UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

EVALUACIÓN DEL DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD PARA COMBATIR ATAQUES EN REDES INALÁMBRICAS WI-FI

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

Autor(a) (es):

Bach. Cieza Celis Jesus Abelardo

ORCID: https://orcid.org/0000-0002-1929-3304

Bach. Ojeda Romero Anthonny Jhonatan

ORCID: https://orcid.org/0000-0002-0890-419X

Asesor:

Mg. Atalaya Urrutia Carlos William

ORCID: https://orcid.org/0000-0002-2761-4868

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2022

APROBACIÓN DEL JURADO

EVALUACIÓN DEL DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD PARA COMBATIR ATAQUES EN REDES INALÁMBRICAS WI-FI

Bach. Cieza Celis
Jesús Abelardo
Autor

Bach. Ojeda Romero
Anthonny Jhonatan
Autor

MG. Atalaya Urrutia Carlos William
Asesor

MG. Samillan Ayala Alberto Enrique
Presidente de Jurado

MG. Minguillo Rubio Cesar augusto
Secretario de Jurado

MG. Atalaya Urrutia Carlos William
Vocal de Jurado

DEDICATORIAS

A mis padres Raymundo y Lidia quienes con su gran esfuerzo, amor y humildad me han permitido llegar a cumplir un sueño más en mi vida, gracias por inculcar en mí el ejemplo de humildad y perseverancia.

A mi tía Flor por su cariño y apoyo incondicional durante todo este proceso y por estar conmigo en los momentos más difíciles de mi vida. A toda mi familia por cada uno de sus esfuerzos, consejos y palabras de aliento durante todo este proceso.

A mi abuelita Teodolinda por apoyarme en los momentos más difíciles y por el amor brindado.

Finalmente, a mis docentes y amigos que sumaron esfuerzos para poder lograr una meta más en mi formación profesional.

Anthonny

A mi madre, a mi familia quienes me dieron vida, educación, apoyo y consejos.

A mis compañeros de estudio, a mis maestros y amigos, quienes sin su ayuda nunca hubiera podido hacer esta tesis. A todos ellos se los agradezco desde el fondo de mi alma. Para todos ellos hago esta dedicatoria.

Jesús

AGRADECIMIENTOS

A toda mi familia por darme ánimo y seguridad durante este proceso.
A mis docentes y en especial a mi tutor por su ayuda, paciencia y dedicación.
A mis amigos de toda la vida que me acompañan desde siempre.
A mi amigo y compañero de tesis, Jesús, con quien sumamos esfuerzos para poder lograr una meta más en nuestra formación profesional.

Anthonny

A mi tutor por el tiempo dedicado y los conocimientos brindados.
A mis padres por la vida y por enseñarme a vivirla.
Por último, pero no por eso menos importante a todos mis familiares y amigos.

Jesús

Resumen

El uso de Internet inalámbrico es de uso común en las empresas y las instituciones en todo nivel, por lo que es necesario prevenir las amenazas que pueden producir los ataques informáticos. La Wi-Fi Alliance ha implementado diversos métodos para asegurar las redes inalámbricas de área local o WLAN (Wireless local area network), estos son los protocolos de autenticación para la seguridad de los datos del usuario como WEP, WPA, WPA2 y WPA3. Los protocolos de seguridad WiFi pasaron por muchos cambios y mejoras desde los años 90 para hacerse más seguros y eficaces, así que fueron agregando cambios tanto en su cifrado, y sus componentes, y se iban agregando actualizaciones para combatir vulnerabilidades y ataques que han ido surgiendo con los años. En el presente trabajo se presentó una descripción general de los protocolos de seguridad WLAN, para analizar y discutir las versiones, problemas y mejoras; esto con la finalidad de hacer una comparación entre estos. Para poder lograr el objetivo de la investigación se seleccionaron los protocolos de seguridad existentes para combatir los ataques en redes inalámbricas, se diseñó un escenario de pruebas para poder evaluar el desempeño de los protocolos, y finalmente, se realizaron pruebas de ataque con el fin de probar los protocolos de seguridad de red que fueron previamente seleccionados. Los resultados obtenidos lograron determinar que, el protocolo WPA3 tuvo mejor desempeño, reflejándose en los tiempos de penetración de 3.23min con el ataque ARP Spoofing + DNS Spoofing, 4.37min con el ataque Man in the middle, 23.15min con el ataque de suplantación de identidad o Phishing, 6min con el ataque DoS, 15.50min con el ataque de fuerza bruta, y 8.45 min con el ataque de diccionario a un ssid oculto. Estos tiempos fueron mucho mayores que los tiempos de penetración en caso de usarse los protocolos WPA y WPA2. Se concluye que el protocolo WPA3 resulta ser el más eficiente a la hora de combatir ataques informáticos, y además es necesario aplicar mecanismos de forma complementaria como el uso de firewalls, VLANs, sistema de detección de intrusos, soluciones de alto nivel como Redes Privadas Virtuales (VPN) y servidores RADIUS para poder excluir, filtrar y monitorear cualquier cambio inadecuado en la WLAN para hacer las correcciones inmediatas.

Palabras Clave: Seguridad informática, Seguridad inalámbrica, Redes inalámbricas, Ciberataques, WLAN, WPA, WPA2, WPA3.

Abstract

The use of wireless Internet is in common use in companies and institutions at all levels, so it is necessary to prevent the threats that computer attacks can produce. The Wi-Fi Alliance has implemented various methods to secure wireless local area networks or WLAN (Wireless local area network), these are the authentication protocols for the security of user data such as WEP, WPA, WPA2 and WPA3. WiFi security protocols went through many changes and improvements since the 90s to become more secure and efficient, so changes were added to both its encryption and its components, and updates were added to combat vulnerabilities and attacks that have emerged. with the years. In the present work a general description of the WLAN security protocols was presented, to analyze and discuss the versions, problems and improvements; this in order to make a comparison between them. In order to achieve the objective of the investigation, the existing security protocols were selected to combat attacks on wireless networks, a test scenario was designed to be able to evaluate the performance of the protocols, and finally, attack tests were carried out in order to test the network security protocols that were previously selected. The results obtained were able to determine that the WPA3 protocol had better performance, reflected in the penetration times of 3.23min with the ARP Spoofing + DNS Spoofing attack, 4.37min with the Man in the middle attack, 23.15min with the spoofing attack. Identity or Phishing, 6 min with the DoS attack, 15.50 min with the brute force attack, and 8.45 min with the dictionary attack on a hidden ssid. These times were much greater than the penetration times when using the WPA and WPA2 protocols. It is concluded that the WPA3 protocol turns out to be the most efficient when it comes to combating computer attacks, and it is also necessary to apply complementary mechanisms such as the use of firewalls, VLANs, intrusion detection system, high-level solutions such as Virtual Private Networks (VPN) and RADIUS servers to be able to exclude, filter and monitor any inappropriate changes in the WLAN to make immediate corrections.

Keywords: Computer security, Wireless security, Wireless networks, Cyberattacks, WLAN, WPA, WPA2, WPA3.

Índice

I. INTRODUCCIÓN

1.1. Realidad Problemática.

El camino inalámbrico a Internet ha pasado a ser parte de la vida cotidiana e infraestructura de organizaciones y establecimientos de todas las extensiones, y es bastante común que las empresas ofrezcan conexión Wi-Fi a sus clientes, pero ante las amenazas cibernéticas, se requiere cierta prevención.

Todos los tipos de organizaciones se están modificando para encarar los desafíos de la economía de las empresas en el mundo globalizado. Las innovaciones en las empresas dan lugar a nuevos tipos de productividad, ventajas en la competitividad y crecimiento de los ingresos que incentivan a la administración con eficiencia de los recursos de conectividad de una empresa. Es casi un hecho que mucho de lo que esperan los clientes y empleados en cuanto a conectividad en la red inalámbrica en las empresas, sea aún mayor con el paso del tiempo, exigiendo tener acceso a una red Wi-Fi para obtener información en tiempo real en cualquier momento y en cualquier lugar; lo cual presenta grandes beneficios a tomar en cuenta, pero a la vez da lugar a enfrentar desafíos, sobre todo en ciberseguridad.

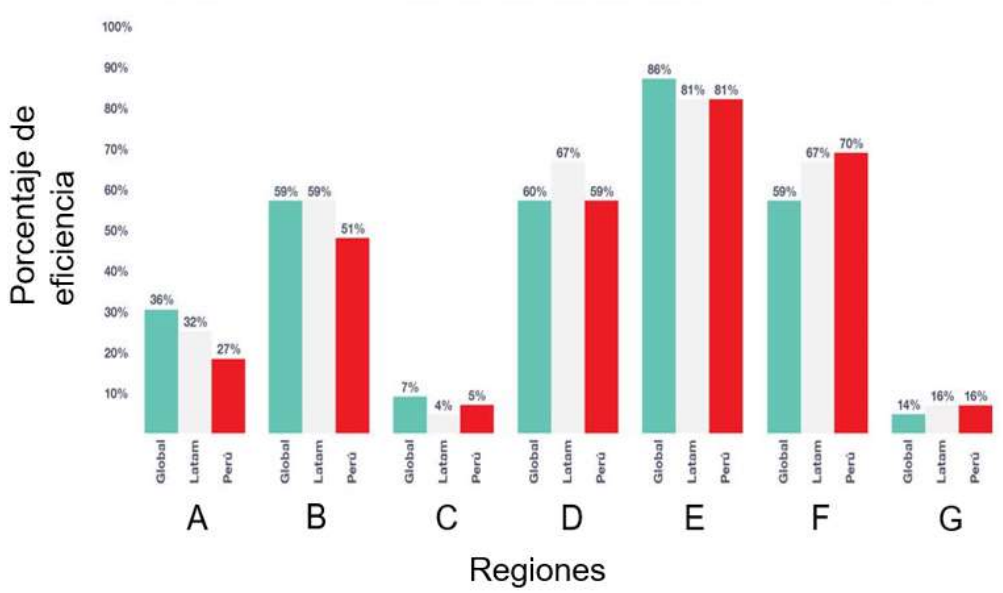
Las empresas que van en progreso son las más propensas a estar arriesgando su seguridad, se ha estimado que 62% de los ataques cibernéticos tienen como objetivo principal las pequeñas y medianas empresas, sucediendo alrededor de 4.000 incidentes relacionado diariamente en todo el mundo. Cuando una empresa se permite una conexión inalámbrica de forma abierta tanto para usuarios, clientes o externos, el rango de vulnerabilidad se amplía en gran medida, esto debido a que son muchos dispositivos y usuarios los que terminan teniendo acceso a la red. (Mendez, 2018).

La seguridad informática es algo en lo que las organizaciones podrían gastar infinitamente en un intento de mantener alejados a los atacantes. En una encuesta elaborada a empresas por (CISCO, 2019) se señala que el 56 % de los encuestados ha tenido un problema de seguridad importante en el último año. El 94 % de los encuestados dijo que son conscientes de que hay que seguir

avanzando para implementar una seguridad eficaz. Y el 43 % admite que, a veces, tienen que tomar atajos para lidiar con problemas de seguridad como se muestra en la siguiente figura.

Figura 1: Estado actual de las organizaciones de hoy en día con respecto a la seguridad informática. Fuente: *(CISCO, 2019)*

De acuerdo a la Encuesta Global de Seguridad de la Información 2019-2020 de Ernst & Young (EY), empresa multinacional para servicios profesionales del mundo, para asesoramiento en la gestión de la empresa, la cual fue publicada por (Gestion.pe, 2020), apenas el 27% de empresas en el Perú da cabida a la ciberseguridad desde el planeamiento de sus nuevas iniciativas; en tanto que un 51% señala que la relación entre la ciberseguridad y la empresa es limitada o indiferente. Además, el 81% expone que la prevención de crisis y el cumplimiento siguen siendo los motivos esenciales para aumentar el presupuesto de seguridad informática. Pese a eso, EY señala que, de las empresas en Perú, el 59% no cuenta con un responsable de ciberseguridad que haga reportes a la dirección o que se encuentre a nivel de gerencia ejecutiva.



A: Incluye el área de ciberseguridad desde la etapa de planificación en sus nuevas iniciativas empresariales.

B: Dice que la relación entre la ciberseguridad y las líneas de negocio es inexistente o neutral.

C: Describe el are de ciberseguridad como un habilitador de innovación.

D: No cuenta con un responsable de ciberseguridad que reporte al directorio.

E: Dice que la prevención de la crisis y el cumplimiento siguen siendo los impulsadores principales para aumentar el presupuesto de ciberseguridad.

F: Ha experimentado un incidente significativo realizado por los empleados en los últimos 12 meses.

G: Del presupuesto de ciberseguridad es usado para programas de transformación digital.

Figura 2: Encuesta Global de Seguridad de la Información 2019-2020 de EY con respecto a la ciberseguridad. Fuente: (Gestion.pe, 2020)

Pero la seguridad de la red inalámbrica no es un asunto que solo le compete a las grandes, medianas o pequeñas empresas, sino que todos los que utilicen una red deben al menos tener cierto conocimiento de las nociones de seguridad básicos, para no convertirse en el objetivo de los delincuentes informáticos al conectarse a una red Wi-Fi, porque cuando se utiliza una red que resulta no ser segura, podría permitir que cualquier persona con la habilidad suficiente pueda interceptar del tráfico de Internet. (Kaspersky, 2014). Con el problema de interceptación de redes, ha pasado a ser un tópico de investigación recurrente

en los últimos años y más con el crecimiento acelerado de la población de usuarios de Wi-Fi. Además, se han desarrollado muchos sistemas que detectan los diversos ataques y previenen las intrusiones en la red inalámbrica (Jeong, Chang, & Na, 2008).

En cuanto a las redes inalámbricas, encontrar un punto de acceso inalámbrico local es solo la mitad del trabajo, a menos que, por supuesto, el punto de acceso se deje abierto sin cifrado y voluntariamente proporcione una dirección IP a cualquiera que se conecte. A pesar de eso, para puntos de acceso inalámbricos debidamente asegurados, aún es posible atacar la implementación de seguridad para determinar las contraseñas seguras que utilizan las computadoras portátiles autorizadas para conectarse (Street, Nabors, Baskin, & Carey, 2010).

En consecuencia, se han implementado diversos métodos para asegurar las redes inalámbricas de área local o WLAN (Wireless local area network). WLAN protocolos de autenticación para la seguridad de los datos del usuario como WEP, WPA, WPA2 y WPA3 (Kaur, 2017). WEP o Privacidad equivalente por cable por sus siglas en inglés, fue el primer estándar IEEE 802.11 que vino con un mecanismo de autenticación simple. WEP tiene grandes debilidades y fue vulnerada en 2001. Un atacante puede encontrar la clave de autenticación de una red con una computadora portátil de capacidad normal en un promedio de 1 a 2 horas. Para eliminar la debilidad anterior, se desarrolló un nuevo protocolo en 2003, llamado Acceso protegido Wi-Fi o WPA. WPA solía eliminar los problemas del método de criptografía WEP. Un año después, en 2004 llegó la segunda versión, llamada WPA2, para reemplazar el protocolo WPA normal. WPA2 desarrolló un método de codificación avanzado para respaldar la seguridad más sólida. Aun así, WPA2 sufrió fallas debido al ataque de reinstalación de claves o KRACK (Key Reinstallation Attack) en 2017 por (Vanhoef & Piessens, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, 2017). Este ataque se aprovecha de fallas de diseño o implementación en protocolos criptográficos para reinstalar una clave que ya está en uso. Esto restablece los parámetros asociados de la clave, como transmitir nonces y

recibir contadores de reproducción. Para mitigar las vulnerabilidades de WPA2, la Wi-Fi Alliance dio a conocer el protocolo de seguridad WPA3, el cual resulta mucho más confiable que su predecesora WPA2 y e incluso que los protocolos más antiguos.

Las principales vulnerabilidades de WPA2, como el handshake de cuatro vías imperfecto y el uso de una PSK (o clave pre-compartida) son cubiertas por WPA3 dado que posee mejoras de seguridad adicionales que hacen que sea menos fácil acceder a las redes adivinando las contraseñas (ASUS, 2021). Pese a esto, el protocolo WPA3, el cual ya estaba listo para implementarse en la última actualización de 802.11, la 802.11ax o Wi-Fi 6, ha ido presentado algunos problemas en su nuevo sistema Dragonfly para conectar dispositivos, dichas vulnerabilidades en conjunto han sido llamadas Dragonblood (Vanhoef & Ronen, 2020). Ante tal escenario la Wi-Fi Alliance se ha pronunciado para señalar que WPA3-Personal se encuentra en las primeras etapas de implementación y el pequeño número de fabricantes de dispositivos afectados ya ha comenzado a implementar parches para resolver los problemas (Wi-Fi Alliance®, 2019).

En el presente trabajo se presenta una descripción general de los protocolos de seguridad WLAN, explicando la estructura de los protocolos de seguridad inalámbricos para analizar y discutir sus versiones, problemas y mejoras; esto con la finalidad de hacer una comparación entre WEP, WPA, WPA2 y WPA3. El estudio conjunto de dichos protocolos, sobre todo con WPA3 no ha sido tratado profundamente. La seguridad de las redes inalámbricas es muy importante dada su amplia aplicación en la actualidad, como instrumentación médica, equipos industriales, monitores de seguridad o incluso en oficina, por lo que se espera que el presente trabajo permita contribuir con el conocimiento en seguridad informática tanto en personas, empresas y universidades, para advertir ataques e intrusiones de terceros cuyo fin es atentar contra la seguridad de la información.

1.2. Trabajos previos.

Singh & Sharma (2019) en su investigación denominada “An Overview Of WLAN Security” de la Universidad de Delhi, presentan una descripción general de las amenazas, los remedios y las soluciones de WLAN. Para hacer que la comunicación WLAN sea segura, existen varios protocolos estándar como WEP, WPA y WPA2. Debido a esto, los organismos estándar han propuesto cuatro soluciones para mejorar la seguridad de la WLAN. Estos son: seguridad básica, Privacidad equivalente por cable (WEP), Acceso protegido Wi-Fi (WPA) y IEEE 802.11i (WPA2), los que utilizan medidas correctivas como autenticación, confidencialidad, administración de claves, control de acceso, integridad y mejora de la disponibilidad. Ellos señalan que los avances de WPA2 fueron: uso de protocolo de enlace de 4 vías y cifrado más fuerte, pero, aun así, la reputación de este último se vio afectada por ataques DoS y KRACK, y a la fecha estaban esperando por nueva documentación del estándar WPA3. Como alternativa para mitigar dichas vulnerabilidades, los autores citan tres esquemas de seguridad denominados fast WLAN initial access authentication protocol (FLAP), Secure Wireless Authentication Scheme (SWAS) y Key Hiding Communication (KHC). Los resultados muestran que el mecanismo FLAP no protege contra ataques DoS y, por lo tanto, obstaculiza la disponibilidad. A FLAP también le preocupan los ataques de repetición y los ataques MitM y que también es visible que los esquemas SWAS y KHC protegen contra la mayoría de los ataques y también son efectivos contra los ataques DoS. Por lo tanto, SWAS y KHC brindan cierta esperanza contra los ataques DoS, que son las principales preocupaciones en WPA2. Los autores esperan que WPA2 se siga utilizando en los dispositivos existentes, mientras que los nuevos dispositivos desarrollados seguirán la compatibilidad con las nuevas versiones de WPA. Por lo tanto, actualmente los investigadores propones tres vías principales en el dominio de la seguridad WLAN: fortalecer el estándar WPA2, desarrollar un nuevo mecanismo de autenticación de entidades y control de acceso y, analizar y fortalecer el próximo estándar WPA3.

Guo, Wang, Zhang, & Zhang (2020), realizaron una propuesta denominada A Secure Session Key Negotiation Scheme in WPA2-PSK Networks, en Seúl, capital de Corea del Sur. La clave pre-compartida Wi-Fi Protected Access II (WPA2-PSK) es una forma activa de seguridad inalámbrica en redes públicas de Wi-Fi. Funciona con una frase de contraseña pre-configurada compartida con todas las estaciones en la misma red Wi-Fi. Las redes WPA2-PSK pueden autenticar estaciones externas, sin embargo, no garantizan la comunicación confidencial si los atacantes internos poseen la contraseña en la red, ya que todas las estaciones derivan su PTK utilizando la misma contraseña. Para evitar que las estaciones internas escuchen el PTK, se propone un esquema de negociación de clave de sesión segura en redes WPA2-PSK (SSKNS). Se introduce una clave de sesión temporal (TSK), que se cifra mediante criptografía de curva elíptica (ECC) y se intercambia de forma segura entre la estación y el AP en el proceso de asociación Wi-Fi. A través del algoritmo AES con TSK, la estación encripta su propio nonce (un número arbitrario que se puede usar solo una vez en una comunicación criptográfica) usado para generar el PTK único en el proceso de 4 vías. La propuesta evalúa principalmente la sobrecarga de tiempo, en comparación con los existentes WPA2-PSK y SAHS, por lo tanto, en el esquema propuesto se mide el tiempo de generación de claves relacionado con el algoritmo ECC de forma independiente y el retraso en la comunicación, incluida la transmisión de datos, el cifrado y descifrado ECC y AES. Los resultados indican que WPA2-PSK y SAHS, SSKNS tienen casi el mismo tiempo de transmisión DTx2 (aproximadamente 1200 us). En el cifrado y descifrado con algoritmo AES256, observamos que SAHS y SSKNS necesitan aproximadamente 189us (4DAESEnc + 4DAESDec) y 46us (DAESEnc + DAESDec) respectivamente. El resultado indica que SSKNS causa menos sobrecarga de tiempo que SAHS y un poco más que WPA2-PSK. Esto se debe al cifrado y descifrado selectivo solo para un mensaje en SSKNS, en lugar de cuatro mensajes, lo que provoca una protección excesiva en SAHS. Los análisis y experimentos de seguridad muestran que SSKNS puede proporcionar de manera efectiva un nivel de seguridad a un costo aceptable, en comparación con los esquemas existentes.

Noh, Kim, Kwon, & Cho (2016), elaboraron un trabajo denominado Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography, en Seúl, Corea del Sur. Este artículo propone el esquema de intercambio seguro de claves para aplicar una criptografía de clave pública. Usando el sistema de clave pública, un apeadero y un lugar de umbralado intercambian una fundamental secundaria que el usuario selecciona. Esta clave se utiliza para la suscitación de claves por pares. Mediante el extracto propuesto, la red puede defender a los usuarios de varios ataques en la misma red Wi-Fi. El procedimiento es el siguiente: un Access Point (AP) difunde frecuentemente una trama que incluye información sobre la red correspondiente, lo que sigue son dos pasos que son los mismos que los de la solicitud de sondeo original y los mensajes de respuesta. Luego cuando una estación solicita autenticación, la estación envía una clave secundaria y una frase de contraseña al AP. Este mensaje está encriptado usando la clave pública de AP. La clave secundaria se utilizará para un solo usuario. Después, el AP descifra el cuarto mensaje usando su clave privada. El AP comprueba una frase de contraseña. Si es correcto, envía un mensaje de respuesta que está encriptado por claves privadas y secundarias. Una vez que la estación recibe el botellín informe, intenta resolver el texto usando dos teclas. Al dilucidar el informe, la estación puede aprender que la estratégica secundaria se intercambió con éxito y este texto es representante por el AP. finalmente, después de la autenticación, la estación y el AP realizan el expediente de congregación en normal con el memorial real. Y mientras, finaliza todo el memorial de límite. Al proteger el estudio de tráfico, los usuarios están a indemne de ataques adicionales, como autenticación falsa y ataque de recuperación de claves.

Lamers, Dijksman, van der Vegt, Sarode, & de Laat (2021) presentaron su investigación denominada “Securing Home Wi-Fi with WPA3 Personal” en Las Vegas, NV, USA. El protocolo WPA3 se convirtió en una parte obligatoria de la certificación Wi-Fi el 1 de julio de 2020, por lo que se espera, se espera que la tasa de adopción de dicho protocolo se tome en consideración en estos últimos años. En la investigación se estudia si es posible proteger una red protegida con WPA3 de tal manera que los ataques de degradación no sean factibles, puesto

que incluso con las recomendaciones de seguridad que la Wi-Fi Alliance emitió recientemente para WPA3, las implementaciones comunes que se ejecutan en modo de transición aún se pueden degradar a WPA2. Para identificar aún más los problemas con las implementaciones actuales de WPA3, se llevaron a cabo cuatro experimentos que son: Comportamiento de conexión automática de las estaciones, Selección de estación BSS, ataque de degradación y ataque de denegación de servicios. Los resultados muestran que aún se pueden degradar varias estaciones en las redes WPA3. Todas las degradaciones en los experimentos se lograron utilizando hardware de consumo de diez años de antigüedad sin software especial o propietario y con poca dificultad inherente para realizar. Cabe resaltar que los resultados de este experimento son comparables para los dos AP que se utilizaron y, por lo tanto, el análisis de los resultados se centra en las estaciones. Dentro de los resultados, también se observan muchas opciones para mejorar y ampliar WPA3. Sin embargo, también es necesario preguntarse cuál de estas opciones traerá la mejora más significativa en términos de seguridad además de ser fácil de usar. Como ya se vio con otros estándares y adiciones de Wi-Fi, la adopción requiere un cambio en el transcurso del tiempo. Por lo tanto, las adiciones deben estar preparadas para el futuro o corren el riesgo de quedar obsoletas antes de que se adopten ampliamente.

Vanhoef & Ronen (2020), publicaron el artículo “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd” en San Francisco, Estados Unidos. La certificación WPA3 tiene como objetivo proteger las redes inalámbricas Wi-Fi y utiliza el handshake Dragonfly para proporcionar un sigilo y resistencia a los ataques del diccionario. En este documento, evaluamos sistemáticamente la seguridad de Dragonfly. Primero, se auditaron las implementaciones y se presentaron pérdidas de tiempo y omisiones de autenticación en WPA3 para luego estudiar el diseño de Dragonfly y analizar los ataques de degradación y denegación de servicio. Los principales resultados son los ataques de canal lateral contra el método de codificación de contraseñas de Dragonfly (por ejemplo, hash a curva), ya inherentes a Dragonfly. También se analizó la complejidad de usar la información filtrada para forzar la

contraseña, esto por ser de interés general debido a los esfuerzos de estandarización en curso en Dragonfly como un protocolo de enlace TLS, intercambios de claves autenticados con contraseña (PAKEs) y hash a curva. Finalmente, se discutió sobre las defensas compatibles con versiones anteriores y se proponen correcciones de protocolo que evitan los ataques.

Moissinac, Ramos, Rendon, & Elleithy (2021) presentaron el documento denominado “Wireless Encryption and WPA2 Weaknesses” en Nevada, Estados Unidos. El cifrado prevalece en muchas formas de comunicaciones modernas, y dado su avance en la seguridad de las comunicaciones inalámbricas, esto debería tener más importancia, ya que cualquier dispositivo puede interceptar fácilmente los datos en su rango. Este documento se enfocó específicamente en la comunicación inalámbrica IEEE 802.11 y la evolución de sus protocolos de encriptación desde WEP hasta el actual WPA3 para identificar las debilidades actuales y los métodos de mejora. Existen mecanismos para ofrecer una mejor protección para las comunicaciones de red inalámbrica, como servidores RADIUS, certificados y nuevos enfoques de intercambio de WPA3. Sin embargo, algunas de estas soluciones no solo implican una sobrecarga de recursos, sino que también se han descubierto vulnerabilidades en el WPA2 e incluso en los protocolos WPA3 más nuevos. Por lo tanto, este documento incluye los algoritmos de criptografía seleccionados y los gastos generales necesarios para implementarlos, como recursos computacionales, certificados y requisitos de servidor externo. Se concluye también que el cifrado de nivel empresarial a más dispositivos en el hogar y en entornos de pequeñas empresas. La solución aprovecha los protocolos existentes y los aplica de manera creativa para realizar esfuerzos de desarrollo nominales e imponer solo una mínima sobrecarga.

Fehér & Sandor (2018) presentaron su proyecto denominado “Effects of the WPA2 KRACK Attack in Real Environment” en Subotica, Serbia. El protocolo Wi-Fi más utilizado en el mundo, el WPA2, contenía una vulnerabilidad y varios problemas descubiertos y publicados por investigadores de ciberseguridad en los últimos años y esto afectó al mundo de las tecnologías de la información y

se pueden esperar más cambios. Este artículo examina los detalles y los efectos de este cambio junto con el comportamiento del usuario para lo cual se desarrolló una investigación de encuestas cuantitativas para recopilar más información sobre el comportamiento de los usuarios promedio, la conciencia de seguridad y para identificar los grupos de usuarios comprometidos. Según la encuesta, el 87,3% de los encuestados tiene Wi-Fi en su hogar. La encuesta fue completada por 379 personas y ampliamente distribuida para obtener resultados más variados, por lo que no se pudo separar a las personas vulnerables de las no vulnerables, pero se logran ver los dos extremos de la escala. Con base en la información recopilada, se puede declarar que los problemas generalmente se están acumulando. El principal problema en esta situación es el elevado número de usuarios afectados. Los usuarios más experimentados ya han actualizado el firmware de sus routers y dispositivos Wi-Fi para evitar este tipo de problemas, pero la mayoría de los propietarios de dispositivos son usuarios finales medios. Este problema consta de varios elementos consistentes, como una contraseña demasiado débil y demasiado corta. La contraseña encriptada adquirida se puede descifrar fácilmente si la contraseña es débil; además, la capacidad informática crece año tras año. Del estudio se desprende también que 108 personas, el 29% de los usuarios examinados, tienen una contraseña de 8 caracteres en su Wi-Fi. La mayoría de las contraseñas contienen mayúsculas y números junto a las minúsculas, lo que significa que una computadora promedio tardaría aproximadamente 2 horas en descifrar estas contraseñas con un simple ataque de fuerza bruta. El estudio concluye diciendo que hasta la publicación de WPA3 y la difusión del nuevo protocolo, la mejor solución para mitigar el riesgo de la nueva vulnerabilidad es parchear el firmware de los dispositivos afectados. Lamentablemente, los dispositivos más antiguos no son compatibles con el fabricante, la mayoría de ellos son vulnerables, por lo que es necesario reemplazarlos. La parte más difícil en esta situación es llegar a los usuarios promedio y motivarlos para que actualicen o reemplacen sus dispositivos o utilicen mitigaciones basadas en software. Algunos proveedores de servicios de Internet ofrecen dispositivos de red Wi-Fi con su suscripción y pueden administrar sus dispositivos conocidos para manejar las vulnerabilidades de seguridad más altas. El elemento esencial más crítico es la

conciencia del usuario y el conocimiento del usuario porque el mercado está lleno de diferentes dispositivos no compatibles sin la actualización automática.

Castillo-Velazquez, Alcalá, & Serrano (2019) presentaron su trabajo llamado “Hardening as a best practice for WLAN Security Meanwhile WPA3 is released” en Guatemala, Guatemala. Desde 2004 hasta hoy es común usar WPA2 que reemplazó al WPA ya desfasado en la seguridad de WLAN. WPA ya había desplazado a WEP en 2003, debido a que este primer protocolo de seguridad se rompió. El problema de seguridad de la WLAN es que WPA2 fue vulnerado en 2017, pero aún WPA3 está en desarrollo, mientras que la gente busca seguridad en su WLAN. Este trabajo ofrece recomendaciones comprobadas cuando se aplica el hardening basado en un análisis para un escenario de prueba. La metodología para la identificación de vulnerabilidades contó con tres elementos: a) el diseño de un escenario de prueba utilizando un BSS (Basic Service Set); b) instalar una máquina virtual con Kali Linux y una tarjeta Wi-Fi (IEEE 802.11 b / g / n) a 2.4 GHz llegando a 50 m, y una antena de 5 dBi; atacando para WEP, WPA y WPA2 usando las herramientas suite air y hostapd-wep. Luego, después de detectar vulnerabilidades, se procede a implementar el hardening. Los resultados muestran que la seguridad de la WLAN se fortalece al implementar el hardening y además se confirmó que WEP era el más fácil de atacar, gastando menos tiempo y esfuerzo, después de WPA y después de WAP2, ya que el tiempo de convergencia está en función de los diccionarios. Como se demostró, es posible y se recomienda utilizar la seguridad empresarial WPA2, incluido tal vez Raspberry como servidor de autenticación. El hardening fue muy útil pero a la hora de implementar características de AP deben ser consideradas, debido a que algunas marcas o modelos de AP no dejan cambiar todas las características que requerimos para realizar un hardening completo.

Liu (2015), presentó su trabajo denominado Defense of WPA/WPA2-PSK Brute Forcer en Shanghái, China. Con la aparición de la fuerza bruta WPA / WPA-PSK de alta velocidad, la seguridad de la WLAN se enfrenta a graves amenazas. Los atacantes pueden adquirir PSK fácilmente para descifrar todos los tráficos. Para solucionar este problema, se proponen una serie de esquemas de defensa,

que incluyen esquemas de defensa para fuerza bruta pasiva y activa. Los esquemas adoptan bloqueadores activos e inyección de paquetes inalámbricos. Y luego se procesa el análisis teórico y se dan los métodos de implementación. La clave para descifrar con éxito es la adquisición de mensajes de protocolo de enlace de 4 vías. Por lo tanto, la defensa de la fuerza bruta WPA / WPA2-PSK es interferir o evitar la adquisición de mensajes 4-Way handshake. Como la alta velocidad de craqueo de la fuerza bruta existente, una vez que el atacante adquiere los mensajes de protocolo de enlace y el ciclo de actualización de PSK es grande, la probabilidad de éxito del craqueo es alta. Para simplificar la discusión, se supondrá que el PSK no se cambia cuando el Access Point está online. Por lo tanto, la probabilidad de éxito del craqueo es igual a la probabilidad de adquisición de mensajes de reconocimiento correctos, particularmente la tasa de mensajes de reconocimiento correctos en los mensajes capturados. Si el esquema de defensa puede reducir la probabilidad de adquisición o no, son los criterios de verificación del esquema de defensa.

Onno, Gelloz, Heen, & Neumann (2012), elaboraron un estudio denominado User-based authentication for wireless home networks en Berlín, Alemania. Este estudio señala que la totalidad de las redes domésticas inalámbricas aplican un tópico de autenticación de clave compartida para autenticar dispositivos. Esto da como consecuencia debilidades de seguridad por obra del protocolo inalámbrico en sí y las condiciones del ambiente doméstico. Más allá de los aspectos de seguridad, existen algunas ventajas para proporcionar una autenticación basada en el usuario para controlar mejor quién accede a la red en lugar de qué dispositivo accede a la red. Los esquemas de autenticación basados en usuarios también facilitan la elaboración de perfiles de usuarios, lo cual es útil para aprovechar más servicios de recomendación. Este documento describe una solución basada en WPA2-802.1X para mitigar las debilidades mencionadas anteriormente mientras se habilita una autenticación basada en el usuario en el hogar. La solución consiste en implementar mecanismos adicionales en una puerta de enlace de red doméstica existente, de la siguiente manera. Se usa un SSID (Service Set Identifier) inalámbrico dedicado que proporciona la configuración de red correcta y el certificado necesario.

Incorporamos un servidor de autenticación FreeRadius dentro de la puerta de enlace. Este servidor de autenticación implementa un método de autenticación PEAPv0 / EAP-MSCHAPv2 que permite una autenticación mutua basada en el certificado del servidor y las credenciales de nombre de usuario / contraseña del cliente. Presenta su certificado de servidor de autenticación a los clientes que deseen autenticar el servidor. Un portal web cautivo redirige a los usuarios no registrados y, a su vez, propone al usuario que ejecute un subprograma. Esta solución debe Facilitar interfaces sencillas de usar y garantizar un equilibrio entre seguridad y usabilidad, especialmente para tareas administrativas. Además, el modelo basado en 802.1X también es compatible con redes cableadas.

Taha & Shen (2012), plantearon un estudio llamado A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET, en Anaheim, California. En este documento, basado en la criptografía de clave pública sin certificado, se propone un esquema de acuerdo de clave y autenticación de capa de enlace, CL-AKA. CL-AKA logra la autenticación mutua entre un MNN y un enrutador móvil (MR) y crea una clave compartida segura entre ellos. A diferencia de los esquemas de seguridad Wi-Fi existentes, CL-AKA usa solo una verificación de certificado para verificar un MR en un MNN mientras verifica implícitamente este MNN en el MR. Por lo tanto, el esquema CL-AKA propuesto tiene un 23,76% menos de sobrecarga de cálculo que el del protocolo WPA2 basado en EAP, menos sobrecarga de comunicación que el del portal cautivo y un nivel de seguridad más alto que el del esquema de autenticación ficticia. Además, las evaluaciones de desempeño demuestran que CL-AKA consume poca energía, lo que lo hace más apropiado para implementar en dispositivos portátiles de menor consumo de energía, como PDA (Asistente Digital Personal) y teléfonos celulares.

Kumar, Chakraborty, Barbhuiya, & Nandi (2016), plantean un trabajo denominado Detection of Stealth Man-In-The-Middle Attack in Wireless LAN en Solan, India. Las redes de área local inalámbricas abstractas (WLAN) están alcanzando un lugar en todas las verticales de la vida. Las WLAN se han

acostumbrado a cambios rápidos con respecto a sus estándares de seguridad en un tiempo corto. El ataque Man in-the-Middle (MITM) es uno de los ataques más desastroso en WLAN. El ataque Stealth MITM (SMITM) es una nueva forma de hacer MITM basada en la intoxicación del Protocolo de resolución de direcciones (ARP). En este ataque, el envenenamiento ARP se realiza directamente a la víctima mediante la falsificación de la estructura del protocolo de respuesta del marco ARP y la explotación de la administración de claves WPA2. En este artículo se propone un Sistema Inalámbrico de Detección de Intrusiones (WIDS) para ataque SMITM. El WIDS propuesto detecta con éxito el ataque SMITM y otros ataques similares como MITM (usando envenenamiento ARP) y IP Spoofing. El sistema se simula para dos escenarios diferentes. Uno es el escenario normal y el segundo es el escenario de ataque. En un escenario normal, BLTabie permanece vacío ya que no hay ningún atacante. El segundo escenario es el escenario de ataque. El atacante sigue escuchando en su interfaz en modo promiscuo una solicitud ARP de la víctima-1 a la víctima-2. Tan pronto como lo recibe, envía una respuesta ARP falsa. El nodo sensor en el rango del nodo atacante captura esta respuesta ARP del atacante y envía una solicitud de sondeo al AP con la IP-MAC de origen de la respuesta ARP. Al recibir la solicitud de sondeo, el AP transmite una solicitud ARP para el par IP-MAC. Según la respuesta ARP, el AP envía una respuesta positiva o negativa al nodo sensor. El nodo sensor luego descubre si se trata de un ataque lP-Spoofing o SMITM o si se trata de un escenario normal. El sistema WIDS propuesto se simula en un simulador de red NS-3 y se encuentra que el esquema funciona correctamente cuando el atacante está estático y bajo la cobertura de un solo sensor durante el período completo del ataque.

Liu, Jin, & Wang (2010), proponen un trabajo llamado Survey on Security Scheme and Attacking Methods of WPA/WPA2 en Chengdu, China. a medida que se descubre la falla de seguridad crítica de WEP, la preocupación de los investigadores se ve cada vez más atraída por el esquema de WPA / WPA2 que incluye 802.1X, protocolo de autenticación y algoritmos de encriptación TKIP y CCMP. En este documento, se proporciona una descripción general de WPA / WPA2. Y luego, se introducen las vulnerabilidades de WPA / WPA2 y las

investigaciones actuales en el método de atacar WPA / WPA2, los cuales son Ataque de fuerza bruta, Ataque de fuerza bruta TMTO, Ataque de fuerza bruta usando GPU, Ataque de función de mezcla de teclas TKIP, Ataque de TKIP Beck & Tews, Ataque CCMP TMTO, entre otros. En el estudio, ellos sugieren que arreglar TKIP o cambiar a CCMP es una opción actual. También se concluye que, a la hora de diseñar un protocolo de seguridad, la seguridad debe tenerse en cuenta desde el principio.

Choi, Chang, Ko, & Hu (2011), proponen un trabajo denominado Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots en Kyoto, Japón. Los puntos de acceso inalámbricos se dividen en gran medida en tres categorías: redes domésticas y de pequeñas empresas, redes empresariales y puntos de acceso. El acceso protegido Wi-Fi (WPA) proporciona soluciones para el hogar, las pequeñas empresas y las redes empresariales, pero los puntos de acceso generalmente no están protegidos en la capa de control de acceso medio (MAC) porque están abiertos al público. En este artículo, se presenta un esquema que establece una conexión inalámbrica segura entre un dispositivo cliente y un punto de acceso en estos entornos abiertos, usando criptografía jerárquica basada en identidad, y cada usuario usa su dirección MAC como clave pública. Este esquema no depende del modo de clave precompartida WPA y proporciona una mejor seguridad, especialmente contra la vulnerabilidad Hole196 que se describe en el documento, en el sentido de que cada cliente se conecta a un punto de acceso virtual único. Además, no está restringido al problema de seguridad de WPAPSK y RC4 en el que WPA todavía se basa. Además, que puede detectar puntos de acceso no autorizados y es resistente a ciertos tipos de ataques de denegación de servicio. Incluso si un atacante falsifica la dirección MAC del punto de acceso o dispositivo cliente o transmite uno de los mensajes de protocolo, no aprende la clave compartida (kA, C) porque no conoce la clave privada del punto de acceso (dA). En consecuencia, el atacante no puede escuchar a escondidas ni modificar los mensajes que se transmiten dentro de una conexión segura establecida mediante nuestro esquema. La integración del esquema dentro de 802.11i se deja como trabajo futuro.

Choi, Chang, Ko, & Hu (2018), realizaron una investigación denominada Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments, en Praga, República Checa. El protocolo de autenticación extensible basado en túneles se ha vuelto fundamental para el control de acceso a redes inalámbricas. Proporciona autenticación, privacidad y autorización para el acceso a la red empresarial protegido por el marco de seguridad WPA / WPA2. WPA2 se considera el estándar más reciente y seguro para la comunicación inalámbrica, especialmente para redes Wi-Fi. Sin embargo, WPA / WPA2-PSK se han visto amenazados últimamente por versiones avanzadas de ataques inalámbricos. En este artículo, se estudian WPA / WPA2: autenticación empresarial con métodos comunes de EAP (Extensible Authentication Protocol) basados en túneles, centrándonos en sus puntos fuertes y débiles y en el impacto de los recientes ataques WPA / WPA2. Este documento evalúa el rendimiento y la resistencia a las amenazas de WPA2 empresarial utilizando EAP basado en túneles, que se considera la pila de protocolos más segura para las redes inalámbricas empresariales. Se estudiaron los métodos EAP habituales de autenticación basados en túneles. A esto le siguió una evaluación práctica en términos de desempeño. Se estudió el impacto de WPA2 empresarial reciente en estos protocolos de autenticación. Se propusieron mitigación y enmiendas recomendadas para resolver los agujeros detectados. Finalmente se presentan los ataques inalámbricos que amenazan el futuro de las comunicaciones inalámbricas. Esto anima a la sociedad de la comunicación a trabajar por un nuevo estándar de protección que proteja de forma nativa la transmisión de datos sensibles. La nueva pila de protocolos seguros para proteger la próxima generación de comunicaciones inalámbricas debe incluir varias modificaciones, como se describe en la sección de recomendaciones, para resistir las técnicas de ataque recientes que amenazan la autenticación, la confidencialidad y la disponibilidad inalámbricas.

1.3. Teorías relacionadas al tema.

¿Qué es seguridad informática?

El significado del término seguridad informática ha evolucionado en los últimos años. Antes de que el problema de la seguridad de los datos se difundiera ampliamente en los medios de comunicación, la idea de la seguridad informática de la mayoría de la gente se centraba en la máquina física. Tradicionalmente, las instalaciones informáticas se han protegido físicamente por tres razones: Para evitar el robo o daño del hardware, evitar el robo o daño de la información, evitar la interrupción del servicio (Avenía Delgado, 2017).

La seguridad informática es el nombre de las medidas de seguridad que se toman para evitar o reducir cualquier interrupción de un ataque a datos, computadoras o dispositivos móviles y cubre no solo salvaguardar la confidencialidad y la privacidad, sino también la disponibilidad e integridad de los datos, los cuales son vitales para la calidad y seguridad de la atención. Las brechas de seguridad pueden ocurrir cuando usamos registros en papel, enviamos información usando máquinas de fax e incluso verbalmente. Sin embargo, las consecuencias de las brechas de seguridad con la información digital son potencialmente mucho más graves, ya que la información se puede distribuir más fácilmente y a una audiencia mucho más amplia (Care Provider Alliance, 2017).

Seguridad informática implica estar protegido por sistemas que se conectan a Internet, entre los que se encuentran hardware, software y datos, contra ataques cibernéticos. En un ámbito informático, la seguridad abarca tanto a la seguridad cibernética y la seguridad física, ambas usadas por empresas para protegerse contra el acceso sin autorización al centro de datos y otros sistemas informáticos (Seemma , Nandhini, & Sowmiya, 2018).

Figura 3: Comparación de los principales desafíos de seguridad de red y privacidad de la información que enfrentan las organizaciones en 2016 con los de 2015 Fuente: (Eian, Lim, Yeap, Yeo, & Zahra, 2020)

Redes inalámbricas

Las redes inalámbricas son redes que utilizan ondas de radio para conectar los dispositivos, sin la necesidad de utilizar cables de ningún tipo.

Los dispositivos que usan redes inalámbricas son los ordenadores ya sean portátiles o de escritorio, asistentes digitales personales o PDA, teléfonos móviles, tablets y dispositivos localizadores. Las redes inalámbricas o WLAN funcionan de manera muy parecida a las redes cableadas o LAN, con la diferencia de que las primeras deben convertir las señales de información en una forma adecuada para la transmisión a través del aire. Las redes inalámbricas se utilizan en sustitución a las redes cableadas o para proporcionar acceso a datos corporativos desde ubicaciones remotas en empresas o instituciones. La infraestructura en WLAN puede ser construida a muy bajo coste en comparación con las alternativas cableadas tradicionales. Pero el ahorro de dinero justifica muy parcialmente la construcción de redes inalámbricas. Si a la gente de una comunidad local se le proporciona un acceso más barato y más fácil a la información, se beneficiarán directamente de lo que Internet tiene para ofrecer. El tiempo y el esfuerzo ahorrado al tener acceso a la red mundial de información se traduce en riqueza a escala local, ya que se puede hacer más trabajo

en menos tiempo y con menos esfuerzo. Las redes inalámbricas permiten a los dispositivos remotos que se conecten sin dificultad, independientemente que estos dispositivos estén a unos metros o a varios kilómetros de distancia. Todo ello sin necesidad de romper paredes para pasar cables o instalar conectores. Esto ha hecho que el uso de esta tecnología sea muy popular, extendiéndose muy rápidamente. Existen muchas tecnologías diferentes que difieren en la frecuencia de transmisión utilizada, la velocidad y el alcance de sus transmisiones. Por otro lado, hay algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos, pero son propensas a la interferencia. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y potencia de transmisión permitidos para cada tecnología. Además, las ondas electromagnéticas no se pueden confinar fácilmente a un área geográfica limitada. Por esta razón, un hacker puede escuchar fácilmente a una red si los datos transmitidos no están codificados. Por lo tanto, se deben tomar todas las medidas necesarias para garantizar la privacidad de los datos transmitidos a través de redes inalámbricas. (Salazar, 2016)

De acuerdo con la tabla 1 se señala las diferencias entre redes inalámbricas y cableadas:

Tabla 1.

Diferencias entre redes inalámbricas y cableadas.

Parámetros de comparación	WLAN	LAN
Significa	Wireless Local Area Network	Local Area Network
Tipo de conexión	Tecnologías inalámbricas	Incluye tecnologías inalámbricas y alámbricas.
Costo y seguridad	Costoso de instalar y menos seguro.	Menos costoso y más seguro.
Cobertura	Grandes regiones como oficinas,	Grandes áreas como edificios.

	edificios, estaciones, etc.	
Rendimiento	Alto rendimiento; rendimiento afectado por el mal tiempo.	Buen rendimiento y no se ve afectado por el clima.
Interferencia	Se puede interferir fácilmente.	No se puede interferir fácilmente.
Ejemplos	Computadoras de escritorio, portátiles, tabletas y móviles conectados a redes Wi-Fi o hotspots.	Computadora de escritorio y portátil conectados a LAN en un edificio u oficina.

Fuente: (Salazar, 2016).

SEGURIDAD EN REDES INALÁMBRICAS

Las redes inalámbricas se definen como redes que no están asociadas por alambres o cables de ningún tipo. La utilización de una red remota permite a las empresas mantener una forma económica de llevar la red a sus edificios sin la necesidad de instalar cables costosos y costosos. Las redes inalámbricas también aseguran una conexión entre varias áreas de equipos aplicando ondas de radio, que es una ejecución que ocurre en el grado físico de la estructura de la red, para asociar dispositivos personales como teléfonos móviles, computadoras portátiles, tabletas a Internet. No solo se conectan dispositivos personales a Internet, las redes inalámbricas se utilizan para conectar dispositivos a los sistemas comerciales y diversas aplicaciones. Por ejemplo, cuando un teléfono inteligente está conectado a la red Wi-Fi que se encuentra en lugares abiertos, la conexión se establece en la red inalámbrica de esa empresa en particular. Todas las redes inalámbricas tienen las características de autoasociación dinámica, autoconfiguración, implementación rápida, mantenimiento simple y bajo costo. Las redes inalámbricas se pueden clasificar en cuatro tipos según el área de aplicación y el alcance de la señal (Salazar, 2016):

1. Redes inalámbricas de área personal (Wireless Personal-Area Networks - WPAN)

2. Redes inalámbricas de área local (Wireless Local-Area Networks - WLAN)
3. Redes inalámbricas de área metropolitana (Wireless Metropolitan-Area Networks - WMAN)
4. Redes inalámbricas de área amplia (Wireless Wide-Area Networks - WWAN).

En la figura 4 nos brinda una visión de los tipos de redes inalámbricas:

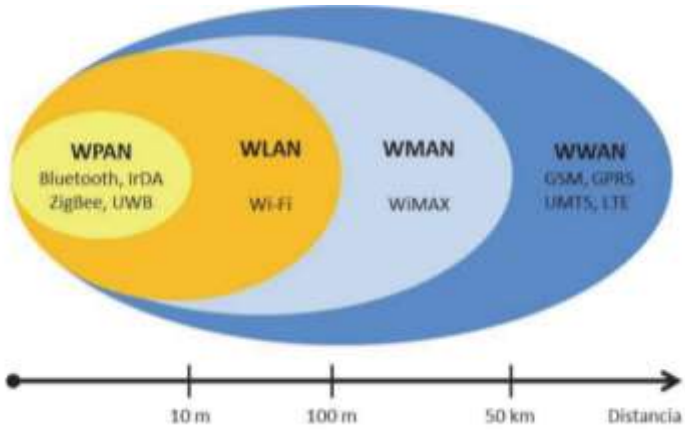


Figura 4: Tipos de redes inalámbricas. Fuente: (Salazar, 2016)

Aunque las redes inalámbricas parecen proporcionar más beneficios que desventajas, debido a su naturaleza inalámbrica, las redes inalámbricas no están protegidas por medios físicos y, en consecuencia, se exponen a innumerables ataques de seguridad. La era tradicional de las redes utiliza varias formas de proteger la red, como el uso de cerraduras y llaves, mano de obra como guardias de seguridad para buscar intrusos que intentan comprometer la red. Sin embargo, debido a la evolución de la tecnología, todos estos ya no son necesarios para proteger la red inalámbrica. De hecho, los usuarios ya no necesitan comprar dichos candados o llaves para asegurarse de que los atacantes de la red no toquen sus cables. Los usuarios pueden lograr la seguridad inalámbrica de muchas formas que no son costosas, a veces gratuitas para proteger la red inalámbrica. Por ejemplo, se puede instalar una simple red privada virtual gratuita en el dispositivo para garantizar una red segura en el dispositivo del usuario. No obstante, antes de configurar una red inalámbrica, los usuarios y las organizaciones deben aprender a pensar en las vulnerabilidades y

amenazas de las redes inalámbricas. Si estas amenazas no se manejan bien, un privilegio que puede parecer demasiado bueno para ser verdad puede convertirse en un horror de pérdida y abuso de información. (Eian, Lim, Yeap, Yeo, & Zahra, 2020)

La seguridad Wi-Fi es la protección de dispositivos y redes conectados en un entorno inalámbrico. Sin seguridad Wi-Fi, cualquier persona que utilice una computadora o dispositivo móvil dentro del area de la señal inalámbrica del router puede acceder fácilmente a un dispositivo de la misma red, como un punto de acceso inalámbrico o un enrutador.

¿Cuáles son algunas formas de proteger una red Wi-Fi?

Una de las mejores prácticas básicas para la seguridad de Wi-Fi es cambiar las contraseñas predeterminadas de los dispositivos de red.

La mayoría de los dispositivos cuentan con contraseñas de administrador predeterminadas, que están destinadas a facilitar la configuración de los dispositivos. Sin embargo, las contraseñas predeterminadas creadas por los fabricantes de dispositivos pueden ser fáciles de obtener en línea (CISCO, 2020).

Cambiar las contraseñas predeterminadas de los dispositivos de red por contraseñas más complejas, y cambiarlas con frecuencia, son formas simples pero efectivas de mejorar la seguridad de Wi-Fi. A continuación, en la tabla 2, se muestran otros métodos de seguridad de la red Wi-Fi:

Tabla 2.

Métodos de seguridad de la red Wi-Fi.

Direcciones de control de acceso a medios (MAC)	Otro enfoque básico para la seguridad de Wi-Fi es usar direcciones MAC, que restringen el acceso a una red Wi-Fi. (Una dirección MAC es un código o número único que se usa para identificar dispositivos individuales en una red). Si bien esta táctica proporciona una mayor medida de seguridad que una red abierta, aún es susceptible de ser atacada por adversarios que utilicen direcciones "falsificadas" o modificadas.
Cifrado	Un método más común para proteger redes y dispositivos Wi-Fi es el uso de protocolos de seguridad que utilizan cifrado. El cifrado en las comunicaciones digitales codifica los datos y luego los decodifica solo para los destinatarios autorizados. En la actualidad, se utilizan varios tipos de estándares de cifrado, incluido el acceso Wi-Fi protegido (WPA) y el acceso Wi-Fi 2 protegido (WPA2).
Redes privadas virtuales (VPN)	Las VPN son otra fuente de seguridad de la red Wi-Fi. Permiten a los usuarios crear túneles seguros con identidad protegida entre redes Wi-Fi desprotegidas e Internet. Una VPN puede cifrar la conexión a Internet de un usuario. También puede ocultar la dirección IP de un usuario mediante el uso de una dirección IP virtual que asigna al tráfico del usuario a medida que pasa por el servidor VPN.
Software de seguridad	Hay muchos tipos de software empresarial y de consumo que también pueden proporcionar seguridad Wi-Fi. Algún software de protección Wi-Fi se incluye con productos relacionados, como software antivirus.

Fuente: (CISCO, 2020)

Los estándares WLAN 802.11 especifican las dos capas más bajas del modelo de red OSI, que son las capas físicas y de enlace de datos. Los principales objetivos de IEEE para la creación de estos estándares fueron enfoques diferentes para la capa física, por ejemplo, diferentes frecuencias, diferentes métodos de codificación y comparten las mismas capas superiores. Lo han logrado y las capas de control de acceso a medios (MAC) de los protocolos 802.11a, b y g son considerablemente idénticas. Aún en la siguiente capa superior, todos los protocolos WLAN 802.11 especifican el uso del protocolo 802.2 para la porción de control de enlace lógico (LLC) de la capa de enlace de datos. Como puede ver en la figura suscrita, en el modelo de red OSI,

protocolos como TCP / IP, IPX, NetBEUI y AppleTalk, todavía existen en capas superiores. En las WLAN, la privacidad se logra mediante la protección del contenido de los datos con cifrado. El cifrado es opcional en las WLAN 802.11, pero sin él, cualquier otro dispositivo inalámbrico estándar puede leer todo el tráfico de la red.

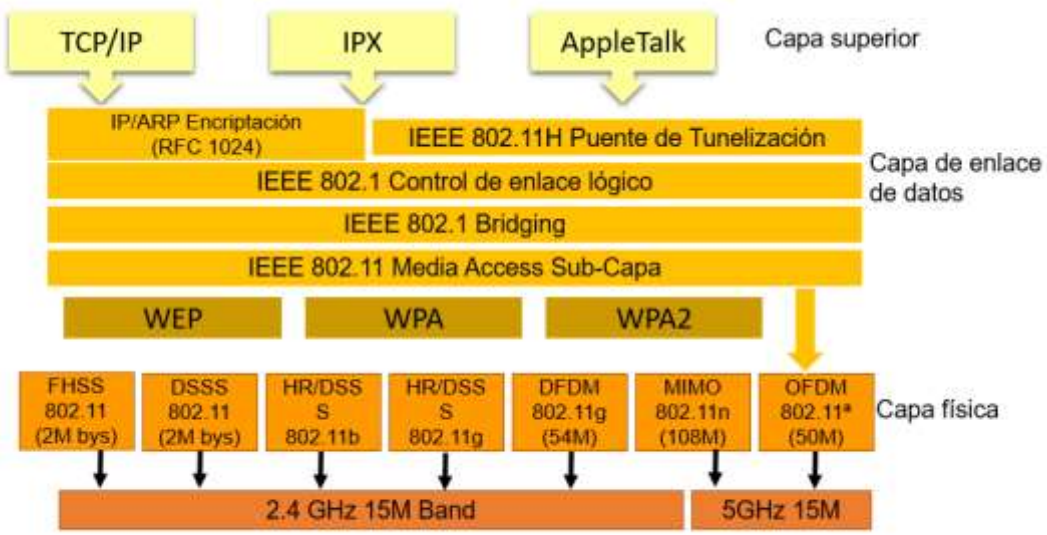


Figura 5: Protocolos y Modelo OSI. (Lashkari, Seyed Danesh, & Samadi, 2009)

Tipos de Protocolos

1. **Privacidad equivalente a cableado (Wired Equivalent Privacy) WEP**

   El protocolo WEP es equivalente a las redes cableadas, es un algoritmo de cifrado empleado en las redes WLAN desde 1999 con la idea de dar una confidencialidad similar a las conseguidas en las redes cableadas. WEP emplea claves de 10 o 26 dígitos hexadecimales para cifrar la información y ya resultó evidente al año siguiente de su introducción en el mercado informático que el algoritmo presentaba graves vulnerabilidades. En el año 2003 la Alianza WI-FI anunció la reprobación de dicho algoritmo. Dos años más tarde, un grupo del FBI mostró públicamente cómo romper una red WI-FI protegida con WEP en tan solo tres minutos con herramientas de código abierto (Brihuega, 2014).

WEP está destinado a brindar seguridad a la LAN cableada mediante encriptación, utilizando el algoritmo RC4 con diferentes lados de la correspondencia de información. WEP está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value). (Lehembre, 2006)
El mensaje encriptado C se determinaba utilizando la siguiente fórmula:
C = M || ICV(M)] + [RC4(K || IV)]

Donde || es un operador de concatenación y + es un operador XOR. Claramente, el vector de inicialización es la clave de la seguridad WEP, así que para mantener un nivel decente de seguridad y minimizar la difusión, el IV debe ser aplicado a cada paquete, para que los paquetes subsiguientes estén encriptados con claves diferentes.

En el lado del remitente:

WEP intenta utilizar cuatro operaciones para cifrar los datos (texto plano). Al principio, la clave secreta utilizada en el algoritmo WEP tiene una longitud de 40 bits con un vector de inicialización (IV) de 24 bits que se concatena para actuar como cifrado. / clave de descifrado.
En segundo lugar, la clave resultante actúa como semilla para un generador de números pseudoaleatorios (PRNG). En tercer lugar, el texto sin formato arroja un algoritmo de integridad y se vuelve a concatenar mediante el texto sin formato. En cuarto lugar, el resultado de la secuencia de teclas y el ICV irá al algoritmo RC4. Se crea un mensaje cifrado final adjuntando el IV delante del texto cifrado. (Reddy & Srikanth, 2019).

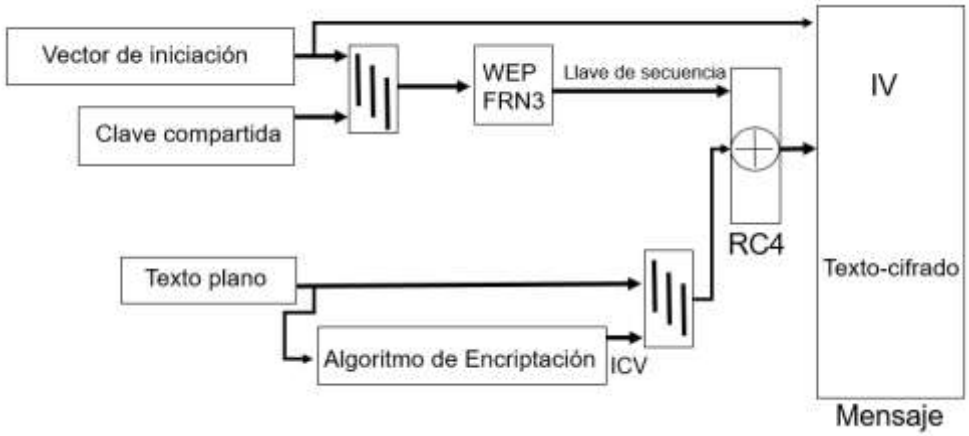


Figura 6: Encriptación WEP del lado del remitente. Fuente: (Lashkari, Seyed Danesh, & Samadi, 2009)

En el lado del destinatario:

WEP intenta utilizar cinco operaciones para descifrar el lado recibido (IV + texto cifrado). Al principio, la clave precompartida y el IV se concatenaron para hacer una clave secreta. En segundo lugar, el texto cifrado y la clave secreta van al algoritmo CR4 y, como resultado, aparece un texto sin formato. En tercer lugar, el ICV y el texto sin formato se separarán. En cuarto lugar, el texto sin formato va al algoritmo de integridad para hacer un nuevo ICV (ICV ') y finalmente el nuevo ICV (ICV') se compara con el ICV original. (Khasawneh, Kajman, Alkhudaidy, & Althubyani, 2014)

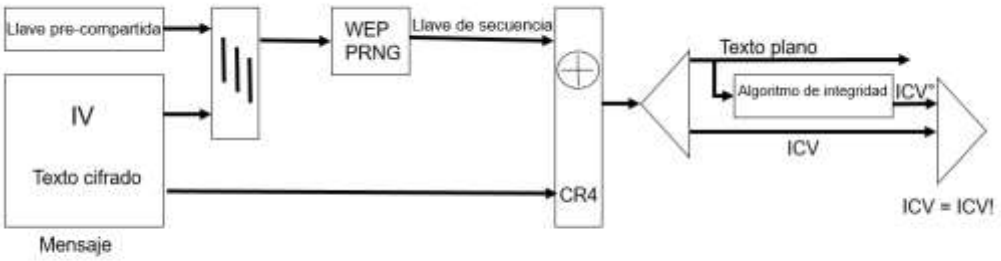


Figura 7: Encriptación WEP del lado del destinatario. Fuente: (Lashkari, Seyed Danesh, & Samadi, 2009)

Debilidad de WEP:

- WEP no anticipa la fabricación de paquetes.
- WEP no anticipa ataques de repetición. Básicamente, un atacante puede grabar y reproducir paquetes como desee y serán reconocidos como auténticos.
- WEP emplea RC4 de manera inapropiada. Las claves utilizadas son frágiles y pueden ser forzadas en PC estándar en horas o minutos, utilizando programas accesibles disponibles.
- WEP reutiliza vectores de inicialización. Una variedad de técnicas criptoanalíticas accesibles que pueden decodificar información sin obtener la clave de cifrado.
- Sin detección, WEP permite que un atacante cambie la información sin obtener la clave de cifrado.
- La administración de claves es insuficiente y la actualización es deficiente.
- El problema en el algoritmo RC-4.
- Producción sencilla de mensajes de autenticación.
- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.
- Los IVs son demasiado cortos (24 bits – hacen falta menos de 5000 paquetes para tener un 50% de posibilidades de dar con la clave) y se permite la reutilización de IV (no hay protección contra la repetición de mensajes).
- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad)

2. Acceso Wi-Fi protegido (Wi-Fi Protected Access) WPA

El protocolo WPA está diseñado para vencer todas aquellas vulnerabilidades encontradas en el protocolo WEP, WPA desarrollo la implementación de un protocolo de integridad de la clave temporal(Tklp), que se basa en modificar

las claves cuando se hace uso del sistema, además, este protocolo mejora la integridad de la información cifrada.

Fue presentado por Wi-Fi Alliance a finales de 2002. Wi-Fi Alliance with Electronics Engineers (IEEE) aseguró las secciones débiles del protocolo WEP recientemente revelado y presentó WPA como una interpretación. Se ha hecho compatible con todos los proveedores y equipos existentes. La principal preocupación es vencer las deficiencias de WEP sin el cambio de equipo. Esto se terminó con la inclusión del Protocolo de integridad de clave temporal (TKIP) para el cifrado y el EAP 802.1X con fines de autenticación para ofrecer una alta seguridad. Para evitar la fabricación de información (cambio de bits), WPA presentó el cálculo de verificación de integridad de mensajes (MIC) conocido como "Michael".

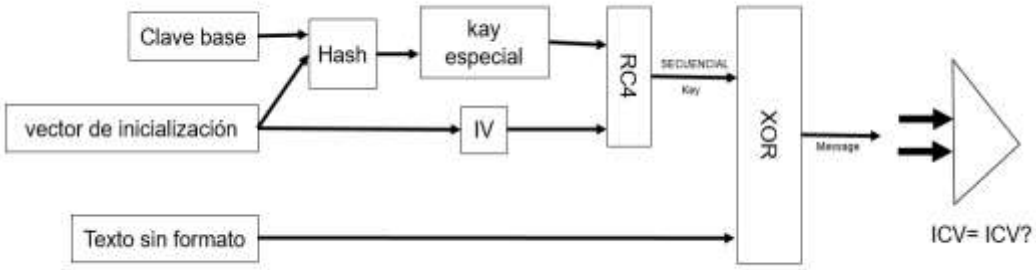


Figura 8: Algoritmo de cifrado WPA (TKIP). Fuente: (Reddy & Srikanth, 2019)

El WPA vino con el propósito de solucionar los problemas en el método de criptografía WEP, sin que los usuarios necesiten cambiar el hardware. El estándar WPA similar a WEP especifica dos formas de operación:

1. WPA personal o WPA-PSK (clave precompartida) que se utiliza para la autenticación de uso doméstico en oficinas pequeñas y en el hogar que no utiliza un servidor de autenticación y la clave de criptografía de datos puede llegar hasta 256 bits. A diferencia de WEP, esta puede ser cualquier cadena alfanumérica y se usa solo para negociar la sesión inicial con el AP. Debido a que tanto el cliente como el AP ya poseen esta clave, WPA proporciona autenticación mutua y la clave nunca se transmite por aire.

2. Enterprise WPA o Comercial que la autenticación se realiza mediante un servidor de autenticación 802.1x, generando un excelente control y seguridad en el tráfico de usuarios de la red inalámbrica. Este WPA usa 802.1X + EAP para la autenticación, pero nuevamente reemplaza WEP con el cifrado TKIP más avanzado. Aquí no se utiliza ninguna clave previamente compartida, pero necesitará un servidor RADIUS. Y obtiene todos los demás beneficios que ofrece 802.1X + EAP, incluida la integración con el proceso de inicio de sesión de Windows y la compatibilidad con los métodos de autenticación EAP-TLS y PEAP.

La razón principal por la que se genera WPA después de WEP es que el WPA permite un cifrado de datos más complejo en el protocolo TKIP (Protocolo de integridad de clave temporal) y también asistido por MIC (Comprobación de integridad de mensajes), cuya función es evitar ataques de tipo bit-flipping que se aplica fácilmente a WEP mediante el uso de una técnica de hash. (Lashkari, Seyed Danesh, & Samadi, 2009)

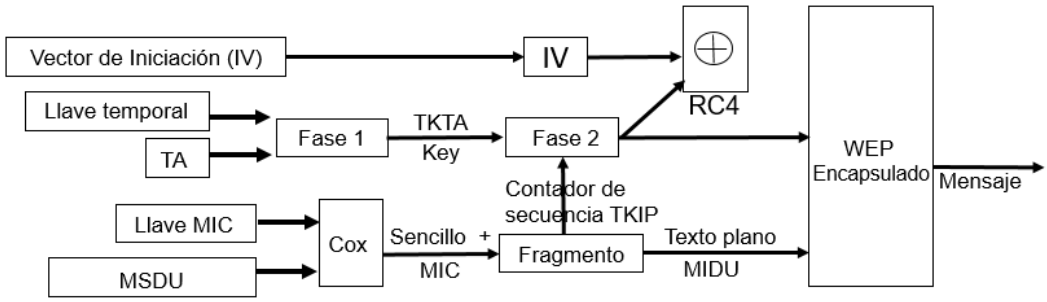


Figura 9: Algoritmo de encriptación WPA (TKIP). Fuente: (Lashkari, Seyed Danesh, & Samadi, 2009)

TKIP usa la misma Técnica RC4 de WEP, pero haciendo un hash antes del aumento del algoritmo RC4. Se realiza una duplicación del vector de inicialización. Una copia se envía al siguiente paso y la otra se mezcla con la clave base.

Luego de realizar el hash, el resultado genera la clave del paquete que va a unir la primera copia del vector de inicialización, ocurriendo el incremento del algoritmo RC4. Después de eso, está la generación de una clave secuencial con un XOR a partir del texto que desea criptografiar, generando luego el

texto criptográfico. Finalmente, el mensaje está listo para enviarse. El cifrado y el descifrado se realizarán invirtiendo el proceso. (Lashkari, Seyed Danesh, & Samadi, 2009)

MIC o Michael: Michael es el nombre del código de integridad del mensaje TKIP. Es un MIC completamente nuevo diseñado que tiene una longitud de 64 bits y se representa como dos palabras littleEndian de 32 bits (K0, K1). La función de Michael primero rellena un mensaje con el valor hexadecimal 0x5a y suficiente relleno cero para llevar la longitud total del mensaje a un múltiplo de 32 bits, luego divide el resultado en una secuencia de palabras de 32 bits M1, M2 ... Mn, y finalmente calcula la etiqueta a partir de la clave y las palabras del mensaje utilizando una estructura iterativa simple:

$(L, R) \leftarrow (K_0, K_1)$

hacer i de 1 a n

$L \leftarrow L \ XOR \ M_i$

$(L, R) \leftarrow Swap(L, R)$

Return (L, R) as the tag

El predicado de verificación de Michael vuelve a ejecutar la función de etiquetado sobre el mensaje y devuelve el resultado de una comparación de bits de esta etiqueta calculada localmente y la etiqueta recibida con el mensaje.

El nivel de seguridad de un MIC generalmente se mide en bits. Si el nivel de seguridad de un MIC es de s bits, entonces, por definición, el tiempo requerido para que un atacante construya una falsificación es, en promedio, después de aproximadamente 2^{-x+1} paquetes.

Nueva disciplina de secuenciación IV para derrotar repetida: Una falsificación que un MIC no puede detectar es un paquete reproducido. Esto ocurre cuando un adversario registra un paquete válido en vuelo y luego lo retransmite. Para vencer las repeticiones, TKIP reutiliza el campo WEP IV como número de secuencia del paquete. Tanto el transmisor como el receptor inicializan el espacio de secuencia de paquetes a cero cada vez que se establecen nuevas claves TKIP, y el transmisor incrementa el número de

secuencia con cada paquete que envía. TKIP requiere que el receptor aplique la secuenciación IV adecuada de los paquetes que llegan. TKIP define un paquete como fuera de secuencia si su IV es igual o más pequeño que un MPDU recibido correctamente anterior asociado con la misma clave de cifrado. Si una MPDU llega fuera de servicio, se considera que es una repetición y el receptor la descarta e incrementa un contador de repetición.

Key mixing:

WEP construye una clave RC4 por paquete concatenando una clave base y el paquete IV. La nueva clave por paquete que se llama la función de mezcla de claves TKIP sustituye una clave temporal por la clave base WEP y construye la clave WEP por paquete de una manera novedosa. Las claves temporales se denominan así porque tienen una vida útil fija y se reemplazan con frecuencia.

La función de mezcla opera en dos fases:

• La fase 1 elimina el uso de la misma clave por parte de todos los enlaces:

• La fase 2 descorrelaciona el IV público de la clave por paquete conocida:

Recuperar o derrotar ataques de colisión de claves:

El cambio de claves entrega las claves nuevas consumidas por los diversos algoritmos TKIP. Generalmente hay tres tipos de claves: claves temporales, claves de cifrado y claves maestras.

Ocupando el nivel más bajo de la jerarquía están las claves temporales consumidas por los algoritmos de autenticación y privacidad de TKIP propiamente dichos. TKIP emplea un par de tipos de claves temporales: una clave de cifrado de 128 bits y una segunda clave de 64 bits para la integridad de los datos. TKIP utiliza un par de claves temporales independientes en cada dirección de una asociación. Por tanto, cada asociación tiene dos pares de claves, para un total de cuatro claves temporales. TKIP identifica este conjunto de claves mediante un identificador de dos bits llamado ID de clave WEP. Ahora se puede dibujar una nueva figura del proceso TKIP con detalles de estas cuatro partes como en la siguiente imagen:

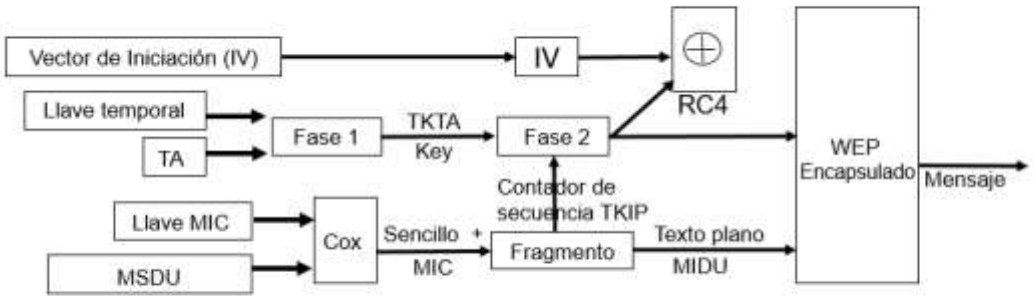


Figura 10: Detalle del algoritmo de encriptación TKIP. Fuente: (Lashkari, Seyed Danesh, & Samadi, 2009)

Mejoras WPA:

- Código de integridad del mensaje criptográfico para superar las reproducciones.
- Nuevo sistema de secuenciación IV para derrotar ataques de repetición.
- Capacidad de mezcla de claves por paquete, para decorar los IVs públicos de claves débiles.
- Cambiar la clave o derrotar a los ataques de colisión de claves.

Debilidades de WPA:

En noviembre de 2003, Robert Moskowitz publicó "Debilidad en la elección de la frase de contraseña en la interfaz WPA". En este artículo explica una fórmula que revelaría la frase de contraseña realizando un ataque de diccionario contra redes WPA-PSK, y para confirmación, a finales de 2004, Takehiro Takahashi, entonces estudiante de Georgia Tech, liberó a WPA Cracker y Josh Wright, un ingeniero de redes y conocido profesor de seguridad, liberó cowpatty casi al mismo tiempo. Ambas herramientas están escritas para sistemas Linux y realizan un ataque de diccionario de fuerza bruta contra redes WPA-PSK en un intento de determinar la frase de contraseña compartida. Ambos requieren que el usuario proporcione un

archivo de diccionario y un archivo de volcado que contenga el protocolo de enlace de cuatro vías WPA-PSK.

3. Acceso Wi-Fi protegido 2 (Wi-Fi Protected Access 2) WPA2

En 2004, la ratificación de WPA2 es ampliamente conocida como la segunda generación de WPA y es reconocido como el protocolo más seguro utilizado en redes inalámbricas. Este protocolo utiliza la implementación del algoritmo de cifrado de bloques del Estándar de cifrado avanzado (AES) de 128 bits para los procesos de autenticación y cifrado. En WPA2 hay dos modos de autenticación que pueden usarse, que son Pre-Shared Key y Enterprise. En lugar de TKIP, WPA2 utiliza una clave transitoria por pares (PTK) para la generación de claves. En lugar de utilizar el algoritmo de Michael, WPA2 utiliza CCMP (Protocolo CBC MAC en modo contador) que aplica el algoritmo del estándar de cifrado avanzado (AES) de cifrado en bloque. Para garantizar la integridad y proporcionar una autenticación precisa, se ha utilizado CCM (CBC-MAC) en WPA2 (Khasawneh, Kajman, Alkhudaidy, & Althubyani, 2014).

Hay dos modos de autenticación en WPA2. WPA2 Personal, o el modo WPA2-PSK (clave pre-compartida), está diseñado para redes domésticas o de oficinas pequeñas con un solo punto de acceso (AP). El cliente y AP se autentican entre sí mediante PSK y prueban la posesión de PSK, sin intercambiarlo. WPA2-Enterprise, denominado modo WPA2-802.1X, está diseñado para redes empresariales con múltiples AP. Requiere un servidor central de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) y se pueden utilizar varios tipos de protocolos de autenticación extensibles (EAP) para la autenticación.

En el modo WPA2-Personal, el cliente y el AP comparten un PSK estático. Desde PSK, se calcula una clave maestra por pares (PMK) utilizando la función de derivación de clave PBKDF2 de la siguiente manera, PMK =

PBKDF2(HmacSha1, PSK, SSID), y luego sigue un protocolo de enlace de 4 vías.

En el modo WPA2-Enterprise, el cliente es autenticado por un servidor RADIUS central usando varios protocolos de autenticación extensible (EAP) y luego el servidor RADIUS genera PMK y lo distribuye de forma segura al cliente y AP. Después de eso, sigue un apretón de manos de 4 vías entre el cliente y AP.

Cada versión tiene dos modos de operación, que son clave precompartida (PSK) y modos de empresa. En el modo PSK, el punto de acceso (AP) autentica una estación (STA) basándose en una contraseña compartida de antemano. Por otro lado, el modo de empresa, AP y STA se autentica mutuamente con la ayuda de un servidor de autenticación. Estas dos versiones comparten una etapa común de configuración inicial de tres fases. Las tres fases que se ilustran en la Figura subyacente son 1) descubrimiento, 2) autenticación y 3) administración de claves. La primera fase de descubrimiento tiene tres intercambios de mensajes. La STA se asocia con el AP anunciando capacidades de seguridad y negociando conjuntos de cifrado.

En la segunda fase de autenticación, STA y AP acuerdan la clave maestra (MK) y derivan la clave maestra por pares (PMK) basada en MK. El MK se deriva de la contraseña previamente compartida en el modo PSK o se genera por el AS y se entrega de forma segura al AP y STA, respectivamente, utilizando RADIUS y 802.1X en el modo empresarial.

Una vez que STA y AP comparten el PMK, estas dos partes pasan a la fase de administración de claves. Ambas partes obtienen la clave temporal por pares (PTK) y confirman la posesión del mismo PTK mediante el protocolo de enlace de cuatro vías. La PTK es nueva en cada asociación, ya que se deriva de la PMK y dos números aleatorios, respectivamente, elegido por cada partido para una sola asociación.

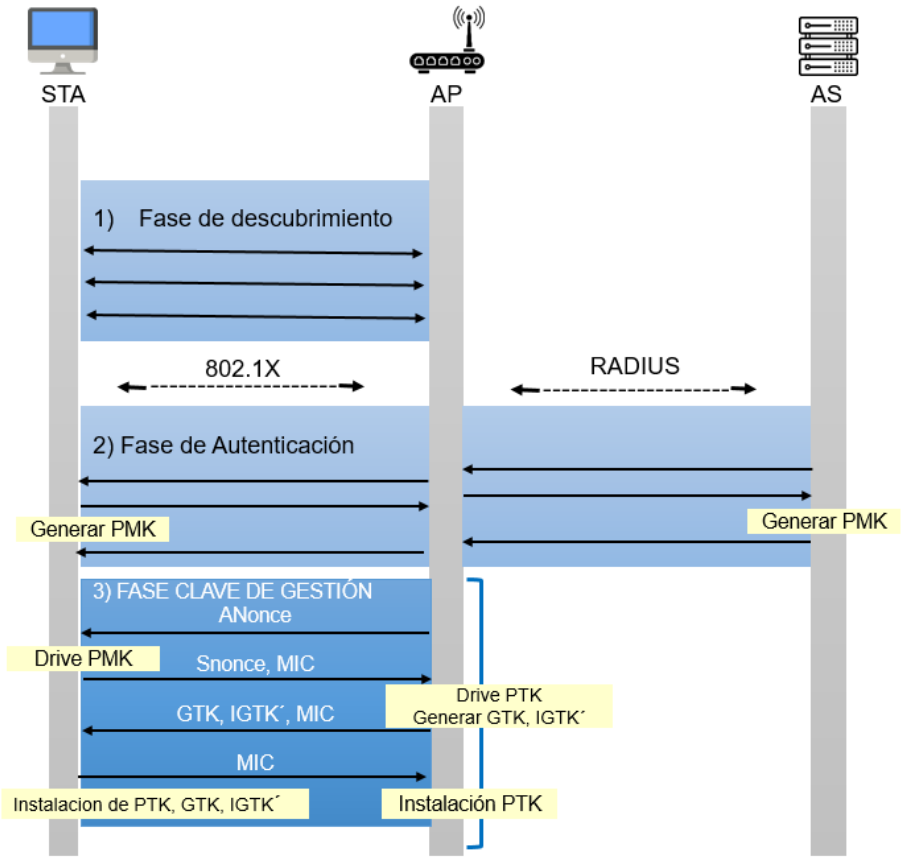


Figura 11: Tres fases en el modo WPA2-Enterprise. El handshake de cuatro vías es parte de la fase de gestión de claves. IGTK en el tercer mensaje del protocolo de enlace de cuatro vías es opcional para el PMF. Fuente: (Kwon & Choi, 2020)

Vulnerabilidades de WPA2:

- Reinstalación de la clave de cifrado por pares (PTK-TK), clave de grupo (GTK), clave de grupo de integridad (IGTK) en el protocolo de enlace de cuatro vías.
- Reinstalación de la clave de grupo (GTK), clave de grupo de integridad (IGTK) en el protocolo de enlace de la clave de grupo.
- Permitir una Solicitud de re-asociación de Transición rápida BSS (FT) retransmitida y reinstalar la Clave de cifrado por pares (PTK-TK) mientras se maneja.
- Reinstalación de la clave STK en el protocolo de enlace de Peer Key y la configuración de enlace directo tunelizado (TDLS) Peer Key (TPK) en el protocolo de enlace TDLS.

- Reinstalación de la clave de grupo (GTK) y la clave de grupo de integridad (IGTK) mientras se maneja una trama de respuesta en modo de suspensión de administración de red inalámbrica (WNM).

Proceso de cifrado CCMP:

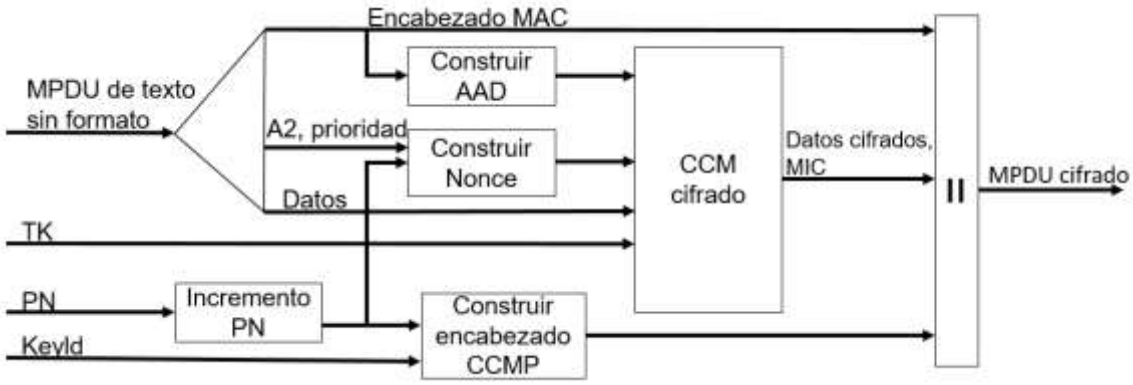


Figura 12: Proceso de cifrado CCMP. Fuente: (Reddy & Srikanth, 2019)

4. Acceso Wi-Fi protegido 3 (Wi-Fi Protected Access 3) WPA3

WPA3, lanzado en 2018, proporciona varias mejoras de seguridad sobre WPA2. La conexión WPA2-Open utiliza comunicaciones de texto sin formato. Para proporcionar seguridad en las comunicaciones y privacidad del usuario incluso en una conexión abierta, WPA3-Open proporciona encriptación individualizada utilizando encriptación inalámbrica oportunista (OWE), el cliente y el AP ejecutan un intercambio de claves Diffie-Hellman no autenticado para crear una clave maestra (PMK) única y luego sigue un protocolo de enlace de 4 vías para derivar PTK de la PMK. Por lo tanto, WPA3-Open proporciona seguridad en las comunicaciones.

WPA3-Personal:

Los cambios más significativos se están realizando dentro de WPA3-Personal, que se centra en una autenticación basada en contraseñas más resistente, incluso cuando los usuarios eligen contraseñas que no cumplen con las recomendaciones de complejidad típicas. WPA3 reemplaza a PSK con la autenticación simultánea de iguales (SAE) de la especificación IEEE 802.11, un protocolo seguro de establecimiento de claves entre dispositivos,

para brindar mayor protección a los usuarios contra intentos de adivinación de contraseñas por parte de terceros.

WPA3-Enterprise:

Proporciona seguridad superior para redes de datos confidenciales con el equivalente a una potencia criptográfica de 192 bits, útil en industrias como el gobierno, la atención médica o las finanzas. El paquete de seguridad de 192 bits garantiza que se implemente una combinación uniforme de herramientas criptográficas en las redes WPA3.

Autenticación del servidor en WPA3 Enterprise

WPA3 Enterprise prohíbe las opciones de configuración del solicitante como "omitir la validación del certificado" o "aceptar cualquier certificado". WPA3 Enterprise dicta que, si el solicitante no puede verificar la identidad del servidor durante la Fase 1, el solicitante no puede ingresar a la Fase 2 automáticamente; el solicitante puede ingresar a la Fase 2 solo si el usuario acepta explícitamente la confianza en el certificado proporcionado por el AS, por ejemplo, mediante una ventana de diálogo. Este mecanismo interactivo se denomina Anulación del usuario del certificado del servidor (UOSC).

La unión Wi-Fi impulsó a WPA3, el estándar de seguridad remota de vanguardia que puede eliminar cualquier indefensión actual. Los aspectos más destacados de WPA3 son Protección contra ataques de fuerza bruta, Secreto de WPA3, Protección de redes abiertas / públicas. WPA3 utiliza el protocolo de enlace SAE (Autenticación simultánea de iguales) para ofrecer Forward Secrecy, que evita que el infractor decodifique el tráfico detectado antiguo. Proporciona al cifrado de datos individualizado un componente que codifica el tráfico remoto para aliviar el peligro de ataques de intermediarios. Proporciona cifrado de 192 bits para asociaciones Wi-Fi, a continuación, se muestra en la figura 13 el protocolo de enlace SAE.

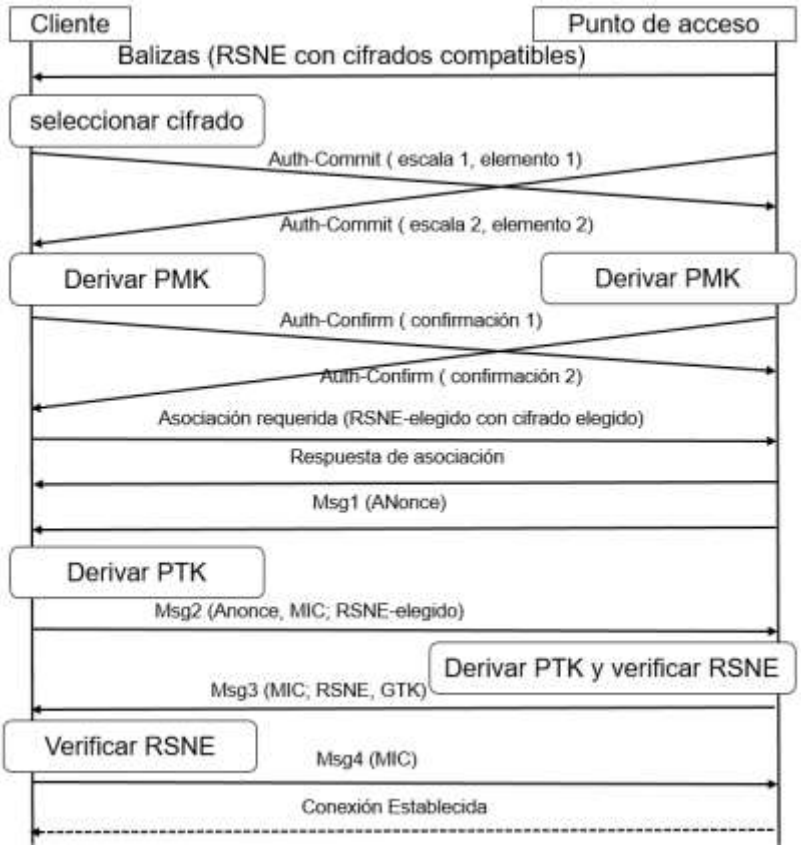


Figura 13: Protocolo de enlace SAE. Fuente: (Reddy & Srikanth, 2019)

CARACTERÍSTICAS EN WPA3

A. Dragonfly, una defensa contra el ataque de adivinación de contraseñas sin conexión

Una clave de sesión en WPA2 se calcula a partir de una contraseña previamente compartida y algunos valores conocidos públicamente. En otras palabras, puede espiar las sesiones de cualquier otro STA si se conoce la contraseña previamente compartida. El espionaje se vuelve bastante fácil en cafés o restaurantes donde las contraseñas están disponibles públicamente. Incluso si la contraseña aún no es información pública, un adversario aún puede adivinar una contraseña candidata y verificar su contraseña adivinada. Esta verificación

es posible porque está disponible un valor hash calculado a partir de la contraseña verdadera durante el apretón de manos de cuatro vías. WPA2 produce una clave secreta de 384 bits llamada PTK. Los primeros 128 bits del PTK se utilizan como clave para generar valores hash seguros. El valor hash da una garantía de la posesión de PTK de uno al otro. La suposición es correcta si el valor hash calculado a partir de la suposición coincide con el valor hash objetivo. Además, el adversario puede acelerar una verificación completa procesándola fuera de línea. Peor aún, el adversario puede extrapolar las claves secretas futuras de una víctima basándose en el compromiso actual. Las claves secretas en el modo personal WPA2 están sujetos a un ataque de adivinación fuera de línea debido a la exposición del valor hash calculado directamente con la contraseña.

La defensa de WPA3 contra el ataque de adivinanzas fuera de línea es no exponer ningún derivado de la contraseña previamente compartida. La contraseña precompartida se transforma en generador mediante la función conocida como se muestra en la Figura posteriormente señalada. El STA y el AP intercambian números aleatorios R_1 y R_2, respectivamente, después asegurándolos en R·G. La clave secreta K se calcula como $R_2 \cdot R_1 \cdot G$. Ambas partes confirman que tienen la misma clave secreta comparando el valor hash de la clave secreta. Estos intercambios adicionales de cuatro mensajes se conocen como el apretón de manos de Dragonfly. Tenga en cuenta que la variante Dragonfly utilizada en WPA3 también se conoce como autenticación simultánea de iguales (SAE). El ataque de adivinación fuera de línea no es aplicable en WPA3-SAE porque no se puede calcular una clave secreta a partir de la adivinación de la contraseña sin conocer dos valores aleatorios. Incluso si la contraseña es información pública, comprometer la clave secreta es bastante difícil debido al desconocimiento de valores aleatorios.

Imagine que se puede encontrar una clave secreta a partir del valor hash con ataques de fuerza bruta. Este hallazgo no ayuda a los compromisos de claves secretas para sesiones futuras, ya que una clave secreta se deriva de valores únicos independientes en cada sesión. En este sentido, se considera que el apretón de manos de Dragonfly satisface el PFS.

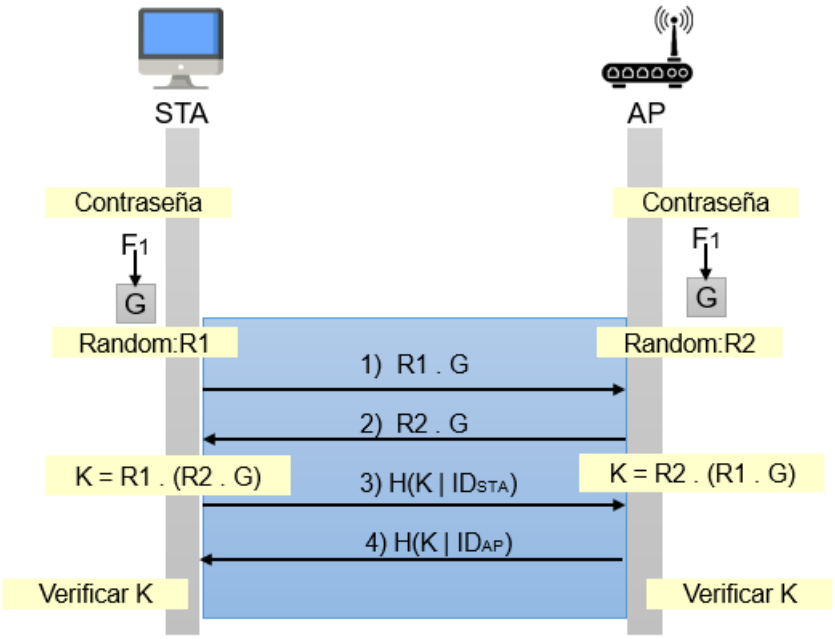


Figura 14: Protocolo Dragonfly resistente al ataque de adivinanzas fuera de línea. El protocolo satisface el secreto directo perfecto. Fuente: (Kwon & Choi, 2020)

B. Redes Wi-Fi abiertas mejoradas

Los administradores de red a menudo se enfrentan a situaciones en las que compartir secretos por adelantado no es asequible. Si este es el caso, las redes Wi-Fi abiertas en WPA2 es una opción. Este modo de operación prescinde de cualquier cifrado o autenticación que exponga a los usuarios de la red a cualquier amenaza de seguridad. Una resolución abordada en el WPA3 es la disposición de la confidencialidad del mensaje basada en una clave secreta efímera. Este nuevo enfoque se denomina red Wi-Fi abierta mejorada, también se denomina cifrado inalámbrico oportunista (OWE).

Como se muestra en la Figura 15, la apertura mejorada se superpone a la fase de autenticación, donde dos mensajes llevan claves públicas de STA y AP. Con base en estas claves públicas, utilizando el algoritmo Elliptic Curve Diffie-Hellman (ECDH), ambas partes derivan una clave secreta efímera que se convierte en PMK. El apretón de manos de cuatro vías inmediatamente continúa para configurar claves secretas para una sesión entrante. La STA y el AP pueden decidir almacenar en caché el PMK durante un período para

evitar costosos cálculos de ECDH para una posible reasociación en un futuro próximo.

Por motivos de confidencialidad, la red abierta mejorada requiere el método de cifrado AES CCMP con una clave de 128 bits y no permite ningún método antiguo y roto como TKIP o incluso WEP. Un PSK compartido pero inseguro puede dar lugar a la divulgación de información a otros usuarios, mientras que OWE es resistente a tales amenazas. Debido a su naturaleza de solo cifrado, OWE es más útil en una cafetería o en cualquier lugar donde sea necesario el cifrado, pero la autenticación no lo es.

En consecuencia, OWE es vulnerable a los ataques man-in-the middle (MITM). Además, es vulnerable a los ataques de denegación de servicio (DoS) ya que un adversario puede enviar mensajes de desasociación o desautenticación en la fase de descubrimiento para interrumpir el protocolo de enlace.

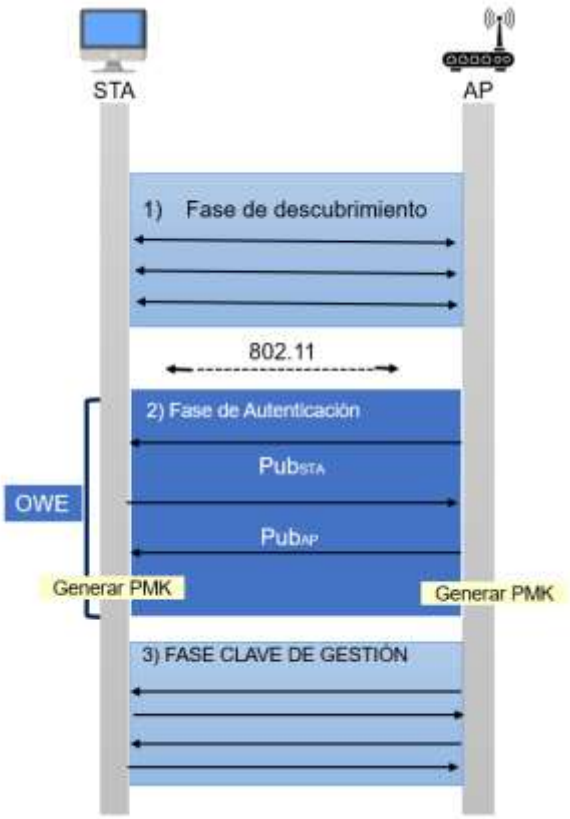


Figura 15: OWE superpuesto sobre la fase de autenticación genera una clave secreta efímera para la confidencialidad. Fuente: (Kwon & Choi, 2020)

C. Protocolo de aprovisionamiento de dispositivos

La configuración protegida Wi-Fi (WPS) es una función en WPA2 para una configuración conveniente e infalible para acceder a la red Wi-Fi. La función es más útil para los usuarios domésticos que saben poco sobre la seguridad de la red Wi-Fi o para dispositivos con interfaces de pantalla, limitadas o nulas para las entradas del usuario. El AP habilitado para WPS lleva un botón o un número de identificación personal (PIN) de ocho dígitos. El usuario de una STA simplemente presiona el botón o ingresa el PIN para establecer canales seguros. El WPS configura automáticamente el nombre de la red inalámbrica (SSID) y PMK. El WPS reemplaza la autenticación en el WPA asegurándose de que el STA esté cerca del AP y confirmando que el STA puede acceder a la información en el AP. Sin embargo, la seguridad de WPA se vio comprometida debido a un número PIN bastante corto y un mecanismo inseguro para la generación de claves.

El protocolo de aprovisionamiento de dispositivos (DPP) es un protocolo de autenticación en WPA3 para mejorar la comodidad y la seguridad sobre WPS. El DPP se compone de ocho mensajes en cuatro fases como se muestra en la Figura 16. No tiene autoridades centrales para coordinar un procedimiento completo. Más bien, el aprovisionamiento en el DPP permite que un relé confiable arranque dispositivos no autenticados al ganar confianza en las claves públicas de un dispositivo a través de canales fuera de banda (OOB) (Bootstrapping en la Figura 16). El relé vincula la clave pública al identificador del dispositivo una vez que el dispositivo demuestra la posesión de una clave privada coincidente. Esto completa la autenticación del dispositivo al relé (Autenticación en la Figura 16). Después de la autenticación, el relé devuelve un token, llamado conector, al dispositivo. El token incluye un blob de autenticación firmado por el relé y la clave pública efímera del relé (aprovisionamiento en la figura 16).

Para un acceso a la red, un dispositivo provisto por DPP intercambia un blob de autenticación con otro dispositivo provisto por DPP. La autenticación mutua ocurre en esta etapa cuando un dispositivo prueba una firma en el conector con la clave pública del relé. Estos dispositivos derivan el PMK

mediante la implementación de un intercambio de claves ECDH (en la Figura 16). La PMK es nueva en cada aprovisionamiento, ya que se basa en las claves públicas efímeras elegidas por ambos dispositivos.

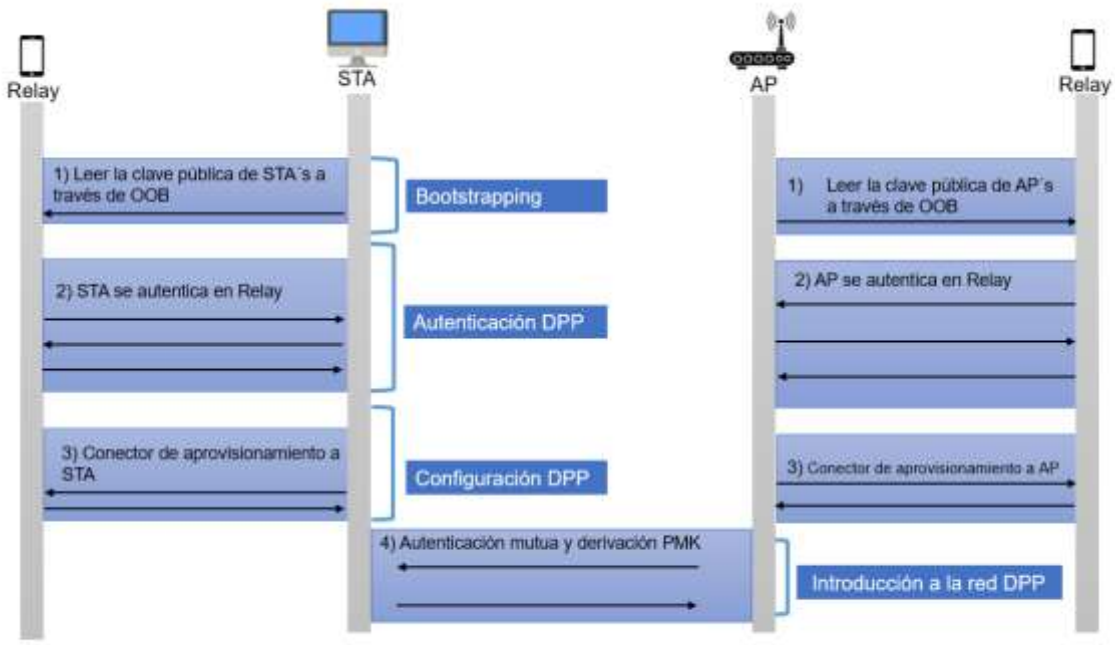


Figura 16: DPP se compone de ocho mensajes en cuatro fases. Los dos dispositivos se autentican mutuamente y acuerdan el PMK para el acceso a la red. Fuente: (Kwon & Choi, 2020)

D. Actualización de seguridad en modo empresarial

Una STA puede conectarse a un AP con diversos grados de opciones de seguridad, como cifrados, funciones hash, intercambios de claves y métodos de autenticación. Uno de los problemas en el modo de empresa WPA2 era demasiadas opciones, algunas de las cuales resultan inseguras. Por ejemplo, el uso de un conjunto de cifrado TLS que realiza un intercambio de claves RSA con un certificado de 1024 bits socavaría significativamente la solidez de la seguridad. Estos problemas son causados por la intratabilidad de la STA en los parámetros negociados en el momento de la iniciación, lo que ofrece la posibilidad de que las STA elijan por la fuerza las opciones menos seguras.

El modo de empresa WPA3 requiere una clave de cifrado de longitud mínima de 256 bits y el uso de conjuntos de cifrado aprobados por los algoritmos

comerciales de seguridad nacional (CNSA). Por ejemplo, el modo de autenticación de mensajes hash de 384 bits (HMACSHA384) para hash, la curva elíptica p384 de NIST para el establecimiento de claves y firmas digitales, y AES-GCM-256 para el cifrado y autenticación de datos. Con CNSA, el método EAP debe ser EAP-TLS. No es posible emplear algoritmos de combinación y combinación de manera insegura para no imponer degradaciones de cifrado.

E. Modo de transición en OWE y SAE

WPA3 proporciona modos de transición en OWE y SAE, respectivamente, para permitir una migración gradual a nuevas versiones. Un AP en el modo de transición para OWE está configurado para crear dos SSID con balizas separadas. Uno es un SSID abierto para la red abierta heredada. El otro es un SSID oculto para OWE. Las STA con capacidad OWE se conectan primero al SSID abierto. En la baliza, la STA aprenderá a buscar balizas de las capacidades OWE de publicidad SSID ocultas. Las STA heredadas simplemente ignoran las nuevas opciones en la baliza.

El modo de transición SAE ejecuta WPA3-SAE y WPA2-PSK en el mismo BSS con el mismo SSID. La contraseña es la misma en ambos modos. Las STA con capacidad WPA3 se conectan a una red utilizando el modo WPA-SAE, mientras que las STA heredadas se conectan a una red utilizando el modo WPA2-Personal.

Un modo de transición para el modo empresarial WPA3 no está disponible porque este modo no es compatible con versiones anteriores. Debido a esta implementación de incompatibilidad, el modo WPA3-Enterprise requiere un día de bandera para cambiar un nivel de seguridad a un nivel superior.

ATAQUES DE REDES INALÁMBRICAS

Muchas empresas han pasado de las tecnologías cableadas a las inalámbricas, lo que ha tenido un impacto negativo en su postura de seguridad. Las redes cableadas son generalmente mucho más fáciles de proteger que las redes inalámbricas, y una implementación deficiente a menudo introduce vulnerabilidades en las redes WiFi. La mayoría de empresas tampoco realizan un análisis de riesgos exhaustivo, lo que significa que esas vulnerabilidades no se identifican ni abordan. Debido a estas fallas de seguridad y la facilidad para explotarlas, los ataques a las redes inalámbricas son comunes (WebTitan, 2021).

¿Cuáles son los ataques a redes inalámbricas más comunes?

Muchos de los ataques a redes inalámbricas más comunes son de naturaleza oportunista. Los piratas informáticos Wi-Fi buscan redes inalámbricas que sean fáciles de atacar.

Los piratas informáticos se conforman de aprovechar los controles de seguridad deficientes para obtener acceso a información confidencial y distribuir malware. ¿Por qué perder el tiempo atacando redes Wi-Fi bien aseguradas cuando hay muchas con poca o ninguna seguridad?

Las redes WiFi mal aseguradas también son el objetivo de ciberdelincuentes y grupos del crimen organizado más sofisticados para hacerse un hueco en la red. Los ataques pueden ser extremadamente lucrativos. El acceso a una red empresarial puede permitir la instalación de ransomware y, si se puede instalar malware en los sistemas POS, se pueden robar los números de tarjetas de crédito / débito de decenas o cientos de miles de clientes.

Tipos de ataques a redes inalámbricas

Existen varios tipos diferentes de ataques Wi-Fi que los piratas informáticos utilizan para espiar las conexiones de red inalámbrica para obtener contraseñas y credenciales bancarias y propagar malware. Los principales tipos de ataques Wi-Fi se detallan a continuación.

Puntos de acceso Wi-Fi falsos, gemelos malvados y ataques del hombre en el medio

Los visitantes de hoteles, cafeterías y centros comerciales a menudo se conectan al Wi-Fi gratuito que se ofrece, pero varios estudios han

demostrado que no siempre se tiene cuidado al conectarse. Los clientes a menudo eligen el punto de acceso Wi-Fi basado en el SSID sin verificar que sea la red inalámbrica configurada por un establecimiento en particular para el uso del cliente.

Los delincuentes pueden configurar fácilmente puntos de acceso Wi-Fi falsos, a menudo utilizando el nombre del establecimiento en el SSID. Un SSID llamado 'Wi-Fi gratuito en el aeropuerto' sería suficiente para que muchas personas se conectaran. Cuando los clientes se conectan a estas redes Wi-Fi no autorizadas, aún pueden acceder a Internet, por lo que es poco probable que se den cuenta de que algo anda mal. Sin embargo, una vez conectados a esa red, todo lo que hagan en línea será monitoreado por los ciberdelincuentes. La información confidencial ingresada en línea, como direcciones de correo electrónico y contraseñas, números de tarjetas de crédito o credenciales bancarias, puede ser robada y será robada.

¿Cómo se hace esto? El atacante simplemente crea un punto de acceso en un teléfono inteligente y lo empareja con una tableta o computadora portátil. El hacker puede sentarse en una cafetería bebiendo un café con leche mientras monitorea el tráfico de todos los que se conectan. Alternativamente, pueden usar un enrutador con el mismo nombre y contraseña que el que está usando actualmente. Esto también puede tener una señal Wi-Fi más fuerte, lo que puede hacer que más personas se conecten. A través del "gemelo malvado", todo el tráfico será claramente visible para el atacante y se podrán capturar todos los datos enviados a través de la red.

Los puntos de acceso falsos y los gemelos malvados se encuentran entre los ataques de redes inalámbricas más comunes. Son fáciles de realizar, requieren poca habilidad técnica y son muy efectivos. Un estudio indicó que más de un tercio de los usuarios de puntos de acceso Wi-Fi no toman precauciones al acceder a puntos de acceso Wi-Fi y se conectan con frecuencia a redes no seguras (WebTitan, 2021).

Wardriving

Wardriving es una técnica que se utiliza para identificar y mapear puntos de acceso vulnerables. El nombre proviene del hecho de que los atacantes conducen por un vecindario y usan una computadora portátil con un dispositivo GPS, antena para identificar y registrar la ubicación de las redes inalámbricas. Esta técnica es eficaz ya que muchas redes Wi-Fi utilizadas por las empresas se extienden más allá de los confines del edificio y se aplican controles de seguridad deficientes para proteger esas redes.

Warshipping

Warshipping es un método más eficiente para atacar redes Wi-Fi, ya que permite que los ataques se realicen de forma remota, incluso si el atacante no está dentro del alcance de una red Wi-Fi. La táctica fue explicada por investigadores de IBM X-Force Red en Black Hat USA. Usaron componentes baratos (menos de $ 100) y fáciles de obtener para crear una computadora de placa única con capacidades Wi-Fi y 3G que funciona con la batería de un teléfono celular. El dispositivo se puede utilizar para conectarse localmente a la red Wi-Fi y enviar información a los atacantes a través de la conexión celular 3G.

Dado que el dispositivo es pequeño, se puede ocultar fácilmente dentro de un paquete pequeño, y llevar ese paquete a un edificio es fácil. Puede enviarse por correo. Dado que el paquete puede estar dirigido a alguien que no trabaja en la empresa, podría permanecer en la sala de correo durante un tiempo antes de que se abra. Dado que se puede rastrear el paquete, los atacantes sabrán cuándo está en el edificio. Alternativamente, podría ocultarse en cualquier número de artículos, desde macetas hasta osos de peluche. Si el dispositivo está dentro del alcance de las redes Wi-Fi, podría usarse para atacar esas redes.

Los códigos de acceso a la red hash se pueden enviar a los atacantes para que los descifren, y el dispositivo puede conectarse a las redes Wi-Fi en el edificio y recopilar datos. El dispositivo podría usarse en un ataque man-in-the-middle haciéndose pasar por una red Wi-Fi interna.

Suplantación de MAC

Muchas empresas utilizan el filtrado MAC para evitar que dispositivos específicos se conecten a sus redes Wi-Fi. Si bien esto es útil para evitar que las personas aprovechen el Wi-Fi gratuito para los clientes, este método de bloqueo de usuarios se puede omitir fácilmente. Es fácil falsificar una dirección MAC y omitir este control de filtrado.

¿Cómo pueden las empresas prevenir los ataques de redes inalámbricas más comunes?

¿Cómo pueden las empresas protegerse contra algunos de los ataques a redes inalámbricas más comunes? Si se conoce que es difícil esquivar la creación de puntos de acceso Wi-Fi engañosos, se pueden tomar medidas para evitar diversos ataques comunes a la red inalámbrica y mantener la red Wi-Fi segura.

- **Aislar la red de invitados**

  Si su red comercial no está aislada de su red Wi-Fi para invitados, podría usarse para obtener acceso a los datos comerciales y podría poner su POS en riesgo de verse comprometido. Utilice un enrutador que ofrezca múltiples SSID; la mayoría de los enrutadores actualizados tienen esa funcionalidad. Estos enrutadores suelen tener una opción SSID de invitado o un portal de invitado separado. Asegúrese de que esté activado cuando se implemente. Alternativamente, su enrutador inalámbrico puede tener una función de aislamiento inalámbrico que evitará que los usuarios de Wi-Fi ingresen a su red interna y otros dispositivos del cliente. Si necesita varios puntos de acceso en todo su establecimiento, es probable que necesite una configuración de túnel VLAN o EoIP: una configuración más complicada que requerirá que busque asesoramiento profesional sobre seguridad.

- **Cifre el tráfico Wi-Fi con WPA2 o WPA3**

  Si posee un enrutador obsoleto que no es compatible con el cifrado WPA2, es momento de actualizarlo. WPA2 es el estándar mínimo para la seguridad de Wi-Fi y, si bien aún se puede descifrar, requiere

mucho tiempo y es difícil. WPA3 ya se ha lanzado y se debe considerar una nueva actualización. También debe asegurarse de que WPS esté apagado.

- **Actualice el firmware de inmediato**

  Todo el software y los dispositivos poseen vulnerabilidades y requieren actualización. El software debe estar parcheado y los dispositivos, como los enrutadores, deberán actualizar su firmware cuando se creen nuevas versiones. Consulte el sitio web del fabricante de su dispositivo periódicamente para obtener detalles sobre las actualizaciones de firmware y asegúrese de que su dispositivo esté actualizado.

- **Crea un SSID seguro**

  Su enrutador tendrá un nombre SSID predeterminado, pero debe cambiarlo para personalizarlo para su empresa. Si lo identifica fácilmente, reducirá la posibilidad de que los puntos de acceso no autorizados se confundan con los suyos. Asegúrese de aplicar el cifrado WPA2 con una clave compartida y publique esa información para sus clientes junto con su SSID en un lugar destacado donde puedan verla.

- **Restringir el acceso Wi-Fi**

  Si su enrutador inalámbrico o punto de acceso es demasiado potente, se puede acceder a él desde fuera de sus instalaciones. Elija un enrutador que le permita alterar la fuerza de su señal y puede asegurarse de que solo sus clientes usarán su conexión. Además, asegúrese de que su punto de acceso Wi-Fi solo esté disponible durante el horario comercial. Si sus puntos de acceso se dejan sin supervisión cuando su empresa está cerrada, aumenta el riesgo de un ataque.

- **Asegure su infraestructura**

  Se puede abusar del acceso de administrador, así que asegúrese de que su nombre de usuario y sus contraseñas sean seguras. Si no se cambian las credenciales predeterminadas, solo será cuestión de tiempo antes de que se abuse de ellas. Cambie el nombre de usuario de 'admin' o cualquier otro nombre de usuario predeterminado. Establezca una contraseña segura que incluya letras mayúsculas y minúsculas, al menos un número y un carácter especial. La contraseña debe tener al menos 8 caracteres, aunque cuanto más, mejor. Alternativamente, use una contraseña de 14 caracteres.

1.4. Formulación del Problema.

Habiendo analizado la situación problemática actual se formuló el siguiente problema de manera interrogativa: ¿Qué protocolo de seguridad resulta más eficiente para combatir los ataques en redes inalámbricas?

1.5. Justificación e importancia del estudio.

Las redes inalámbricas conforman una parte esencial en la arquitectura de red actual. Se necesitan para la aceptación y administración de móviles y otorga conectividad a los dispositivos que son inaccesibles, costosas o no prácticas para las conexiones por cable. Aun así se necesitan medidas adicionales para el control del acceso a las redes Wi-Fi. En gran parte de libros y artículos se señalan riesgos mas no ofrecen una solución completamente segura. El estándar 802.11 para redes inalámbricas señala los métodos de encriptación y autenticación, pero a nivel empresarial, se deben implementar de manera escalable y manejable. Los peligros en redes inalámbricas desprotegidas son muchos. Los tráficos en redes inalámbricas son fácilmente rastreables y los hackers pueden recopilar información de propiedad, contraseñas, direcciones de servidores de intranet e inicios de sesión. Los intrusos pueden robar ancho de banda de Internet, y enviar información indeseable mediante spam o usar la red como un instrumento para atacar a otros objetivos. Pueden captar y hacer modificaciones en el tráfico para suplantar al usuario, con consecuencias

financieras o legales. Además, un atacante de baja tecnología puede causar estragos en un negocio al lanzar inundaciones de paquetes inalámbricos contra sus Access Points, Servers cercanos, y pasar a la red cableada.

1.6. Hipótesis.

El Protocolo WPA3 es más eficiente para combatir los ataques en redes inalámbricas Wi-Fi

1.7. Objetivos.

1.7.1. Objetivo general.

Evaluar el desempeño de los protocolos de seguridad de redes para combatir ataques en redes inalámbricas Wi-Fi

1.7.2. Objetivos específicos.

- Seleccionar los protocolos de seguridad existentes para combatir los ataques en redes inalámbricas.
- Diseñar un escenario de pruebas para poder evaluar el desempeño de los protocolos de seguridad de red para combatir ataques en redes inalámbricas.
- Realizar pruebas de ataque con el fin de probar cada protocolos de seguridad de red que fueron previamente implementados

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

La investigación es de tipo cuantitativa - cuasiexperimental porque mediante la recopilación y análisis de información se logrará comprobar la hipótesis de la investigación.

2.2. Población y muestra.

La población comprende todos los elementos a los que se refiere el proyecto, esto es, al conjunto del total de unidades para el muestreo. En el estudio que se propone se analizarán los protocolos de seguridad existentes con respecto a su desempeño para combatir las vulnerabilidades existentes en los protocolos de seguridad en redes inalámbricas Wi-Fi, por ello se definen los siguientes aspectos:

Protocolos de seguridad en redes inalámbricas Wi-Fi:

Los protocolos de seguridad en redes inalámbricas Wi-Fi que serán comprendidos dentro de la población a estudiar serían: WPA, WPA2 y WPA3, esto según los estándares IEEE 802.11 y la Wi-Fi Alliance, y se detallan en la tabla 3.

Tabla 3.

Protocolos de seguridad en redes inalámbricas comprendidos en la población.

	WPA	**WPA 2**	**WPA3**
Significa	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Desarrollado en:	2003	2004	2018
Encriptación:	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Tamaño de llave	128 bit	128 bit	128 bit 256 bit
Autenticación	Pre Shared Key & 802.1x with EAP	Pre Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integridad	64 Bit MIC	CCMP With AES	SHA-2

Fuente: (IPcisco.com, 2020)

En el presente caso se tomarán a los tres protocolos en vigencia como la muestra total a evaluar. Cabe aclarar que se ha obviado al protocolo WEP que se considera obsoleto, aunque todavía se utiliza a veces, ya sea porque algunos administradores de red no cambiaron la seguridad predeterminada en sus enrutadores inalámbricos o porque los dispositivos son demasiado antiguos como para admitir métodos de cifrado más nuevos como WPA. (Kaspersky, 2021)

Ataques en redes inalámbricas Wi-Fi: IEEE 802.11 señala a los servicios de seguridad en el ámbito de las redes inalámbricas Wi-Fi: Autenticación, Confidencialidad e Integridad. Según se señala en la tabla 4:

Tabla 4.

Servicios de seguridad en redes inalámbricas Wi-Fi.

Servicio	**Ataques**
Autenticación: Se vulnera mediante acciones realizadas por los atacantes para tener dominio del equipo atacado. Tiene como objetivo "hacer caer en el error" al sistema de la víctima para poder acceder a este. Por lo general este engaño se logra tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña	Spoofing IP splicing-hijacking Utilización de backdoors Utilización de exploits **Ataque de fuerza bruta** **Ataque de diccionario a un ssid oculto** Jamming o flooding
Confidencialidad: Se vulnera específicamente para robar data personal, desde la identificación de una persona hasta datos de tarjetas de crédito o cuentas de banco. La información obtenida puede ser vendida o incluso sometida a intercambio para que otras personas la compren y usen.	Espionaje Clave WEP Evil Twin AP **Phishing** **Man in the Middle** Ransomware Inducción chopchop Ataque estadístico. **ARP Spoofing + DNS Spoofing**
Integridad: Se vulnera mediante la introducción de modificaciones o la encriptación de datos y posterior exigencia de una forma de rescate para mostrar la clave de	Fragmentación 802,11 marco de inyección Replay **Ataque de denegación de servicios (DoS)**

	desencriptación.
	La modificación no autorizada de sistemas operativos, tablas de bases de datos, datos de producción y configuración de infraestructura también se consideran vulneran a la integridad de los datos

Fuente: (Tafur & Chavez, 2018).

Para el presente trabajo y por la facilidad de acceso a herramientas para implementar las vulnerabilidades, se han seleccionado los siguientes para la muestra:

Tabla 5.

Muestra de vulnerabilidades en protocolos de protección

Servicio	**Vulnerabilidad**
Autenticación	Ataque de fuerza bruta Ataque de diccionario a un ssid oculto
Confidencialidad	Phishing Man in the Middle ARP Spoofing + DNS Spoofing
Integridad	Ataque de denegación de servicios (DoS)

Fuente: Elaboración Propia.

2.3. Variables, Operacionalización.

Tabla 6.

Operacionalizacion de la variable Independiente.

Variable Independiente	Dimensiones	Indicadores	Ítems	Técnicas e Instrumentos de recolección de datos
	Cifrado	• Tamaño del IV (vector de iniciación)	Escala valorativa	**Técnica**: Revisión Documental **Instrumento:** Ficha de registro de datos
	Mecanismos de entrega de datos	• Mecanismos de Integridad de la cabecera.	Escala valorativa	**Técnica**: Revisión Documental **Instrumento:** Ficha de registro de datos
	Autorización		Escala valorativa	**Técnica**: Revisión Documental

Protocolos de seguridad de redes inalámbricas Wi-Fi	• Distribución de clave forma manual / por computadora	**Instrumento:** Ficha de registro de datos

Fuente: Elaboración Propia.

Tabla 7.

Operacionalizacion de la variable Dependiente.

Variable Dependiente	Dimensiones	Indicadores	Items	Técnicas e Instrumentos de recolección de datos
Vulnerabilidades en redes inalámbricas Wi-Fi	Confidencialidad	Promedio de tiempo de éxito de ataque **Phishing**	$\frac{\sum_{i=1}^{n} AtPhi_i}{n}$	**Técnica**: Revisión Documental **Instrumento:** Ficha de registro de datos
		Promedio de tiempo de éxito de ataque **Man in the Middle**	$\frac{\sum_{i=1}^{n} AtMiTM_i}{n}$	
		Promedio de tiempo de éxito de ataque	$\frac{\sum_{i=1}^{n} AtSpo_i}{n}$	

		ARP Spoofing + DNS Spoofing		
	Integridad	Promedio de tiempo de éxito de ataque de DoS	$\frac{\sum_{i=1}^{n} AtDoS_i}{n}$	**Técnica**: Revisión Documental **Instrumento:** Ficha de registro de datos
	Autenticación	Promedio de tiempo de éxito de ataque **de fuerza bruta**	$\frac{\sum_{i=1}^{n} AtBrut_i}{n}$	**Técnica**: Revisión Documental **Instrumento:** Ficha de registro de datos
		Promedio de tiempo de éxito de Ataque de	$\frac{\sum_{i=1}^{n} AtDiccio_i}{n}$	

	diccionario **a un ssid oculto**	

Fuente: Elaboración Propia.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Se hará uso de los siguientes instrumentos para la recolección de datos:

a) Revisión Documental: Se revisó el documento de (Tafur & Chavez, 2018), el cual cuenta con formatos de evaluación de protocolos de seguridad en redes inalámbricas Wi-Fi y los cuales han servido parcialmente para la evaluación de los protocolos como se muestra en la tabla siguiente.

Tabla 8.

Técnicas de recolección de datos.

Técnica	Instrumento	Elementos de la población	Descripción
Revisión Documental	Formatos para evaluación de protocolos de seguridad en redes inalámbricas Wi-Fi (Anexos 2-10)	Documentos y fichas establecidas para la evaluación de protocolos de seguridad Wi-Fi	Evaluación de desempeño de protocolos de seguridad en redes inalámbricas Wi-Fi

Fuente: Elaboración Propia

2.5. Procedimiento de análisis de datos.

Se utilizó las siguientes formulas:

Indicadores en variable independiente:

- **Tamaño del IV (vector de iniciación):** El tamaño del IV básicamente está ligado al algoritmo de cifrado y del protocolo de criptografía por lo general es tan largo como el tamaño de bloque o como el tamaño de la clave, por lo que será un indicador del cifrado del protocolo.

- **Mecanismos de Integridad de la cabecera:** Los protocolos de seguridad ofrecen mecanismos de integridad, tales como Integrity Check Value – Valor de verificación de integridad (iCV), el algoritmo Michael en el caso de WPA y WPA2 y el Algoritmo Galois Counter Mode en WPA3.
- **Distribución de clave forma manual:** Mientras WEP cuenta con un sistema abierto y de clave compartida, WPA y WPA2 están implementados con sistemas de clave precompartida y del mismo modo WPA3 cuenta con un sistema de autenticación llamado Dragonfly.

Para el caso de las variables independientes, se procederá a utilizar una escala valorativa para medir los indicadores por cada protocolo según lo señalado en el ANEXO 2

Luego se procederá a colocar los resultados en la tabla del anexo 3, y se procederá a operar conforme lo señalado en los anexos 4-6.

Indicadores en variable dependiente:

- **Promedio de tiempo de éxito de ataque Phishing:** Se utilizará este indicador para medir la confidencialidad.

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{\sum_{i=1}^{n} AtPhi_i}{n}$$

Dónde: AtPhi= tiempo de éxito de ataque Phishing

n=número de ataques Ataques Phishing realizados

- **Promedio de tiempo de éxito de ataque Man in the middle:** Se utilizará este indicador para medir la confidencialidad.

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ Middle\ = \frac{\sum_{i=1}^{n} AtMiTM_i}{n}$$

Dónde: AtMiTM= tiempo de éxito de ataque Ataques de Man in the middle

n=número de Ataques Man in The Middle realizados

- **Promedio de tiempo de éxito de ataque ARP Spoofing + DNS Spoofing:** Se utilizará este indicador para medir la confidencialidad.

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing\ = \frac{\sum_{i=1}^{n} AtSpo_i}{n}$$

Dónde: AtSpo= tiempo de éxito de ataque ARP Spoofing + DNS Spoofing

n=número de Ataques ARP Spoofing + DNS Spoofing realizados

- **Promedio de tiempo de éxito de ataque DoS:** Se utilizará este indicador para medir la integridad.

$$Promedio\ de\ tiempo\ de\ éxito\ DoS\ = \frac{\sum_{i=1}^{n} AtDoS_i}{n}$$

Dónde: AtDoS= tiempo de éxito de ataque DoS
n=número de Ataques DoS realizados

- **Promedio de tiempo de éxito de ataque de fuerza bruta:** Se utilizará este indicador para medir la autenticación.

$$Promedio\ de\ tiempo\ de\ éxito\ DoS\ = \frac{\sum_{i=1}^{n} AtBrut_i}{n}$$

Dónde: AtBrut= tiempo de éxito de ataque de fuerza bruta
n=número de Ataques de fuerza bruta realizados

- **Promedio de tiempo de éxito de ataque de diccionario a un ssid oculto:** Se utilizará este indicador para medir la autenticación.

$$Promedio\ de\ tiempo\ de\ éxito\ DoS\ = \frac{\sum_{i=1}^{n} AtDiccio_i}{n}$$

Dónde: AtDiccio= tiempo de éxito de ataque de diccionario
n=número de Ataques de diccionario realizados

Luego de obtener los resultados, se procederán a colocar los resultados obtenidos en la tabla del anexo 7, y se procederá a operar conforme lo señalado en los anexos 8-10.

Para la recolección de datos en ambos escenarios se hace uso de las siguientes herramientas de auditoria Wi-Fi:

- Kali Linux
- WIFISLAX
- Xiaopan Os.
- Ettercap

2.6. Criterios éticos.

Los criterios éticos se relacionaron con la evaluación de protocolos de redes inalámbricas Wi-Fi por ello se aplicó el siguiente criterio.

a. Criterio de conformidad

El estudio busca estar alineado con las leyes que el Colegio de Ingenieros del Perú establece dentro de sus políticas internas respecto a la ética profesional que caracteriza a los profesionales de esta rama de la ciencia, por ello, se buscará que los expertos seleccionados manifiesten compromiso con el Código Deontológico del Colegio Profesional en mención, considerando las penalidades sujetas al incumplimiento de objetividad y transparencia.

2.7. Criterios de Rigor Científico.

La presente investigación se ejecutará bajo un enfoque cuantitativo, por lo que validará la eficiencia de los protocolos antes indicados, bajo criterios científicos que permitan su transferibilidad en contexto similares, midiendo los indicadores propuestos, generados a partir de la recolección de resultados y orden correspondiente, de manera exhaustiva, clara y concisa.

a. Criterio de claridad

Bajo este criterio se busca que lo manifestado en el presente estudio sea entendible en el lenguaje aplicado, sin llegar a cometer ambigüedad de definición de términos o conflictos de elementos, alterando el entendimiento del responsable de la implementación en la organización.

b. Criterio de objetividad

Los resultados deberán ser medibles y concretos dentro de la conducta que manifiesten, permitiendo datos concretos del contexto y de la realidad obtenida tras la implementación de la metodología propuesta.

c. Criterio de coherencia

Las descripciones de actividades deberán manifestar correspondencia lógica entre la teoría y lo plasmado en el desarrollo del presente estudio, con

el fin de reforzar la premisa de los protocolos de seguridad deben ser implementados y cuál de ellos puede resultar más eficiente.

d. Criterio de pertinencia

El contenido del presente estudio buscará respetar los principios de seguridad de la información y términos familiarizados a la seguridad de la información. Considerando evitar confusión con términos de riesgos financieros, riesgos de salud, riesgos operacionales, entre otros similares.

e. Criterio de suficiencia

El presente estudio buscará cubrir lo exigido por los principios de la seguridad informática, y deberá manifestar suficiencia en sus actividades e instrumentos construidos.

f. Criterio de relevancia

El presente estudio será importante para lograr el entendimiento de la implementación de protocolos en redes inalámbricas wi-fi y determinan claramente los pro y contras al implementar cada protocolo dentro de una organización o red doméstica.

III. RESULTADOS.

VARIABLE INDEPENDIENTE

3.1. Resultados en Tablas y Figuras.

Se inicia con la variable independiente donde se continuará con el análisis respectivo, se tomará como referencia a datos establecidos en cada protocolo inalámbrico y a ciertas especificaciones técnicas. Se dará los siguientes valores cuantitativos:

Tabla 9.
Escala Valorativa de cuantificación de indicadores (Variable Independiente).

CARACTERISTICA	CALIFICACIÓN
Muy Malo	0
Malo	1
Regular	2
Muy bueno	3
Excelente	4

Fuente: (Tafur & Chavez, 2018)

INDICADOR 1: Cifrado

Escenario Doméstico

Tabla 10.
Cifrado de protocolos.

INDICES	WPA	WPA2	WPA3
Algoritmo de cifrado	3	3	4
Tamaño del IV	2	3	3

Fuente: Elaboración propia.

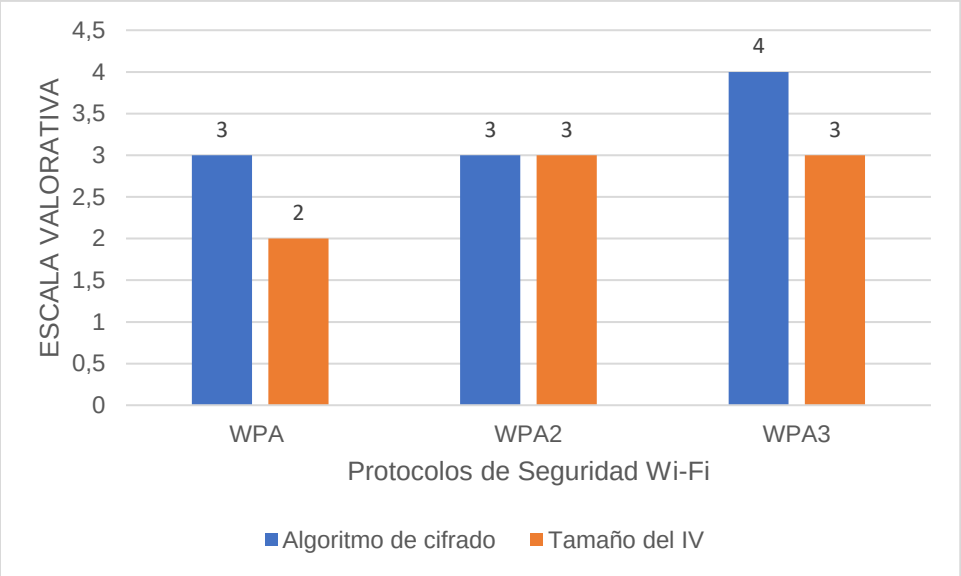


Figura 17: INDICADOR - CIFRADO. Fuente: Elaboración Propia.

Interpretación:

El protocolo inalámbrico WPA utiliza un algoritmo TKIP como instrumento de encriptación, que ayudan a resolver la debilidad del vector de inicialización de WEP con la inclusión del vector con una longitud de (48 bits), así permitiendo lograr una combinación de caracteres de claves distintas previniendo ataques. Las WPA-AES se generan automáticamente y son repartidas automáticamente eludiendo su modificación manual cada determinado tiempo. El cifrado en el protocolo WPA2 a diferencia de WPA, se distingue por utilizar el estándar AES en lugar del cifrado de flujo RC4. Finalmente, el cifrado es de 128 bits en modo WPA3-Personal. El protocolo WPA3 también reemplaza el intercambio de claves precompartidas (PSK) con la autenticación simultánea de iguales, una forma más segura de realizar el intercambio de claves inicial que con los protocolos anteriores.

INDICADOR 2: Mecanismos de Entrega de Datos

Tabla 11.
Mecanismos de entrega de datos.

INDICES	WPA	WPA2	WPA3
Mecanismos de Integridad de la cabecera.	2	3	4

Fuente: Elaboración propia.

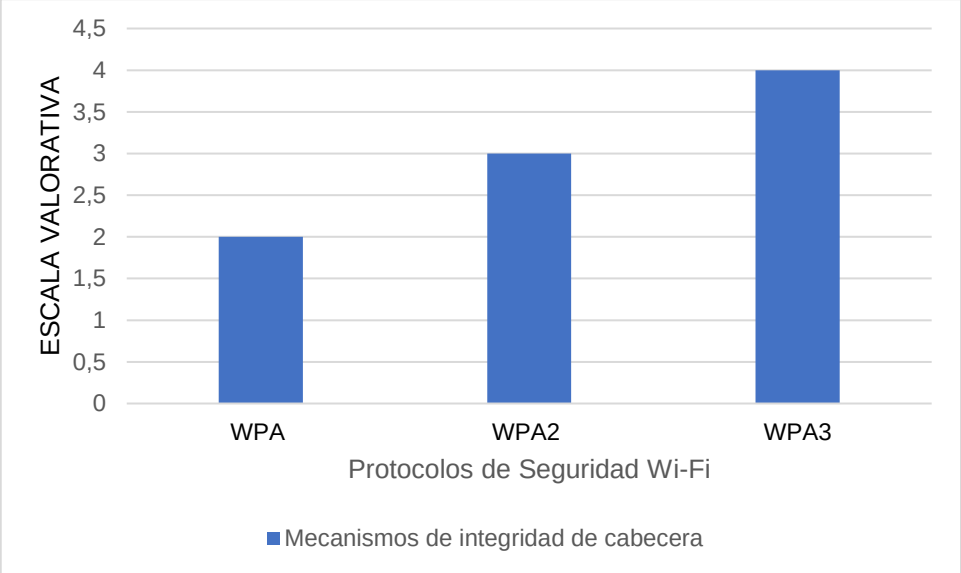


Figura 18: Mecanismos de cabecera. Fuente: Elaboración Propia.

Interpretación:

En el caso de WPA-TKIP y WPA-AES, es el algoritmo Michael el que es usado para el cálculo de código de integridad que evita que el atacante capture paquetes y que estos sean modificados y reenviados. Este algoritmo fue limitado por Hardware basado en RC4 debido a que no proporcionan seguridad contra ataques de fuerza bruta. Pasando a WPA2, se asegura la cabecera del frame y los datos mediante CCMP. WPA2 cifra el MIC con el cifrado de modo contador de AES. Finalmente, por el lado de WPA3, se utiliza GCMP el cual utiliza el mismo algoritmo de cifrado AES, pero de un modo de operación ligeramente diferente llamado Galois Counter Mode, o también conocido como GCM. Este nuevo modo de

operación es más eficiente, tanto a la hora de operar con los bloques de datos, como también su implementación. AES-GCM no es un protocolo nuevo, de hecho, llevamos varios años usándolo en protocolos como OpenVPN, IPSec, HTTPS y conexiones TLS en general. Sin embargo, sí es una novedad su estandarización para usarlo en Wi-Fi.

INDICADOR 3:

Autorización

Tabla 12.
Autorización.

INDICES	WPA	WPA2	WPA3
Distribución de clave forma manual	1	1	2
Autenticación de maquina	1	2	3

Fuente: Elaboración propia.

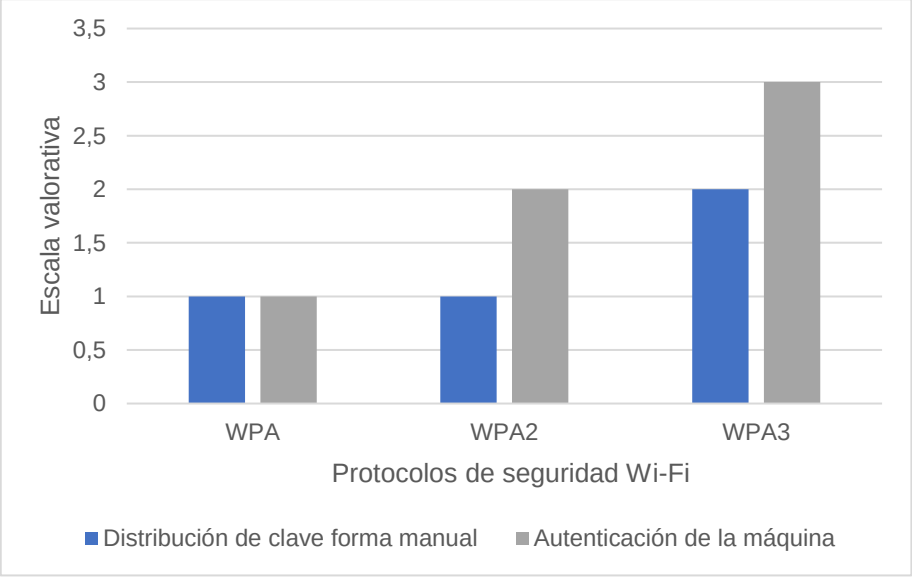


Figura 19: Distribución de clave. Fuente: Elaboración Propia.

Interpretación:

Con WPA-TKIP la configuración de las claves es de forma manual en los Access Point y clientes, y deja abierta la

vulnerabilidad de parte del usuario dado a que no se generan claves suficientemente fuertes. El mecanismo de integridad mejorada no permite la inyección de tráfico, pero permite disociaciones por las autenticaciones haciendo uso de MAC y con WPA-AES hace uso de una configuración robusta verificando a cada usuario y no solo a la MAC, tiene una generación única de claves automáticas dejando de lado las claves compartidas por todos los usuarios de un entorno. Si deseamos vulnerar una infraestructura montada es difícil pero si utilizamos un cifrado ya vulnerado llega a ser susceptible a los ataques en las contraseñas, es susceptible a interferencias por parte del Access Point.

WPA2 usa dos modos de pre-autenticación dando posibilidad al usuario el establecimiento de procesos de autenticación con puntos de accesos próximos. WPA2-TKIP que resulta similar a WPA, al contar con una clave distribuida manualmente al usar el cifrado y WPA2-AES que hace uso de un cifrado mejorado respecto a sus predecesores, mediante una configuración más robusta, generando claves automáticas únicas por cada usuario evitando la distribución manual. Finalmente, con WPA3 tenemos La "Autenticación simultánea de iguales (SAE)" para proporcionar una autenticación basada en contraseña más confiable. **WPA3** proporciona a los usuarios una protección de seguridad mejorada al verificar la información de la contraseña y utilizar contraseñas para la verificación de identidad en lugar de la exportación de claves.

Tabla 13.

Subtotales del Análisis de la Variable Independiente.

Dimensiones	**Indicadores**	**WPA**	**WPA2**	**WPA3**
Método de Cifrado	Algoritmo de cifrado	3	3	4
	Tamaño del IV	2	3	3

Mecanismos de Entrega de Datos	Mecanismos de integridad de la cabecera	2	3	4
Autorización	Distribución de clave forma manual	1	1	2
	Autenticación de máquina	1	2	3
RESULTADOS TOTALES		9	**12**	**16**

Fuente: Elaboración propia.

Tabla 14.
Sumatoria de Análisis de la variable Independiente.

DIMENSIONES	**WPA**	**WPA2**	**WPA3**
Método de Cifrado	5	6	7
Mecanismos de Entrega de Datos	2	4	4
Autorización	2	3	5
RESULTADOS TOTALES	9	12	16

Fuente: Elaboración propia.

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador) Entonces:

PT= 7 + 4 + 5 = 16

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW) = (PT_PW / PT) *100%

Tabla 15.
Porcentaje Total de Cada Protocolo Analizado.

WPA	**WPA2**	**WPA3**
56,25%	75%	100%

Fuente: Elaboración propia.

Tabla 16.
Porcentaje por Protocolo de Variable Independiente

INDICES	WPA	WPA2	WPA3
PT_PW	9	12	16
PT	16	16	16
PORCENTAJE POR PROTOCOLO	56,25	75	100

Fuente: Elaboración propia.

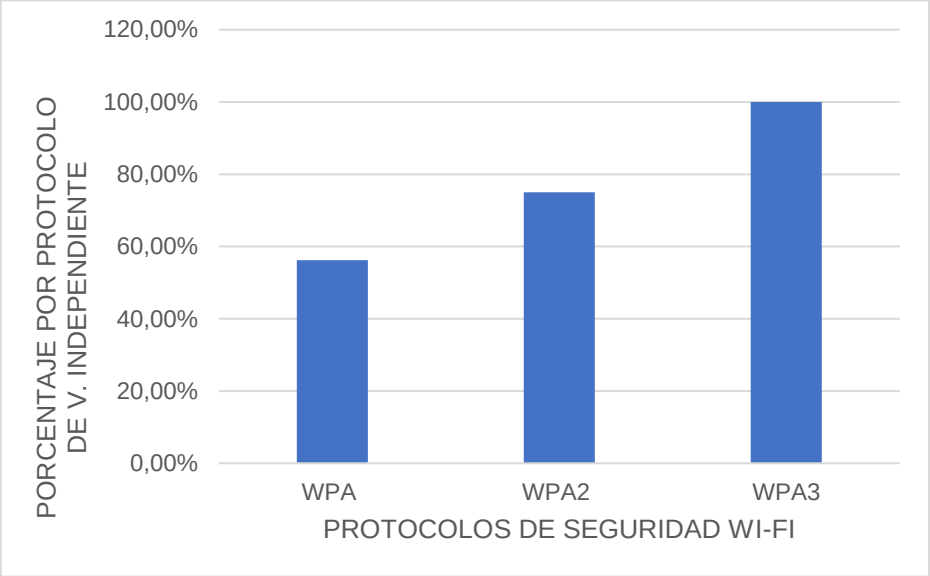


Figura 20: Porcentaje por Protocolo de Variable Independiente. Fuente: Elaboración Propia.

VARIABLE DEPENDIENTE

Con respecto a la variable dependiente, se hicieron 30 ataques por cada protocolo para determinar un tiempo promedio

INDICADOR DE CONFIDENCIALIDAD

Ataque Phishing

Ataque Phishing en Protocolo WPA

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque Phishing:

Tabla 17.
Tiempos de éxito de ataque Phishing con el protocolo WPA.

Valor 1	7.9
Valor 2	**8.1**
Valor 3	**8.0**

Valor 4	**8.0**
Valor 5	**7.9**
Valor 6	**7.9**
Valor 7	**7.7**
Valor 8	**8.1**
Valor 9	**7.9**
Valor 10	**8.0**
Valor 11	**7.8**
Valor 12	**8.1**
Valor 13	**8.3**
Valor 14	**8.0**
Valor 15	**7.8**
Valor 16	**8.2**
Valor 17	**7.8**
Valor 18	**7.8**
Valor 19	**8.3**
Valor 20	**7.8**
Valor 21	**8.2**
Valor 22	**8.1**
Valor 23	**8.2**
Valor 24	**8.2**
Valor 25	**8.2**
Valor 26	**7.8**
Valor 27	**8.0**
Valor 28	**7.8**
Valor 29	**8.2**
Valor 30	**8.0**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{\sum_{i=1}^{n} AtPhi_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{7{,}9 + 8{,}1 + \cdots 8{,}2 + 8}{30} = \frac{240}{30} = 8$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA fueron 8 minutos.

Ataque Phishing en Protocolo WPA2

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque Phishing:

Tabla 18.
Tiempos de éxito de ataque Phishing con el protocolo WPA2.

Valor 1	**12.3**
Valor 2	**12.0**
Valor 3	**11.7**
Valor 4	**12.0**
Valor 5	**12.0**
Valor 6	**12.0**
Valor 7	**11.9**
Valor 8	**12.2**
Valor 9	**11.8**
Valor 10	**11.9**
Valor 11	**12.0**
Valor 12	**12.3**
Valor 13	**12.0**
Valor 14	**12.1**
Valor 15	**12.1**
Valor 16	**11.9**
Valor 17	**11.9**
Valor 18	**12.1**
Valor 19	**11.7**
Valor 20	**12.0**
Valor 21	**12.0**
Valor 22	**12.2**
Valor 23	**12.3**
Valor 24	**12.0**
Valor 25	**11.9**
Valor 26	**12.0**
Valor 27	**12.1**
Valor 28	**12.1**
Valor 29	**11.9**
Valor 30	**11.7**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{\sum_{i=1}^{n} AtPhi_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{12{,}3 + 12{,}0 + \cdots 11{,}9 + 11{,}7}{30} = \frac{360}{30} = 12$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA2 fueron 12 minutos.

Ataque Phishing en Protocolo WPA3

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque Phishing:

Tabla 19.
Tiempos de éxito de ataque Phishing con el protocolo WPA3.

Valor 1	**23.3**
Valor 2	**22.9**
Valor 3	**23.2**
Valor 4	**23.3**
Valor 5	**23.2**
Valor 6	**23.4**
Valor 7	**23.0**
Valor 8	**23.2**
Valor 9	**23.1**
Valor 10	**23.3**
Valor 11	**23.4**
Valor 12	**23.1**
Valor 13	**23.4**
Valor 14	**23.1**
Valor 15	**23.1**
Valor 16	**23.3**
Valor 17	**23.4**
Valor 18	**23.2**
Valor 19	**23.1**
Valor 20	**23.0**
Valor 21	**23.2**
Valor 22	**23.2**
Valor 23	**23.3**
Valor 24	**23.1**
Valor 25	**23.0**
Valor 26	**23.4**
Valor 27	**23.0**
Valor 28	**23.5**
Valor 29	**22.9**
Valor 30	**23.1**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{\sum_{i=1}^{n} AtPhi_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Phishing = \frac{23{,}3 + 23{,}9 + \cdots 22{,}9 + 23{,}1}{30} = \frac{696}{30}$$

$$= 23{,}2$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA3 fueron 23,2 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo.

Tabla 20.
Tiempo de éxito ante el ataque Phishing de los protocolos de seguridad Wi-Fi.

Protocolos Wi-Fi	**WPA**	**WPA2**	**WPA3**
Suplantación de identidad (Phishing)	8min	12 min	23.2min

Fuente: Elaboración Propia.

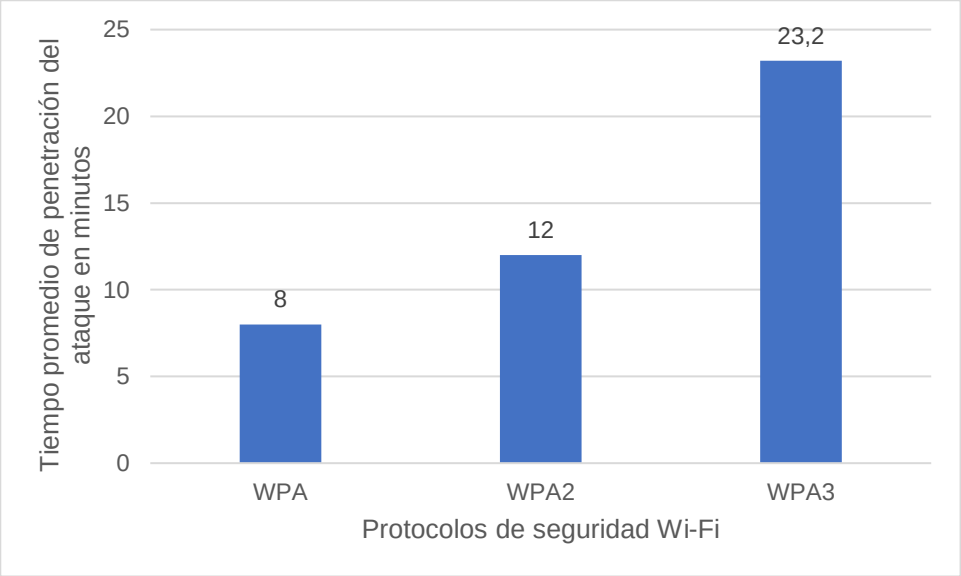


Figura 20: Tiempo de éxito ante el ataque Phishing de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

Ataque Man in the middle

Ataque Man in the middle en Protocolo WPA

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque Man in the middle:

Tabla 21.
Tiempos de éxito de ataque Man in the middle con el protocolo WPA.

Valor 1	**3.0**
Valor 2	**2.8**
Valor 3	**3.2**
Valor 4	**2.9**

Valor 5	**3.1**
Valor 6	**2.9**
Valor 7	**3.0**
Valor 8	**2.8**
Valor 9	**2.9**
Valor 10	**3.2**
Valor 11	**2.9**
Valor 12	**3.2**
Valor 13	**3.1**
Valor 14	**2.8**
Valor 15	**3.2**
Valor 16	**2.8**
Valor 17	**3.1**
Valor 18	**2.8**
Valor 19	**2.9**
Valor 20	**3.1**
Valor 21	**3.1**
Valor 22	**3.0**
Valor 23	**3.0**
Valor 24	**3.1**
Valor 25	**2.7**
Valor 26	**3.2**
Valor 27	**2.9**
Valor 28	**3.2**
Valor 29	**3.0**
Valor 30	**2.8**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{\sum_{i=1}^{n} AtMiTM_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{3{,}0 + 2{,}8 + \cdots 3{,}0 + 2{,}8}{30} = \frac{90}{30} = 3$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA fueron 3 minutos.

Ataque Man in the middle en Protocolo WPA2

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque Man in the middle:

Tabla 22.
Tiempos de éxito de ataque Man in the middle con el protocolo WPA2.

Valor 1	3.8
Valor 2	**3.7**
Valor 3	**3.8**
Valor 4	**3.2**
Valor 5	**3.8**
Valor 6	**3.4**
Valor 7	**3.8**
Valor 8	**3.4**
Valor 9	**3.4**
Valor 10	**3.8**
Valor 11	**3.3**
Valor 12	**3.3**
Valor 13	**3.5**
Valor 14	**3.2**
Valor 15	**3.6**
Valor 16	**3.4**
Valor 17	**3.6**
Valor 18	**3.4**
Valor 19	**3.2**
Valor 20	**3.6**
Valor 21	**3.4**
Valor 22	**3.8**
Valor 23	**3.2**
Valor 24	**3.7**
Valor 25	**3.2**
Valor 26	**3.4**
Valor 27	**3.7**
Valor 28	**3.3**
Valor 29	**3.4**
Valor 30	**3.5**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{\sum_{i=1}^{n} AtMiTM_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{3{,}8 + 3{,}7 + \cdots 3{,}4 + 3{,}5}{30} = \frac{105}{30} = 3{,}5$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA fueron 3,5 minutos.

Ataque Man in the middle en Protocolo WPA3

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque Man in the middle:

Tabla 23.
Tiempos de éxito de ataque Man in the middle con el protocolo WPA3.

Valor 1	**4.4**
Valor 2	**4.3**
Valor 3	**4.6**
Valor 4	**4.3**
Valor 5	**4.4**
Valor 6	**4.3**
Valor 7	**4.3**
Valor 8	**4.3**
Valor 9	**4.4**
Valor 10	**4.3**
Valor 11	**4.5**
Valor 12	**4.3**
Valor 13	**4.5**
Valor 14	**4.6**
Valor 15	**4.5**
Valor 16	**4.3**
Valor 17	**4.3**
Valor 18	**4.6**
Valor 19	**4.3**
Valor 20	**4.4**
Valor 21	**4.5**
Valor 22	**4.4**
Valor 23	**4.4**
Valor 24	**4.5**
Valor 25	**4.4**
Valor 26	**4.3**
Valor 27	**4.3**
Valor 28	**4.6**
Valor 29	**4.4**
Valor 30	**4.3**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{\sum_{i=1}^{n} AtMiTM_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ Man\ in\ the\ middle = \frac{4{,}4 + 4{,}3 + \cdots 4{,}4 + 4{,}3}{30} = \frac{13{,}2}{30} = 4{,}4$$

Obteniendo que en promedio el tiempo de éxito del ataque Phishing en el protocolo WPA fueron 4,4 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo.

Tabla 24.
Tiempo de éxito ante el ataque Man in the middle de los protocolos de seguridad Wi-Fi.

Protocolos WiFi	**WPA**	**WPA2**	**WPA3**
Man in the middle	3min	3,5min	4,4 min

Fuente: Elaboración Propia.

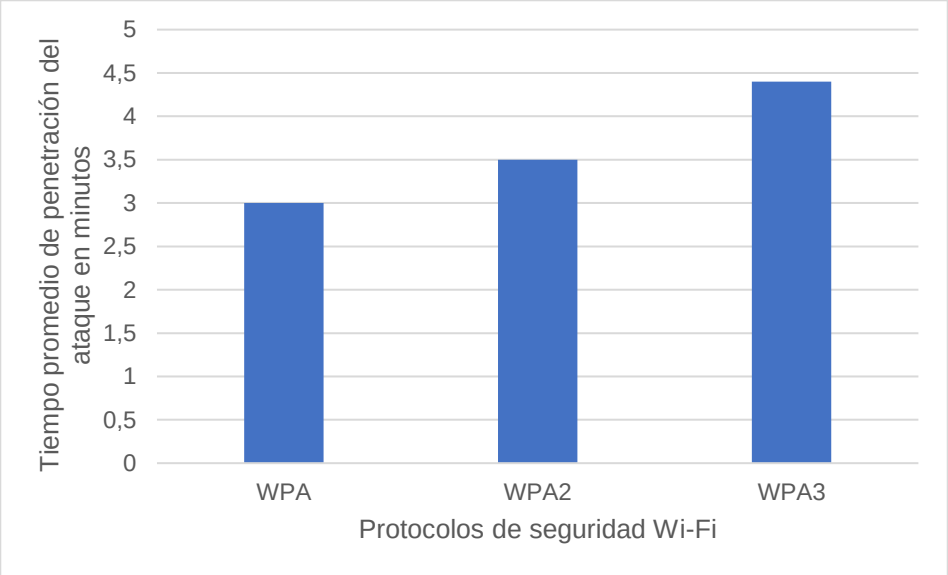


Figura 21: Tiempo de éxito ante el ataque Man in the middle de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

Ataque ARP Spoofing + DNS Spoofing

Ataque ARP Spoofing + DNS Spoofing en Protocolo WPA

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque ARP Spoofing + DNS Spoofing:

Tabla 25.
Tiempos de éxito de ataque ARP Spoofing + DNS Spoofing con el protocolo WPA.

Valor 1	**1.7**
Valor 2	**2.1**
Valor 3	**2.1**
Valor 4	**2.1**
Valor 5	**2.0**
Valor 6	**1.9**
Valor 7	**2.1**
Valor 8	**1.9**
Valor 9	**2.2**
Valor 10	**2.0**
Valor 11	**1.8**
Valor 12	**2.1**
Valor 13	**1.9**
Valor 14	**2.1**
Valor 15	**1.8**
Valor 16	**2.2**
Valor 17	**2.2**
Valor 18	**2.1**
Valor 19	**2.0**
Valor 20	**1.8**
Valor 21	**2.1**
Valor 22	**2.2**
Valor 23	**2.1**
Valor 24	**1.7**
Valor 25	**1.9**
Valor 26	**2.1**
Valor 27	**1.8**
Valor 28	**1.9**
Valor 29	**2.1**
Valor 30	**1.9**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing = \frac{\sum_{i=1}^{n} AtSpo_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing = \frac{1{,}7 + 2{,}1 + \cdots 2{,}1 + 1{,}9}{30} = \frac{60}{30} = 2$$

Obteniendo que en promedio el tiempo de éxito del ataque **ARP Spoofing + DNS Spoofing** en el protocolo WPA fueron 2 minutos.

Ataque ARP Spoofing + DNS Spoofing en Protocolo WPA2

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque ARP Spoofing + DNS Spoofing:

Tabla 26.
Tiempos de éxito de ataque ARP Spoofing + DNS Spoofing con el protocolo WPA2.

Valor 1	**2.7**
Valor 2	**2.3**
Valor 3	**2.5**
Valor 4	**2.7**
Valor 5	**2.2**
Valor 6	**2.2**
Valor 7	**2.3**
Valor 8	**2.1**
Valor 9	**2.6**
Valor 10	**2.5**
Valor 11	**2.5**
Valor 12	**2.6**
Valor 13	**2.4**
Valor 14	**2.4**
Valor 15	**2.3**
Valor 16	**2.6**
Valor 17	**2.5**
Valor 18	**2.4**
Valor 19	**2.1**
Valor 20	**2.4**
Valor 21	**2.5**
Valor 22	**2.2**
Valor 23	**2.6**
Valor 24	**2.6**
Valor 25	**2.3**
Valor 26	**2.1**
Valor 27	**2.2**
Valor 28	**2.6**
Valor 29	**2.3**
Valor 30	**2.2**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing = \frac{\sum_{i=1}^{n} AtSpo_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing$$
$$= \frac{2{,}7 + 2{,}3 + \cdots 2{,}3 + 2{,}2}{30} = \frac{7{,}2}{30} = 2{,}4$$

Obteniendo que en promedio el tiempo de éxito del ataque **ARP Spoofing + DNS Spoofing** en el protocolo WPA2 fueron 2,4 minutos.

Ataque ARP Spoofing + DNS Spoofing en Protocolo WPA3

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque ARP Spoofing + DNS Spoofing:

Tabla 27.
Tiempos de éxito de ataque ARP Spoofing + DNS Spoofing con el protocolo WPA3.

Valor 1	**3.4**
Valor 2	**3.3**
Valor 3	**3.4**
Valor 4	**3.2**
Valor 5	**3.1**
Valor 6	**3.1**
Valor 7	**3.3**
Valor 8	**3.3**
Valor 9	**3.6**
Valor 10	**3.2**
Valor 11	**3.4**
Valor 12	**3.1**
Valor 13	**3.3**
Valor 14	**3.2**
Valor 15	**3.2**
Valor 16	**3.6**
Valor 17	**3.3**
Valor 18	**3.6**
Valor 19	**3.3**
Valor 20	**3.4**
Valor 21	**3.4**
Valor 22	**3.2**
Valor 23	**3.2**
Valor 24	**3.1**
Valor 25	**3.4**
Valor 26	**3.1**
Valor 27	**3.3**
Valor 28	**3.6**
Valor 29	**3.3**
Valor 30	**3.4**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing = \frac{\sum_{i=1}^{n} AtSpo_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ARP\ Spoofing\ +\ DNS\ Spoofing = \frac{3{,}4 + 3{,}3 + \cdots 3{,}3 + 3{,}4}{30} = \frac{99}{30} = 3{,}3$$

Obteniendo que en promedio el tiempo de éxito del ataque **ARP Spoofing + DNS Spoofing** en el protocolo WPA3 fueron 3,3 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo.

Tabla 28.
Tiempo de éxito ante el ataque ARP Spoofing + DNS Spoofing de los protocolos de seguridad Wi-Fi.

Protocolos Wi-Fi	**WPA**	**WPA2**	**WPA3**
ARP Spoofing + DNS Spoofing	2min	2,4min	3,3min

Fuente: Elaboración Propia.

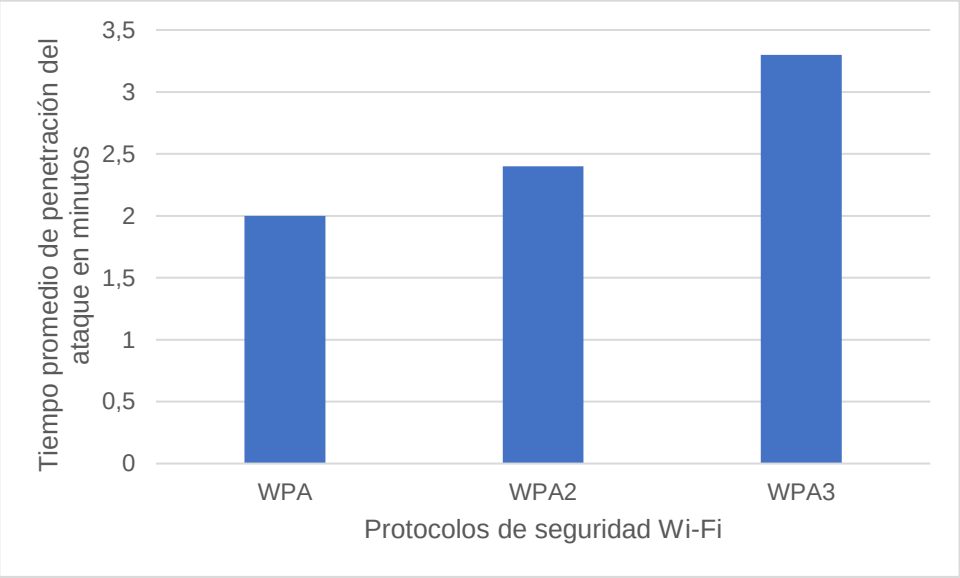


Figura 22: Tiempo de éxito ante el ataque ARP Spoofing + DNS Spoofing de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

INDICADOR DE INTEGRIDAD

Ataque DoS

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque DoS:

Tabla 29.
Tiempos de éxito de ataque DoS con el protocolo WPA.

Valor 1	**3.1**
Valor 2	**3.4**
Valor 3	**3.4**
Valor 4	**3.4**
Valor 5	**3.7**
Valor 6	**3.6**
Valor 7	**3.3**
Valor 8	**3.3**
Valor 9	**3.4**
Valor 10	**3.4**
Valor 11	**3.7**
Valor 12	**3.4**
Valor 13	**3.7**
Valor 14	**3.4**
Valor 15	**3.2**
Valor 16	**3.5**
Valor 17	**3.4**
Valor 18	**3.4**
Valor 19	**3.2**
Valor 20	**3.5**
Valor 21	**3.2**
Valor 22	**3.1**
Valor 23	**3.7**
Valor 24	**3.2**
Valor 25	**3.3**
Valor 26	**3.1**
Valor 27	**3.3**
Valor 28	**3.7**
Valor 29	**3.3**
Valor 30	**3.6**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{\sum_{i=1}^{n} AtDos_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{3{,}1 + 3{,}4 + \cdots 3{,}3 + 3{,}6}{30} = \frac{102}{30} = 3{,}4$$

Obteniendo que en promedio el tiempo de éxito del ataque DoS en el protocolo WPA fueron 3,4 minutos.

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque DoS:

Tabla 30.
Tiempos de éxito de ataque DoS con el protocolo WPA2.

Valor 1	**4.0**
Valor 2	**3.7**
Valor 3	**4.0**
Valor 4	**4.2**
Valor 5	**4.0**
Valor 6	**4.0**
Valor 7	**4.2**
Valor 8	**3.7**
Valor 9	**4.1**
Valor 10	**3.7**
Valor 11	**4.0**
Valor 12	**3.7**
Valor 13	**3.9**
Valor 14	**4.2**
Valor 15	**4.2**
Valor 16	**4.0**
Valor 17	**3.7**
Valor 18	**4.1**
Valor 19	**4.0**
Valor 20	**4.1**
Valor 21	**4.1**
Valor 22	**4.0**
Valor 23	**3.8**
Valor 24	**4.1**
Valor 25	**3.8**
Valor 26	**4.2**
Valor 27	**4.1**
Valor 28	**4.1**
Valor 29	**3.9**
Valor 30	**4.2**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{\sum_{i=1}^{n} AtDos_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{4{,}0 + 3{,}7 + \cdots 3{,}9 + 4{,}2}{30} = \frac{120}{30} = 4$$

Obteniendo que en promedio el tiempo de éxito del ataque DoS en el protocolo WPA2 fueron 4 minutos.

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque DoS:

Tabla 31.
Tiempos de éxito de ataque DoS con el protocolo WPA3.

Valor 1	**6.1**
Valor 2	**5.6**
Valor 3	**5.9**
Valor 4	**6.1**
Valor 5	**6.2**
Valor 6	**5.9**
Valor 7	**5.7**
Valor 8	**5.9**
Valor 9	**6.2**
Valor 10	**6.2**
Valor 11	**6.0**
Valor 12	**5.8**
Valor 13	**6.2**
Valor 14	**5.9**
Valor 15	**5.9**
Valor 16	**5.7**
Valor 17	**6.1**
Valor 18	**6.1**
Valor 19	**5.7**
Valor 20	**6.0**
Valor 21	**6.0**
Valor 22	**6.3**
Valor 23	**5.8**
Valor 24	**6.0**
Valor 25	**5.7**
Valor 26	**6.2**
Valor 27	**6.3**
Valor 28	**6.2**
Valor 29	**6.2**
Valor 30	**6.0**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{\sum_{i=1}^{n} AtDoS_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ DoS = \frac{6{,}1 + 5{,}6 + \cdots 6{,}2 + 6{,}0}{30} = \frac{180}{30} = 6$$

Obteniendo que en promedio el tiempo de éxito del ataque DoS en el protocolo WPA3 fueron 6 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo.

Tabla 34.
Tiempo de éxito ante el ataque DoS de los protocolos de seguridad Wi-Fi.

Protocolos Wi-Fi	**WPA**	**WPA2**	**WPA3**
DoS	3,4min	4min	6min

Fuente: Elaboración Propia.

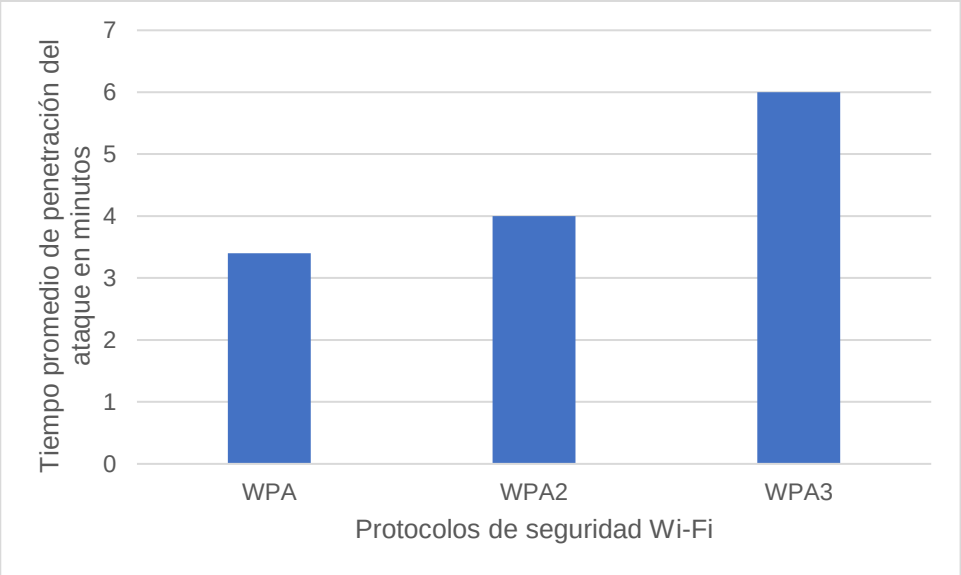


Figura 23: Tiempo de éxito ante el ataque DoS de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

INDICADOR DE AUTENTICACIÓN

Ataque de fuerza bruta (Aircrack-ng)

Ataque de fuerza bruta (Aircrack-ng) en Protocolo WPA

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 33.
Tiempos de éxito de ataque de fuerza bruta con el protocolo WPA.

Valor 1	**5.2**
Valor 2	**5.5**
Valor 3	**5.4**
Valor 4	**5.4**
Valor 5	**5.3**
Valor 6	**5.7**
Valor 7	**5.5**
Valor 8	**5.4**
Valor 9	**5.2**
Valor 10	**5.4**
Valor 11	**5.6**
Valor 12	**5.3**
Valor 13	**5.3**
Valor 14	**5.3**
Valor 15	**5.5**
Valor 16	**5.4**
Valor 17	**5.2**
Valor 18	**5.3**
Valor 19	**5.6**
Valor 20	**5.6**
Valor 21	**5.6**
Valor 22	**5.3**
Valor 23	**5.4**
Valor 24	**5.7**
Valor 25	**5.5**
Valor 26	**5.4**
Valor 27	**5.2**
Valor 28	**5.3**
Valor 29	**5.2**
Valor 30	**5.3**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{\sum_{i=1}^{n} AtBrut_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{5{,}2 + 5{,}5 + \cdots 5{,}2 + 5{,}3}{30}$$
$$= \frac{162}{30} = 5{,}4$$

Obteniendo que en promedio el tiempo de éxito del ataque de fuerza bruta en el protocolo WPA fueron 5,4 minutos.

Ataque de fuerza bruta (Aircrack-ng) en Protocolo WPA2

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 34.
Tiempos de éxito de ataque de fuerza bruta con el protocolo WPA2.

Valor 1	**6.4**
Valor 2	**6.3**
Valor 3	**6.3**
Valor 4	**6.7**
Valor 5	**6.4**
Valor 6	**6.5**
Valor 7	**6.5**
Valor 8	**6.7**
Valor 9	**6.5**
Valor 10	**6.4**
Valor 11	**6.6**
Valor 12	**6.4**
Valor 13	**6.5**
Valor 14	**6.7**
Valor 15	**6.4**
Valor 16	**6.3**
Valor 17	**6.6**
Valor 18	**6.6**
Valor 19	**6.8**
Valor 20	**6.4**
Valor 21	**6.8**
Valor 22	**6.3**
Valor 23	**6.2**
Valor 24	**6.4**
Valor 25	**6.8**
Valor 26	**6.8**
Valor 27	**6.3**
Valor 28	**6.3**
Valor 29	**6.5**
Valor 30	**6.8**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{\sum_{i=1}^{n} AtBrut_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{6{,}4 + 6{,}3 + \cdots 6{,}5 + 6{,}8}{30}$$

$$= \frac{195}{30} = 6{,}5$$

Obteniendo que en promedio el tiempo de éxito del ataque de fuerza bruta en el protocolo WPA2 fueron 6,5 minutos.

Ataque de fuerza bruta (Aircrack-ng) en Protocolo WPA3

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 35.
Tiempos de éxito de ataque de fuerza bruta con el protocolo WPA3.

Valor 1	**15.7**
Valor 2	**15.7**
Valor 3	**15.8**
Valor 4	**15.2**
Valor 5	**15.5**
Valor 6	**15.4**
Valor 7	**15.6**
Valor 8	**15.8**
Valor 9	**15.7**
Valor 10	**15.4**
Valor 11	**15.4**
Valor 12	**15.5**
Valor 13	**15.5**
Valor 14	**15.6**
Valor 15	**15.6**
Valor 16	**15.5**
Valor 17	**15.7**
Valor 18	**15.4**
Valor 19	**15.3**
Valor 20	**15.3**
Valor 21	**15.2**
Valor 22	**15.3**
Valor 23	**15.4**
Valor 24	**15.3**
Valor 25	**15.8**
Valor 26	**15.4**
Valor 27	**15.5**

Valor 28	**15.6**
Valor 29	**15.3**
Valor 30	**15.4**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{\sum_{i=1}^{n} AtBrut_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ fuerza\ bruta = \frac{15{,}7 + 15{,}7 + \cdots 15{,}3 + 15{,}4}{30}$$

$$= \frac{465}{30} = 15{,}5$$

Obteniendo que en promedio el tiempo de éxito del ataque de fuerza bruta en el protocolo WPA3 fueron 15,5 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo:

Tabla 36.
Tiempo de éxito ante el ataque de fuerza bruta de los protocolos de seguridad Wi-Fi.

Protocolos Wi-Fi	**WPA**	**WPA2**	**WPA3**
Ataque de fuerza bruta	5,4min	6,5min	15,5min

Fuente: Elaboración propia.

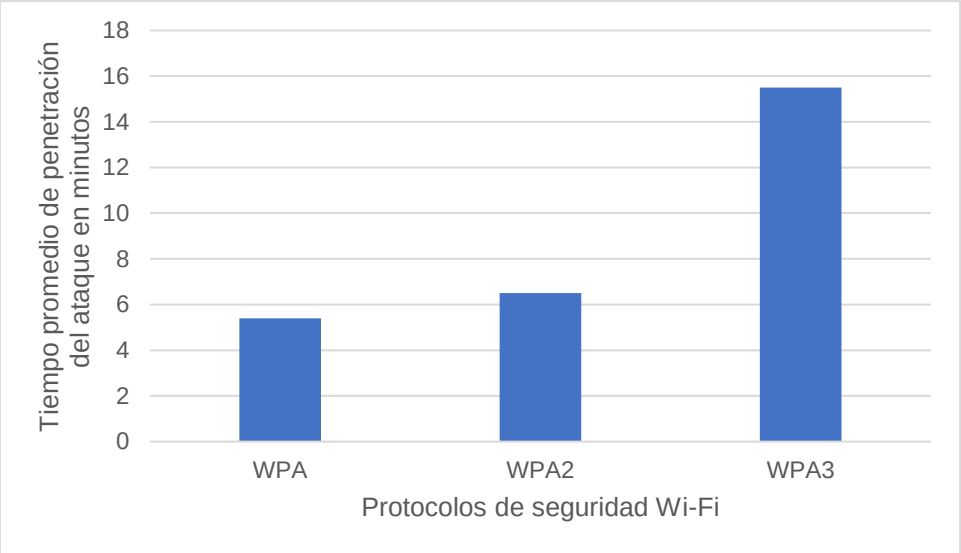


Figura 24: Tiempo de éxito ante el ataque de fuerza bruta de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

Ataque de diccionario a un ssid oculto

Ataque de diccionario a un ssid oculto en Protocolo WPA

Con respecto al protocolo WPA se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 37.
Tiempos de éxito de ataque de diccionario con el protocolo WPA.

Valor 1	**3.3**
Valor 2	**3.3**
Valor 3	**2.9**
Valor 4	**2.9**
Valor 5	**2.9**
Valor 6	**2.8**
Valor 7	**3.3**
Valor 8	**3.2**
Valor 9	**2.9**
Valor 10	**2.7**
Valor 11	**2.9**
Valor 12	**3.2**
Valor 13	**3.0**
Valor 14	**3.0**
Valor 15	**2.8**
Valor 16	**2.9**
Valor 17	**3.2**
Valor 18	**2.8**
Valor 19	**3.0**
Valor 20	**3.1**
Valor 21	**3.0**
Valor 22	**3.1**
Valor 23	**3.2**
Valor 24	**2.9**
Valor 25	**2.9**
Valor 26	**3.0**
Valor 27	**3.1**
Valor 28	**3.1**
Valor 29	**2.9**
Valor 30	**2.7**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{\sum_{i=1}^{n} AtDiccio_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{3{,}3 + 3{,}3 + \cdots 2{,}9 + 2{,}7}{30}$$
$$= \frac{90}{30} = 3$$

Obteniendo que en promedio el tiempo de éxito del ataque de diccionario en el protocolo WPA fueron 3 minutos.

Ataque de diccionario a un ssid oculto en Protocolo WPA2

Con respecto al protocolo WPA2 se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 38.
Tiempos de éxito de ataque de diccionario con el protocolo WPA2.

Valor 1	**5.1**
Valor 2	**5.2**
Valor 3	**5.2**
Valor 4	**4.9**
Valor 5	**5.1**
Valor 6	**5.0**
Valor 7	**5.0**
Valor 8	**5.3**
Valor 9	**4.9**
Valor 10	**5.2**
Valor 11	**5.1**
Valor 12	**5.0**
Valor 13	**5.3**
Valor 14	**5.2**
Valor 15	**5.0**
Valor 16	**5.0**
Valor 17	**5.2**
Valor 18	**4.9**
Valor 19	**5.1**
Valor 20	**5.2**
Valor 21	**5.4**
Valor 22	**5.0**
Valor 23	**5.3**
Valor 24	**5.0**
Valor 25	**5.2**
Valor 26	**4.9**
Valor 27	**5.1**
Valor 28	**5.1**
Valor 29	**5.0**
Valor 30	**5.0**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA2, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{\sum_{i=1}^{n} AtDiccio_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{5{,}1 + 5{,}2 + \cdots 5{,}0 + 5{,}0}{30}$$

$$= \frac{153}{30} = 5{,}1$$

Obteniendo que en promedio el tiempo de éxito del ataque de diccionario en el protocolo WPA2 fueron 5,1 minutos.

Ataque de diccionario a un ssid oculto en Protocolo WPA3

Con respecto al protocolo WPA3 se obtuvieron los siguientes tiempos de éxito del ataque:

Tabla 39.
Tiempos de éxito de ataque de diccionario con el protocolo WPA3.

Valor 1	**8.5**
Valor 2	**8.3**
Valor 3	**8.7**
Valor 4	**8.4**
Valor 5	**8.7**
Valor 6	**8.4**
Valor 7	**8.4**
Valor 8	**8.5**
Valor 9	**8.3**
Valor 10	**8.3**
Valor 11	**8.7**
Valor 12	**8.3**
Valor 13	**8.7**
Valor 14	**8.7**
Valor 15	**8.6**
Valor 16	**8.6**
Valor 17	**8.4**
Valor 18	**8.7**
Valor 19	**8.5**
Valor 20	**8.4**
Valor 21	**8.3**
Valor 22	**8.4**
Valor 23	**8.8**
Valor 24	**8.4**
Valor 25	**8.8**
Valor 26	**8.5**
Valor 27	**8.5**

Valor 28	**8.3**
Valor 29	**8.3**
Valor 30	**8.5**

Fuente: Elaboración Propia.

Luego de hacer los 30 intentos por cada ataque con el protocolo WPA3, se procede a realizar un promedio de dichos tiempos utilizando la siguiente fórmula:

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{\sum_{i=1}^{n} AtDiccio_i}{n}$$

$$Promedio\ de\ tiempo\ de\ éxito\ ataque\ de\ diccionario = \frac{8{,}5 + 8{,}3 + \cdots 8{,}3 + 8{,}5}{30}$$

$$= \frac{255}{30} = 8{,}5$$

Obteniendo que en promedio el tiempo de éxito del ataque de diccionario en el protocolo WPA3 fueron 8,5 minutos.

Luego procedemos a comparar los tiempos de éxito en promedio con cada protocolo:

Tabla 40.
Tiempo de éxito ante el ataque de diccionario de los protocolos de seguridad Wi-Fi.

Protocolos Wi-Fi	**WPA**	**WPA2**	**WPA3**
Ataque de diccionario	3min	5,1min	8,5min

Fuente: Elaboración Propia.

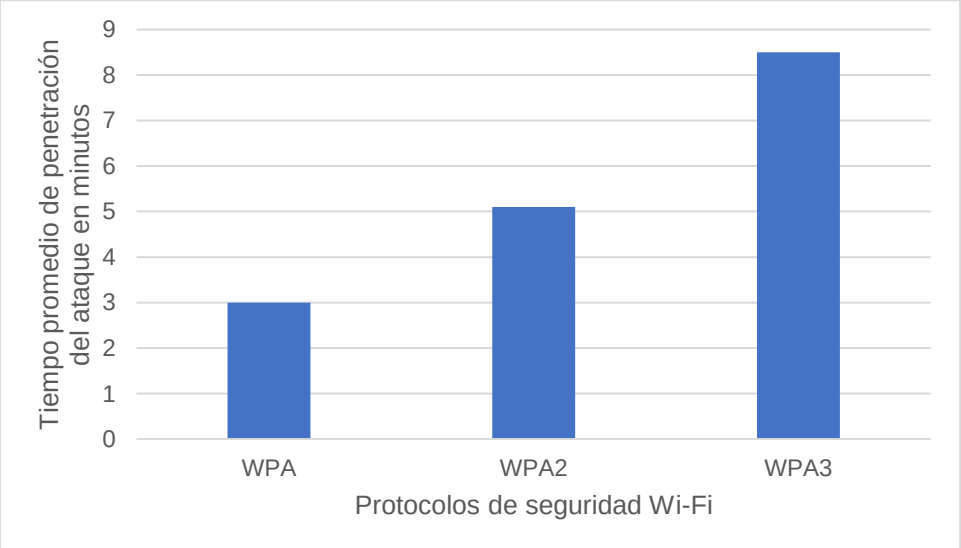


Figura 25: Tiempo de éxito ante el ataque de fuerza bruta de los protocolos de seguridad Wi-Fi. Fuente: Elaboración Propia.

Luego de confrontar a los protocolos con los ataques informáticos procedemos a ingresarlos en la siguiente tabla:

Tabla 41.
Subtotales del Análisis de la Variable Independiente.

Dimensiones	Indicadores	WPA	WPA2	WPA3
Confidencialidad	Promedio de tiempo de éxito de ataque **Phishing**	8min	12 min	23,2min
	Promedio de tiempo de éxito de ataque **Man in the Middle**	3min	3,5min	4,4 min
	Promedio de tiempo de éxito de ataque **ARP Spoofing + DNS Spoofing**	2min	2,4min	3,3min
Integridad	Promedio de tiempo de éxito de ataque de DoS	3.4min	4 min	6min
Autenticación	Promedio de tiempo de éxito de ataque **de fuerza bruta**	5.4min	6.5min	15.5min
	Promedio de tiempo de éxito de Ataque de diccionario **a un ssid oculto**	3 min	5.10min	8.5 min
RESULTADOS TOTALES		24,8min	**33,4min**	**60,9min**

Fuente: Elaboración propia.

Tabla 42.
Sumatoria de Análisis de la Variable dependiente.

DIMENSIONES	WPA	WPA2	WPA3
Confidencialidad	13	17,9	30,9
Integridad	3,4	4	6
Autentificación	8,4	11,5	24
RESULTADOS TOTALES	24,8	33,4	60,9

Fuente: Elaboración propia.

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador) Entonces:

PT= 30,9 + 6 + 24 =60,9

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW) = (PT_PW / PT) *100%

Tabla 43.
Porcentaje Total de Cada Protocolo Analizado.

WPA	WPA2	WPA3
40,72%	54,84%	100%

Fuente: Elaboración propia.

Tabla 44.
Porcentaje por Protocolo de Variable dependiente.

INDICES	WPA	WPA2	WPA3
PT_PW	24,8	33,4	60,9
PT	60,9	60,9	60,9
PORCENTAJE POR PROTOCOLO	40,72	54,84	100

Fuente: Elaboración propia.

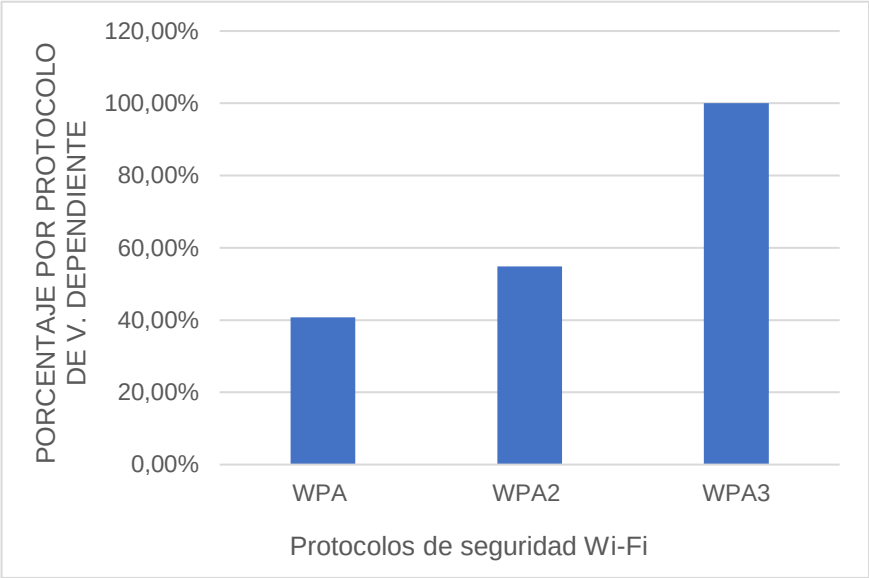


Figura 26: Porcentaje por Protocolo de Variable dependiente.
Fuente: Elaboración propia.

3.2. Discusión de resultados.

WPA mitigan de forma directa los ataques mencionados anteriormente no obstante cabe indicar que WPA en cualquiera de sus variantes sigue siendo vulnerable a ataques de contraseñas a causa de que el algoritmo de cifrado ha sido vulnerado al ataque de denegación de servicios DoS.

WPA2 al igual que su antecesor mitiga los ataques de forma directa debido a que hace uso de un mejor algoritmo de encriptación. WP3 por su parte proporciona mayor protección ante ataques, incluso cuando no se cuenta con una contraseña fuerte, además que tiene un cifrado de tráfico entre dispositivos y puntos de acceso, de manera que intensifica la protección en redes públicas. Dicho cifrado de 192 bits para redes empresariales o personales, es importante para cuándo donde se traten datos confidenciales. Además, cuenta con una configuración más amable y simplificada para el emparejamiento de dispositivos. Los tiempos de éxito de ataque además son mucho mayores en todos los ataques cuando se confrontan con WPA3, puesto que si bien los protocolos no protegen al 100% de dichos ataques, se recomiendan tomar en cuenta recomendaciones adicionales tales como: **Rotación de la contraseña WiFi**: Tanto si se usa una contraseña WiFi a nivel doméstico, como a nivel empresarial, las contraseñas se deben cambiar periódicamente. **Deshabilitar TKIP**: Su uso está desaconsejado en la actualidad y se debería deshabilitar. Si

es estrictamente necesario se puede mantener haciendo uso de contraseñas seguras de al menos 12 caracteres. **Medir la propagación de la señal:** Para mejorar la cobertura WiFi y para evitar que la señal inalámbrica salga del perímetro, se puede usar un software de site survey como Acrylic WiFi Heatmaps para medir la cobertura.

3.3. Aporte práctico.

Selección de los protocolos de seguridad Wi-Fi existentes para combatir las vulnerabilidades en redes inalámbricas.

Desde los primeros días de su adopción, las redes inalámbricas se han considerado inseguras, a diferencia de las cableadas. Para hacer que las redes inalámbricas sean más seguras y efectivas, se han desarrollado y actualizado protocolos de seguridad Wi-Fi para compensar las fallas de seguridad. El presente trabajo ha optado por seleccionar el total de protocolos de seguridad de Wi-Fi, a saber, WPA, WPA2 y WPA3, y realizó una evaluación de estos para permitir a los usuarios obtener una comprensión profunda de la seguridad de Wi-Fi al elegir dispositivos inalámbricos.

Si inicia sesión en su enrutador inalámbrico o punto de acceso y verifica la sección de seguridad inalámbrica, generalmente presentará cuatro opciones de protocolos de seguridad Wi-Fi: Acceso protegido Wi-Fi (WPA), Wi-Fi Acceso protegido versión 2 (WPA2) y acceso protegido Wi-Fi versión 3 (WPA3), como se indicará a continuación:

WPA: mejora temporal para WEP

En 2003, a medida que WEP se fue haciendo más débil, WPA fue adoptado por Wi-Fi Alliance como una alternativa para WEP. La tecnología de cifrado de 256 bits se introdujo en WPA, que es un aumento obvio en comparación con el cifrado de 64 y 128 bits del sistema WEP. En el estándar WPA, existe una diversidad entre los dos modos: WPA-Enterprise y WPA-Personal, que utilizan diferentes métodos de cifrado. WPA-Personal es un método común para proteger redes inalámbricas y es adecuado para la mayoría de las redes

domésticas. WPA-Enterprise proporciona la seguridad necesaria para las redes inalámbricas en entornos empresariales donde se implementa un servidor RADIUS.

WPA2: mejora basada en WPA

WPA2 fue ratificado como el nuevo estándar de seguridad Wi-Fi en 2004. La mejora más significativa en el estándar de seguridad WPA2 es la implementación del Estándar de cifrado avanzado (AES), que proporciona mayor seguridad y rendimiento. Todavía existe una vulnerabilidad que trae problemas de seguridad porque un pirata informático puede obtener acceso a una red WPA2 segura y obtener acceso a ciertas claves para atacar otros dispositivos en la misma red. Es un problema de seguridad que importa para las redes empresariales, en lugar de para los usuarios de la red doméstica.

WPA3: la seguridad Wi-Fi de próxima generación

Con el objetivo de "simplificar la seguridad de Wi-Fi, permitir una autenticación más sólida y ofrecer una mayor capacidad criptográfica para mercados de datos altamente sensibles", WPA3 fue propuesto por Wi-Fi Alliance en junio de 2018. La llegada de WPA3 corrige la protección contra las fallas en WPA2 como ataques de diccionario. Para redes públicas como cafeterías u hoteles, WPA3 tiene una seguridad realmente buena porque encriptará automáticamente la conexión sin necesidad de credenciales.

En el siguiente cuadro comparativo se mostrarán las cuatro generaciones de protocolos de seguridad Wi-Fi en todos los aspectos de forma sucinta:

Tabla 45.

Comparación rápida de protocolos: WPA vs. WPA2 vs. WPA3.

	WPA	**WPA2**	**WPA3**
Año de lanzamiento	2003	2004	2018
Método de cifrado	Protocolo de integridad de clave temporal(TKIP) con RC4	CCMP and Advanced Encryption Standard	Advanced Encryption Standard(AES)
Tamaño de la clave de sesión	128-bit	128-bit	128-bit(WPA3-Personal) 192-bit(WPA3-Enterprise)
Tipo de cifrado	Flujo	Bloque	Bloque
Integridad de los datos	Message Integrity code	CBC-MAC	Secure Hash Algorithm
Gestión de claves	Mecanismo 4-way handshaking	Mecanismo 4-way handshaking	Autenticación simultánea de Equals handshark
Autenticación	Pre-Shared Key (PSK) & 802.1x With EAP variant	Pre-Shared Key (PSK) & 802.1x With EAP variant	Autenticación simultánea de Equals(SAE) & 802.1x with EAP variant

Fuente: Elaboración Propia.

Además, se indica información adicional a tomar en cuenta sobre las diferencias y comparativa entre los protocolos de seguridad:

- En cuanto al método de cifrado, WPA todavía utiliza el cifrado de flujo RC4 inseguro de WEP, pero proporciona seguridad adicional a través de TKIP. Mientras que WEP y WPA usaban cifrado RC4, WPA2 usa el algoritmo de cifrado AES-CCMP más fuerte, al igual que WPA3. AES se ha implementado para proteger el tráfico diario de Internet, así como ciertos niveles de información clasificada en el gobierno de los EE. UU.
- Se genera una clave de sesión durante el proceso de protocolo de enlace SSL cada vez que alguien se conecta al sitio web. Las claves de sesión suelen estar entre 40 y 256 bits. El número indica el tamaño de la llave. Una clave más grande tiene más combinaciones posibles.
- Y a diferencia de WPA y WPA2 que utiliza un protocolo de enlace de 4 vías imperfecto para habilitar las conexiones inalámbricas, que es la fuente de la vulnerabilidad KRACK, el protocolo de enlace de autenticación simultánea de iguales en WPA3 autentica correctamente un dispositivo en una red para proteger las conexiones contra ataques.
- WPA3 reemplaza PSK con SAE, una forma más segura de realizar el intercambio de claves inicial. Al mismo tiempo, el tamaño de la clave de sesión de WPA3 aumenta a 128 bits en el modo WPA3-Personal y a 192 bits en WPA3-Enterprise, lo que hace que la contraseña sea más difícil de descifrar que los estándares de seguridad Wi-Fi anteriores.

DISEÑO DE UN ESCENARIO DE PRUEBAS

Escenario de pruebas

Para este escenario de pruebas, se contemplan los protocolos de seguridad: WPA, WPA2 y WPA3. La autenticación la realiza el mismo mecanismo de cifrado.

Software y hardware requerido:

Para este escenario se considera el uso de una computadora portátil (laptop), que actúa como cliente usuario, la misma que se enlaza a un punto de acceso (D-Link), el cual soporta los protocolos de seguridad descritos en este escenario. También se cuenta con otra computadora portátil, en la cual se conecta una antena adaptador USB Wi- Fi marca Alfa Networks modelo WUSB600N para una mejor recepción de señales Wi-Fi, que hacen las veces de atacante, para realizar las pruebas de intrusión y craqueo. El software de auditoría, escaneo y ruptura estarán instalados en esta última portátil.

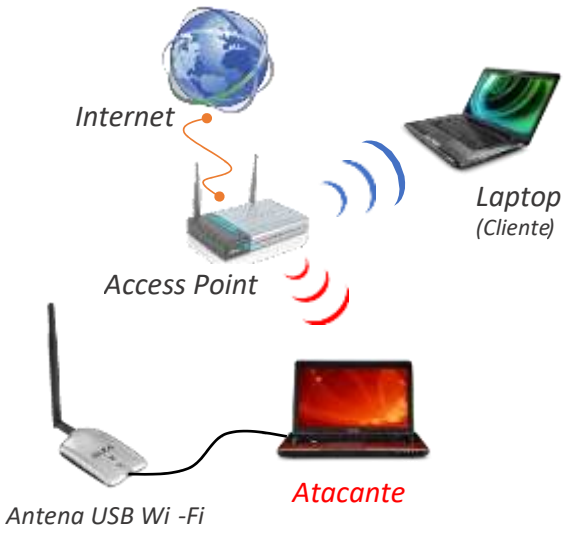


Figura 27: Escenario de pruebas. Fuente: (Tafur & Chavez, 2018)

Software utilizado: Kali Linux

Kali Linux es una distribución de Linux derivada de Debian mantenida por Offensive Security. Fue desarrollado por Mati Aharoni y Devon Kearns. Kali Linux es un sistema operativo especialmente diseñado para analistas de redes, probadores de penetración o, en palabras simples, es para aquellos que trabajan bajo el paraguas de la ciberseguridad y el análisis. El sitio web oficial de Kali Linux es Kali.org. Ganó popularidad cuando prácticamente se usó en Mr. Robot Series. No fue diseñado para fines generales, se supone que debe ser utilizado por profesionales o por aquellos que saben cómo operar Linux / Kali. Para saber cómo instalar Kali Linux consulte su documentación oficial (Geeksforgeeks, 2021).

Ventajas:

- Tiene más de 600 herramientas de seguridad de red y pruebas de penetración preinstaladas.
- Es completamente gratuito y de código abierto. Para que puedas usarlo gratis e incluso contribuir a su desarrollo.
- Es compatible con muchos idiomas.
- Genial para aquellos que son intermedios en Linux y tienen sus manos en los comandos de Linux.
- Se puede usar fácilmente con Rasberry Pi.

Desventajas:

- No se recomienda para aquellos que son nuevos en Linux y quieren aprender Linux (ya que está orientado a la penetración)
- Es un poco más lento.
- Es posible que algunos programas no funcionen correctamente.

Kali Linux debe ser utilizado por aquellos que son probadores de penetración profesionales, expertos en ciberseguridad, piratas informáticos éticos o aquellos que saben cómo operarlo. En palabras simples, si sabe cómo usar Linux y sus comandos de terminal, arquitectura, sistema y administración de archivos, entonces está listo para usar Kali Linux. Y si no es así, le recomendamos que primero comience con la distribución de Ubuntu y obtenga Linux y, después de practicar suficiente, podría probar Kali Linux. Esto no solo le ahorrará tiempo de búsqueda

en Internet, sino que también le permitirá usarlo con facilidad. Sin embargo, si es un probador de penetración profesional o está estudiando pruebas de penetración, no hay mejor conjunto de herramientas que Kali Linux.

Wifislax

Wifislax es un sistema operativo de distribución (SO) Linux basado en Slackware. Está diseñado para pruebas de penetración en Wi-Fi y para la práctica de piratería ética. Contiene una variedad de herramientas de pentesting Wi-Fi como Fluxion, Kismet, Aircarck, Airgeddon, MITM y muchas otras herramientas (Raza, 2018).

Puede romper redes Wi-Fi protegidas por WEP, WPA, WPA2. Tiene una interfaz de línea de comandos. WPA Security es difícil de descifrar, pero aún es posible. Las redes WEP son muy fáciles de descifrar. Es por eso que, hoy en día, todos los Wi-Fi son compatibles con WPA.

Este sistema operativo es legal cuando lo usa White Hat Hacker, pero cuando un Black Hat Hacker lo usa, definitivamente hace cosas ilegales en él.

Ettercap

Ettercap es una herramienta creada por Alberto Ornaghi (ALoR) y Marco Valleri (NaGA) y es básicamente una suite para ataques man in the middle en una LAN. Para aquellos a los que no les gusta la interfaz Command ike (CLI), se proporciona una interfaz gráfica sencilla (Openmaniak, 2008).

Ettercap es capaz de realizar ataques contra el protocolo ARP posicionándose como "man in the middle" y, una vez posicionado así, es capaz de:

- Infectar, reemplazar, borrar datos en una conexión.
- Descubrir contraseñas para protocolos como FTP, HTTP, POP, SSH1.
- Proporcione certificados SSL falsos en las secciones HTTPS a las víctimas.

Airmon-ng

Este script se puede utilizar para habilitar el modo de monitor en interfaces inalámbricas. También se puede usar para volver del modo de monitor al modo administrado. Al ingresar el comando airmon-ng sin parámetros, se mostrará el estado de las interfaces (KALITOOLS, 2016).

uso: airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>

Dónde:

- <start | stop> indica si desea iniciar o detener la interfaz. (Obligatorio)

- <interface> especifica la interfaz. (Obligatorio)
- [canal] configura opcionalmente la tarjeta en un canal específico.
- <check | check kill> " check " mostrará cualquier proceso que pueda interferir con la suite aircrack-ng. Se recomienda encarecidamente que estos procesos se eliminen antes de utilizar la suite aircrack-ng. "Check kill " comprobará y eliminará los procesos que puedan interferir con la suite aircrack-ng.

Aircrack-ng

Es un conjunto de herramientas de seguridad de redes inalámbricas. Nos permite monitorear y exportar paquetes de datos, atacar puntos de acceso y clientes, y descifrar claves WEP y WPA. He incluido algunos enlaces en la parte inferior si alguien quiere investigar más sobre la tecnología inalámbrica, RC4 o Aircrack-ng (MCCAULEY, 2018).

Aireplay-ng

Se emplea para generar tráfico inalámbrico no autorizado. Se puede usar junto con aircrack-ng con el fin de descifrar claves WEP y WPA. El propósito principal de aireplay-ng es inyectar marcos. Hay varios tipos diferentes de ataques poderosos que se pueden realizar usando aireplay-ng, como el ataque de desautenticación, que ayuda a capturar datos de protocolo de enlace WPA, o el ataque de autenticación falsa, en el que los paquetes se inyectan en el punto de acceso a la red mediante la autenticación de para crear y capturar nuevos IV (Azad, 2020).

Otros tipos de ataques se incluyen en la siguiente lista:

- Ataque de reproducción de paquete interactivo
- Ataque de reproducción de solicitud ARP
- Ataque chopchop de KoreK
- Ataque de café con leche
- Ataque de fragmentación

Packetforge-ng

Es una herramienta para crear paquetes cifrados que posteriormente se pueden utilizar para inyección. Puede crear varios tipos de paquetes, como solicitudes arp, UDP, ICMP y paquetes personalizados. El uso más común es crear solicitudes ARP

para su posterior inyección. Para crear un paquete cifrado, debe tener un archivo PRGA (algoritmo de generación pseudoaleatorio). Se utiliza para cifrar el paquete que crea. Esto se obtiene típicamente de aireplay-ng chopchop o ataques de fragmentación (Otreppe, 2018).

Selección de los protocolos de seguridad de red y realización de pruebas de ataque con el fin de probar los protocolos de seguridad de red.

- **Instalacion de maquina virtual en VMware-Kali Linux**
  1. Para realizar la instalación de la maquina virtual en VMware es necesario seleccionar el tipo de sistema operativo que se va a instalar. A continuacion se presenta la figura con el sistema operativo que se instaló.

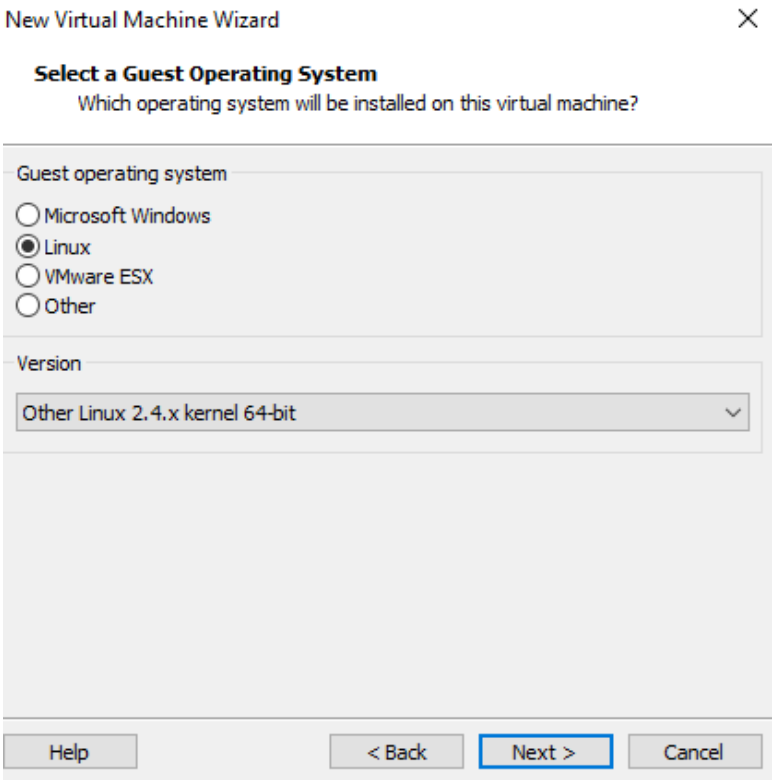


Figura 28: Selección del sistema operativo. Fuente: Elaboración Propia.

  2. Después de seleccionar el sistema operativo se procede a colocar un nombre para la máquina virtual y se escoge la ruta en donde se almacenó. A continuación, se presenta una figura misma que indica el nombre de la máquina y la dirección.

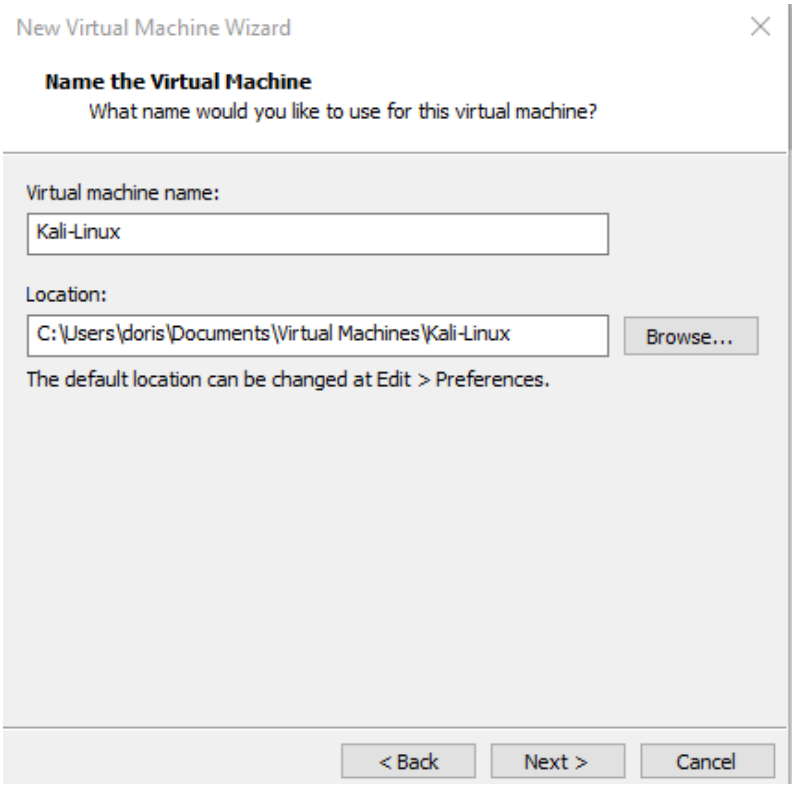


Figura 29: Nombre de la máquina virtual y dirección. Fuente: Elaboración Propia.

3. Es importante agregar espacio en disco que ha tenido la máquina virtual, puesto del espacio que se le asigna a la máquina virtual se obtiene del disco duro físico. En la figura 3 se indica el tamaño de disco que se le asignó a la presente máquina.

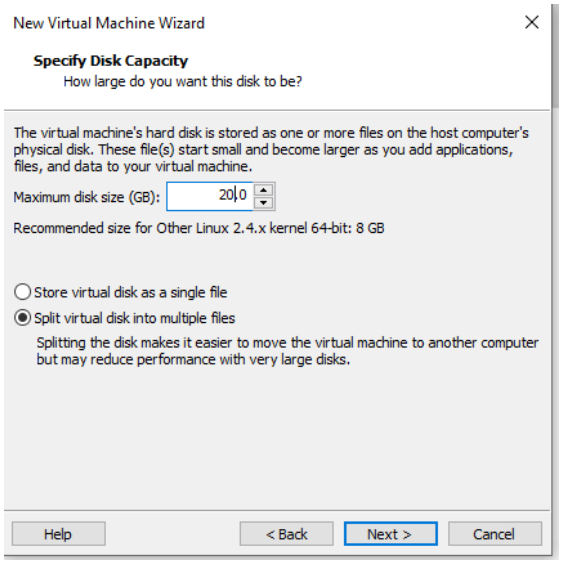


Figura 30: Asignación de espacio a la máquina virtual. Fuente: Elaboración Propia.

4. Es necesario verificar las características de la máquina virtual, para proceder con la instalación del sistema operativo, dentro de la ventana de hardware se selecciona la imagen del sistema que se va a instalar y que se ha descargado con anterioridad. En la figura 4 se visualiza la configuración que tendrá esta máquina.

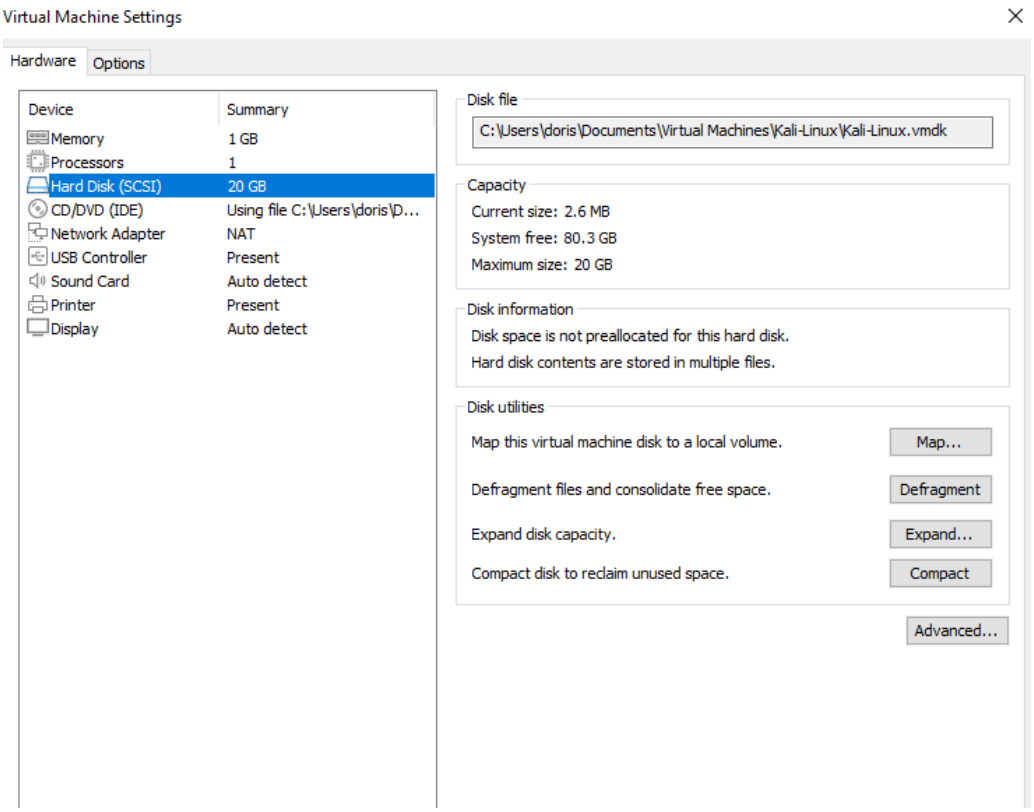


Figura 31: Configuración de la máquina virtual. Fuente: Elaboración Propia.

5. Cuando la configuración de la máquina virtual se encuentre lista se procede con la instalación del sistema operativo, en este caso se está instalando Kali Linux, para ello se han seguido los pasos que se muestran a continuación.
   - Seleccionar **instalación grafica** para poder visualizar una interfaz gráfica.

Figura 32: Instalación en modo grafico. Fuente: Elaboración Propia.

- Seleccionar el idioma de preferencia, en este caso se ha seleccionado idioma inglés.

Figura 33: Selección del idioma. Fuente: Elaboración Propia.

- Escoger el país para el idioma, en este caso se ha optado por seleccionar Estados Unidos.

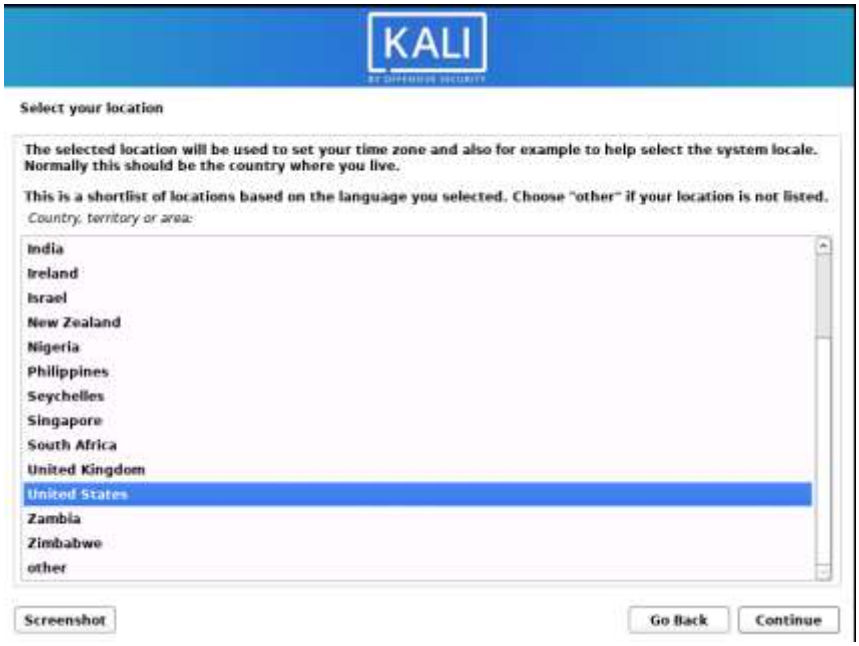


Figura 34: Elección de la localización. Fuente: Elaboración Propia.

- Configurar el idioma del teclado por esta ocasión se ha dejado en inglés.

Figura 35: Configuración del idioma del teclado Fuente: Elaboración Propia.

- Al finalizar la configuración del idioma se procede a realizar la instalación de los componentes tal como se muestra en la figura 30.

Figura 36: Instalación de componentes. Fuente: Elaboración Propia.

- Al finalizar la instalación de los componentes se procede a configurar la red, para ello se coloca un nombre de host o se lo deja con el predeterminado que es el que se muestra en la figura 31.

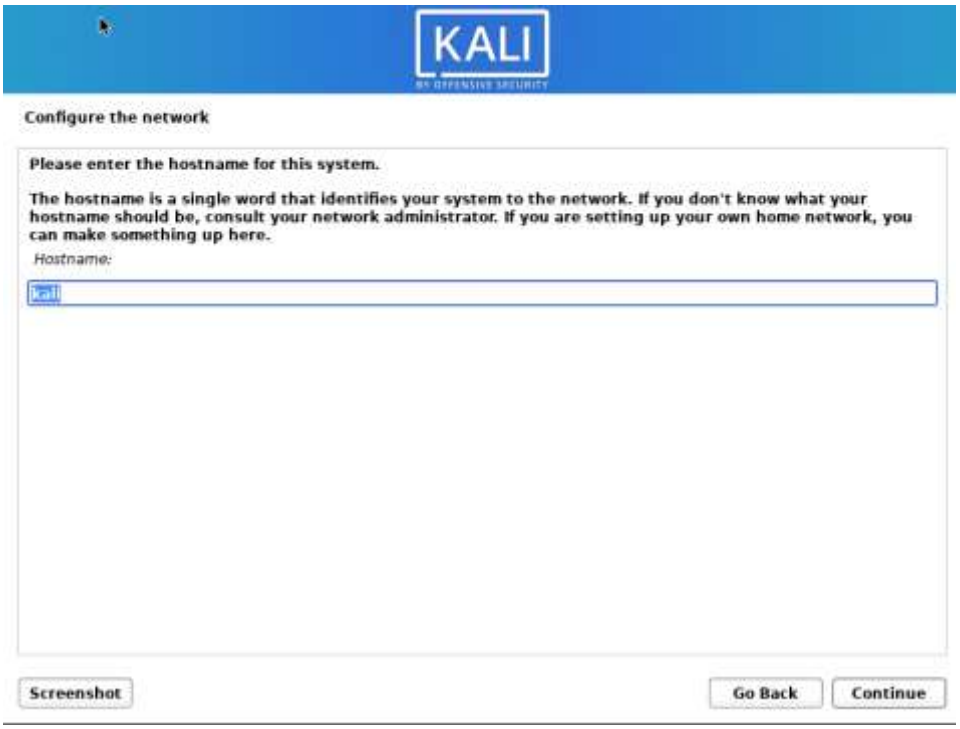


Figura 37: Configuración del hostname. Fuente: Elaboración Propia.

- La configuración de la red requiere un nombre de dominio en caso de no requerirlo para la continuación del proyecto se puede dejar en blanco.

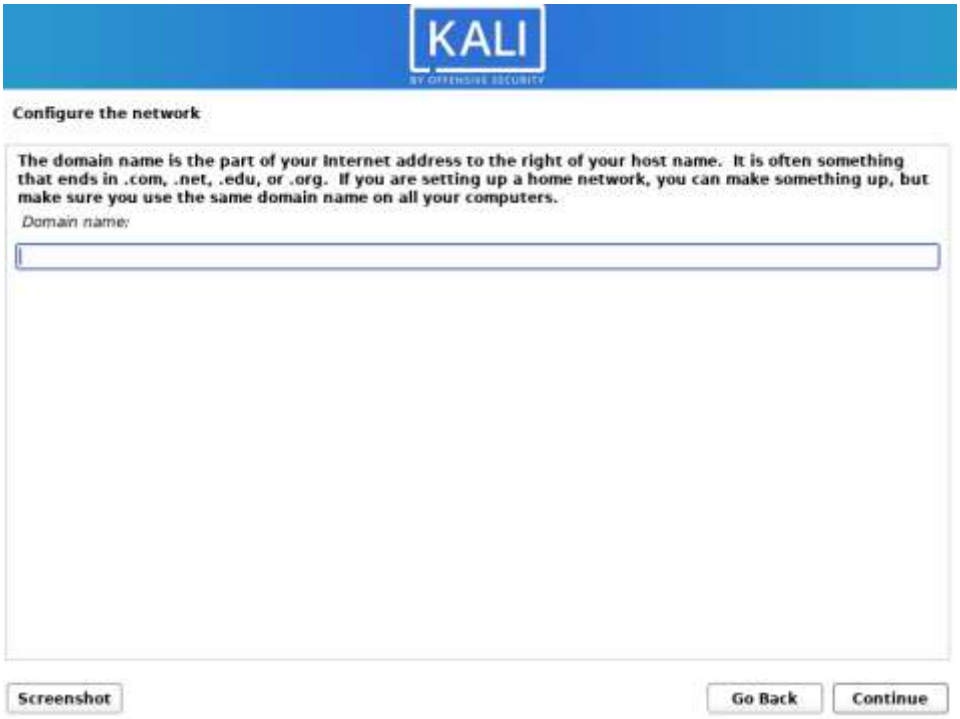


Figura 38: Configuración del dominio. Fuente: Elaboración Propia.

- Al finalizar la configuración de la red es necesario configurar el usuario y contraseña que se utilizó para acceder al sistema operativo, en esta ocasión se ha configurado el usuario como Kali tal como se muestra en la siguiente figura.

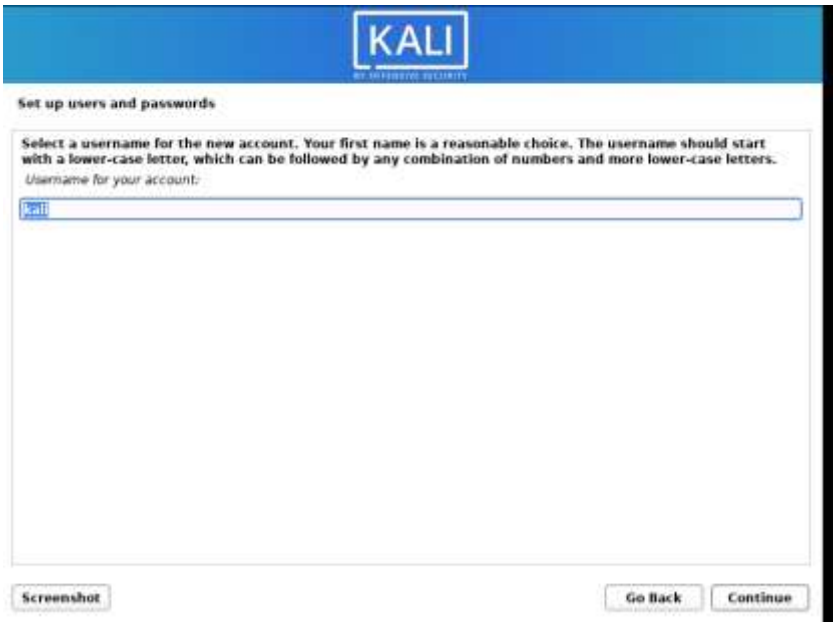


Figura 39: Configuración del usuario. Fuente: Elaboración Propia.

- Es importante asignar una contraseña para el usuario antes configurado.

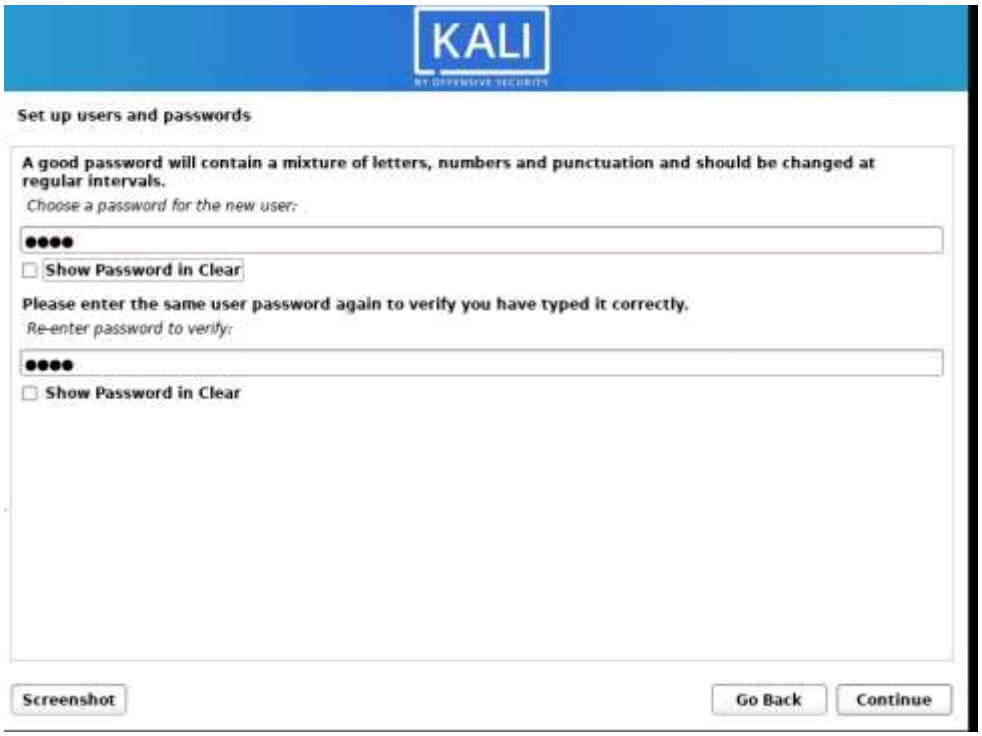


Figura 40: Configuración de contraseña. Fuente: Elaboración Propia.

- Es importante realizar la configuración del horario, en la siguiente figura se indica la configuración que se ha optado por realizar.

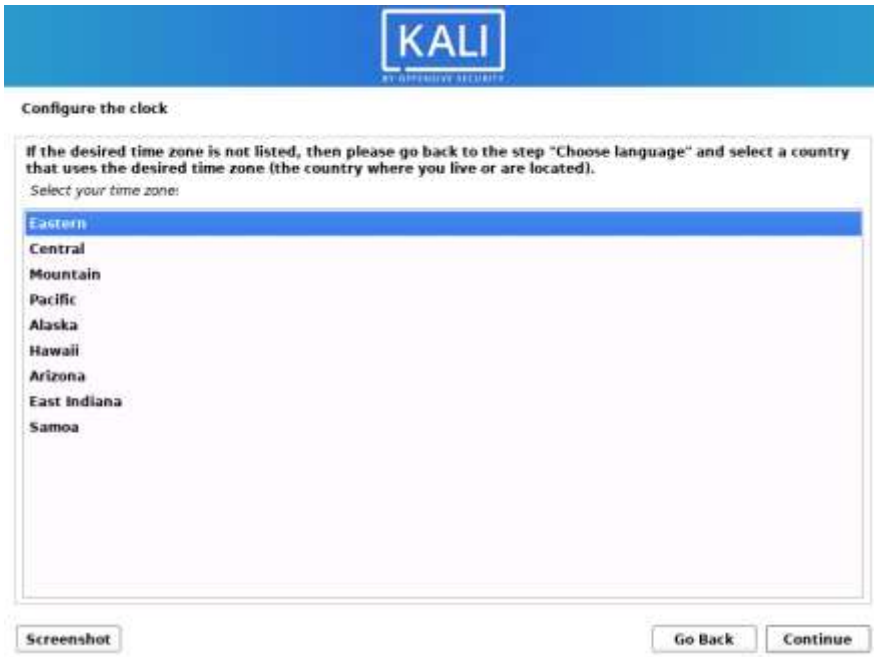


Figura 41: Configuración del reloj. Fuente: Elaboración Propia.

- A continuación se detectó los discos y la particion de cada uno de ellos, en esta ocasión se ha optado por utilizar todo el disco que se había configurado previamente.

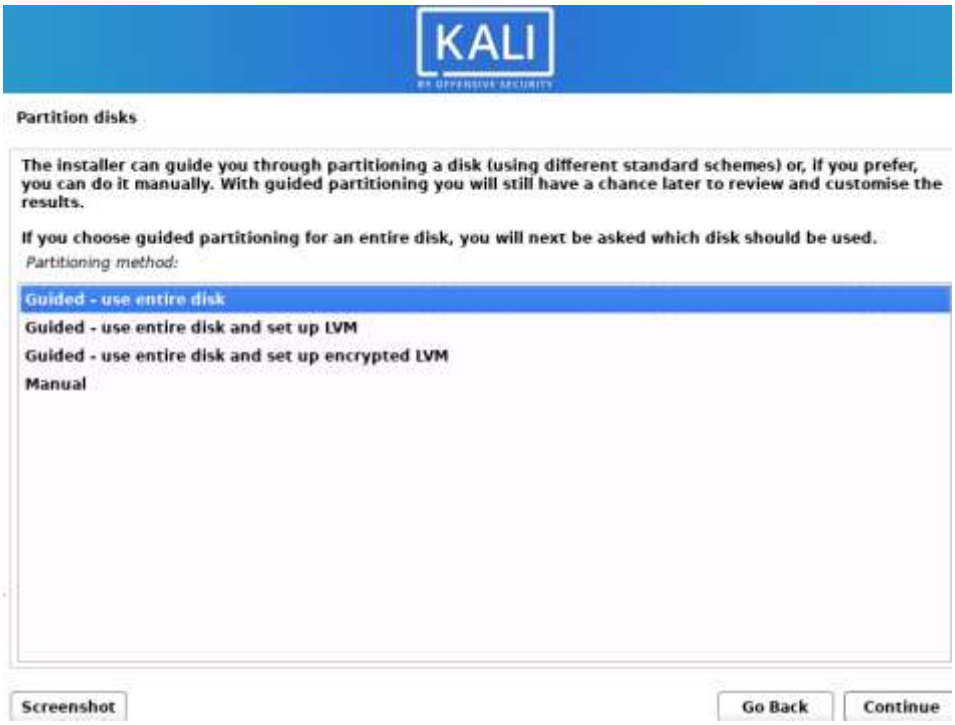


Figura 42: Detección de discos. Fuente: Elaboración Propia.

- Es importante confirmar el disco en el cual se va a instalar el sistema operativo

Figura 43: Confirmación del disco a utilizar. Fuente: Elaboración Propia.

- Luego de finalizar la configuracion del disco en el cual se va a realizar la instalación, se termina con la particion y luego guardar lo cambios del disco tal como se muestra en la siguiente figura.

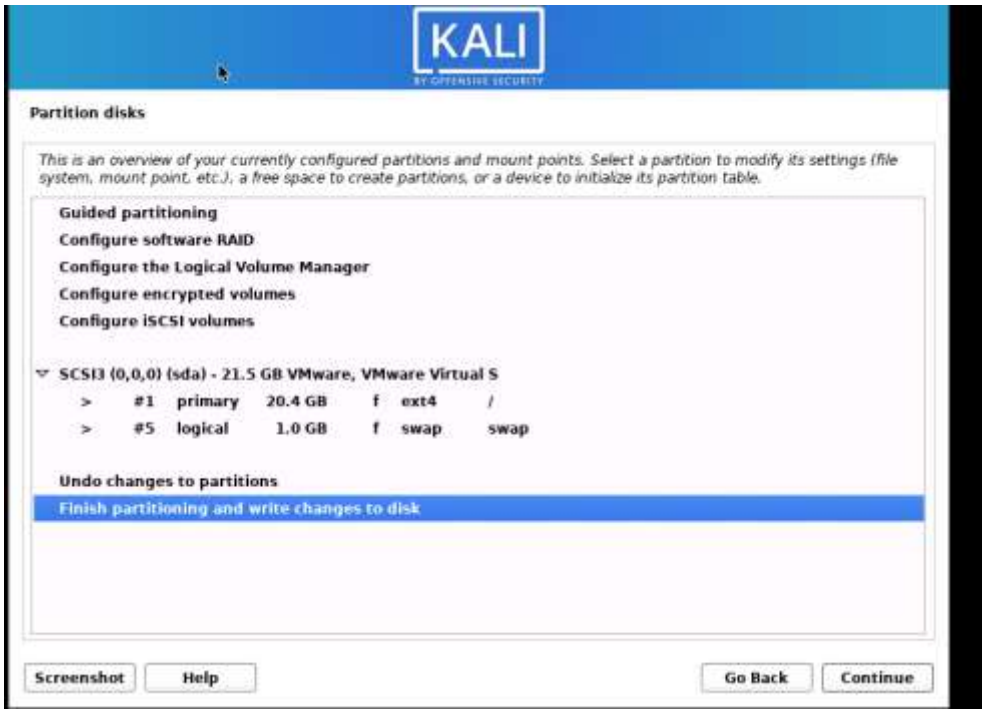


Figura 44: Finalizar y escribir los cambios. Fuente: Elaboración Propia.

- Una vez que los cambios se han escrito correctamente en el disco se procede a confirmarlos.

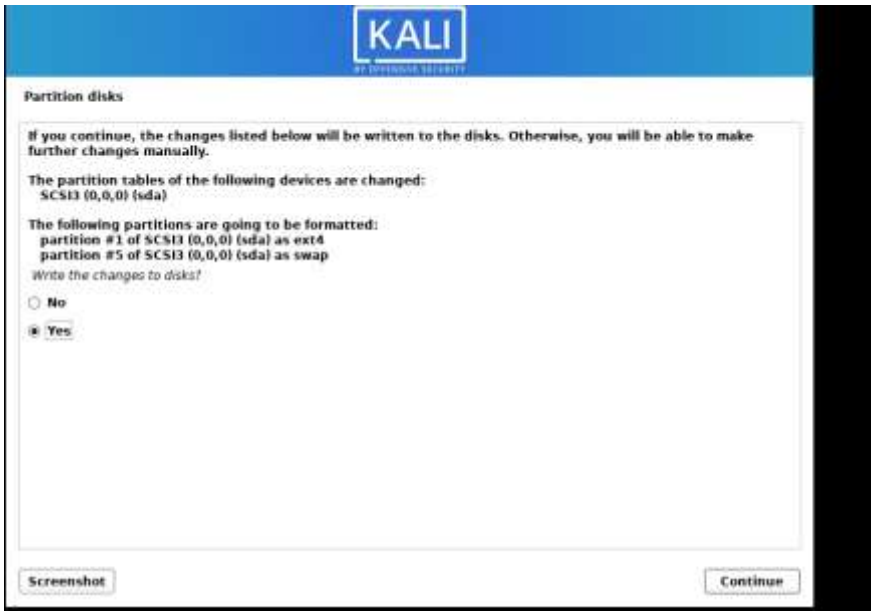


Figura 45: Confirmación de los cambios del disco. Fuente: Elaboración Propia.

- Luego de confirmar los cambios se procedió a realizar la instalación del sistema operativo base.

Figura 46: Instalación del sistema operativo base. Fuente: Elaboración Propia.

- Cuando se ha finalizado la instalación del sistema operativo base se procedió a continuar con las herramientas predeterminadas de kalilinux.

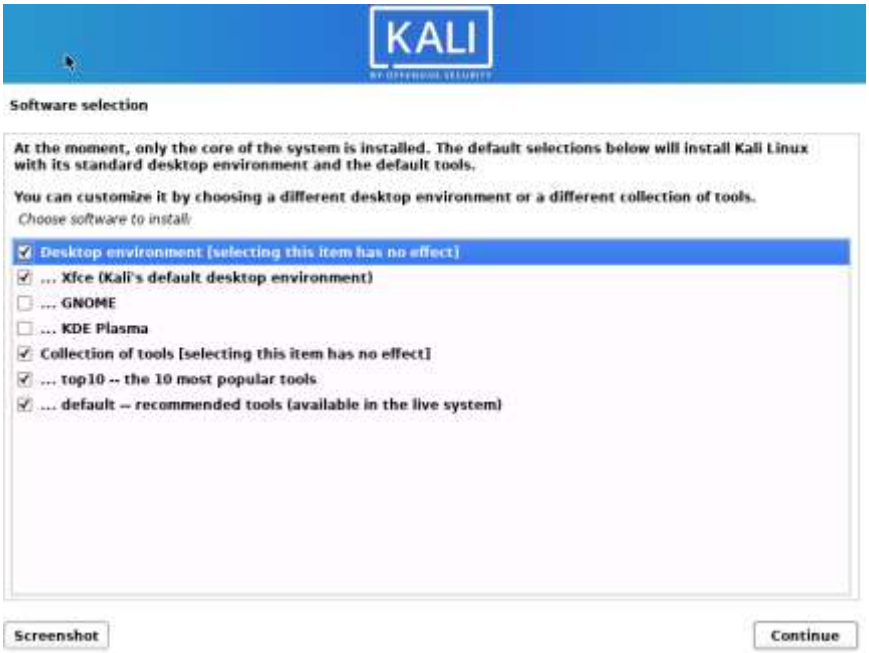


Figura 47: Instalación de las herramientas. Fuente: Elaboración Propia.

- Una vez que se han escogido las herramientas que se desea instalar comenzó la instalación tal como se muestra en la figura 42.

Figura 48: Instalación del software. Fuente: Elaboración Propia.

- Es importante instalar el cargador de arranque ya que es la unidad principal del registro de arranque.

Figura 49: Instalación de la unidad principal. Fuente: Elaboración Propia.

- Ha sido necesario escoger el dispositivo en donde se realizó la instalación de la unidad principal.

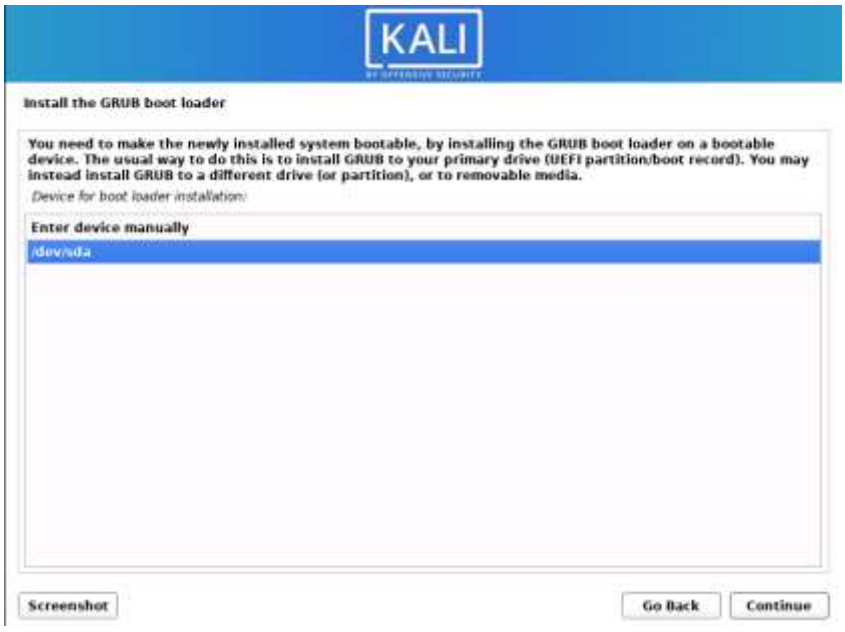


Figura 50: Dispositivo donde se instalará la unidad principal. Fuente: Elaboración Propia.

- Finalmente empezara la última instalación de Kali Linux.

Figura 51: Instalación Final. Fuente: Elaboración Propia.

- Al finalizar la instalación e Kali Linux se presentó una ventana en donde indica que la instalación se ha completado, es necesario dar clic a continuación para que se dé inicio al modo grafico del sistema operativo

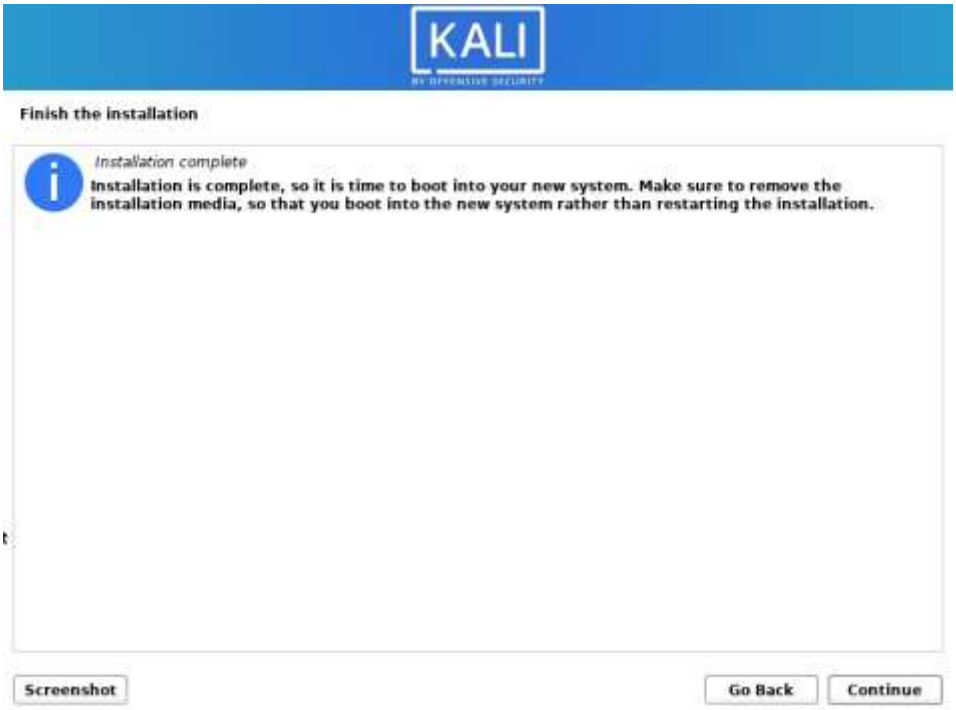


Figura 52: Instalación completada. Fuente: Elaboración Propia.

CASOS PRACTICOS

1. Ataque Man In The Middle - ARP Spoofing + DNS Spoofing en WPA2.

El siguiente caso tiene como objetivo redirigir e intervenir el trafico de una victima mediante arp spoofing y realizar un envenenamiento con DNS Spoofing. Para realizar este ataque se hizo uso de la herramienta ETTERCAP, para ello es necesario seguir los siguientes pasos:

a) Configuar el servicio, para ello es necesario abrir el archivo de configuracion **etter.conf** y cambiarle el usuario por defecto ya que ha sido quien realizó las acciones. Es por ello que se colocara 0 para que se tome como referencia al usuario root.

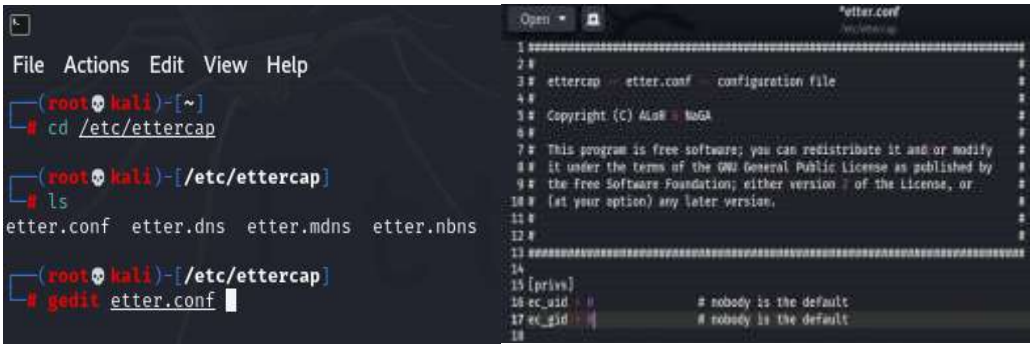


Figura 53: Configuración del archivo etter.conf. Fuente: Elaboración Propia.

b) Es necesario configurar el archivo **etter.dns** ya que es donde se ha establecido el redireccionamiento de nombres de domino y se indica la ip de Kali ya que es donde se levantó el servidor web.

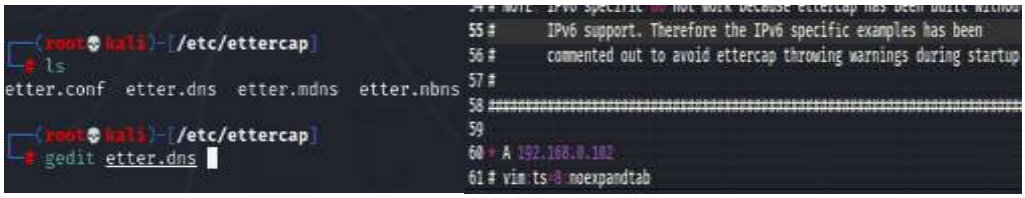


Figura 54: Configuración del archivo etter.dns. Fuente: Elaboración Propia.

c) Es importante iniciar el servidor web luego de que se haya realizado al configuracion en los archivos antes mencionados.

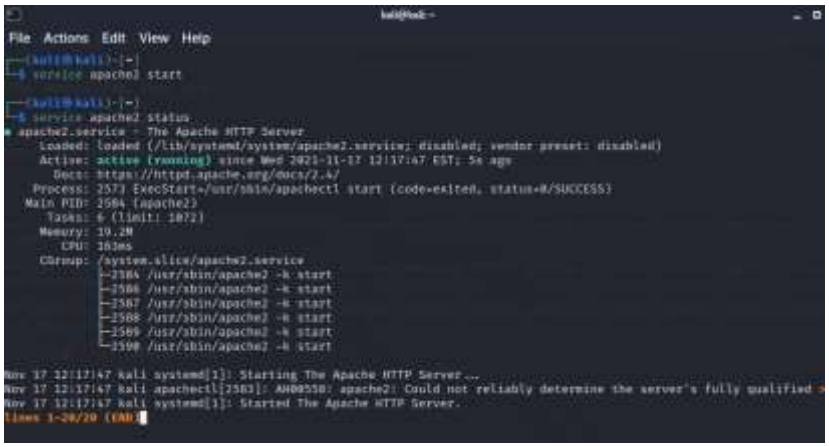


Figura 55: Iniciación del servidor Web. Fuente: Elaboración Propia.

d) Luego que se haya iniciado correctamente el servicio web se debe ingresar a la interfaz de ettercap para ello ejecutamos el comando **ettercap -G** y seleccionamos la interfaz de red con la cual se trabajara.

Figura 56: Configuración de la interfaz de red mediante el comando ettercap-G. Fuente: Elaboración Propia.

e) Es importante escanear los hosts de la red en cual se ha trabajado, para ello es necesario dar clic en el icono de buscar.

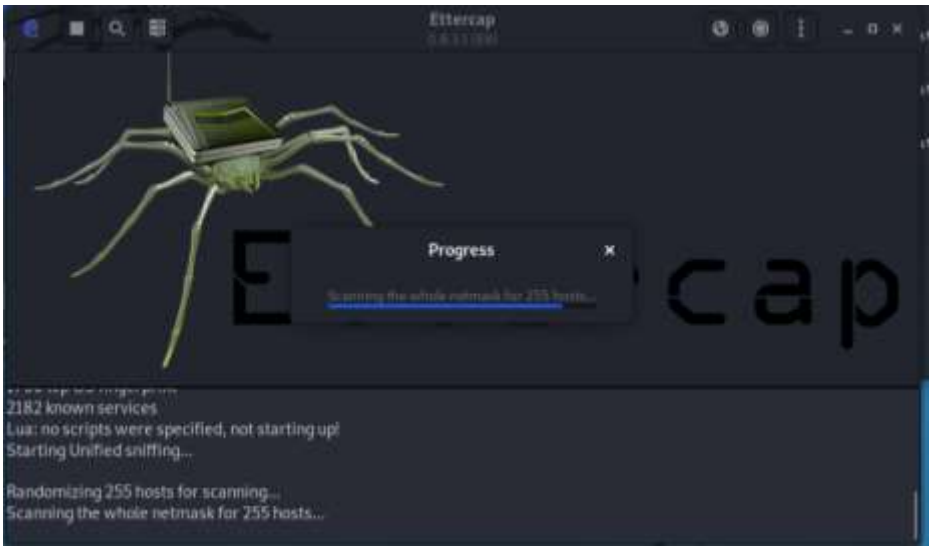


Figura 57: Escaneo de los hosts de red. Fuente: Elaboración Propia.

f) Cuando se termine de escanear todos los hosts que se encuentran conectados a la red se procede a listar para seleccionar con cual de ellos se realizara el ataque.

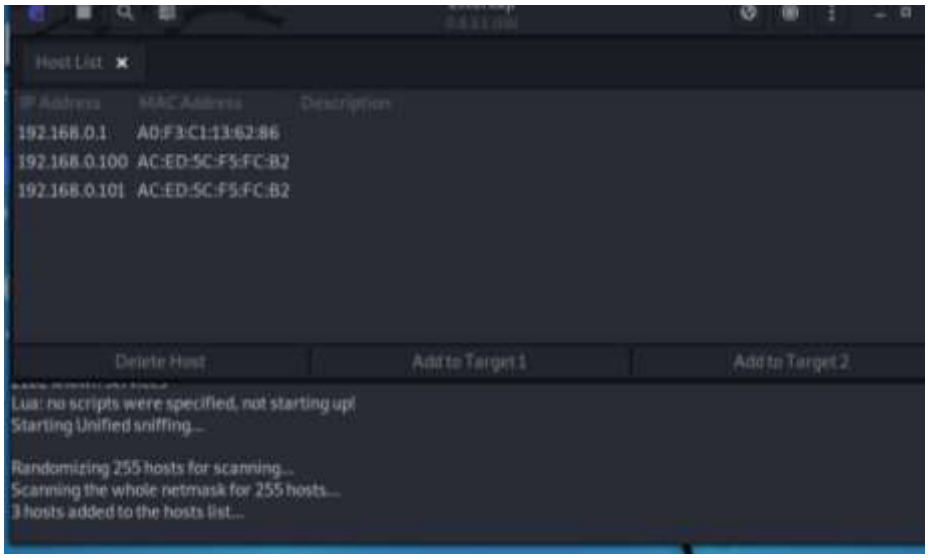


Figura 58: Selección del host(Victima). Fuente: Elaboración Propia.

g) Agregamos al target 1 la ip de la víctima y al target 2 la puerta de enlace por la cual se suplantara.

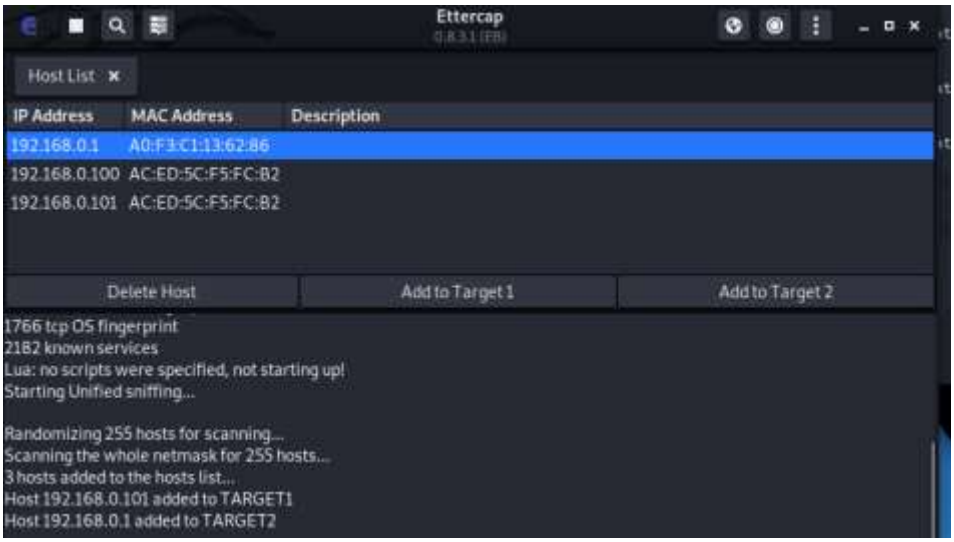


Figura 59: Configuración del IP y puerta de enlace de la víctima. Fuente: Elaboración Propia.

h) Posteriomente corresponde ir al apartado de pluggins, y escoger Manage plugginns para de esa manera proceder a activar el dns spoofing.

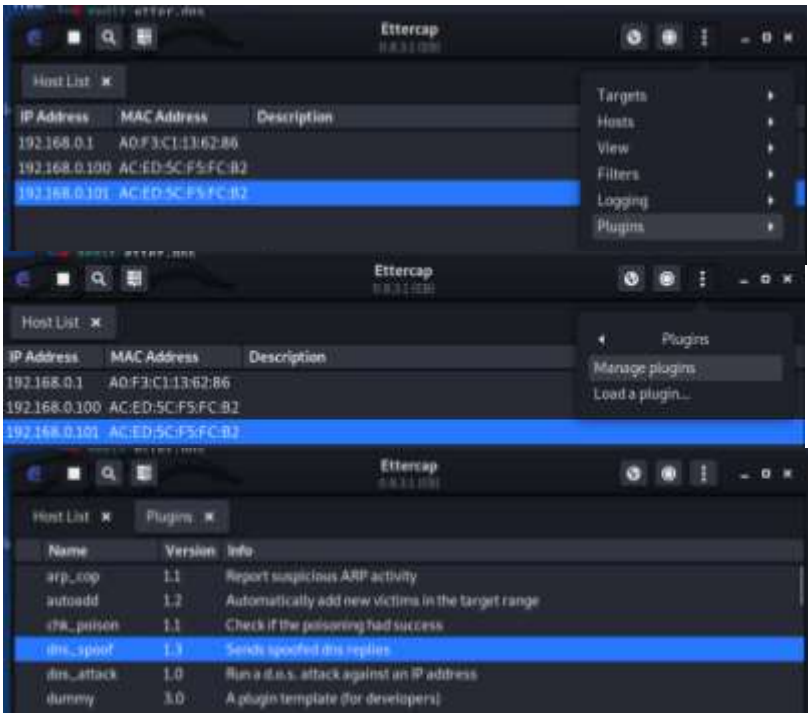


Figura 60: Activación del DNS Spoofing. Fuente: Elaboración Propia.

i) Despues que se haya seleccionado en dns_spoof se inicia el ataque hacia la víctima seleccionada.

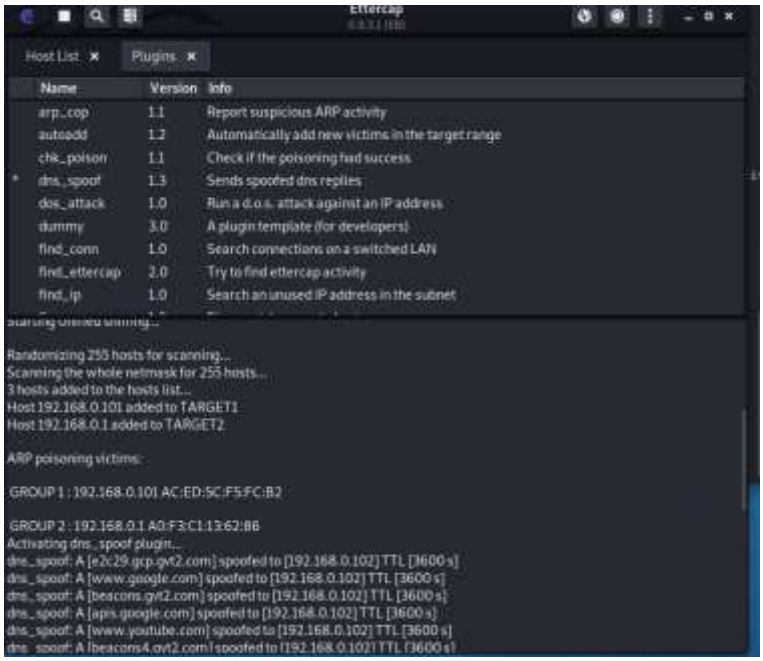


Figura 61: Inicio del ataque a la víctima seleccionada. Fuente: Elaboración Propia.

j) Para comprobar que el ataque tuvo éxito se accede a la maquina victima y se trata de ingresar a cualquier pagina web, si ingresa a la pagina que se desea sin ningún problema, entonces el ataque no tuvo éxito; pero si no ingresa a la pagina y muestra otra ventana como en este caso el index de apache, eso significa que el ataque tuvo éxito.

Figura 62: Ataque DNS Spoofing exitoso en WPA2. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle - ARP Spoofing + DNS Spoofing en WPA2.

El ataque Ataque Man In The Middle (ARP Spoofing + DNS Spoofing) en el protocolo WPA2 tuvo exito ya que la victima no pudo ingresar a ningun domino, puesto que el trafico se estaba dirigiendo a otro nombre de dominio.

Ataque man in the middle ARP Spoofing y DNS Spoofing con el protocolo WPA

Para realizar el mismo ataque al protocolo WPA es necesario configurar el router que se está utilizando y seguir los mismos pasos indicados anteriormente.

Figura 63: Selección y activación del DNS Spoofing en WPA Fuente: Elaboración Propia.

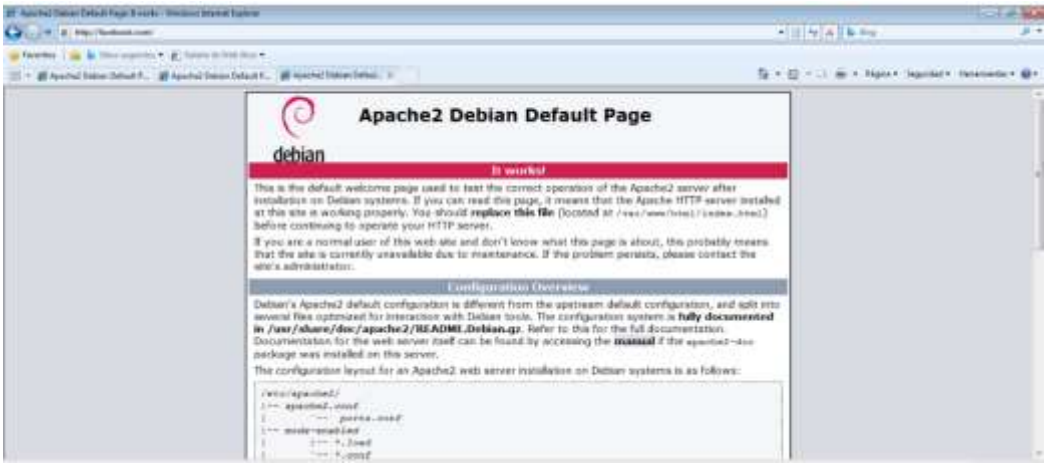


Figura 64: Ataque DNS Spoofing exitoso en WPA. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle - ARP Spoofing + DNS Spoofing en WPA.

El ataque descrito anteriormente tuvo éxito en el protocolo WPA puesto que la víctima no logra ingresar a ninguna página web ya que el tráfico se está redirigiendo a la máquina del atacante, el ataque en este protocolo se realiza en menor tiempo que en WPA2 puesto que su cifrado es menos seguro.

Ataque man in the middle ARP Spoofing y DNS Spoofing con el protocolo WPA3

Para realizar el mismo ataque al protocolo WPA3 es necesario configurar el router que se está utilizando y seguir los mismos pasos indicados anteriormente.

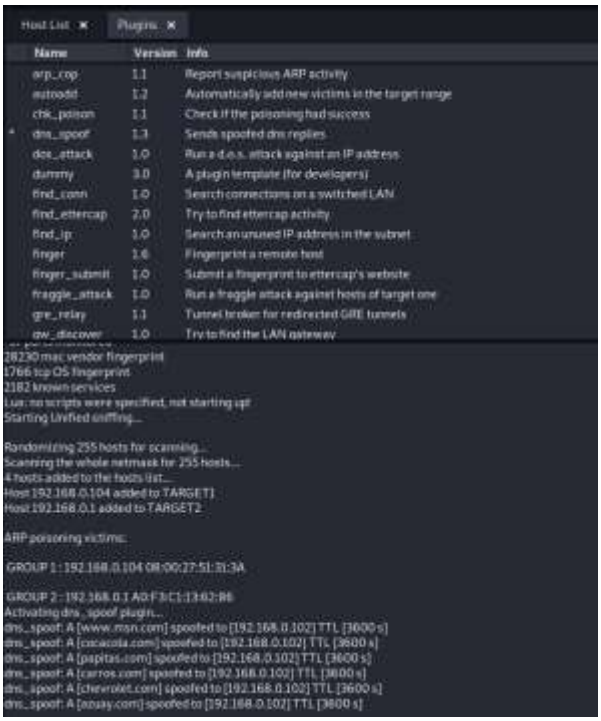


Figura 65: Selección y activación del DNS Spoofing en WP3. Fuente: Elaboración Propia.

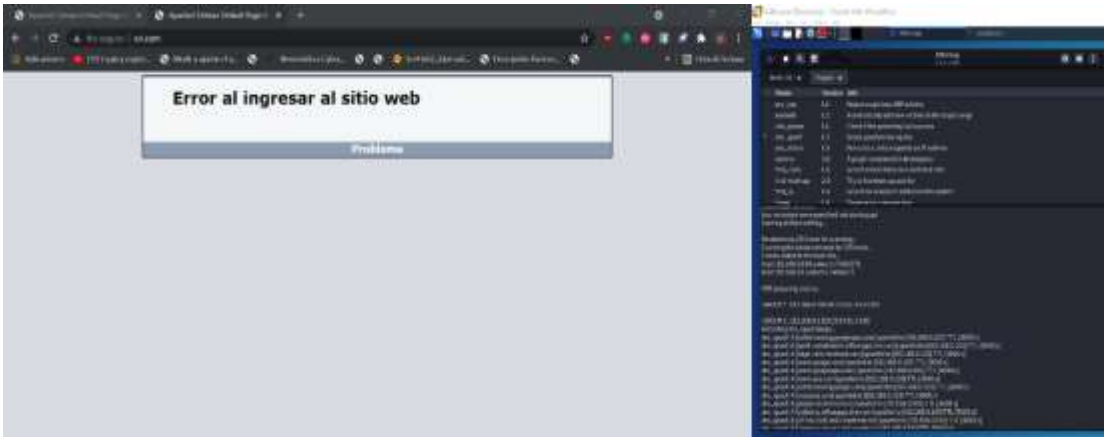


Figura 66: Ataque DNS Spoofing exitoso en WPA3. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle - ARP Spoofing + DNS Spoofing en WPA3.

Este ataque tuvo éxito al utilizar el protocolo WPA3 ya que la víctima no puede ingresar a ningún sitio web, aunque en mayor tiempo que en WPA y WPA2. Este ataque fue exitoso porque hace uso de la IP de la víctima y de la puerta de enlace.

2. **Ataque Man In The Middle en WPA2**

   El ataque man in the middle permite capturar las transmisiones entre las víctimas y también puede modificar las comunicaciones, en el presente ataque se hizo uso de la herramienta ETTERCAP de Kali Linux y para ello se han seguido los siguientes pasos:

a) Lo primero que se hizo al realizar este ataque es verificar los IPs de las máquinas a utilizar

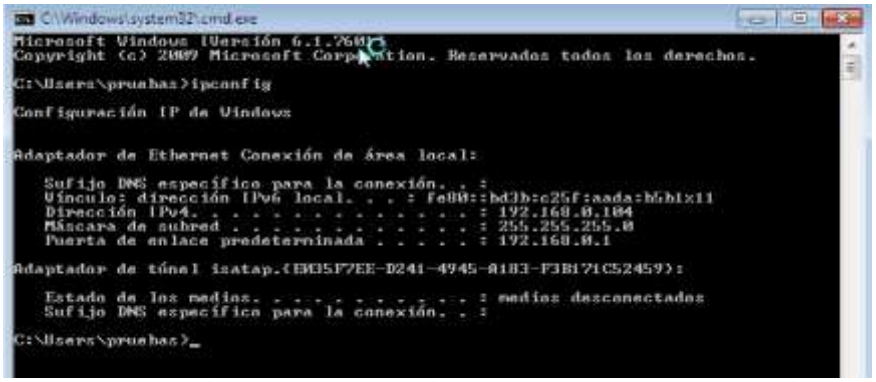


Figura 67: Verificación del IP de la víctima. Fuente: Elaboración Propia.

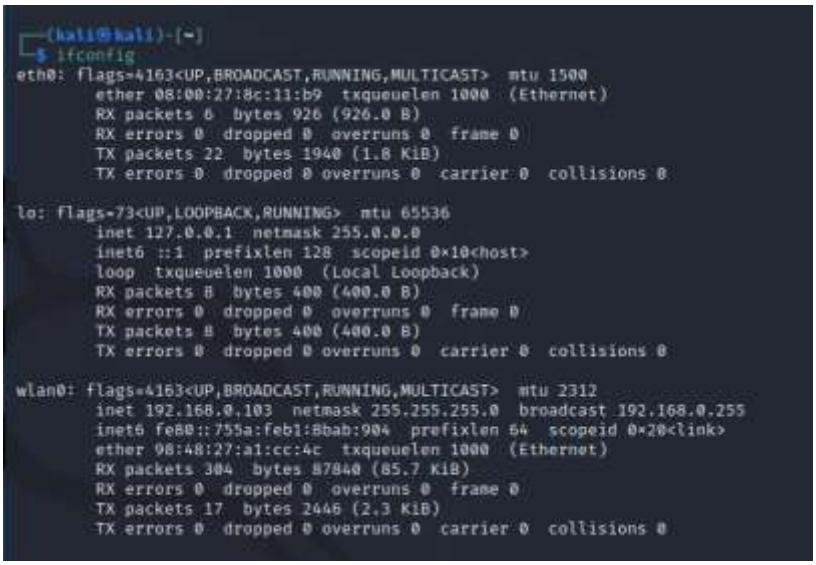


Figura 68: Verificación del IP de la maquina con Kali Linux. Fuente: Elaboración Propia.

b) Se ingresó a la herramienta ETTERCAP, que se hizo mediante el comando ettercap -G como se muestra a continuación. Al ingresar fue necesario escoger la red en la cual trabajará para el ataque.

Figura 69: Acceso a la herramienta ETTERCAP en WPA2. Fuente: Elaboración Propia.

c) Es importante realizar un escaneo de todos los hosts que tiene la red seleccionada

Figura 70: Escaneo de los hosts en la red seleccionada. Fuente: Elaboración Propia.

d) Cuando se finalizó el escaneo, se listan los hosts con el fin de conocer la direccion IP de la victima.

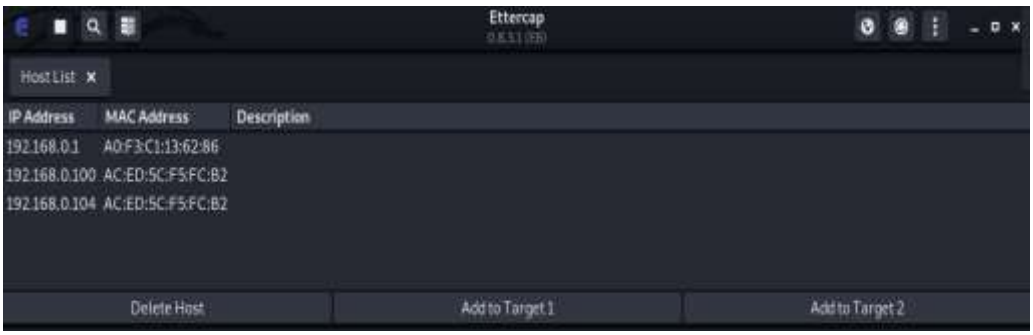


Figura 71: Listado de los hosts en la red seleccionada. Fuente: Elaboración Propia.

e) Al momento que se haya identificado a la víctima, se procede a señalarlo como target 1 y a su puerta de enlace se agregara al target 2 tal y como se hizo en el anterior ataque.

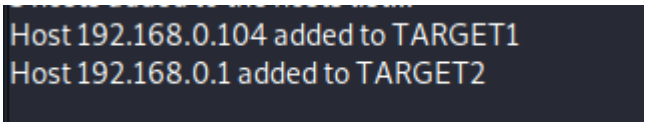


Figura 72: Marcación del IP y la puerta de enlace como Target 1 y 2 respectivamente. Fuente: Elaboración Propia.

f) Con la dirección de la víctima agregada, se procede a dar clic en ARP Poisoning.

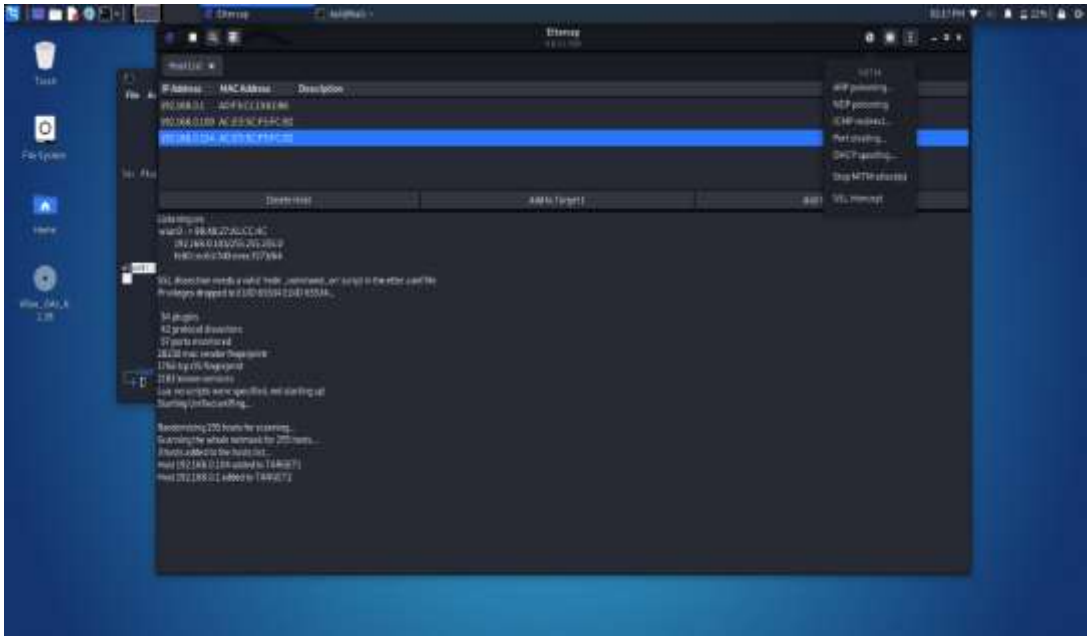


Figura 73: ARP Poisoning en la victima selecionada de la lista de hosts. Fuente: Elaboración Propia.

g) Luego de seleccionar el arp se debe verificar que se encuentre marcado “sniff remote conections”. Al realizar eso ya se esta interceptando los paquetes que provienen de la victima.

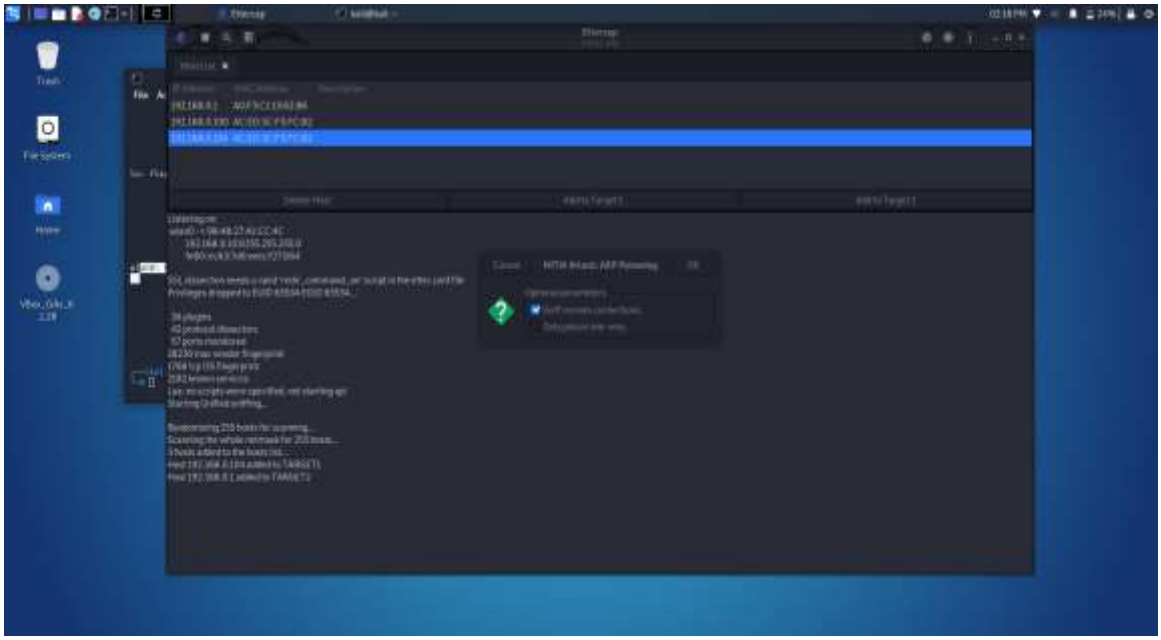


Figura 74: Selección de la opción Sniff remote connections. Fuente: Elaboración Propia.

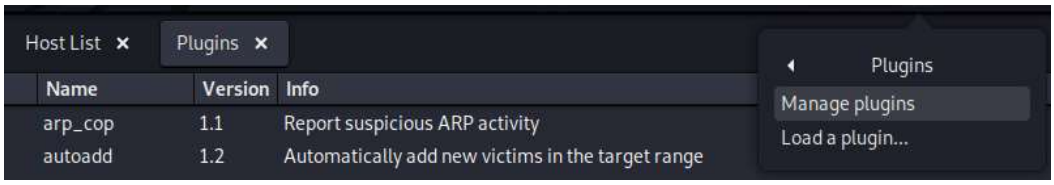


Figura 75: Vista de plugins. Fuente: Elaboración Propia.

h) Posteriormente se debe seleccionar la opcion remote-browser para obtener las URL visitadas.

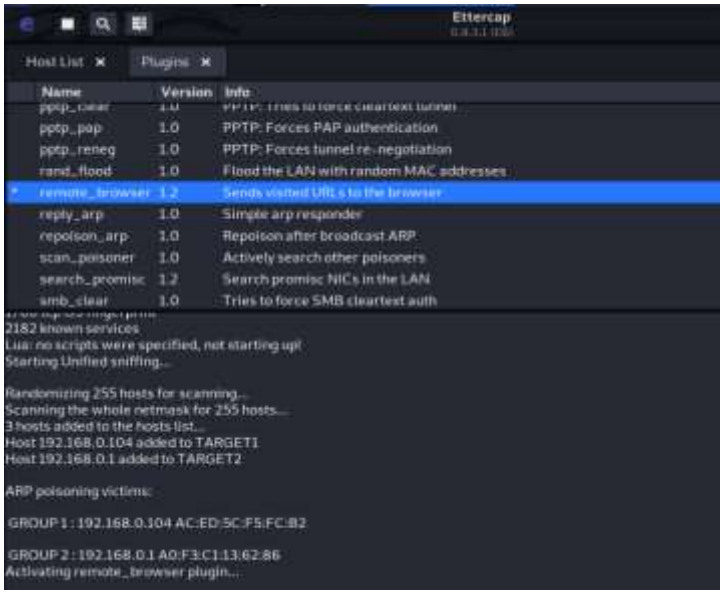


Figura 76: Configuración de la opción del comando remote-browser. Fuente: Elaboración Propia.

i) Para comprobar se puede acceder a una pagina web desde la maquina victima, se puede observar que la pagina se carga un poco mas lento, tambien se puede verificar en la consola de windows que la mac de la puerta de enlace se ha cambiado por la mac del equipo del atacante kali.

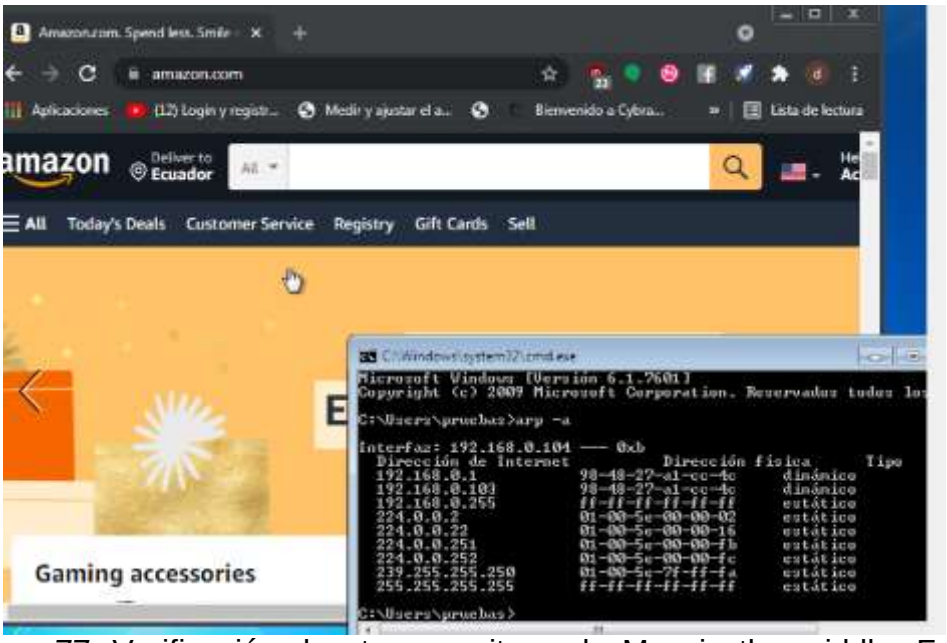


Figura 77: Verificación de ataque exitoso de Man in the middle. Fuente: Elaboración Propia.

j) En la máquina del atacante kali se puede visualizar que se va desplegando las paginas web visitadas de la victima.

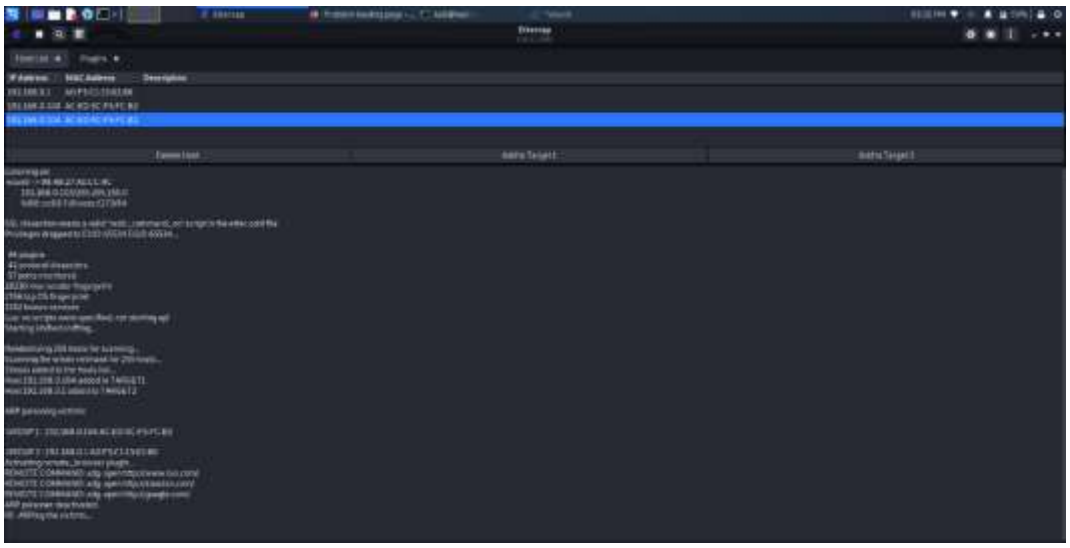


Figura 78: Historial de páginas web de la víctima desde la computadora del atacante. Fuente: Elaboración Propia.

k) Otra manera de corroborar el ataque es con la ayuda de Wireshark en donde se puede realizar un analisis del trafico de la víctima, que es redirigido hacia el atacante y luego redirigido hace la puerta de enlace predeterminada.

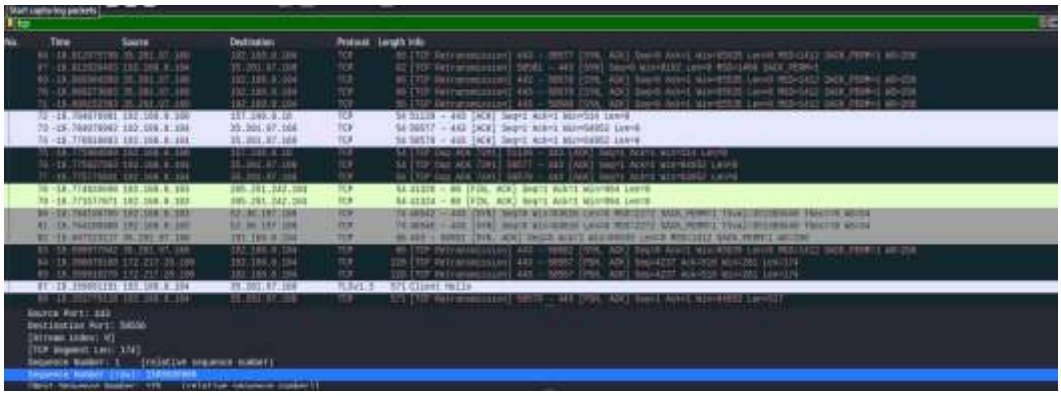


Figura 79: Verificación del ataque mediante la herramienta Wireshark. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle en WPA2

El ataque man in the middle en el protocolo WPA2 tuvo éxito ya que se logró capturar con éxito el tráfico de la víctima, para corroborar este ataque se ha utilizado wireshark herramienta que permite realizar un análisis de tráfico y también se ha observado que la puerta de enlace en la victima ha cambiado.

Ataque man in the middle con el protocolo WPA

Es importante que para realizar el mismo ataque al protocolo WPA se configure el Access point que se está utilizando, con el fin de conocer si este ataque es exitoso con dicho protocolo.

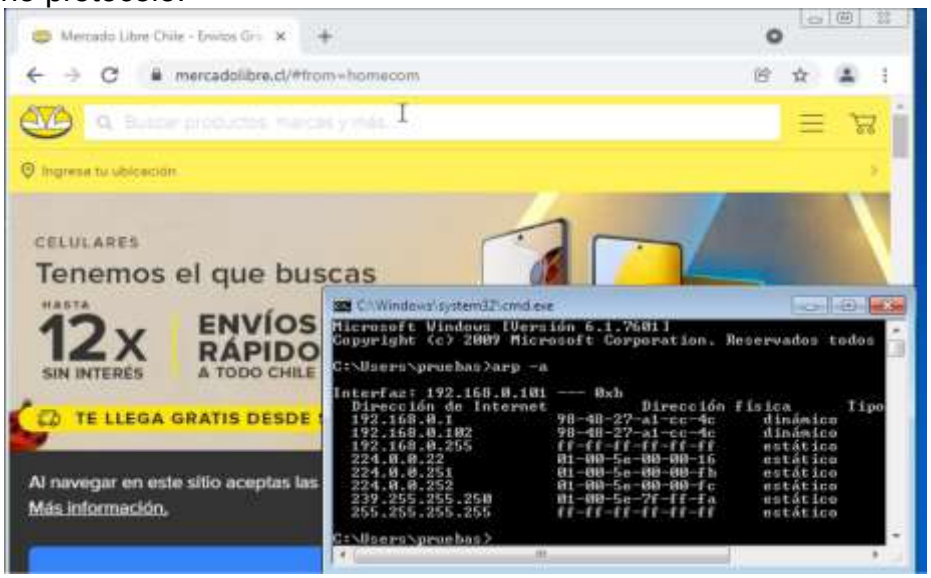


Figura 80: Verificación del IP de la víctima en WPA. Fuente: Elaboración Propia.

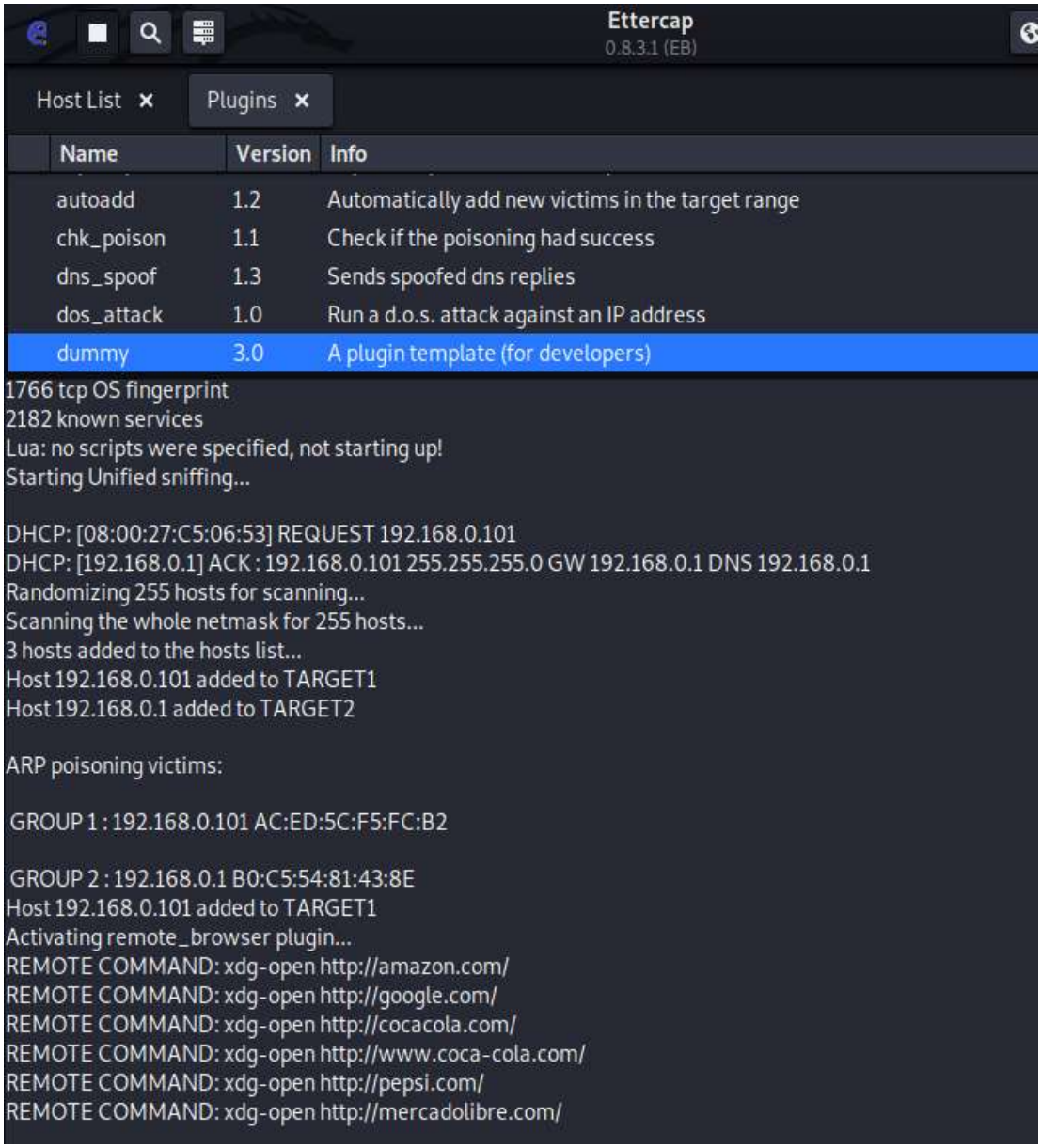


Figura 81: Configuración de la opción del comando remote-browser en WPA. Fuente: Elaboración Propia.

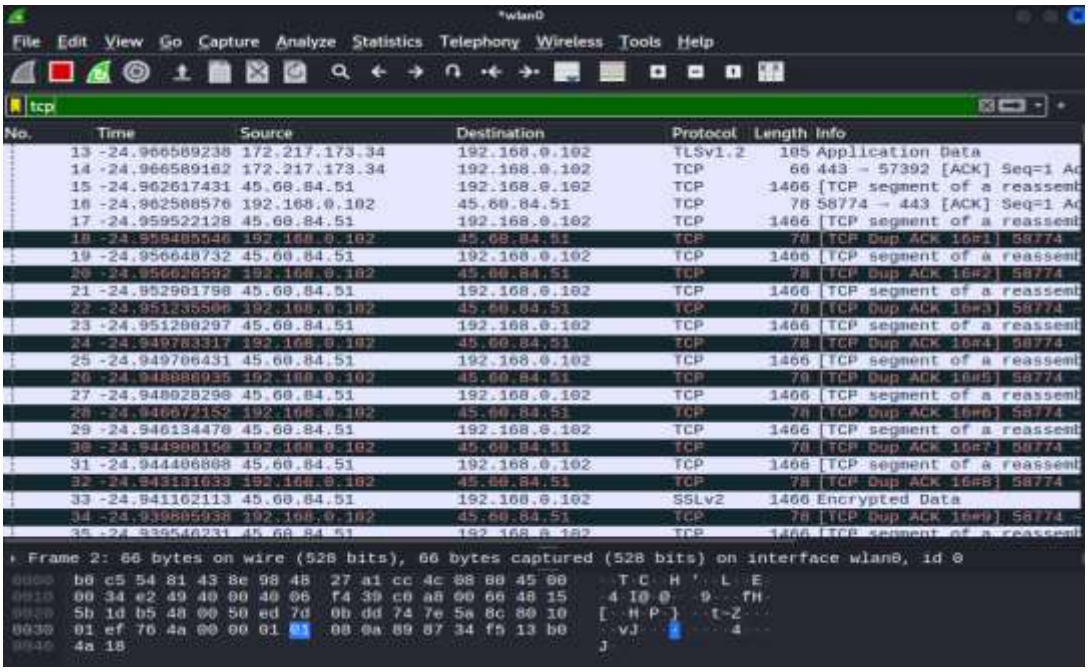


Figura 82: Verificación del ataque en WPA mediante la herramienta Wireshark. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle en WPA

Como bien se conoce el protocolo WPA tiene mayor vulnerabilidad que el protocolo WPA2 es por ello que al ejecutar el ataque man in the middle se penetra con éxito permitiendo capturar todo el tráfico que la maquina victima genera, el ataque tiene se penetra en la victima en una menor cantidad de tiempo en comparación con WPA2, lo cual lo hace más vulnerable al momento que se activa un ataque.

Ataque man in the middle con el protocolo WPA3

Es importante que para realizar el mismo ataque al protocolo WPA3 se configure el Access point que se está utilizando.

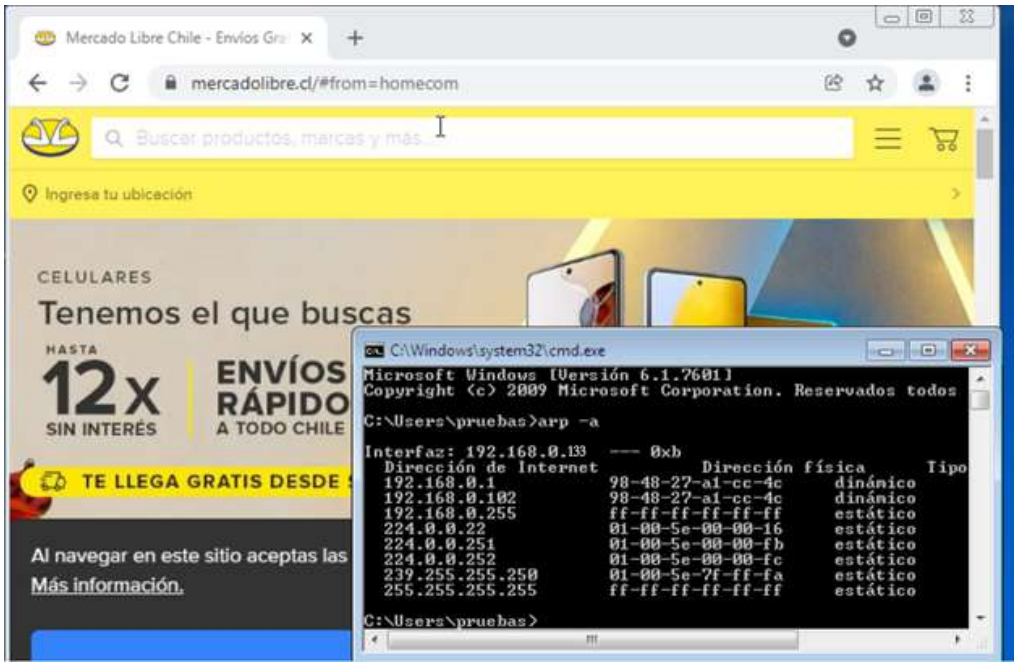


Figura 83: Verificación del IP de la víctima en WPA3. Fuente: Elaboración Propia.

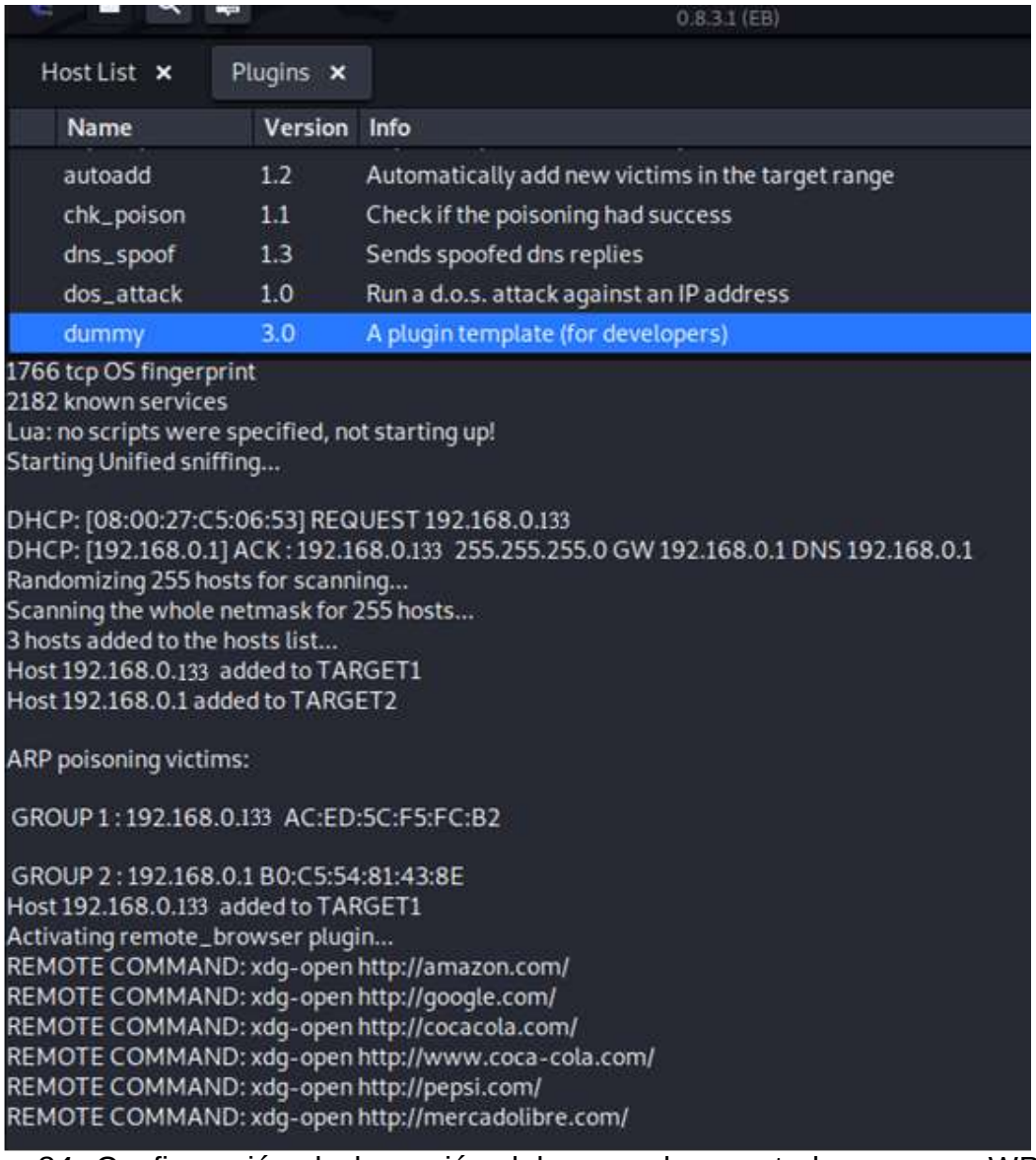


Figura 84: Configuración de la opción del comando remote-browser en WPA3. Fuente: Elaboración Propia.

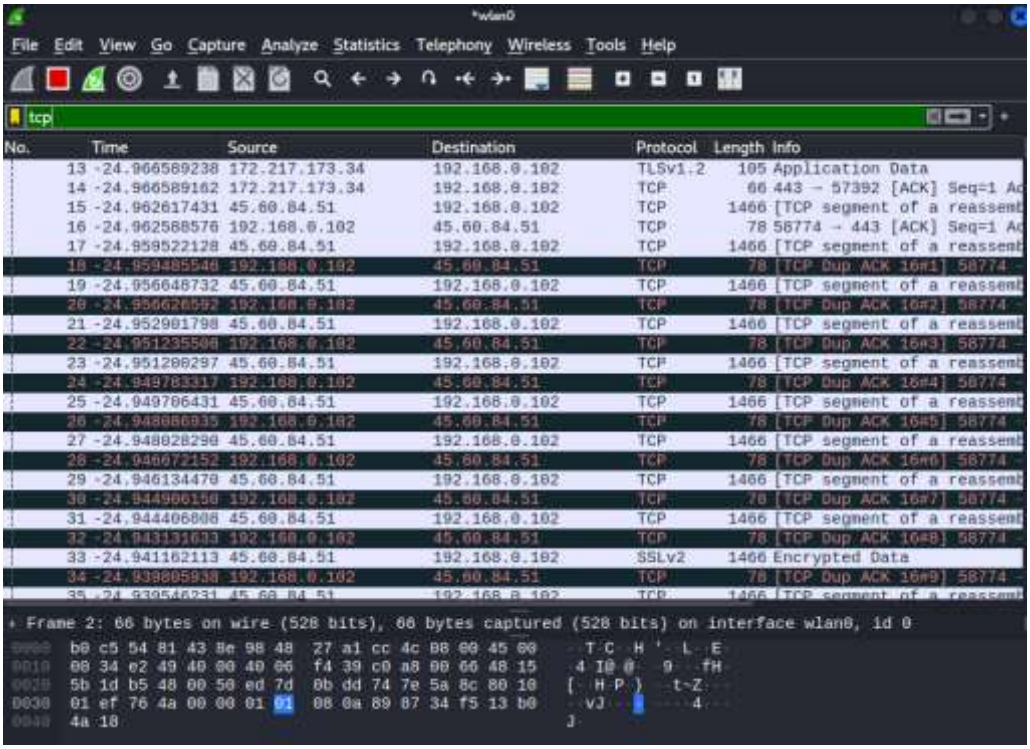


Figura 85: Verificación del ataque en WPA3 mediante la herramienta Wireshark. Fuente: Elaboración Propia.

Descripción del Ataque Man In The Middle en WPA3

El presente ataque tuvo éxito en el protocolo WPA3, aunque en un tiempo mucho mayor que en los protocolos WPA2 y WPA que se implementaron anteriormente.

3. Ataque de Fuerza Bruta en WPA2

El ataque de fuerza bruta se presenta cuando el atacante intenta descifrar contraseñas mediante la aplicación de un método conocido como prueba y error con la finalidad tratar de obtener la combinación correcta, esto se realiza probando todo tipo de combinaciones posible hasta lograr conseguir la clave.

Para realizar este ataque es importante seguir los siguientes pasos:

a) Verificar si existe una tarjeta inalámbrica para ello es necesario utilizar el comando que se muestra en la siguiente figura.

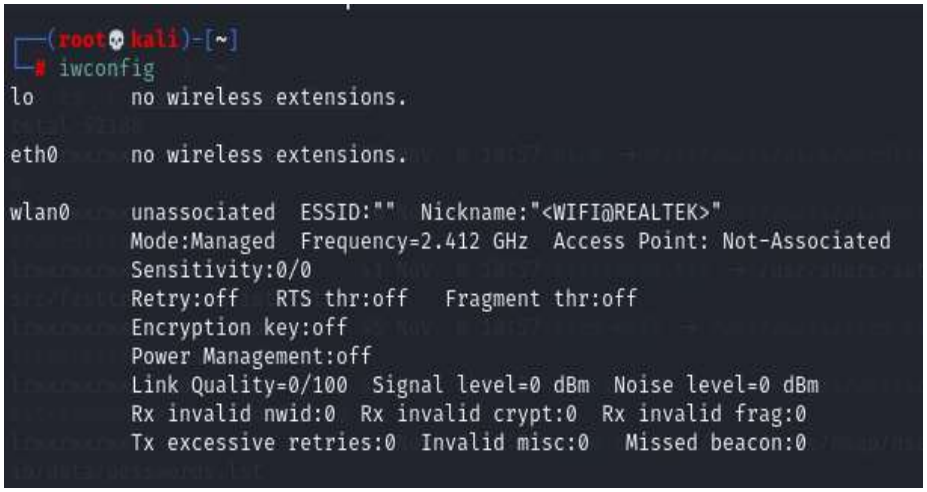


Figura 86: Verificación de la tarjeta inalámbrica en el equipo atacante. Fuente: Elaboración Propia.

b) Al momento que se conozca que si existe la tarjeta inalámbrica es necesario convertirla en modo monitor, para cambiar a este modo es importante utilizar el comando que se muestra a continuación.

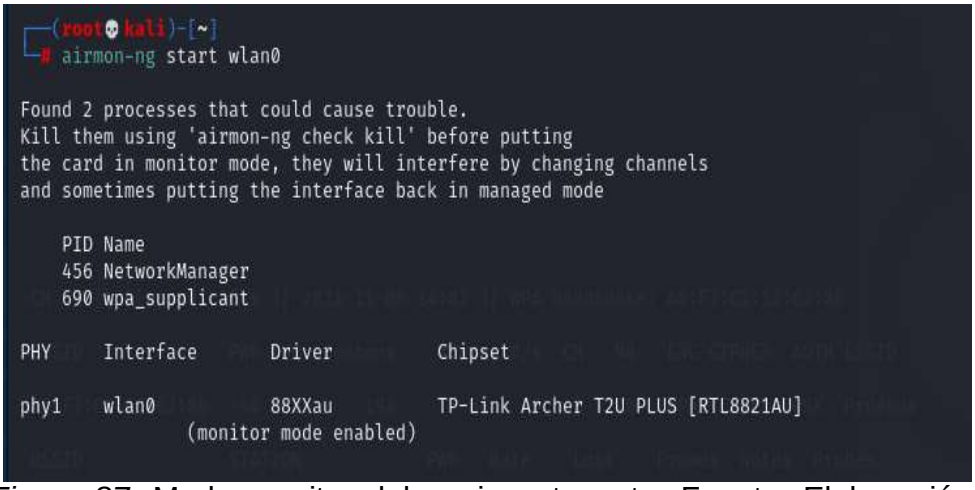


Figura 87: Modo monitor del equipo atacante. Fuente: Elaboración Propia.

c) Al haber ejecutado el comando para convertir la red inalámbrica en modo monitor se puede apreciar que hay procesos que se deben eliminar para que no se presenten interferencias al momento de utilizar dicha red es por ello que se ejecuta el comando que se presenta a continuación.

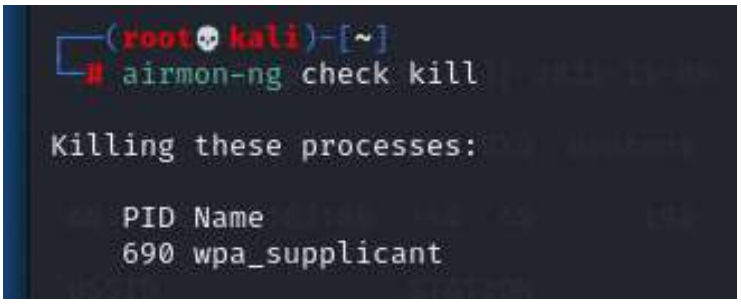


Figura 88: Ejecución del comando Check kill para eliminar procesos ajenos al ataque. Fuente: Elaboración Propia.

d) Luego de matar los procesos antes presentados se procede a verificar que la red inalámbrica se cambió al modo monitor para ellos se ejecuta el siguiente comando.

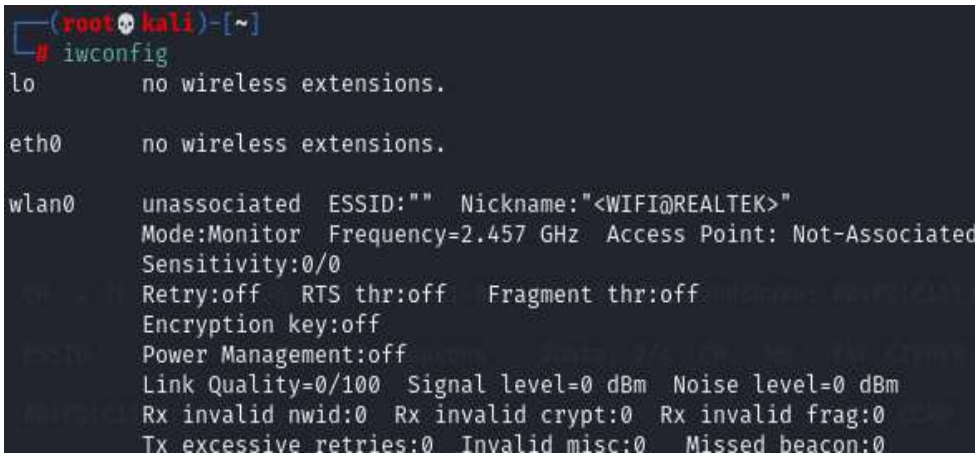


Figura 89: Verificación de la red inalámbrica. Fuente: Elaboración Propia.

e) Es importante visualizar todas las redes inalámbricas para identificar las redes que la antena Wifi es capaz de reconocer y con el fin de conocer el nombre de la red, el canal y la seguridad que este posee.

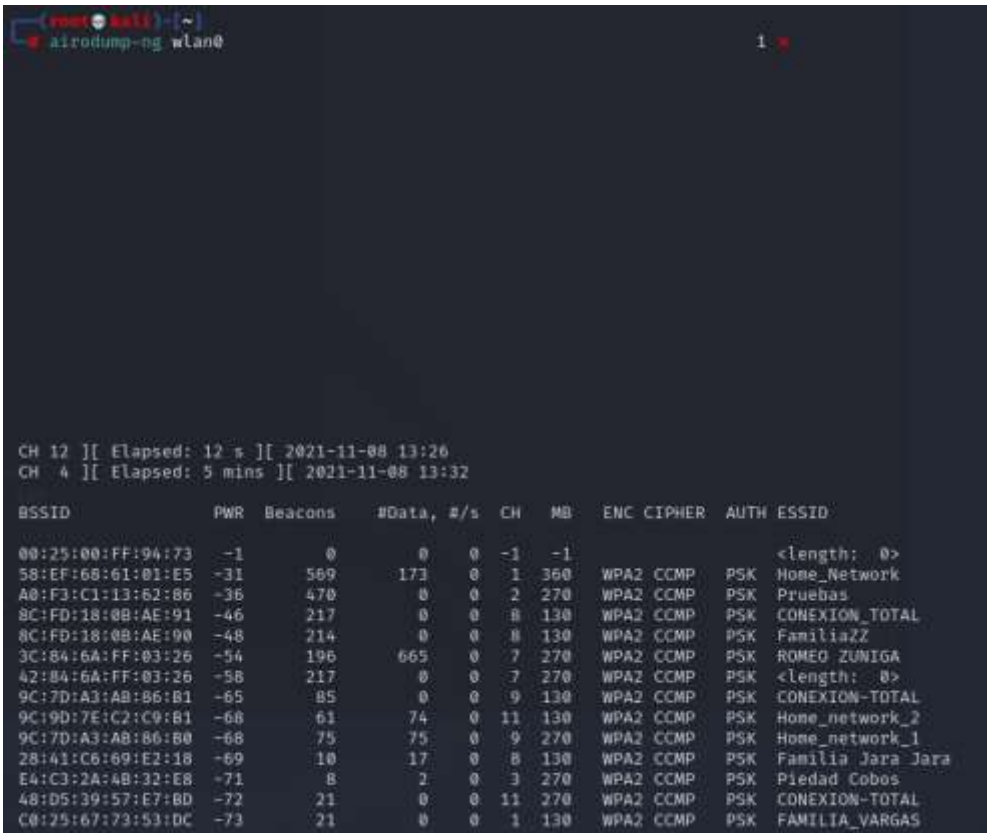


Figura 90: Reconocimiento de la víctima objetivo. Fuente: Elaboración Propia.

f) Una vez que se haya identificado la red a la cual se va a realizar el ataque se procede a realizar la captura de tráfico con el fin de obtener el handshake.

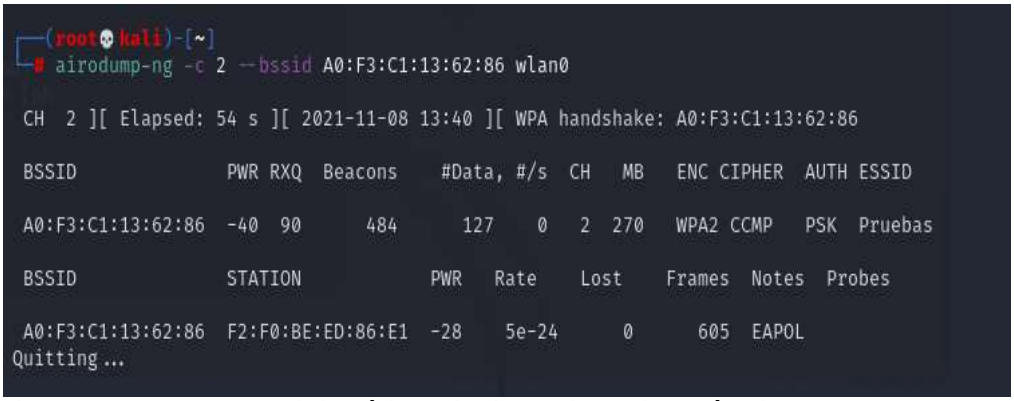


Figura 91: Captura del tráfico de la red en la máquina atacante. Fuente: Elaboración Propia.

g) Es importante que el handshake se guarde en una ruta conocida ya que posteriormente se utilizara el archivo .cap para el descifrado de la contraseña, en este caso se ha optado por guardar el archivo con el nombre wpa201 en la carpeta tmp, esto con el fin de acceder de manera más rápida al archivo.

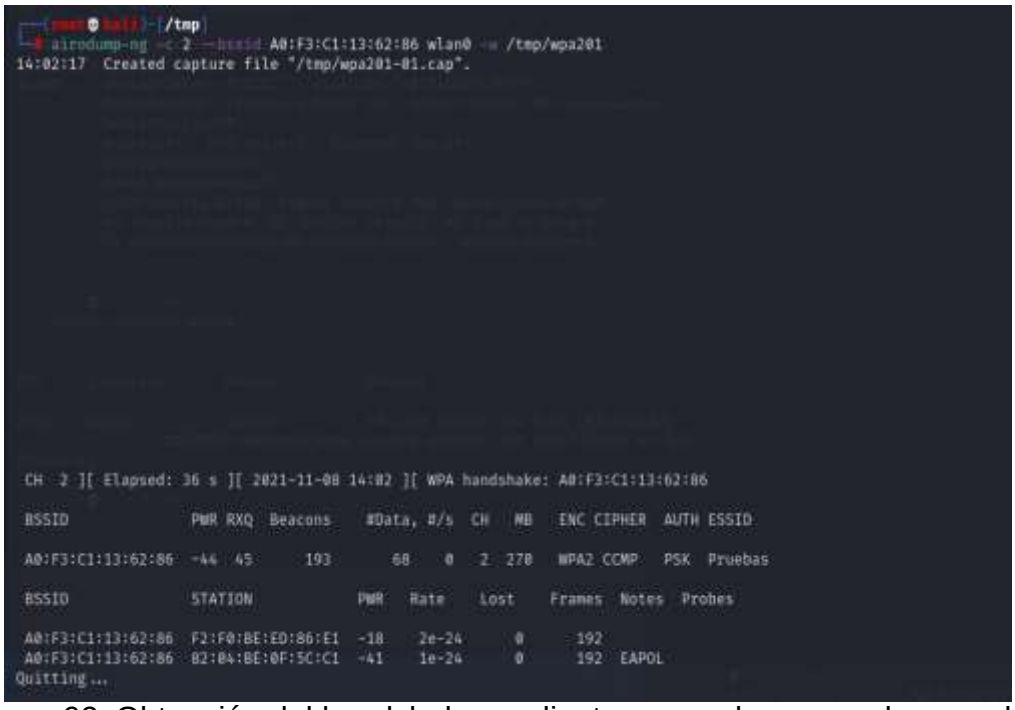


Figura 92: Obtención del handshake mediante comandos en modo consola. Fuente: Elaboración Propia.

h) Para comprobar que el documento se haya guardado se comprueba dirigiéndose a la carpeta tmp y se procede a listar tal como se muestra a continuación.

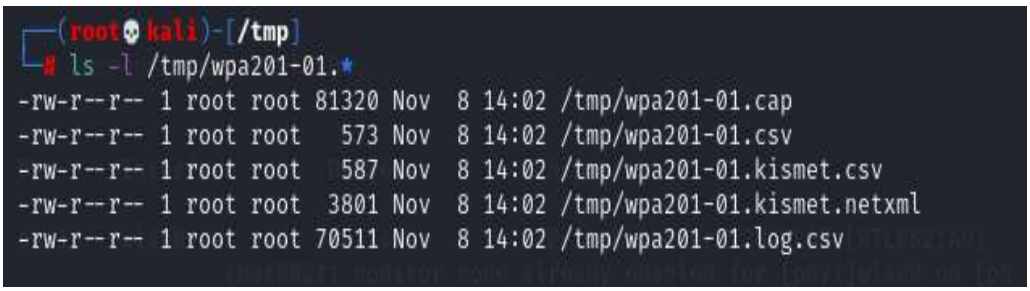


Figura 93: Comprobación del guardado del archivo .cap. Fuente: Elaboración Propia.

i) El archivo .cap se puede abrir con la herramienta Wireshark para visualizar el tráfico que se ha guardado en dicho archivo, el tráfico que se observa corresponde únicamente a la red que se seleccionó.

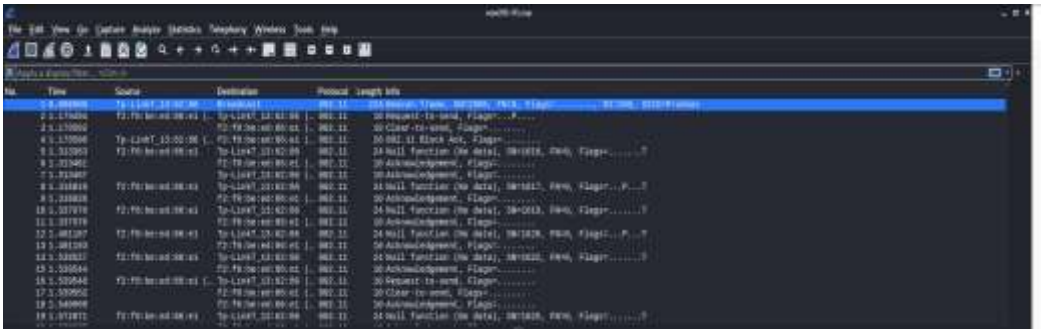


Figura 94: Visualización del archivo .cap mediante la herramienta Wireshark. Fuente: Elaboración Propia.

j) Luego de observar el tráfico encriptado que se capturo se procede hacer uso de la herramienta aircrak-ng misma que permitirá descifrar o romper la contraseña para ello se utiliza un diccionario el cual contiene una lista de palabras con el cual se realizara una combinación de palabras hasta que encuentre una coincidencia con la clave del Access point.

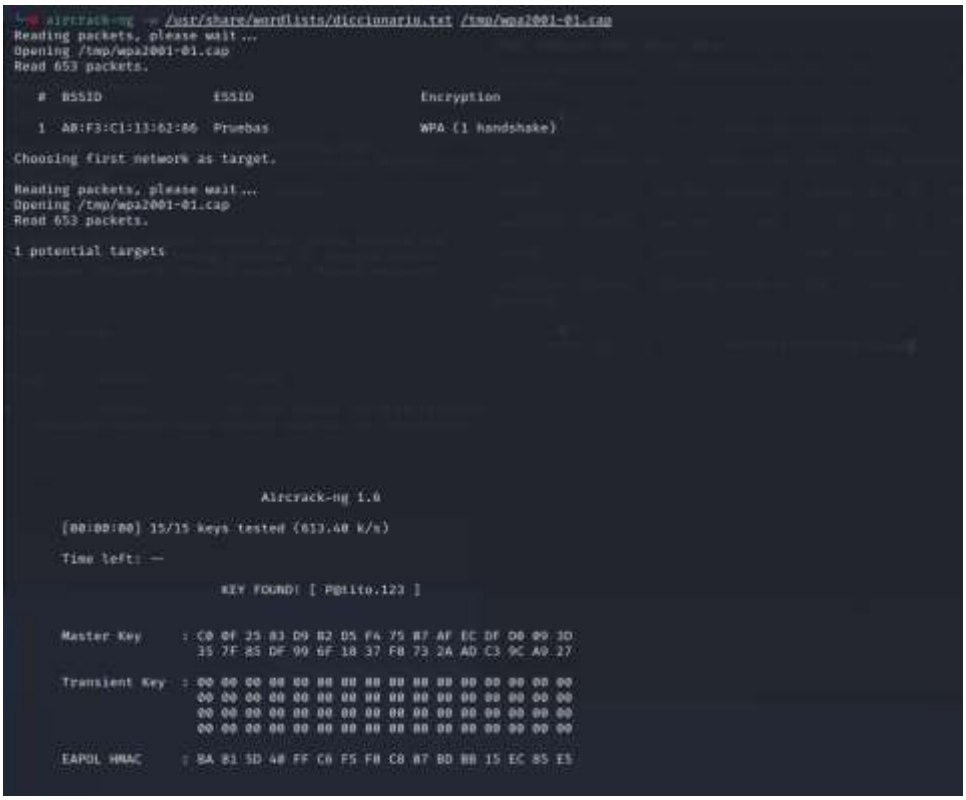


Figura 95: Descifrado de la contraseña mediante aircrak-ng. Fuente: Elaboración Propia.

Descripcion del Ataque de Fuerza Bruta en WPA2

El ataque de fuerza bruta al utilizar protocolo WPA2 tuvo éxito puesto que se logró conocer la contraseña del Access point por lo tanto se podrá ingresar sin ningún problema a dicha red. Este ataque depende de la fuerza que tenga la clave ya que si la clave cuenta únicamente con números demorara menor tiempo en descifrar que una clave que contenga letras, números, signos, ya que las combinaciones que realice van de acuerdo a las que se encuentren en el archivo. Es importante conocer además que el ataque de fuerza bruta se basa en intentar, ya que depende de múltiples factores como por ejemplo si el diccionario está construido solo con palabras y la contraseña cuenta con números es improbable que se obtenga la contraseña.

Ataque de fuerza bruta con el protocolo WPA

Para llevar a cabo el ataque de fuerza bruta hacia el protocolo WPA se debe seguir los mismos pasos que se describen anteriormente ya que nada cambia, la única diferencia que se visualizara es que al momento de analizar las redes se podrá corroborar que el protocolo ha cambiado por WPA tal como se muestra a continuación.

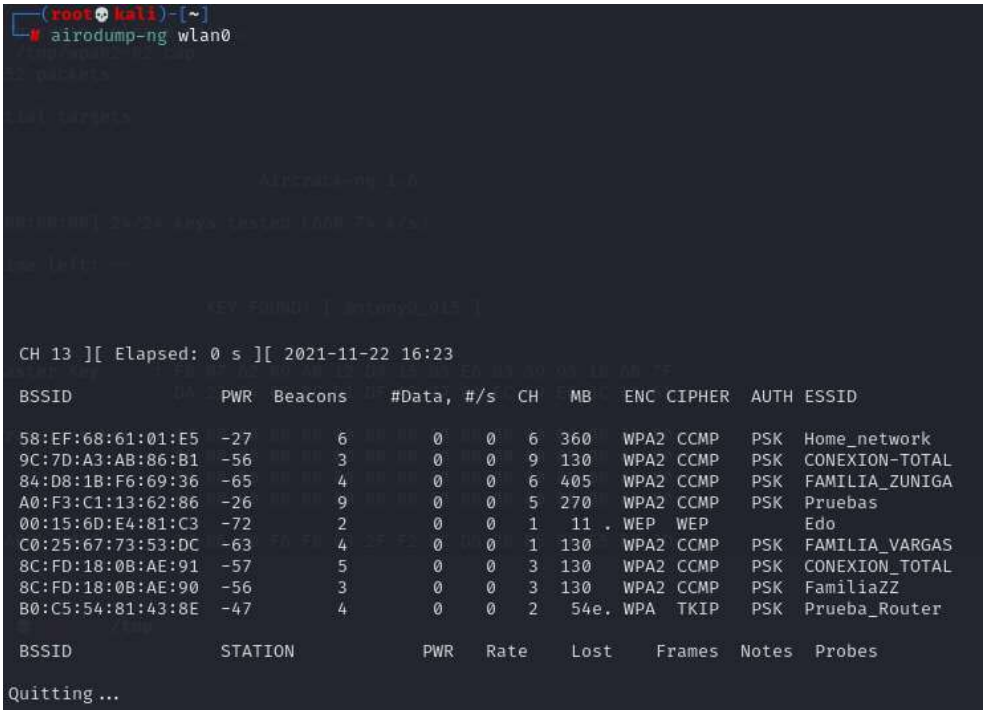


Figura 96: Reconocimiento de la víctima objetivo con WPA. Fuente: Elaboración Propia.

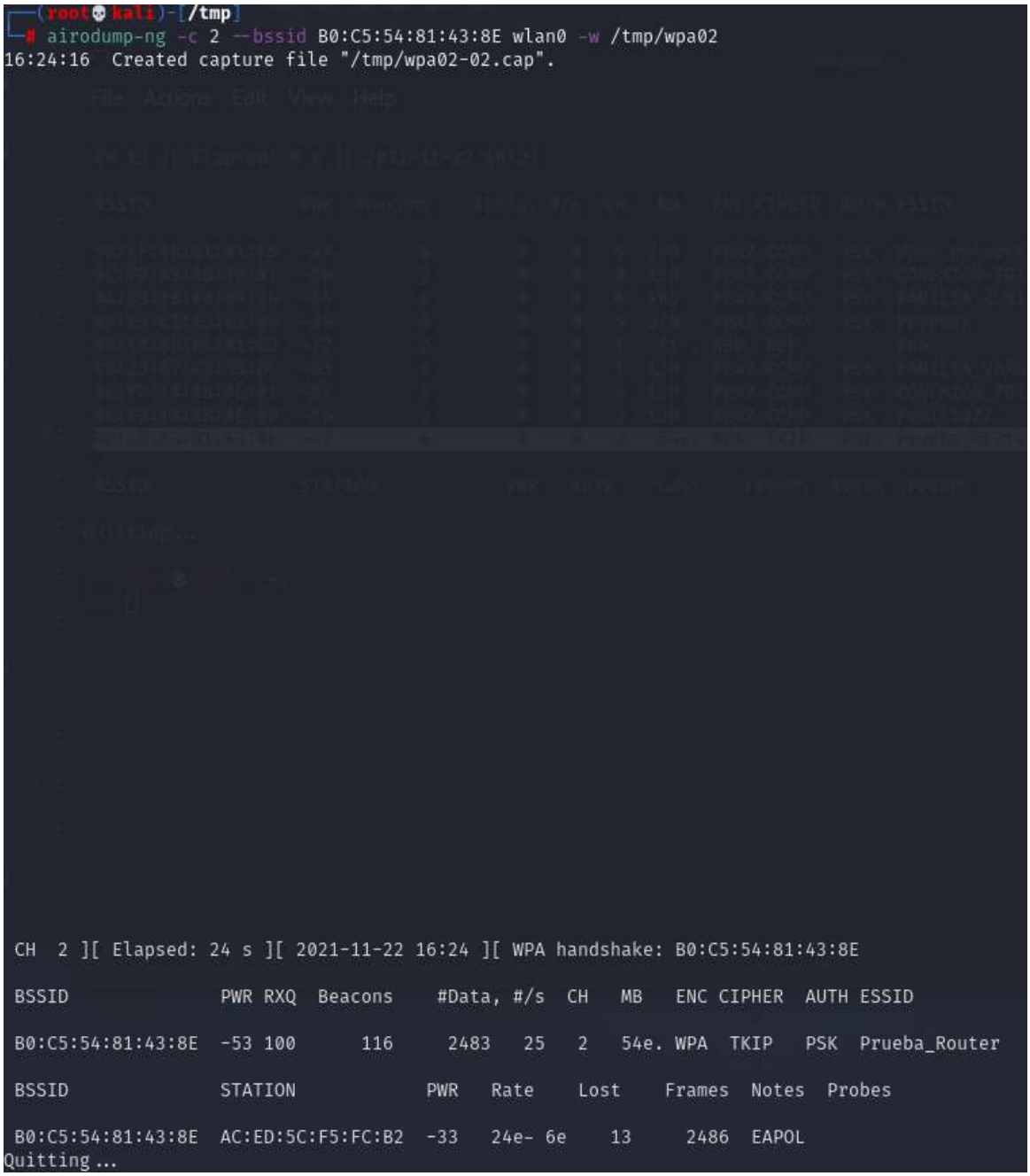


Figura 97: Obtención del handshake mediante comandos en modo consola WPA.

Fuente: Elaboración Propia.

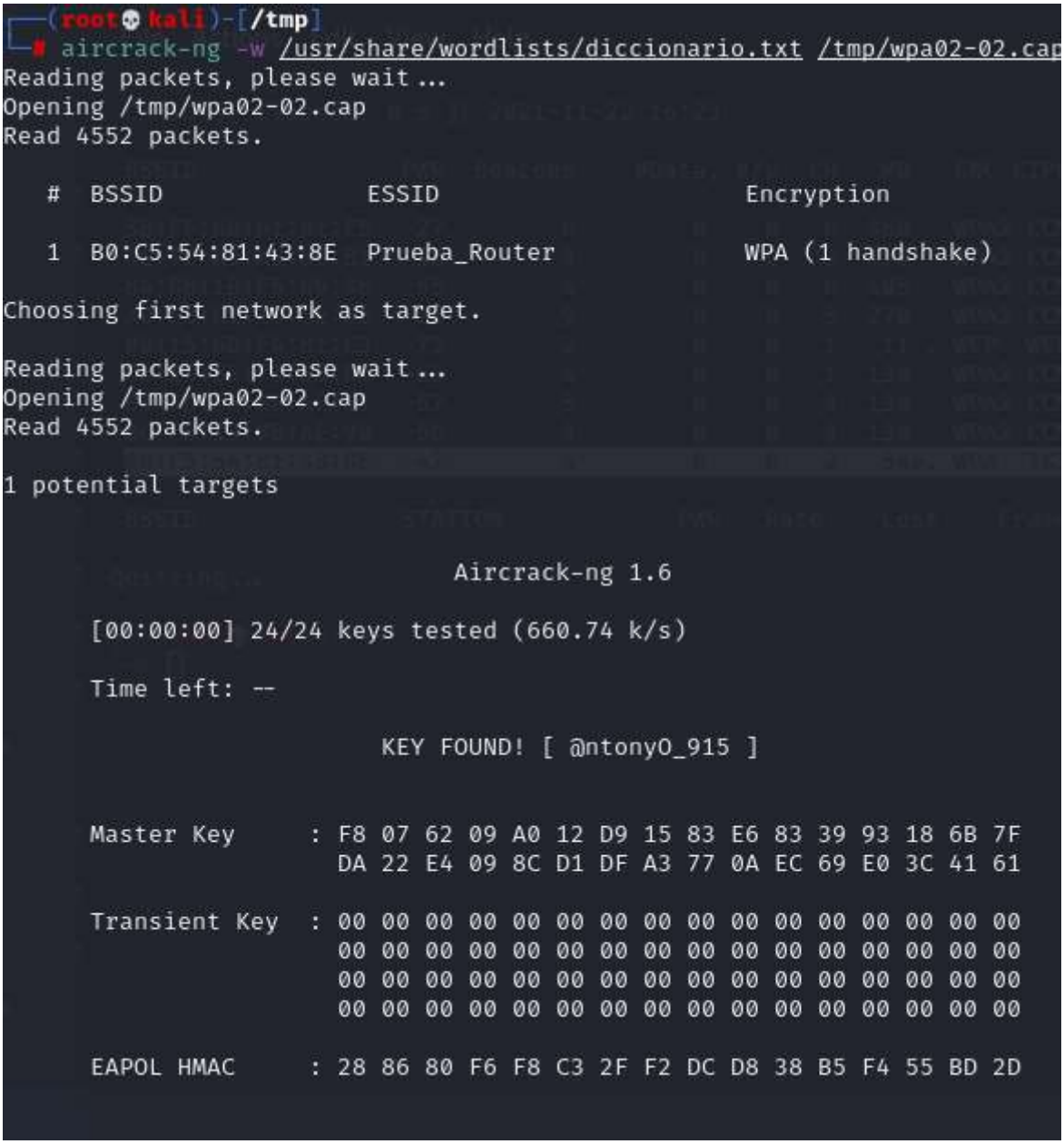


Figura 98: Descifrado de la contraseña mediante aircrak-ng. Fuente: Elaboración Propia.

Descripcion del Ataque de Fuerza Bruta en WPA

El ataque de fuerza bruta tuvo éxito al utilizar el protocolo WPA esto se comprueba en la imagen prestada anteriometne ya que ahí se visualiza que se obtuvo con facilidad la clave de la red a la cual se dirigio en ataque, es importante mencionar que el tiempo de respuesta del ataque en este protocolo es mas rapido que en el protocolo WPA2 esto se da por el tipo de cifrado que utiliza.

Ataque de fuerza bruta con el protocolo WPA3

Para llevar a cabo el ataque de fuerza bruta hacia el protocolo WPA3 se debe seguir los mismos pasos que se describen anteriormente ya que nada cambia la única diferencia que se presenta es que al momento de analizar las redes se podrá corroborar que el protocolo ha cambiado por WPA3.

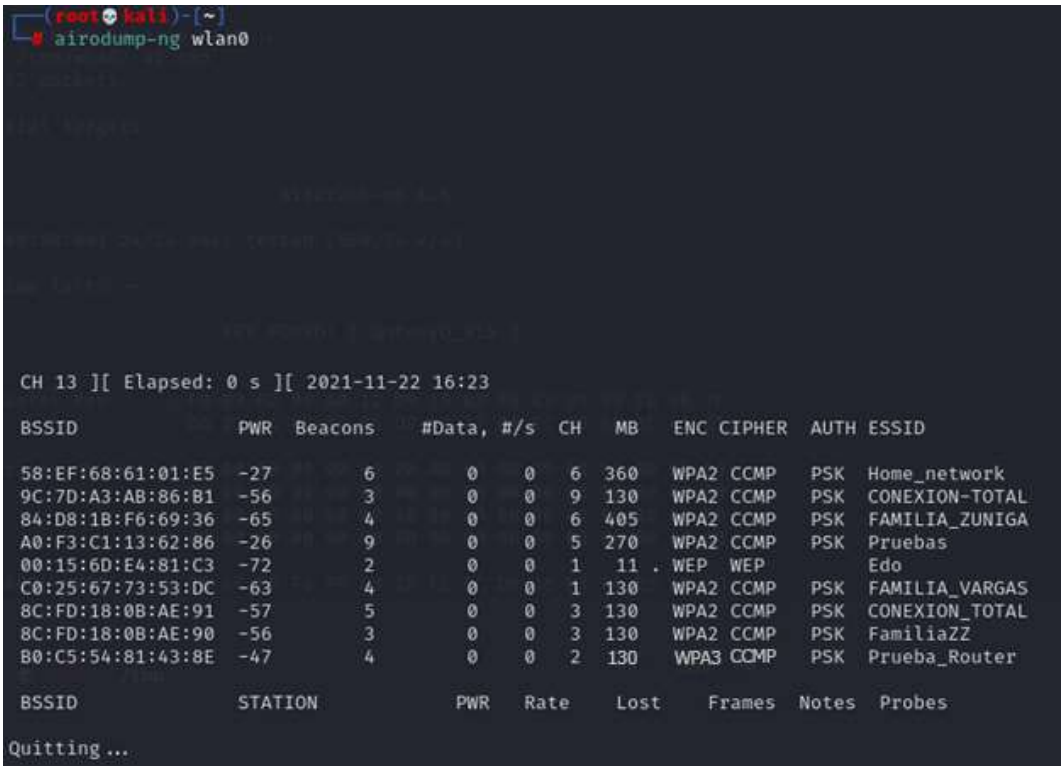


Figura 99: Reconocimiento de la víctima objetivo con WPA3. Fuente: Elaboración Propia.

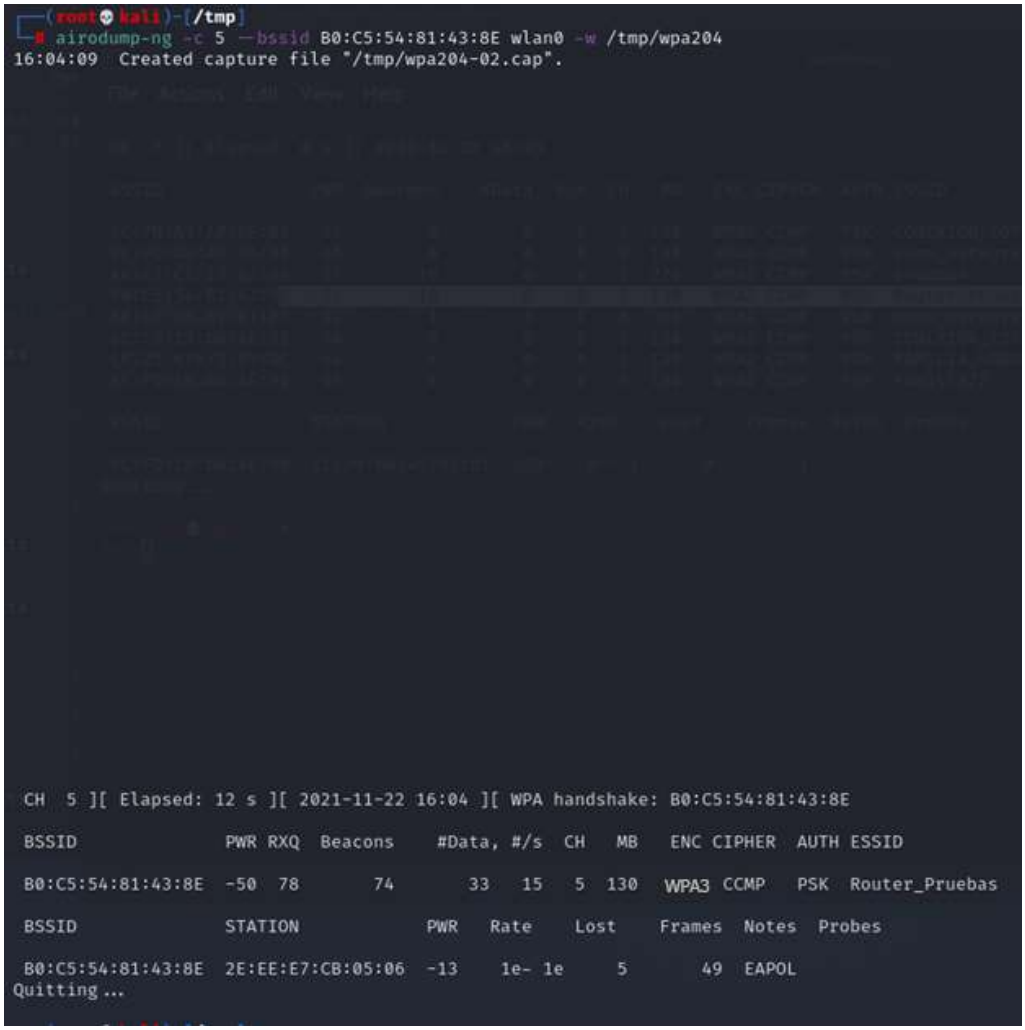


Figura 100: Obtención del handshake mediante comandos en modo consola.

Fuente: Elaboración Propia.

Figura 101: Descifrado de la contraseña mediante aircrak-ng. Fuente: Elaboración Propia.

Descripcion del Ataque de Fuerza Bruta en WPA3

El ataque de fuerza bruta tuvo éxito al utilizar el protocolo WPA3 esto se comprueba en la imagen anterior ya que ahí se evidencia que se logo obtener la clave del Access point, el tiempo de respuesta del ataque hacia este protocolo es mas lento que los antes presentados.

4. Ataque DoS a red wifi en WPA2

El ataque DoS permite para desconectar a un cliente en específico o a su vez para saturar el Access point (Router). Para realizar este ataque se requiere utilizar los comandos que se muestran a continuación:

a) Visualizar si se cuenta con un adaptador de red inalámbrico para ello utilizamos el comando que se muestra a continuación.

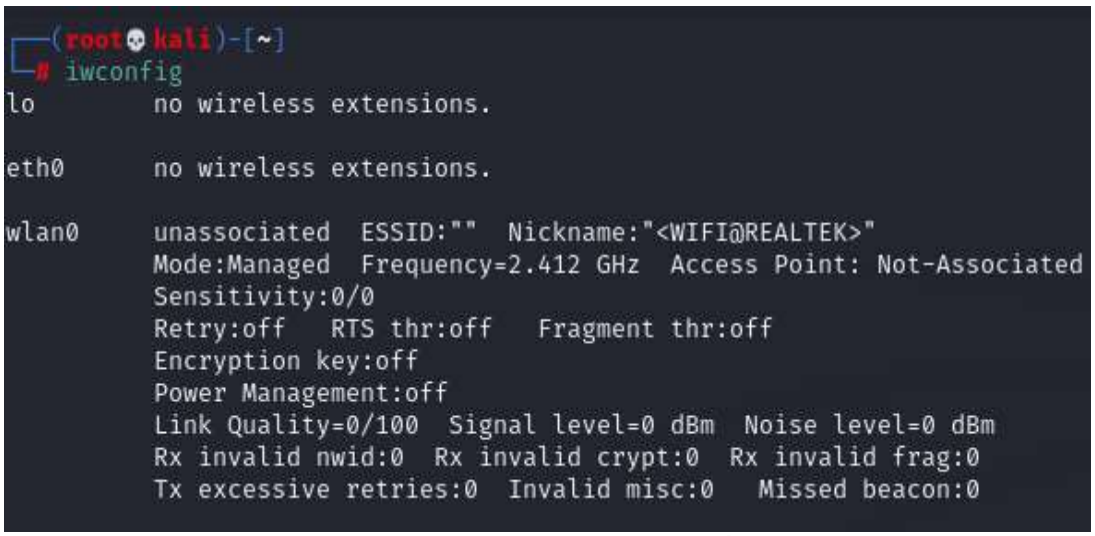


Figura 102: Reconocimiento de la red inalámbrica WPA2. Fuente: Elaboración Propia.

b) Después de que se haya identificado que existe una red inalámbrica se procede a poner en modo monitor para ello se ejecuta el comando que se muestra a continuación.

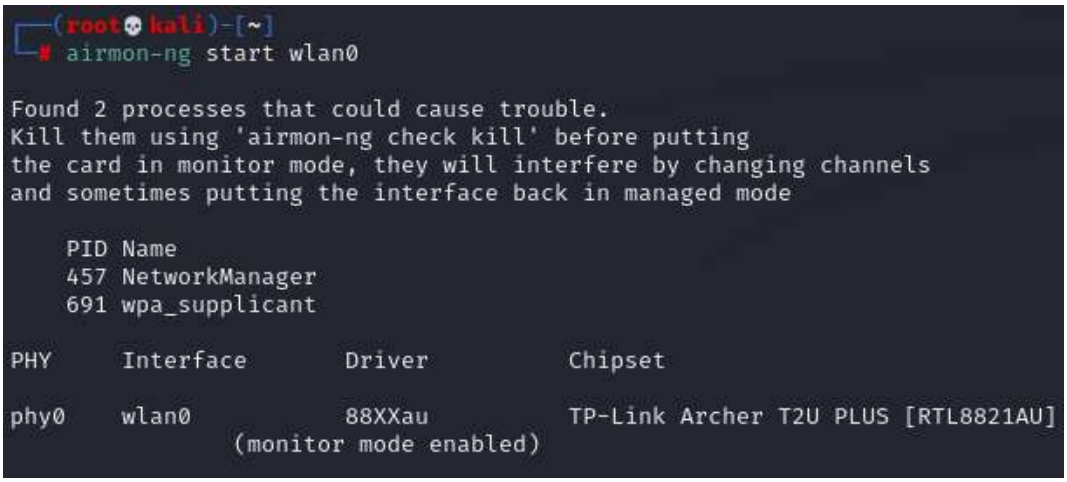


Figura 103: ejecución del comando airmon-ng start wlan0 que pone la interfaz inalámbrica en modo monitor. Fuente: Elaboración Propia.

c) Cuando la red haya cambiado a modo monitor es necesario realizar un escaneo de redes para conocer el bssid, canal, protocolo de seguridad y para conocer si la red que va a ser atacada cuenta con clientes.

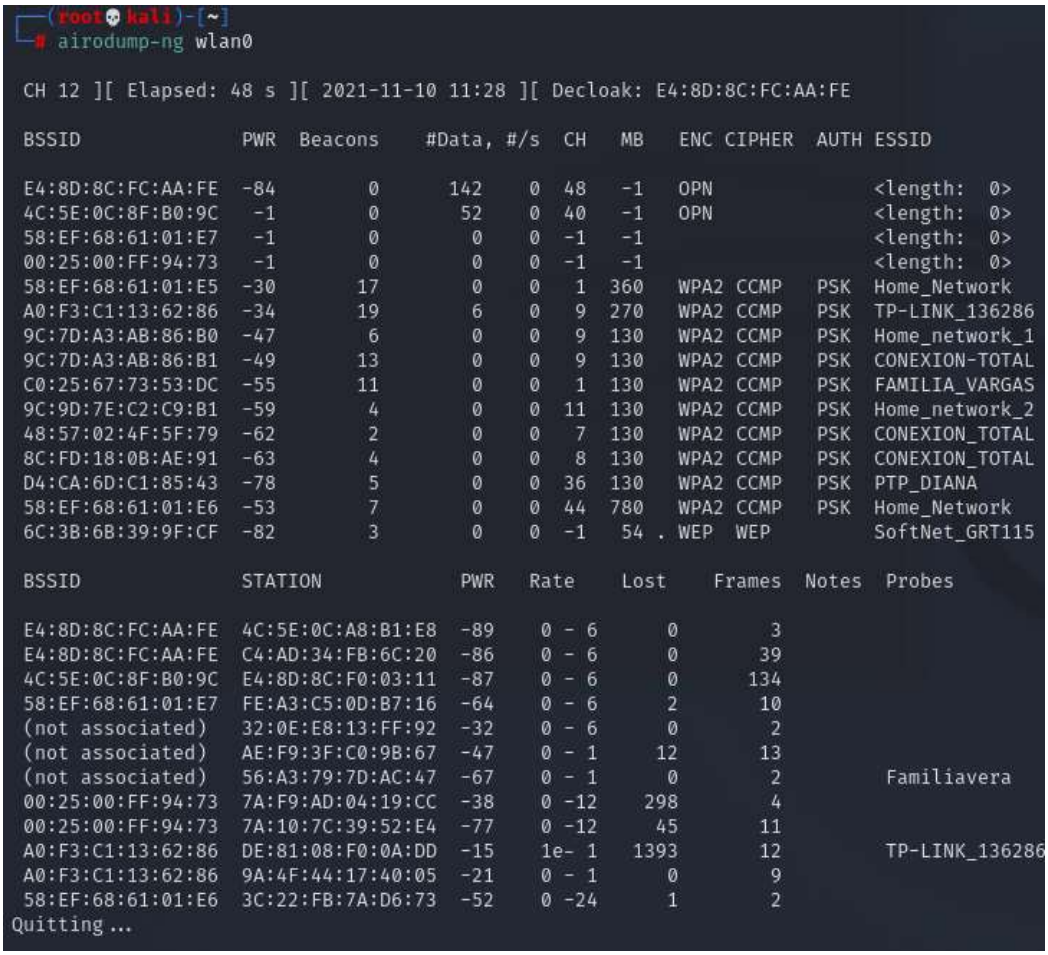


Figura 104: Reconocimiento de la red objetivo y comprobación de cliente. Fuente: Elaboración Propia.

d) Para conocer con mayor detalle los clientes que se encuentran autenticados a la red de interés se ejecuta el comando que se muestra a continuación, ya que permite conocer únicamente los clientes de dicha red.

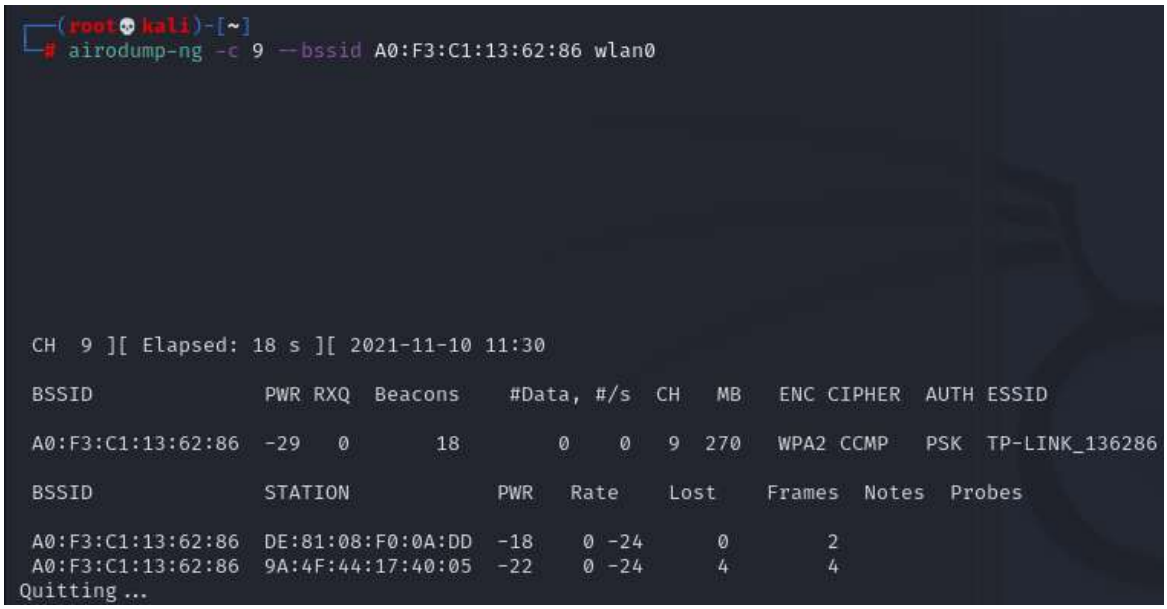


Figura 105: Establecimiento del objetivo mediante el comando airodump-ng -c 9 == bssid. Fuente: Elaboración Propia.

e) Después que se haya identificado correctamente los parámetros del router se procede a saturar el mismo con el fin de que ningún cliente pueda mantener una conexión.

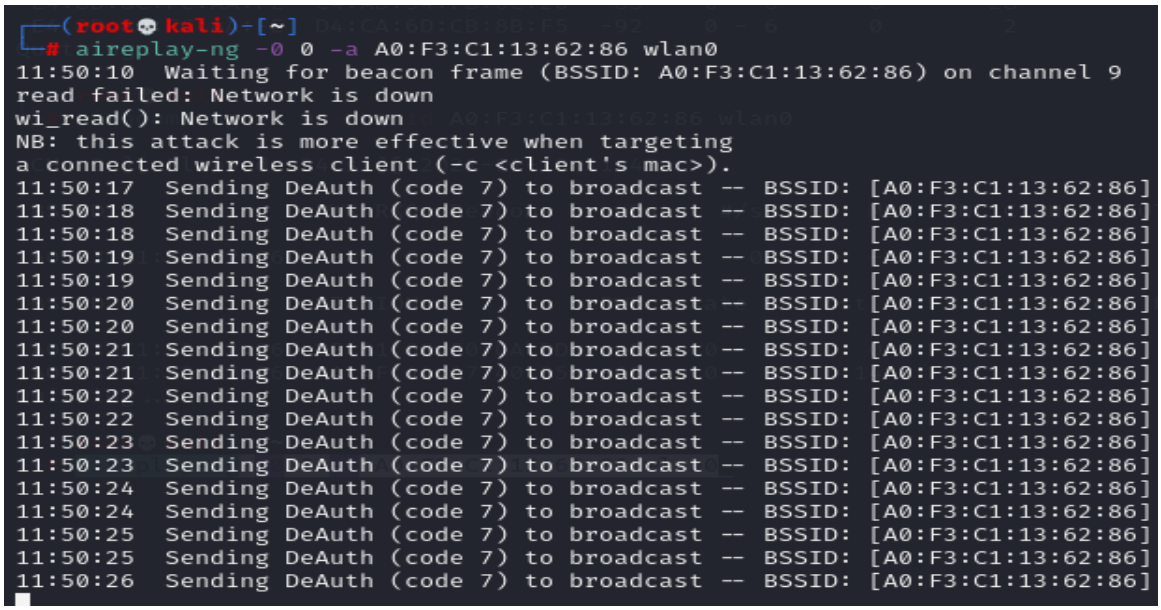


Figura 106: Saturación del router. Fuente: Elaboración Propia.

f) En caso de que no se desee saturar el router se puede desautenticar a un cliente para ello utilizamos el comando que se muestra a continuación, para esto es importante conocer la MAC del cliente que se desea desautenticar.

```
┌──(root💀kali)-[~]
└─# aireplay-ng -0 0 -a A0:F3:C1:13:62:86 -c DE:81:08:F0:0A:DD wlan0
12:19:47  Waiting for beacon frame (BSSID: A0:F3:C1:13:62:86) on channel 9
12:19:52  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [66|63 ACKs]
12:19:53  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [57|60 ACKs]
12:19:54  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [25|60 ACKs]
12:19:54  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 2|59 ACKs]
12:19:55  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 3|61 ACKs]
12:19:56  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|60 ACKs]
12:19:56  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|56 ACKs]
12:19:57  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|49 ACKs]
12:19:58  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|60 ACKs]
12:19:58  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|62 ACKs]
12:19:59  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|55 ACKs]
12:19:59  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 3|55 ACKs]
12:20:00  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 0|26 ACKs]
12:20:01  Sending 64 directed DeAuth (code 7). STMAC: [DE:81:08:F0:0A:DD] [ 1|40 ACKs]
```

Figura 107: Desautenticación de un cliente usando su dirección MAC. Fuente: Elaboración Propia.

g) Luego el cliente se muestra fuera de conexión como se señala en la siguiente figura:

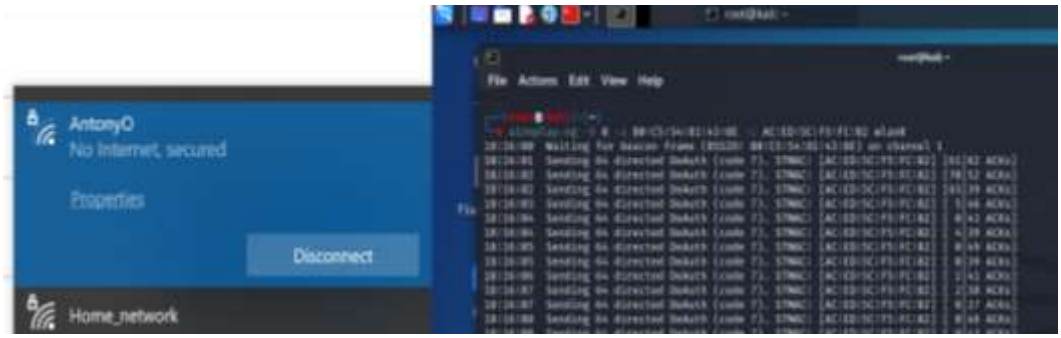


Figura 108: Cliente desautenticado en WPA2. Fuente: Elaboración Propia.

Descripción del Ataque DoS a red wifi en WPA2

El ataque DoS en el protocolo WPA2 fue efectivo ya que se logró saturar el router de pruebas dejando sin comunicación a sus clientes, también se logró desautenticar a uno de los clientes que se encontraba conectado, este ataque tuvo un tiempo de respuesta un poco tardío debido al cifrado que posee el protocolo.

Ataque DoS con el protocolo WPA

Para realizar el ataque DoS hacia el protocolo WPA es importante seguir los mismos pasos que se siguieron para WPA2 ya que lo único que cambia es la configuración del protocolo en el Access point y como se puede visualizar en las siguientes imágenes el tráfico que se obtenga será del protocolo WPA.

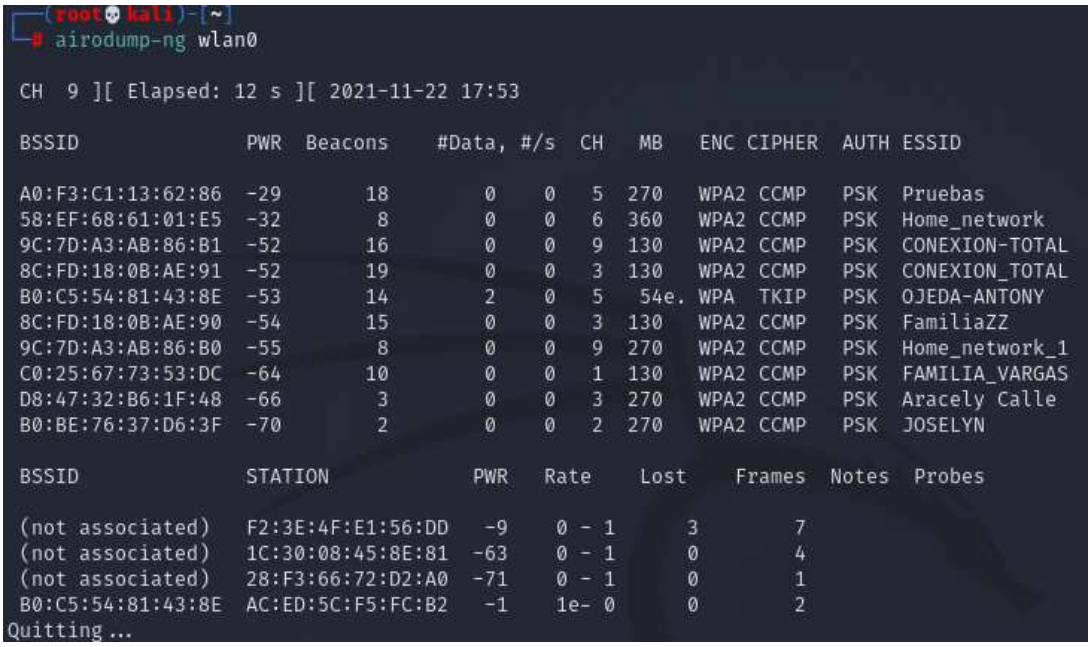


Figura 109: Reconocimiento de la red inalámbrica WPA. Fuente: Elaboración Propia.

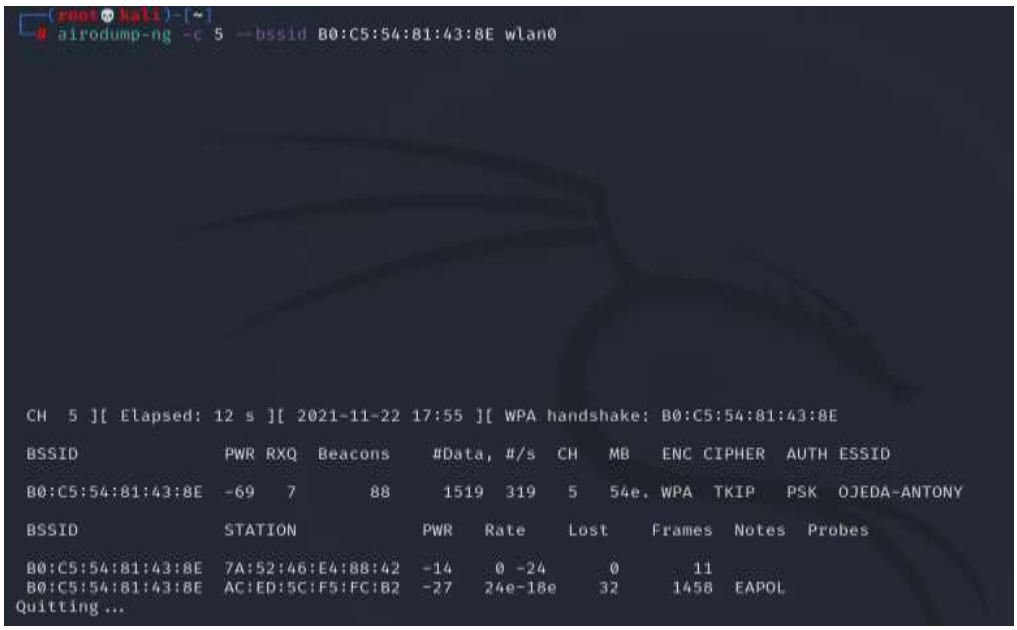


Figura 110: Establecimiento del objetivo mediante el comando airodump-ng -c 9 == bssid. Fuente: Elaboración Propia.

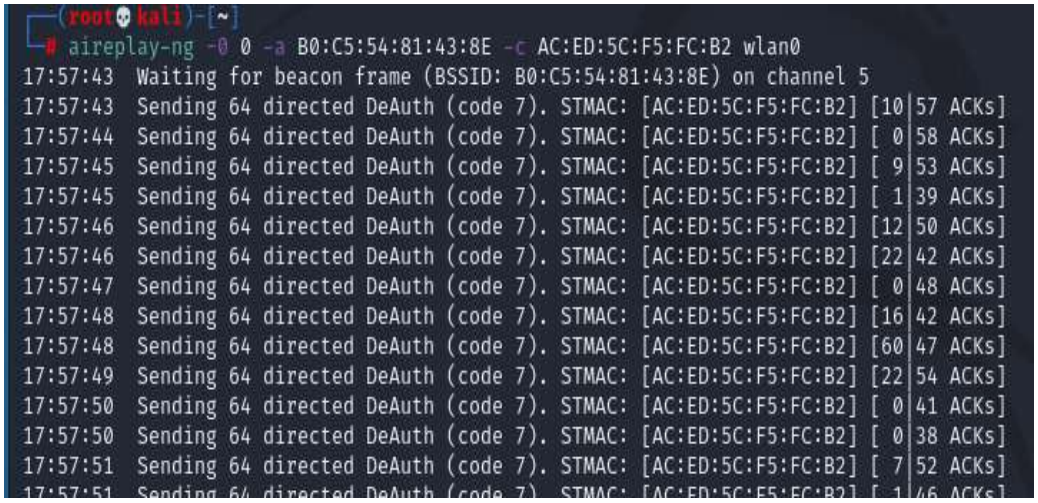


Figura 111: Saturación del router. Fuente: Elaboración Propia.

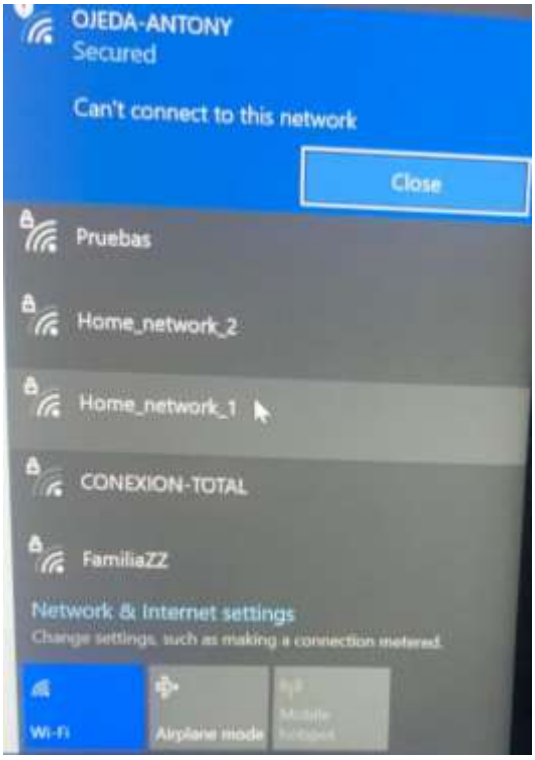


Figura 112: Cliente desautenticado en WPA. Fuente: Elaboración Propia.

Descripción del Ataque DoS a red wifi en WPA

El ataque DoS en el protocolo WPA se realiza en menor tiempo que en WPA2 esto se debe al tipo de cifrado que tiene cada protocolo. Este ataque fue exitoso porque se desauténtico al cliente con éxito dejándolo sin comunicación y sin poder volver a conectarse a la misma red, también se saturo el router con éxito y en menor tiempo ya que ningún cliente podía entablar una conexión hacia dicha red.

Ataque DoS con el protocolo WPA3

Para realizar el ataque DoS hacia el protocolo WPA3 es importante seguir los mismos pasos que se indicaron anteriormente ya que la única diferencia es la configuración del protocolo en el Access point, como se visualiza a continuación el tráfico que se obtiene es del protocolo WPA3.

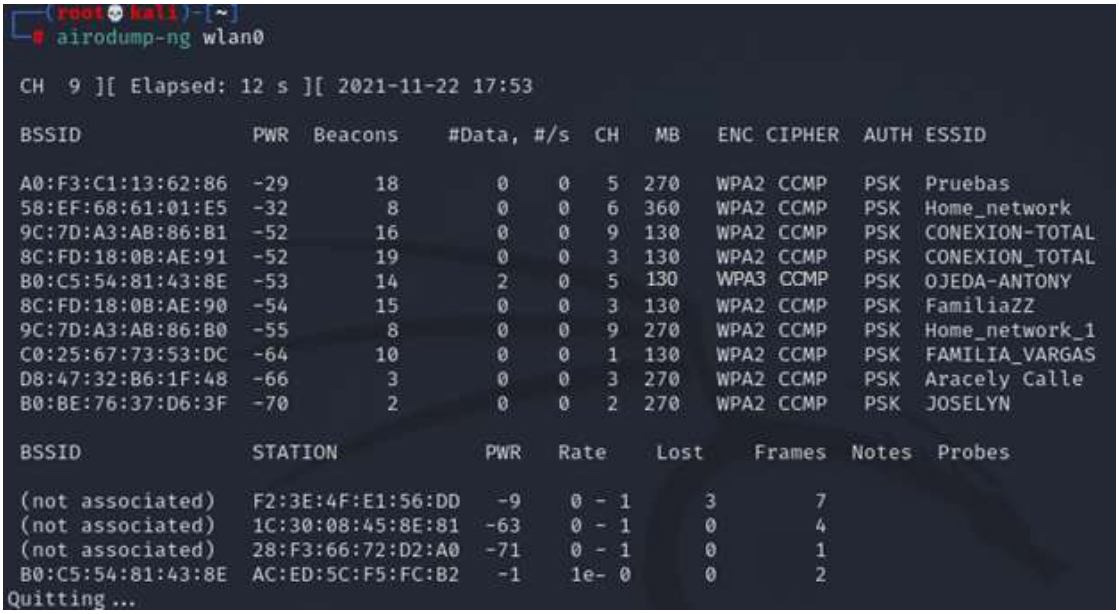


Figura 113: Reconocimiento de la red inalámbrica WPA. Fuente: Elaboración Propia.

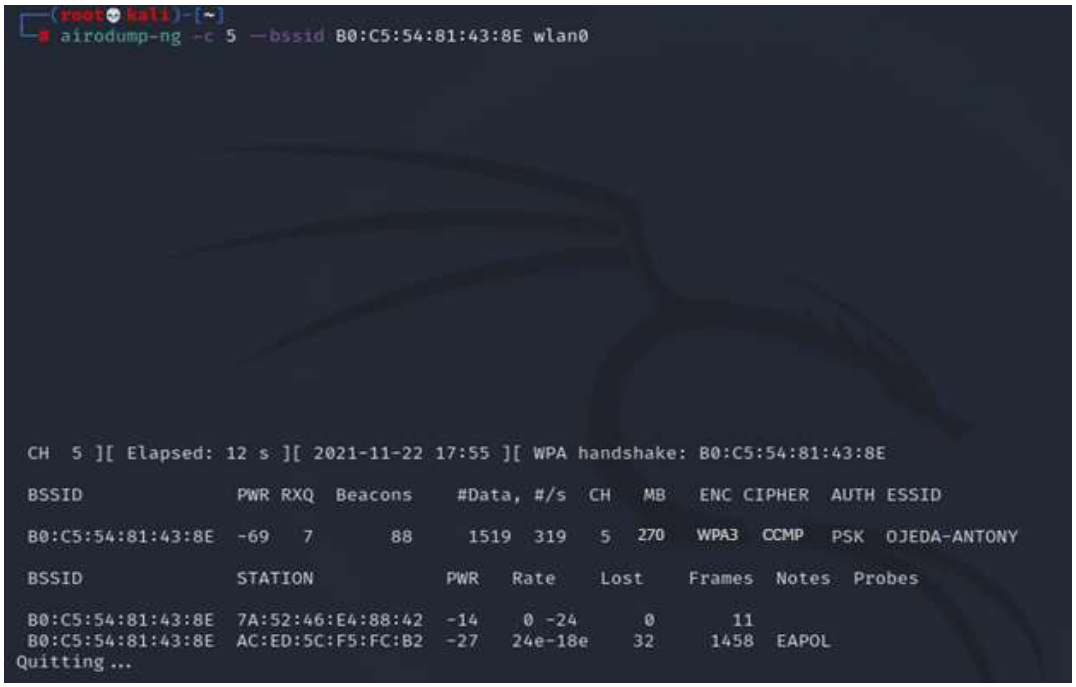


Figura 114: Establecimiento del objetivo mediante el comando airodump-ng -c 9 == bssid. Fuente: Elaboración Propia.

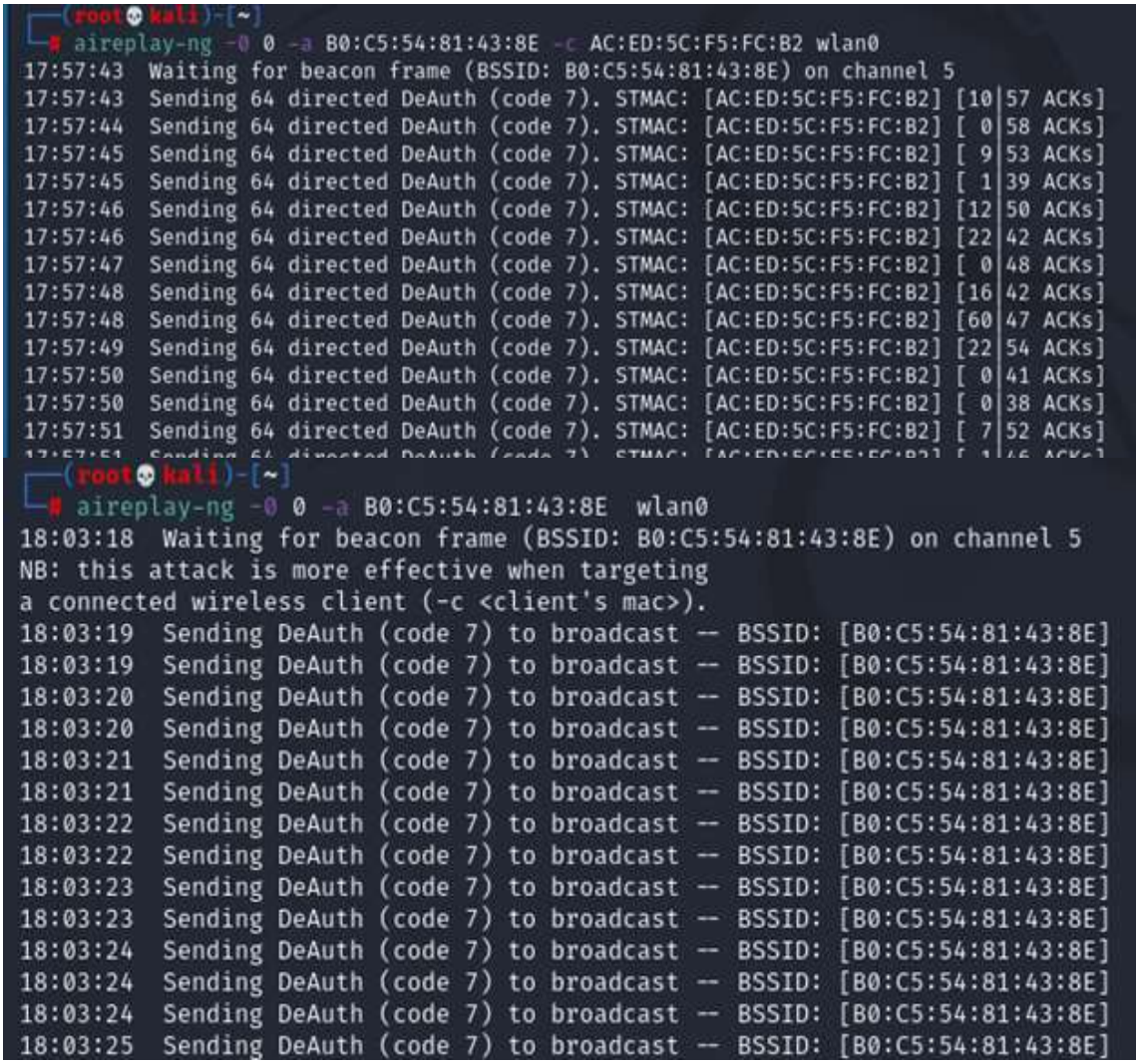


Figura 115: Saturación del router. Fuente: Elaboración Propia.

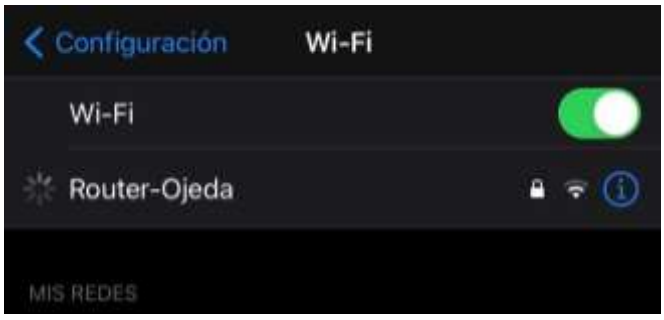


Figura 116: Cliente desautenticado. Fuente: Elaboración Propia.

Descripción del Ataque DoS a red wifi en WPA3

El ataque DoS en el protocolo WPA3 tuvo éxito ya que se logra desautenticar al cliente y saturar el Access point, este ataque hacia el protocolo WPA3 tomas más tiempo.

5. Suplantación de identidad de WPA2

La suplantación de identidad consiste en hacerse pasar por otra persona con fines de robar datos, realizar engaños o fraudes para obtener un beneficio económico, también se puede presentar ciber-acoso o a su vez extorsión. Para llevar a cabo este ataque es necesario seguir los siguientes pasos.

a) Ingresar a Wisflax, WPA y finalmente en la herramienta Linset, tal como se muestra a continuación.

Figura 117: Acceso a la herramienta LINSET. Fuente: Elaboración Propia.

b) Después que se ingrese a linset se realizara un escaneo general de toda la maquina con el fin de ver todos los ajustes que se necesitaran posteriormente.

Figura 118: Escaneo de la herramienta en la máquina atacante. Fuente: Elaboración Propia.

c) Al momento que termine de realizar todo el escaneo se podrá visualizar las interfaces de red que existen en la máquina, en este caso solo hay una interfaz ya que se cuenta únicamente con una tarjeta inalámbrica, se selecciona la tarjeta que se tiene y continuamos.

Figura 119: Reconocimiento de la interfaz de red. Fuente: Elaboración Propia.

d) Es importante escanear todos los canales para conocer cuál de ellos es de interés para el ataque. En caso de que se requiera analizar únicamente un canal se deberá seleccionar la opción 2 en este caso se optara por la opción1.

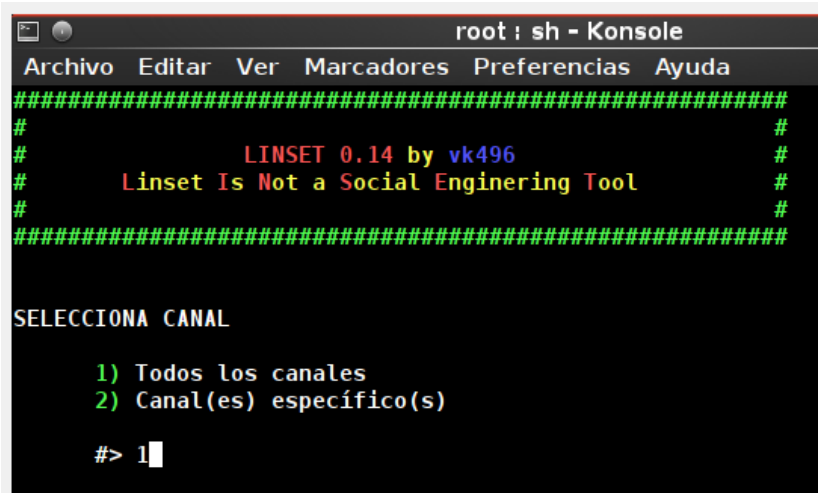


Figura 120: Selección del canal. Fuente: Elaboración Propia.

e) Se escanean todos los canales que la red inalámbrica alcanza a leer, dentro de este escaneo se puede observar el bssid, el protocolo, el canal y el nombre de la red.

Figura 121: Escaneo de los canales. Fuente: Elaboración Propia.

f) Cuando encuentre la red a vulnerar se puede cerrar la ventada de escaneo y posteriormente se visualiza todos los wifis con diferentes opciones de tal manera que se deberá escoger la red que se quiere vulnerar.

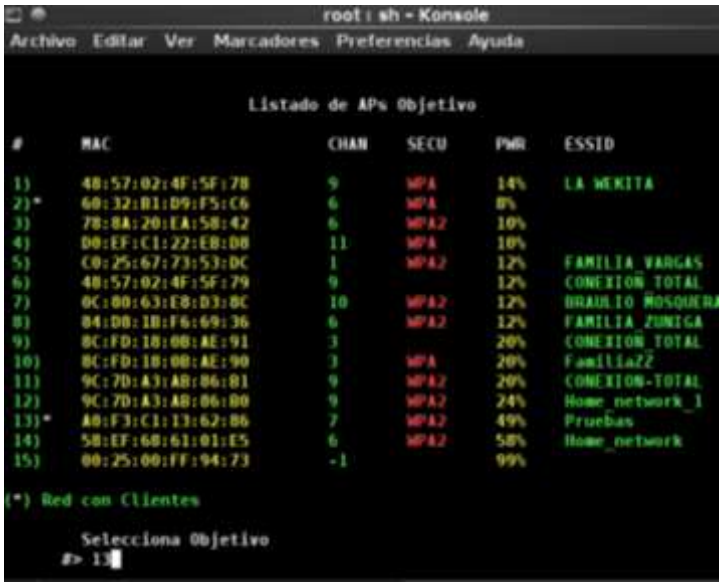


Figura 122: Selección de la “víctima” objetivo. Fuente: Elaboración Propia.

g) Una vez que se selecciona la red a vulnerar se visualizará el SSID, Canal, Velocidad y la MAC del router, también se visualiza 3 opciones, en este caso se escogerá la opción 1 ya que es la que la herramienta linset recomienda.

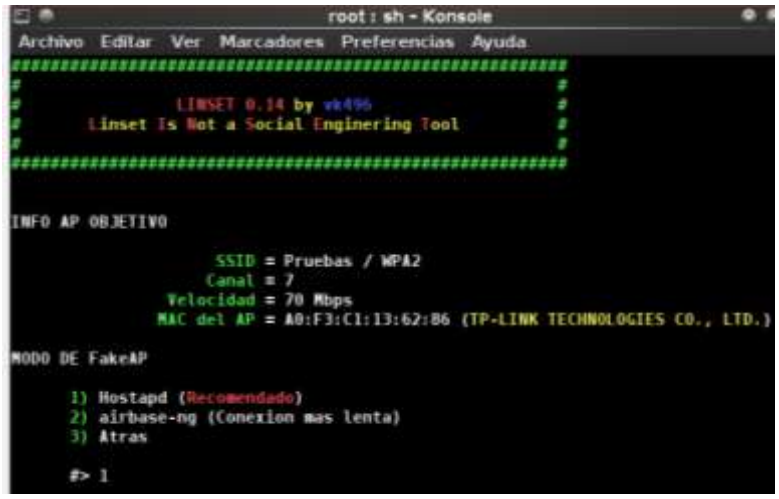


Figura 123: Selección de la opción hostapd que permite que una tarjeta de interfaz de red actúe como un punto de acceso y servidor de autenticación. Fuente: Elaboración Propia.

h) A continuación, indica que se debe ingresar una ruta para guardar el paquete que permitirá obtener la contraseña en este caso se dejará la ruta predeterminada de tal manera que se presionará ENTER.

Figura 124: Selección de la ruta para guardar el paquete con la contraseña. Fuente: Elaboración Propia.

i) Es importante comprobar el handshake, existen 3 opciones, pero en este caso se utilizara la opción Pyrit dado que tiene muchas funcionalidades enfocadas principalmente a descifrar claves.

Figura 125: Selección de la comprobación de Handshake. Fuente: Elaboración Propia.

j) A continuación, se procederá a capturar el handshake del cliente, para ello se ha optado por escoger la opción 1 ya que permite realizar una des autenticación masiva del Access Point.

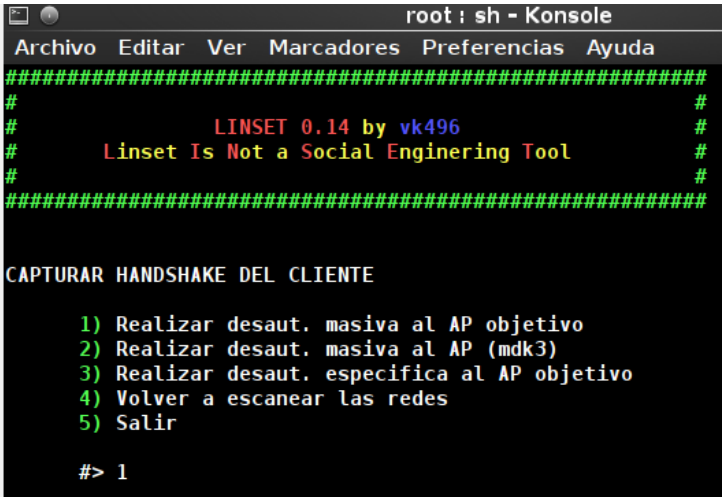


Figura 126: Captura del handshake del cliente. Fuente: Elaboración Propia.

k) Una vez que se tenga el paquete con la posible contraseña se procederá a comprobar si ya se tiene el hansdhake para ello se escoge la opción 1.

Figura 127: Comprobación de la captura de handshake. Fuente: Elaboración Propia.

l) Después se comprobará si ha capturado el handshake correctamente si en la ventana que se presenta a continuación se presenta la palabra Corrupto significa que se puede llevar a cabo el ataque de tal manera que se debe escoger la opción 1.

Figura 128: Realización del ataque luego de capturar el handshake. Fuente: Elaboración Propia.

m) Después de haber iniciado el ataque es importante seleccionar la opción una para obtener la interfaz web que le llegara a la víctima para que ingrese la contraseña de la red que es de interés.

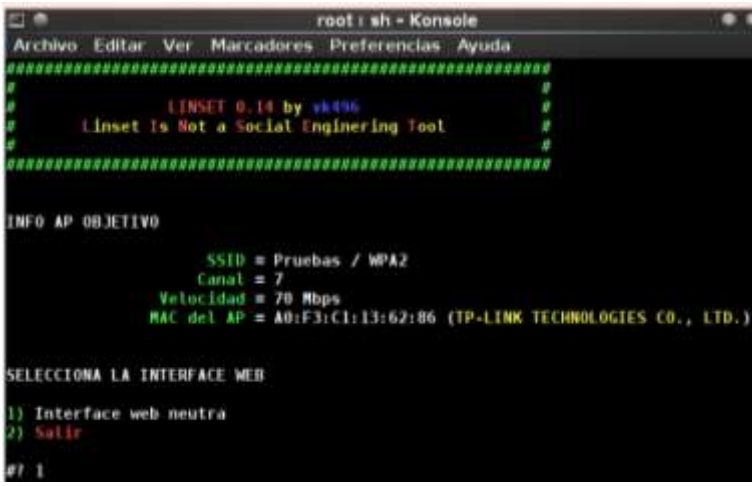


Figura 129: Selección de la interfaz web para la víctima. Fuente: Elaboración Propia.

n) Después de seleccionar la interfaz web que se enviará a la víctima es importante escoger un idioma para ello se deberá seleccionar el idioma de su preferencia, en este caso se selecciona la opción 2.

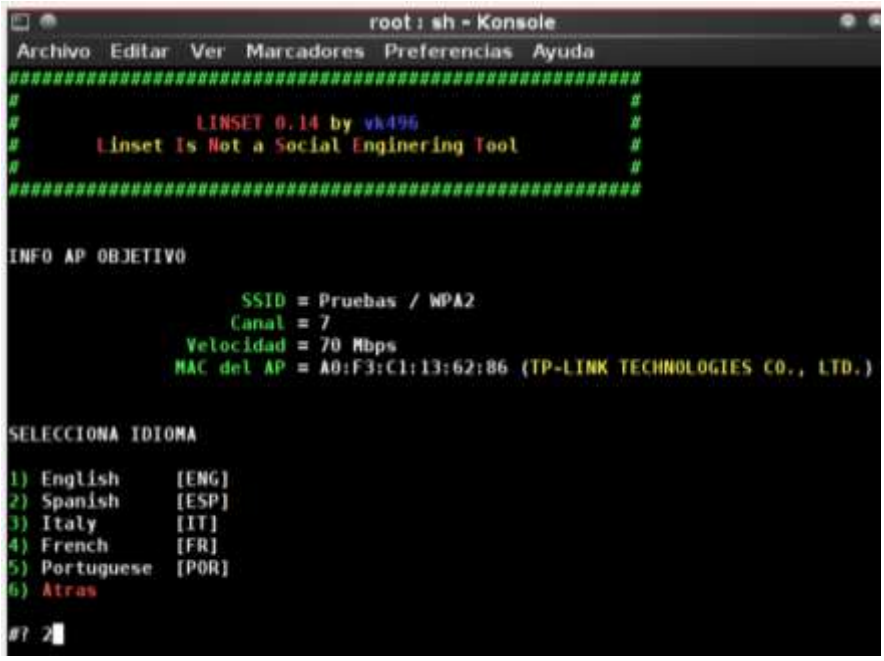


Figura 130: Selección del idioma de la interfaz web para la víctima. Fuente: Elaboración Propia.

o) Después de que se haya seleccionado la interfaz web y el idioma se procederá a desconectar el cliente con el fin de que el cliente se autentique al Access point que se suplanto.

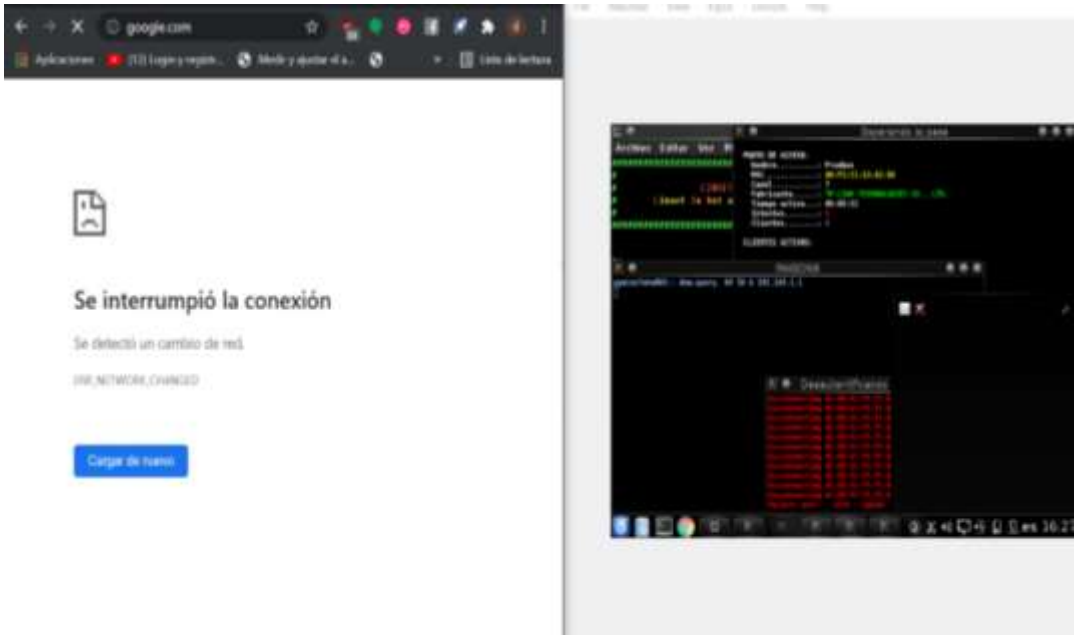


Figura 131: Interrupción de la conexión de la víctima. Fuente: Elaboración Propia.

p) Al momento que el cliente pierda la conexión y actualice de nuevo la página aparece la interfaz que se muestra en la siguiente imagen, en donde el cliente deberá ingresar la contraseña del router.

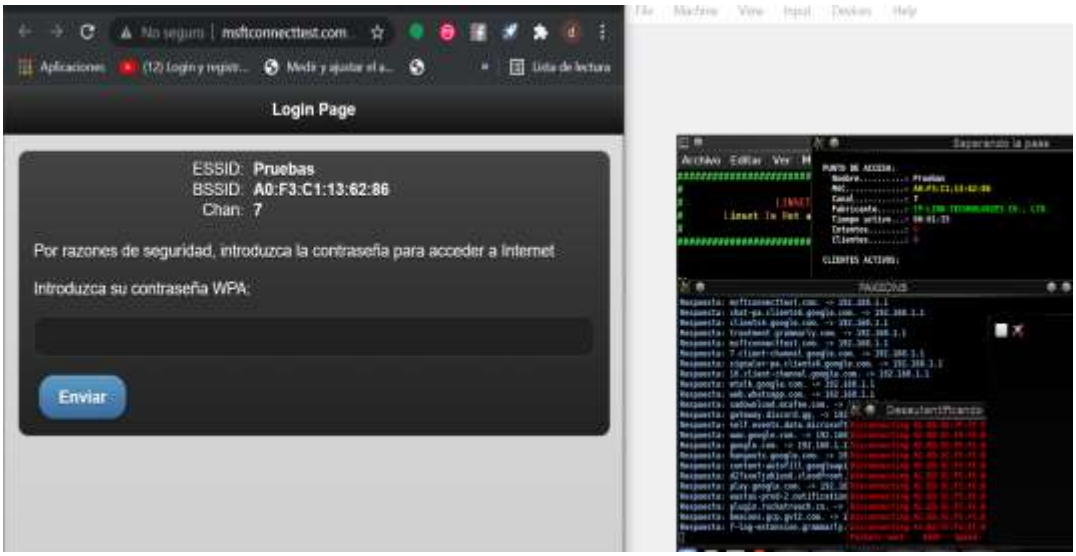


Figura 132: Acceso a interfaz por parte de la víctima. Fuente: Elaboración Propia.

q) Después de que el cliente ingrese la contraseña el atacante obtendrá la clave del router en una ventana igual a la que se muestra en la siguiente figura y el cliente pobra observar un mensaje que indica que la conexión se restablecerá en pocos minutos.

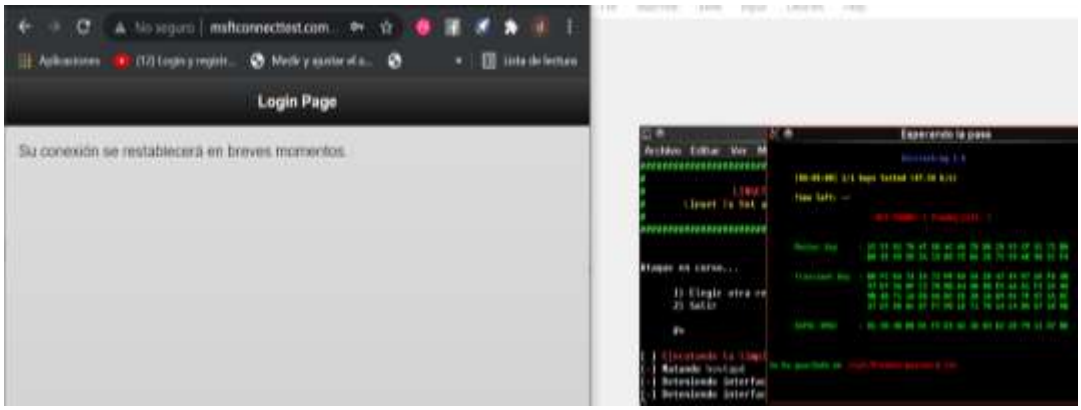


Figura 133: Obtención de la contraseña del router mediante la interfaz. Fuente: Elaboración Propia.

Descripción del Ataque de Suplantación de identidad de WPA2

La suplantación de identidad en el protocolo WPA2 tuvo éxito puesto que se logró obtener la clave del Access point ya que se envió una página web al cliente que se encontraba conectado a esa red indicando que tuvo un problema de conexión que necesita ingresar nuevamente la contraseña para poder mantener una conexión a la red, la suplantación de identidad en este protocolo tarda más tiempo en penetrarse que en el protocolo WPA esto se da debido al tipo de seguridad y encriptación que tienen.

Suplantación de identidad con el protocolo WPA

Para llevar a cabo el ataque de suplantación de identidad en el protocolo WPA es recomendable seguir los pasos que se describen anteriormente debido a que es el mismo ataque que ya se realizó la única diferencia notoria es el cambio de protocolo en el router que se ejecutando las pruebas.

Figura 134: Escaneo de los canales. Fuente: Elaboración Propia.

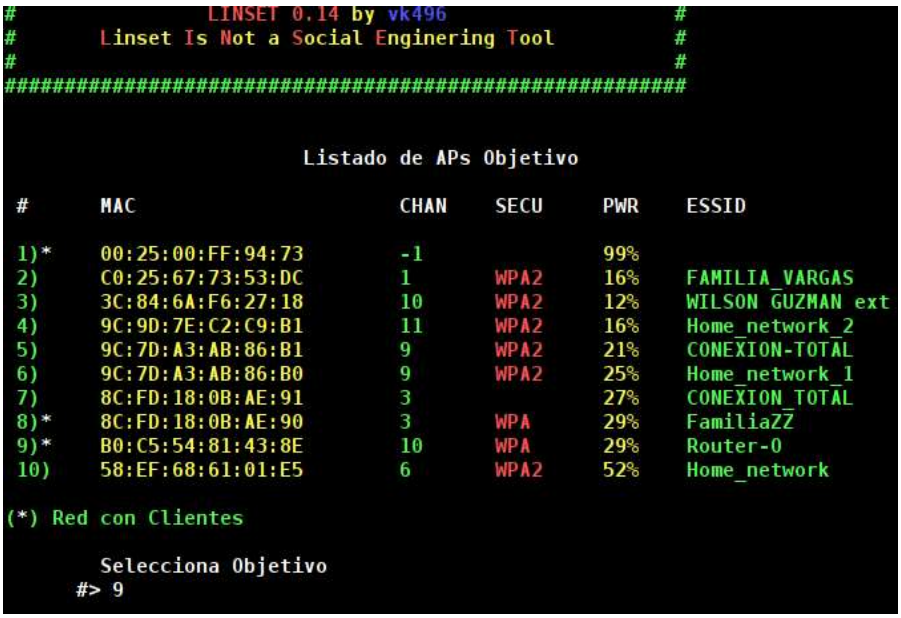


Figura 135: Selección de la víctima objetivo. Fuente: Elaboración Propia.

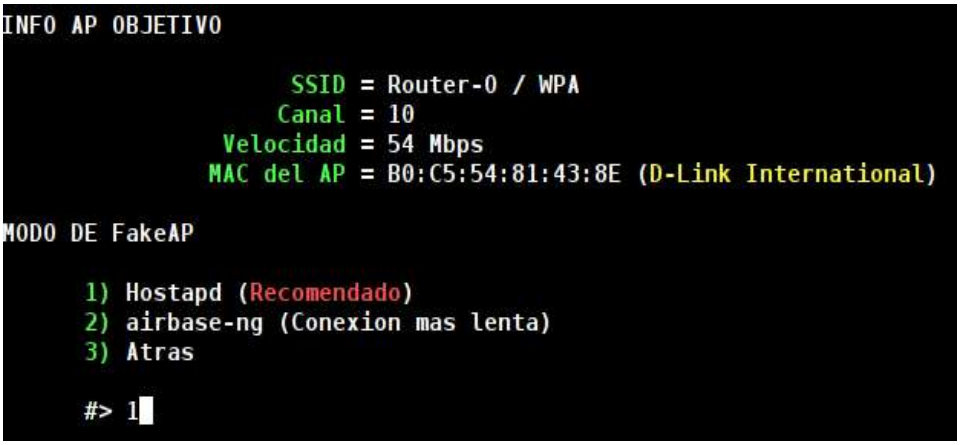


Figura 136: Selección de la opción hostapd que permite que una tarjeta de interfaz de red actúe como un punto de acceso y servidor de autenticación. Fuente: Elaboración Propia.

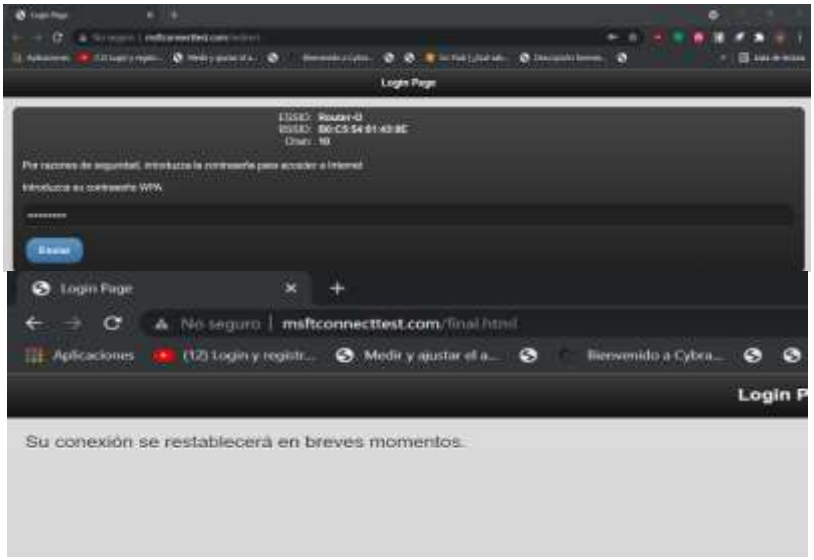


Figura 137: Acceso a interfaz por parte de la víctima. Fuente: Elaboración Propia.

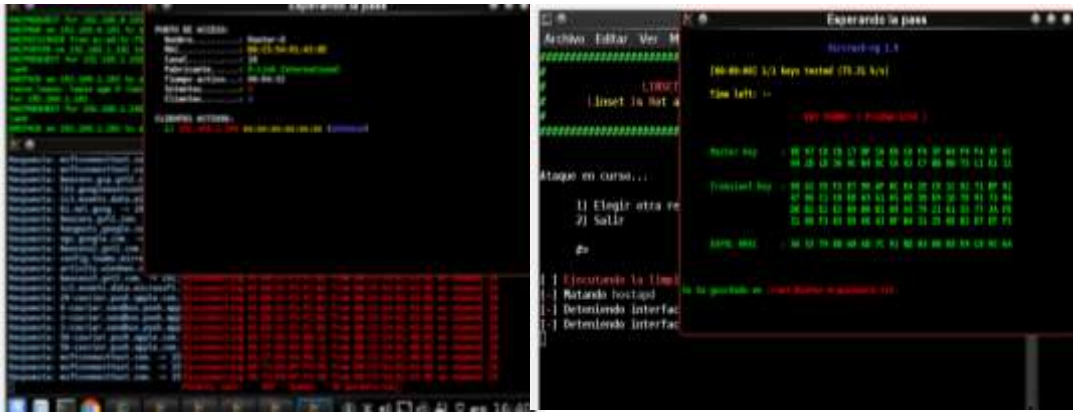


Figura 138: Obtención de la contraseña del router mediante la interfaz. Fuente: Elaboración Propia.

Descripción del Ataque de Suplantación de identidad de WPA

El ataque de suplantación de identidad en el Protocolo WPA tuvo éxito ya que envió con éxito la interfaz web a los clientes que intentaban mantener una conexión con el router que fue interceptado dando paso a que los clientes ingresen la contraseña. El tiempo de espera con este protocolo es más corto que en WPA2.

Suplantación de identidad con el protocolo WPA3

Para llevar a cabo el ataque de suplantación de identidad en el protocolo WPA3 es recomendable seguir los pasos que se describen anteriormente debido a que es el mismo ataque que ya se realizó la única diferencia notoria es el cambio de protocolo en el router.

Figura 139: Escaneo de los canales. Fuente: Elaboración Propia.

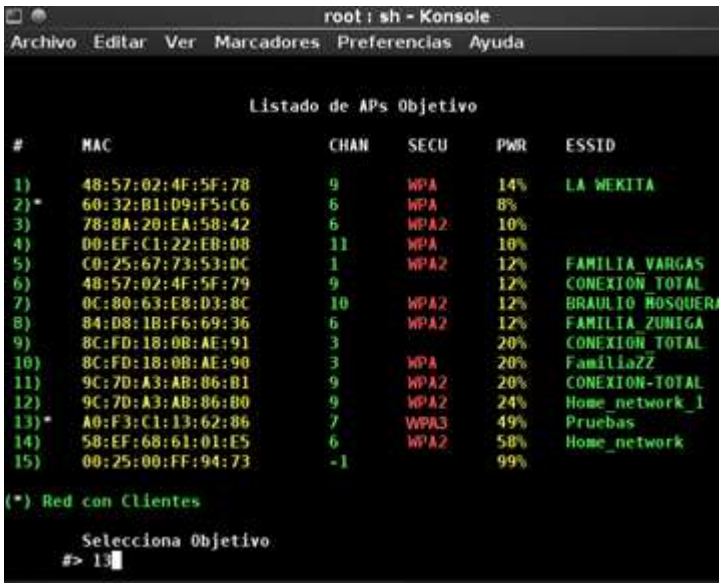


Figura 140: Selección de la víctima objetivo. Fuente: Elaboración Propia.

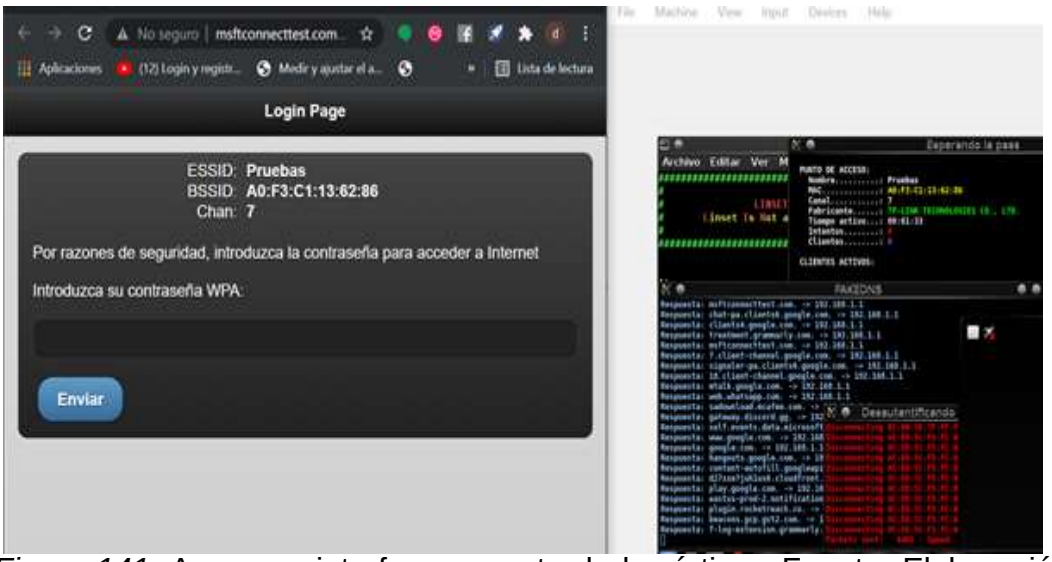


Figura 141: Acceso a interfaz por parte de la víctima. Fuente: Elaboración Propia.

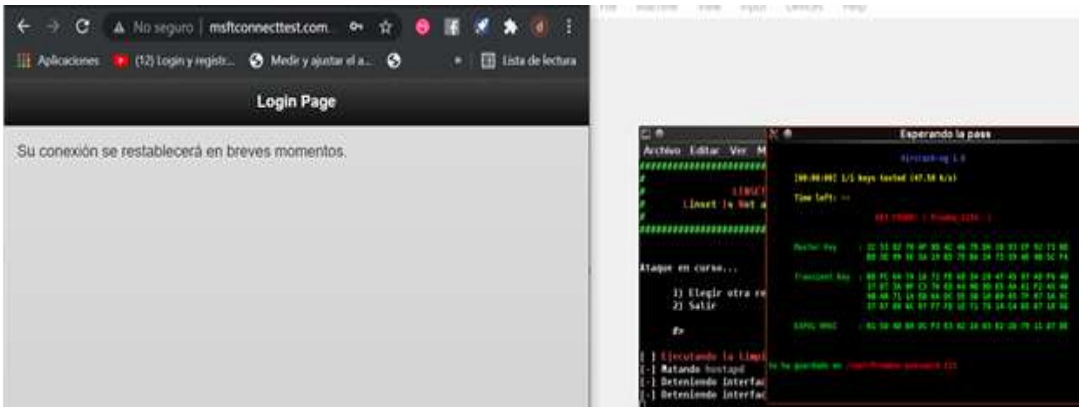


Figura 142: Obtención de la contraseña del router mediante la interfaz. Fuente: Elaboración Propia.

Descripción del Ataque de Suplantación de identidad de WPA3

El ataque de suplantación de identidad en el Protocolo WPA3 tuvo éxito ya que envió la interfaz web a los clientes que intentaban mantener una conexión con el router que fue interceptado dando paso a que los clientes ingresen la contraseña para una posible conexión, aunque en mucho mayor tiempo que en WPA2 y WPA

6. Ataque de diccionario a un bssid oculto en WPA2

El ataque de diccionario consiste en crear un archivo de texto con posibles palabras que suelen utilizar en las contraseñas, se dice que este ataque es más efectivo que el de fuerza bruta ya que este no realiza combinaciones de letras, números, signos, etc. únicamente se base en utilizar palabras existentes en la lengua española, este tipo de ataque tiene poca probabilidad de éxito ya que si la contraseña del router no existe dentro del archivo de texto el ataque no será efectivo. Un SSID Oculto es aquel que no se muestra dentro de las redes disponibles que suelen apreciarse en el pc o en un Smartphone.

Para llevar a cabo este ataque se utilizará los pasos que se muestran a continuación:

a) Es importante realizar una previa configuración al router, en donde se indique que se desea habilitar la conexión inalámbrica oculta.

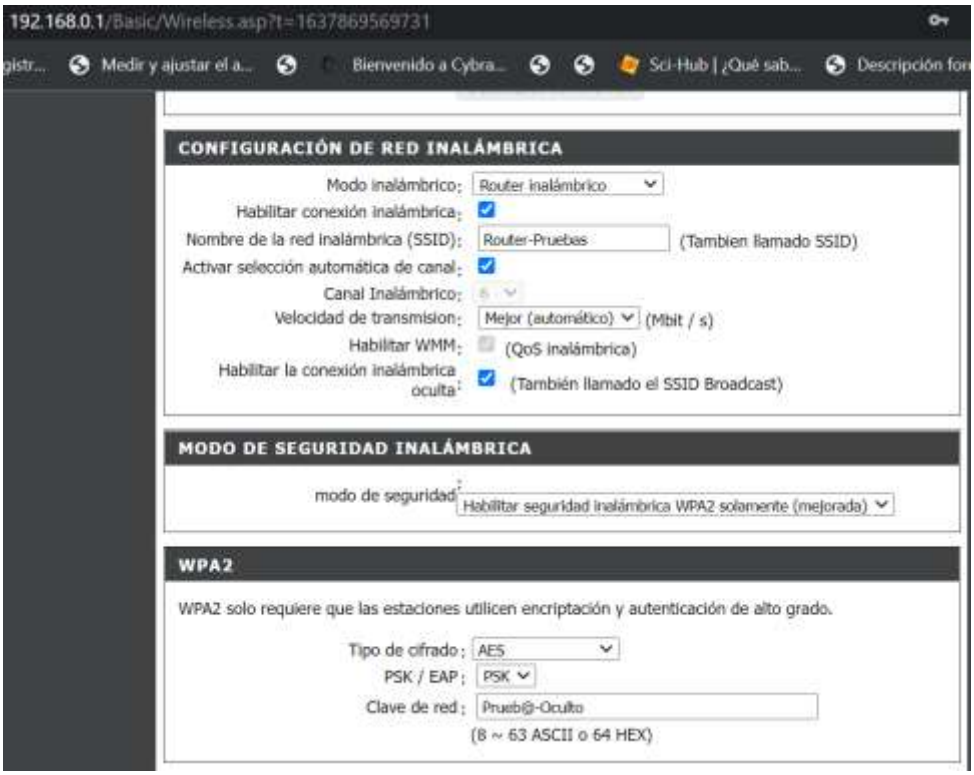


Figura 143: Configuración del router para ataque de diccionario con bssd oculto. Fuente: Elaboración Propia.

b) Cuando se haya finalizado con la configuración del equipo es importante conocer el estado en el cual se encuentra la tarjeta inalámbrica, también es importante matar todos los procesos que puedan interferir después para ello se utiliza los comandos que se muestran a continuación.

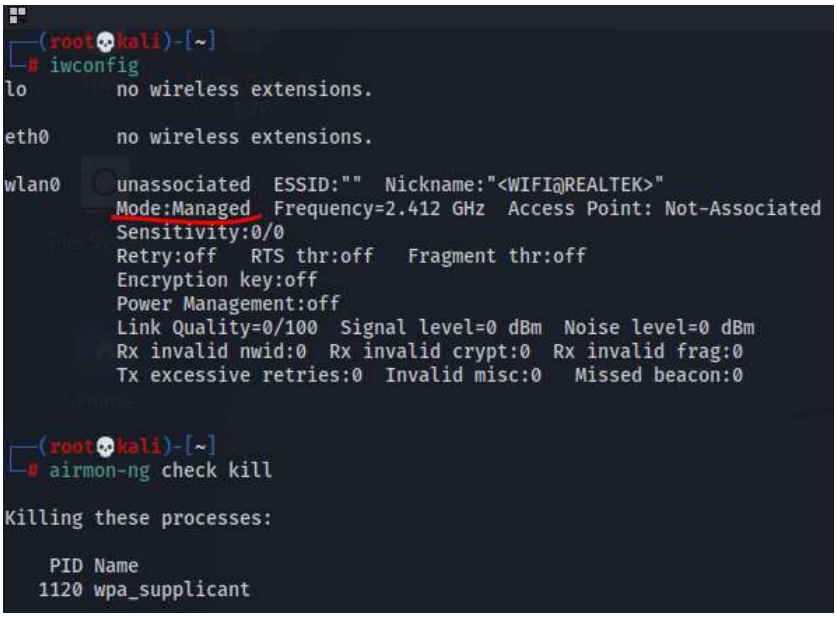


Figura 144: Comprobación de la tarjeta inalámbrica oculto. Fuente: Elaboración Propia.

c) Después de que se haya verificado el modo de la tarjeta inalámbrica y se haya matado a todos los procesos se procede a cambiar el modo de la tarjeta a monitor, posteriormente se comprobara que se haya cambiado de estado para este paso se utilizan los comandos que se muestran en la siguiente imagen.

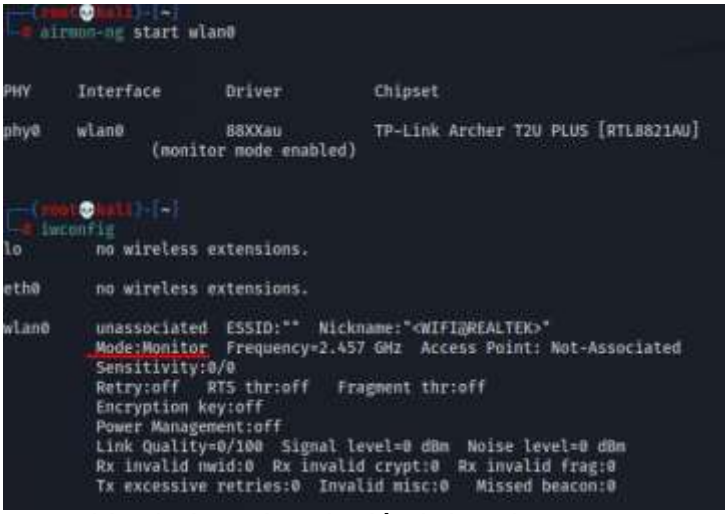


Figura 145: Cambio de la tarjeta inalámbrica de atacante a modo monitor. Fuente: Elaboración Propia.

d) Al momento que la tarjeta inalámbrica haya cambiado a modo monitor se procede a realizar un escaneo del tráfico de las redes que se encuentran en el aire. Recordemos que la red a la cual se va a auditar se encuentra oculta de tal manera que no se podrá visualizar en las redes disponibles, en cuanto al escaneo del tráfico se podrá visualizar con la palabra **length** lo cual permite que el atacante no identifique la red que quiere auditar.

   Para realizar el escaneo de redes se utiliza el comando **airodump-ng wlan0 (nombre de la tarjeta en modo monitor).**

   A continuación, se muestra el tráfico de redes en el cual se visualiza que en este caso a la red que se va a auditar si se encuentra oculta, puesto que no visualiza dentro de las redes disponibles.

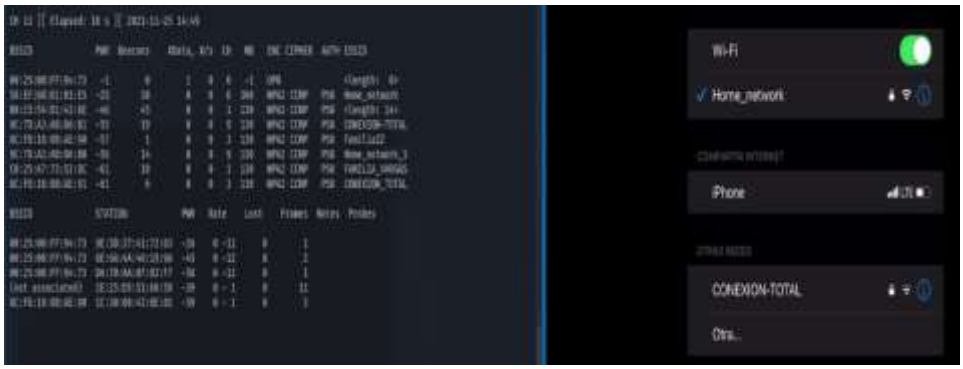


Figura 146: Escaneo de tráfico de redes inalámbricas. Fuente: Elaboración Propia.

e) Al momento que se haya verificado que la red que se va a auditar se encuentra oculta lo que se espera es que algún cliente se conecte a dicha red ya que en ese caso el nombre de la red se podrá visualizar en el escaneo del tráfico de redes que se está realizando.

Para este caso se ha tomado como cliente a un IPhone que se va a conectar a la red que se desea atacar, al momento que el cliente realice la conexión se puede visualizar que el nombre la red aparece en el escaneo.

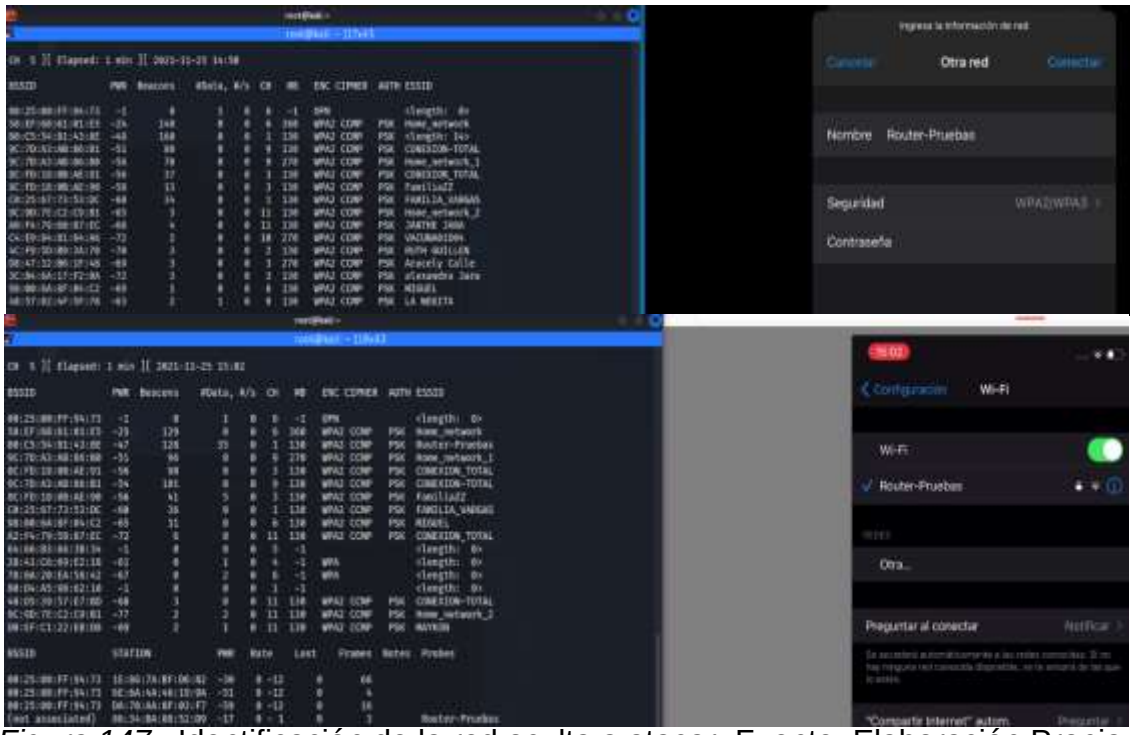


Figura 147: Identificación de la red oculta a atacar. Fuente: Elaboración Propia.

f) Cuando ya se conozca el nombre de la red a la cual se va a dirigir el ataque se procede a capturar y guardar el tráfico específicamente de la red que nos interesa para ello utilizamos el siguiente comando: **airodump-ng -c 1(canal de la red) -w prueba (nombre de archivo en el que se va a guardar el tráfico) –bssid B0:C5: 54:81:43:8E (MAC del Access Point) wlan0(tarjeta de red)**

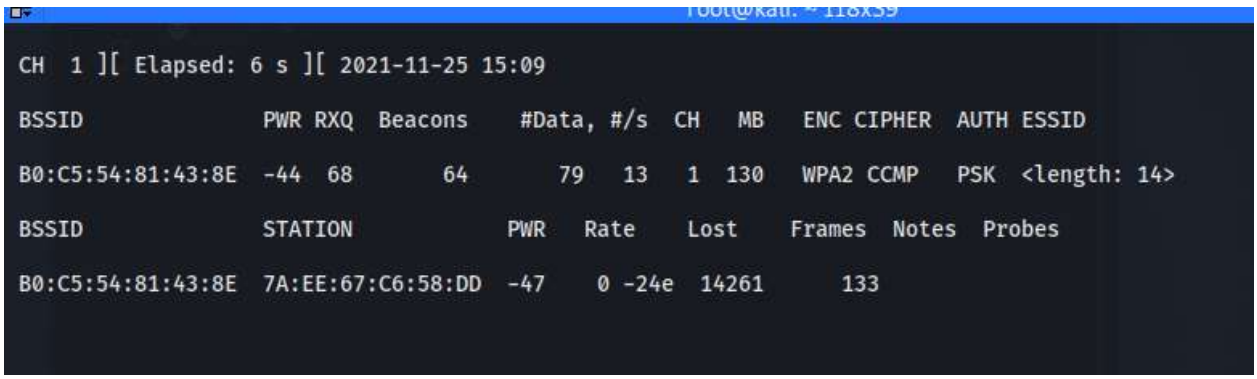


Figura 148: Captura de los datos de la red objetivo. Fuente: Elaboración Propia.

g) Una vez que se haya ejecutado el comando para la captura del tráfico es necesario hacer una desasociación de un dispositivo o de un cliente para poder capturar el handshake o a su vez se deberá esperar que un nuevo cliente realice una conexión al Access point que se está auditando.

En este caso se realizada la desasociación del dispositivo que se encuentra conectado para ello utilizaremos este comando: **aireplay-ng -0(número para realizar el deauth) 2(número de veces que se va a realizar el deauth) -a B0:C5:54:81:43:8E (MAC del Access Point) -c 7A:EE:67:C6:58:DD (MAC del Cliente) wlan0 (tarjeta de red).**

- Como se puede ver en la siguiente imagen al ejecutar por primera vez el comando que permite la desasociación del dispositivo no se obtiene el handshake, en este caso se tuvo que volver a ejecutar el mismo comando para lograr obtener el handshake tal como se muestra en la próxima imagen.

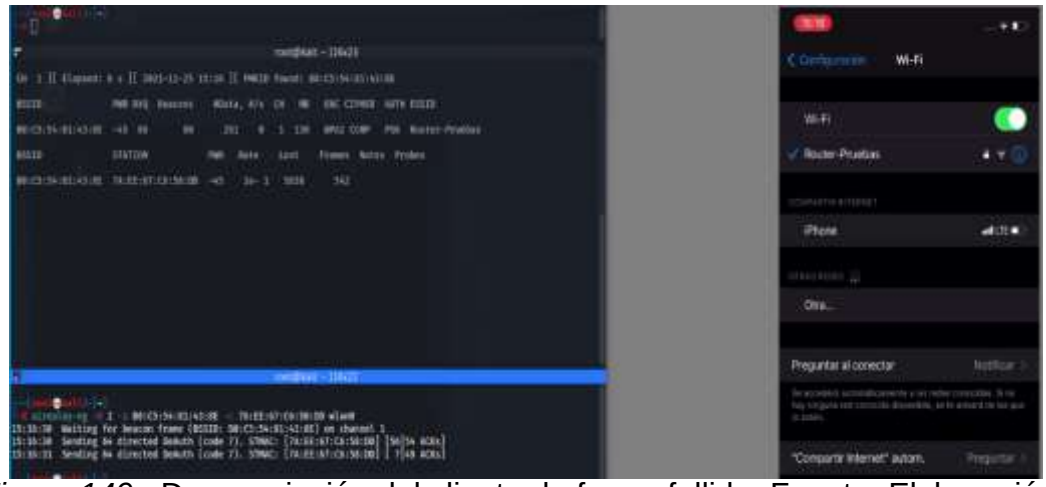


Figura 149: Desasociación del cliente de forma fallida. Fuente: Elaboración Propia.

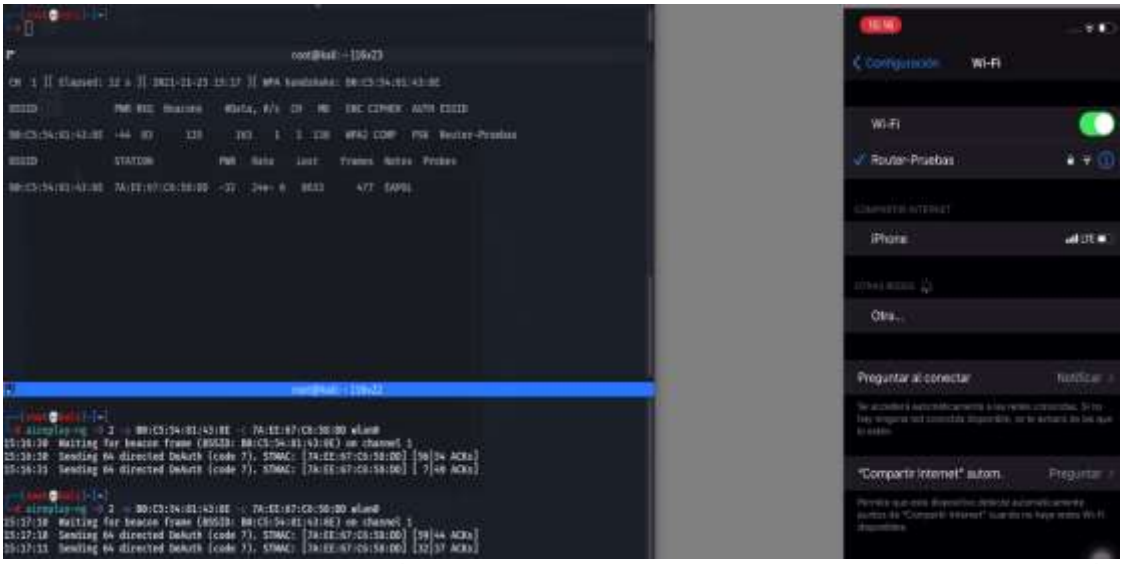


Figura 150: Desasociación del cliente de forma exitosa. Fuente: Elaboración Propia.

h) Una vez que se haya obtenido el handshake es importante contar con el diccionario que ayudara a buscar y a descifrar la contraseña del equipo auditado. En este caso se verificará si la contraseña configurada en el router se encuentra en el diccionario que ya se tiene para ello se utiliza el comando que se muestra en la siguiente imagen.

   - Es importante mencionar que para este caso la contraseña del router si se encuentra en el diccionario, pero habrá casos en los que no exista la contraseña del equipo dentro del diccionario.

```
┌──(root💀kali)-[~]
└─# cat /usr/share/wordlists/pruebadiccionario.txt |grep Prueb@-Oculto
Prueb@-Oculto
```

Figura 151: Prueba de diccionario mediante comandos en kali Linux. Fuente: Elaboración Propia.

i) Para conocer la contraseña del equipo al que se está atacando es importante usar el comando que se muestra en la siguiente imagen, dentro de este comando se coloca la ruta en donde se encuentra el diccionario con las posibles contraseñas, también se coloca el nombre del archivo donde se guardó el tráfico capturado, debido a que con estos dos archivos importantes se podrá conocer la contraseña que el atacante desea.

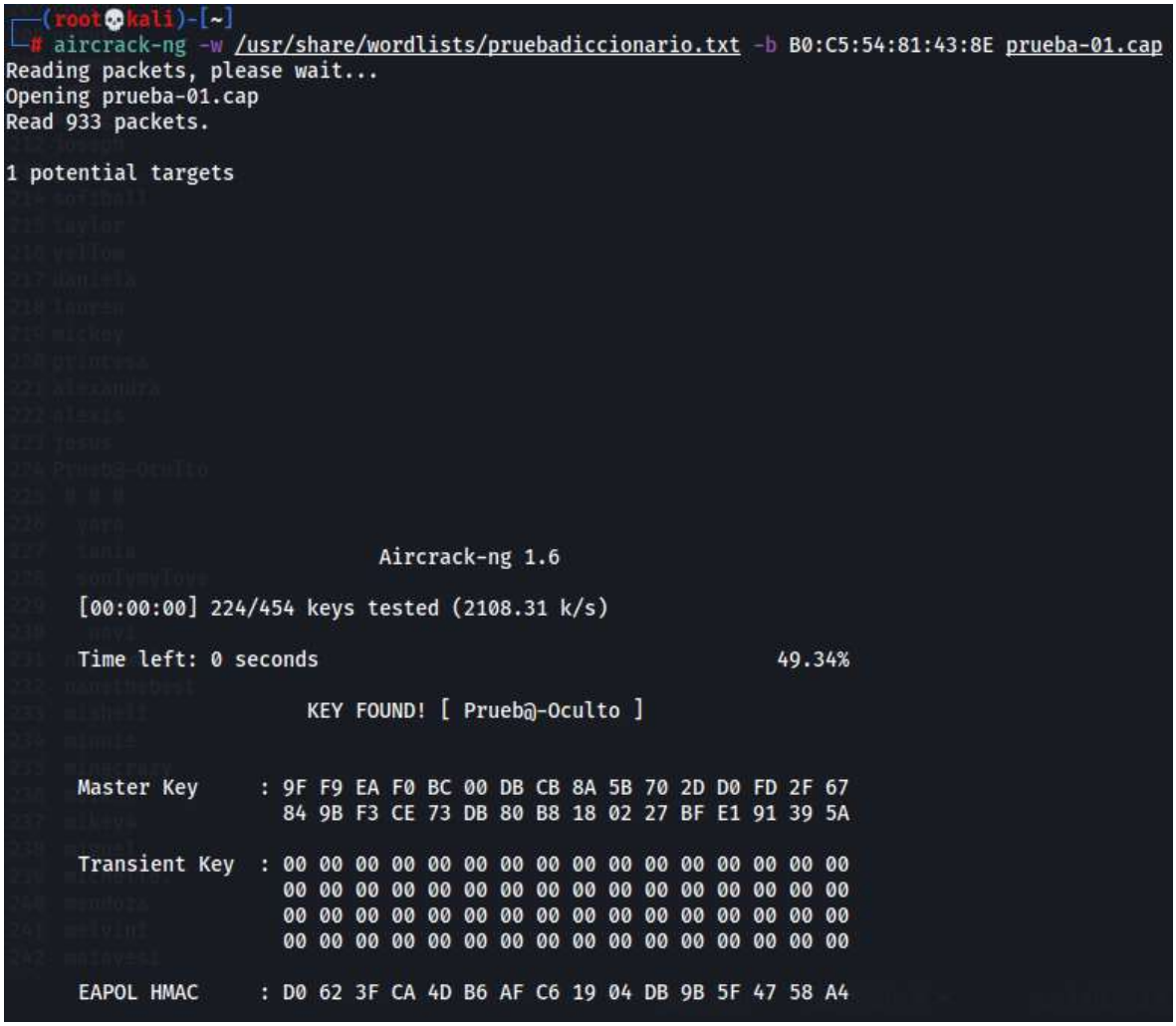


Figura 152: Clave encontrada con la búsqueda de la contraseña con el diccionario y el archivo de tráfico de datos. Fuente: Elaboración Propia.

Ataque de diccionario a un ssid oculto con protocolo WPA

Para este ataque es importante realizar una previa configuración al Access point en el cual se haga un cambio de protocolo, finalmente se deberá seguir los mismos pasos que se indicaron anteriormente.

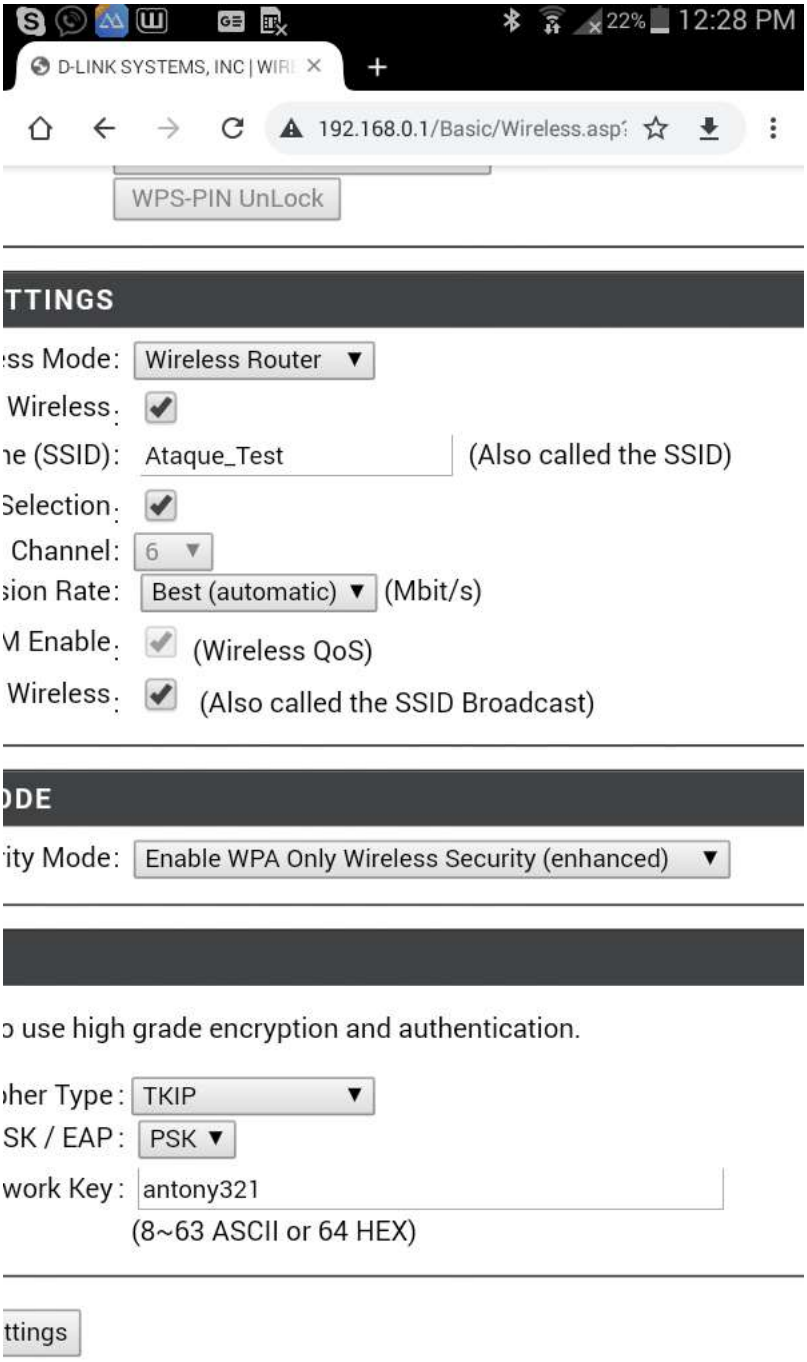


Figura 153: Configuración del router para ataque de diccionario con bssd oculto. Fuente: Elaboración Propia.

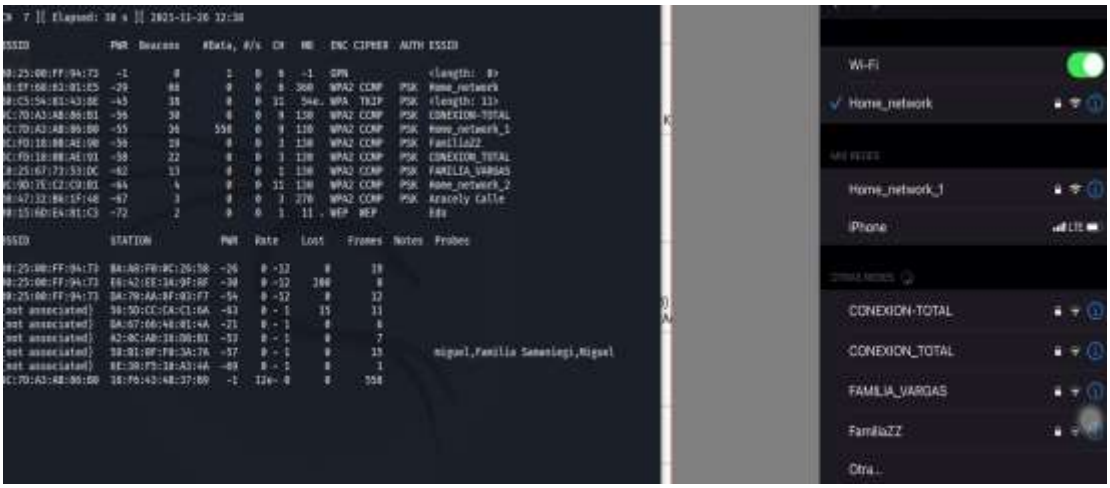


Figura 154: Desasociación del cliente de forma fallida oculto. Fuente: Elaboración Propia.

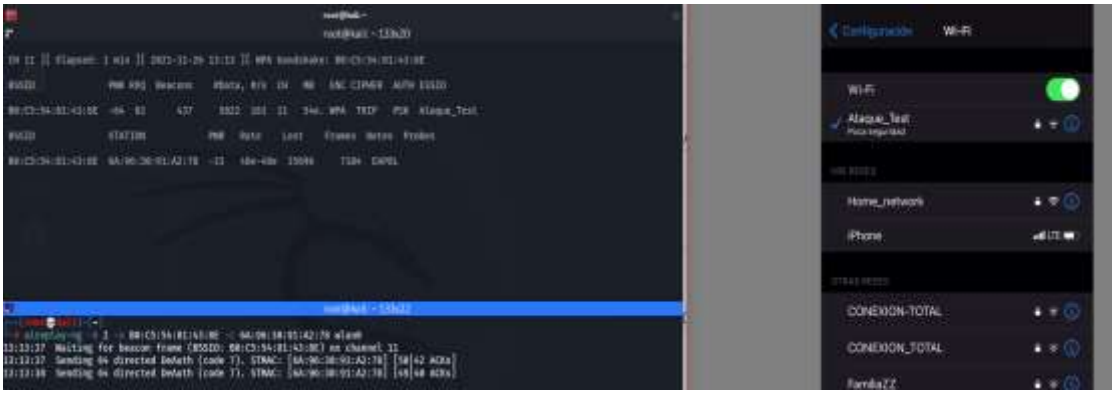


Figura 155: Desasociación del cliente de forma exitosa. Fuente: Elaboración Propia.

Figura 156: Prueba de diccionario mediante comandos en kali Linux. Fuente: Elaboración Propia.

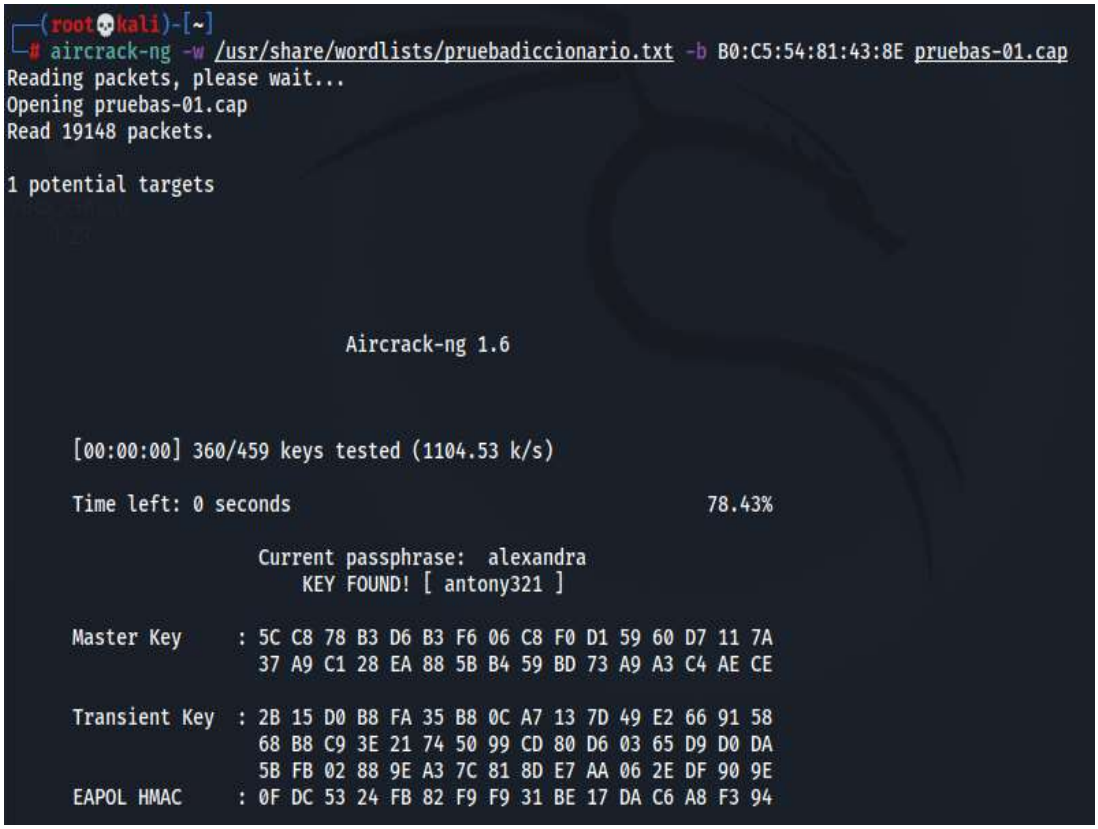


Figura 157: Clave encontrada con la búsqueda de la contraseña con el diccionario y el archivo de tráfico de datos. Fuente: Elaboración Propia.

Ataque de diccionario a un ssid oculto con protocolo WPA3

Para este ataque es importante realizar una previa configuración al Access point en el cual se haga un cambio de protocolo, finalmente se deberá seguir los mismos pasos que se indicaron anteriormente.

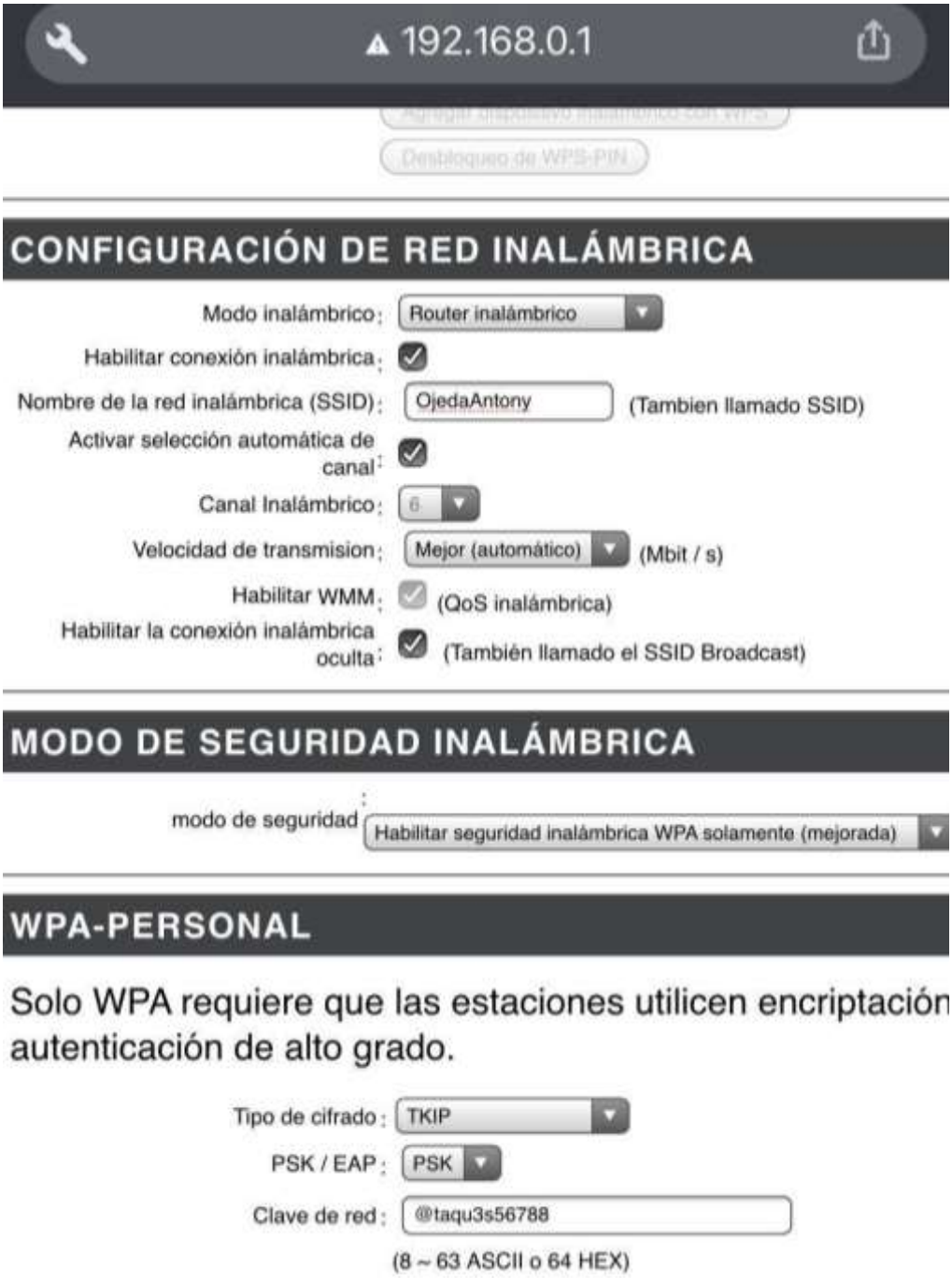


Figura 158: Configuración del router para ataque de diccionario con bssd oculto. Fuente: Elaboración Propia.

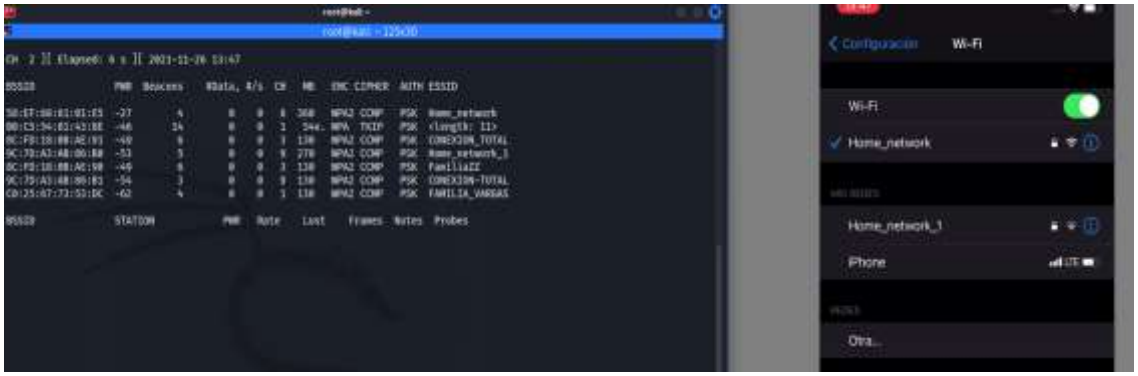


Figura 159: Desasociación del cliente de forma fallida. Fuente: Elaboración Propia.

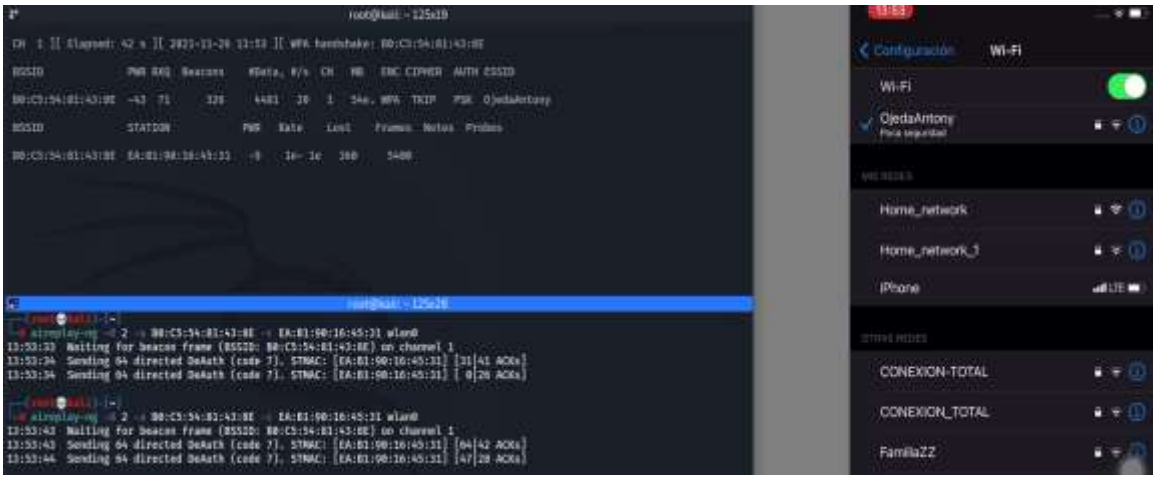


Figura 160: Desasociación del cliente de forma exitosa. Fuente: Elaboración Propia.

Figura 161: Prueba de diccionario mediante comandos en kali Linux. Fuente: Elaboración Propia.

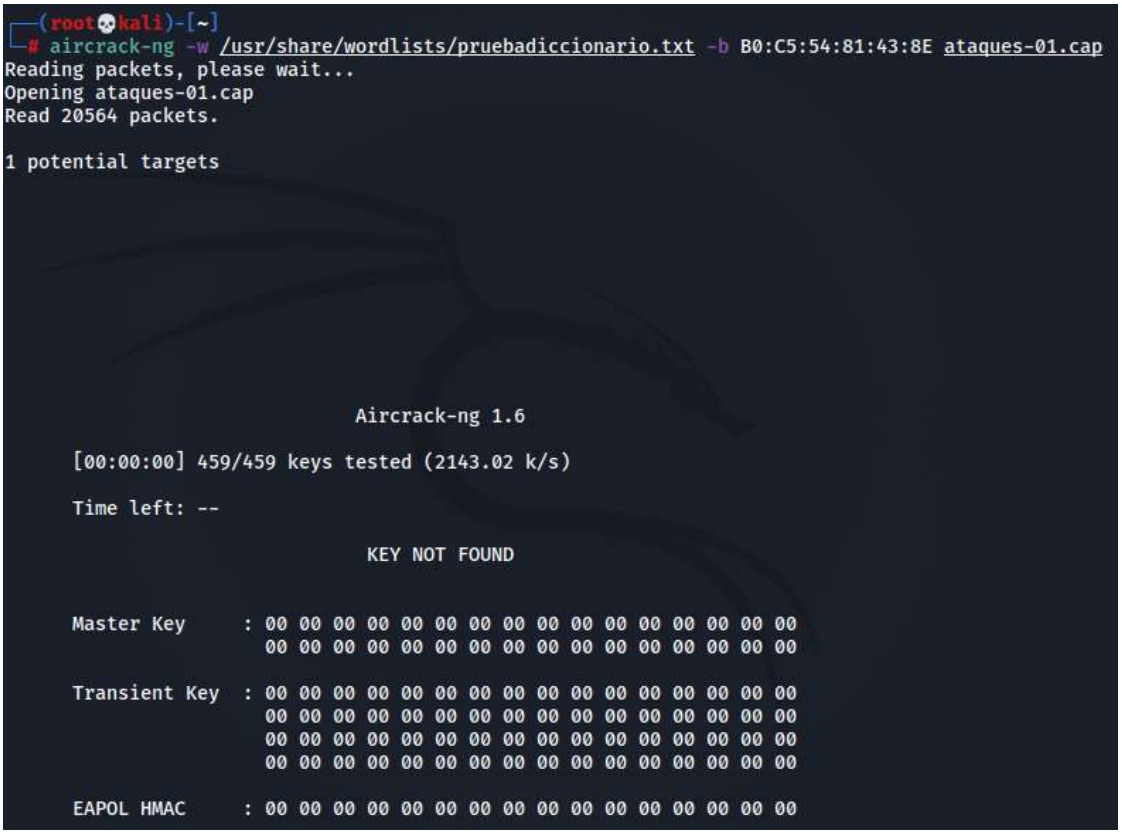


Figura 162: Clave encontrada con la búsqueda de la contraseña con el diccionario y el archivo de tráfico de datos. Fuente: Elaboración Propia.

Descripción del Ataque de diccionario a un bssid oculto en WPA, WPA2 y WPA3

El ataque de diccionario con un ssid oculto en el protocolo WPA2, WPA3 y en el WPA tiene éxito siempre y cuando la contraseña del equipo que se está atacando se encuentre dentro del diccionario caso contrario no será exitoso puesto que no lograra identificar la palabra clave del equipo. También es importante esperar que un cliente se conecte al ssid oculto que se desea atacar para conocer cuál es la Mac y el canal en el que se encuentra trabajando, caso contrario únicamente se visualizara el tráfico de redes que no son oculta, por lo general el tiempo que tarda en encontrar la contraseña dependerá del tamaño del diccionario ya que si se tiene 5000 palabras y la última es la que coincide con la del equipo significa que tuvo que analizar 4999 palabras antes de encontrar la correcta.

Para comprobar que este ataque es efectivo en el protocolo WPA, WPA2 y WPA3 (el tiempo de éxito va en forma ascendente) si la palabra clave del equipo se encuentra en el diccionario se ha optado por hacer múltiples pruebas con claves que no serán incluidas en el diccionario.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

- El uso de las redes inalámbricas de área local se ha visto incrementado debido a su bajo costo y su relativamente fácil instalación, y también debido en gran parte a la comodidad que para el usuario doméstico y corporativo representa mantener la comunicación sin cables.

- Muchas veces, las redes inalámbricas son instaladas por personal no especializado en tema de seguridad, por lo que dichas redes instaladas son abiertas, lo que causa exposición de toda la información que se transmite o convirtiéndolas vulnerables y expuestas a ataques informáticos.

- El protocolo WEP a estas alturas resulta más que inapropiado, obsoleto y peligroso en un escenario donde se necesite una seguridad en cualquier nivel, debido a que se desempeña los niveles más bajos de su funcionamiento y lógica de encriptación, por ejemplo, en la colisión de valores del IV.

- A pesar de que recientemente se están descubriendo algunas vulnerabilidades y algunos equipos no sean compatibles, WPA3 resulta ser la solución más segura para proteger las redes inalámbricas de área local.

- Tanto WPA como WPA2 pueden ser considerados como herramientas de desempeño de seguridad aceptables para todos los dispositivos que no soporten WPA3, pero no hay duda que WPA3 será en pocos años el estándar que brinde mayor seguridad inalámbrica debido a que corrige las debilidades de sus protocolos predecesores.

4.2. Recomendaciones.

- No solo se debe considerar como única opción el uso del Protocolo WPA3 como único mecanismo seguro, sino que además se deben tener en cuenta mecanismos de forma complementarias como el uso de firewalls, VLANs, sistema de detección de intrusos, soluciones de alto nivel como Redes Privadas Virtuales (VPN) y servidores RADIUS para poder excluir, filtrar y monitorear cualquier cambio inadecuado en la WLAN para hacer las correcciones inmediatas.

- El equipo que se utiliza para las redes inalámbricas de área local generalmente ha sido diseñado para cubrir una determinada área al aire libre, por lo que se debe tomar en cuenta que su uso en espacios que sean cerrados o sean afectados por contacto en línea recta sin interferencia entre dos equipos inalámbricos, tendrá como consecuencia una cobertura menor. También es importante a tomarse en cuenta que se debe abarca el área deseada, pues al extender la señal hasta lugares donde no se requiere puede provocar que extraños escuchen, rastreen y posiblemente ataquen la red.

- Los puntos de acceso, pueden tener capacidad de aceptar muchos clientes conectados a la red, pero se debe tomar en cuenta que mientras más clientes estén conectados en dicha red, menor será el rendimiento. El número de clientes que se recomienda para un Access Point o Router inalámbrico fluctúa entre 20 a 25 hosts.

REFERENCIAS.

Abo-Soliman, M., & Azer, M. (2018). Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments. *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, (págs. 268-273). Prague.

ASUS. (06 de Jun de 2021). *https://www.asus.com/support/FAQ/1042478/*. Obtenido de [Wireless] What is WPA3? What are the advantages of using WPA3?: https://www.asus.com/latin/support/FAQ/1042478/

Avenía Delgado, C. (2017). *Fundamentos de seguridad Informatica.* Bogota: Fondo editorial Areandino.

Azad, U. (8 de Diciembre de 2020). *Aireplay-ng*. Obtenido de Aireplay-ng: https://linuxhint.com/aireplay_ng/

Brihuega, D. A. (2014). BackTrack 5 Hacking de redes inalámbricas. En D. A. Brihuega, *BackTrack 5 Hacking de redes inalámbricas* (págs. 100-101). Paracuellos de Jarama, Madrid: RA-MA Editorial.

Care Provider Alliance. (Diciembre de 2017). *An introduction to Cyber Security.* Obtenido de An introduction to Cyber Security: https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/An-Introduction-to-Cyber-Security.pdf

Castillo-Velazquez, J.-I., Alcalá, M., & Serrano, D. J. (2019). Hardening as a best practice for WLAN Security Meanwhile WPA3 is released. *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, (págs. 1-5).

Choi, J., Chang, S.-Y., Ko, D., & Hu, Y.-C. (2011). Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots. *2011 IEEE International Conference on Communications (ICC)*, (págs. 1-5). Kyoto.

CISCO. (2019). *Estándares mínimos de seguridad ¿Cuanta seguridad es suficiente?* San José: Cisco Press.

CISCO. (20 de Marzo de 2020). *What Is Wi-Fi Security?* Obtenido de What Is Wi-Fi Security?: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html

Eian, I., Lim, K., Yeap, M., Yeo, H., & Zahra, F.-t. (2020). Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges. *Preprints*, 1-2.

Ezeme, O. (2014). *Analysis of IEEE 802.11: Architecture, Protocols, QoS and Interference. .* Ontario.

Fehér, D., & Sandor, B. (2018). Effects of the WPA2 KRACK Attack in Real Environment. *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, (págs. 239-242).

Gast, M. (2005). *802.11 Wireless Networks The Definitive Guide.* O'Reilly.

Geeksforgeeks. (5 de Julio de 2021). *Introducción a Kali Linux*. Obtenido de Introducción a Kali Linux: https://www.geeksforgeeks.org/introduction-to-kali-linux/

Gestion.pe. (11 de Diciembre de 2020). *Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia?* Obtenido de https://gestion.pe/publirreportaje/ciberseguridad-en-el-peru-que-tan-preparados-estamos-para-enfrentar-la-ciberdelincuencia-noticia/?ref=gesr&foto=2

Guo, J., Wang, M., Zhang, H., & Zhang, Y. (2020). A Secure Session Key Negotiation Scheme in WPA2-PSK Networks. *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, (págs. 1-6). Seoul.

Gutierrez, O. E. (2020). Comunicaciones móviles y redes inalámbricas. En O. E. Gutierrez, *Comunicaciones móviles y redes inalámbricas* (págs. 110-113-114). Cordoba: JOrge Sarmiento Editor-Universitas.

IPcisco.com. (2020). *Wireless Security Protocols*. Obtenido de https://ipcisco.com/lesson/wireless-security-protocols/

Jeong, C. Y., Chang, B. H., & Na, J. C. (2008). A Survey on Visualization for Wireless Security . *Fourth International Conference on Networked Computing and Advanced Information Management.*, (págs. 129-132). Corea.

Jimenez, H., Rodriguez, R., & Tiparra, J. (1978). *Diagnóstico de TEA.* Madrid: Latinoamérica SA.

KALITOOLS. (28 de Agosto de 2016). *Airmon-ng*. Obtenido de Airmon-ng: https://en.kali.tools/?p=167

Kaspersky. (20 de Noviembre de 2014). *Aumenta la seguridad de la red inalámbrica con estos sencillos consejos*. Obtenido de

https://www.kaspersky.es/resource-center/preemptive-safety/wireless-network-security-simple-tips

Kaspersky. (08 de Noviembre de 2021). *WEP, WPA, WPA2 y WPA3: diferencias y explicación*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/wep-vs-wpa

Kaur, J. (2017). Wireless Security Issues and their Emerging Trends. *International Journal of Control Theory and Applications* , 85-90.

Khasawneh, M., Kajman, I., Alkhudaidy, R., & Althubyani, A. (Marzo de 2014). *A Survey on Wi-Fi Protocols:WPA and WPA2.* Obtenido de https://www.researchgate.net/publication/290743584_A_Survey_on_Wi-Fi_Protocols_WPA_and_WPA2

Kumar, V., Chakraborty, S., Barbhuiya, F., & Nandi, S. (2016). Detection of stealth Man-in-the-Middle attack in wireless LAN. *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, (págs. 290-295). Solan.

Kwon, S., & Choi, H.-K. (2020). Evolution of Wi-Fi Protected Access: Security Challenges. *IEEE Consumer Electronics Magazin*, 1-3.

Lamers, E., Dijksman, R., van der Vegt, A., Sarode, M., & de Laat, C. (2021). Securing Home Wi-Fi with WPA3 Personal. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, (págs. 1-8).

Lashkari, A., Seyed Danesh, M., & Samadi, B. (2009). A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i). *2009 2nd IEEE International Conference on Computer Science and Information Technology.*, (págs. 1-3). Cyberjaya Malaysia.

Lehembre, G. (2006). Hacking: Seguridad Wi-Fi – WEP, WPA. *hakin9*, 3-4.

Liu, Y. (2015). Defense of WPA/WPA2-PSK Brute Forcer. *2015 2nd International Conference on Information Science and Control Engineering*, (págs. 185-188). Shanghai.

Liu, Y., Jin, Z., & Wang, Y. (2010). Survey on Security Scheme and Attacking Methods of WPA/WPA2. *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, (págs. 1-4). Chengdu.

MCCAULEY, B. (18 de Agosto de 2018). *Introduction to Wireless Security with Aircrack-ng*. Obtenido de Introduction to Wireless Security with Aircrack-ng: https://www.secureideas.com/blog/2018/09/introduction-to-wireless-security-with-aircrack-ng.html

Mendez, L. (29 de Mayo de 2018). *4 formas de proteger la red WiFi de tu empresa*. Obtenido de Blog Cisco Latinoamérica: https://gblogs.cisco.com/la/en-leobardo-4-formas-de-proteger-la-red-wifi-de-tu-empresa/

Moissinac, K., Ramos, D., Rendon, G., & Elleithy, A. (2021). Wireless Encryption and WPA2 Weaknesses. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference*, (págs. 1007-1015).

Noh, J., Kim, J., Kwon, G., & Cho, S. (2016). Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography. *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, (págs. 1-4). Seoul.

Onno, S., Gelloz, R., Heen, O., & Neumann, C. (2012). User-based authentication for wireless home networks. *2012 IEEE Second International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, (págs. 218-220). Berlin.

Openmaniak. (3 de Febrero de 2008). *Introducción a Ettercap*. Obtenido de Introducción a Ettercap: https://openmaniak.com/ettercap.php

Otreppe, T. (14 de Agosto de 2018). *packetforge-ng*. Obtenido de packetforge-ng: https://linuxcommandlibrary.com/man/packetforge-ng

Palma, J., & Marín, R. (2008). *Inteligencia Artificial.* Madrid: McGrawHill. doi:978-84-481-5618-3

Perez, S., & Facchini, H. (2017). *Dispositivos y Protocolos en Redes LAN Y WAN.*

Rackley, S. (2007). *Wireless Networking.* Oxford: Elsevier.

Raza, A. (2018). *Introducción al sistema operativo Wifislax*. Obtenido de Introducción al sistema operativo Wifislax: https://steemit.com/mgsc/@ali1357/introduction-to-wifislax-operating-system-212a3b2663ca3

Reddy, I., & Srikanth, V. (2019). *Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3).* Hyderabad.

Ribes, R. J. (2013). Redes Locales. En R. J. Ribes, *Redes Locales* (pág. 256). Madrid: Macmillan Iberia, S.A.

Rojas, K. (2018). Identificación de efectos negativos de la TEA en el aprendizaje. *IEEE conference Techology children especial*, 200-215.

Salazar, J. (2016). Redes Inalámbricas. *České vysoké učení technické v Praze*, 6-7.

Seemma , P., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering*, 125-128.

Singh, R., & Sharma, T. (2019). An Overview Of WLAN Security. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 11, NOVEMBER 2019* , (págs. 1-5).

Street, J., Nabors, K., Baskin, B., & Carey, M. (2010). *Dissecting the hack.* Syngress.

SZNAJDLEDER, P. (2012). *Java a fondo - estudio del lenguaje y desarrollo de aplicaciones - 2a ed.* México: Alfaomega.

Tafur, C., & Chavez, J. (2018). *ANÁLISIS DE PROTOCOLOS DE PROTECCIÓN DE REDES INALÁMBRICAS WI-FI PARA LA DETECCIÓN DE VULNERABILIDADES FRENTE A POSIBLES ATAQUES QUE ATENTEN CONTRA LA SEGURIDAD DE LA INFORMACIÓN.*

Taha, S., & Shen, X. (2012). A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET. *2012 IEEE Global Communications Conference (GLOBECOM)*, (págs. 1004-1009). Anaheim.

Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (págs. 1313–1328). New York, NY, United States: SIGSAC: ACM Special Interest Group on Security, Audit, and Control.

Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *2020 IEEE Symposium on Security and Privacy (SP)*, (págs. 517-533). San Francisco, CA, USA.

Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *2020 IEEE Symposium on Security and Privacy (SP)*, (págs. 517-533).

WebTitan. (19 de Junio de 2021). *Most Common Wireless Network Attacks*. Obtenido de Most Common Wireless Network Attacks: https://www.webtitan.com/blog/most-common-wireless-network-attacks/

Wi-Fi Alliance®. (10 de Abril de 2019). *Wi-Fi Alliance® security update*. Obtenido de https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update-april-2019

ANEXOS.

Anexo 1. Resolución de aprobación de cambio del título del proyecto de investigación.

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0575-2022/FIAU-USS

Pimentel, 19 de septiembre de 2022

VISTO:
El Acta de reunión N°0509-2022 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante Oficio 0195-2022/FIAU-IS-USS de fecha 5 de septiembre de 2022, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó aprobar el cambio de jurado evaluador de tesis que se detallan en el Acta de reunión N° 0509 - 2022, de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y AMBIENTE, a a cargo de los estudiantes y /o egresados del Programa de estudios INGENIERÍA DE SISTEMAS, hasta la fecha que indica la presente resolución.

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0575-2022/FIAU-USS

Pimentel, 19 de septiembre de 2022

APELLIDOS	TEMA DE TESIS	JURADO ANTERIOR	JURADO NUEVO
ALARCON GUEVARA IVON VANESSA / RAMOS MENDOZA NADALI GLORIA	EVALUACIÓN DE LA CALIDAD EN USO DE PLATAFORMAS DE COMERCIO ELECTRÓNICO BASADAS EN SOFTWARE LIBRE CON MAYOR USO POR EMPRESAS PERUANAS, UTILIZANDO EL ESTANDAR ISO/IEC 25000	**PRESIDENTE:** DR. VASQUEZ LEYVA OLIVER **SECRETARIO:** ING. OCAMPO MORENO ROSA LILIANA **VOCAL:** DR. TUESTA MONTEZA VICTOR LEXCI	**PRESIDENTE:** DR. VASQUEZ LEYVA OLIVER **SECRETARIO:** MG. BRAVO RUIZ JAIME ARTURO **VOCAL:** DR. TUESTA MONTEZA VICTOR LEXCI
CALDERÓN YNOÑAN PAMELA DEL CARMEN / PRIETO NEIRA FRANCK ALBERSON	INTEGRACIÓN DE UN ENFOQUE ÁGIL CON TÉCNICAS DE DISEÑO CENTRADO EN USUARIO (DCU) PARA LA MEJORA DE EXPERIENCIA DE USUARIO (UX)	**PRESIDENTE:** DR. RAMOS MOSCOL MARIO FERNANDO **SECRETARIO:** MG. SIALER RIVERA MARIA NOELIA **VOCAL:** MG. CELIS BRAVO PERCY JAVIER	**PRESIDENTE:** MG. BANCES SAAVEDRA DAVID ENRIQUE **SECRETARIO:** MG. ATALAYA URRUTIA CARLOS WILLIAM **VOCAL:** MG. MINGUILLO RUBIO CESAR AUGUSTO
CHANCAFE CASTRO JULIO JOEL	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE PARA UNA MUNICIPALIDAD BASADO EN ISO/IEC 29110.	**PRESIDENTE:** MG..AGUINAGA TELLO JUAN ADOLFO **SECRETARIO:** MG. CACHAY MACO JUNIOR EUGENIO **VOCAL:** DR. CHIRINOS MUNDACA CARLOS ALBERTO	**PRESIDENTE:** MG..AGUINAGA TELLO JUAN ADOLFO **SECRETARIO:** MG. CACHAY MACO JUNIOR EUGENIO **VOCAL:** MG. ARCILA DIAZ JUAN CARLOS
CHUCO AGUILAR GERSON RAUL	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27001 PARA MEJORAR EL NIVEL DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN UNA EMPRESA CONSTRUCTORA DE OBRAS CIVILES	**PRESIDENTE:** DR. CALDAS NUÑEZ JESUS MANUEL **SECRETARIO:** MG. CACHAY MACO JUNIOR EUGENIO **VOCAL:** MG. BANCES SAAVEDRA DAVID ENRIQUE	**PRESIDENTE:** MG. MEJIA CABRERA HEBER IVAN **SECRETARIO:** MG. CACHAY MACO JUNIOR EUGENIO **VOCAL:** MG. BANCES SAAVEDRA DAVID ENRIQUE
CIEZA CELIS JESÚS ABELARDO / OJEDA ROMERO ANTHONNY JHONATAN	EVALUACIÓN DEL DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD PARA COMBATIR ATAQUES EN REDES INALÁMBRICAS WI-FI	**PRESIDENTE:** DR. RAMOS MOSCOL MARIO FERNANDO **SECRETARIO:** DR. CALDAS NUÑEZ JESUS MANUEL **VOCAL:** MG. ATALAYA URRUTIA CARLOS WILLIAM	**PRESIDENTE:** MG. SAMILLAN AYALA ALBERTO ENRIQUE **SECRETARIO:** MG. MINGUILLO RUBIO CESAR AUGUSTO **VOCAL:** MG. ATALAYA URRUTIA CARLOS WILLIAM
CIEZA RIOS ELMER / TANTAJULCA ROJAS NERLITA MARDELI	DESARROLLO DE UN PROCESO DE PRUEBAS BASADA EN ESTÁNDARES PARA MEJORAR LA EFICIENCIA DE LA VERIFICACIÓN Y VALIDACIÓN DEL PRODUCTO EN MICRO EMPRESAS PERUANAS QUE DESARROLLAN SOFTWARE	**PRESIDENTE:** DR. RAMOS MOSCOL MARIO FERNANDO **SECRETARIO:** DR. VASQUEZ LEYVA OLIVER **VOCAL:** MG. BRAVO RUIZ JAIME ARTURO	**PRESIDENTE:** DR. TUESTA MONTEZA VICTOR ALEXCI **SECRETARIO:** DR. VASQUEZ LEYVA OLIVER **VOCAL:** MG. BRVO RUIZ JAIME ARTURO

Anexo 2. Escala Valorativa de cuantificación de indicadores: Variable Independiente.

CARACTERISTICA	CALIFICACIÓN
Muy Malo	0
Malo	1
Regular	2
Muy bueno	3
Excelente	4

Anexo 3. Subtotales del Análisis de la Variable Independiente.

Dimensiones	**Indicadores**	**WPA**	**WPA2**	**WPA3**
Método de Cifrado	Algoritmo de cifrado			
	Tamaño del IV			
Mecanismos de Entrega de Datos	Mecanismos de integridad de la cabecera			
Autorización	Distribución de clave forma manual			
	Autenticación de máquina			
RESULTADOS TOTALES				

Anexo 4. Sumatoria de Análisis de la Variable Independiente.

DIMENSIONES	**WPA**	**WPA2**	**WPA3**
Método de Cifrado			
Mecanismos de Entrega de Datos			
Autorización			
RESULTADOS TOTALES			

Anexo 5. Porcentaje Total de Cada Protocolo Analizado – Variable independiente.

INDICES	WPA	WPA2	WPA3
PT_PW			
PT			
PORCENTAJE POR PROTOCOLO			

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador)

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW) = (PT_PW / PT) *100%

Anexo 6. Porcentaje por Protocolo de Variable Independiente.

WPA	WPA2	WPA3

Anexo 7. Subtotales del Análisis de la Variable Dependiente.

Dimensiones	Indicadores	WPA	WPA2	WPA3
Confidencialidad	Promedio de tiempo de éxito de ataque **Phishing**			
	Promedio de tiempo de éxito de ataque **Man in the Middle**			
	Promedio de tiempo de éxito de ataque **ARP Spoofing + DNS Spoofing**			
Integridad	Promedio de tiempo de éxito de ataque de DoS			

Autenticación	Promedio de tiempo de éxito de ataque **de fuerza bruta**	
	Promedio de tiempo de éxito de Ataque de diccionario **a un ssid oculto**	
RESULTADOS TOTALES		

Anexo 8. Sumatoria de Análisis de la Variable dependiente.

DIMENSIONES	**WPA**	**WPA2**	**WPA3**
Confidencialidad			
Integridad			
Autentificación			
RESULTADOS TOTALES			

Anexo 9. Porcentaje Total de Cada Protocolo Analizado – Variable dependiente.

INDICES	**WPA**	**WPA2**	**WPA3**
PT_PW			
PT			
PORCENTAJE POR PROTOCOLO			

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador)

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW) = (PT_PW / PT) *100%

Anexo 10. Porcentaje por Protocolo de Variable dependiente.

WPA	**WPA2**	**WPA3**