Trabajo Final de Grado

Herramienta de gestión y análisis de redes bajo sistemas GNU/Linux

Autor: Álvaro Varela Sánchez

Tutor: Joaquín López Sánchez-Montañés

Diciembre 2021

Contexto

Siempre que se mencionan a los sistemas basados en UNIX, concretamente a sistemas operativos GNU/Linux, suelen asociarse a entornos complejos enfocados a experimentados desarrolladores y usuarios avanzados. El uso diario y configuraciones sencillas como por ejemplo la conexión a una red, pueden presentar verdaderos quebraderos de cabeza para el usuario final.

Por otro lado, dentro de estos mismos sistemas y aplicaciones de código libre, existe una rama enfocada a la infraestructura de red, y la gestión avanzada de los dispositivos como las tarjetas de redes wifi. Generalmente, este tipo de actividades suelen asociarse, de nuevo, a usuarios avanzados normalmente con una finalidad ofensiva para por ejemplo, identificar los dispositivos conectados a una red o la obtención de las claves de conexión a una red inalámbrica.

Así, el desarrollo de herramientas que faciliten al usuario menos avanzado, poder configurar de forma sencilla su conexión a Internet en sistemas operativos GNU/Linux, o tener control sobre su tarjeta de red o los equipos conectados a una red personal, suponen un gran avance para favorecer el uso de los sistemas de código libre.

Palabras clave: GNU, Linux, código libre, redes, wifi.

Object

Whenever UNIX-based systems are mentioned, specifically GNU/Linux operating systems, they are usually associated with complex environments focused on experienced developers and advanced users. Daily use and simple configurations such as connection to a network, can be a big headache for the end user.

On the other hand, within these same systems and free code applications, there is a branch focused on the network infrastructure and the advanced management of devices such as WiFi network cards. Generally these types of activities are associated with advanced users and offensive purposes, for example identifying the devices connected to a network or obtaining the connection keys from a wireless access point.

Thus the development of tools to help the less advanced users to be able to simply configure their Internet connection in GNU / Linux operating systems, or to have control over their network cards and connected devices to a personal network, supposes a great progress to promote the use of free code systems.

Keywords: GNU, Linux, código libre, redes, wifi.

índice

1 Introducción

1.1 Introducción a los sistemas GNU/Linux

Es muy común asociar la palabra Linux a un sistema operativo de código libre, pero en realidad esto no es del todo cierto. Linux fue creado por Linus Torvalds a partir del sistema operativo Unix y con la ayuda de la comunidad de desarrolladores. La idea principal radicaba en crear un sistema Unix avanzado y moderno que incluyese características tales como la multitarea, la gestión de memoria virtual y bibliotecas compartidas entre otras funcionalidades. Pero Linux no es un sistema operativo, sino una parte fundamental de este, que en realidad hace referencia al núcleo del sistema operativo conocido como «kernel», palabra de origen inglés. La principal idea de este desarrollo era poder crear un «software» de código libre apoyado en una comunidad de desarrolladores distribuidos por todo el mundo.

Si se pudieran resumir las funcionalidades del «kernel», habría que destacar la gestión de los distintos dispositivos a través de los controladores o «drivers», la gestión de la memoria virtual, el el manejo del sistema de ficheros y el desarrollo de los protocolos de comunicaciones de red. En definitiva, Linux permite al usuario utilizar los distintos elementos del equipo a través de un interfaz de usuario basado en aplicaciones, aplicaciones ajenas al núcleo y desarrolladas por terceros.

Como curiosidad mencionar que el logotipo de Linux es un pingüino.

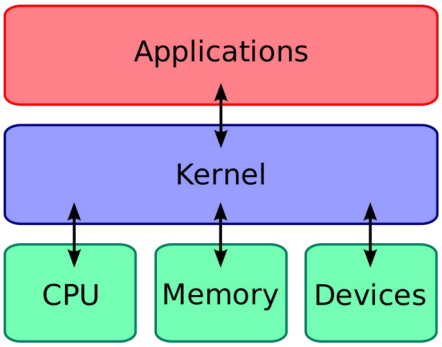

Imagen 1 - Ejemplo de kernel de Linux

Por otro lado encontramos el sistema operativo GNU, acrónimo en inglés para «GNU's Not Unix» , desarrollado originalmente por Richard Stallma y la comunidad de desarrolladores. Se compone de distintos programas desarrollados entre distintas personas y publicados de forma libre. GNU utiliza el núcleo de Linux para gestionar los recursos del equipo y que los distintos programas puedan utilizarlos, así, la combinación de ambas soluciones permite obtener un sistema operativo completo

y funcional, denominado distribución GNU/Linux. Existen innumerables distribuciones desarrolladas de manera completamente distinta compartiendo un denominador común, la base GNU/Linux. Cada una de estas distribuciones tiene un enfoque distinto, existen las que están dirigidas al usuario doméstico, otro grupo tienen en el punto de mira a usuarios más experimentados o desarrolladores. También encontramos distribuciones enfocadas al mundo académico, y las hay dirigidas a jugadores. Como vemos, un ecosistema muy diverso pero con una filosofía en común, programas de código libre apoyados en el kernel de Linux.

En este caso, el proyecto GNU utiliza un ñu como logotipo oficial.

Imagen2 - Proyecto Linux

Imagen 3 - Proyecto GNU

Dentro de esta amalgama de «software», encontramos aplicaciones o herramientas comunes en todos los sistemas. Un claro ejemplo es GNU Bash, una interfaz de usuario de línea de comandos desarrollada por la comunidad GNU. La idea principal de sus desarrolladores era la de sustituir la antigua shell sh y ser el intérprete de comandos predeterminado para la mayoría de las distribuciones GNU/Linux. Bash permite la ejecución de scripts o programas sencillos sin necesidad de una compilación previa. Al estar presente en la mayoría de distribuciones, facilita desarrollar soluciones con una amplia compatibilidad dentro del ecosistema Linux, permitiendo su ejecución en cualquier sistema operativo GNU/Linux.

1.2 Objetivos del trabajo

Se busca crear una aplicación sencilla que permita administrar las conexiones de red inalámbricas, las tarjetas de red wifi y analizar los distintos equipos conectados a una red. Todo esto estará enfocado hacia entornos GNU/Linux, utilizando el lenguaje de la shell Bash, presente en la gran mayoría de distribuciones.

Las principales características se describen a continuación:

- Adopción de una política de código libre en el desarrollo.
- Uso de sistemas operativos GNU/Linux.
- Sencillez y simplicidad en el uso, adaptado a los usuarios menos experimentados.
- Versatilidad en su funcionamiento y uso.
- Uso de herramientas estándar accesibles para todos los usuarios.

1.3 Planificación del trabajo

A continuación se detalla la planificación de trabajo establecida:

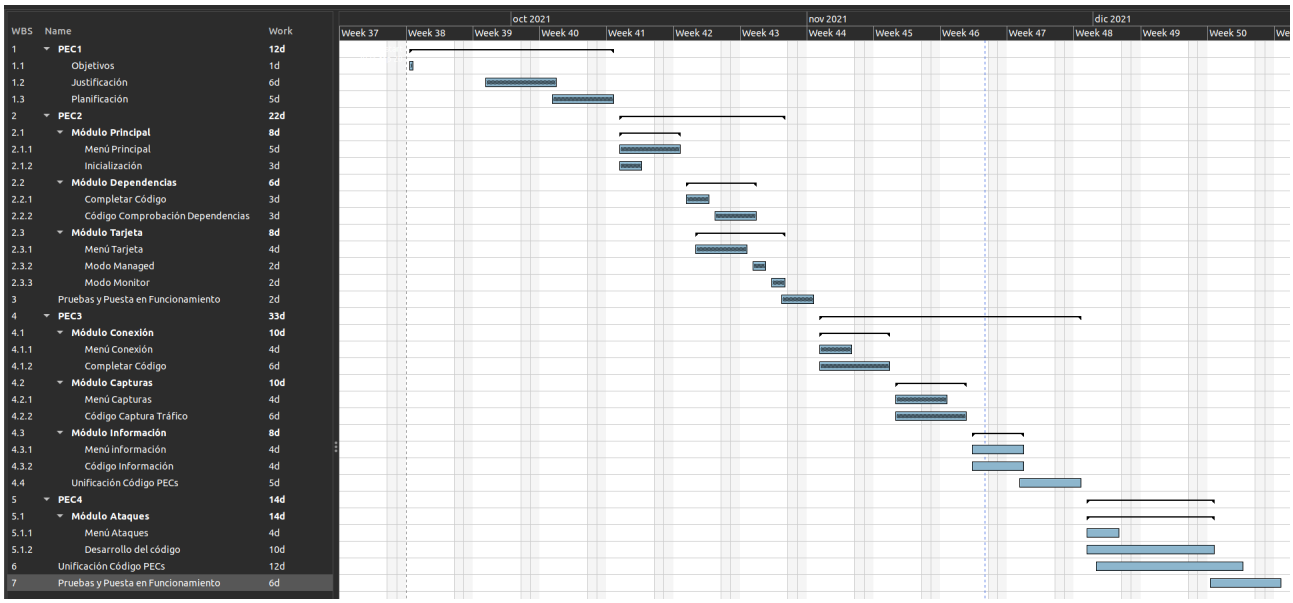

Figura 1 – Planificación del trabajo

1.4 Estudio económico

En general, los sistemas basados en GNU/Linux pertenecen a la comunidad gracias a las políticas de «software» libre. Esto implica que en raras ocasiones, el uso de este tipo de aplicaciones supone un coste para el usuario final. Pocas distribuciones GNU/Linux suponen algún gasto al usuario, un ejemplo de este tipo de «software» de pago es la versión «Red Hat Enterprise Linux», distribución enfocada a sistemas de servidor para empresas.

Además, todo el «software» utilizado en la creación de la documentación, las aplicaciones de planificación del trabajo, herramientas de edición de imágenes e incluso el entorno de desarrollo o IDE, se basan en código libre. A continuación se detallan los distintos programas utilizados y su función:

- Sistema operativo, Ubuntu 21.10.
- Navegador web, Mozilla Firefox.
- Editor de textos, LibreOffice Writer.

- Gestor de proyectos, Planner.
- Edición de imágenes, PhotoFlare.
- IDE, Sublime Text.
- Terminal de comandos, Gnome Terminal.

Por lo tanto, todos los sistemas «software» utilizados en este proyecto son de código libre sin coste alguno, reduciendo los gastos al mínimo. Son los elementos «hardware» los que suponen un desembolso mayor, concretamente el equipo de trabajo portátil y la tarjeta de red utilizada:

- Tarjeta de red
  - Marca: Tp-Link
  - Modelo: Archer T2UH
  - Descripción: adaptador USB wifi Dual-Band AC600
  - En ningún caso este dispositivo supera los 30 euros de gastos. También se han utilizado tarjetas de red integradas en el equipo de trabajo.
- Equipo de trabajo
  - Marca: HP
  - Modelo: OMEN 15
  - Descripción: El equipo no dispone de sistema operativo de fábrica. Está compuesto por un microprocesador «AMD Ryzen», una «GPU Nvidia», disco duro con tecnología «NVME» de 1TB y tarjeta wifi integrada de la marca «Intel».

Si bien este equipo supera los 1000 euros, no es necesario este nivel de equipamiento. Se han realizado pruebas sobre equipos más «modestos» obteniendo resultados igual de positivos. Más adelante, se detallarán los requisitos mínimos necesarios. Tampoco se han considerado necesarios añadir más elementos físicos para el correcto funcionamiento del sistema.

2 Requisitos del proyecto

2.1 Requisitos Hardware

Los requisitos necesarios para poder ejecutar de manera correcta este proyecto son excasos. Como mínimo, serán necesarios al menos 2 GigaBytes de memoria RAM, 20 GigaBytes de disco duro y un procesador con un al menos 2 núcleos y 4 hilos. A partir de estas especificaciones, cualquier equipo personal de trabajo permite ejecutar las herramientas necesarias de forma adecuada, pudiendo elegir un equipo de sobremesa o un equipo portátil personal. En este aspecto, existen distribuciones GNU/Linux, como por ejemplo Linux Mint, con requerimientos «hardware» bajos, necesitando únicamente 2 GigaBytes de memoria RAM y 20 GigaBytes de capacidad de disco. Esto

nos permite poder utilizar prácticamente cualquier equipo informático que tenga una antigüedad de hasta 15 años.

2.2 Requisitos Software

El principal requisito en este apartado es el uso de un sistema operativo basado en GNU/Linux con soporte para GNU/Bash. Concretamente y enfocado en este proyecto, se utiliza la distribución Ubuntu 21.10 «Impish Indri» versión de 64 bits desarrollada por la empresa Canonical. El entorno gráfico utilizado es «Gnome» versión 40.5; finalmente, la versión de la aplicación GNU/Bash instalada es la 5.1.8(1).

Si bien se ha elegido este sistema, se puede utilizar cualquier otra distribución que utilice la shell de «Bash», siendo esta una de las principales ventajas del sistema la diversidad de entornos compatibles. Todas las herramientas utilizadas son compatibles con distintos sistemas operativos dentro del cosistema GNU/Linux, destacando las siguientes distribuciones:

- Debian y derivados (Ubuntu, Linux Mint, Kali Linux, PopOS, etc.)
- Fedora, CentOS, RedHat.
- Arch Linux, Manjaro.
- OpenSuse.

Para el correcto funcionamiento de todo el conjunto, será necesario disponer de varias aplicaciones. En algunos casos estas herramientas estarán integradas en los distintos sistemas operativos, pero en otros entornos será necesario instalar en función de la distribución utilizada. En el apartado «Aplicaciones y Herramientas» se detallarán cada una de ellas, su función, los pasos de instalación si fuese necesario y el desarrollador de cada una de ellas.

2.2.1 Instalación y configuración Sistema Operativo

A continuación se describe el proceso de instalación y configuración del sistema operativo. Como ya se ha mencionado previamente, se utilizará un sistema GNU/Linux Ubuntu 21.10 64-bit.

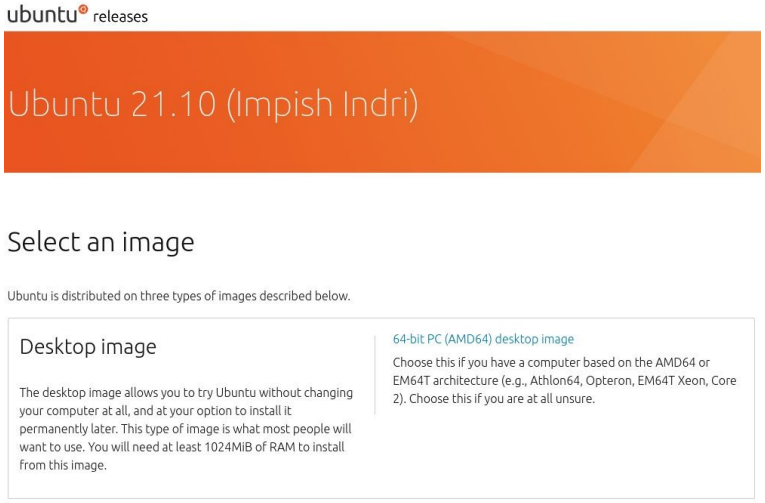

Figura 2 – Imagen de descarga de Ubuntu

En primer lugar es necesario descargar la imagen ISO de la web del desarrollador en el siguiente enlace:

https://releases.ubuntu.com/21.10/

En el propio sitio web aparecen los requisitos que debe cumplir el equipo de trabajo, resumidos en la tabla inferior:

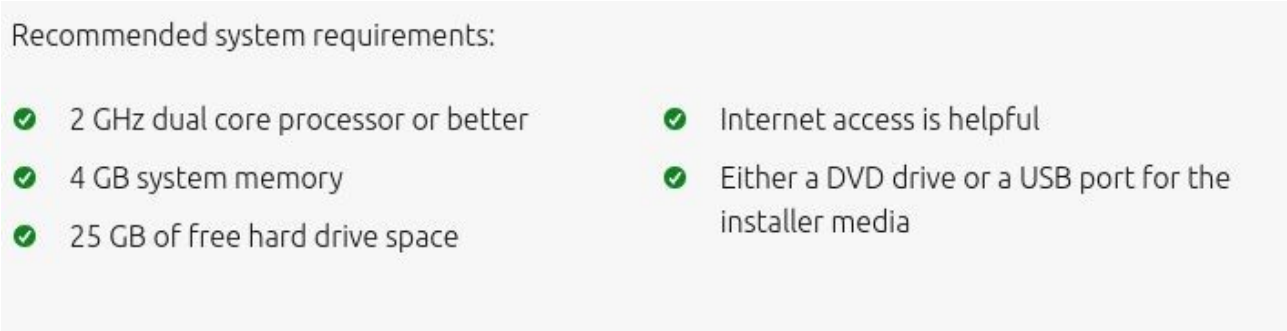

Figura 3 – Requisitos mínimos Ubuntu

Es el momento de instalar la imagen ISO en una memoria USB. Para ello y dependiendo del sistema operativo que estemos utilizando, existen múltiples herramientas para llevar a cabo esta acción. Por poner un ejemplo, si utilizamos Microsoft Windows como sistema, existe la herramienta «Rufus»; si por el contrario utilizamos una distribución Linux, existe «USB Creator». En ambos casos son simples ejemplos de código libre, pudiendo existir otras aplicaciones con las mismas funciones.

- Rufus. Disponible en: https://rufus.ie/es/
- USB Creator. Disponible en: https://www.linuxliveusb.com/

Dentro del sitio web de cada aplicación, se describe el método a seguir para poder generar una memoria USB con funcionalidades de auto arranque, partiendo de la imagen ISO descargada.

Una vez se cuenta con el dispositivo USB y la imagen de Ubuntu, comenzamos la instalación. Debemos iniciar el equipo a través de la memoria USB; esta acción dependerá del equipo y la

configuración de la BIOS utilizada. En caso de duda sobre este procedimiento, será necesario acudir a la web de fabricante del equipo para obtener mayor información de los pasos a seguir.

Comienza la instalación del sistema operativo en el equipo. Los siguientes pasos a seguir, serán con la elección del idioma, la selección de la ubicación geográfica, el destino de la instalación y el usuario y contraseña.

Posteriormente, seleccionamos la instalación normal, sin añadir «software» de terceros.

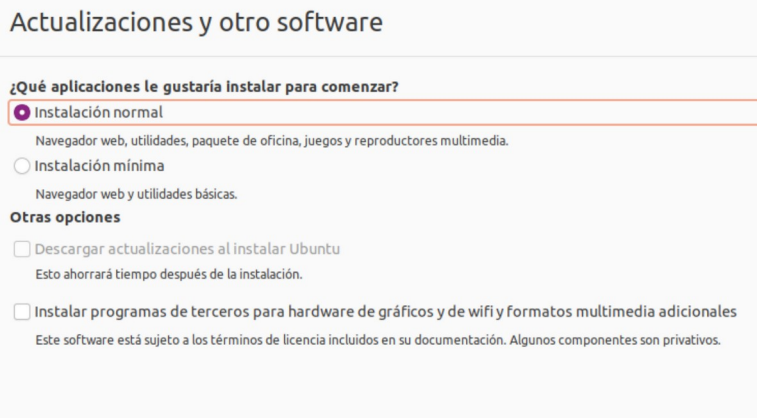

Figura 4 – Selección tipo de instalación

Ahora debemos seleccionar la forma en que el disco duro se va a estructurar, para ello, debemos elegir la opción por defecto, donde el propio programa crea las particiones necesarias para instalar el sistema adecuadamente, creando al mismo tiempo, los sistemas de ficheros.

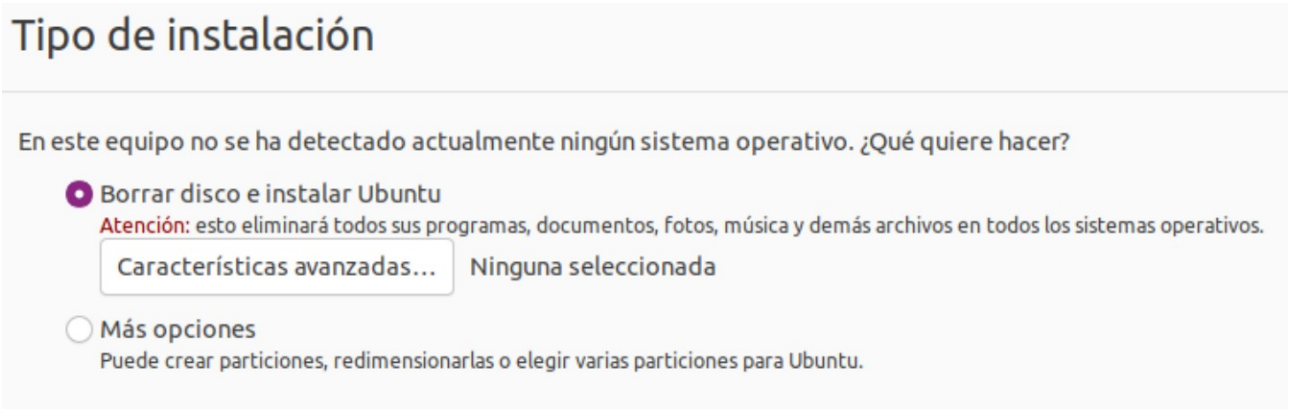

Figura 5 – Selección del disco de instalación

A continuación completamos la información solicitada con el nombre del equipo, y el usuario y la clave utilizadas. Tras estos pasos comienza la copia de los archivos.

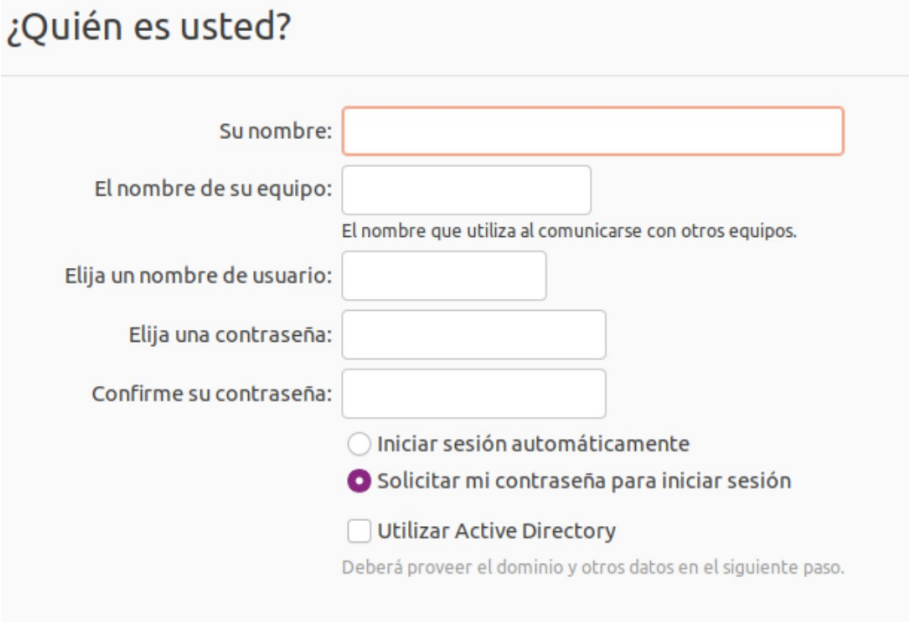

Figura 6 – Selección del usuario y contraseña

Al finalizar la instalación, el paso último requiere del reinicio del equipo para poder aplicar los cambios correctamente. Al presionar el botón de reinicio, un mensaje nos indicará que debemos retirar el USB de instalación antes de continuar.

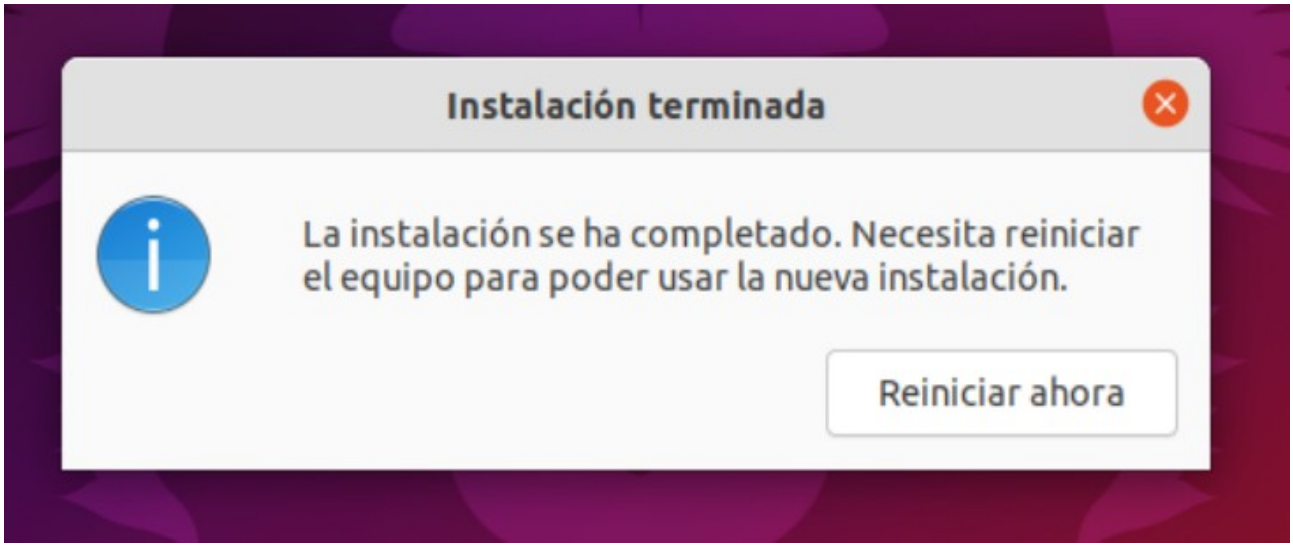

Figura 7 – Instalación finalizada

Una vez reiniciado el equipo, es hora de comenzar con la configuración del sistema y para ello empezamos actualizando los repositorios y todos los «paquetes» o programas instalados de origen. Para llevar a cabo esta actualización, utilizamos los siguientes comandos:

```
sudo apt update && sudo apt upgrade
```

Estos comandos y de forma general, son similares en todas las distribuciones GNU/Linux basadas en Debian. En caso de utilizar otro tipo de distribuciones, será necesario acudir a la documentación

del desarrollador para poder continuar con todos los pasos. En el caso de utilizar por ejemplo cualquier distribución basada en «Arch», los comandos a utilizar serán los siguientes:«»

```
sudo pacman -Syu
```

Una vez finalizada la actualización de todos los programas, será necesario reiniciar de nuevo el equipo de trabajo. Este proceso puede tardar bastante tiempo en función de la versión del sistema, la velocidad de la conexión a Internet y de las características del equipo.

2.2.2 Herramientas y Aplicaciones

El siguiente paso conlleva instalar todas aquellas herramientas y aplicaciones necesarias para la correcta ejecución de la aplicación. En muchas ocasiones y dependiendo de la distribución que el usuario esté ejecutando, muchos de estos programas estarán integrados en el propio sistema; aún así, a continuación se detalla como instalar cada una de ellas en la distribución de «Canonial», aunque en el resto de versiones de Linux se ha de actuar de manera similar, cada caso concreto dependerá de un comando específico. De nuevo se recuerda que existe documentación de cada distribución facilitada por el desarrollador.

Herramientas necesarias:

- aa-complain. Comando para establecer las políticas de seguridad de cada aplicación. Permite que ciertas aplicaciones se ejecuten correctamente sin fallos en los permisos de ejecución.
  - Comandos de instalación: `sudo apt install apparmor-utils`
  - Enlace: https://apparmor.net/
- aircrack-ng. Conjunto de herramientas enfocadas a la seguridad de redes inalámbricas. Contiene diversas aplicaciones con distintas funciones, entre las que se encuentran la monitorización, el ataque de redes y la captura de tráfico.
  - Comandos de instalación: `sudo apt install aircrack-ng`
  - Enlace: https://www.aircrack-ng.org/
- arp-scan. Herramienta de detección de equipos conectados a una red mediante el envío y recepción de mensajes utilizando el protocolo ARP.
  - Comando de instalación: `sudo apt install arp-scan`
  - Enlace: https://linux.die.net/man/1/arp-scan
- tcpdump. Aplicación para la captura y análisis de tráfico de red.
  - Comandos de instalación: `sudo apt install tcpdump`
  - Enlace: https://www.tcpdump.org/
- ip. Herramienta de manipulación de dispositivos de red.
  - Comando de instalación: `sudo apt install iproute2`

  - Enlace: https://linux.die.net/man/8/ip
- iw. Herramienta de manipulación de dispositivos de red wifi.
  - Comando de instalación: `sudo apt install iw`
  - Enlace: https://linux.die.net/man/8/iw
- iwlist. Herramienta de manipulación de dispositivos de red wifi.
  - Comando de instalación: `sudo apt install wireless-tools`
  - Enlace: https://linux.die.net/man/8/iwlist
- macchanger. Herramienta destinada a realizar cambios en la dirección «MAC» del dispositivo.
  - Comando de instalación: `sudo apt install macchanger`
  - Enlace: https://github.com/alobbs/«MAC»changer
- nmap. Aplicación de análisis de red.
  - Comando de instalación: `sudo apt install namp`
  - Enlace: https://nmap.org/
- tracepath. Aplicación de análisis de direcciones de rutas de red.
  - Comando de instalación: `sudo apt install iputils-tracepath`
  - Enlace: https://linux.die.net/man/8/tracepath
- tshark. Aplicación para la captura y análisis de tráfico de red.
  - Comando de instalación: `sudo apt install tshark`
  - Enlace: https://www.wireshark.org/docs/man-pages/tshark.html
- rfkill. Herramienta para habilitar o deshabilitar los dispositivos de red.
  - Comando de instalación: `sudo apt install rfkill`
  - Enlace: https://linux.die.net/man/1/rfkill

2.3 Requisitos de red

2.3.1 Introducción Redes

Dentro de la informática existe un campo dedicado a las redes de interconexión de dispositivos. Actualmente y debido a la influencia en la sociedad, su importancia es cada vez mayor. Dentro de este tipo de redes existen multitud de características y diferencias entre unas y otras, de mayor o menor tamaño, locales o compartidas, Internet, inalámbricas, etc., pero todas ellas se fundamentan en el mismo principio, crear una interconexión entre distintos dispositivos. Cada una de las distintas

redes tendrán una serie de características muy específicas, siendo una de las más importantes los dispositivos utilizados para poder crear el tipo de red específico y dar el servicio requerido.

Centrándonos en redes locales tipo LAN «Red de área local» y WLAN «Red de área local inalámbrica», en ambos casos serán necesarios una serie de periféricos o dispositivos enfocados a realizar tareas de gestión de redes. De forma genérica, cada dispositivo conectado a una red estará identificado por una dirección IP y una dirección MAC, y en todos los casos, siempre existirá un emisor y un receptor en todo comunicación. Estos son elementos necesarios en cualquier caso. A su vez, existirán dispositivos con mayor o menor importancia según la función que relicen.

A continuación se enumeran los periféricos de mayor importancia encargados de la gestión de la red:

- «Router» o encaminador en español; realiza tareas de interconexión de dispositivos estableciendo un camino de comunicación. Para ello, cada dispositivo se identifica mediante una dirección IP y un puerto específico a través de los cuales se envía y recibe la información generada. El «router» es capaz de reconocer cada uno de los segmentos de direcciones IP y enviar un paquete específicamente a un destinatario en concreto, impidiendo que el resto de dispositivos reciban dicho tráfico. Como vemos, un mismo encaminador tendrá asignadas varias direcciones IP lo que le permite realizar traducciones o comunicaciones entre distintas redes. Este tipo de dispositivos pueden contener características inalámbricas, realizando las mismas funciones pero adaptadas a entornos inalámbricos.

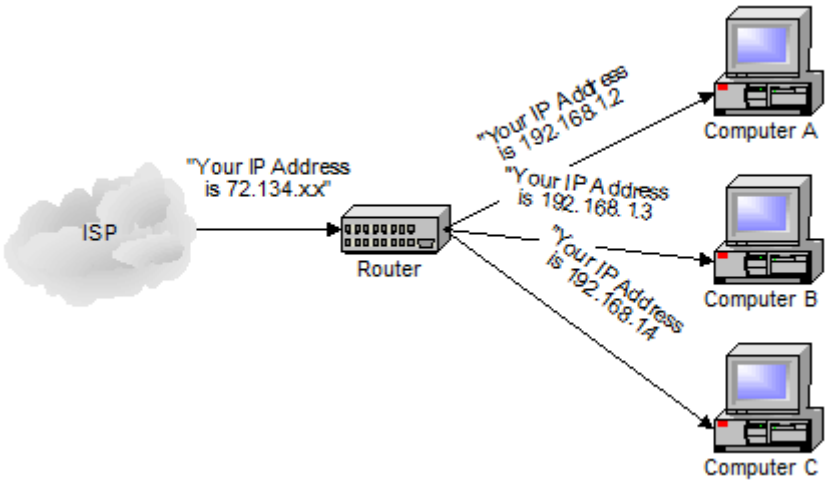

Imagen 4 – Funcionamiento Router

- «Switch» o conmutador en español; de nuevo realiza tareas de interconexión de dispositivos estableciendo un camino de comunicación, pero en este caso utiliza las direcciones MAC para establecer el camino de la comunicación. La comunicación se retransmite únicamente a los dispositivos involucrados en la conversación identificados con la dirección MAC correspondiente.

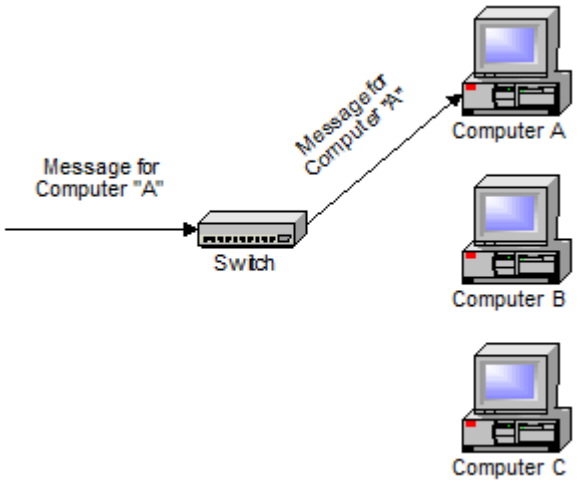

Imagen 5 – Funcionamiento Switch

En ambos casos, existe un tipo de tráfico transmitido a toda la red denominado «broadcast». Estos paquetes de información son visibles para todos los integrantes de la red y normalmente tienen una función muy concreta, gestionar la red y los distintos servicios de los dispositivos. En ocasiones, este tipo de tráfico puede albergar información relativa a los periféricos que la gestionan, pudiendo ser de utilidad a posibles atacantes.

2.3.2 Introducción Redes inalámbricas

En primer lugar debemos conocer, al menos de manera genérica, el funcionamiento básico de las redes wifi para poder comprender posteriormente el funcionamiento del «script» y de las distintas características implementadas. Debemos comenzar partiendo de la base de que las redes inalámbricas como bien indica su nombre, utilizan el aire como medio de transporte, a diferencia de las redes tradicionales las cuales utilizan medios físicos como el cableado de cobre. Existe una normativa Europa donde se regulan las bandas permitidas para la transmisión de datos y el ancho de los canales así como la potencia utilizada. De forma resumida, existe la banda de 2,4GHz que comprende los canales desde el número 1 (2412 MHz) hasta el número 14 (2484 MHz). Por otro lado se encuentra la banda de 5GHz, utilizando los canales desde el número 36 (5180 MHz) hasta el canal 165 (5825 MHz). Existe una tercera banda de 6GHz pero de momento es una tecnología en proceso de expansión y no se encuentran dispositivos con esta capacidad de manera extendida.

En España, al igual que en Europa, el uso de estas frecuencias está regulado y únicamente se permite el uso de los canales 1-13 en frecuencias de 2,4GHz, y de los canales del 36 al 64 y del 100 al 140 en lo que a la banda de 5GHz se refiere. En ambos casos la potencia máxima permitida oscilará entre los 23dBm y los 30dBm.

A continuación se muestran dos gráficos con los distintos canales y su frecuencia de transmisión:

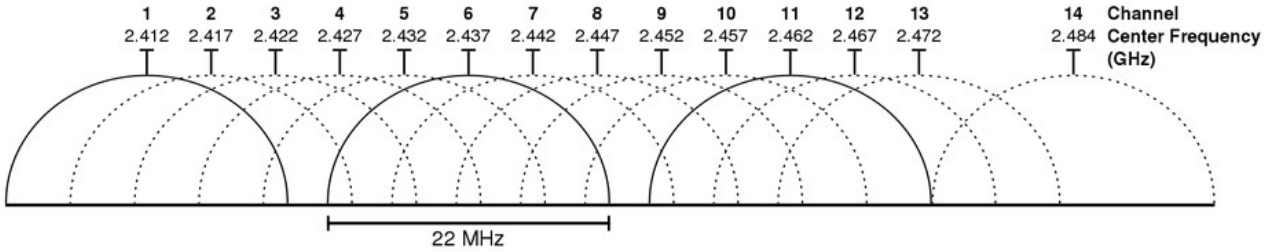

Imagen 6 – Frecuencias 2,4GHz

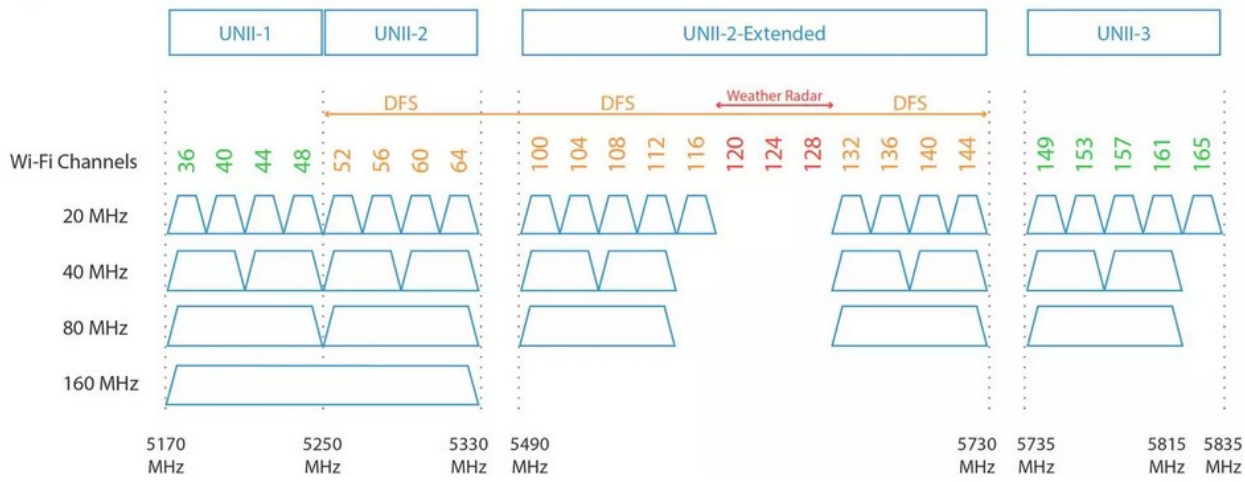

Imagen 7 – Frecuencias 5GHz

Por otro lado, debemos entender que las redes wifi utilizan las mismas herramientas o protocolos para el intercambio de información que una red cableada normal, la única diferencia sustancial es la creación de una nueva capa externa de radio la cual permite gestionar los atributos necesarios para la conexión mediante tarjetas inalámbricas. Todos estos nuevos estándares técnicos se definen en el conjunto de normas *IEEE 802.11 wireless LAN*, definidas por el Instituto de Ingenieros Eléctricos y Electrónicos o IEEE.

Para realizar una conexión, todo equipo o STA (station) debe disponer de una tarjeta de red wifi, capaz de enlazar con puntos de acceso o AP (Acces Point) o con otro dispositivo con capacidades inalámbricas. Este tipo de tarjetas se encuentran en la mayoría de dispositivos actuales, desde televisiones y enchufes inteligentes, hasta ordenadores y teléfonos móviles. Cada tarjeta wifi posee una única dirección «MAC» (Media Access Control) que la distingue del resto.

El proceso de conexión es sencillo, debemos localizar el punto de acceso mediante el nombre de la red, conocido como «SSID» (Service Set Identifier), además de poseer la clave que nos otorga el acceso necesario. Todo punto de acceso es único, y se identifica mediante su «SSID» y su «BSSID» (Basic Service Set), este último corresponde con la dirección «MAC» del AP.

Además de las características necesarias para poder enlaza con una red wifi, existen algunas tarjetas que pueden cambiar el modo de funcionamiento. Existe distintos modos con diversas funcionalidades, por ejemplo el modo «managed» o administrativo se identifica como la forma de

trabajo más común, gracias a la cual se pueden realizar conexiones a puntos de acceso. Por otro lado encontramos el modo «monitor», presente únicamente en ciertas tarjetas y que permite realizar análisis de redes de forma pasiva, «escuchando» el entorno e identificando los distintos equipos inalámbricos. Existen otros modos de funcionamiento que no veremos en este proyecto al no considerarse relevantes en nuestro sistema.

Por último, debemos conocer como se produce la conexión a una nueva red, proceso denominado como fase de «4-way handshake». Básicamente lo que se produce es un intercambio de mensajes entre el dispositivo y el AP mediante el protocolo «EAPOL» (Extensible authentication protocol over LAN); estos mensajes utilizan unas claves que permiten validar el dispositivo, para posteriormente cifrar la comunicación.

Existen diversos algoritmos de cifrado, WEP, WPA, WPA2 y WPA3, siendo el protocolo WEP el menos seguro y el WPA3 el más seguro y moderno. En cualquier caso, el protocolo más extendido corresponde a WPA2, aunque la intención es implementar WPA3 en todos los AP lo antes posible, lo que permitiría aumentar la robustez y seguridad de las comunicaciones wifi.

A continuación se muestra un esquema del intercambio de claves:

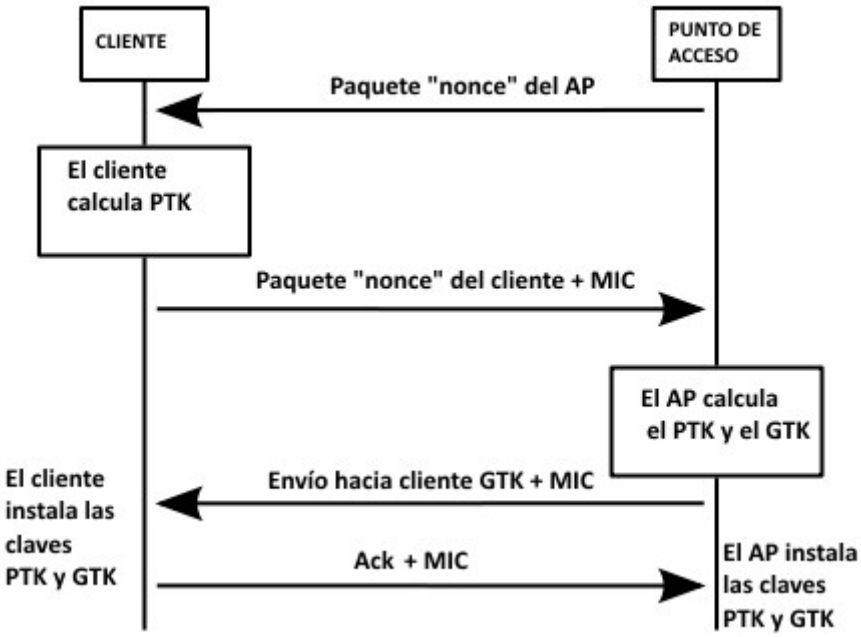

Imagen 8 – 4-way Handshake

2.3.3 Elementos Hardware

Hasta ahora, hemos visto todos los requisitos que debe cumplir el equipo de trabajo, su sistema operativo y todo lo necesario para su ejecución. También hemos identificado los dispositivos involucrados en la gestión de una red y la forma en que un dispositivo se conecta a la misma. Ahora, se detallarán las especificaciones de una red inalámbrica. En primer lugar y como requisito fundamental, es necesario disponer de una tarjeta inalámbrica con especificaciones 802.11, en

concreto tarjetas que soporten los protocolos 802.11b, 802.11g y 802.11n, frecuencias utilizadas normalmente en España. Las potencias utilizadas nunca deben superar los 20dBm. Los protocolos 802.11b, 802.11g y 802.11n establecen las características de la banda de 2.4GHz; 802.11a y 802.11ac especifican los atributos de la banda de 5GHz sin que superen potencias máximas de 30dBm.

Este tipo de requisitos los cumplen la mayoría de tarjetas de red inalámbricas que se venden en la actualidad, incluyendo a todas las tarjetas integradas en los equipos personales de trabajo o portátiles.

Para obtener mayor información sobre la tarjeta wifi, se podrán utilizar cualquiera de estos comandos:

```
lspci -v | grep -i network
```

```
lshw -class network
```

Concretando los sistemas utilizados en este proyecto, en todas las pruebas de desarrollo se han utilizado 2 tarjetas de red distintas, la primera corresponde a la tarjeta integrada en el equipo de trabajo mencionado en apartados anteriores. Concretamente es una tarjeta del fabricante «Intel» modelo «Wi-Fi 6 AX200».

Imagen 9 - Intel Wi-Fi 6 AX200

La segunda tarjeta utilizada corresponde al modelo «Archer T2UH» del fabricante «Tp-Link». En este caso y al ser un dispositivo conectado a través del puerto USB, deberemos utilizar el siguiente comando para obtener información detallada:

```
lshw -class network
```

Imagen 10 - Tp-Link Archer T2UH

A continuación se adjunta una tabla con las especificaciones inalámbricas de la tarjeta «Archer T2UH»:

CARACTERÍSTICAS INALÁMBRICAS	
Estándares Inalámbricos	IEEE 802.11ac, IEEE 802.11a, IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frecuencia	5GHz 2.4GHz
Tasa de Señal	5GHz 11ac: Hasta 433Mbps (dinámico) 11a: Hasta 54Mbps (dinámico) 2.4GHz 11n: Hasta 150Mbps (dinámico) 11g: Hasta 54Mbps (dinámico) 11b: Hasta 11Mbps (dinámico)
Sensibilidad de Recepción	5GHz： 11a 6Mbps: -94dBm 11a 54Mbps: -78dBm 11n HT20 MCS0: -94dBm 11n HT20 MCS7: -77dBm 11n HT40 MCS0: -92dBm 11n HT40 MCS7: -74dBm 11ac VHT80 MCS0: -89dBm 11ac VHT80 MCS9: -64dBm 2.4GHz: 11b 1Mbps: -99dBm 11b 11Mbps: -91dBm 11g 6Mbps: -94dBm 11g 54Mbps: -77dBm 11n HT20 MCS0: -95dBm 11n HT20 MCS7: -76dBm 11n HT40 MCS0: -92dBm 11n HT40 MCS7: -73dBm

Figura 8 – Especificaciones Archer T2UH

Otro de los requisitos necesarios en el desarrollo, es la de disponer de un punto de acceso inalámbrico o AP, bien un router con conexión wifi, bien un repetidor o cualquier otro equipo con la capacidad de crear una red inalámbrica. Para realizar las prácticas de este proyecto, se han utilizado una pareja de puntos de acceso de redes inalámbricas «wifi mesh» de la marca «Tenda» y modelo «MW3».

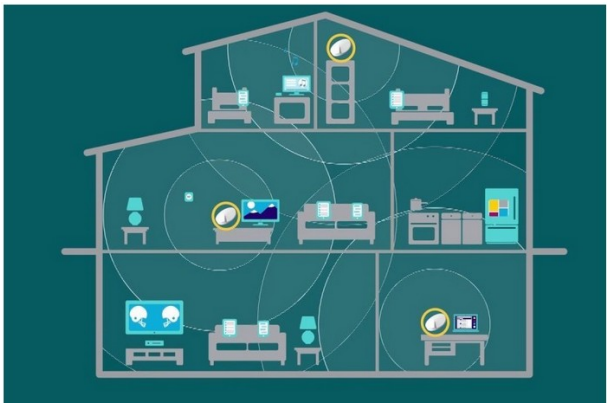

Imagen 11 - Ejemplo de red «wifi mesh» en un hogar

Las redes «wifi mesh» son una solución frente a la gran cantidad de dispositivos conectados, como al reparto del ancho de banda, que sufren las redes inalámbricas en la actualidad. La gran demanda de este tipo de redes, ha generado una nueva necesidad de administrar correctamente el tráfico generado y los dispositivos conectados. «wifi mesh»utiliza una estructura en malla compuesta por la estación base principal, normalmente el «router», y equipos satélite distribuidos por las distintas estancias. Todos estos elementos se comunican entre ellos creando una red «única» de cara al usuario. Este tipo de redes son capaces de calcular cuál de los equipos satélites es el más apropiado para establecer una conexión con un equipo en concreto y así garantizar el mayor ancho de banda posible, intercambiando información entre los distintos nodos. Esto reduce la carga de un AP distribuyendo los dispositivos entre los equipos satélites.

2.3.4 Instalación y configuración de los elementos de red

A continuación se muestra el proceso de configuración del entorno de trabajo. Comenzamos por comprobar el controlador de la tarjeta de red utilizando el siguiente comando:

```
lshw -class network
```

Resultado:

```
logical name: wlx18a6f70bccc5
configuration: broadcast=yes driver=mt76x0u driverversion=5.13.0-20-generic firmware=N/A link=no multicast=yes wireless=IEEE 802.11
```

Con esto, hemos obtenido el nombre de la tarjeta de red «wlx18a6f70bccc5» y el driver utilizado «mt76x0u».

3 Análisis y diseño

Una vez establecidos los requisitos del sistema, vamos a explicar la principal tarea de esta aplicación, facilitar la gestión de los sistemas de red en un entorno GNU/Linux a través del intérprete de comandos. Para ello se utiliza «Bash», el intérprete de comandos Linux, como entorno de desarrollo y presente en la mayoría de distribuciones actuales. Esta elección se fundamenta en la

facilidad, versatilidad y compatibilidad con el gran abanico de sistemas Linux presentes; de esta manera cualquier usuario de Linux, podrá utilizar esta aplicación sin ningún tipo de problemas y sin la necesidad de instalar librerías externas. Otro entorno de desarrollo podría haber utilizado el lenguaje de programación «Python», pero sería necesario instalar el propio programa «Python» en su versión correcta y utilizar distintas librerías para poder ejecutar aplicaciones externas del sistema Linux. El uso de «Bash» permite ejecutar directamente las herramientas sin necesidad de librerías que intervengan en las interconexiones, además de simplificar el control sobre el sistema operativo.

Por otro lado, sería necesario que todos los equipos además de cumplir los requisitos propios de las herramientas de Linux, cumplan con los requisitos del lenguaje utilizado. Siguiendo con el ejemplo de «Python», sería necesario saber para qué versión se ha desarrollado, qué librerías son necesarias y su retro compatibilidad con versiones anteriores del lenguaje. Utilizando el intérprete de comandos «Bash» evitamos todos esos inconvenientes, manteniendo todas las funcionalidades sin que el programa se vea mermado en cuanto a funcionalidades se refiere.

Una vez elegido el lenguaje correcto de desarrollo, el código se divide en módulos debido a la cantidad de funcionalidades y extensión. De esta forma, el código será mucho más legible y fácil de entender. La programación modular facilita la solución de problemas y corrección del código, y la reutilización de funcionalidades en tareas repetitivas que se ejecutan múltiples veces. Por este motivo se crean 6 módulos principales:

- Módulo Conector. Este módulo será el encargado de iniciar el programa y comprobar que los argumentos son los correctos. Mostrará un menú principal el cual permitirá el acceso a los distintos módulos con sus funcionalidades correspondientes.
- Módulo tarjeta. En este apartado, se desarrollan todas las características que afectan a la tarjeta directamente. Se trata de cambiar los modos de la tarjeta, modo monitor y modo «managed», reiniciar la tarjeta y realizar un cambio de dirección «MAC» y cambiar el «hostname» del equipo. Dispondrá de un menú específico para estas opciones.
- Módulo conexión. Aquí se ofrecen las herramientas necesarias para gestionar las conexiones de red; conectarse a una red, desconectarse, eliminar conexiones previamente almacenadas entre otros. También ofrece la posibilidad de realizar una búsqueda de los puntos de acceso del entorno.
- Módulo análisis. Permite analizar una red, a la que previamente se ha realizado una conexión. Facilita la obtención de información como los dispositivos conectados y el fabricante de los mismos, así como los servicios y puertos de cada equipo.
- Módulo captura. En esta sección, se habilitan las opciones de captura de tráfico, bien de una red previamente conectada, o del aire directamente, seleccionando la frecuencia y el canal o bien capturando todo el ancho de banda.
- Módulo ataques. Este apartado analiza posibles ataques realizados sobre una red conocida. La idea principal es poder detectar un posible ataque y al atacante, mediante técnicas de análisis de tráfico y protocolos.

Al mismo tiempo, se crean otros 3 módulos secundarios:

- Módulo canales. Esta sección se encarga de comprobar los canales y frecuencias admitidas por la tarjeta de red wifi seleccionada.
- Módulo dependencias. Esta parte del código comprueba que todas las herramientas y aplicaciones necesarias para ejecutar de manera correcta el proyecto, se encuentran instaladas.
- Módulo deauth. Por último, este módulo se utiliza como complemento del módulo ataques, permitiendo realizar ataques de deautenticación.

3.1 Módulo Principal

3.1.1 Características principales

El nombre del «script» principal es «Conector.sh». El programa se inicia con la llamada a este programa mediante la siguiente instrucción:

```
sudo ./Conector.sh «tarjeta de red»
```

Vemos que la invocación se divide en tres partes. La primera parte hace referencia a los permisos de usuario necesarios para ejecutar el «script». Mediante la palabra «sudo» forzamos una ejecución con privilegios de usuario root o administrador. «./Conector.sh» indica el fichero ejecutable que debemos seleccionar. Por último, el argumento «tarjeta de red» indica la tarjeta de red inalámbrica que el programa debe utilizar, proporcionada por el usuario.

Ejemplo de ejecución correcta:

```
sudo ./Conector.sh wlo1
```

A partir de aquí comienza la ejecución del módulo principal de la aplicación. En primer lugar se realizan ciertas comprobaciones para asegurar la correcta ejecución. El script comprueba que la llamada del programa contiene los argumentos necesarios, los privilegios de ejecución y el nombre de la tarjeta wifi.

Primero se comprueba que la tarjeta wifi indicada existe y si encuentran instalada en el sistema. Si este paso es correcto, se comprueba que el usuario efectivamente posee privilegios de usuario root a través de la siguiente sentencia:

```
if [ "$(/usr/bin/id -u)" != "0" ]
```

En Linux, el comando «id -u» muestra el usuario actual y su número de identificador. Por otro lado, el usuario «root» tiene asociado un valor de 0. Finalmente comparamos si el usuario actual, el que está realizando la ejecución del programa, tiene un identificar igual 0 o no.

Tras comprobar que los privilegios son los correctos, continúa el programa creando las carpetas necesarias para almacenar la información recopilada durante la ejecución del programa. Se crean las carpetas «Info» donde se guarda la información recopilada de los análisis de red, la carpeta «Logs»

donde se almacenan los logs de ejecución y la carpeta «Capturas», donde se guardan las posibles capturas de tráfico realizadas por el usuario.

A continuación se ejecuta una llamada al módulo «dependencias», donde se comprueba que todas las herramientas necesarias se encuentran instaladas en el sistema.

Finalmente se realizan comprobaciones relacionadas con la tarjeta de red y los servicios implicados en su gestión, a través de las herramientas «aa-complain» y «rfkill». La primera modifica los permisos de ejecución para que «tcpdump» funcione correctamente. La segunda habilita el uso de las tarjetas de red inalámbricas.

Por último se realiza la llamada al menú principal de la aplicación, mediante la función «general», mostrando al usuario la siguiente pantalla:

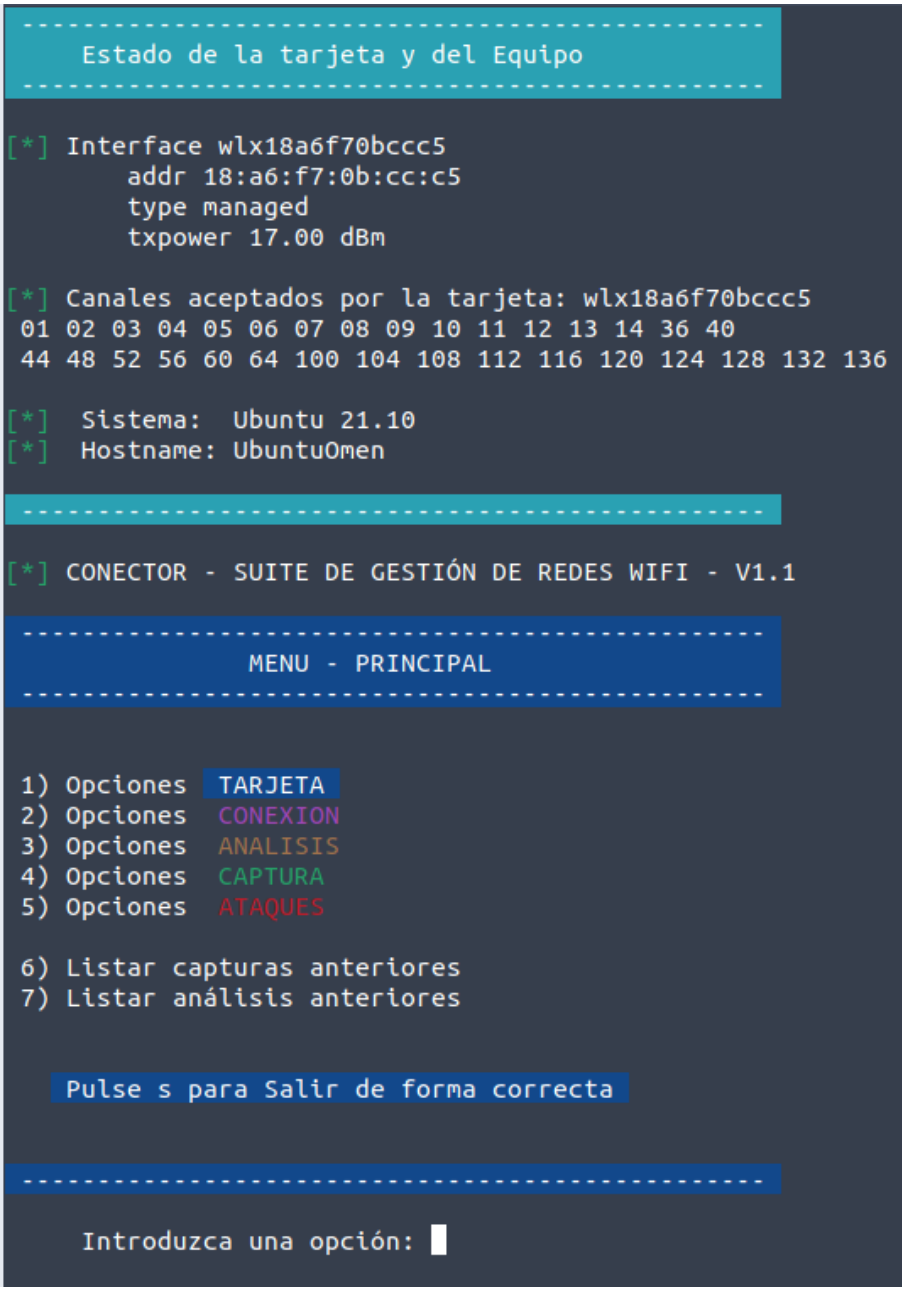

Figura 9 – Menú principal

Vemos que la pantalla se divide en dos zonas claramente diferenciadas por colores.

En la parte superior con un azul menos intenso encontramos la ventana de estado. Aquí se muestra en todo momento el estado de la tarjeta, el nombre de la misma, su dirección «MAC», el modo en el que se encuentra y la potencia máxima de la tarjeta. Se indican los canales soportados por la propia tarjeta, tanto en la banda de 2.4GHz como en la banda de 5GHz si se diese el caso. Un poco más abajo, se muestra la distribución GNU/Linux utilizada y el nombre del equipo o «hostname». Esta ventana de estado permanecerá a lo largo de toda la ejecución, reflejando en todas las opciones los cambios que se vayan produciendo durante la ejecución. Esto permite al usuario conocer en todo momento el funcionamiento de la tarjeta y su equipo.

La segunda parte destaca por un azul más intenso, y hace referencia al menú principal donde se ofrecien al usuario todas las posibilidades de la herramienta. El usuario deberá introducir el número de la opción que desee ejecutar.

Opciones:

1. «Opciones TARJETA» muestra todas las opciones relacionadas con la tarjeta wifi, como cambiar su modo de funcionamiento, cambiar el canal y la frecuencia, la dirección «MAC» o el «hostname».
2. «Opciones CONEXION» activará el módulo relacionado con la gestión de las conexiones de redes wifi.
3. «Opciones ANALISIS» ejecutará el módulo que permite realizar un análisis de una red internamente y recopilar infor«MAC»ión tal como los equipos conectados, analizar servicios, puertos, tráfico, etc.
4. «Opciones CAPTURA» permite realiza capturas de tráfico, bien de una red interna o bien del entorno del rango de alcance de la tarjeta inalámbrica.
5. «Opciones ATAQUES», este módulo permite analizar la red buscando posibles ataques sobre la misma.5)
6. «Listar capturas anteriores» muestra todas las capturas de tráfico realizadas con anterioridad.
7. «Listar análisis anteriores» muestra todos los análisis de red realizados con anterioridad.
8. s) «SALIR», finaliza la ejecución del programa de forma correcta, desactivando cualquier estado inconsistente de la tarjeta wifi e indicando si la tarjeta se encuentra conectada a una red, siendo este el caso, mostrará un mensaje ofreciendo la posibilidad de realizar una desconexión de forma ordenada.

3.1.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Comprobar los privilegios de ejecución
- Comprobar los argumentos introducidos en la llamada
- Crear los ficheros y carpetas necesarios
- Comprobar los programas instalados a través del módulo «dependencias»
- Mostrar el estado actual de la tarjeta y el sistema
- Mostrar el menú principal de la aplicación

3.2 Módulo Dependencias

3.2.1 Características principales

En este apartado, el programa realiza una comprobación de loa requisitos necesarios para la ejecución de manera correcta. Para ello, busca en el sistema un listado de comandos y comprueba que están instalados correctamente. De no ser así, se ofrece al usuario la posibilidad de instalarlos; en caso contrario, se muestra un mensaje de advertencia, indicando la posibilidad de que las distintas características no se ejecuten debidamente.

Durante el proceso de comprobación, se informa al usuario el estado de cada una de las herramientas, y si la herramienta se encuentra instalada en el sistema o es necesario proceder a su instalación.

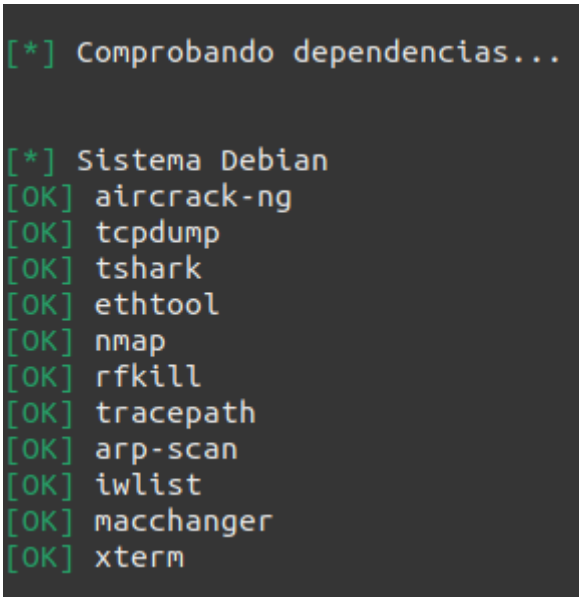

Figura 10 – Dependencias correctas

Si una de estas aplicaciones no estuviera integrada en el sistema operativo, se mostraría un mensaje al usuario ofreciendo la posibilidad de continuar sin esta aplicación o por otro lado, ejecutar un instalador.

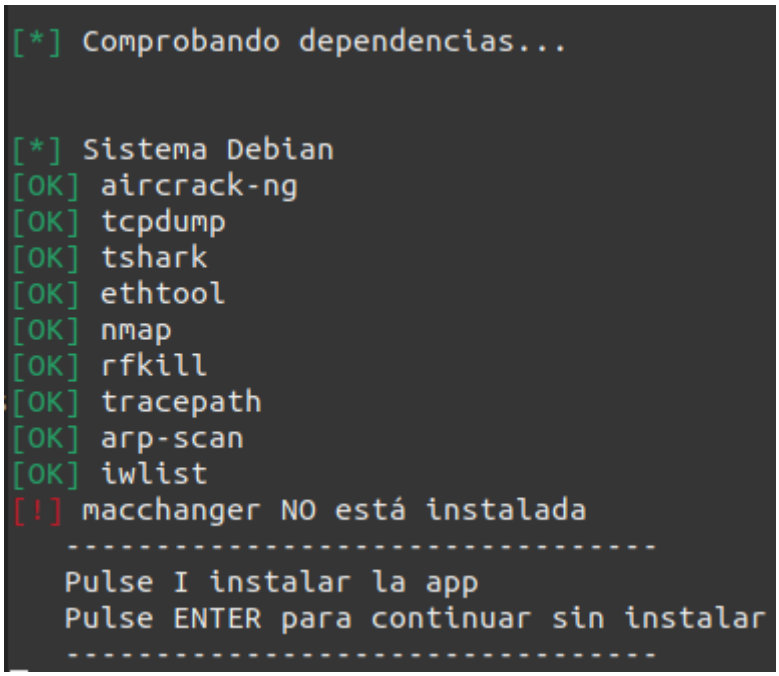

Figura 11 – Dependencias incorrectas

Una vez finalizada la comprobación de todas las herramientas, continúa el módulo principal generando el menú principal.

Las herramientas de las que se realiza una comprobación son las siguientes:

- aircrack-ng. Herramientas de seguridad de redes inalámbricas.
- arp-scan. Aplicación que permite identificar dispositivos en una red.
- Ethtool. Herramienta de manipulación dispositivos de red.
- ip. Herramienta de manipulación dispositivos de red.
- iw. Herramienta de manipulación dispositivos de redes wifi.
- iwlist. Herramienta de manipulación dispositivos de red.
- macchanger. Herramienta para modificar las direcciones «MAC» de las tarjetas de red.
- netdiscover. Herramienta de exploración de redes.
- nmap. Herramienta de exploración de redes y detección de vulnerabilidades.
- rfkill. Herramienta para habilitar dispositivos wifi.
- route. Herramienta de análisis de direcciones de rutas.
- tcpdump. Herramienta especializada en la captura y análisis de tráfico de red.
- tracepath. Herramienta que permite trazar el camino seguido hacia una dirección de red.
- tshark. Herramienta especializada en la captura y análisis de tráfico de red.

- xterm. Emulador de terminal.

3.2.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Comprobar los programas instalados.
- Ofrecer la posibilidad de instalar aquellos que no estén presentes.

3.3 Módulo Tarjeta

3.3.1 Características principales

Este tercer módulo se centra en la tarjeta inalámbrica de red. Ofrece al usuario la posibilidad de cambiar el estado de la tarjeta, su modo de funcionamiento, su dirección «MAC», el nombre del equipo o ««hostname»» y reiniciar la tarjeta.

Para ello, ofrece un menú interactivo al usuario donde puede elegir entre las distintas opciones. De nuevo se muestra en la parte superior la ventana de estado, facilitando al usuario el control del estado de los dispositivos.

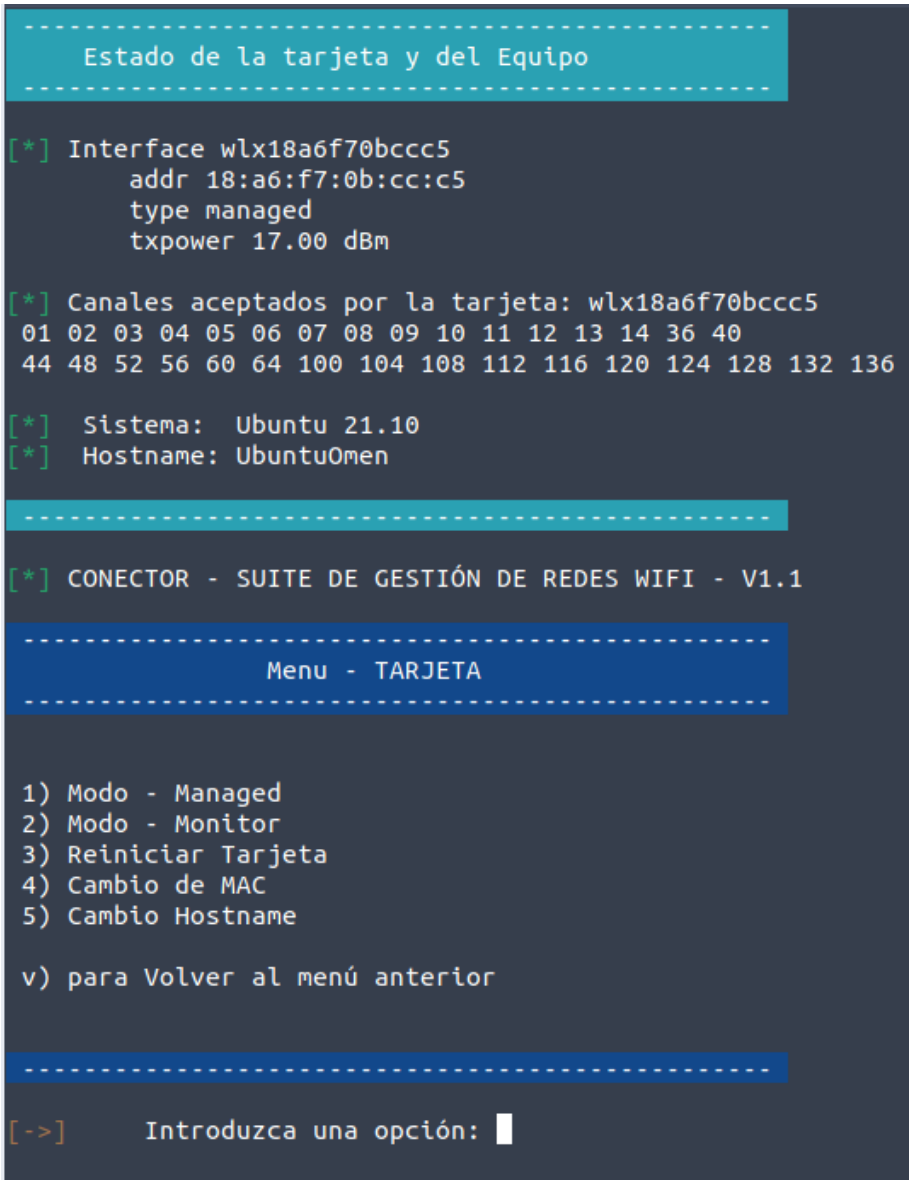

Figura 12 – Menú opciones de tarjetas

1) Modo Managed. En este apartado la tarjeta será modificada para actuar como modo administrativo. Este modo permite un funcionamiento «normal», pudiendo conectarse a redes inalámbricas como un cliente más. En este modo se encuentran la mayoría de tarjetas de red incluidas en los distintos dispositivos, desde los dispositivos móviles a los ordenadores portátiles.

2) Modo Monitor. En este estado, la tarjeta se encuentra en modo «escucha», de esta manera, la tarjeta está preparada para capturar los paquetes de una red wifi. Estos paquetes se desplazan por el aire en determinadas frecuencias, determinadas por la región geográfica en que nos situemos. La captura que se realiza contiene todo el tráfico que en ese momento circule por la frecuencia configurada en la tarjeta. Así, podemos capturar tanto el tráfico de clientes conectados como de clientes sin conexión. Este modo también permite la inyección de paquetes, utilizados generalmente en ataques de red.

No todas las tarjetas aceptan este modo de funcionamiento, siendo necesario verificar que el chip de red incluido en la propia tarjeta lo soporta.

3) Reiniciar tarjeta. Con esta opción se reinicia la tarjeta de red, recuperando su estado inicial por defecto. Esta opción es muy útil ya que en muchas ocasiones y tras realizar diversos cambios de estado en la tarjeta, esta puede no ser estable, por lo que conviene realizar un reinicio del estado.

4) Cambio de «MAC». Marcando esta opción, el usuario tendrá la posibilidad de modificar la dirección «MAC» del dispositivo de red wifi. Una vez elegida esta opción, se ofrecen otro menú dedicado al cambio de dirección.

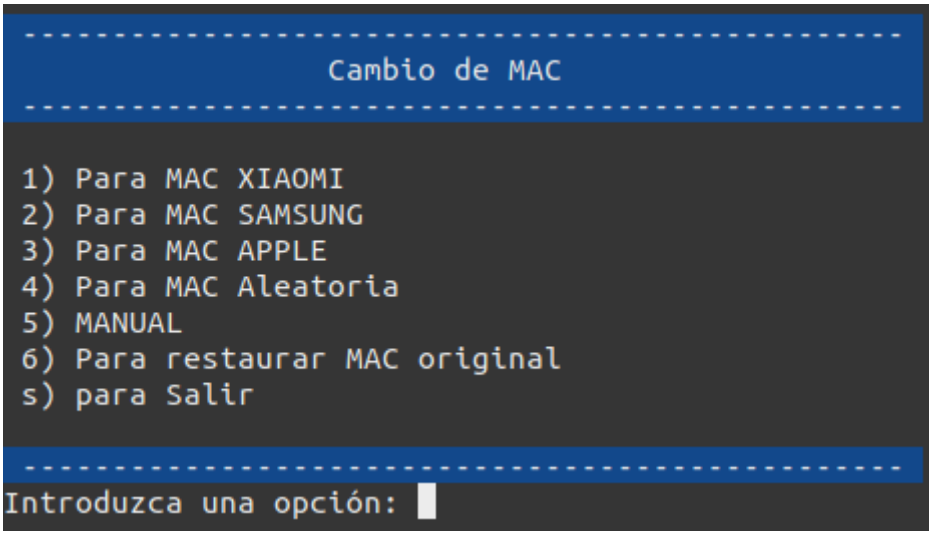

Figura 13 – Menú opciones «MAC»

Se ofrecen distintas opciones de cambio de «MAC». La opción 1 utiliza una «MAC» del fabricante Xiaomi. La segunda utiliza una dirección de Samsung. La tercera usa Apple como fabricante. En la cuarta opción, el sistema genera una dirección «MAC» aleatoria. La opción número cinco permite al usuario introducir manualmente la dirección deseada. Por último, la opción 6 restaura la dirección «MAC» original del equipo.

Se han elegido estos fabricantes debido al gran número de dispositivos distribuidos por todo el mundo. Son los tres mayores fabricantes de dispositivos móviles del mundo, por lo que es fácilmente encontrar direcciones «MAC» de este tipo, al realizar capturas de tráfico para su posterior análisis.

5) Cambio de «hostname». Del mismo modo que en el apartado anterior, se ofrecen al usuario un número de opciones acordes con el cambio de dirección «MAC». Si el usuario ha seleccionado una dirección «MAC» del fabricante Samsung, lo coherente es que el nombre del equipo tenga un nombre relacionado al menos con ese fabricante. De esta manera por ejemplo, un atacante que esté analizando nuestra red pensará que nuestro equipo es un simple dispositivo móvil del fabricante coreano.

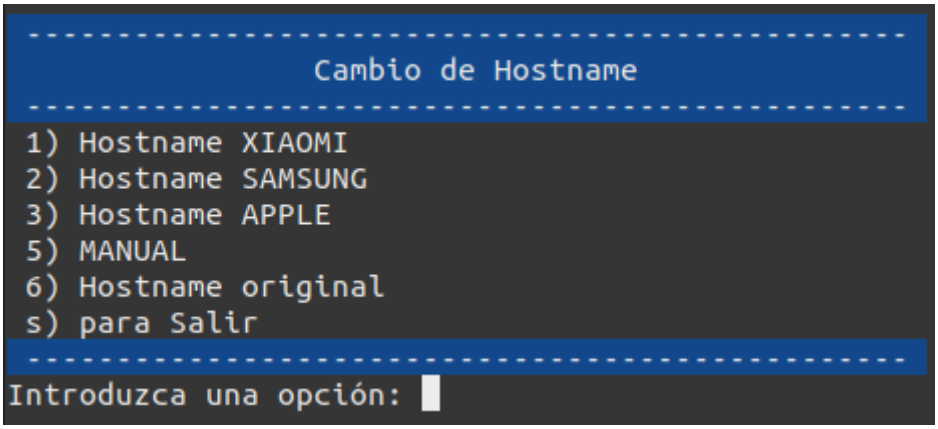

Figura 14 – Menú opciones «hostname»

De nuevo las opciones mostradas pertenecen a los fabricantes Xiaomi, Samsung y Apple; también se ofrece la posibilidad de introducir manualmente el nombre, y como última opción, recuperar el nombre original del equipo.

3.3.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Establecer la tarjeta en modo administrativo.
- Establecer la tarjeta en modo monitor.
- Reiniciar la tarjeta.
- Cambiar la dirección «MAC» de la tarjeta wifi.
- Cambiar el nombre del equipo.

3.4 Módulo Conexión

3.4.1 Características principales

El modulo de conexiones se centra en todas aquellas acciones que tengan que ver con la interacción de redes wifi de forma directa, es decir, permite conectar y desconectar la tarjeta a una red, también eliminar conexiones anteriormente almacenadas, conocer el estado actual de las posibles conexiones, añadir nuevas rutas de direccionamiento, enlazar con las opciones de tarjeta proporcionadas en el módulo anterior y por último realizar un escaneo o análisis del aire, para localizar las posibles redes wifi y sus características.

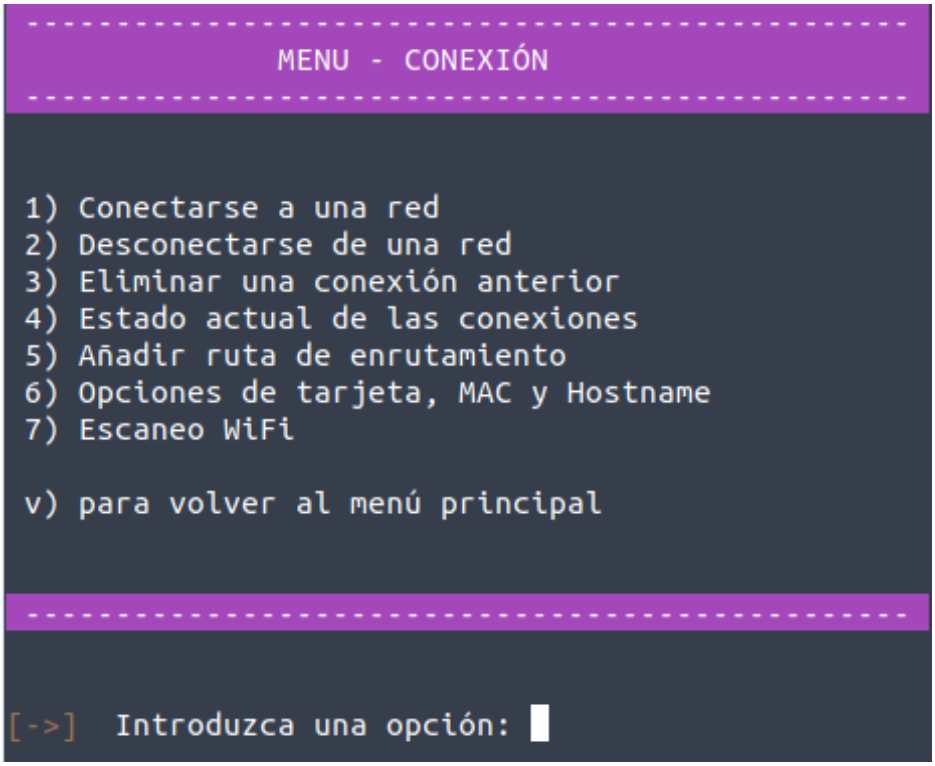

Figura 15 – Menú opciones Conexión

1) Conectarse a una red. En esta primer parte, el programa nos facilita la conexión a una red inalámbrica, nos proporciona un entorno amigable y sencillo para conectarnos a una red concreta, conociendo por supuesto el nombre y la clave. Además, nos ofrece la posibilidad de cambiar la dirección «MAC» de la tarjeta y el nombre del equipo durante el proceso. El procedimiento para realizar la conexión se realiza a través de los siguientes pasos:

    1. Seleccionamos la opción «1) Conectarse a una red».
    2. A continuación nos ofrece la posibilidad de cambiar la dirección «MAC» de la tarjeta, deberemos seleccionar si elegimos cambiarla pulsando la letra S o por el contrario mantenemos la dirección original pulsando la letra N. En el caso de contestar afirmativamente, el programa automáticamente nos redirige al módulo tarjeta punto 4, «Cambio de «MAC»».
    3. A continuación nos ofrece de nuevo la posibilidad de cambiar el nombre del equipo. De nuevo deberemos seleccionar entre la opción afirmativa pulsando la tecla S o rechazando la acción pulsando la tecla N. En el caso de solicitar el cambio, la ejecución realiza la solicitud al módulo de tarjeta punto 5 «Cambio de hostname».
    4. Independientemente de las opciones elegidas en los dos puntos anteriores, el programa continúa realizando una búsqueda de los puntos de acceso o AP visibles para la tarjeta wifi. Nos mostrará toda la información relativa a los AP como su nombre o «SSID», dirección «MAC» o «BSSID», el canal «Channel», la potencia de la señal o «Signal» y el tipo de seguridad implementada «Security».

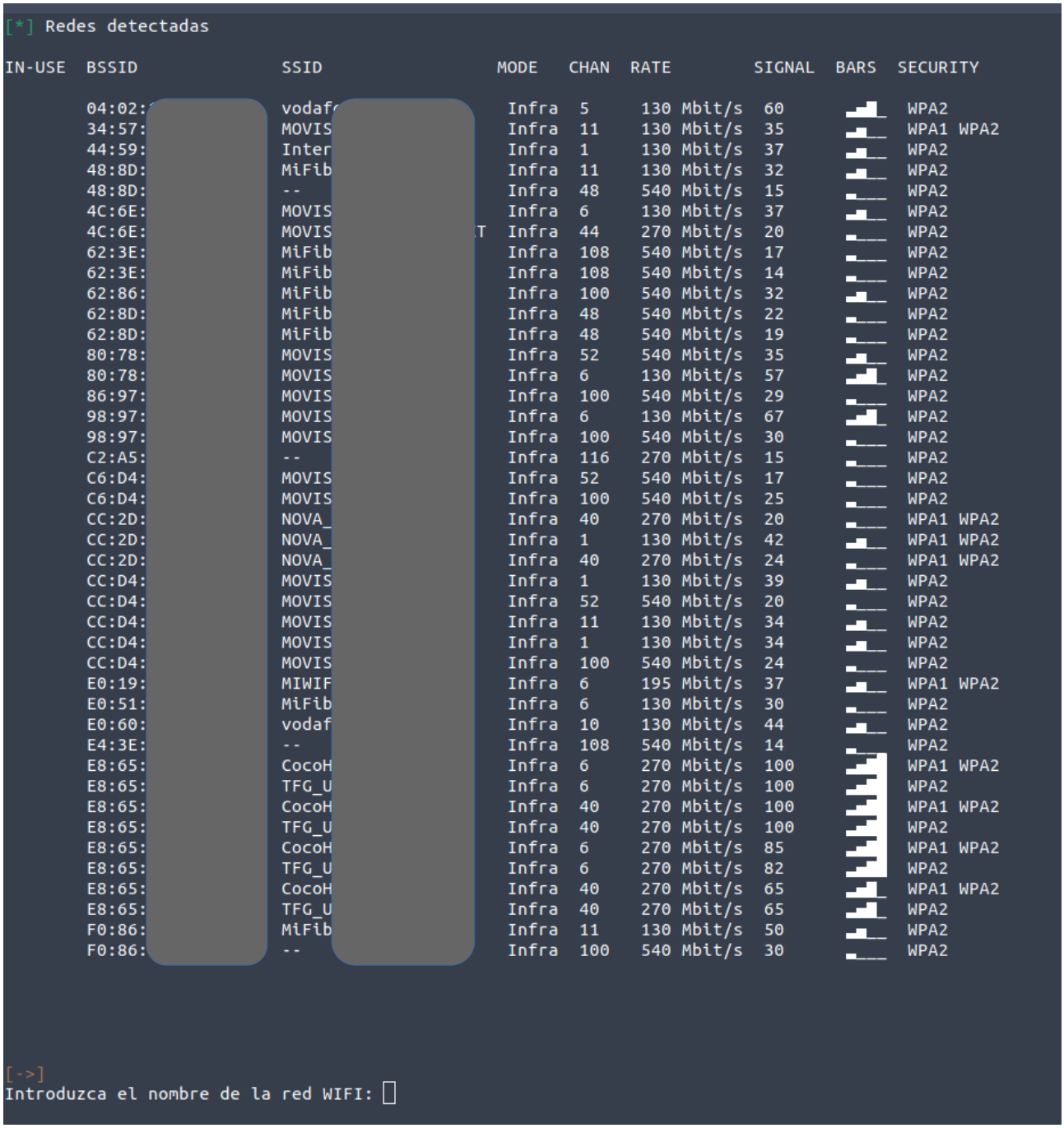

Figura 16 – Puntos de acceso detectados

5. El siguiente paso es seleccionar la red escribiendo el nombre o «ESSID» elegidos. A continuación deberemos proporcionar la clave de la red.

6. En este punto se realizará la conexión con la red seleccionada y la clave insertada. Una vez finalizado el proceso, se nos mostrará un resumen de la finalización con éxito de la conexión y las rutas de direccionamiento hacia el router principal, las conexiones activas y las direcciones IP asignadas; finalmente se muestra la opción de añadir nuevas rutas de direccionamiento pulsando la tecla S para aceptar o N para

rechazar. Este último punto facilita poder añadir a la tarjeta a nuevas redes de enrutamiento sin perder conectividad.

7. Al seleccionar positivamente la elección de añadir una nueva de enrutamiento o direccionamiento, se mostrará una opción donde se deberá introducir el rango y máscara de red del nuevo direccionamiento. Si por ejemplo la nueva red pertenece al rango 10.10.0.1, deberemos introducir 10.10.0.0/16. Seguidamente, el proceso requiere introducir la dirección del nuevo router, en el caso del ejemplo podría ser 10.10.0.1. Finalmente se nos mostrará la nueva tabla de direccionamientos si todo ha funcionado correctamente. En el caso de no conseguir enlazar con la nueva red, se mostrará el mensaje «*Network is unreachable*».
8. Finalmente, se volverá a mostrar el menú principal de red y la ventana de estado, donde se indicará la nueva conexión wifi, con los datos de la conexión.

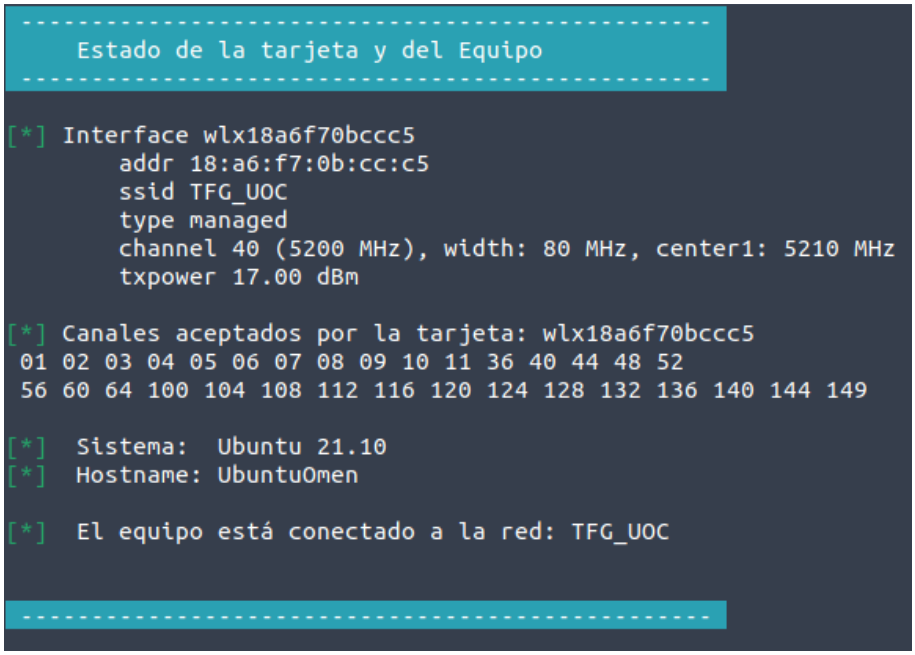

Figura 17 – Ventana de estado

Destacar que el programa detecta el estado de la tarjeta y las conexiones, si por ejemplo se inicia el proceso de conexión a una nueva red, y la tarjeta ya se encuentra asociada a otra red, el «script» detectará esta situación mostrando un mensaje de error e impidiendo la nueva conexión hasta que no se produzca una desconexión. También detecta si la tarjeta se encuentra en modo monitor, lo que impide las conexiones a redes.

2) Desconectarse de una red. Esta opción simplemente facilita la acción de desconexión de una red wifi. Para ello el programa muestra la conexión de red existente, y al mismo tiempo, solicita introducir la red de la que nos queremos desconectar.

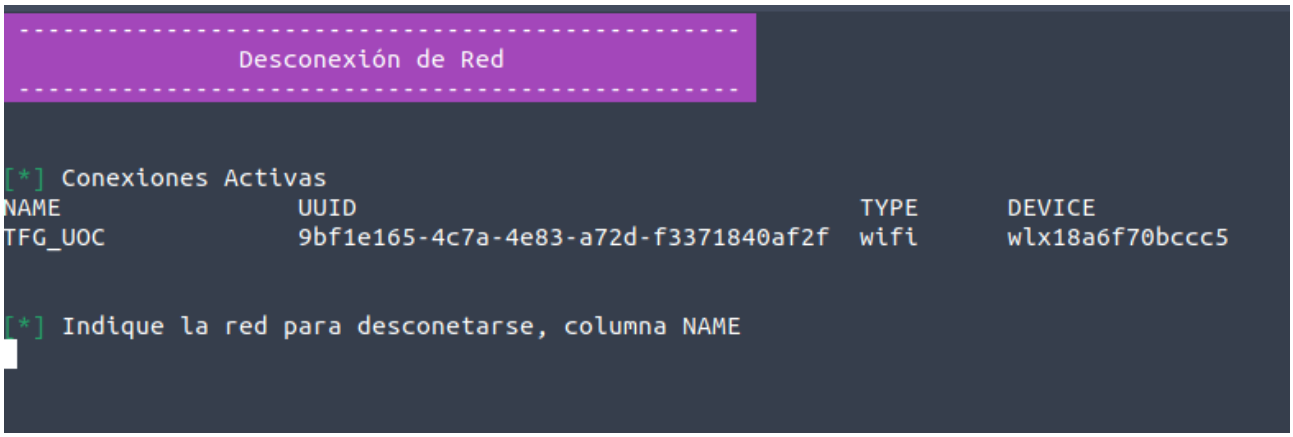

Figura 18 – Desconexión de una red wifi

Una vez realizada la desconexión, se mostrará un mensaje indicando el resultado positivo de esta acción e indicando si deseamos eliminar de forma permanente esta conexión del sistema. En este punto, cabe destacar la forma de trabajo de las distribuciones GNU/Linux en general respecto a la conexiones de red. Una vez se he establecido conexión con una red, sea inalámbrica o cableada, el sistema operativo almacena la conexión con un nombre y un identificador UUID. De esta manera, el sistema «recuerda» estas redes para futuras conexiones, sin necesidad de volver a realizar la configuración. Seleccionando la opción «Eliminar permanentemente», se eliminará del sistema la conexión de forma completa, debiendo realizar de nuevo la configuración en el caso de realizar una nueva conexión con la red.

De nuevo indicar que el programa detecta el estado de la tarjeta y las conexiones, en el caso de iniciar el proceso de desconexión, si se detecta que la tarjeta no se encuentra asociada a ninguna red, el «script» acabará mostrando un mensaje de error.

3) Eliminar conexiones anteriores. En este punto y como se ha explicado en el apartado anterior, se eliminan las conexiones guardadas en el sistema anteriormente, borrándolas del sistema operativo. El programa ofrece la opción de elegir cual de las conexiones almacenadas se eliminará.

4) Estado actual de las conexiones. Este apartado muestra el estado actual de la conexión. El «script» muestra todas las conexiones del equipos, inalámbricas y cableadas e indica, todas las direcciones IP asignadas al equipo.

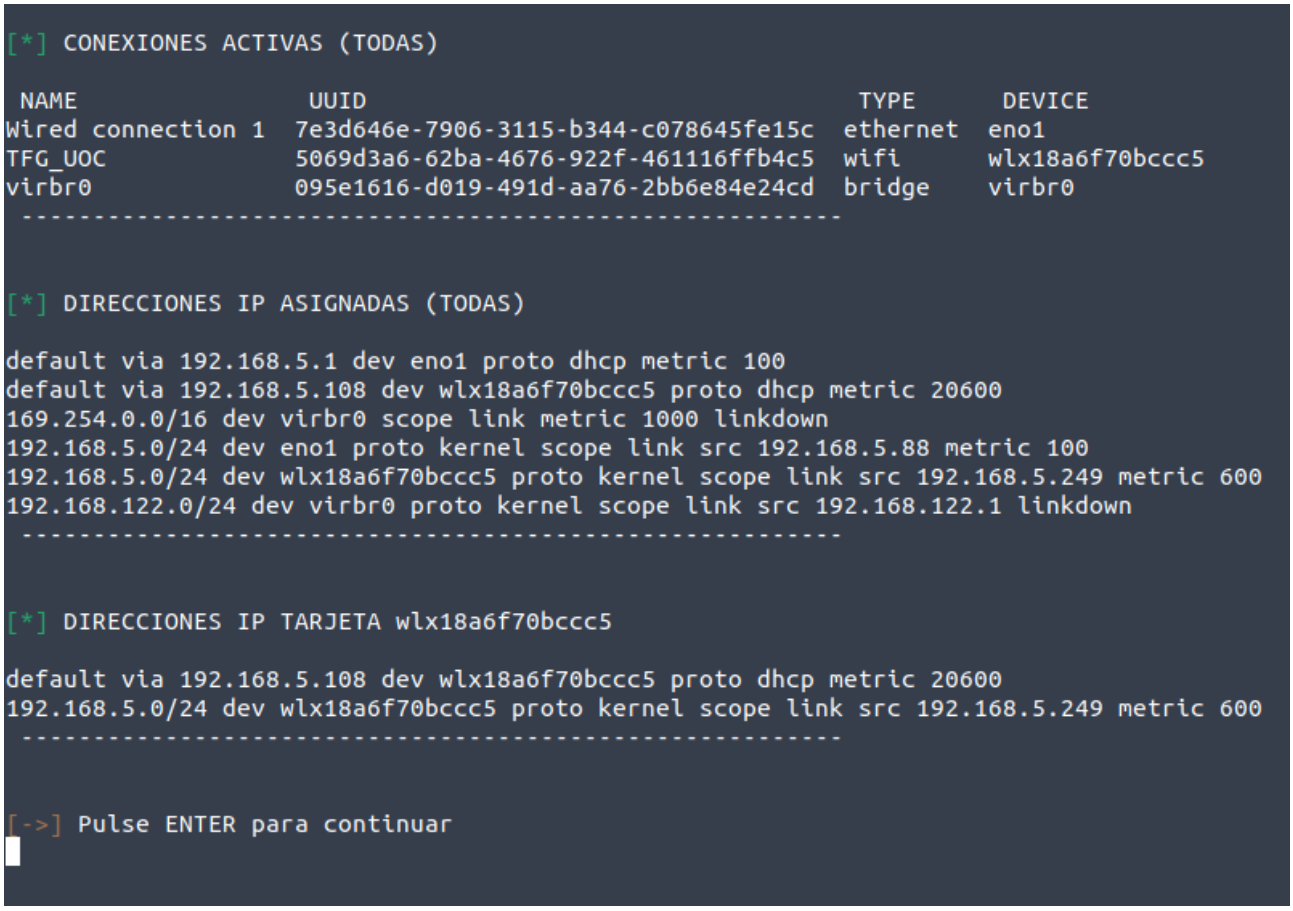

Figura 19 – Estado de las conexiones

5) Añadir nueva ruta de enrutamiento. En este punto se facilita el poder añadir la tarjeta a nuevas redes sin perder conectividad, de esta manera, podremos acceder a varias redes distintas a la simultáneamente sin perder conexión con ninguna de ellas. Por poner un ejemplo: si antes de realizar el proceso de conexión a una red wifi estamos conectados por cable a una red con un rango 192.168.0.0/24 y posteriormente realizamos la conexión con la red inalámbrica con un rango 10.10.10.0/24, la tarjeta necesita «aprender» todos los caminos posibles a todos los equipos en ambas redes y rangos. Para ello se agregan nuevos direccionamientos de red o rutas, de esta manera, no se perderá conexión con ningún equipo de ambas redes.

6) Opciones de tarjeta (Módulo Tarjeta). Mediante esta opción se realiza una llamada al módulo 3 referente a la tarjetas y las opciones sobre esta.

7) Realiza un escaneo wifi. Este último punto realiza un análisis del entorno, comprobando todas las frecuencias visibles por la tarjeta wifi en su rango de acción, localizando todos aquellos equipos que de alguna manera sean visibles. Finalmente, devuelve un listado con la información de los puntos de acceso.

3.4.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Establecer a través de la tarjeta seleccionada, una conexión con una red wifi elegida.
- Realizar una desconexión de la red wifi actual.
- Eliminar del sistema todas las conexiones antiguas almacenadas.
- Comprobar el estado actual de las conexiones.
- Añadir posibles nuevas rutas de direccionamiento.
- Enlazar con el módulo de tarjeta para cambiar el estado de esta.
- Realizar un análisis del entorno para localizar las redes inalámbricas.

3.5 Módulo Análisis

3.5.1 Características principales

Dentro de este módulo se busca poder analizar los posibles dispositivos conectados a una red, concretamente se busca localizar todos los equipos o dispositivos conectados así como la mayor información posible de cada uno de ellos. Evidentemente este análisis únicamente podrá realizarse siempre que nuestro equipo esté conectado a una red inalámbrica, en caso contrario, el propio programa mostrará un mensaje indicando que no es posible realizar este tipo de acciones si no se ha establecido una conexión previamente.

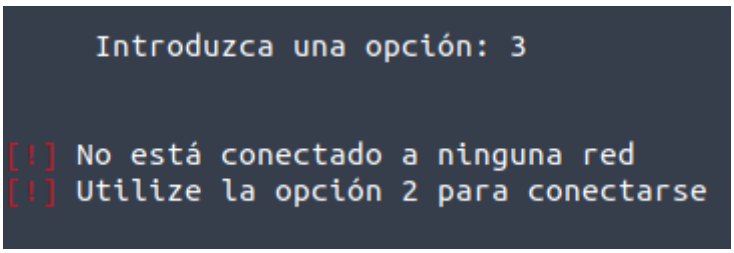

Figura 20 – Advertencia de no conexión

Una vez establecida una conexión con un AP, se podrá realizar el análisis de los dispositivos ubicados en esta misma red. Para ello, se mostrará un menú con las opciones disponibles:

Figura 21 – Menú Análisis

El programa solicitará un nombre para el análisis y un rango de direcciones. El nombre puede ser cualquier cadena que identifique de alguna manera el estudio a realizar. El rango de direcciones podrá contener una única dirección IP como por ejemplo 192.168.0.1, o todo un segmento de red como puede ser 192.168.0.1/24. El análisis se realizará únicamente sobre la dirección indicada; en el caso de ser todo un segmento, el análisis se realizará sobre todos los equipos del rango de direcciones. Cabe destacar que ciertas opciones recomendarán al usuario la cantidad de direcciones indicadas, puesto que debido a la complejidad y a los tiempos del análisis, puede conveniente limitar ciertos estudios.

En la parte inferior del programa, se muestran todas las direcciones IP activas en el equipo, esto permitirá al usuario conocer los distintos segmentos de red dentro de los que el equipo es capaz de trabajar, facilitando al usuario la elección de las distintas direcciones a estudiar.

Una vez indicados el nombre y el rango de direcciones, se mostrarán en el menú de análisis añadiendo facilidad de uso:

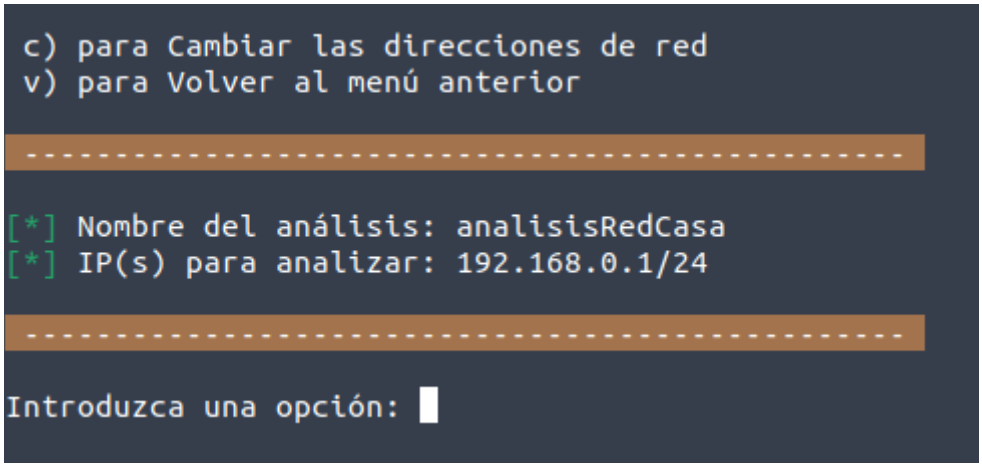

Figura 22 – Nombre y direcciones IP seleccionadas

Es importante indicar que todos los análisis se realizarán utilizando las direcciones IP y los puertos abiertos de cada equipo conectado a la red. Todas las herramientas utilizadas para realizar los distintos análisis, son de código libre, y se enumeran a continuación:

1. Arp-scan. La primera de estas herramientas es «arp-scan», una herramienta enfocada en el descubrimiento de equipos de red mediante el protocolo «ARP». Es una aplicación sencilla que muestra información básica de los equipos conectados como son la dirección IP y la dirección MAC.
2. NetDiscover. Al igual «arp-scan», «NetDiscover» utiliza el protocolo «ARP» para realizar el descubrimiento de red y de los equipos presentes. Permite un mayor abanico de opciones, como por ejemplo la opción «-p», la cual realiza un el estudio de manera «invisible» aunque implica mayores tiempos de espera. Esta opción, facilita poder realizar un estudio sin que el el resto de la red detecte nuestra presencia.
3. Nmap. Finalmente aparece la aplicación con mayor potencia dentro de este ámbito, «Nmap». «Nmap» es una herramienta de exploración y seguridad, además de permitir acciones como la detección de puertos abiertos, identificación de sistemas operativos y análisis de posibles vulnerabilidades. Es la herramienta más potente de las tres, pero al mismo tiempo es la que supone una mayor complejidad en su uso.

Como vemos en el menú de usuario de la *Figura 22*, la primera parte muestra las opciones disponibles enumeradas del 1 al 8. Las cinco primeras opciones nos permiten utilizar la herramienta «Nmap», con distintas opciones y argumentos, obteniendo distintos resultados en cada una de ellas. Las opciones 6 y 7 utilizan el protocolo «ARP» para el descubrimiento de dispositivos, aquí se obtendrá menos información que en los apartados anteriores, mostrando únicamente si está conectado o no. La dos últimas opciones permiten cambiar el nombre y el rango de direcciones seleccionados, y volver al menú principal.

Todos los resultados de las distintas alterntivas, se almacenan en un fichero dentro de la ruta «./Info/NombreDelEstudio/fechaactual/tipodeanalisis.txt».

A continuación se detallan los distintos análisis y sus opciones:

1. Nmap -O. Esta opción ejecuta la herramienta con los argumentos «-T3 -O -v -p22,25,53,80,137-139,143,336,443,445,554,1900,5000,5431,7000,7100,8009,8080,9000,30000,49152,62078»

La opción «-T3» indica el tipo de comportamiento, concretamente el 3 indica un comportamiento normal, esto quiere decir que se realizará el estudio de manera paralela, se analizan varios equipos al mismo tiempo y sin realizar pausas entre dispositivos. La opción «-O» muestra el posible sistema operativo del dispositivo, la opción «-v» fuerza al programa a mostrar información más detallada de todo el proceso. Por último, la opción «-p» indica los puertos que serán analizados, reduciendo los tiempos considerablemente; de no indicarse esta opción, la herramienta analizaría los 1000 puertos más significativos. Los puertos indicados incluyen puertos comunes, como los usados en navegación web, conexiones ssh o telnet y puertos exclusivos de sistemas operativos y protocolo «DNS» entre otros.

2. Nmap -T2. Esta opción utiliza los argumentos «-T2 -Pn -v -p22,25,53,80,137-139,143,336,443,445,554,1900,5000,5431,7000,7100,8009,8080,9000,30000,49152,62078»

«-T2» indica que se realiza un intento de detección cada 0,4 segundos y de manera individual, es decir, un único intento por equipo sin paralelismos. Esto facilita poder encubrir las acciones ante posibles atacantes o equipos con protecciones de análisis de red. «-Pn» trata a todos los hosts como si estuvieran activos, analizando sus puertos en todos los casos.

3. Nmap -T1. En este caso los argumentos utilizados son «-T1 -sn -vvv»

De nuevo la opción «-T1» indica que se realiza un único intento sin paralelismos y que estos intentos se realizan en intervalos de 15 segundos. La opción «-sn» evita realizar ningún análisis de puertos, evitando el protocolo «PING» y con ello una identificación de nuestro dispositivo en la red.

4. Nmap 65535. Los argumentos utilizados en esta cuarta opción son únicamente la opción de recorrer todos los puertos disponibles, que abarcan desde el puerto1 hasta el 65535. Es una opción donde los tiempos de ejecución son extensos, por lo que es recomendable utilizar una única dirección IP en vez de todo un segmento de red.

5. Nmap -A. En este caso las opciones elegidas son «-A -T4». La primera opción indica que se obtenga la máxima información posible sin importar nuestro anonimato, incluyendo posibles vulnerabilidades del dispositivo, lo que ralentiza mucho el escaneo. «-T4» fuerza la velocidad de los intentos implicando una agresividad mayor. De nuevo es recomendable utilizar una única dirección IP en vez de todo un segmento de red.

6. Arp-scan. Se ejecuta directamente sobre el intervalo de direcciones IP asignadas, y se utiliza el argumento «-r 4 -W». La opción «-r» indica cuantos intentos se realizan por dispositivo, en nuestro caso 4; la segunda opción permite almacenar en formato pcap la captura de tráfico de la información recibida durante el análisis de la red.

7. NetDiscover. Se realiza un escaneo de la red mediante el protocolo «ARP» enviando y recibiendo este tipo de tramas. Además, se ofrece la opción al usuario de utilizar este método de manera pasiva, así, la aplicación buscará equipos en la red sin emitir ningún tipo de tráfico, simplemente permanecerá a la escucha, asegurando nuestro anonimato en la red.

8. Tablas direccionamiento y saltos de conexión. Este apartado permite conocer las tablas de enrutamiento y los saltos necesarios entre los distintos rangos de dirección para contactar con una IP final.

Al finalizar cada uno de los análisis, se muestra un pequeño resumen con la información más relevante. Se muestra el nombre del fichero creado y su ruta, además de mostrar el resto de ficheros que puedan existir dentro de esa misma ruta, ruta que corresponde con el nombre elegido al incio como identificador de los distintos análisis.

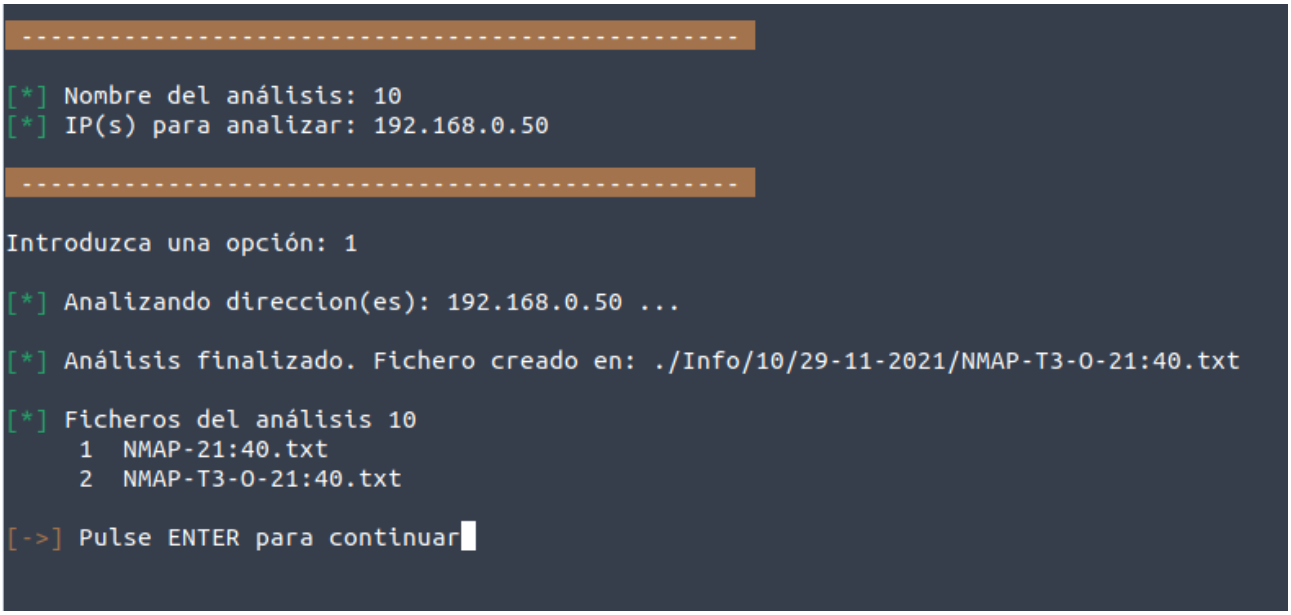

Figura 23 – Resumen del análisis

3.5.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Realizar distintos tipos de análisis, con mayor o menor grado de agresividad y efectividad.
- Identificar el sistema operativo de los dispositivos conectados.
- Identificar servicios presentes en la red.
- Localizar puertos abiertos.
- Descubrir el direccionamiento de red y la tabla de enrutamiento.

3.6 Módulo canales

3.6.1 Características principales

Este módulo permite comprobar las características de la tarjeta de red seleccionada por el usuario. Concretamente se comprueban todos los canales y frecuencias soportados. No es un módulo accesible por el usuario, solamente es utilizado por otros módulos para realizar comprobaciones de los canales accesibles.

3.6.2 Funciones

- Crear una lista con los canales y frecuencias soportados.
- Mostrar una lista de los canales accesible.

3.7 Módulo Captura

3.7.1 Características principales

En este penúltimo módulo del programa encontramos las opciones relacionadas con la captura del tráfico de red. Una captura de tráfico permite guardar en un dispositivo de almacenamiento toda la información transmitida en una red. Como ya hemos visto anteriormente toda comunicación involucra al menos a dos agentes, el emisor y el receptor; normalmente en esta comunicación, se incluyen otros dispositivos relacionados con la gestión de la retransmisión como pueden ser el «router» o el «switch».

Las capturas se pueden llevar a cabo tanto en redes cableadas como en redes inalámbricas. Al realizar una captura del tráfico en una red local LAN, se almacena en un fichero toda la comunicación generada en esa red, al menos la visible para el equipo que está generando la captura, de manera que se pueda analizar posteriormente con las herramientas adecuadas.

Por otro lado, nuestro programa se centra en la captura de las redes inalámbricas, por lo que el script será capaz de almacenar todo el tráfico transmitido en un canal y ancho de banda concretos. Debemos tener en cuenta que todas las conversaciones y transmisiones de tráfico en una red wifi, utilizan el aire como medio de transporte, por lo que la totalidad de la información se encuentra en este medio, lo que permite recopilar mayor información que en una captura de una red LAN. Esto puede suponer una brecha de seguridad enorme, pero como se ha visto en el capítulo «Introducción redes inalámbricas», existe un complejo sistema de cifrado de la información diseñado para evitar que terceros accedan a información personal.

Así, para poder establecer una comunicación wifi cifrada se recurrirá al protocolo anteriormente explicado denominado «EAPOL». Este sistema de cifrado presenta una robustez alta, permitiendo asegurar la inviolabilidad de los datos transmitidos. Sin embargo, con el tiempo se han detectado fallos en el protocolo que permiten en ciertos casos muy concretos, llegar a obtener la contraseña de la red inalámbrica y de esta forma, acceder a la misma.

El método para vulnerar dicha contraseña, consiste en obtener el intercambio de mensajes durante el primer «saludo» de un dispositivo con el AP, capturando los paquetes «EAPOL» transmitidos, concretamente los cuatro de la fase de «4-way handshake». Es importante especificar que son necesarios al menos 3 de estos 4 paquetes para poder descifrar la clave. Una vez capturados estos paquetes y conociendo el nombre de la red, mediante fuerza bruta y en la mayoría de los casos apoyados en un potente diccionario de palabras, puede llegar a obtenerse la contraseña de la red wifi.

En este módulo vamos a poder realizar capturas de tráfico en dos escenarios concretos, el primer caso realiza una captura dentro de una red, por lo que deberemos estar previamente conectados a esta red; el script detecta automáticamente si la tarjeta de red está asociada a una red inalámbrica y comienza la captura sin ofrecer más opciones, ya que se activa de manera autónoma. Por otro lado y si no existe conexión previa, el usuario podrá seleccionar entre cuatro opciones distintas:

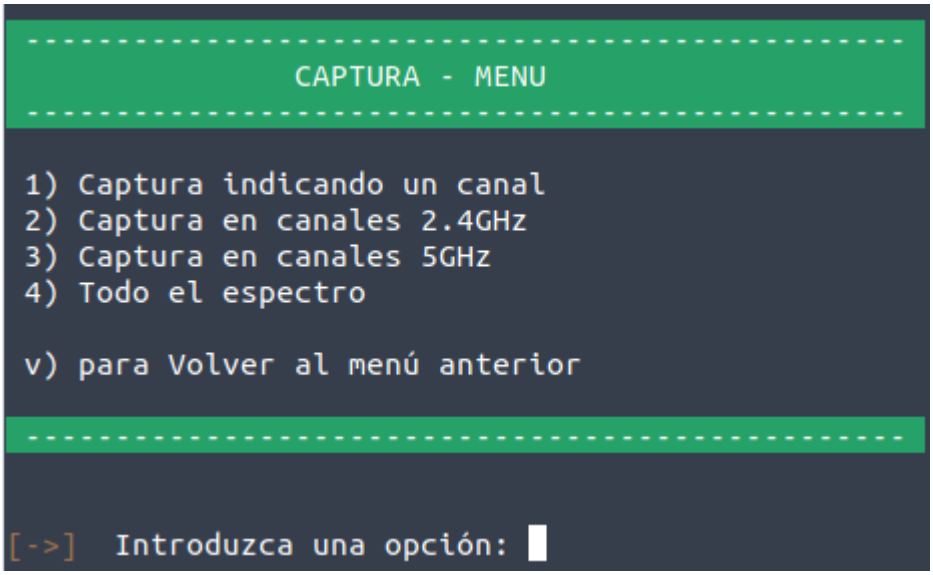

Figura 24 – Menú Captura

1. Selección de canal. En este caso el usuario podrá indicar el canal en el que se realizará la captura. Este canal puede estar en la banda de 2.4GHz o en la banda de 5GHZ y se ofrecerá por pantalla la lista de canales admitidos.
2. Canales 2.4GHz. Se realizará una captura de todos los canales de la banda de 2.4GHz admitidos por la tarjeta de red wifi.
3. Canales 5GHz. Se realizará una captura de todos los canales de la banda de 5GHz admitidos por la tarjeta de red wifi.
4. Todo el espectro. En este último apartado, se realiza una captura de todo el espectro soportado por la tarjeta en ambas frecuencias.

En cualquiera de los cuatro casos, todas las capturas realizadas se almacenan en la ruta «./Capturas/*fecha/*», siendo el campo «fecha» la fecha de realización de la captura. Además, en todas las opciones se abrirá una ventana emergente mostrando información de la captura como el canal y los posibles «EAPOL» capturados, las redes y clientes detectados, el número de paquetes y la potencia de señal entre otros.

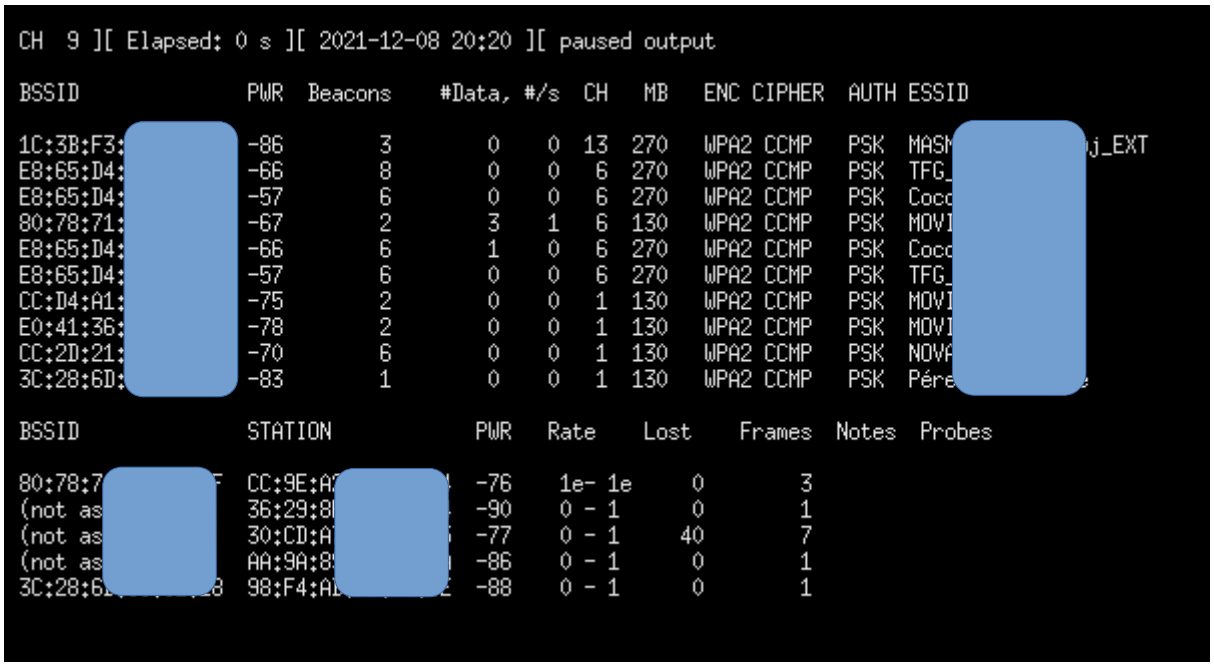

Figura 25 – Información de la Captura

Por último, una vez finalizada la captura, se ofrece la posibilidad al usuario de comprobar los si se han capturado paquetes de tipo «4-way handshake».

3.7.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Realizar capturas en un canal seleccionado.
- Realizar capturas en la banda 2.4GHz.
- Realizar capturas en la banda 5GHz.
- Realizar capturas en ambas bandas, en todo el espectro wifi compatible con la tarjeta de red.
- Realizar búsquedas de paquetes «EAPOL» en las capturas realizadas.

3.8 Módulo Ataques

3.8.1 Características principales

Este último módulo está dedicado a analizar los posibles ataques que se realicen sobre la red. Como ya hemos visto en capítulos anteriores, dentro la seguridad de las redes inalámbricas existen diversos protocolos de seguridad, entre los que se encuentran WEP, WPA y WPA2. En la actualidad, el único recomendado es el WPA2, ya que el resto se consideran inseguros, por lo que este módulo se centrará únicamente en los posibles ataques sobre el protocolo WPA2. Es necesario recordar que WPA3 no está implantado de forma generalizada, pero sería la selección más adecuada y segura.

En el caso concreto de WPA2, también en apartados anteriores hemos analizado como este protocolo utiliza el intercambio de cuatro paquetes dedicados a la autenticación del dispositivo conocidos como «4-way handshake». Son estos mismos paquetes los que pueden convertir a este protocolo en vulnerable.

El ataque de desautenticación o «deauthtentication» en inglés, consiste en enviar o inyectar una serie de paquetes con una información concreta a uno o varios clientes, para que de esta manera se vean forzados a cortar la comunicación con el punto de acceso wifi y salir expulsados de la red. Este tipo de ataques tienen como objetivo capturar los paquetes «handshake» de los protocolos WPA/WPA2 obligando a los clientes a desconectarse y realizar una nueva conexión con el punto de acceso, capturando las tramas «4-way handshake». Esto es posible porque dentro del protocolo 802.11 existen las tramas de tipo desautenticación no encriptadas, por lo que cualquier dispositivo conectado o no a la red, puede realizar una inyección de este tipo de paquetes a cualquier otro cliente. A continuación se describen los pasos a seguir para realizar este tipo de ataques:

1. Localizar la red objetivo, necesariamente una red inalámbrica, ya que este tipo de ataques es exclusivo de este tipo de redes. Es necesario almacenar el campo «bssid» de la red, correspondiente a la dirección MAC del punto de acceso.
2. Identificar un cliente conectado a esta red y almacenar su dirección MAC si únicamente se quiere realizar el ataque enfocado en un único dispositivo. Por otro lado, se puede realizar el ataque sobre toda la red sin necesidad de almacenar ninguna dirección MAC de cliente, lo que se conoce de forma coloquial como «tirar abajo toda la red».
3. Disponer de una tarjeta inalámbrica con la capacidad de realizar cambios en su modo de funcionamiento, para poder trabajar en modo monitor y así ser capaces de inyectar tráfico.
4. Iniciar el ataque transmitiendo los paquetes de tipo desautenticación sobre el punto de acceso y el cliente elegido.

Existen distintas formas de realizar el envío de paquetes, aunque en este caso se elige utilizar la herramienta «aireplay-ng» ubicada dentro del conjunto de herramientas ofrecidas por la solución «aircrack-ng». Esta herramienta permite realizar el envío de paquetes ejecutando el siguiente comando:

```
sudo aireplay-ng -0 1 -a AP_MAC -c Cliente_MAC Tarjeta_inalámbrica
```

Las opciones del comando proporcionan información de su ejecución:

- opción -0: este valor especifica que el tipo de ataque es de tipo «deauth». El 1 indica el número de paquetes enviados, en este caso 1.
- opción -a: este argumento indica la dirección MAC del punto de acceso, el campo «bssid».
- opción -c: en este caso se debe indicar la dirección MAC del cliente conectado a la red. En caso de no indicar nada en esta opción, el ataque se realizaría sobre todos los clientes conectados a esa red.

- Por último, se debe especificar la tarjeta de red inalámbrica; es necesario que la tarjeta se encuentre en modo monitor para realizar el envío de paquetes. El script detecta si la tarjeta se encuentra en este modo, en caso contrario es capaz de cambiar el estado de manera autónoma.

El módulo ofrece entre tres opciones a elegir, la primera proporciona las herramientas necesarias para detectar este tipo de ataques, realizando un análisis del entorno wifi en busca del tipo de paquetes específicos denominados «deauthentication». La segunda opción, ofrece la posibilidad al usuario de realizar este tipo de ataques con el único propósito de efectuar comprobaciones sobre las redes propias. La última de las posibilidades, permite al usuario realizar un pequeño análisis de redes inalámbricas para determinar posibles cliente de una red y guardar toda la información necesaria, como pueden ser el canal de la red o las direcciones MAC, para realizar posteriormente un ataque.

Figura 26 – Menú Ataques

- Opción 1. Esta opción no posee complejidad ninguna de cara al usuario, donde solo debe indicar esta opción para que el sistema comience de manera automática a capturar el tráfico inalámbrico y analizarlo en busca de posibles ataques de deautenticación. Como información complementaria, se abre una ventana emergente mostrando el estado actual del entorno. En el caso de interceptar este tipo de tramas, el programa realizará una captura del tráfico solamente con estos paquetes específicos, para un análisis posterior, y se mostrará un mensaje al usuario indicando la detección del ataque.

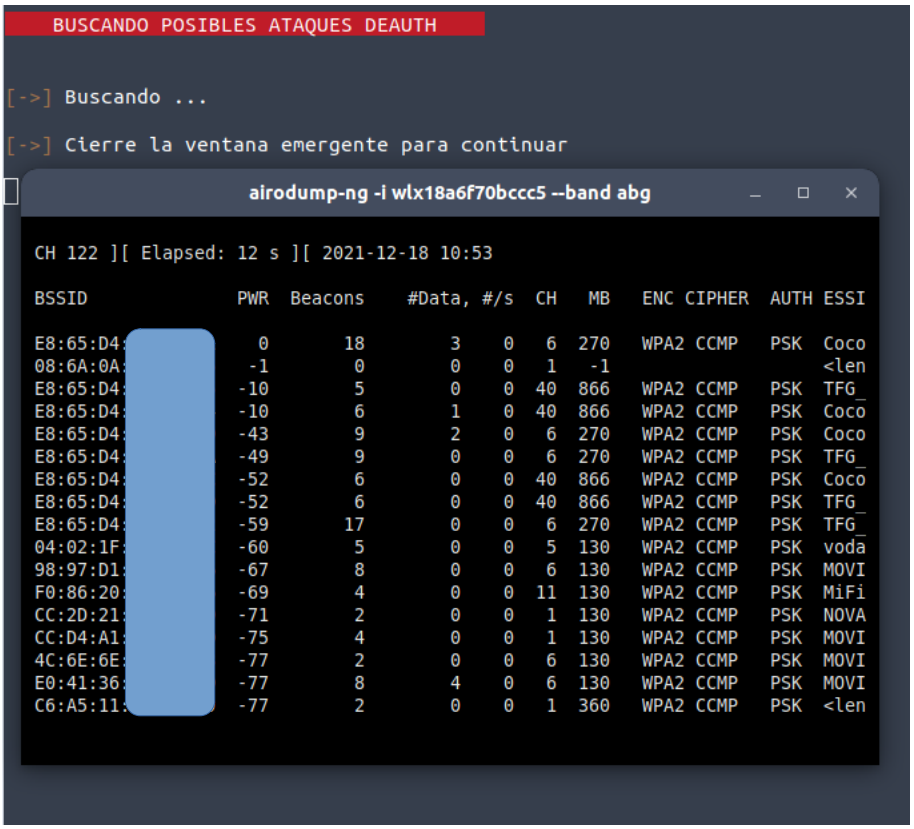

Figura 27 – Detección ataque deautenticación

- Opción 2. En este caso el usuario podrá realizar un ataque de deautenticación sobre una rede y verificar la efectividad del mismo. Es importante indicar que este tipo de ataques debe realizarse expresamente en entornos propios y controlados, y con la única intención de realizar pruebas de seguridad, en ninguno caso deben aplicarse estas técnicas sobre entornos ajenos.

  De nuevo, se abre una ventana emergente mostrando información de lo que está ocurriendo a nivel inalámbrico, mientras, el script ofrece una serie de pasos al usuario que este debe ir completando con la información adecuada. En primer lugar se solicita el canal de trabajo de la red wifi, en segundo lugar se necesita conocer la dirección MAC del AP y por último se debe indicar el cliente objeto del ataque. Recordemos que en el caso de no indicar ningún cliente, el ataque se realizará sobre la totalidad de la red y los dispositivos conectados a la misma.

- Opción 3. En este aparatado el usuario puede realizar un pequeño análisis del entorno, localizando redes inalámbricas, clientes conectados y canales y frecuencias. Así, se facilita la obtención de la información para realizar un ataque a posterior. Será necesario obtener los datos del canal de la red, la dirección MAC del AP y la dirección MAC del cliente. Tras el análisis se mostrarán al usuario los posibles clientes conectados de la red elegida.

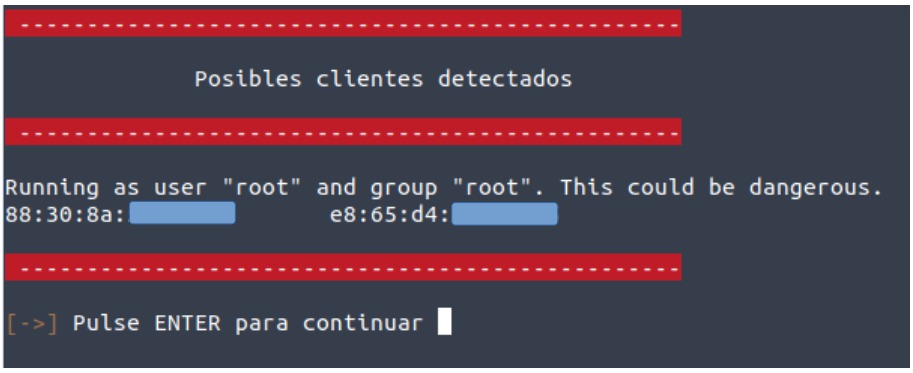

Figura 28 – Clientes Detectados

3.8.2 Funciones

Las principales funciones de este módulo son las siguientes:

- Realizar análisis del tráfico para detectar posibles ataques de tipo «Deauth».
- Realiza pruebas de ataque tipo «Deauth» para comprobar la estabilidad de la infraestructura de red.
- Analizar una red inalámbrica para localizar los dispositivos conectados.

4 Pruebas de funcionamiento

4.1.1 Elementos Hardware

Una vez se establecen los equipos físicos que se utilizarán en el desarrollo, se procede a su instalación y comprobación de funcionamiento. Se realizan distintas pruebas para identificar posibles problemas de compatibilidad o funcionamiento.

Pruebas realizadas:

- Se instalan todos los controladores, tanto de los elementos integrados en el equipo personal de trabajo, como de la tarjeta externa de red utilizada.
- Se realizan pruebas con ambas tarjetas de red inalámbricas, tanto externa como interna. Se realizan acciones de conexión a diferentes redes, validando el comportamiento y su estabilidad. Las pruebas se realizan a través del entorno gráfico y mediante el intérprete de comandos.
- Del mismo modo, se desconectan de las distintas redes y se eliminan conexiones guardadas. De nuevo estos procesos se hacen en los entornos gráfico y línea de comandos.
- Se realizan cambios de modo de funcionamiento en ambas tarjetas, se cambian de modo «managed» o administrativo a modo monitor y viceversa. Se comprueba la estabilidad en ambos modos y el correcto funcionamiento.

- Una vez establecido el modo monitor en cada una de las tarjetas, se realizan cambios entre los distintos canales, además de modificar el ancho de banda de los canales establecidos, conocida como «HT», entre HT20, con un ancho de 20MHz por canal y HT40, con 40MHz por canal.
- En este mismo modo, se realizan captura de tráfico.
- Por último, se ejecutan distintas inyecciones de tráfico con resultados satisfactorios.

4.1.2 Elementos Software

Las pruebas se inician con la instalación del sistema operativo. Una vez finalizada esta fase, se comprueban que todos los dispositivos son detectados dentro del sistema operativo de forma correcta. Posteriormente se instalan cada una de las herramientas necesarias para ejecutar de manera correcta el script al completo con todas sus funciones.

Se ejecutan, de manera independiente, cada una de las aplicaciones instaladas con los argumentos necesarios, comprobando que todo funciona perfectamente. De esta manera, se asegura la compatibilidad tanto con el sistema operativo como con los dispositivos instalados.

Se prueba cada una de las opciones y módulos del proyecto, primer en orden creciente en las opciones y posteriormente de forma aleatoria, comprobando que en ambos casos el sistema es estable y responde adecuadamente. En este mismo punto, se fuerza al sistema introduciendo opciones incorrectas o información en un formato incorrecto.

4.1.3 Prueba en conjunto

Finalmente, se ejecutan pruebas de funcionamiento utilizando los elementos hardware presentes junto con los elementos software instalados. De nuevo se vuelven a probar cada uno de los módulos y sus respectivas opciones, de manera ordenada y de forma aleatoria.

Cada uno de los distintos módulos desarrollados son verificados en cuanto a la estabilidad y compatibilidad con todos los elementos integrados en el sistema. Además, se desarrollan pequeños scripts o programas totalmente independientes de la solución final con el fin de aumentar la cantidad de pruebas de funcionamiento y confirmar así la correcta ejecución de todos los elementos. Esto facilita el desarrollo del código de programación y la correcta sintaxis del mismo, así como realizar pruebas de distintas soluciones frente a un mismo problema.

5 Conclusiones

Es evidente que día a día surgen nuevas tecnologías y soluciones, que de manera irremediable, se van incorporando a nuestra vida cotidiana. Desde pequeños dispositivos como teléfonos móviles y relojes inteligentes, hasta equipos de trabajo como sobremesas y ordenadores portátiles. Cada dispositivo pertenece a un ecosistema distinto, donde poder albergar las distintas aplicaciones y software dedicado específicamente para este grupo. Así, los desarrolladores de aplicaciones deberán elegir un ecosistema, y de esta manera, enfocar sus esfuerzos hacia este tipo de dispositivos.

Uno de los ecosistemas más importantes y que más está creciendo en los últimos años, es el del código libre; software desarrollado por empresas o desarrolladores privados y de uso totalmente gratuito para cualquier persona. Este movimiento no incluye únicamente programas enfocados a una tarea específica como escuchar música o editar textos, también existe software más complejo dedicado a gestionar los equipos informáticos, y es ahí donde nace el grupo «GNU/Linux». Un conjunto de programas desarrollados de forma distribuida por distintas personas o entidades, unificados en un único paquete para crear un sistema operativo. Por supuesto, es un sistema operativo de código libre condición *sine qua non* no entraría en esta categoría. Como hemos visto a lo largo del proyecto, tanto «GNU» como el «kernel Linux» pertenecen a la categoría de sistemas de código libre, desarrollados por la comunidad para la comunidad.

Sin embargo, este tipo de sistemas siempre ha estado rodeado por una idea de complejidad que en muchos casos no ha favorecido su expansión entre los usuarios de equipos informáticos. Se ha extendido la idea de que este tipo de sistemas operativos se centran exclusivamente en personas con un alto nivel de conocimiento, como pueden ser los desarrolladores de aplicaciones o los administradores de sistemas o de redes; incluso se asocia a grupos de piratas informáticos o «hacker», aunque generalmente este término se asocia a ladrones de datos y de sistemas informáticos, cuando en realidad este tipo de personas son las que investigan los posibles fallos y brechas de seguridad para avisar y poner solución, es decir, son los buenos y no los malos como se piensa.

Así, poco a poco este tipo de sistemas han ido creciendo y los desarrolladores se han dado cuenta que la mejor forma de incentivar la adopción de software libre, es centrándose en la simplificación de su uso y ofreciendo sencillez a los usuarios. Sin embargo, una de las características de este tipo de sistemas que ha fomentado la idea de complejidad es la famosa consola del sistema o «shell». No se concibe un sistema «GNU/Linux» sin una consola «shell», son elementos inseparables, al menos de momento.

La idea de tener que escribir una serie de comandos u órdenes en un entorno sin ventanas o elementos gráficos que añadan sencillez para realizar las distintas tareas, aumenta la idea de complejidad entre los usuarios más inexpertos. Existen sistemas operativos donde copiar un fichero es tan sencillo como seleccionar un icono gráfico y arrastrar a otra ubicación, mientras que en sistemas «Linux» es necesario aprenderse una seria de comandos que permitan realizar la misma acción. Esto puede suponer todo un reto para ciertos usuarios menos experimentados y favorecer la huida a sistemas más sencillos fuera del entorno de código libre. Pero poco a poco se ha ido solventando este tipo de incomodidades, y aunque la consola de sistema sigue siendo parte fundamental de los sistemas «GNU/Linux», poco a poco se ha incentivado el uso de entornos gráficos amigables.

Sin embargo, la consola «shell» juega un papel fundamental, ofreciendo una versatilidad y un control sobre los sistemas incomparable. Aquellas personas que conocen y utilizan la consola de comandos, son conscientes de sus capacidades y de las opciones que ofrece tanto a los usuarios menos avanzados como a aquellos más experimentados. Pero es cierto que ciertas acciones cotidianas pueden llegar a repetirse con cierta frecuencia, favoreciendo el uso de automatizaciones o

la creación de pequeños programas que facilitan ciertas tareas más complejas y tediosas. Este tipo de programas más pequeños son los «scripts», adaptados a cualquier necesidad. Tareas complejas pueden simplificarse a través de este tipo de automatizaciones, gracias a la potencia que ofrece la consola de comandos. Todo programa instalado en el sistema operativo, ofrece la posibilidad de usar comandos y argumentos, lo que permite poder ejecutar todas las acciones que ofrece la herramienta a través del intérprete de comandos, sin necesidad de entorno gráfico.

La complejidad que suponen este tipo de sistemas no se centra solamente en el uso de aplicaciones, la propia configuración del entorno, puede suponer un verdadero quebradero de cabeza para usuarios medios. La configuración y manejo de las redes, tanto inalámbricas como cableadas, es en algunos casos una tarea ardua; controlar las redes a las que nos conectamos o configurar la tarjeta adecuadamente son tareas sencillas que pueden llegar a complicarse en exceso si no se tienen los conocimientos adecuados. Más aun si hablamos de tareas de mayor complejidad, como cambiar el modo de trabajo de una tarjeta de red, detectar equipos conectados a una red, o analizar los servicios presentes en la misma. Son tareas consideradas como complejas que pueden simplificarse con la ayuda de la consola de comandos y la automatización de los «scripts». Al utilizar la «shell de bash» disponemos de un intérprete de comandos con una potencia de automatización y control del sistema absoluta, facilitando todas las tareas mencionadas anteriormente.

Todas las distribuciones basadas en «GNU/Linux» ofrecen una consola o intérprete de comandos. Generalmente esta consola comparte ecosistema con el resto de distribuciones, permitiendo una compatibilidad absoluta en cuanto a comandos y sintaxis se refiere. Así, un desarrollador podrá utilizar un mismo script en distintas distribuciones sin necesidad de instalar librerías de terceros o conectores especializados. Esta característica aporta universalidad, idea fundamental dentro del código libre, ampliando las posibilidades y opciones, apoyados por una comunidad de desarrolladores y usuarios totalmente distribuida a lo largo del planeta.

El desarrollo de este proyecto se ha centrado exclusivamente en entornos de redes inalámbricas y todas las posibilidades que ofrecen. Se ha intentado añadir simplicidad a tareas generalmente complejas debido a su ejecución a través de la consola de comandos. Tareas como acceder a una red o realizar una búsqueda de dispositivos conectados, pueden resultar acciones más o menos sencillas para usuarios inexpertos. Pero, la captura de tráfico o el análisis de los servicios de los distintos equipos dentro de una red, así como la inyección de tramas y el análisis de posibles ataques, son tareas sin lugar a dudas complejas de realizar. El uso del intérprete de comandos no facilita esta tarea, aunque si proporciona las capacidades necesarias para llevarlas a cabo. Este proyecto ha buscado poder simplificar todas estas acciones, desde las más sencillas hasta las que suponen una mayor complejidad, para que cualquiera usuario pueda sentirse cómodo de poder realizarlas.

En definitiva, los sistemas «GNU/Linux» siempre han sido considerados como elementos complejos restringidos a unos pocos expertos en informática. Pero poco a poco los desarrolladores han comprendido la importancia de la sencillez, y han creado distribuciones para todo tipo de usuarios, abarcando los requisitos más simples de un uso cotidiano, hasta la complejidad de un desarrollador o un analista de seguridad de redes. Independientemente de la complejidad de cada sistema, la base es la misma en todos los casos, un compendio de aplicaciones desarrolladas de

manera distribuidas y un núcleo común para gestionar la interacción con los elementos hardware del sistema. Esto permite a las distintas distribuciones ejecutar un mismo «script» basado por ejemplo en una «shell bash», ofreciendo enormes posibilidades de compatibilidad entre los distintos sistemas operativos. Un único desarrollador puede de manera sencilla, abarcar un gran número de sistemas y usuarios, automatizando comandos y ejecuciones de aplicaciones. Facilita la democratización del uso y desarrollo de la tecnología software, apoyado en una comunidad totalmente distribuida y basada en el código libre y la libertad de uso.

6 Glosario

802.11. Estándar de normas inalámbricas creadas por el Instituto de Ingenieros Eléctricos y Electrónicos o IEEE, que definen la tecnología Wi-Fi.

AMD (*Advanced Micro Devices).* Compañía estadounidense fabricante de semiconductores.

AP (*Acces Point).* Punto de acceso inalámbrico de una red informática.

ARP (*Address Resolution Protocol).* protocolo utilizado para la resolución de nombres de la capa de enlace de red.

BIOS (*Basic Input/Output System). S*istema básico de entrada-salida, aplicación estándar utilizada como interfaz de firmware en los computadores.

dBm. Decibelio es una unidad de medida de potencia utilizada en señales de radio y fibra óptica.

GNU (*GNU's Not Unix*). Proyecto de creación de software libre de manera distribuida.

GPU (*Graphics Processing Unit). U*nidad de proceso gráfico, es un procesador especializado en operaciones con coma flotante, utilizadas para el procesamiento gráfico.

Hacker. Persona con grandes conocimientos informáticos que estudia posibles brechas y fallos de seguridad en un sistema informático para ponerlas en conocimiento y desarrollar las mejoras necesarias.

IDE (*Integrated Development Enviroment*). Entorno de desarrollo que proporciona servicios integrales para facilitar al programador el desarrollo de software.

Intel. Compañía estadounidense fabricante de semiconductores.

ISO. Fichero que contiene una imagen de un sistema de ficheros.

Dirección IP. Identificador de dispositivo de la capa de red.

Kernel. Hace referencia al núcleo de un sistema operativo, encargado del acceso a los elementos hardware del dispositivo.

Dirección «MAC» (*Media Access Control)*. Identificador asignado por el IEEE utilizado en la capa de enlace.

LAN o Local Area Network. Hace referencia a la interconexión de varios dispositivos los cuales comparten una línea de comunicaciones común o un enlace inalámbrico.

Modo Managed. Modo de funcionamiento de las tarjetas de redes inalámbricas para conectarse a puntos de acceso wifi.

Modo Monitor. Modo de funcionamiento de las tarjetas de redes inalámbricas para analizar el espectro de red.

Nvidia. Fabricante de semiconductores especializado en unidades de procesamiento gráfico.

Nvme o NVM Express. Protocolo de acceso y transporte de información asociado a unidades de almacenamiento flash y de estado sólido.

Pcap. Formato de fichero de captura de tráfico. Se deben utilizar herramientas específicas para su lectura como Wireshark o tcpdump.

RAM o Random Access Memory, es memoria de acceso aleatorio utilizada por el ordenador para cargar los programas en ejecución.

Ryzen. Línea de producto de microprocesadores de la compañía AMD.

Router. Enrutador, dispositivo de red con la capacidad de interconectar dispositivos mediante rutas de enlace.

SSH o Secure Shell. Hace referencia al protocolo utilizado para establecer conexiones remotas de manera segura.

WEP o Wired Equivalent Privacy: Protocolo de seguridad de cifrado de conexiones de redes inalámbricas.

WPA o Wireless Protected Acces: Protocolo de seguridad de cifrado de conexiones de redes inalámbricas.

WPA2 o Wireless Protected Acces: Versión actualizada de WPA.

7 Bibliografía y referencias

7.1 Bibliografía

WILLIAM SHOTTS. *The Linux command line: a complete introduction. San Francisco, USA:* No starch press, 2019. ISBN: 9781593279523. Disponible en: https://nostarch.com/tlcl2

JAMES F. KUROSE – KEITH W. ROSS. *Computer Networking. A Top-Downapproach.* Amherst, USA. Pearson, 2017. ISBN: 9780273768968. Disponible en: https://www.pearson.com/us/higher-education/program/Kurose-Computer-Networking-A-Top-Down-Approach-7th-Edition/PGM1101673.html

NIK ALLEYNE. *Mastering Tshark Network Forensics. Mississauga, Canada: n3Security Inc., 2020.* ISBN: 9781775383024. Disponible en: https://www.securitynik.com/

7.2 Referencias

The Linux Kernel Archives [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.kernel.org

Linux Kernel [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://ayudalinux.com/que-es-el-kernel-en-linux-para-que-sirve/

GNU Operating System [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.gnu.org/

Wikipedia [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://en.wikipedia.org/

TP-LINK [en línea] [fecha de consulta: 24 de octubre de 2021]. Disponible en: https://www.tp-link.com/es/home-networking/adapter/archer-t2uh/

RedesZone [en línea] [fecha de consulta: 19 de noviembre de 2021]. Disponible en: https://www.redeszone.net/tutoriales/redes-wifi/bandas-frecuencias-wi-fi/

Aircrack-ng [en línea] [fecha de consulta: 14 de diciembre de 2021]. Disponible en: https://www.aircrack-ng.org/doku.php?id=Main

7.3 Imágenes

Imagen 1 - Ejemplo de kernel de Linux [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://ayudalinux.com/que-es-el-kernel-en-linux-para-que-sirve/

Imagen 2 - Proyecto Linux [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.kernel.org

Imagen 3 – Proyecto GNU [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.gnu.org/graphics/agnuhead.es.html

Imagen 4 – Funcionamiento Router [en línea] [fecha de consulta: 07 de diciembre de 2021]. Disponible en: https://www.xatakamovil.com/tutoriales/que-router-switch-hub-que-se-diferencian

Imagen 5 – Funcionamiento Switch [en línea] [fecha de consulta: 07 de diciembre de 2021]. Disponible en: https://www.xatakamovil.com/tutoriales/que-router-switch-hub-que-se-diferencian

Imagen 6 – Frecuencias 2,4GHz [en línea] [fecha de consulta: 19 de noviembre de 2021]. Disponible en: https://www.adslzone.net/reportajes/wifi/2-4-5-ghz

Imagen 7 – Frecuencias 5GHz [en línea] [fecha de consulta: 19 de noviembre de 2021]. Disponible en: https://www.adslzone.net/reportajes/wifi/2-4-5-ghz

Imagen 8 – 4-way Handshake [en línea] [fecha de consulta: 19 de noviembre de 2021]. Disponible en: http://fibraoptica.blog.tartanga.eus/2017/10/30/ampliacion-de-la-red-wifi-del-cifp-tartanga-y-actualizacion-del-firmware-de-los-aps-contra-la-vulnerabilidad-wpa-psk-krack/

Imagen 9 – Intel Wi-Fi 6 AX200 [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.amazon.es/Intel-AX200-Gig-Wi-Fi-Escritorio/dp/B085M7VPDP

Imagen 10 – Archer T2UH [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.tp-link.com/es/home-networking/adapter/archer-t2uh/

Imagen 11 – Ejemplo red mesh [en línea] [fecha de consulta: 23 de octubre de 2021]. Disponible en: https://www.xataka.com/especiales/redes-wifi-mesh-que-son-como-funcionan-y-por-que-pueden-mejorar-tu-red-wifi-en-casa