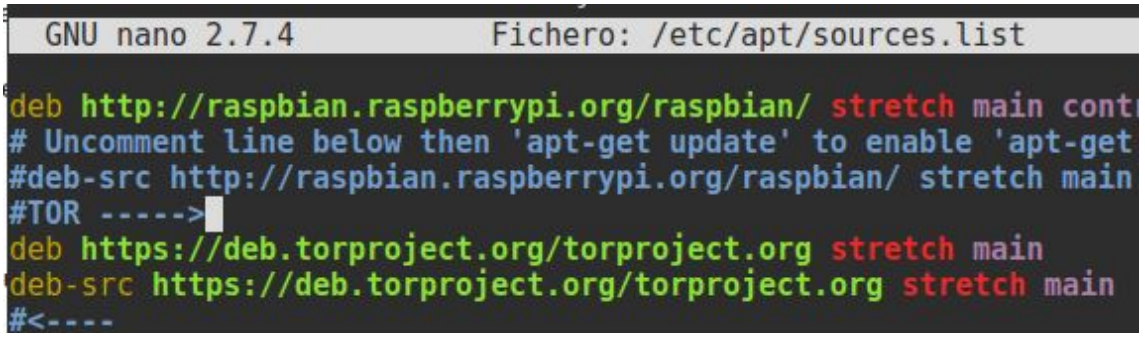
Fuente: Elaboración Propia

9.5 Instalación y Configuración Servicio Tor

Hay dos maneras de instalar el servicio TOR, desde los repositorios de ubuntu o desde los propios creadores de tor.

Instalación desde los creadores de TOR:
Para instalarlo desde los creadores de tor se debe de agregar las direcciones de las cuales se descargan los paquetes.

sudo nano /etc/apt/sources.list



Fuente: Elaboración Propia

Se guarda y se sale del fichero:

ctrl + o -> se guarda.

ctrl + x -> se sale.

Lo siguiente es añadir las claves con las que estarán firmadas los paquetes para su instalación.(decirle al sistema que confíe en esos paquetes y verificar que los paquetes a instalar son los que tienen que ser)

Se procede a instalar la primera clave ->

gpg --keyserver keys.gnupg.net --recv A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89

gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -

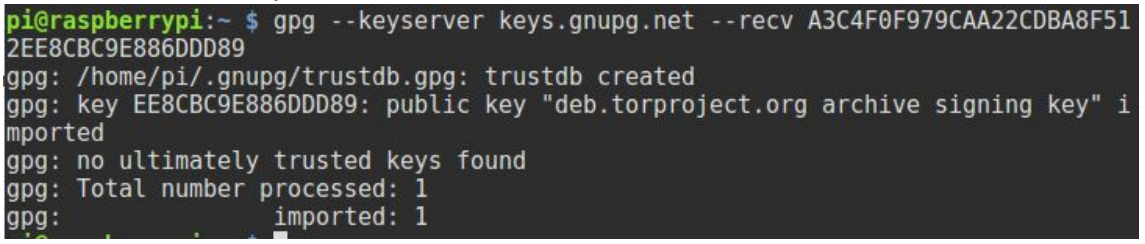
Si ocurre un error como el de la imagen de abajo.

Fuente: Elaboración Propia

Se procede a instalar el programa: “dirmngr”

sudo apt-get install dirmngr

Se vuelve a probar a instalar la clave ->



Fuente: Elaboración Propia

```
pi@raspberrypi:~ $ gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo
apt-key add -

OK
```

Fuente: Elaboración Propia

Se actualiza la lista de paquetes ->

sudo apt-get update

Y se instala el programa TOR ->

sudo apt-get install tor deb.torproject.org-keyring

Instalación desde los repositorios:

Antes de instalar el servicio TOR primero se actualiza la lista de repositorios y paquetes de la raspberry:

"sudo apt-get update"

"sudo apt-get upgrade"

Ahora que se tiene los paquetes y la lista de repositorios actualizados se procede a instalar el servicio TOR ->

`"sudo apt-get install tor -y"`

el parámetro -y es para aceptar la instalación el programa sin que luego lo pregunte.

Proceso instalación en conjunto:

Una vez está instalado lo que se debe hacer es una copia del fichero de configuración ->

`"sudo cp /etc/tor/torrc /etc/tor/torrc-old".`

Se procede a modificar el fichero de configuración del servicio TOR -> `"sudo nano /etc/tor/torrc".`

En el fichero de configuración habría que tener las siguientes líneas de la siguiente manera: "como todo está comentado en el fichero lo que hacemos sería escribir todo al final del fichero".

```
Log notice file /var/log/tor/notices.log
VirtualAddrNetwork 10.192.0.0/10
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1
TransPort 192.168.50.1:9040
DNSPort 192.168.50.1:53
```

```
  GNU nano 2.7.4                Fichero: /etc/tor/torrc

Log notice file /var/log/tor/notices.log
VirtualAddrNetwork 10.192.0.0/10
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1
TransPort 192.168.50.1:9040
DNSPort 192.168.50.1:53
```

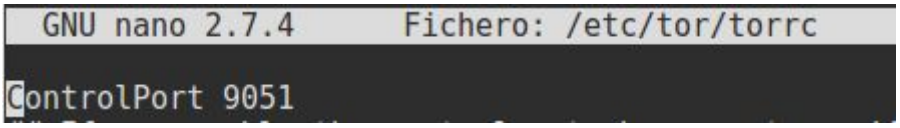
Fuente: Elaboración Propia

Cambiar la IP de escucha por la de la raspberry que en este caso será la red 50 y no equivocarse en nada.

Además se debe de descomentar el control port del fichero de configuración:

#ControlPort 9051 -> ControlPort 9051

Como se puede observar lo que se hace es borrar "#" y con eso queda descomentar la línea "ControlPort"



Fuente: Elaboración Propia

Para guardar la configuración -> "ctrl + o"
Para salir del nano -> "ctrl + x"

Ahora se creará el fichero donde estarán los logs del servicio TOR -> `"sudo touch /var/log/tor/notices.log"`

Cambiar el propietario del fichero ->

`"sudo chown debian-tor /var/log/tor/notices.log"`

Y se le cambia los permisos al fichero ->

`"sudo chmod 644 /var/log/tor/notices.log"`

```
pi@raspberrypi:/etc/tor $ sudo touch /var/log/tor/notices.log
pi@raspberrypi:/etc/tor $ sudo chown debian-tor /var/log/tor/notices.log
pi@raspberrypi:/etc/tor $ sudo chmod 644 /var/log/tor/notices.log
pi@raspberrypi:/etc/tor $
```

Fuente: Elaboración Propia

Para que el servicio tor se inicie en los próximos arranques ->

`"sudo update-rc.d tor enable"`

9.6 Instalación y Configuración Servidor DHCP

Primero se actualizará la lista de repositorios y paquetes de la raspberry:

`"sudo apt-get update"`
`"sudo apt-get upgrade"`

Se procede a instalar el servicio del servidor DHCP ->

"sudo apt-get install isc-dhcp-server -y"

Una vez instalado el servicio se crea una copia del fichero de configuración ->

"sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.old".

Una vez hecho la copia de seguridad se puede ir al fichero de configuración del servicio y modificarlo ->

“sudo nano /etc/dhcp/dhcpd.conf”

En el fichero de configuración se procede a hacer lo siguiente:

1.- Comentar las dos líneas que tienen que ver con el servicio DNS con ‘#’ de tal manera que queden así:
#option domain-name “example.org”;
#option domain-name-servers ns1.example.org, ns2.example.org;

2.- El tiempo que otorga las direcciones IP se puede modificar según convenga.
default-lease-time 600;
max-lease-time 7200;

3.- Ahora se busca la linea “authoritative;” que estará comentada con ‘#’, entonces lo que se hará es descomentarlo borrando solo el ‘#’ y ya estaría.

4.- Al final del fichero se configura la red del punto de acceso otorgándoles un servidor DNS, IP…

```
  GNU nano 2.7.4          Fichero: /etc/dhcp/dhcpd.conf

# DHCP Red Anonima
subnet 192.168.50.0 netmask 255.255.255.0 {
        # Rango de IPS disponibles
        range 192.168.50.10 192.168.50.40;
        option broadcast-address 192.168.50.255;
        # IP Raspberry
        option routers 192.168.50.1;
        # nombre de dominio interno
        option domain-name "red-tor";
        # Servidores DNS a los que hacemos la consulta: Google
        option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

Fuente: Elaboración Propia

5.- Se guarda la configuración -> “ctrl +o”

6.- Para salir del nano -> “ctrl + x”

7.- Ahora lo que se debe hacer es modificar el fichero de configuración -> “sudo nano /etc/default/isc-dhcp-server”, posicionarse al final del fichero y modificar la línea, si no se encuentra se añade -> ‘INTERFACES=””’ a -> ‘INTERFACES=”wlan0”’

8.- Para que el servicio se inicie cada vez que se inicie la máquina -> “sudo update-rc.d isc-dhcp-server enable”

9.- Por último queda verificar que el servicio está funcionando sin ningún fallo.

“sudo systemctl status isc-dhcp-server”

```
pi@raspberrypi:~ $ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated; vendor preset: enable
   Active: active (running) since Sat 2018-04-28 11:45:33 CEST; 15h ago
     Docs: man:systemd-sysv-generator(8)
  Process: 605 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=
   CGroup: /system.slice/isc-dhcp-server.service
           └─654 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf wlan0
```

Fuente: Elaboración Propia

9.7 Instalación y Configuración Servicio Hostapd

Primero habría que instalar el servicio hostpad ->

”sudo apt-get install hostapd -y”.

Se crea el fichero donde se le indica la configuración del punto de acceso ->

“sudo nano /etc/hostpad/hostpad.conf”

Dentro del fichero se introduce las siguientes líneas:

```
  GNU nano 2.7.4         Fichero: /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
ssid=ProjectoRP3
hw_mode=g
channel=8
wmm_enabled=1
ht_capab=[HT40][SHORT-GI-20][DSSS_CCK-40]
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=PuntoDeAccesoAnonimo
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Fuente: Elaboración Propia

Hay que indicar el driver que dispone el adaptador wifi, si se está utilizando la raspberry pi3 el driver es el que sale en la imagen y si no, habría que buscar que driver se usa.

El ‘ssid’ es el nombre que se verá en los dispositivos, asi que se puede elegir el nombre que uno desee.

El canal se puede elegir el que más guste, o utilizando aplicaciones por el móvil como ‘wifi analizer’ se puede identificar el mejor canal.
Y la clave ‘wpa_passphrase’ se puede introducir lo que se desee, porque seria la contraseña con la que las otras máquinas puedan acceder al punto de acceso.

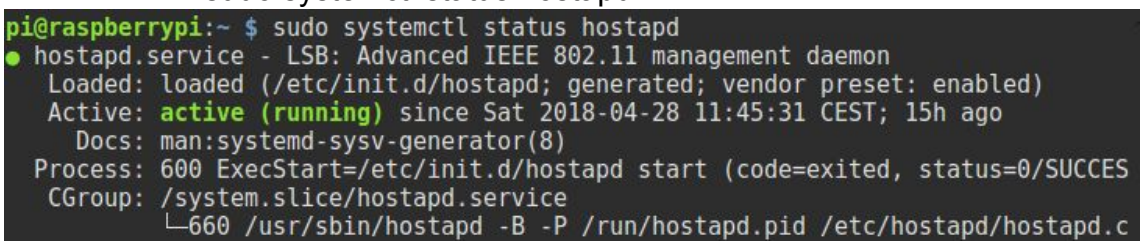
Para que el servicio “hostpad” pueda encontrar el fichero se modifica el fichero ->
“sudo nano /etc/default/hostapd”.

Una vez dentro del fichero se descomenta y modifica la línea ->
‘DAEMON_CONF=””’ y la dejamos ->
‘DAEMON_CONF=”/etc/hostapd/hostapd.conf”’

Para guardar la configuración -> “ctrl + o”
Para salir del nano -> “ctrl + x”

Lo que se debe hacer ahora es activar el servicio para que cada vez que se inicie el sistema el servicio HOSTAPD también se inicie ->
“sudo update-rc.d hostapd enable”

Ahora solo queda comprobar que el servicio está funcionando perfectamente.
“sudo systemctl status hostapd”



Fuente: Elaboración Propia

9.8 Tablas de Enrutamiento IP Servicio Tor

Configuración de las tablas de enrutamiento para la red tor:

Primero eliminamos las anteriores tablas de enrutamiento:
“sudo iptables -F”
“sudo iptables -t nat -F”

Si se desea permitir la conexión del ssh lo que se debe hacer es abrir el puerto 22.
“sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22”

Para enrutar las consultas DNS al puerto 53 interno:

“sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53”

Para enrutar todo el tráfico TCP des la interfaz wlan0 al puerto 9040:

“sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040”

Para verificar las tablas de enrutamiento de la red:

“sudo iptables -t nat -L”

```
pi@raspberrypi:~ $ sudo iptables -F
pi@raspberrypi:~ $ sudo iptables -t nat -F
pi@raspberrypi:~ $ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22
pi@raspberrypi:~ $ sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53
pi@raspberrypi:~ $ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040
pi@raspberrypi:~ $ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  anywhere             anywhere             tcp dpt:ssh redir ports 22
REDIRECT   udp  --  anywhere             anywhere             udp dpt:domain redir ports 53
REDIRECT   tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN redir ports 90
40

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Fuente: Elaboración Propia

Para guardar la configuración ->

‘sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"’

Se procede a reiniciar la raspberry -> “sudo reboot”.

9.9 Instalación y configuración servicio I2P

Lo primero que se debe hacer a la hora de instalar el servicio I2P es agregar los repositorios de los creadores.

sudo nano /etc/apt/sources.list

```
 GNU nano 2.7.4                Fichero: /etc/apt/sources.list

#I2P ---->
deb https://deb.i2p2.de/ stretch main
deb-src https://deb.i2p2.de/ stretch main
#<----
```

Fuente: Elaboración Propia

Se guarda y se sale del fichero:

ctrl + o -> se guarda.

ctrl + x -> se sale.

Lo siguiente es añadir las claves con las que estarán firmadas los paquetes para su instalación.(decirle al sistema que confíe en esos paquetes y verificar que los paquetes a instalar son los que tienen que ser)

Para realizar este paso se debe de descargar la clave y luego hacer la instalación de la clave.

wget https://geti2p.net/_static/i2p-debian-repo.key.asc

```
pi@raspberrypi:~ $ wget https://geti2p.net/_static/i2p-debian-repo.key.asc
--2018-05-27 01:46:36--  https://geti2p.net/_static/i2p-debian-repo.key.asc
Resolviendo geti2p.net (geti2p.net)... 91.143.92.136, 2a02:180:a:65:2456:6542:11
01:1010
Conectando con geti2p.net (geti2p.net)[91.143.92.136]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 15200 (15K) [text/plain]
Grabando a: “i2p-debian-repo.key.asc”

i2p-debian-repo.key 100%[==================>]  14,84K  --.-KB/s    in 0,07s

2018-05-27 01:46:36 (221 KB/s) - “i2p-debian-repo.key.asc” guardado [15200/15200
]
```

Fuente: Elaboración Propia

Ahora si se añade la clave:

sudo apt-key add i2p-debian-repo.key.asc

```
pi@raspberrypi:~ $ sudo apt-key add i2p-debian-repo.key.asc
OK
```

Fuente: Elaboración Propia

A continuación se procede a actualizar la lista de repositorios y paquetes del sistema.

“sudo apt-get update”

“sudo apt-get upgrade”

El siguiente paso será instalar el programa I2P con el anillo de claves que es el que se asegurara que se reciben bien las actualizaciones.

sudo apt-get install i2p i2p-keyring

Lo que se debe de hacer a continuación es verificar si el servicio se encuentra en marcha.

i2prouter status <- sin ser root ni usar sudo

```
pi@raspberrypi:~ $ i2prouter status
I2P Service is not running.
```

Fuente: Elaboración Propia

Como se tiene de antes puesto en marcha y funcionando el servicio TOR lo que se debe de realizar es parar el servicio y que al iniciar el sistema el servicio se encuentre apagado.

sudo systemctl stop tor

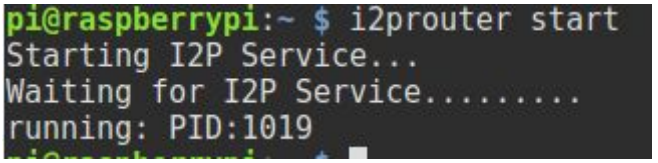
sudo systemctl disable tor

```
pi@raspberrypi:~ $ sudo systemctl stop tor
pi@raspberrypi:~ $ sudo systemctl disable tor
Synchronizing state of tor.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable tor
```

Fuente: Elaboración Propia

Ahora se procede a iniciar el programa I2P.

i2prouter start <- sin ser root ni usar el sudo



Fuente: Elaboración Propia

9.10 Pruebas de funcionamiento y seguridad de la red TOR

Con los siguientes comandos verificamos que todos los servicios están activados y funcionando:

"sudo service tor status"

"sudo service hostapd status"

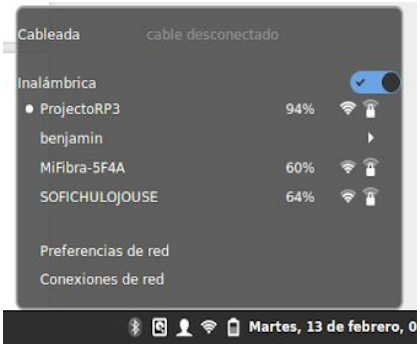
"sudo service isc-dhcp-server status"

Prueba1 ->

En la primera prueba no funcionaba el internet [solucion].

Prueba2 ->

Y ahora funciona perfectamente



Fuente: Elaboración Propia

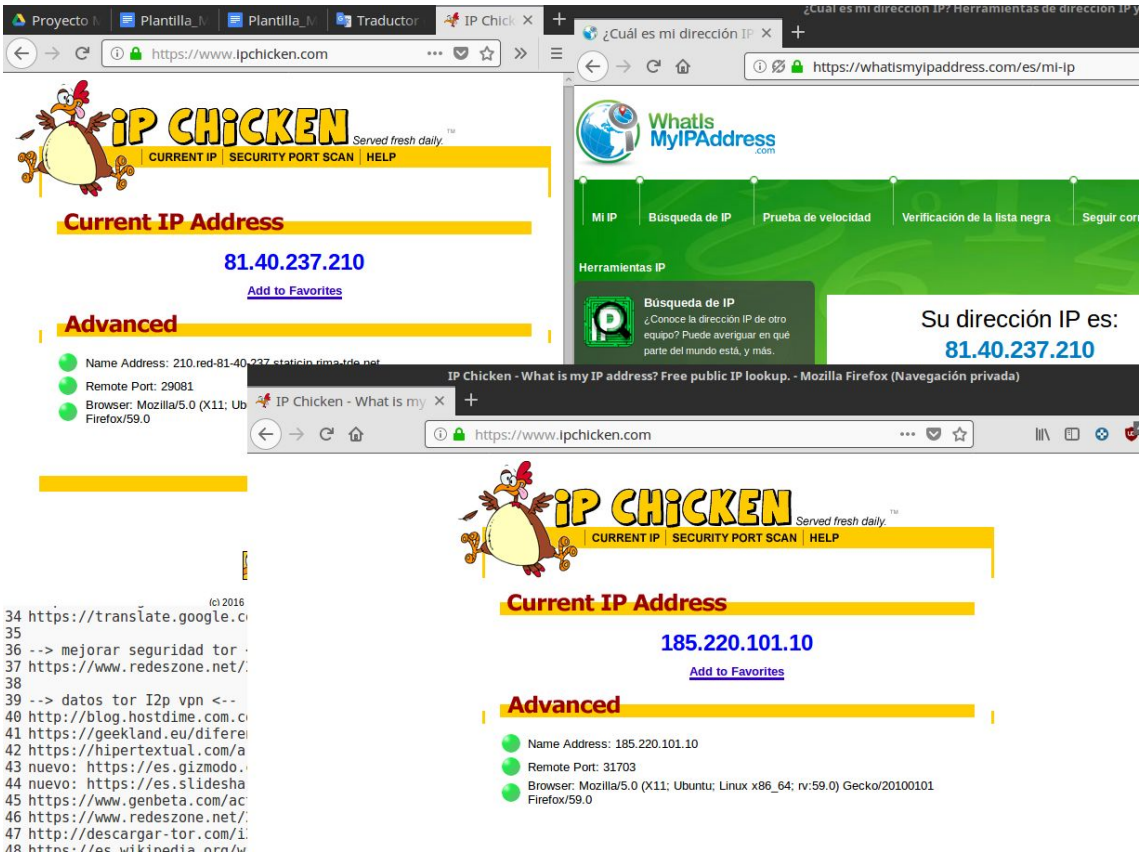
Prueba3 ->

Esta prueba consiste en verificar que realmente accedemos a internet anónimamente.

Para verificar que el servicio TOR está funcionando perfectamente y que hace su trabajo lo que se debe de hacer es verificar que la dirección IP pública ha cambiado por otra IP publica de la red TOR.

Pero para hacer este tipo de prueba lo primero que se debe de hacer es en la red normal sin TOR habría que averiguar la dirección IP pública, y luego hacer lo mismo una vez dentro de la red TOR y se puede observar que la dirección IP pública ha cambiado por otra que no es la de la red de casa.

Para averiguar la dirección IP pública se puede utilizar cualquier página web como las utilizadas o otras [ip pública].



Fuente: https://www.ipchicken.com/ y https://whatismyipaddress.com/

Pero por seguridad se debe de verificar si esa dirección IP pública se encuentra dentro de las direcciones de la red TOR, para ello se debe de descargar e actualizar la lista de direcciones IP de la red TOR y verificar si la obtenida se encuentra en esa lista [páginas].

-> Para bajarse en un fichero la lista de las direcciones IP.

```
wget --no-check-certificate
https://exitlist.torproject.org/exit-addresses -O tor.txt
```

-> Para Buscar en el fichero la IP que se utiliza

```
grep -R -n "IP pública" tor.txt
```

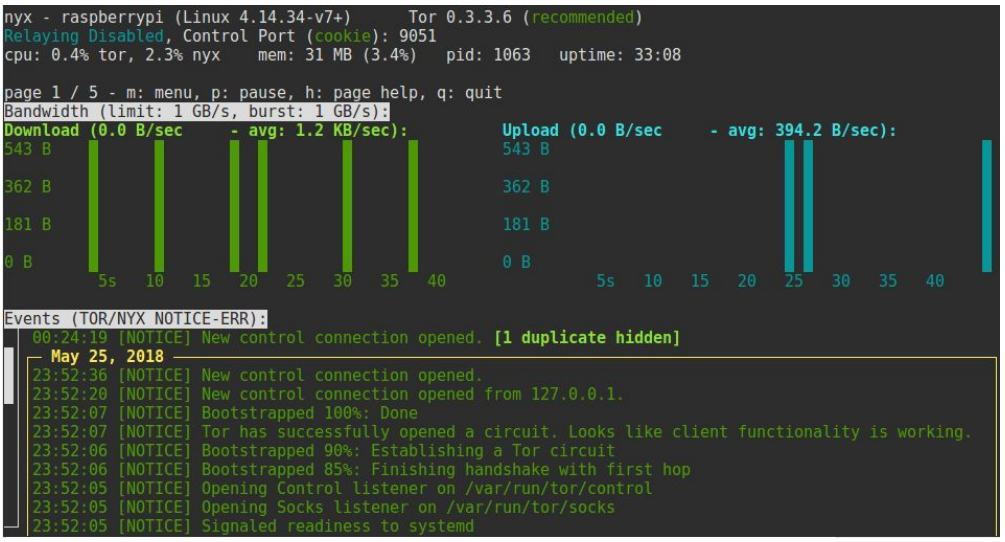
Prueba 4 ->
Esta prueba consiste en monitorizar el servicio TOR.

Los creadores de la red TOR mencionan el programa nyx con el que se puede monitorizar y cambiar la configuración de la red TOR.

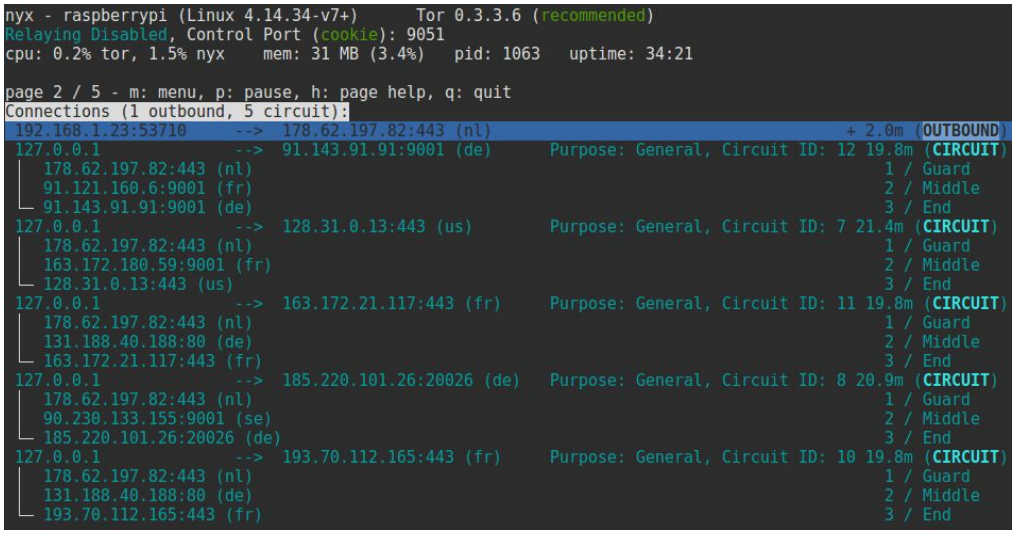
Instalación del programa nyx:

```
sudo pip install nyx
```

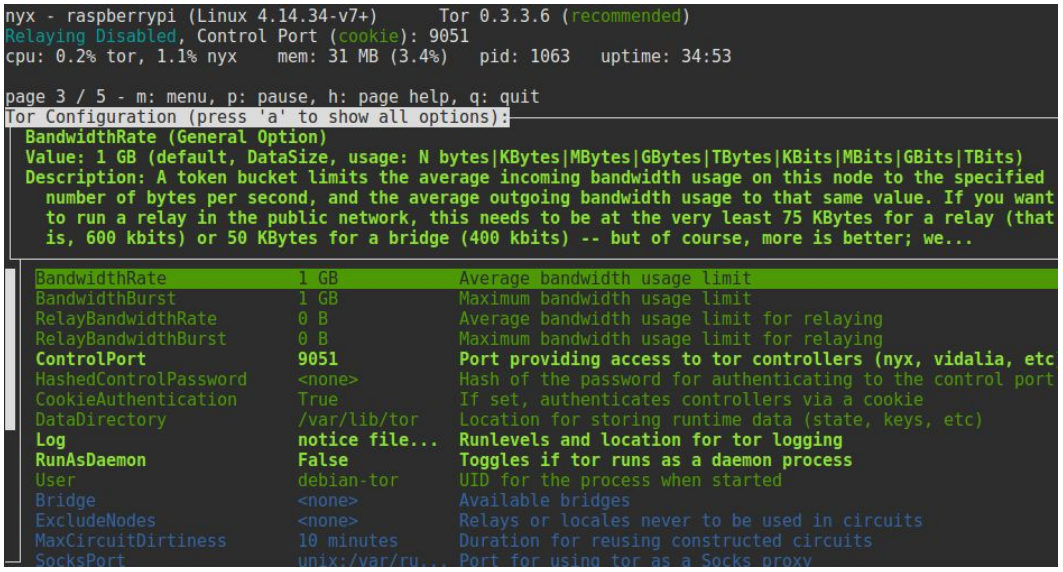
Con el programa nyx se puede observar la carga, la descarga, los circuitos creados, cambiar la configuración del servicio TOR y verificar que funciona correctamente la red TOR.



Fuente: Elaboración Propia



Fuente: Elaboración Propia



Fuente: Elaboración Propia

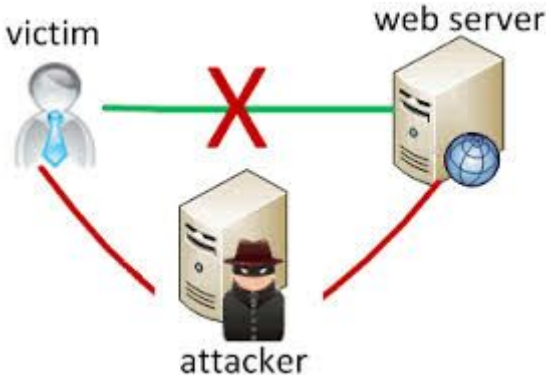
Prueba 5 ->
Para las siguientes pruebas de seguridad se optó por usar el sistema kali linux debido a que fue creado para la auditoría y la seguridad informática.

Se realizarán las pruebas dentro y fuera de la red del punto de acceso para verificar si se puede lograr ver los paquetes que hay en la red TOR y verificar que es segura.

Como todo lo que se navega dentro del punto de acceso sale por la tarjeta de red ethernet, lo que se hará es posicionarse en la red de la tarjeta ethernet, para verificar si se puede capturar los paquetes de la red interna del punto de acceso e intentar a quien va dirigida cada paquete o los paquetes en sí como están formados.

Para poder lograr lo que se desea se pasará a encender la máquina kali linux, la máquina debe de estar conectada a la misma red que la tarjeta de red del punto de acceso.

Se procede a realizar un ataque “man in the middle”, para lograrlo se usará el programa bettercap con el que atacaremos a la víctima que en este caso sería el punto de acceso.



Fuente: https://nerdygeekz.com/maninthemiddle-attack/

Para iniciar el bettercap se debe de abrir una terminal, en la terminal se escribirá bettercap para iniciar el programa.

Una vez iniciado el programa dentro escribimos:

net.probe on -> se escanea la red hasta ver la dirección IP de la máquina víctima.

set.arp.spoof.targets ipVictima -> para hacerle creer a la víctima que tu eres la puerta de enlace y que todo el tráfico pase por ti.

net.probe off -> para finalizar el escaneo.

arp.spoof on -> para capturar los paquetes.

```
root@kali:~# bettercap
bettercap v2.6 (type 'help' for a list of commands)

192.168.1.0/24 > 192.168.1.25  » [19:33:57] [sys.log] [inf] Checking latest stable release ...
192.168.1.0/24 > 192.168.1.25  » [19:33:58] [sys.log] [inf] You are running 2.6 which is the latest stable version.
192.168.1.0/24 > 192.168.1.25  » net.probe on
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.17 detected as b0:ea:bc:bc:12:19.
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.19 detected as a8:a7:95:5e:02:d3 (Hon
Hai Precision Ind. Co.).
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.23 detected as b8:27:eb:50:ee:c6 (Rasp
berry Pi Foundation).
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.26 detected as d8:61:62:05:30:2e.
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.15 detected as 4c:49:e3:4a:36:28.
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.14 detected as 5c:c3:07:8f:8a:a7.
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.20 detected as f4:1b:a1:a1:b9:88 (Appl
e).
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.13 detected as bc:3d:85:ca:88:4f.
192.168.1.0/24 > 192.168.1.25  » [19:34:04] [endpoint.new] Endpoint 192.168.1.24 detected as 28:cf:e9:29:0a:b1 (Appl
e).
192.168.1.0/24 > 192.168.1.25  » [19:34:06] [endpoint.new] Endpoint 192.168.1.200 detected as 2c:95:69:06:2b:89.
192.168.1.0/24 > 192.168.1.25  » set arp.spoof.targets 192.168.1.23
192.168.1.0/24 > 192.168.1.25  » net.probe off
192.168.1.0/24 > 192.168.1.25  » arp.spoof on
[19:34:24] [sys.log] [inf] Enabling forwarding.
192.168.1.0/24 > 192.168.1.25  » [19:34:24] [sys.log] [inf] ARP spoofer started, probing 1 targets.
192.168.1.0/24 > 192.168.1.25  »
```

Fuente: Elaboración Propia

Se inicia el wireshark, para capturar los paquetes con el wireshark y después analizarlos.

Para poner en marcha el wireshark se debe de buscar el programa wireshark y después realizar click encima, elegir la interfaz con la que se captura el paquete en este caso será la

interfaz de red puesto que se está usando el sistema dentro de una máquina virtual.

Mientras se están capturando los paquetes se procede a utilizar una máquina que se encuentre dentro del punto de acceso y navegar por internet.

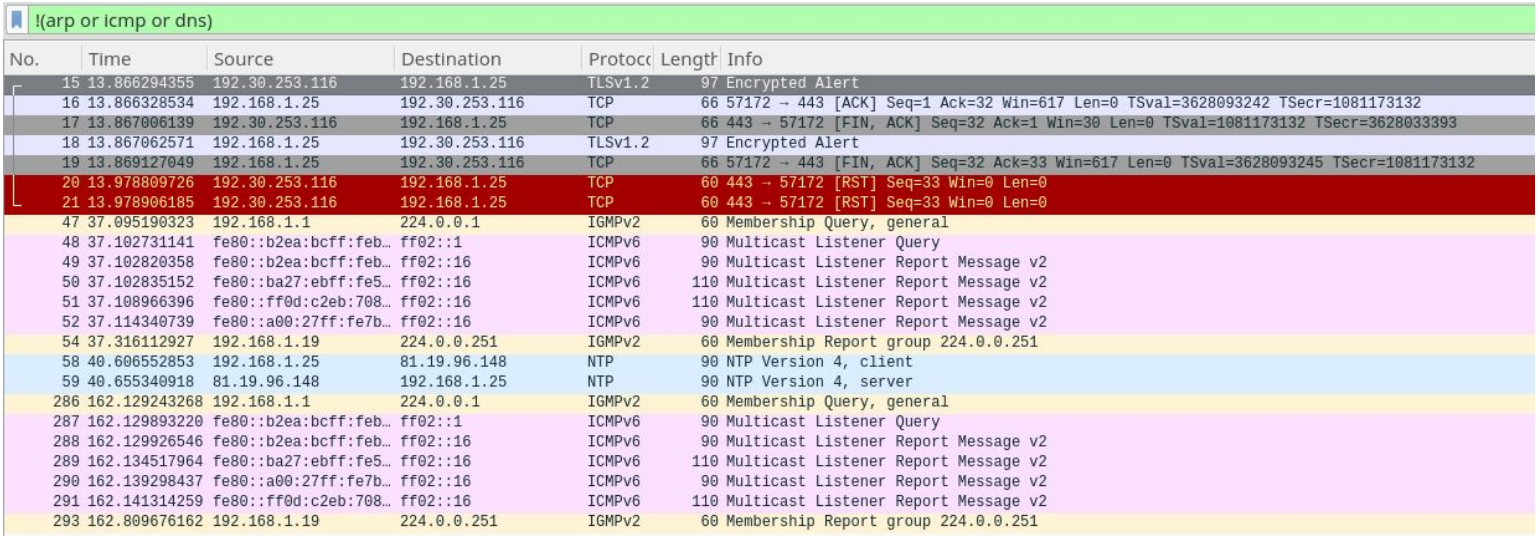
Desde un cliente que se encuentra dentro del punto de acceso se procedió a navegar por páginas http, para hacer el servicio TOR más vulnerable y poder identificar mejor los paquetes.

Después de navegar por internet se procede a analizar los paquetes que el wireshark ha logrado capturar.

Para poder ver mejor y quitar paquetes no deseados se procede a aplicar filtros al wireshark con esto lo que se logra es quitar una gran parte de paquetes que no se desea ver.

Filtros utilizados:

!(arp)
!(arp or icmp)
!(arp or icmp or dns)
ip.addr == 192.168.1.23



!(arp or icmp or dns)

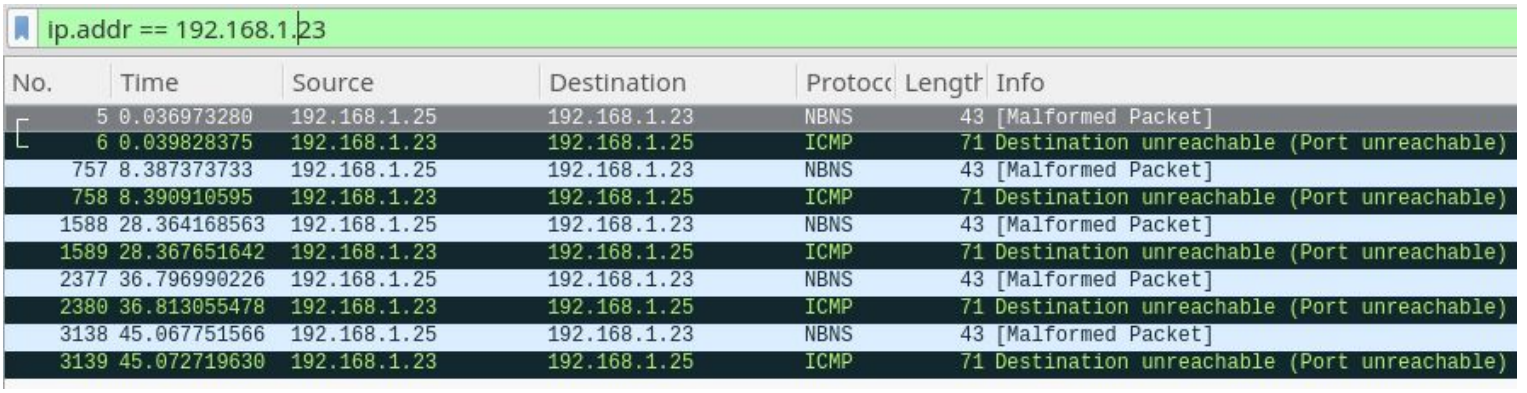
No.	Time	Source	Destination	Protocc	Length	Info
15	13.866294355	192.30.253.116	192.168.1.25	TLSv1.2	97	Encrypted Alert
16	13.866328534	192.168.1.25	192.30.253.116	TCP	66	57172 → 443 [ACK] Seq=1 Ack=32 Win=617 Len=0 TSval=3628093242 TSecr=1081173132
17	13.867006139	192.30.253.116	192.168.1.25	TCP	66	443 → 57172 [FIN, ACK] Seq=32 Ack=1 Win=30 Len=0 TSval=1081173132 TSecr=3628033393
18	13.867062571	192.168.1.25	192.30.253.116	TLSv1.2	97	Encrypted Alert
19	13.869127049	192.168.1.25	192.30.253.116	TCP	66	57172 → 443 [FIN, ACK] Seq=32 Ack=33 Win=617 Len=0 TSval=3628093245 TSecr=1081173132
20	13.978809726	192.30.253.116	192.168.1.25	TCP	60	443 → 57172 [RST] Seq=33 Win=0 Len=0
21	13.978906185	192.30.253.116	192.168.1.25	TCP	60	443 → 57172 [RST] Seq=33 Win=0 Len=0
47	37.095190323	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
48	37.102731141	fe80::b2ea:bcff:feb…	ff02::1	ICMPv6	90	Multicast Listener Query
49	37.102820358	fe80::b2ea:bcff:feb…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
50	37.102835152	fe80::ba27:ebff:fe5…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
51	37.108966396	fe80::ff0d:c2eb:708…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
52	37.114340739	fe80::a00:27ff:fe7b…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
54	37.316112927	192.168.1.19	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
58	40.606552853	192.168.1.25	81.19.96.148	NTP	90	NTP Version 4, client
59	40.655340918	81.19.96.148	192.168.1.25	NTP	90	NTP Version 4, server
286	162.129243268	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
287	162.129893220	fe80::b2ea:bcff:feb…	ff02::1	ICMPv6	90	Multicast Listener Query
288	162.129926546	fe80::b2ea:bcff:feb…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
289	162.134517964	fe80::ba27:ebff:fe5…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
290	162.139298437	fe80::a00:27ff:fe7b…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
291	162.141314259	fe80::ff0d:c2eb:708…	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
293	162.809676162	192.168.1.19	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251

Fuente: Elaboración Propia

Pero al analizar los paquetes que hay, no se logra identificar el tráfico de los clientes que se encuentran dentro del punto de acceso, así que se vuelve a realizar una segunda captura de paquetes.

Con la segunda prueba tampoco se logra identificar los paquetes que sean de los clientes que se encuentran dentro del punto de acceso.

Lo que se logra identificar es el ataque que se le hace al punto de acceso.


ip.addr == 192.168.1.23

No.	Time	Source	Destination	Protocc	Length	Info
5	0.036973280	192.168.1.25	192.168.1.23	NBNS	43	[Malformed Packet]
6	0.039828375	192.168.1.23	192.168.1.25	ICMP	71	Destination unreachable (Port unreachable)
757	8.387373733	192.168.1.25	192.168.1.23	NBNS	43	[Malformed Packet]
758	8.390910595	192.168.1.23	192.168.1.25	ICMP	71	Destination unreachable (Port unreachable)
1588	28.364168563	192.168.1.25	192.168.1.23	NBNS	43	[Malformed Packet]
1589	28.367651642	192.168.1.23	192.168.1.25	ICMP	71	Destination unreachable (Port unreachable)
2377	36.796990226	192.168.1.25	192.168.1.23	NBNS	43	[Malformed Packet]
2380	36.813055478	192.168.1.23	192.168.1.25	ICMP	71	Destination unreachable (Port unreachable)
3138	45.067751566	192.168.1.25	192.168.1.23	NBNS	43	[Malformed Packet]
3139	45.072719630	192.168.1.23	192.168.1.25	ICMP	71	Destination unreachable (Port unreachable)

Fuente: Elaboración Propia

Se procede a continuar con el siguiente paso que es capturar paquetes dentro del punto de acceso.

Para lograrlo se procede a realizar otro ataque parecido, pero esta vez a una máquina cliente en concreto que se encuentra dentro del punto de acceso.

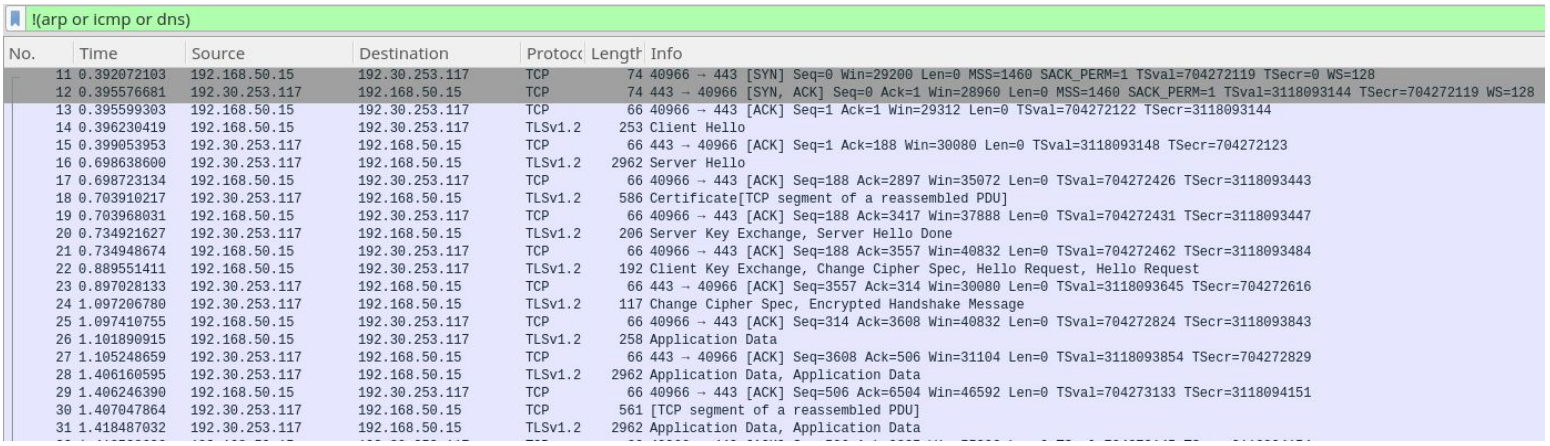
Una vez se procede a hacer el ataque, se pone en marcha de nuevo el wireshark, para capturar los paquetes del cliente.

El cliente procede a navegar por páginas http para hacer más vulnerable el servicio TOR y poder identificar mejor los paquetes.

Filtros utilizados:

!(arp)
!(arp or icmp)
!(arp or icmp or dns)
ip.addr == 192.168.50.10

A la hora de analizar los paquetes se puede observar que hay paquetes encriptados, aunque se haya navegado por páginas http.



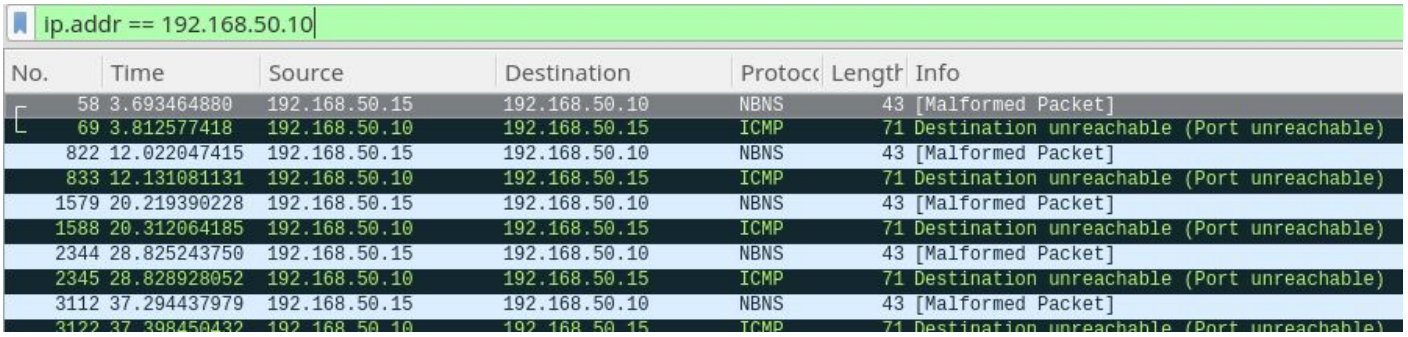
!(arp or icmp or dns)

No.	Time	Source	Destination	Protocc	Lengtl	Info
11	0.392072103	192.168.50.15	192.30.253.117	TCP	74	40966 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=704272119 TSecr=0 WS=128
12	0.395576681	192.30.253.117	192.168.50.15	TCP	74	443 → 40966 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3118093144 TSecr=704272119 WS=128
13	0.395599303	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=704272122 TSecr=3118093144
14	0.396230419	192.168.50.15	192.30.253.117	TLSv1.2	253	Client Hello
15	0.399053953	192.30.253.117	192.168.50.15	TCP	66	443 → 40966 [ACK] Seq=1 Ack=188 Win=30080 Len=0 TSval=3118093148 TSecr=704272123
16	0.698638600	192.30.253.117	192.168.50.15	TLSv1.2	2962	Server Hello
17	0.698723134	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=188 Ack=2897 Win=35072 Len=0 TSval=704272426 TSecr=3118093443
18	0.703910217	192.30.253.117	192.168.50.15	TLSv1.2	586	Certificate[TCP segment of a reassembled PDU]
19	0.703968031	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=188 Ack=3417 Win=37888 Len=0 TSval=704272431 TSecr=3118093447
20	0.734921627	192.30.253.117	192.168.50.15	TLSv1.2	206	Server Key Exchange, Server Hello Done
21	0.734948674	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=188 Ack=3557 Win=40832 Len=0 TSval=704272462 TSecr=3118093484
22	0.889551411	192.168.50.15	192.30.253.117	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
23	0.897028133	192.30.253.117	192.168.50.15	TCP	66	443 → 40966 [ACK] Seq=3557 Ack=314 Win=30080 Len=0 TSval=3118093645 TSecr=704272616
24	1.097206780	192.30.253.117	192.168.50.15	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
25	1.097410755	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=314 Ack=3608 Win=40832 Len=0 TSval=704272824 TSecr=3118093843
26	1.101890915	192.168.50.15	192.30.253.117	TLSv1.2	258	Application Data
27	1.105248659	192.30.253.117	192.168.50.15	TCP	66	443 → 40966 [ACK] Seq=3608 Ack=506 Win=31104 Len=0 TSval=3118093854 TSecr=704272829
28	1.406160595	192.30.253.117	192.168.50.15	TLSv1.2	2962	Application Data, Application Data
29	1.406246390	192.168.50.15	192.30.253.117	TCP	66	40966 → 443 [ACK] Seq=506 Ack=6504 Win=46592 Len=0 TSval=704273133 TSecr=3118094151
30	1.407047864	192.30.253.117	192.168.50.15	TCP	561	[TCP segment of a reassembled PDU]
31	1.418487032	192.30.253.117	192.168.50.15	TLSv1.2	2962	Application Data, Application Data

Fuente: Elaboración Propia

Debido a que se puede observar que los paquetes están encriptados, se determina que aunque se navega por páginas http, la navegación a internet es segura.

En la captura se puede observar el ataque man in the middle que se le hace a la victima.



ip.addr == 192.168.50.10

No.	Time	Source	Destination	Protocc	Lengtl	Info
58	3.693464880	192.168.50.15	192.168.50.10	NBNS	43	[Malformed Packet]
69	3.812577418	192.168.50.10	192.168.50.15	ICMP	71	Destination unreachable (Port unreachable)
822	12.022047415	192.168.50.15	192.168.50.10	NBNS	43	[Malformed Packet]
833	12.131081131	192.168.50.10	192.168.50.15	ICMP	71	Destination unreachable (Port unreachable)
1579	20.219390228	192.168.50.15	192.168.50.10	NBNS	43	[Malformed Packet]
1588	20.312064185	192.168.50.10	192.168.50.15	ICMP	71	Destination unreachable (Port unreachable)
2344	28.825243750	192.168.50.15	192.168.50.10	NBNS	43	[Malformed Packet]
2345	28.828928052	192.168.50.10	192.168.50.15	ICMP	71	Destination unreachable (Port unreachable)
3112	37.294437979	192.168.50.15	192.168.50.10	NBNS	43	[Malformed Packet]
3122	37.398450432	192.168.50.10	192.168.50.15	ICMP	71	Destination unreachable (Port unreachable)

Fuente: Elaboración Propia

9.11 Pruebas de Funcionamiento de la Red I2P

Una vez se puso en marcha el servicio se realizó una prueba, en la que se intentó acceder a internet y lo que se obtuvo fue que no se podía acceder a internet.

Después de la prueba se pasó a configurar las iptables y también los parámetros de red, ancho de banda compartido, conexion clientes...

Después de configurarlo y se probó a verificar si ahora se podía navegar por internet y aun asi no se logró acceder a internet.

Debido a que se intentó varios intentos para que los clientes puedan acceder a internet sin poder conseguirlo y a la falta de tiempo se optó a no continuar con el servicio I2P y a seguir con TOR.

9.12 Control Raspberry

9.12.1 Usuarios y Contraseñas

Para más seguridad se debería de cambiar las contraseñas de los usuarios que lleva el sistema, porque de lo contrario cualquier persona que sepa la dirección de la raspberry e intente conectarse y vea que la contraseña no esta cambiada sería un fallo de seguridad dentro de nuestra red anónima, y además de que se debería de tener una contraseña segura y larga para cada usuario.

Un ejemplo de tener unas contraseñas demasiado fáciles de romper seria:
Al usuario root:

- sudo passwd root
  Contraseña antigua: sin contraseña
  Contraseña nueva: 123456789

Al usuario pi:

- sudo passwd pi
  Contraseña antigua: raspberry
  Contraseña nueva: 1234

9.12.2 Configuración Servidor SSH

Para poder administrar, instalar programàs remotamente en la raspberry, se debería tener instalado el servidor SSH.

Antes de comenzar a instalar el servicio ssh habría que actualizar la lista de repositorios y los paquetes de la raspberry:
"sudo apt-get update"
"sudo apt-get upgrade"

Para instalar el servidor ssh en el raspberry, abrimos la terminal y ejecutamos el siguiente comando:

- sudo apt-get install openssh-server

Para que cada vez que se inicie la raspberry el servicio del ssh server se inicie ejecutamos el siguiente comando:

- sudo systemctl enable ssh

9.12.3 Control Temperatura

Como las raspberrys se calientan mucho, sería recomendable tener un medio de refrigeración, como una ventiladora, un disipador o ambas juntas.

Para ver la temperatura hay dos maneras con un programa o por comandos, fallo del programa programa , por lo que

optamos crear un script, para que cada vez quisiéramos saber la temperatura solo ejecutemos el script [ayuda script].

Por si queremos crear más de un script creamos una carpeta llamada script, en el cual crearemos un fichero -> temperatura.sh, y si no lo creamos en la carpeta que queramos el fichero.

```
pi@raspberrypi:~ $ ls
Desktop    Downloads  Pictures  python_games  Videos
Documents  Music      Public    Templates
pi@raspberrypi:~ $ mkdir script
pi@raspberrypi:~ $ cd script/
pi@raspberrypi:~/script $ nano temperatura.sh
pi@raspberrypi:~/script $
```

Fuente: Elaboración Propia

Ahora dentro del fichero añadimos las líneas que necesitamos para controlar la temperatura de la cpu y gpu que son los que calientan y elevan la temperatura de la raspberry. Además podemos mostrar la fecha y el nombre de la raspberry.

```
  GNU nano 2.7.4                File: temperatura.sh

#!/bin/bash
cpu=$(cat /sys/class/thermal/thermal_zone0/temp)
echo "$(date) @ $(hostname)"
echo "----------------------------------------"
echo "Temperatura CPU ===> $((cpu/1000))'C"
echo "Temperatura GPU ===> $(/opt/vc/bin/vcgencmd measure_temp)"
echo "----------------------------------------"
```

Fuente: Elaboración Propia

Para ejecutar el script tenemos que otorgarle permisos de ejecución.
Con el chmod le cambiamos los permisos al fichero. Con el parámetro +x le otorgamos permisos de ejecución al fichero:
"sudo chmod +x temperatura.sh"

Comprobamos la temperatura de la raspberry.

```
pi@raspberrypi:~/script $ ./temperatura.sh
Tue 30 Jan 18:06:00 UTC 2018 @ raspberrypi
----------------------------------------
Temp.CPU => 35'C
Temp.GPU => temp=34.9'C
----------------------------------------
pi@raspberrypi:~/script $
```

Fuente: Elaboración Propia

9.13 Fallo Instalación Raspberry

Si a la hora de descomprimir solo nos descomprime una carpeta “MIRAMOS DENTRO” y si hay ficheros y carpetas -> lo que hacemos entonces sería, copiar el contenido de la carpeta dentro de la sd y volvemos a probar que encienda.

Si al final no enciende probar si es un fallo de la raspberry, probando de utilizar la SD en otra raspberry.

9.14 Error lm-sensor

Se intentó utilizar el programa lm-sensors para ver la temperatura de la raspberry pero hubo un problema, lo que sucedía es que no mostraba la temperatura de la raspberry y nos daba errores por lo que optamos por el script script.

9.15 Error Prueba 1

La primera prueba de funcionamiento de toda la configuración de los servicios obtuvimos un error.
Para lograr saber cual era el error, primero revise el status de todos los servicios
Como todo aparentaba estar bien decidí probar un enrutamiento diferente:

------->
Otra manera de salir a internet lo que tenemos que hacer es modificar el fichero -> “/etc/sysctl.conf”
Para ello hacemos una copia de seguridad del fichero -> “sudo cp /etc/sysctl.conf /etc/sysctl.conf.old”

Ahora entramos en el fichero para modificarlo ->
“sudo nano /etc/sysctl.conf”
Y nos vamos a la línea -> “#net.ipv4.ip_forward=1”.
En un principio se encuentra comentado con un ‘#’ lo único que tenemos que hacer es borrar ‘#’ y ya.
Para guardar la configuración -> “ctrl + o”
Para salir del nano -> “ctrl + x”

Ahora hacemos es establecer una conexión entre la tarjeta eth0 y wlan0, y que todo el tráfico pase por la tarjeta de red eth0:
“sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE”
“sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT”
“sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT”
Volvemos a guardar las iptables -> ‘sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"’

<------

Como la nueva manera de enrutar no funciona me decidí en revisar el journal(visor de sucesos del sistema), con el que pare y inicie uno a uno los servicios porque haci lo tenemos más fácil a la hora de revisar el error.

Una vez de haber terminado de reiniciar los servicios fui al journal -> “journalctl -xe”
revise todos los sucesos y vi que el servicio tor daba un error que cuando hacías un status en el servicio no salía, revise la configuración del servicio tor y lo repare.

Se puede revisar la configuración del tor con el siguiente comando:

tor --verify-config

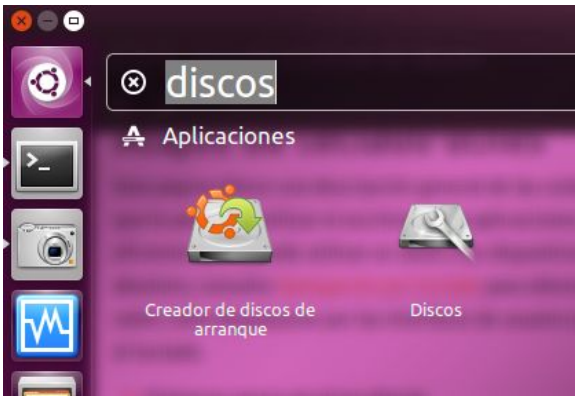
El comando indica si hay algún fallo en el fichero de configuración del servicio tor.

9.16 Tutorial USB cifrado

Para la creación del USB cifrado lo primero es instalar el repositorio que permite el cifrado, para ello abriremos un terminal y escribiremos el siguiente comando.

```
sudo apt-get install cryptsetup gnome-disk-utility
```

Una vez completado el paso anterior, para hacer el USB cifrado abrimos el apartado discos para formatearlo.



Fuente: Elaboración propia

Una vez sabemos el USB que queremos formatear, lo seleccionamos y le damos el formato [LUKS + ext4]

Fuente: Elaboración Propia

9.17 Error con USB Cifrado en Raspberry Pi 3

Nos encontramos con que la Raspberry Pi no guardaba la contraseña del USB Cifrado. Tras la búsqueda de información descubrimos que nos faltaba el programa gnome-keyring, así que fue instalado inmediatamente con el comando:

```
sudo apt-get install gnome-keyring
```

9.18 Tutorial NFS en Raspberry Pi 3

Servidor Raspberry Pi 3

Instalación NFS sobre Raspbian.

```
sudo apt-get install nfs-common nfs-server -y
```

Dar permisos sobre el USB.

```
sudo chmod -R 777 /media/pi/USBCifrado
```

Abrir el archivo de exportación de NFS donde se configuran las rutas para compartir y sus permisos.

```
sudo nano /etc/exports
```

Esta es la sintaxis para los recursos compartidos y permisos de NFS.

```
/media/pi/USBCifrado representa la ruta para
compartir en Raspbian
```

IP representa la dirección IP o rango y restringe ciertos tipos de acceso como leer y escribir (rw) o solo lectura (ro) también se puede usar * para decir que coja todas las IP's.

```
/[Ruta] "IP"("permisos",sync)

/media/pi/USBCifrado
192.168.18.0/24(rw,sync,no_subtree_check,no_root_squ
ash)
```

Al no poder hacerse de otra manera se tuvo que añadir el apartado “no_root_squash” que permite actuar como root en el servidor, no es algo muy seguro, pero fue la única manera de solucionar el uso de NFS.

Hay que decirle a NFS que lea el archivo exports recién creado.

```
sudo exportfs
```

Reiniciar servicio NFS.

```
sudo systemctl stop nfs-server
sudo systemctl start nfs-server
```

Cliente

Instalar el cliente NFS.

```
sudo apt-get install nfs-common -y
```

Crear el punto de montaje de nuestro recurso compartido NFS, esta es la carpeta virtual local que se usará para acceder a la carpeta en el servidor NFS.

```
sudo mkdir -p /mnt/raspbian
```

Cambiar los permisos del punto de montaje de NFS.

```
sudo chmod 777 /mnt/raspbian
```

Montar la ruta de acceso compartido del servidor NFS en el cliente NFS.

```
sudo mount 192.168.18.136:/media/pi/USBCifrado
/mnt/raspbian
```

9.19 Pruebas de seguridad descartadas

Para realizar las pruebas se descartaron Burp Suite, Zap, Arachni porque eran para verificar la seguridad de páginas web, pero lo que se necesita es verificar es que realmente se navega anonimamente por internet y que la red interna se encuentra a salvo de ataques.

Burp Suite:

Versión Profesional ->

Esta versión es la de pago con la que se obtiene más opciones a utilizar.

Versión Community ->

Esta es la versión gratuita con la que se obtiene menos opciones a utilizar pero con lo suficiente para analizar la red.

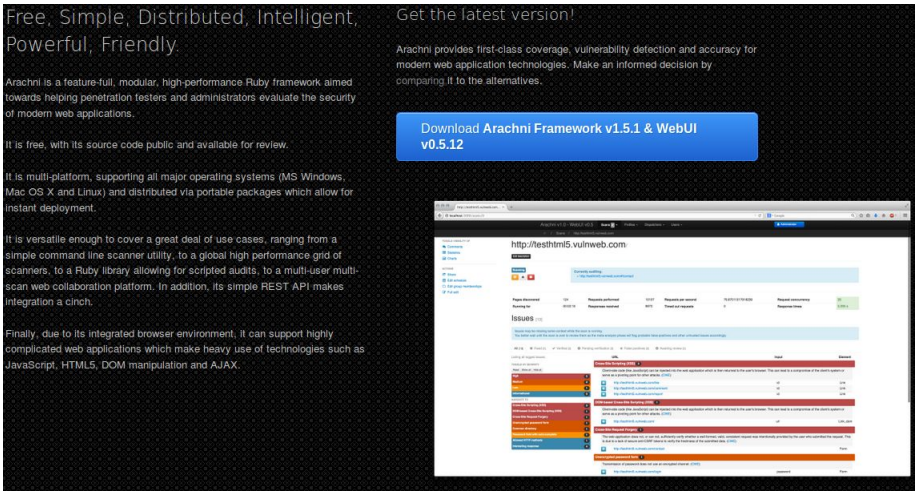
Fuente: https://www.e-spincorp.com/documentation/difference-between-burp-suite-free-and-paid-pro-version/

-> Arachni.

Para instalar el programa se puede elegir entre dos opciones, desde la página web o desde github.

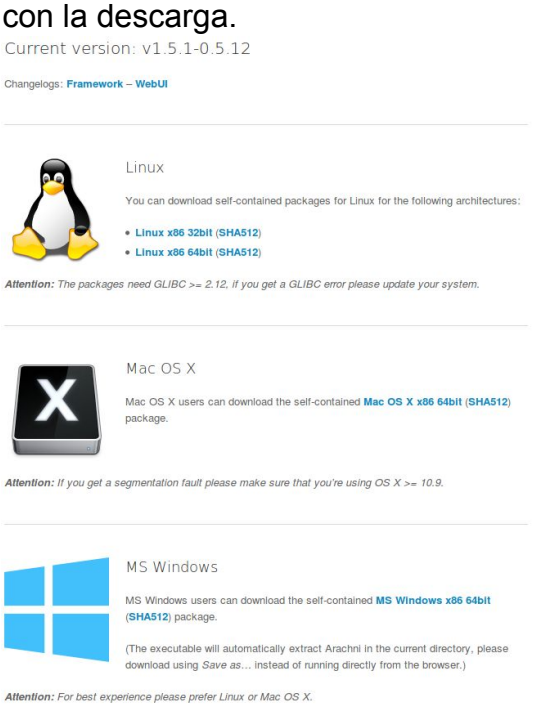
La instalación se realiza desde la página web del programa.

Una vez en la web del programa, en la pantalla principal aparece para descargar la última versión, se da un click encima para comenzar con la instalación.



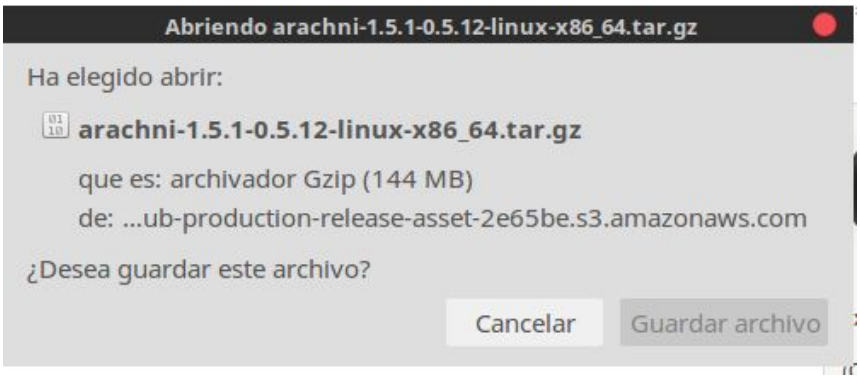
Fuente: http://www.arachni-scanner.com/

La siguiente pantalla se elige desde que tipo de sistema se utilizara el programa, en este caso es un linux de 64bits, con lo que se hace click sobre el enlace para comenzar con la descarga.



Fuente: http://www.arachni-scanner.com/download/

Saltará una ventana en la que pregunta que se desea hacer se le da sobre guardar y se espera a que se termine de descargar para continuar.



Fuente: Elaboración Propia

Una vez haya terminado de descargar se descomprime el fichero.
Primero se dirige a la carpeta en la que se encuentra descargado el programa.

"cd Descargas"

Descomprimir el fichero

"tar -xzvf arachni-1.5.1-0.5.12-linux-x86_64.tar.gz"

```
benjamin@benjamin-HP ~ $ cd Descargas/
benjamin@benjamin-HP ~/Descargas $ tar -xzvf arachni-1.5.1-0.5.12-linux-x86_64.tar.gz
arachni-1.5.1-0.5.12/
arachni-1.5.1-0.5.12/TROUBLESHOOTING
arachni-1.5.1-0.5.12/VERSION
```

Fuente: Elaboración Propia

```
benjamin@benjamin-HP ~/Descargas $ cd arachni-1.5.1-0.5.12/
benjamin@benjamin-HP ~/Descargas/arachni-1.5.1-0.5.12 $ cd bin/
benjamin@benjamin-HP ~/Descargas/arachni-1.5.1-0.5.12/bin $ ls
arachni                arachni_rpc                    arachni_web_create_user
arachni_console        arachni_rpcd                   arachni_web_import
arachni_multi          arachni_rpcd_monitor           arachni_web_scan_import
arachni_reporter       arachni_script                 arachni_web_script
arachni_reproduce      arachni_shell                  arachni_web_task
arachni_restore        arachni_web                    readlink_f.sh
arachni_rest_server    arachni_web_change_password
benjamin@benjamin-HP ~/Descargas/arachni-1.5.1-0.5.12/bin $
```

Fuente: Elaboración Propia

-> OWASP Zed Attack Proxy Project.(ZAP)

Para instalar el programa se debe de dirigir a la página principal del programa y hacer click sobre Download ZAP.

Fuente: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

La cual redirigirá al github del programa para descargarlo con varias opciones en la que da a elegir que sistema y que tipo de instalación se desea hacer, como en este caso se usa linux, se opta por descargar "Linux Package".

Downloads

Simon Bennetts edited this page 8 days ago · 198 revisions

Not sure how to start using ZAP? Read the Getting Started Guide (pdf).

Checksums for all of the ZAP downloads are maintained in the relevant version files.

As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.

ZAP 2.7.0 Standard

Windows (64) Installer	2017-11-28	111 MB	Download now
Windows (32) Installer	2017-11-28	75 MB	Download now
Linux Installer	2017-11-28	126 MB	Download now
Linux Package	2017-11-28	124 MB	Download now
MacOS Installer	2017-11-28	179 MB	Download now
Cross Platform Package	2017-11-28	230 MB	Download now

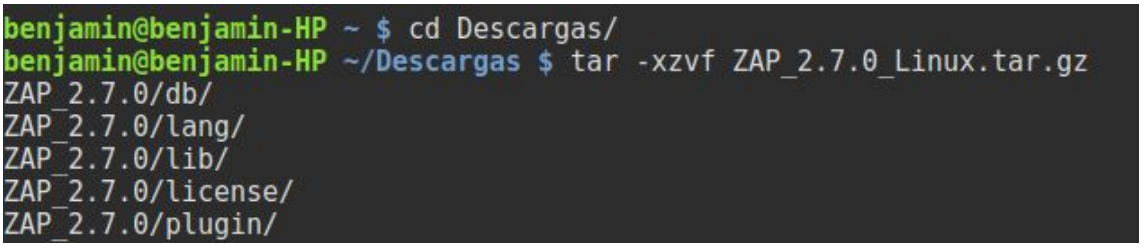
Fuente: https://github.com/zaproxy/zaproxy/wiki/Downloads

Una vez haya terminado de descargar se descomprime el fichero.
Primero se dirige a la carpeta en la que se encuentra descargado el programa.

"cd Descargas"

Descomprimir el fichero

"tar -xzvf ZAP_2.7.0_Linux.tar.gz"



Fuente: Elaboración Propia