UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Trabajo Final previo a la obtención del título de Magíster
en Ciberseguridad

AUTORES: Ing. Alfredo Francisco Salazar Herrera

Ing. David Andrés Barahona Cuji

Ing. Jhon Vinicio Delgado Delgado

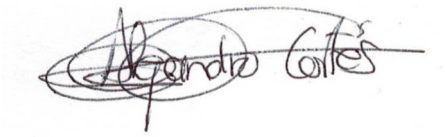
Ing. Juan Carlos Suárez León

TUTOR: Ing. Alejandro Cortés

Seguridad en Redes WIFI

APROBACIÓN DEL TUTOR

Yo, Alejandro Cortés certifico que conozco al autores/as del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido



Alejandro Cortés López

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

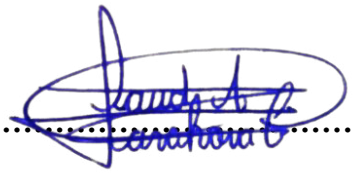
Nosotros, ALFREDO FRANCISCO SALAZAR HERRERA, DAVID ANDRÉS BARAHONA CUJI, JHON VINICIO DELGADO DELGADO y JUAN CARLOS SUAREZ LEON declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

…….

Alfredo Francisco Salazar Herrera

C.I.: 0603530783



…….

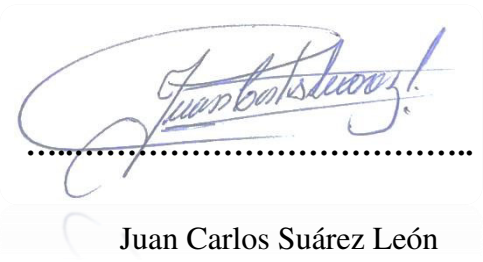
David Andrés Barahona Cují

C.I: 1722365861

……..

Jhon Vinicio Delgado Delgado

C.I.: 0301806048



……..

Juan Carlos Suárez León

C.I: 1715683411

DEDICATORIA

Queremos dedicar este logro a todas las personas que nos han acompañado en nuestro camino hacia la culminación de nuestra maestría.

En primer lugar, agradecemos a nuestros profesores y asesores académicos, quienes nos guiaron y brindaron su apoyo a lo largo de todo el proceso de investigación. Su conocimiento, experiencia y orientación fueron fundamentales para el desarrollo de nuestro trabajo de investigación. Estamos profundamente agradecidos por su dedicación y por compartir con nosotros su pasión por el conocimiento.

También queremos expresar nuestro agradecimiento a nuestros compañeros de clase, quienes fueron una fuente constante de inspiración, colaboración y apoyo. Juntos, enfrentamos desafíos, compartimos ideas y aprendimos unos de otros. Su amistad y compañerismo hicieron de este viaje académico una experiencia enriquecedora.

A nuestras familias y seres queridos, les agradecemos por su amor incondicional, paciencia y apoyo constante. Su aliento y comprensión nos impulsaron a seguir adelante incluso en los momentos más difíciles. Este logro es también suyo, ya que nunca dejaron de creer en nosotros.

La culminación de este trabajo de investigación y de maestría es el resultado del esfuerzo colectivo y del apoyo recibido de tantas personas maravillosas. Este logro no hubiera sido posible sin ustedes. Les dedicamos este trabajo con profundo agradecimiento y gratitud, sabiendo que su influencia ha dejado una huella imborrable en nuestras vidas.

AGRADECIMIENTO

Queremos expresar nuestro más sincero agradecimiento a todas las personas que nos brindaron su apoyo incondicional y contribuyeron de manera significativa en la realización de nuestro trabajo de investigación de fin de maestría.

En primer lugar, agradecemos a nuestros supervisores y asesores académicos, por su invaluable orientación, conocimientos y dedicación a lo largo de todo el proceso de investigación. Sus consejos, comentarios y retroalimentación constructiva fueron fundamentales para el desarrollo de nuestro trabajo. Estamos profundamente agradecidos por su apoyo constante y por ser una fuente de inspiración académica.

También queremos expresar nuestra gratitud al comité de revisión, por su tiempo, esfuerzo y evaluaciones exhaustivas. Sus sugerencias y aportes críticos nos ayudaron a mejorar la calidad y el rigor de nuestro trabajo de investigación.

Además, deseamos agradecer a nuestros compañeros de clase, quienes fueron una fuente constante de colaboración, intercambio de ideas y apoyo mutuo. Compartir experiencias y conocimientos con ellos enriqueció nuestro proceso de aprendizaje y contribuyó a nuestro crecimiento académico y personal.

No podemos olvidar mencionar a nuestros amigos y seres queridos, quienes nos brindaron su incondicional apoyo emocional y comprensión a lo largo de esta exigente etapa. Sus palabras de aliento, paciencia y amor fueron nuestro sostén en los momentos de desafío.

Por último, queremos agradecer a nuestras familias por su constante respaldo, sacrificio y amor incondicional. Su apoyo y comprensión fueron fundamentales para superar obstáculos y lograr este importante hito académico.

RESUMEN

La metodología OWISAM nace como una herramienta para solventar la necesidad existente de establecer controles de seguridad que se deben cumplir en las redes inalámbricas e identificar los riesgos que se deben minimizar ante ataques informáticos para así garantizar la protección de la infraestructura Wi-Fi, basada en el estándar 802.11.

La presente investigación, tiene como objetivo recrear dentro de ambientes controlados los principales riesgos de las redes Wi-Fi descritos en la metodología OWISAM y establecer una guía de acción para evitar ser víctimas de robo de información al caer en estas vulnerabilidades.

Con esta finalidad se han efectuado los ataques más comunes dentro de redes Wi-Fi y se han evaluado las vulnerabilidades aún existentes, se ha elaborado una guía de recomendaciones para cada uno de los diez principales riesgos de OWISAM y se ha verificado que, aplicando las recomendaciones establecidas en este documento, se puede tener una red Wi-Fi más segura y evitar el robo de información.

Palabras Clave: Vulnerabilidad, Wi-Fi, riesgo, encriptación, cifrado, autenticación.

ABSTRACT

The OWISAM methodology was born as a tool to solve the existing need to establish security controls that must be met in wireless networks and identify the risks that must be minimized in the face of computer attacks to provide/guarantee the protection of the Wi-Fi infrastructure, based on the 802.11 standard.

The purpose of this research is to recreate within controlled environments the main risks of Wi-Fi networks described in the OWISAM methodology and to establish an action guide to avoid being victims of information theft when falling into these vulnerabilities.

To this end, the most common attacks within Wi-Fi networks have been demonstrated and the vulnerabilities that still exist have been evaluated, a recommendation guide has been prepared for each of the ten main OWISAM risks and it has been verified that, applying the recommendations established in this document, you can have a more secure Wi-Fi network and avoid information theft.

Keywords: Vulnerability, Wi-Fi, risk, encryption, identified, authentication.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

CAPÍTULO 1

Introducción

Una red Wi-Fi es una red de telecomunicaciones que utiliza el estándar IEEE 802.11 para conectar los dispositivos dentro de ella, estos dispositivos hacen uso para comunicarse entre sí señales de radiofrecuencia, las que pueden estar en el rango de los 2.4 GHz o 5 GHz. También cumplen los protocolos definidos en el estándar IEEE 802.11 para que la comunicación entre todos los equipos dentro de la red sea posible.

La seguridad de redes Wi-Fi se refiere a todos los mecanismos utilizados para mantener a los datos compartidos dentro de la red protegidos y bajo los tres pilares de la seguridad de la información, que son: la confidencialidad, la integridad y la disponibilidad. Es importante tener en cuenta que dentro del modelo OSI las redes Wi-Fi utilizan en la capa física ondas de radiofrecuencia para el transporte de datos, a diferencia de los medios guiados, cuando se tiene un medio no guiado como lo son las ondas RF, cualquier agente que se encuentre dentro del espacio en el cual se irradian las señales puede escucharlas y si no se han implementado las seguridades adecuadas, podría incluso interpretarlas.

Es bastante común que en espacios donde se comparten redes Wi-Fi libres o gratuitas, se produzcan muchos incidentes de seguridad. Los atacantes aprovechan el desconocimiento de las víctimas y utilizan cualquier vulnerabilidad en la red, para hacerse de información privada y así obtener un beneficio propio a costa de la víctima. Para resolver este problema se han implementado una gran cantidad de parches y actualizaciones para volver a las redes Wi-Fi más seguras, por ejemplo, el estándar Wired Equivalent Privacy (WEP) que a la final no proveyó a los usuarios la

suficiente protección y tuvo que evolucionar al estándar Wi-Fi Protected Access (WPA), que al igual que WEP, hoy en día ya es un estándar obsoleto, pero es su época sirvieron para dar protección y confianza al usuario y cimentar las bases de estándares más complejos, con menos vulnerabilidades y más eficientes (Hadi, 2022).

Teniendo en cuenta la rápida evolución de la tecnología, incluyendo las comunicaciones inalámbricas y en particular las redes Wi-Fi, es muy común que un usuario promedio no esté al tanto de todo el desarrollo que existe, así como tampoco sea consciente de las vulnerabilidades y riesgos que tiene el acceder a esta tecnología. Las organizaciones que imponen la normativa se encuentran a la vanguardia de estos temas y trabajan día a día para mitigar este grave problema, pero de todas formas el nivel de seguridad dependerá de la conciencia que tienen el usuario ante los riesgos que hay a su alrededor. Es por esto por lo que se reúne en este documento las principales vulnerabilidades a las que se exponen los usuarios al conectarse en una red Wi-Fi y se las simula en ambientes controlados, a fin de generar una guía de apoyo, para que cualquier persona interesada pueda seguir y tenga la seguridad de que está preparado para hacer frente a todo tipo de ataque dentro de su red Wi-Fi.

Dentro de esta investigación se aborda toda la evolución de las redes Wi-Fi, y los mecanismos de seguridad que se han implementado según las necesidades fueron surgiendo. Se recrean los ataques más comunes en los distintos estándares y las soluciones para mitigarlos, también se trata la importancia de mantener nuestras redes Wi-Fi seguras y las consecuencias de descuidar la seguridad de estas. Asimismo, se estudia de forma técnica cada vulnerabilidad y se profundiza en explicar cómo se ha mitigado la misma y si no lo han hecho como evitar ser víctimas de su explotación.

La investigación se la realiza tanto de forma documental como experimental, apoyándose en casos reportados y documentados, así como en la documentación oficial de la IEEE sobre el desarrollo del estándar 802.11. Primero se realiza un breve resumen de esta tecnología y su evolución, luego se definen los estándares de seguridad que se han implementado y cuales están vigentes así como cuales han quedado obsoletos, a continuación se definen las principales vulnerabilidades presentes en las redes Wi-Fi y qué métodos se utilizaron y a día de hoy aún se utilizan para su explotación, continuando se recrean dentro de un laboratorio controlado estas vulnerabilidades, y finalmente se establecen mecanismos de seguridad implementados para evitar ser víctimas de ellas y recomendaciones al usuario para protegerse de cualquier ataque.

Debido al alto uso de dispositivos móviles (Laptops, Tablets, Smartphones) nace la necesidad de saber que tan segura es la conexión de estos dispositivos con/hacia el Internet (a través de Routers/bridges, etc), por lo consiguiente lo primero que viene al momento de pensar en Ciberseguridad es el tipo de cifrado/protocolo que se están usando para realizar dichas conexiones (handshake), por lo que es imperativo no solo entender las ventajas que pueden a llegar a tener un protocolo sobre otro, sino también se debe conocer las desventajas, limitaciones y vulnerabilidades que cada protocolo dentro del marco de seguridad, partiendo de esto y realizando las pruebas apropiadas se podría guiar, recomendar, entender, y evitar aquellos protocolos que son susceptibles a hackeo. (Wi-Fi Alliance, 2019)

Como sabemos al momento de la creación de las comunicaciones (Wifi) la seguridad no estaba en mente por lo que en un principio fue abierto/ o a la vez el cifrado fue muy débil como lo fue WEP (1990 -2004), el cual ofrecía cifrado básico (64-128 bit) lo que permitía ser vulnerado en un tiempo relativamente corto [Cisco, 2021].

Como intento de mejorar el cifrado Wifi, WPA (128-256 bit) fue creada en 2003 la misma que introdujo el uso del protocolo de cifrado TKIP/PSK, lo que sumado al mayor uso de bits supuso una mejoría en el tema de seguridad, pero no fue suficiente y con el pasar del tiempo y la mejora tanto de las técnicas como el poder de los CPU/GPU en computadoras personales permitió que WPA (el cifrado en sí) sea vulnerado.

A sabiendas de que las conexiones Wifi estaban siendo vulneradas WPA2 fue creada y con esta se mejoró muchas deficiencias de WPA al igual que se dejó de lado protocolos de cifrado débil como PSK y se usó AES (Curtis, 2017).

Recientemente con la inclusión de nuevas tecnologías como Wifi-6 se mejoró el cifrado mediante el uso de WPA3, el cual aumenta el largo de los bits (192/256/384 bits), con esto se pretende que el hash (incluso de una clave corta/débil) al momento de cifrarlo no sea posible los ataques de tipo de fuerza bruta offline, lo que ayuda a incluso con la obtención del hash a través del robo de handshake no se podría recuperar la clave (Cisco, 2021., Curtis, 2017).

- **OWISAM-TR-001: Red de comunicaciones Wi-Fi abierta.**

Considerada como la red inalámbrica más insegura, una red de comunicaciones Wi-Fi abierta es aquella que no le solicita al usuario una contraseña para permitirle el ingreso a la misma, es decir cualquier persona puede conectarse o desconectarse de esta, lo que vuelve bastante vulnerable cualquier tipo de dato que en ella se transfiera, si no está debidamente protegido. Dentro de este grupo también se puede considerar a las redes Wi-Fi cuta contraseña de acceso es de conocimiento público ya actúa igual que una red sin contraseña, es decir cualquier individuo puede conectarse y analizar el tráfico del resto de usuarios. Este tipo de redes es más común encontrarla

en sitios de alta afluencia, por ejemplo, en terminales de transporte, edificios públicos, hoteles, parques o incluso en algunos eventos.

- **OWISAM-TR-002: Presencia de cifrado WEP en redes de comunicaciones.**

Se enfoca en la presencia de cifrado WEP en redes de comunicaciones. WEP (Wired Equivalent Privacy) es un protocolo de seguridad utilizado en redes inalámbricas que fue diseñado para proporcionar una seguridad similar a la que se encuentra en las redes cableadas. Sin embargo, debido a sus numerosas vulnerabilidades, WEP se considera obsoleto y no se recomienda su uso en la actualidad.

Este informe técnico analiza la presencia de WEP en redes de comunicaciones y explica por qué su uso es inseguro. También se describen algunas de las debilidades de WEP y cómo los atacantes pueden aprovecharlas para comprometer la seguridad de la red. Además, se discuten las alternativas más seguras al cifrado WEP, como WPA (Wi-Fi Protected Access) y WPA2. En general, OWISAM-TR-002 es un recurso útil para cualquier persona interesada en la seguridad de las redes de comunicaciones inalámbricas y en cómo proteger sus datos y sistemas de posibles amenazas.

- **OWISAM-TR-003: Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS)**

Está destinado a evaluar la seguridad de las redes inalámbricas, particularmente la configuración de seguridad de Wi-Fi Protected Setup (WPS). La Wi-Fi Alliance lanzó la función Wi-Fi Protected Setup en 2007 con el objetivo de facilitar la configuración de redes inalámbricas

en hogares y pequeñas empresas. Esta función permite a los usuarios configurar dispositivos de manera rápida y sencilla sin tener un conocimiento profundo de la seguridad de las redes inalámbricas.

- **OWISAM-TR-004: Clave WEP/WPA/WPA2/WPA3 basada en diccionario.**

Uno de los métodos más comunes utilizados por los piratas informáticos para comprometer la seguridad de las redes inalámbricas Wi-Fi son los ataques basados en diccionarios. Estos ataques utilizan fallas en los protocolos de seguridad Wi-Fi para obtener contraseñas utilizando diccionarios, listas predefinidas de palabras y/o contraseñas comunes. Debido a las técnicas de cifrado y autenticaciones utilizadas, los protocolos WEP, WPA y WPA2 están particularmente susceptibles a los ataques de diccionario. WEP es menos seguro que WPA porque es más antiguo y susceptible a varios tipos de ataques, en los que se incluyen los ataques de diccionario.

- **OWISAM-TR-005: Mecanismos de autenticación inseguros (LEAP, PEAP-MD5)**

Lightweight Extensible Authetication Protocol LEAP, fue creado por Cisco que predominantemente se usaba en conjunto con un servidor RADIUS para autenticar usuarios, la forma que este protocolo actúa es en forma pseudo-mutual de autenticación tanto en clientes como el servidor mediante el uso de las funciones hash MS-CHAP y MS-CHAPv2.

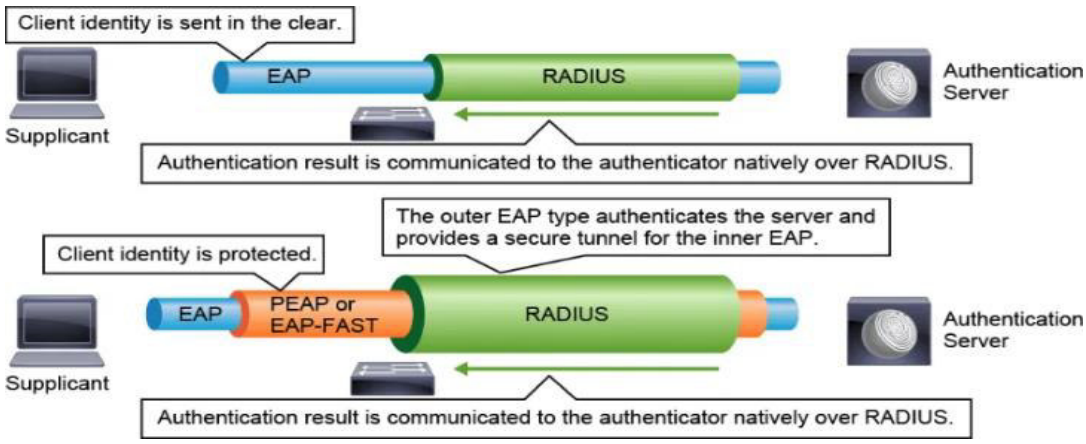
La gran desventaja/vulnerabilidad de LEAP es que al momento del cambio de información (cliente-servidor) es que la clave dentro del handshake está en texto plano (no cifrada) por lo que,

si un atacante pudiese interceptar el handshake, solo debería descifrar los valores de la clave, o realizar un ataque de ingeniería social para obtener la misma.

Otro inconveniente es que el algoritmo de hash MS-CHAPv2 es vulnerable a ataques de diccionario (offline), por lo que un atacante podría hacerse con el handshake/hash e intentar crackear la clave cifrada en otro lugar (con esto evita que la cuenta del usuario sea bloqueada en caso de repetidas claves incorrectas) usando un diccionario mediante el ataque de fuerza bruta.

Figura 1

Paquete EAP & PEAP



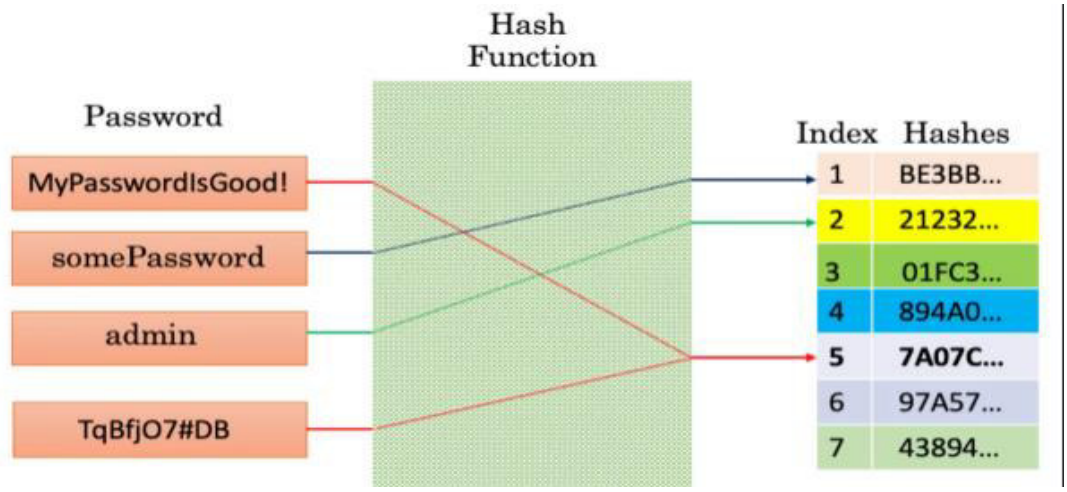
Nota. Imagen de paquete EAP/PEAP por (Garcarz, 2019)

Protected Extensible Authentication Protocol, fue creada por Cisco con el fin de corregir varias vulnerabilidades por lo que es una versión protegida de EAP en la cual el uso de TLS como túnel de cifrado ha sido implementado para cubrir las falencias anteriores y poder cifrar todos los componentes dentro de la encapsulación (incluido el nombre del usuario).

El problema resurge cuando se usa MD5 como el agente para el hash ya que como se ha podido demostrar MD5 es un protocolo vulnerable, esto debido a que no es resistente a la colisión con lo que se puede crear un hash idéntico (misma numeración) y hacer pasarlo como genuino, esto crea problemas ya que el usuario/dispositivo no puede discernir que hash es el auténtico.

Figura 2

Proceso de cifrado MD5 de palabra a hash.



Nota. Imagen de proceso de hash MD5por (Andrews, 2019)

- **OWISAM-TR-006: Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).**

WPS (Wi-Fi Protected Set up) es un protocolo que fue creado con un enfoque en la simplicidad y conectividad, muy similar al mecanismo usado por Bluetooth (en cuanto a los pasos a seguir para conectar dispositivos), con el afán de intentar que todos los usuarios tengan conectividad en sus dispositivos, WPS trabaja de tal manera que personas sin conocimientos técnicos de redes puedan por sí mismos conectar sus dispositivos a la red/router, ya que solo bastaría presionar un botón en el router o digitar un código aleatorio para poder tener conectividad,

esto en si es considerado una ventaja, pero las falencias en temas de seguridad y lo exposición a no poder controlar que dispositivos se conectan hace que WPS traiga más desventajas que beneficios. Y como ya se ha comprobado la activación de WPS se la puede hacer incluso son tener acceso físico al dispositivo/router por lo que este mecanismo es poco usado y en los routers viene desactivado de defecto. (Neagu C, 2022)

Figura 3

Router con botón WPS.

Nota. Imagen de Router con capacidad WPS por (Neagu C, 2022).

- **OWISAM-TR-007: Red Wi-Fi no autorizada por la organización**

Un ataque gemelo malvado tiene lugar cuando un atacante configura un punto de acceso Wi-Fi falso con la esperanza de que los usuarios se conecten a él en lugar de a uno legítimo. Toda la información que los usuarios intercambian con la red cuando se conectan a este punto de acceso pasa por un servidor que está bajo el control del atacante. Un atacante puede crear un gemelo malvado con un teléfono inteligente u otro dispositivo con capacidad para Internet y algún software

fácilmente disponible. Los ataques de gemelos malvados son más comunes en las redes Wi-Fi públicas que no son seguras y dejan sus datos personales vulnerables.

Así es como funciona un típico ataque Wi-Fi de gemelos malvados:

Paso 1: Buscando la ubicación correcta. Los piratas informáticos suelen buscar ubicaciones concurridas con Wi-Fi gratuito y popular. Esto incluye espacios como cafeterías, bibliotecas o aeropuertos, que suelen tener varios puntos de acceso con el mismo nombre. Esto facilita que la red falsa del hacker pase desapercibida.

Paso 2: Configuración de un punto de acceso Wi-Fi. Luego, el pirata informático toma nota del identificador de conjunto de servicios (SSID) de la red legítima y configura una nueva cuenta con el mismo SSID. Pueden usar casi cualquier dispositivo para hacer esto, incluidos teléfonos inteligentes, computadoras portátiles, tabletas o enrutadores portátiles. Pueden usar un dispositivo llamado Wi-Fi Pineapple para lograr un rango más amplio. Los dispositivos conectados no pueden distinguir entre conexiones genuinas y versiones falsas.

Paso 3: Animar a las víctimas a conectarse al Wi-Fi del gemelo malvado. El hacker puede acercarse a sus víctimas para crear una señal de conexión más fuerte que las versiones legítimas. Esto convence a las personas de seleccionar su red en lugar de las más débiles y obliga a algunos dispositivos a conectarse automáticamente.

Paso 4: Configuración de un portal cautivo falso. Antes de que pueda iniciar sesión en muchas cuentas Wi-Fi públicas, debe enviar datos en una página de inicio de sesión genérica. Los piratas informáticos gemelos malvados configuraron una copia de esta página, con la esperanza de engañar a las víctimas desprevenidas para que revelaran sus credenciales de inicio de sesión. Una vez que los piratas informáticos los tienen, pueden iniciar sesión en la red y controlarla.

Paso 5: Robar los datos de las víctimas. Cualquiera que inicie sesión se conecta a través del hacker. Este es un clásico ataque de hombre en el medio que le permite al atacante monitorear la actividad en línea de la víctima, ya sea desplazándose por las redes sociales o accediendo a sus cuentas bancarias. Supongamos que un usuario inicia sesión en cualquiera de sus cuentas. En ese caso, el pirata informático puede robar sus credenciales de inicio de sesión, lo que es especialmente peligroso si la víctima usa las mismas credenciales para varias cuentas.

- **OWISAM-TR-008: Portal hotspot inseguro.**

Un portal cautivo es un sistema utilizado en redes de computadoras para controlar el acceso a la red y redirigir a los usuarios a una página web específica antes de permitirles acceder a Internet. Por lo general, se utiliza en lugares públicos como aeropuertos, hoteles y cafeterías, donde los administradores de la red quieren asegurarse de que los usuarios acepten los términos de uso y proporcionar información importante antes de permitirles navegar por la web.

Los hotspots inseguros y los portales cautivos pueden presentar varios problemas de seguridad para los usuarios, ya que suelen utilizarse para conectarse a Internet en lugares públicos como cafeterías, aeropuertos, hoteles, entre otros. Algunos de los problemas que pueden surgir son:

Suplantación de identidad: los atacantes pueden crear hotspots falsos que parezcan legítimos, engañando a los usuarios para que se conecten a ellos y proporcionen información personal como contraseñas, nombres de usuario, entre otros.

1. Espionaje de tráfico: los atacantes pueden utilizar técnicas para interceptar el tráfico de red entre el usuario y el punto de acceso, permitiéndoles acceder a información sensible como mensajes, correos electrónicos, contraseñas, etc.

2. Malware: los atacantes pueden aprovechar los portales cautivos para distribuir malware a los usuarios que se conectan a ellos, utilizando técnicas como phishing o descarga automática de archivos.
3. Man-in-the-middle: los atacantes pueden realizar ataques de hombre en el medio para interceptar la comunicación entre el usuario y el servidor, **lo** que les permite modificar o falsificar la información que se está intercambiando.

Ataques de denegación de servicio: los atacantes pueden utilizar técnicas para saturar el ancho de banda disponible en el hotspot, impidiendo que los usuarios legítimos puedan conectarse y acceder a Internet.

- **OWISAM-TR-009: Cliente intentando conectar a red insegura.**

Una red insegura es una red de comunicaciones, ya sea inalámbrica o por cable, que carece de medidas de seguridad adecuadas y suficientes para proteger los datos y la información que se transmiten a través de ella. En una red insegura, los dispositivos conectados y la información transmitida son vulnerables a diferentes tipos de amenazas, como el espionaje, la interceptación de datos, el acceso no autorizado y otros ataques cibernéticos.

Las redes inseguras a menudo carecen de cifrado de datos, autenticación de usuarios, control de acceso y otras características de seguridad importantes. Ejemplos comunes de redes inseguras incluyen redes Wi-Fi públicas no protegidas, como las que se encuentran en cafeterías, aeropuertos y hoteles.

- **OWISAM-TR-010: Rango de cobertura de la red demasiado extenso.**

Dentro de la configuración de una red inalámbrica la distancia a cubrir debe ser revisada con mucho cuidado, ya que si la señal/cobertura es demasiado extendida (Overextended Wi-Fi

network coverage) puede permitir que atacantes puedan conectarse a la misma (con o sin autorización).

Por lo que se recomienda realizar un sondeo acerca de los movimientos de los dispositivos para poder saber el alcance que debería tener la señal, la distancia a cubrir en ningún caso debería sobrepasar el límite perimetral físico del edificio, oficina etc. porque podría servir para que terceros (maliciosos o no) tengan la posibilidad de conectarse a esta, o peor aún utilizar un (extender-range) para prolongar aún más el alcance de la red. El problema radica en que los dispositivos (Routers) siempre estarán (broadcasting) lo que no es más que una constante envió de paquetes conteniendo información que deberá ser respondida por el dispositivo(s) (cliente (s)) y después de un cambio de información (handshake) la conexión estará establecida o denegada, esto no parara a menos que se implementen métodos no solo de autenticación sino de bloqueo a determinados dispositivos que coincidan con ciertos criterios (como muchas conexiones medio-abiertas) en un lapso muy corto de tiempo, o que no coincidan la MAC address física con la preconfigurada (MAC binding).

Problema de investigación

Mantener una conexión a internet a través de dispositivos móviles durante todo el día, es hoy algo muy común, razón por la que muchas veces la seguridad de las conexiones WLAN pasa inadvertida y para gran parte de los usuarios es irrelevante. En este escenario los cibercriminales han encontrado un sinfín de vulnerabilidades, que a diario explotan con nuevas y más avanzadas técnicas.

En este estudio se abordarán los distintos tipos de ataques que se utilizan para vulnerar la seguridad Wi-Fi, teniendo en cuenta que estos han ido evolucionando a la par de la tecnología y de los estándares de transmisión de datos inalámbricos (Berghel, H., y Uecker, J., 2005). Se recrearán estos ataques dentro de ambientes controlados, para identificar que vulnerabilidades se utilizaron y definir cuáles han sido o no han sido corregidas.

Finalmente se elaborará un documento con recomendaciones basadas en los datos obtenidos, tanto de la investigación práctica como de la investigación teórica, pudiendo aportar a cualquier usuario de redes wifi una guía para mantener segura su conexión y alerta de cualquier intento de ataque por parte de cibercriminales.

Objetivos

- Determinar el nivel de seguridad y confidencialidad que proporcionan las configuraciones de red al evaluarlas a través de la metodología OWISAM.
- Recrear los ciberataques más comunes a redes wifi para identificar tanto vulnerabilidades como métodos de explotación, y así definir si estos ya fueron corregidos o cómo corregirlos en el caso de que aún no.
- Establecer conclusiones y recomendaciones a las deficiencias de seguridad encontradas en los distintos tipos de redes inalámbricas que un usuario común puede encontrar.
- Definir las precauciones que un usuario debe tener al conectarse y navegar en una red wifi vulnerable, diferenciándolas por el nivel de seguridad y el tipo de encriptación que establezcan.

Metodología

Para este proyecto se buscan establecer una serie de recomendaciones para evitar ser vulnerables a los riesgos más comunes que se tienen en la redes de comunicación Wi-Fi, para obtener estas recomendaciones, se tomarán como punto de partida los diez principales riesgos identificados por OWISAM, se simularán estos riesgos en habientes controlados y se ejecutarán los ataques más comunes para cada riesgo a fin de que con esta experiencia se pueda emitir de forma clara y precisa las recomendaciones pertinentes para cada uno de los riesgos. Este proceso contará de los siguientes pasos:

Planificación: En esta etapa se define el alcance y los objetivos del análisis de vulnerabilidades Wi-Fi, se establecen los recursos necesarios para llevar a cabo el análisis, y se determina la metodología y las herramientas a utilizar.

Recopilación de información: En esta fase se recopila información sobre la infraestructura Wi-Fi a analizar, incluyendo el tipo de dispositivos, el tipo de autenticación utilizada, el tipo de cifrado, entre otros detalles.

Identificación de puntos de acceso: En esta fase se identifican los puntos de acceso Wi-Fi que se encuentran en el área de análisis y se registran sus detalles, como por ejemplo el nombre del SSID, el canal utilizado, la intensidad de la señal, etc.

Análisis de vulnerabilidades: En esta fase se lleva a cabo la exploración de vulnerabilidades, se emplean herramientas que permiten analizar el tráfico de red y los protocolos utilizados en la red Wi-Fi, y se intenta encontrar debilidades que puedan ser explotadas.

Explotación de vulnerabilidades: Una vez se han identificado vulnerabilidades, se intenta explotarlas para obtener acceso no autorizado a la red Wi-Fi o a los dispositivos conectados a ella.

Documentación de resultados: En esta etapa se registran todos los resultados obtenidos durante el análisis de vulnerabilidades Wi-Fi. Se documenta la metodología empleada, las herramientas utilizadas, los puntos de acceso identificados, las vulnerabilidades encontradas y las recomendaciones para corregir las debilidades detectadas.

Reporte final: Se elabora un informe final en el que se detallan los resultados obtenidos, las vulnerabilidades encontradas, las posibles consecuencias de explotar esas vulnerabilidades y las recomendaciones para mitigar los riesgos.

Marco Teórico

Un problema crucial en el ámbito de la seguridad informática es la seguridad de las redes inalámbricas. Las redes Wi-Fi se utilizan a menudo en espacios residenciales, comerciales y públicos, lo que las convierte en un objetivo apetecible para los delincuentes. Las herramientas especializadas, como las que se encuentran en Kali Linux, se utilizan para dar una amplia gama de capacidades para pruebas de penetración y auditorías de seguridad con el fin de comprender y mejorar la seguridad de estas redes.

Los mecanismos para salvaguardar las comunicaciones inalámbricas con métodos de cifrado y autenticación están establecidos por los protocolos WEP, WPA y WPA2. Sin embargo, cada uno de estos protocolos tiene ciertos puntos débiles y vulnerabilidades que pueden ser aprovechados por los atacantes.

Kali Linux es una distribución de Linux centrada en la seguridad y las pruebas de penetración. Para llevar a cabo auditorías de seguridad en redes inalámbricas, esta plataforma se ha convertido en un recurso muy apreciado por expertos e investigadores en seguridad. Aircrack-ng, y Reaver son sólo algunas de las muchas herramientas instaladas que vienen con Kali Linux y ofrecen sofisticadas capacidades para evaluar la seguridad de las redes inalámbricas.

Herramientas a utilizar:

Aircrack-ng: Es una colección de herramientas que son utilizadas para llevar a cabo auditorías de seguridad de redes inalámbricas. Tiene herramientas como airodump-ng que se utiliza para la captura de paquetes, aireplay-ng para inyección de paquetes, y airecrack-ng para recuperar claves WEP y WPA/WPA2 (Paspuel, 2018).

Reaver: Es una herramienta de fuerza bruta utilizada para obtener el PIN WPS de una red inalámbrica habilitada para WPS. Realiza múltiples intentos de PIN hasta encontrar el correcto y, a continuación, se puede utilizar para autenticarse en la red y obtener acceso.

Wireshark: es una herramienta de análisis de protocolos de red de código abierto y gratuita. Se utiliza para capturar y analizar el tráfico de red en tiempo real en un entorno de red. Wireshark permite a los administradores de red examinar el tráfico de la red y solucionar problemas, así como realizar tareas de seguridad de red, monitoreo y desarrollo de protocolos. La principal función de Wireshark es capturar paquetes de datos que se transmiten a través de una red y presentarlos en un formato legible para el análisis. Puede capturar el tráfico en una amplia variedad de interfaces de red, como Ethernet, Wi-Fi, Bluetooth, USB, entre otras. Una vez capturados los paquetes, Wireshark muestra una lista detallada de cada paquete capturado, incluyendo información sobre las direcciones IP de origen y destino, los puertos utilizados, los protocolos involucrados y los datos contenidos en el paquete. Esto permite a los administradores de red y desarrolladores analizar el tráfico de red para identificar problemas de rendimiento, diagnosticar errores de comunicación y entender cómo interactúan los diferentes componentes de una red.

Ettercap: es una herramienta de seguridad y análisis de redes de código abierto. Se utiliza para realizar ataques de tipo "Man-in-the-Middle" (MITM) en redes locales. Con Ettercap, los administradores de redes y los profesionales de seguridad pueden analizar el tráfico de red, realizar pruebas de penetración y detectar posibles vulnerabilidades en la red.

Metodología OWISAM (Open Wireless Security Assessment Methodology)

La Metodología Abierta de Evaluación de Seguridad Wireless OWISAM, nace como respuesta a la necesidad de una metodología fácil de utilizar y rápida de implementar para analizar la seguridad en redes wifi. A diferencia de otras metodologías como OWASP u OSSTMM. OWISAM analiza mucho más profundo los riesgos existentes en el entorno de las redes inalámbricas y propone un listado de 10 controles de seguridad Wireless para analizar el riesgo de seguridad al que está expuesta cualquier organización que implemente una red Wi-Fi dentro de su perímetro. Adicional a estos controles, OWISAM identifica los 10 riesgos de seguridad más comunes que afectan a las redes de comunicación inalámbricas y cuya mitigación debe ser prioritaria para evitar fuga de información.

Los diez principales riesgos OWISAM

OWISAM-TR-001: Red de comunicaciones Wi-Fi abierta

Este riesgo hace referencia a los peligros de conectarse en redes Wi-Fi que no disponen de una clave de seguridad para autenticarse o que la clave para autenticarse es de conocimiento público. Una red Wi-Fi abierta permite que cualquier host dentro de su cobertura pueda interceptar el tráfico que se genera dentro de ella. Dentro de una red Wi-Fi abierta cualquier información que se transmita puede ser interceptada e interpretada con ataques Man In The Middle, si no está correctamente encriptada, mediante un sniffer se puede interpretar el tráfico HTTP, o incluso con ayuda de un SSL Stripping se podría levantar el protocolo HTTPS, también las solicitudes DNS que viajan en texto plano podrían ser detectadas por un atacante.

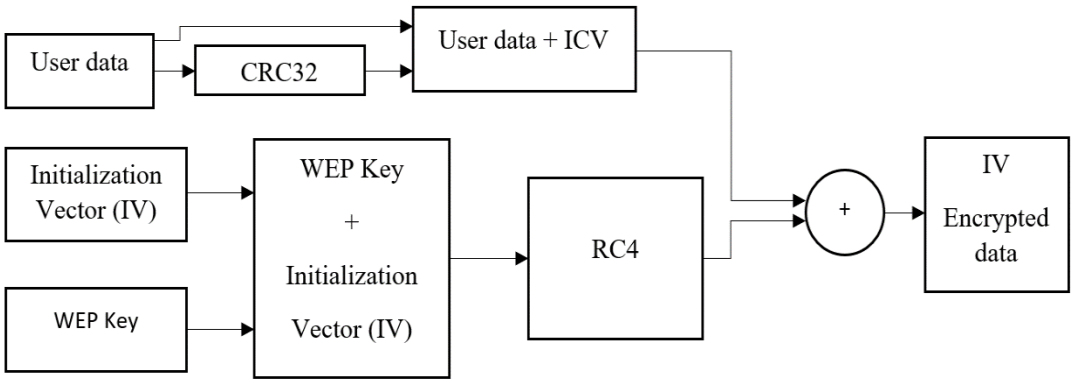
OWISAM-TR-002: Presencia de cifrado WEP en redes de comunicaciones

El cifrado WEP (Wired Equivalent Privacy o Privacidad Equivalente al Cable) fue el primer método de seguridad para redes inalámbricas especificado dentro del estándar IEE 802.11, hoy en día se lo considera un mecanismo de seguridad poco robusto y muy fácil de descifrar. (Tafur Bardales, 2018).

WEP a fin de cifrar las comunicaciones utiliza un algoritmo RC4 (Rivest Cipher 4), este algoritmo se caracteriza por la baja cantidad de recursos computacionales que requiere, esta fue una de las razones de su implementación, ya que en la época que vio la luz el hardware disponible adolecía de capacidad computacional. Para proporcionar confiabilidad, WEP implementó el algoritmo CRC-32 o verificación de redundancias cíclica de 32 bits, con el fin de detectar errores o modificaciones en la transmisión del mensaje (Fernández-Oliva Madrigal, 2020).

Figura 4

Esquema de encriptación WEP



Nota. Adaptado de WEP encryption scheme, por Mateusz Buczkowski, 2018, ¿How we ended up in WPA3? – Wi-Fi Security Evolution (https://www.grandmetric.com/).

Como se observa en la figura, la encriptación WEP se divide en dos subprocesos, en el primero, mediante el algoritmo CRC32 se genera un ICV (Integrity Vector Check o un Vector Comprobador de Integridad) que se añade a los datos del usuario, esto para asegurar la integridad en la transmisión. En el segundo subproceso se realiza la encriptación mediante RC4, primero los 24 bits del IV (Initialization Vector o Vector de Inicialización) que cambia con cada paquete enviado se suman a los 40 o 104 bits de la clave WEP que comparten todos los usuarios autenticados, formando una semilla de 64 o 128 bits de longitud, dependiendo del tamaño de la clave WEP, esta semilla pasa por un generador de códigos pseudoaleatorios RC4. Los resultados de estos dos subprocesos se añaden generando los datos encriptados WEP. (Fernández-Oliva Madrigal, 2020)

OWISAM-TR-003: Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).

La principal característica de WPS es su capacidad para simplificar la configuración de la seguridad inalámbrica mediante la utilización de una clave de acceso única de 8 dígitos llamada "PIN" (Personal Identification Number). Al ingresar el PIN en el dispositivo inalámbrico, el router inalámbrico autentica automáticamente el dispositivo sin la necesidad de introducir una contraseña compleja o extensa. Sin embargo, esta facilidad de uso también ha hecho que WPS sea vulnerable a ciertos ataques de seguridad, como los ataques de fuerza bruta que intentan adivinar el PIN.

La arbitraria elección de PIN generado por ciertos dispositivos WPS puede permitir el acceso no autorizado. Los dispositivos que siguen las especificaciones WPS más antiguas utilizan un PIN de ocho dígitos, que consta de dos mitades independientes. El primer dígito de la primera mitad indica su tipo (generado mediante un algoritmo estático) y los siete siguientes son aleatorios.

El segundo dígito de la segunda mitad es siempre un chequeo de sumas de comprobación para garantizar la integridad del PIN.

En el análisis de vulnerabilidad descubierto en OWISAM-TR-003, se muestra que es posible descubrir el PIN de ocho dígitos en pocos segundos, ya que la mitad aleatoria del número es mucho más débil de lo que debería ser. Un atacante con un alcance de radio suficientemente grande puede interceptar el intercambio de mensajes de la configuración sin cables (Wi-Fi) e intentar obtener el PIN de WPS con facilidad.

Una red Wi-Fi siempre puede ser víctima de WPS, a pesar de que utilicemos sistemas de autenticación distintos al PSK si está configurado con este protocolo. Si uno de los AP de la red tiene WPS habilitado, es habitual intentar primero que nada un ataque a WPS (Orcero, 2018).

OWISAM-TR-004: Clave WEP/WPA/WPA2 basada en diccionario.

El protocolo WEP (Wired Equivalent Privacy) está basado en el algoritmo RC4 que utiliza claves de cifrado de 64 o 128 bits que se comparten entre los dispositivos de la red. La clave secreta PSK (Preshared Secret Key) que tiene una longitud de 40 o 104 bits se concatena con un IV (Initialization Vector) que tiene un tamaño de 24 bits y generan un keystream por cada paquete el cual es utilizado por el algoritmo RC4 para cifrar y descifrar la información.

Sin embargo, el proceso de autenticación WEP es frágil y los ataques de diccionario lo pueden comprometer fácilmente. Los atacantes pueden capturar paquetes de datos que se transmiten entre dispositivos en la red y usar herramientas de descifrado para obtener la clave WEP. Luego el atacante puede acceder a la red inalámbrica sin restricciones una vez que se ha comprometido la clave. Por lo tanto, si se cuenta con las herramientas suficientes un atacante

fácilmente podría romper este protocolo y robar toda la información que circula por una red vulnerada.

Wi-Fi Protected Access, o WPA, se desarrolló para hacer más segura la comunicación con respecto del protocolo WEP. El mecanismo de autenticación EAP y el algoritmo de cifrado temporal TKIP, que son más poderosos, y son los que se utilizan en este protocolo. Sin embargo, también tiene sus debilidades; si se utilizan contraseñas débiles o cortas, WPA también es vulnerable a los ataques de diccionario y si la contraseña es sencilla puede ser vulnerada con mayor facilidad. Los atacantes pueden interceptar todo el tráfico de la red inalámbrica y usar una variedad de herramientas de ataques de fuerza bruta y descifrado para descubrir la contraseña.

Una versión más moderna y segura del protocolo WPA es WPA2, también conocido como Wi-Fi Protected Access 2. Utiliza el protocolo de autenticación 802.1X, que proporciona una autenticación más segura que la de WPA, y el cifrado Advanced Encryption Standard (AES), que ofrece una mayor seguridad. “WPA2 utiliza el cifrado de clave dinámica, que cambia la clave con frecuencia y la hace más difícil de descifrar.” (Ghimiray, 2022)

OWISAM-TR-005: Mecanismos de autenticación inseguros (LEAP, PEAP-MD5,)

Los protocolos LEAP, PEAP-MD5, han estado por mucho tiempo como parte de la seguridad/cifrado en el cambio de credenciales dentro de las comunicaciones Wireless, y aunque han sufrido importantes cambios/mejoras hasta donde el algoritmo de cifrado/factorización les ha permitido, pero tan pronto como se descubrió huecos/falencias, como que no todo el contenido dentro de los paquetes/tramas no eran cifradas como (usuario/clave), o que la manera de cifrar sufría falencias debido a que el mecanismo para cifrar dividía o acortaba la clave, propicio que

más ataques (mediante fuerza bruta) sean fructíferos y frecuentes, una vez conocido las falencias solo fue cuestión de obtener los handshake/tramas con sus respectivos hash para poder romper el cifrado, y eso es lo que se intentara mostrar especialmente en el protocolo MS-CHAPv2 que incluso después de prometer mejoras en respecto a MS-CHAPv1, aun es susceptible a ataques de fuerza bruta, al igual que el MD5 lo es también por lo que estos protocolos son considerados obsoletos, con todo los peligros que trae estos protocolos aún se puede observar su uso especialmente en servidores de autenticación empresariales usados en conjunto con WPA2 que como ya vimos en el apartado 4, también tiene falencias. (Schneier,2012)

OWISAM-TR-006: Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).

WPS no permite más que el uso de números, con un máximo de (8) caracteres lo que hace muy fácil el poder vulnerarlo, sin importar si este número es aleatorio (creado por el servidor o cliente) los parámetros/complejidad serán los mismos, por lo que no será particularmente difícil que mediante un ataque obtener la clave de conexión, pero si tomamos en cuenta que en una combinación de 8 caracteres hay una probabilidad de 100 millones de combinaciones posibles, aparte debemos saber que el digito #8 es usado como checksum (estamos en 7 caracteres ahora) y si a esto sumamos que tan solo los 4 primeros caracteres son usados para comparación/autenticación (parte 1), mientras los otros 3 caracteres son usados para validación conjuntamente con el resultado de los 4 primeros lo que nos reduce a aproximadamente 11,000 combinaciones posibles lo que en si no es difícil de crackear con una computadora de alto rango. (Horowitz, 2021)

OWISAM-TR-007: Red Wi-Fi no autorizada por la organización.

Dentro de una organización puede existir la posibilidad de personas pertenecientes a la misma o no, creen redes no autorizadas, las mismas que permiten de acuerdo con su seguridad ser atacadas.

Al ser una tecnología sin cables, cualquier persona dentro de su alcance puede realizar acciones maliciosas. Se mencionan los siguientes tipos de amenazas:

Denegación de servicio (DoS): consiste en sobrecargar los puntos de acceso o enrutadores mediante solicitudes masivas de servicio, lo que impide que los usuarios legítimos utilicen los servicios proporcionados.

Man-in-the-middle: el atacante se sitúa entre el emisor y el receptor, suplantando a una de las partes y engañando a la otra para que crea que está comunicándose con el destinatario legítimo. También se puede suplantar el punto de acceso.

Ataques por fuerza bruta: se intenta averiguar las claves criptográficas de la comunicación o las contraseñas de acceso a la red Wi-Fi probando todas las posibilidades. Aunque parezca poco probable, existen herramientas en línea que facilitan el descubrimiento de claves débiles o redes sin cifrado.

Espionaje: se captura de forma no autorizada el tráfico de red utilizando herramientas como antenas de largo alcance. El objetivo es obtener información transmitida, que puede ser completa si no está cifrada, o identificar patrones de comportamiento para intentar descifrarla.

MAC Spoofing: consiste en suplantar la dirección MAC de un dispositivo permitido cuando el punto de acceso tiene una lista de direcciones MAC autorizadas. (INCIBE,2019)

OWISAM-TR-008: Portal hotspot inseguro.

Un hotspot es un punto de acceso es una ubicación física donde las personas pueden conectar sus dispositivos móviles a Internet, generalmente mediante Wi-Fi, a través de una red de área local inalámbrica (WLAN) o mediante un punto de acceso móvil. Un punto de acceso móvil se crea mediante la conexión de datos de su teléfono inteligente para conectar su computadora portátil a Internet. (Intel, 2022)

En un hotspot se puede implementar un portal cautivo que es una página web que se muestra a los usuarios de una red inalámbrica antes de que se les otorgue acceso a Internet. Esto proporciona autenticación y autorización segura para empleados y clientes que acceden a su red Wi-Fi. Los portales cautivos también se pueden utilizar para una variedad de propósitos, como marketing o seguimiento de la actividad de los clientes. (TP-Link, 2022)

Una de las vulnerabilidades del portal cautivo es el ataque de DNS-Tunneling, El sistema de nombres de dominio, o DNS, es un protocolo fundamental de Internet que traduce las URL amigables para los humanos en direcciones IP amigables para las máquinas. Los ataques basados en DNS aprovechan el protocolo DNS para canalizar malware y otros datos a través de un modelo cliente-servidor. El sistema de resolución de DNS es un servidor que transmite las solicitudes de direcciones IP a los servidores de dominio raíz y de nivel superior. Establece una conexión entre la víctima y el atacante a través de la resolución de DNS. (Palo Alto Networks, s.f.)

OWISAM-TR-009: Cliente intentando conectar a red insegura.

Los clientes están expuestos a una serie de riesgos de seguridad y privacidad cuando se conectan a una red no segura, como una red Wi-Fi abierta o una red sin las medidas de seguridad adecuadas.

Una red que carece de mecanismos de seguridad adecuados para salvaguardar los datos transferidos entre dispositivos conectados se considera insegura. Las redes Wi-Fi que carecen de cifrado o tienen normas de seguridad débiles, las redes que carecen de autenticación adecuada o las redes que no utilizan medidas de seguridad adicionales como cortafuegos o detección de intrusos podrían entrar en esta categoría.

Los piratas informáticos son capaces de interceptar la comunicación de red que se envía entre el cliente y otros dispositivos en la red para recopilarla y leerla. Estos ataques pueden implicar el análisis del tráfico, la captura de paquetes y el despliegue de herramientas especializadas para descifrar datos críticos. Por tanto, los datos enviados entre el cliente y otros dispositivos, como contraseñas, información personal o datos sensibles pueden ser interceptados y comprometidos al conectarse a una red insegura. De ello pueden derivarse robos de identidad, accesos ilegales a cuentas en línea, divulgación de información privada y otros problemas de seguridad y privacidad.

OWISAM-TR-010: Rango de cobertura de la red demasiado extenso.

Para tener una mejor idea del (rango de cobertura) primero debemos entender que las señales viajan como ondas (direccional – bidireccional, etc) ya sea dentro del espectro 2.5Ghz o 5Ghz, que son las más comúnmente usadas, estas señales se debilitaran o perderán poder cada cierta distancia o por obstáculos (como paredes, objetos etc.) a esto debemos sumarle el poder de

transmisión (20%, 40%, 100% etc.) que este configurado el dispositivo, sumado a la sensibilidad del dispositivo recibidor etc.

Todo lo expuesto arriba, crea un complejo escenario que deberán tomar en cuenta con los resultados de los diferentes parámetros antes de concebir el tipo de Metodología (100% inalámbrica, hibrida, mesh, bus etc.) y su posterior implementación tanto en el tipo de dispositivos (con su alcance) y la localización de cada uno de estos (para impedir perdidas considerables de señal) o lo que es peor aún tener una señal demasiado robusta/fuerte, que sobrepase las necesidades reales y se convierta en un elemento más de intento de ataques.

Lo que nos lleva a entender que una cobertura demasiado extensa, en si es la mala concepción de una red, a la cual le hemos dado mayor volumen, mayor número de dispositivos (Routers, APs etc.) de lo que realmente es necesario lo cual a lo mejor permitiría que un dispositivo no tenga problemas de señal/cobertura, pero si crea un problema en cuanto a la seguridad/privacidad, ya que al ser demasiado extensa fácilmente será blanco de intentos de intercepción, clonación etc., debido a que al tener una buena/fuerte señal puede ser usada por terceros/ajenos a la organización para intentar ser parte/uso de esta.

CAPÍTULO 2

Desarrollo

Una vez se ha expuesto toda la teoría relevante a la seguridad de redes Wi-Fi, se procede con la verificación de cada una de las vulnerabilidades expuestas, mediante pruebas dentro de ambientes controlados, tomando en cuenta los 10 principales riesgos detallados dentro de la metodología OWISAM.

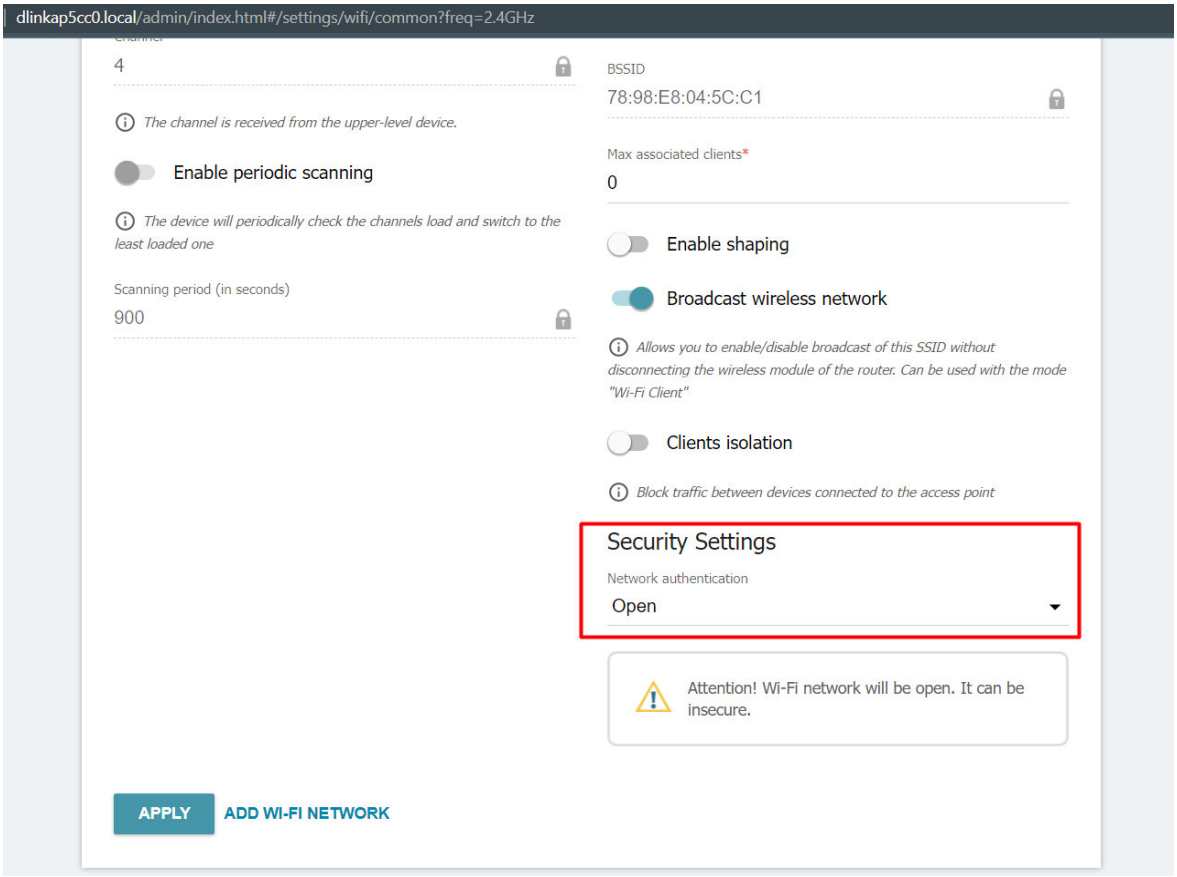
OWISAM-TR-001: Red de comunicaciones Wi-Fi abierta

Para este riesgo es necesario simular una red Wi-Fi abierta, como las que se pueden encontrar en lugares públicos, principalmente en centros comerciales, hoteles y estaciones de transporte. Para este fin se tiene un equipo: Wireless N300 Router (DIR-615) de la marca D-Link, este es el punto de acceso a la red inalámbrica, por lo que en su WAN debe conectarse a una red con salida a internet.

Primero se configura el equipo en el apartado de autenticación de red como abierto, es decir que no solicite una contraseña a los usuarios que quieran conectarse, el mismo equipo en su página de configuración muestra una advertencia indicando que “La red Wi-Fi estará abierta. Esto puede ser inseguro” se aplica el cambio como se muestra en la figura.

Figura 5

Configuración de red Wi-Fi abierta equipo D-Link



Nota. Pantalla de configuración de un rúter D-Link Wireless N300 Router (DIR-615)

Una vez se ha configurado una red Wi-Fi abierta y con salida a internet, basta con conectarse a la misma y mediante un software de escucha y captura de paquetes, analizar el tráfico que pasa a través de Access Point. Para hacer una red abierta mucho más atractiva, los atacantes suelen colocarle SSIDs atractivos como FreeWifi, o Red Abierta. Para la captura y análisis del tráfico se utiliza la herramienta Wireshark, que es un software libre. Es importante mencionar que todos los ataques que se mostrarán a continuación, también se pueden realizar en redes con clave de autenticación una vez esta ha sido vulnerada.

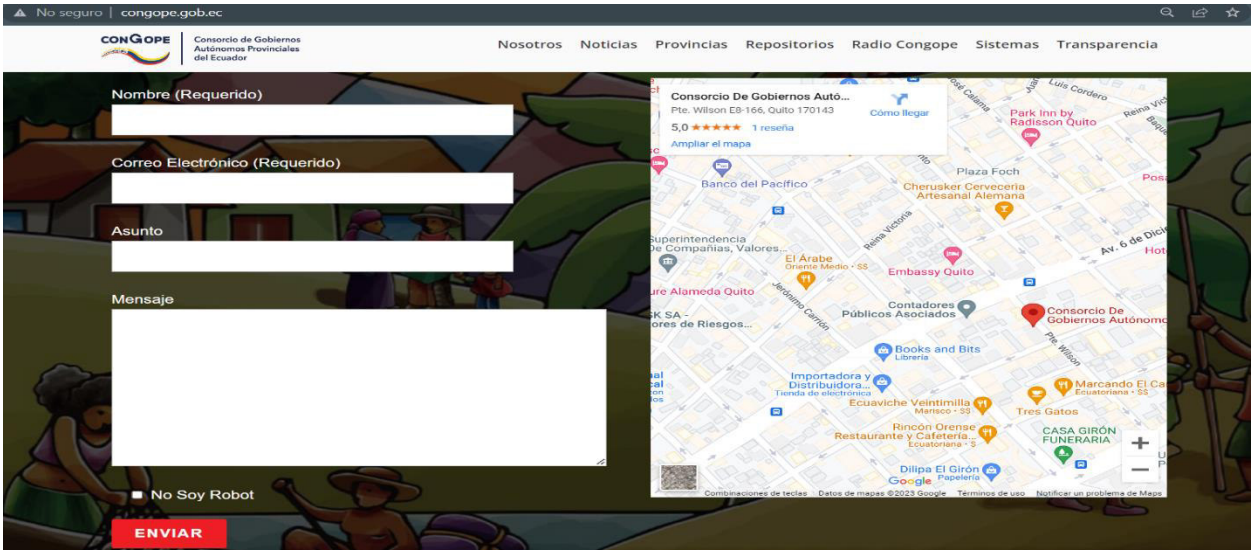
Ataque Man In the Middle

Un ataca de hombre en el medio consiste en obtener la capacidad de leer, e incluso modificar los mensajes generados entre dos víctimas, este ataque se puede realizar en cualquier red Wi-Fi una vez se forma parte de esta, en redes abiertas es más fácil ya que no se requiere conocer la clave de autenticación. Para este ejemplo, mientras se mantiene Wireshark a [i]la escucha, se simula a un usuario conectado a la red Wi-Fi abierta, que comete el error de emitir información en texto plano, hoy en día son muy pocas las páginas web que aún trabajan con protocolos inseguros como HTTP.

Para este ejemplo se utiliza una página web gubernamental que aún no se ha migrado a HTTPS, la página es: http://www.congope.gob.ec/ perteneciente al Consorcio de Gobiernos autónomos del Ecuador. En esta página web se puede encontrar un formulario de contacto, donde el usuario debe introducir su nombre, un correo, un asunto y un mensaje. Adicionalmente la página como medida de seguridad implementa un botón que indica “No soy un robot” antes de permitirnos enviar la información. Este formulario se lo puede observar en la siguiente figura.

Figura *6*

Formulario de contacto, página CONGOPE



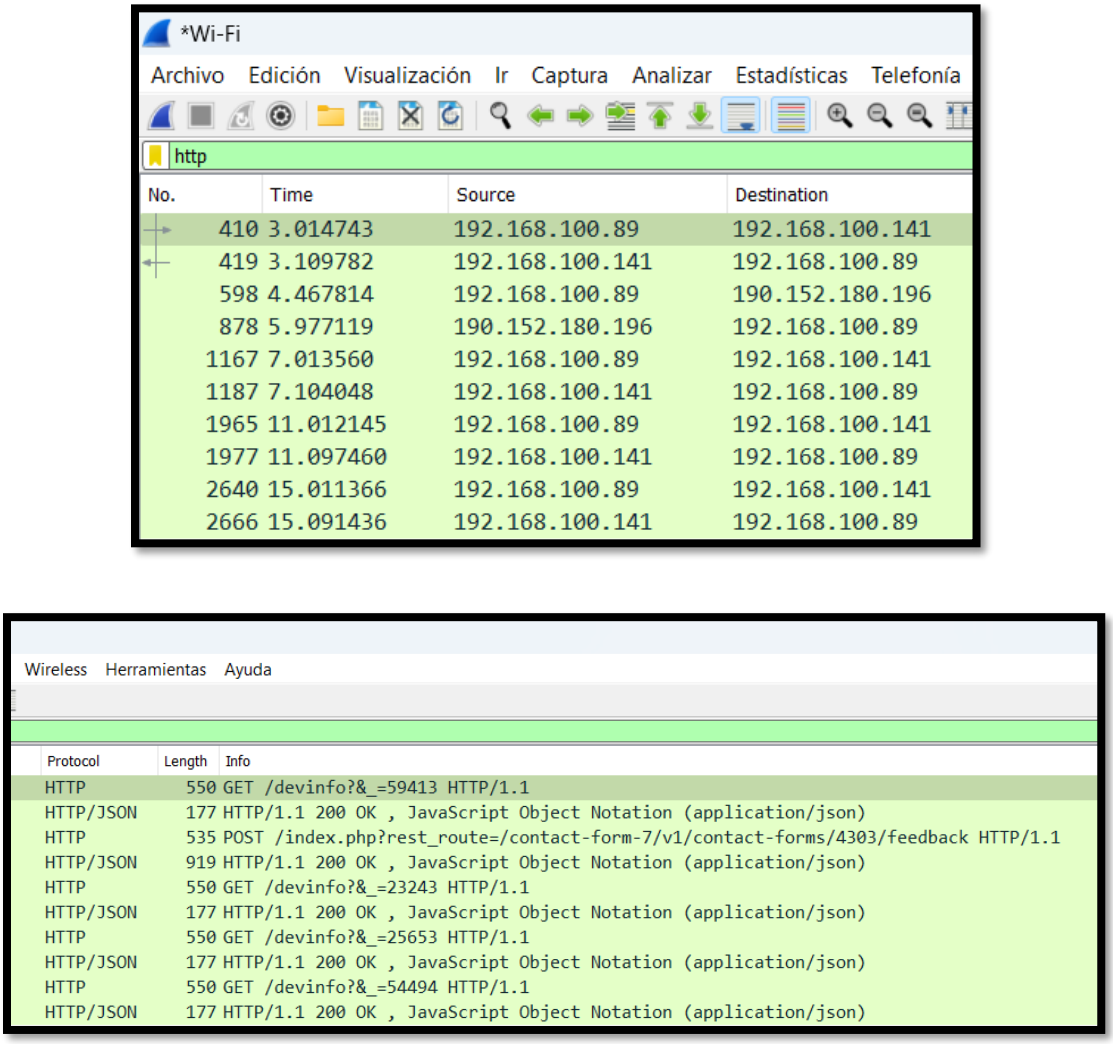
Nota. Página web que utiliza protocolo HTTP para el envío de formularios.

Un usuario conectado mediante la red abierta, al enviar este formulario con sus datos se expone a que otro usuario dentro de la red con ayuda de un sniffer como Wireshark identifique este paquete y extraiga la información contenida, para este caso al ser un formulario de mensaje los datos que se pueden extraer no son sensibles, pero de la misma forma se lo puede realizar para accesos a correos o entidades bancarias que no dispongan de protocolos más seguros.

Para continuar con la simulación se realiza el envío del formulario por parte del host atacado y se extraen todos los paquetes con protocolo http a través del host atacante, observando los resultados de la siguiente figura:

Figura 7

Captura de tráfico http mediante Wireshark



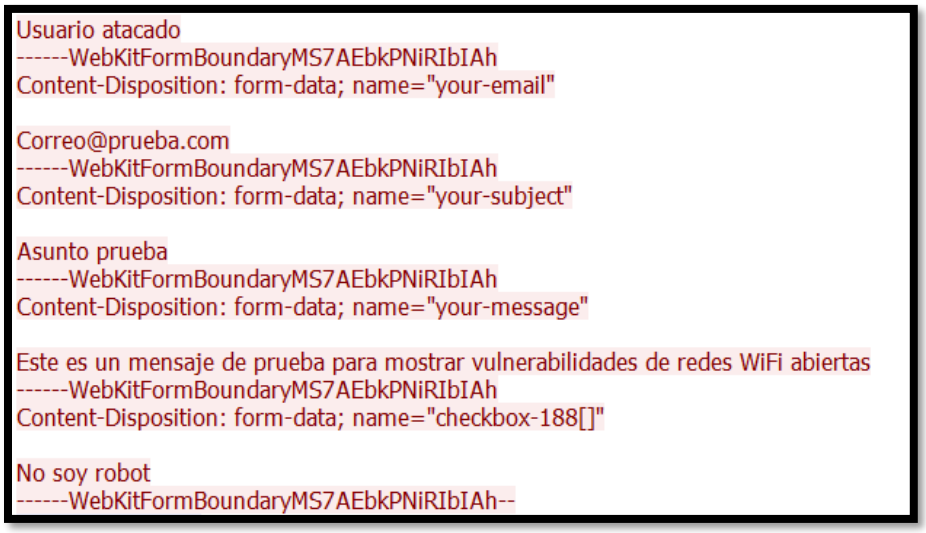
Nota. Captura tomada del tráfico inalámbrico mediante Wireshark, filtrado por paquetes HTTP.

Para identificar el paquete con la información de host atacado, se tiene que revisar la IP de origen y la de destino o identificar el método post, mismo que se observa en la tercera línea del listado de paquetes capturados, analizando este paquete podemos extraer toda la información enviada por parte del host atacado, para este caso en nombre: “Usuario atacado”, correo:

“Correo@prueba.com”, asunto: “Asunto prueba” y mensaje: “Este es un mensaje de prueba para mostrar vulnerabilidades de redes Wi-Fi abiertas” como se muestra en las siguientes figuras:

Figura 8

Secuencia HTTP del paquete analizado



Nota. Secuencia del paquete HTTP analizado mediante el sniffer Wireshark.

SSL Stripping

Un ataque de SSL stripping consiste en interceptar una conexión segura entre un host y un servidor web y forzarla está conexión a trabajar sin cifrado. El ataque tiene como objetivo engañar al host haciéndole creer que mantiene una conexión segura, mientras el atacante es capaz de ver toda la información que se transmite dentro de esa conexión. Este tipo de ataque se aprovecha de la vulnerabilidad de algunos servidores web que permiten acceder a su contenido a través de conexiones HTTP no cifradas. El atacante intercepta la conexión segura entre el usuario y el servidor, y luego altera los paquetes de datos para que el usuario se conecte a una versión no segura del sitio web en lugar de la versión segura. Para realizar un SSL stripping, el atacante necesita estar

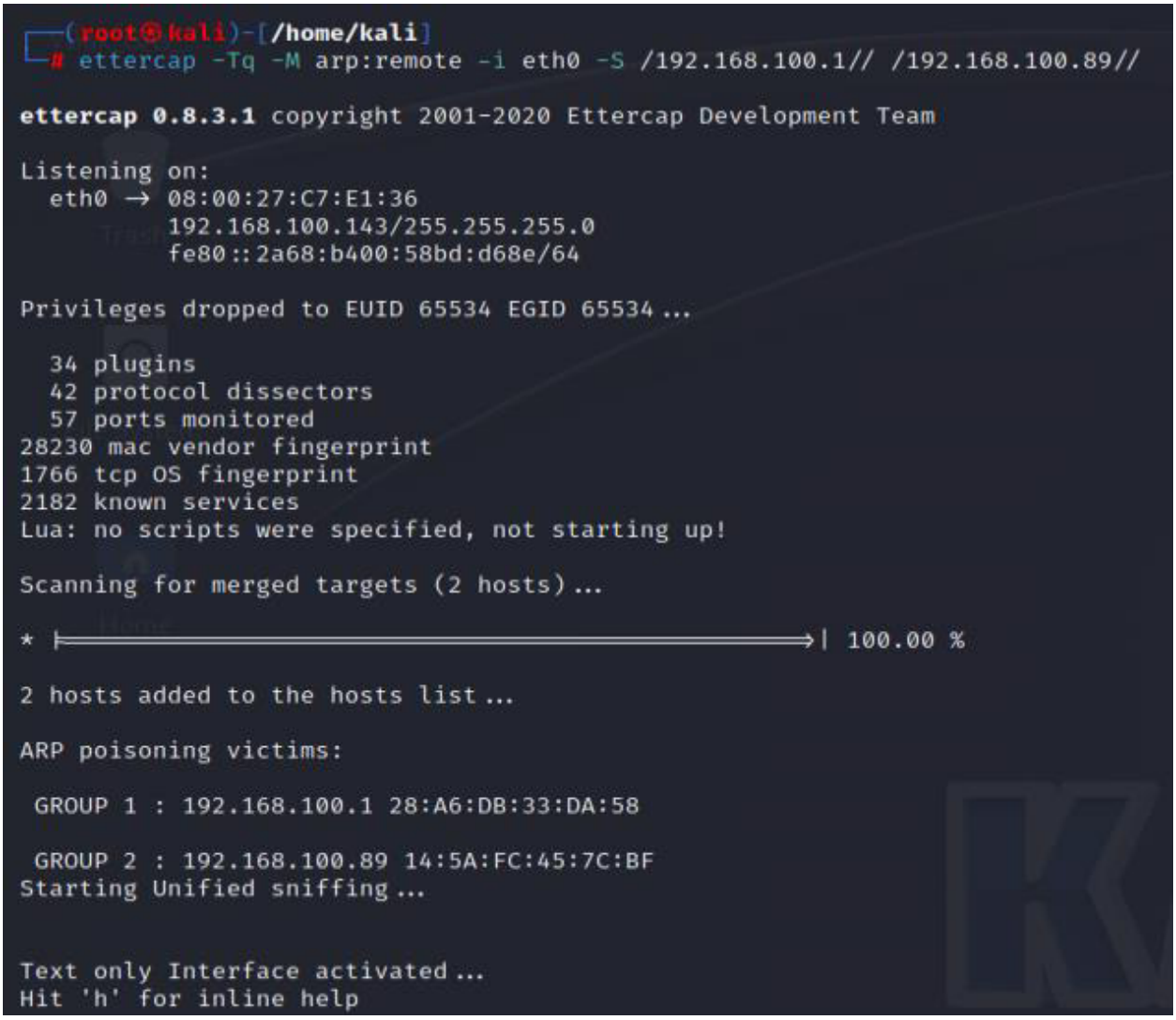
en una posición privilegiada en la red para poder interceptar el tráfico, lo que se facilita cuando se tienen redes Wi-Fi abiertas.

El proceso para realizar este tipo de ataque inicia con un envenenamiento de tablas ARP, las tablas ARP registran la dirección IP y la dirección MAC de todos los hosts dentro de un dominio de broadcast, el envenenamiento consiste en hacer creer a la víctima que la dirección IP del Gateway corresponde la dirección MAC del atacante, así toda conexión que realice la víctima hacia internet pasará primero por el equipo del atacante. Para se puede hacer usa de la herramienta ettercap disponible en Kali Linux.

Para efectuar correctamente este ataque es importante identificar bien la interfaz de red que se utilizará, así como las IP de la víctima y del Gateway, tal y como se muestra en la siguiente figura:

Figura 9

Envenenamiento de tabla ARP con ettercap



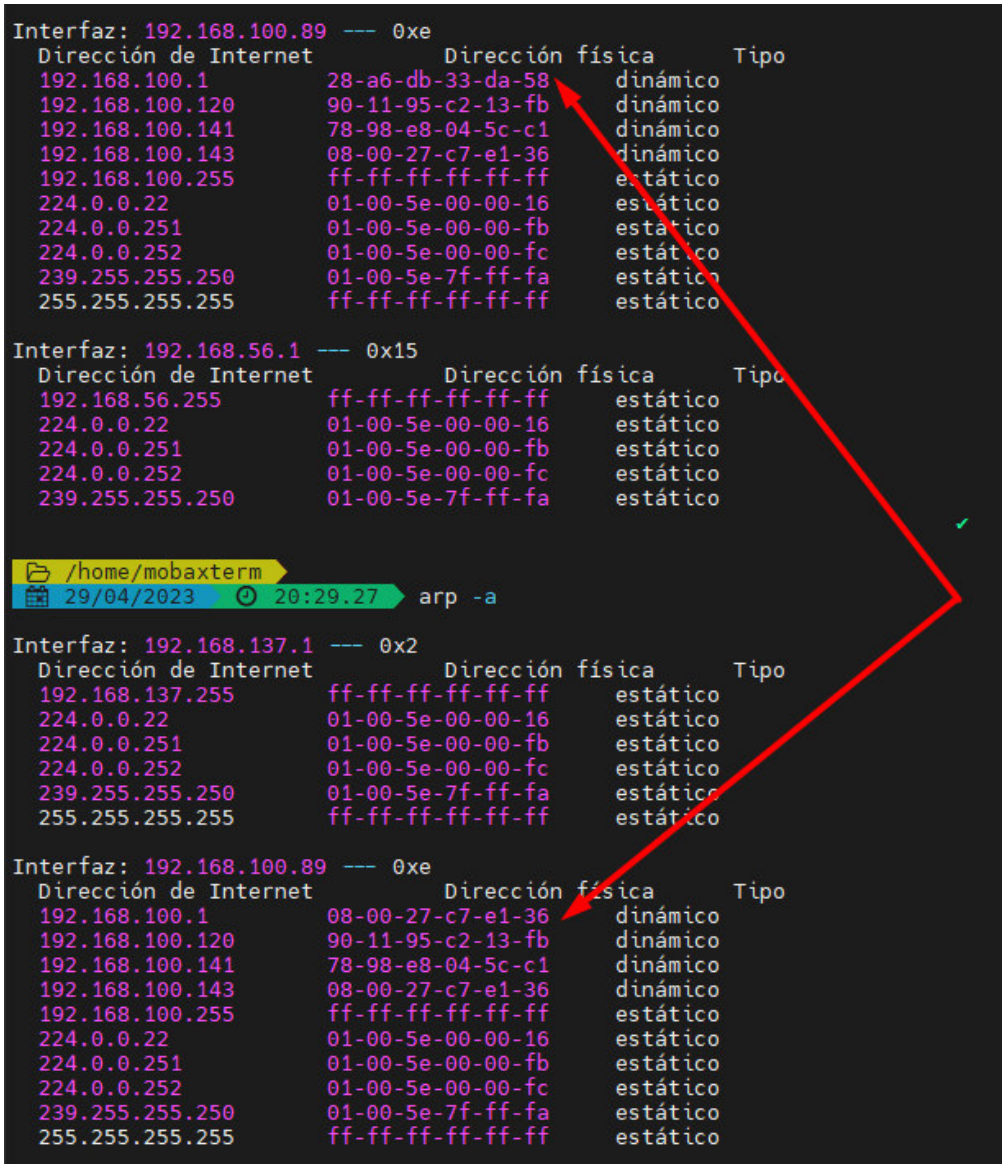
Nota. Aplicación ettercap utilizada para envenenamiento de tabla ARP, se hace creer a la víctima que la dirección MAC del Gateway es la MAC de la máquina atacante.

Una vez se ejecuta el ataque de envenenamiento ARP, es muy fácil comprobar si se lo realizó correctamente, basta con comparar la tabla ARP registrada en la host víctima antes y después de ejecutado el ataque, al comparar la dirección MAC asociada al Gateway se notará el

cambio, como se muestra en la siguiente figura, la nueva dirección MAC del Gateway es la del equipo atacante.

Figura 10

Tabla ARP de la máquina víctima antes y después de envenenamiento ARP



Nota. Se puede observar cómo cambia la dirección MAC asociada a la IP 192.168.100.1 (Gateway) dentro de la tabla ARP del host víctima del ataque.

También se puede utilizar la interfaz gráfica de ettercap y facilitar el ataque, a continuación, se detallan los pasos a seguir para realizar un SSL Stripping mediante la interfaz gráfica de Ettercap en Kali Linux:

Instalar Ettercap: para instalar Ettercap, se puede utilizar el siguiente comando en la terminal de Kali Linux: sudo apt-get install ettercap-graphical.

1. Configurar IP forwarding: para permitir que los paquetes de red se redirijan a través de Ettercap, se debe habilitar el reenvío de IP con el siguiente comando: echo 1 > /proc/sys/net/ipv4/ip_forward.

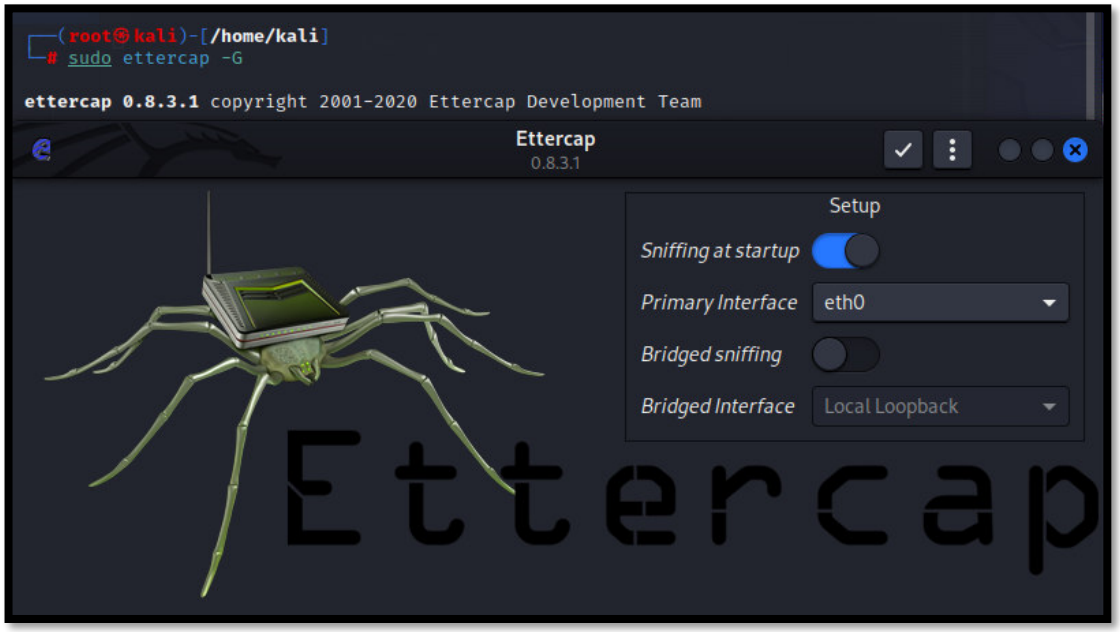
Figura 11

Habilitar el reenvío IP en Kali Linux desde consola.

2. Abrir Ettercap: se puede abrir Ettercap en modo gráfico desde la terminal con el siguiente comando: sudo ettercap -G.

Figura 12

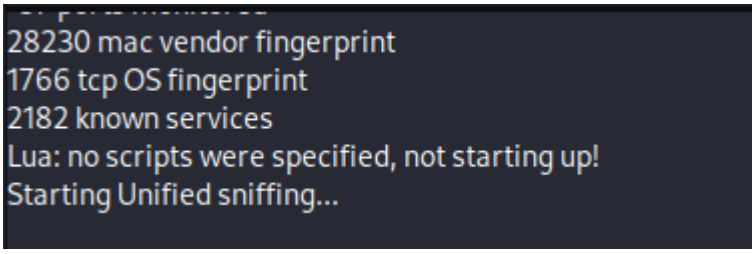
Interfaz gráfica de ettercap, ejecutada desde consola en Kali Linux.



3. Seleccionar la interfaz de red: en Ettercap, se debe seleccionar la interfaz de red que se utilizará para interceptar el tráfico de red. Seleccionar "Sniff" en el menú principal y aceptar en el ícono de visto en la parte suprior de la ventana, esto inicia el Unified sniffing

Figura 13

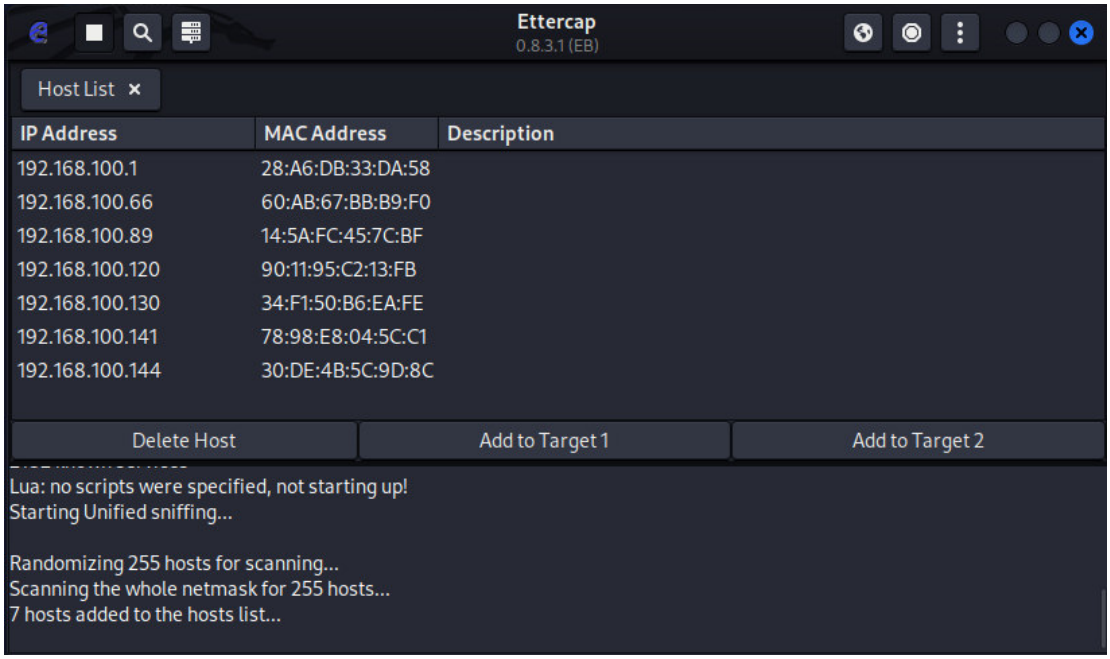
Mensaje de inicio del Unified sniffing en ettercap.



4. Escanear la red: para encontrar los dispositivos en la red, se puede seleccionar "Hosts" y luego "Scan for hosts". Esto mostrará una lista de dispositivos en la red.

Figura 14

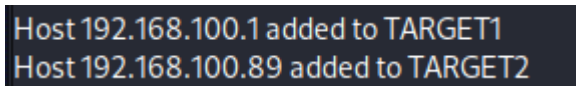
Lista de host mostrada por ettercap luego del escaneo.



5. Añadir los objetivos: para añadir los objetivos, se puede seleccionar "Hosts" y luego "Host list". Se deben seleccionar los dispositivos a los que se quiere interceptar el tráfico de red.

Figura 15

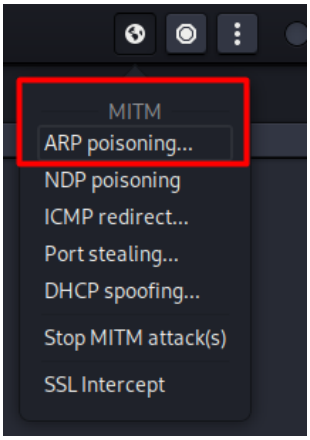
Lista de host objetivos para el ataque en ettercap



6. Iniciar el ataque: para iniciar el ataque de SSL stripping, se puede seleccionar "Mitm" y luego "ARP poisoning". Esto permitirá que Ettercap redirija el tráfico de red entre los objetivos.

Figura 16

Herramienta de ARP poisoning en ettercap.



7. Habilitar el SSL stripping: para habilitar el SSL stripping en Ettercap, se debe seleccionar "Plugins" y luego "Manage the plugins". En la ventana que aparece, se debe buscar el plugin "Ettercap SSL strip" y habilitarlo.

Figura 17

Habilitar plugin SSL strip en ettercap

Una vez finalizado un ataque de SSL Stripping correctamente, si el usuario intenta acceder a una página segura que implementa HTTPS, el atacante intentará desagradar esta conexión a HTTP, si la página y el navegador permiten esta degradación, el equipo víctima será vulnerable a la intercepción de la información enviada mediante un sniffer como se explicó en la sección pasada.

Hoy en día ya es muy difícil que este ataque se efectué con éxito ya que los navegadores implementan varias seguridades para prevenir la vulnerabilidad y proteger a los usuarios, entre estas tenemos:

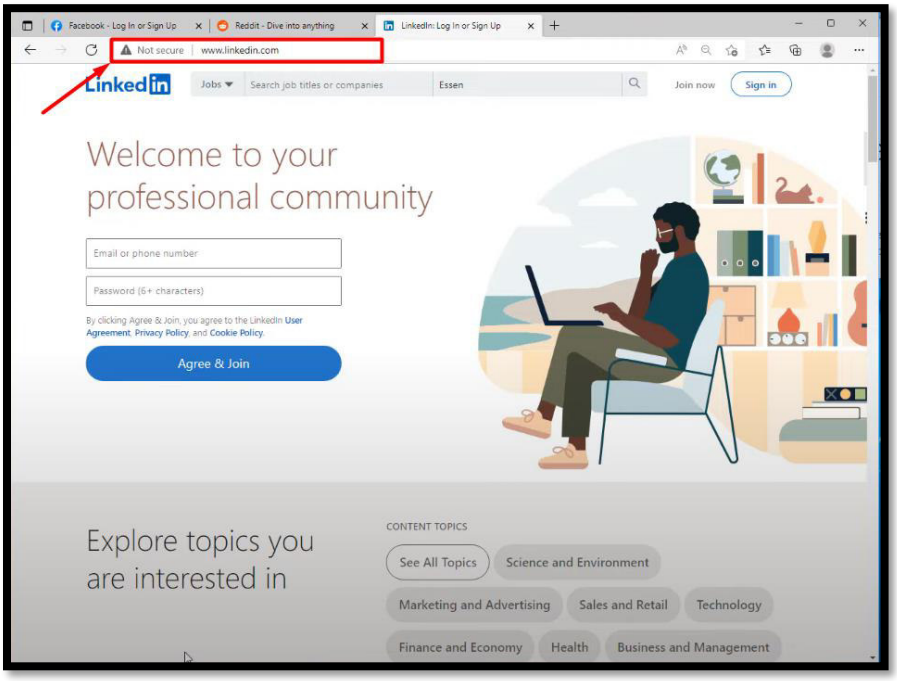
- HSTS (HTTP Strict Transport Security)**:** esta es una política de seguridad implementada en el servidor web que indica al navegador que se debe utilizar una conexión HTTPS segura para todas las comunicaciones con el sitio web. Cuando un usuario intenta conectarse a un sitio web que utiliza HSTS, el navegador no permitirá que se establezca una conexión HTTP no segura.
- Redirección HTTPS: algunos sitios web utilizan una redirección automática del tráfico HTTP a HTTPS. Si un usuario intenta conectarse a un sitio web utilizando una conexión HTTP no segura, el servidor web redirigirá automáticamente al usuario a una conexión HTTPS segura.
- Certificados SSL/TLS: los navegadores utilizan certificados SSL/TLS para autenticar la identidad del sitio web y cifrar las comunicaciones HTTPS. Si un certificado no es válido o es auto-firmado, el navegador mostrará una advertencia al usuario indicando que la conexión no es segura.
- Bloqueo de contenido mixto: los navegadores modernos bloquean el contenido mixto (HTTP y HTTPS) en una página web. Si un sitio web utiliza contenido no seguro en una conexión segura, el navegador bloqueará el contenido y mostrará una advertencia al usuario.
- Autenticación de dominios: algunos navegadores utilizan la autenticación de dominios para proteger al usuario de los ataques de phishing. Si un sitio web utiliza

un dominio que no coincide con el certificado SSL/TLS, el navegador mostrará una advertencia al usuario indicando que el sitio web no es seguro.

A continuación, en la figura se verifica la página web de la rede social LinkedIn degradadas a HTTP mediante un ataque SSL Stripping, cabe recalcar que las capturas se tomaron en el navegador Microsoft Edge hace más de 2 años, al momento las seguridades implementadas por el navegador ya no permiten acceder a estos sitios por HTTP.

Figura 18

Página de LinkedIn ejecutada con un protocolo HTTP mediante navegador Microsoft Edge, luego de ataque SSL stripping.



OWISAM-TR-002: Presencia de cifrado WEP en redes de comunicaciones

El cifrado WEP (Wired Equivalent Privacy) desde su lanzamiento en 1997 se ha caracterizado por presentar varias vulnerabilidades, mismas que han sido explotadas y obligaron

la utilización de cifrados más seguros. Como principal vulnerabilidad del cifrado WEP se tiene su esquema de cifrado RC4 (Rivest Cipher 4), a continuación, se enlistan brevemente los problemas asociados:

WEP utiliza un número de inicialización (IV) de 24 bits para cifrar los datos. Sin embargo, debido a la forma en que se implementa, el espacio de claves efectivo se reduce, lo que permite que los IV se repitan más rápidamente. Esto facilita el ataque de fuerza bruta y la recuperación de la clave. A esta vulnerabilidad se la conoce como IV Weakness o flujo de inicialización débil.

WEP utiliza una clave de cifrada estática compartida por todos los dispositivos en la red. Esto significa que, si un atacante logra obtener la clave, puede descifrar todo el tráfico de red.

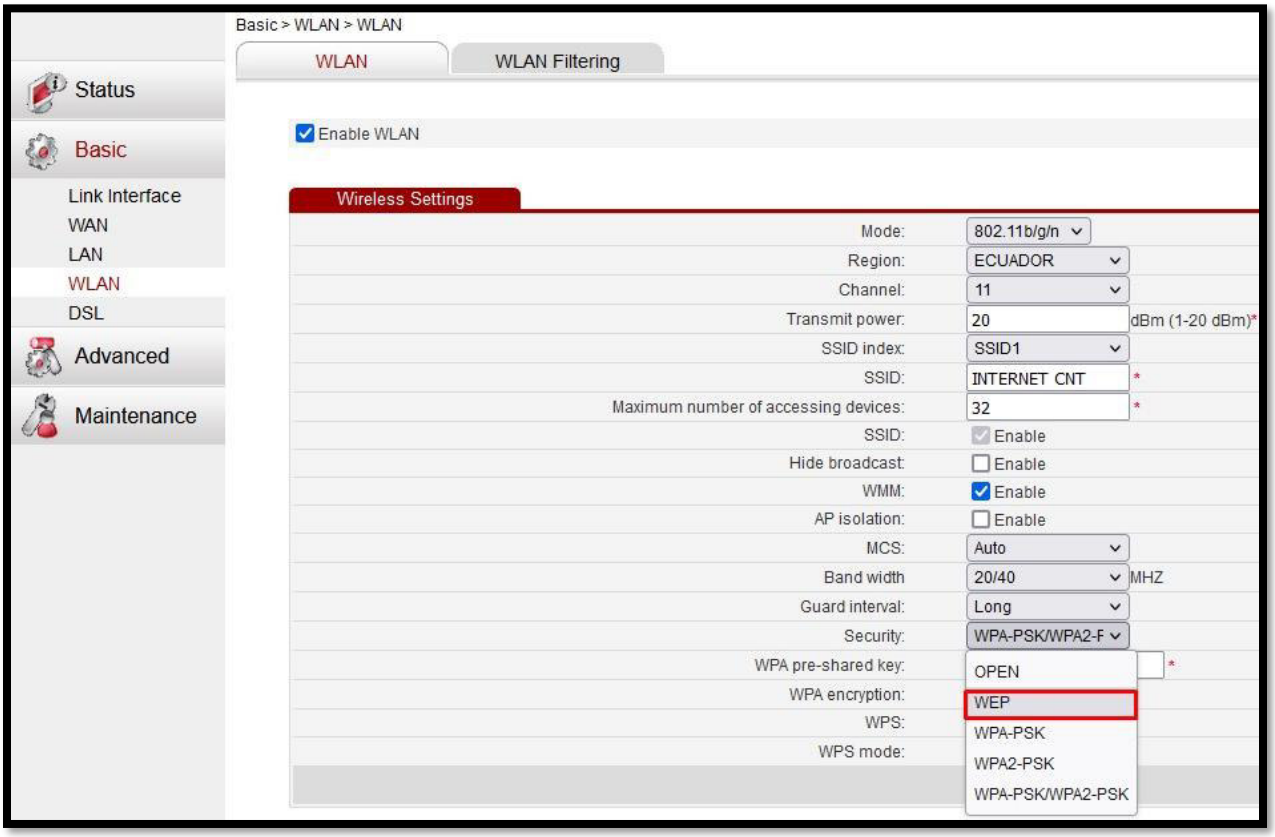
WEP no proporciona autenticación mutua entre el punto de acceso y los dispositivos cliente, lo que permite que un atacante se haga pasar por un punto de acceso legítimo y capture información sensible.

Para establecer medidas de prevención ante estas vulnerabilidades, se recrea una red Wi-Fi con cifrado WEP dentro de un ambiente controlada, luego descifrará la contraseña de acceso a esta red utilizando las vulnerabilidades antes descritas, con este fin se utilizará únicamente un Access Point Huawei HG532s al que se le configurará con cifrado WEP y adicional se requiere un host, en este caso un computador para efectuar el ataque.

Primero se configura el Access Point con seguridad WEP y se introduce una clave de 64 bits, para nuestro caso serán 10 dígitos hexadecimales que irán de 1 al 9 y luego el número 0 (1234567890). En la figura se puede observar la configuración según lo indicado.

Figura 19

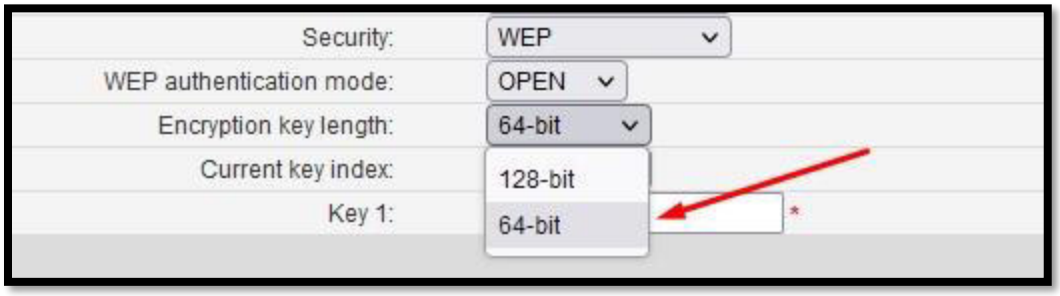
Pantalla de configuración, Access Point Huawei HG532s



A fin de simplificar el proceso, en el tamaño de encriptación se seleccionan 64 bits, como se muestra en la siguiente figura, teniendo en cuenta que el proceso para una clave de 128 bits es el mismo, solo que toma más recursos la obtención de la clave.

Figura 20

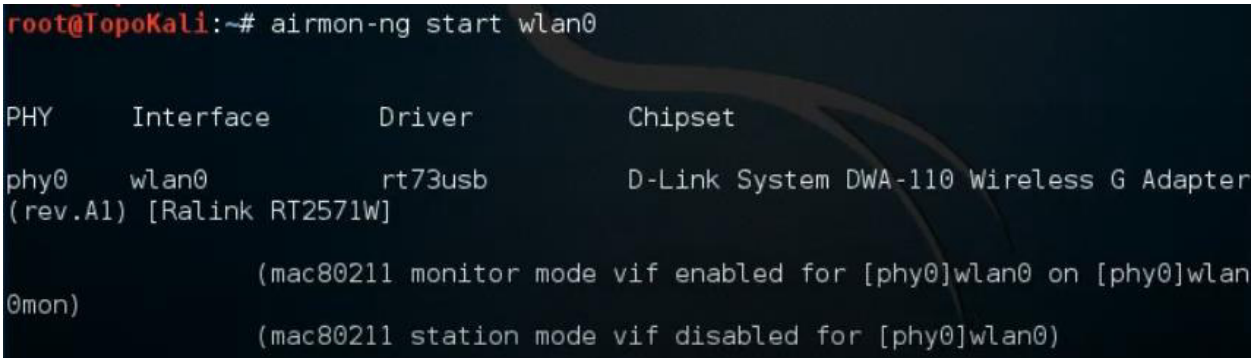
Tamaño de la clave de encriptación, AP Huawei HG532s



Con el comando airmon-ng start wlan0 iniciamos el modo de monitoreo en la interfaz inalámbrica wlan0, este modo permite la captura y análisis del tráfico de la red inalámbrica también crea una nueva interfaz virtual con el nombre “mon0”.

Figura 21

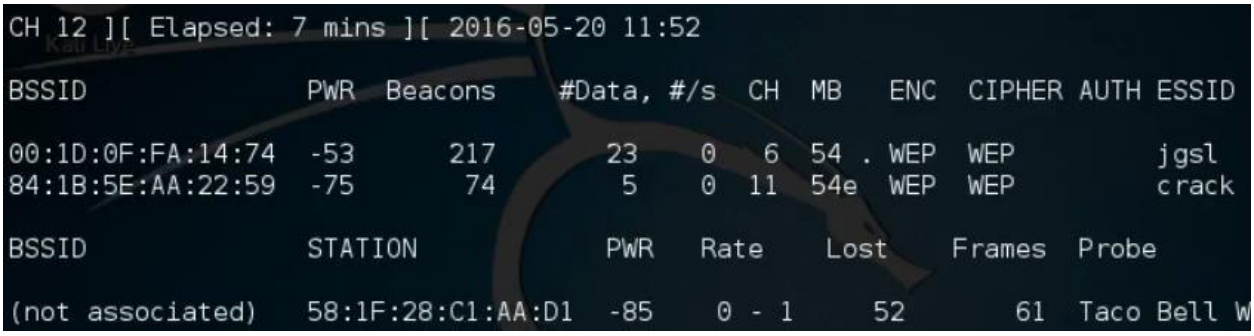
Inicialización del modo monitor con la herramienta airmon-ng



Con el comando airodump-ng wlan0mon, en pantalla se mostrarán información detallada sobre las redes inalámbricas cercanas, aquí veremos detalles como BSSID (Identificador único de la red), el ESSID (nombre de la red), el número de canal, la potencia de la señal, la tasa de transferencia, los dispositivos conectados y otros datos relevantes.

Figura 22

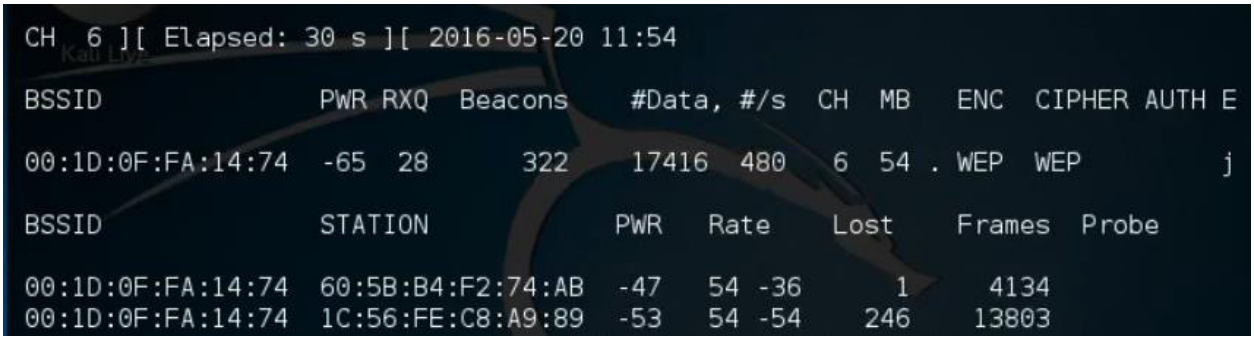
Información de redes inalámbricas cercanas obtenida con la herramienta airodump-ng



Con el comando airodump-ng -c 6 –bbsid [MAC AP] wlan0, el programa airodump-ng realizará un escaneo activo en el canal 6, capturando información detallada de la red inalámbrica específica identificada por su dirección MAC.

Figura 23

Escaneo activo del canal 6 realizado con la herramienta airodump-ng



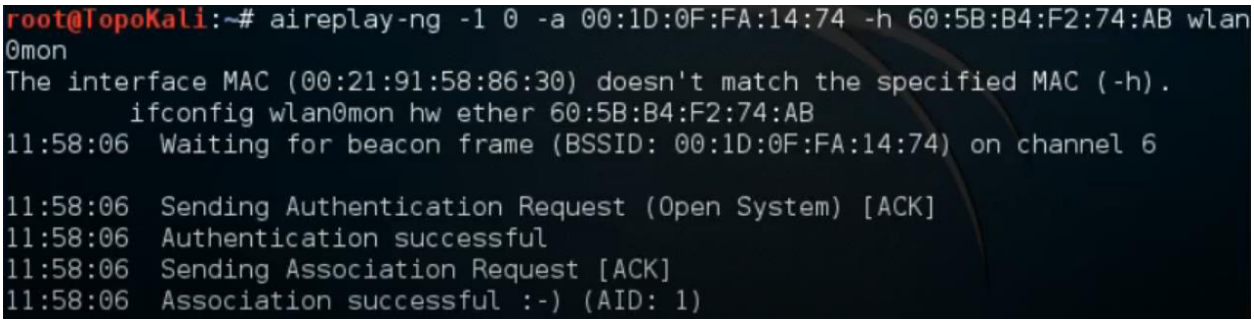
Identificamos la dirección MAC de un equipo asociado 60:58:B4:F2:74:AB, a continuación, utilizamos el comando airodump-ng -c 6 – bbsid [MAC AP] -w [nombre] wlan0, para grabar en un archivo todos los logs en un archivo con el nombre elegido.

Con el comando aireplay-ng -1 0 -a [MAC AP] -h [MAC víctima] wlan0mon, aireplay-ng enviará paquetes de des autenticación al punto de acceso (AP) especificado, haciéndole creer que la víctima se está desconectando constantemente de la red.

- "-1" indica que se va a utilizar el método de ataque de des autenticación.
- "0" especifica el número de reintentos de des autenticación que se enviarán. En este caso, se establece en cero, lo que significa que se enviarán reintentos continuamente hasta que se detenga el ataque.
- "-a [MAC AP]" especifica la dirección MAC del punto de acceso (AP) de la red objetivo.
- "-h [MAC víctima]" indica la dirección MAC de la víctima que se desea des autenticar.
- "wlan0mon" es la interfaz de red inalámbrica en modo de monitorización que se utilizará para llevar a cabo el ataque. Es importante verificar que esta interfaz esté en modo de monitorización antes de ejecutar el comando.

Figura 24

Ataque de des autenticación lanzado con la herramienta aireplay-ng



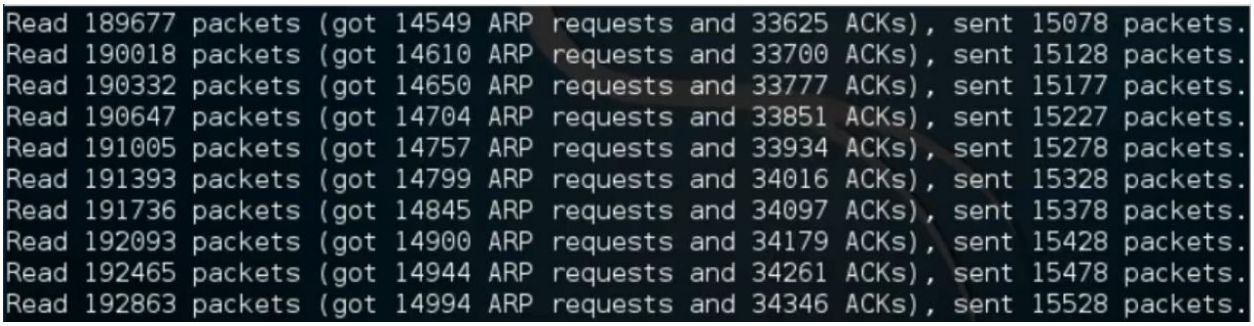
A continuación, con el comando aireplay-ng -3 -b [MAC AP] -h [MAC víctima] wlan0mon. Aireplay-ng intentará capturar y reinyectar paquetes en la red objetivo.

- "-3" indica que se va a utilizar el método de ataque de reinyección de tráfico.

- "-b [MAC AP]" especifica la dirección MAC del punto de acceso (AP) de la red objetivo.
- "-h [MAC víctima]" indica la dirección MAC de la víctima cuyo tráfico se desea reinyectar.

Figura 25

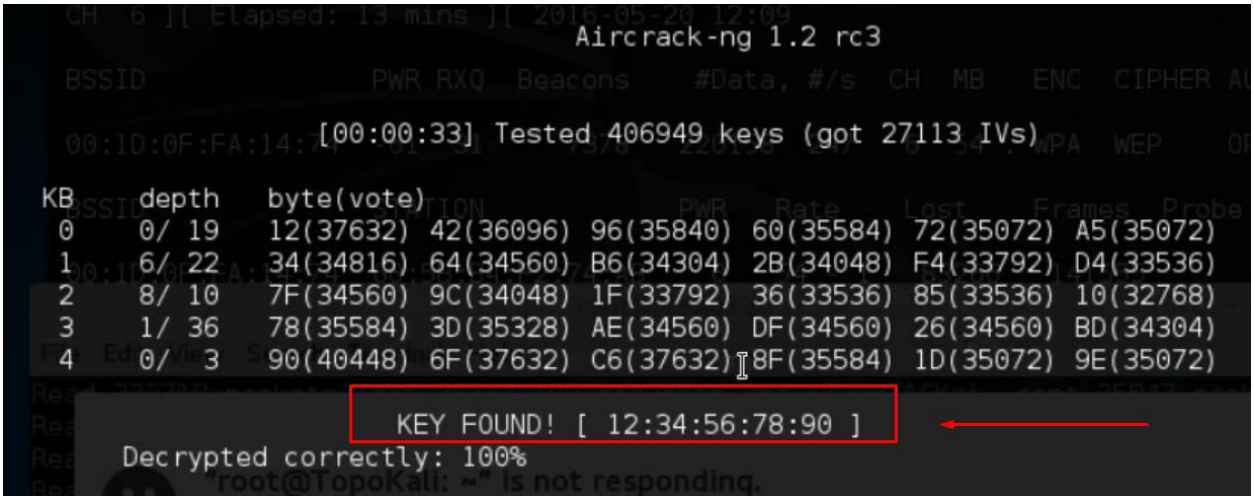
Ataque de reinyección de tráfico lanzado con la herramienta aireplay-ng



Una vez se tenga una cantidad considerable de respuestas de paquetes ARP, procedemos a buscar el archivo donde se guardó el registro de la data. Con el comando aircrack-ng [nombre del archivo.cap], aircrack-ng intentará descifrar la clave de seguridad de la red inalámbrica utilizando técnicas de fuerza bruta o ataques basados en diccionario. Analizará el archivo de captura en busca del handshake de autenticación, que es una parte importante del proceso de autenticación entre un dispositivo cliente y el punto de acceso (AP) de la red. Es importante tener en cuenta que el éxito del crackeo de la clave dependerá de diversos factores, como la fortaleza de la clave, la calidad del handshake capturado y los recursos computacionales disponibles.

Figura 26

Clave encontrada con la herramienta Aircrack-ng



Cuando finalice este proceso, el programa nos mostrará la clave, como se puede observar son los 10 dígitos introducidos inicialmente en el Access Point de prueba, el programa nos muestra estos dígitos en formato hexadecimal.

OWISAM-TR-003: Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).

Planificación:

La información se recopilará sobre la red inalámbrica objetivo, que en este caso se encuentra en un entorno controlado.

Recopilación de información:

El nombre de la red (SSID), la dirección MAC, la configuración de seguridad y otros detalles relevantes serán recopilados. Esto se puede lograr mediante el uso de la herramienta de escaneo de redes inalámbricas con WPS wash.

Recopilación de información:

Encontrar la red objetivo que será auditada es el primer paso para poder auditar cualquier tipo de red inalámbrica. Después de configurar y establecer el entorno, podemos comenzar el ataque, para lo cual primero necesitamos realizar un escaneo. Esta es la etapa inicial de cualquier tipo de pentesting. Se debe obtener la máxima información posible para usar todo lo obtenido en las siguientes etapas del ataque. El éxito o el fracaso de un ataque a una red inalámbrica depende de esta información.

En esta primera etapa vamos a obtener la mayor cantidad de información sobre los puntos de acceso y los dispositivos que están conectados a ellos. Por lo que debemos poder obtener por lo mínimo la siguiente información para continuar con el ataque:

- Lista de puntos de acceso que se encuentran a nuestro alcance
- Direcciones MAC tanto de los clientes como de los puntos de acceso.
- El canal de operación de las redes
- El tipo de autenticación implementado
- Niveles de la intensidad de las señales Wi-Fi

En este caso se utilizará la herramienta “wash” la cual viene con Reaver que es un que se utiliza para escanear redes inalámbricas y determinar si está habilitado el modo de configuración WPS.

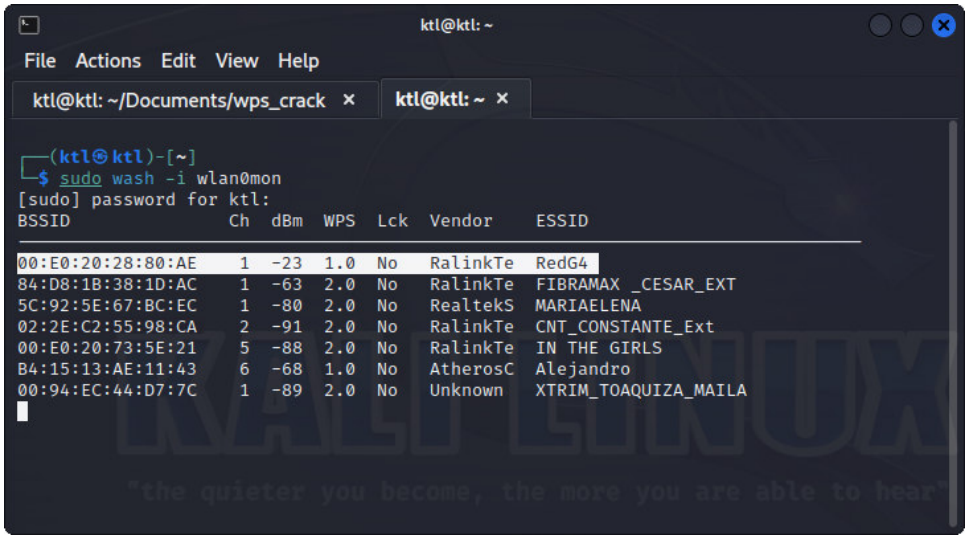
Identificación de dispositivos:

Para realizar este paso debemos poner la tarjeta inalámbrica en modo de monitoreo. Una vez que la interfaz esté en modo monitor, ejecutamos la herramienta “wash”. Wash comenzará a escanear las redes inalámbricas cercanas y mostrará los datos de si tienen habilitado el modo de configuración WPS.

Si la columna "Lck" muestra “No” o está vacía, significa que la red está habilitada para WPS y puede ser susceptible a los ataques. Si la columna “Lck” muestra "Sí", significa que la red tiene WPS habilitado, pero se encuentra bloqueado, lo que significa que los ataques de fuerza bruta al PIN de WPS no son posibles. La salida del comando podemos ver en la figura **27** donde se puede ver que nuestra red de prueba está configurada con WPS.

Figura 27

Salida del comando wash con escaneo de redes con WPS

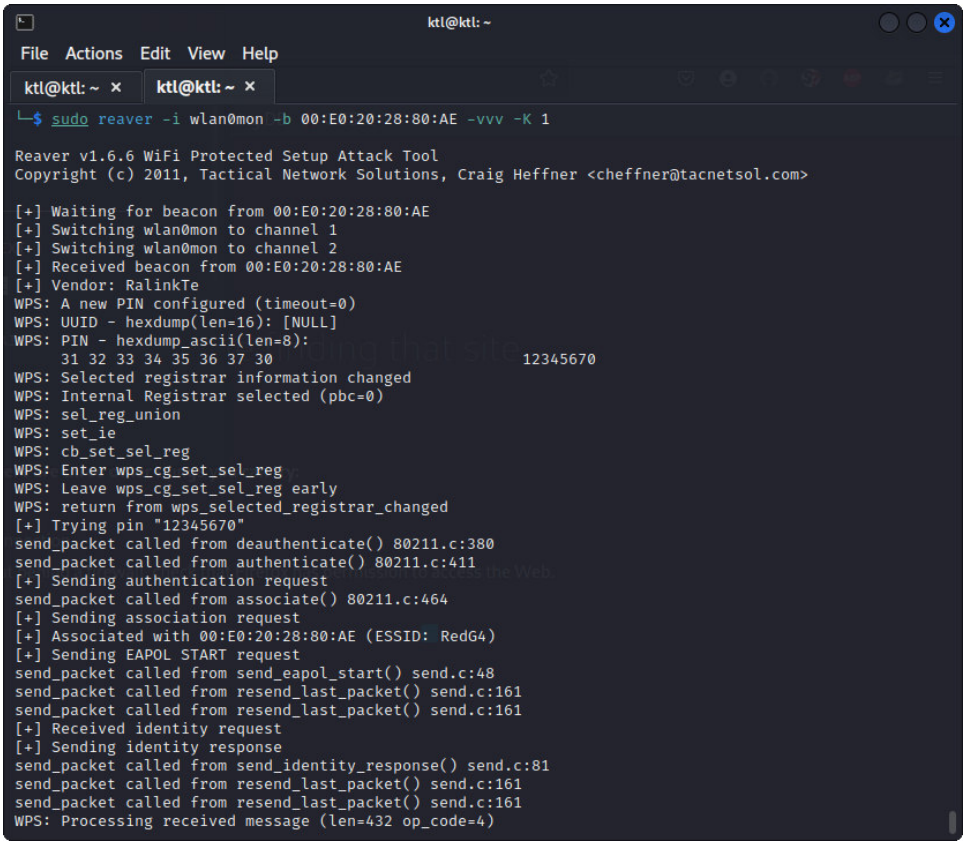


Ataques:

Una vez que se han encontrado las redes que tienen activada esta configuración que para nuestro caso es la red “RedG4” procedemos con el ataque utilizando la herramienta Reaver para obtener el PIN WPS. Para esto ejecutamos el comando como se indica en la figura 28.

Figura 28

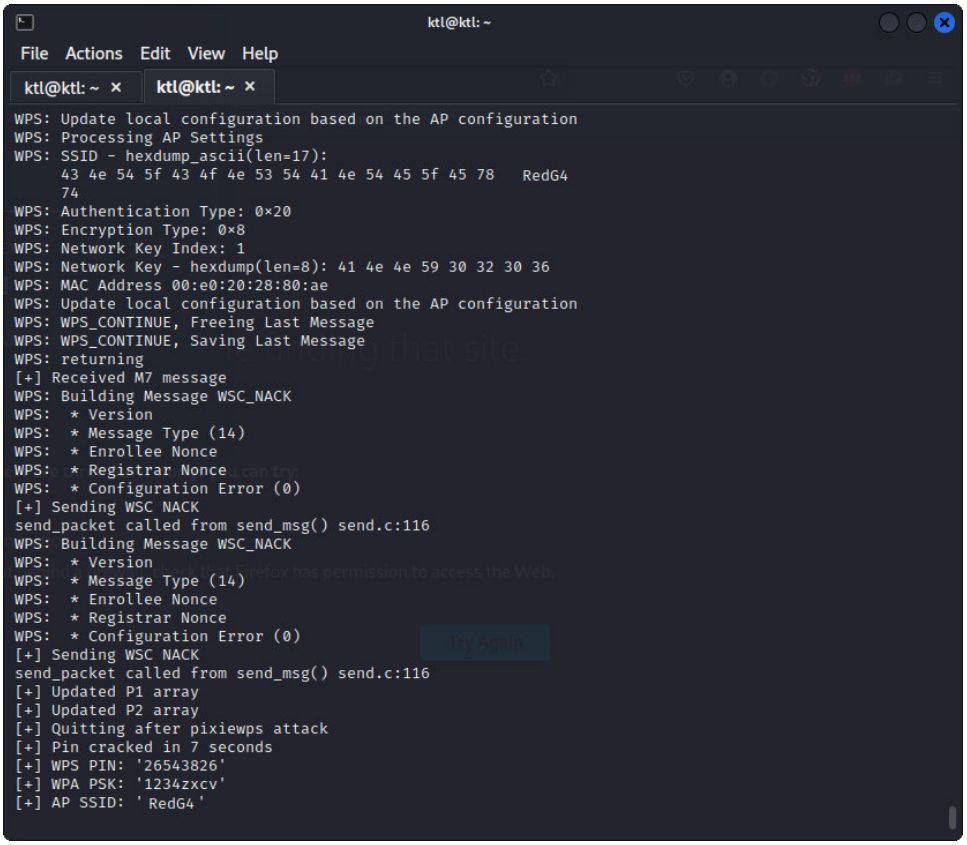
Comando para Realizar Ataque Usando Reaver



Reaver intentará usar ataques con fuerza bruta para obtener el PIN WPS de la red objetivo y dependiendo de la complejidad del PIN, puede llevar algún tiempo. Reaver mostrará la pantalla como se indica en la figura 29 una vez que obtenga el PIN WPS. El PIN se utilizará para autenticarse y obtener acceso a la red vulnerando totalmente la seguridad de esta.

Figura 29

Captura de PIN WPS y Contraseña Obtenida con Reaver



OWISAM-TR-004: Clave WEP/WPA/WPA2 basada en diccionario.

Planificación:

Se obtendrá la información sobre la red inalámbrica objetivo que en este caso está en un ambiente controlado. Los datos que recopilaremos son el nombre de la red (SSID), la dirección MAC, la configuración de seguridad y otros detalles relevantes. Esto se puede lograr utilizando herramientas de escaneo de redes inalámbricas como Kismet o airodump-ng.

Recopilación de información:

De la misma manera que para OWISAM-TR-003 se aplican lo mismo para este caso a excepción de que se usará la herramienta airodump-ng para recopilar toda esta información, pero existen numerosas herramientas que pueden realizar descubrimientos de redes inalámbricas como Kismet o Meraki WiFi Stumbler. Una vez capturada la información se puede analizar manualmente los paquetes y obtener las redes cercanas y los clientes que se encuentran conectados e incluso los datos que fueron enviados.

Identificación de dispositivos:

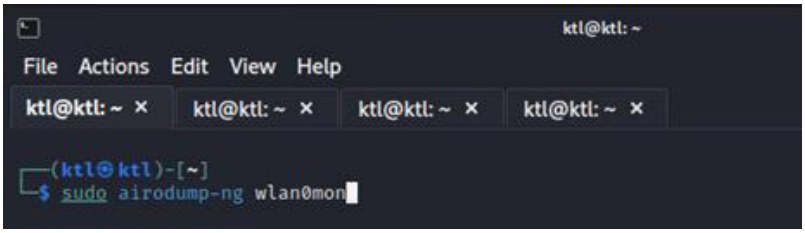
Para empezar, examinaremos el protocolo WEP**.** Existe una amplia gama de herramientas disponibles para realizar ataques al protocolo WEP que pueden usarse. Aircrack-ng, que se utilizará en estas pruebas, es una suite completa que permite el análisis de paquetes de redes.

La herramienta airodump-ng, que forma parte de la suite Aircrack-ng, se utiliza para llevar a cabo el escaneo inalámbrico. Según la página oficial de Aircrack-ng (s.f.) la herramienta airodump-ng es especialmente adecuada para recopilar IVs WEP (Vectores de Inicialización) o handshakes WPA/WPA2 con la intención de utilizarlos con aircrack-ng. Airodump-ng se utiliza para la captura de paquetes, capturando tramas 802.11 sin procesar.

Para utilizar esta herramienta usaremos el sistema operativo Kali Linux, ya que dentro de esta distribución que es utilizada para la seguridad informática ya viene instalado esta suite. Ejecutamos el comando “sudo airodump-ng wlan0mon” que se muestra en la figura 30.

Figura 30

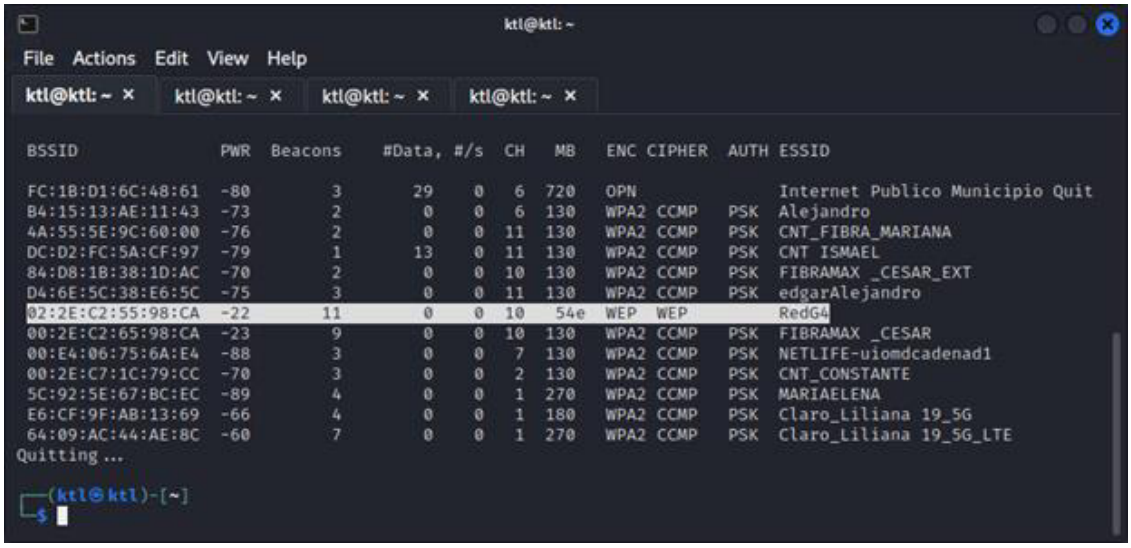
Comando Airodump-ng



La figura 31 muestra los resultados que obtuvimos al ejecutar el comando anterior. Se puede ver en la sección ESSID la red que hemos configurado en nuestro entorno con el nombre de RedG4, para llevar a cabo nuestra auditoria.

Figura 31

Salida de Comando Airodump-ng



Como se puede ver en la figura nos muestra varias columnas que detallamos a continuación:

- BSSID: Corresponde a la dirección física (MAC) del punto de acceso

- PWR: Nivel de potencia de la señal
- Beacons: Numero de tramas enviadas
- #Data: Numero de paquetes capturados
- CH: Canal del punto de acceso
- MB: Máxima velocidad de comunicación
- ENC: Protocolo de encriptación usado.
- CIPHER: Tipo de cifrado
- AUTH: Protocolo de autenticación usado
- ESSID: Nombre de la red

Una vez que se ha obtenido la información necesaria de la red objetivo se procede con la siguiente fase que es el ataque a la red objetivo RedG4.

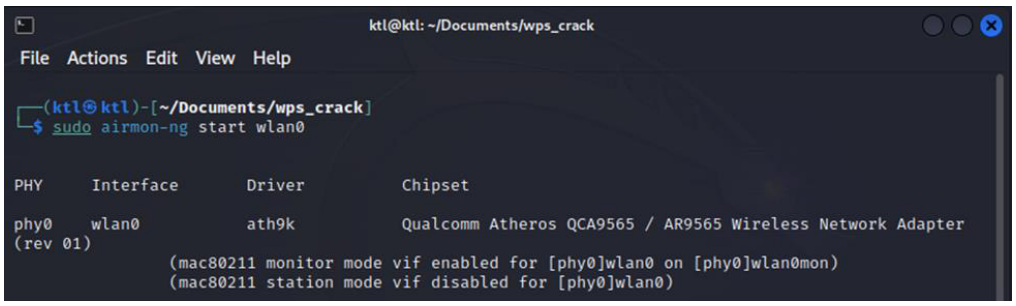
Ataques:

Ataque al protocolo WEP:

Procedemos a configurar en modo monitor nuestra interfaz inalámbrica con el comando que se indica en la figura 32.

Figura 32

Inicio de modo monitor con airmon-ng



Una vez ejecutado el comando anterior sin ningún tipo de error se procede utilizar la herramienta airodump-ng. Como se puede observar en la figura 33.

Figura 33

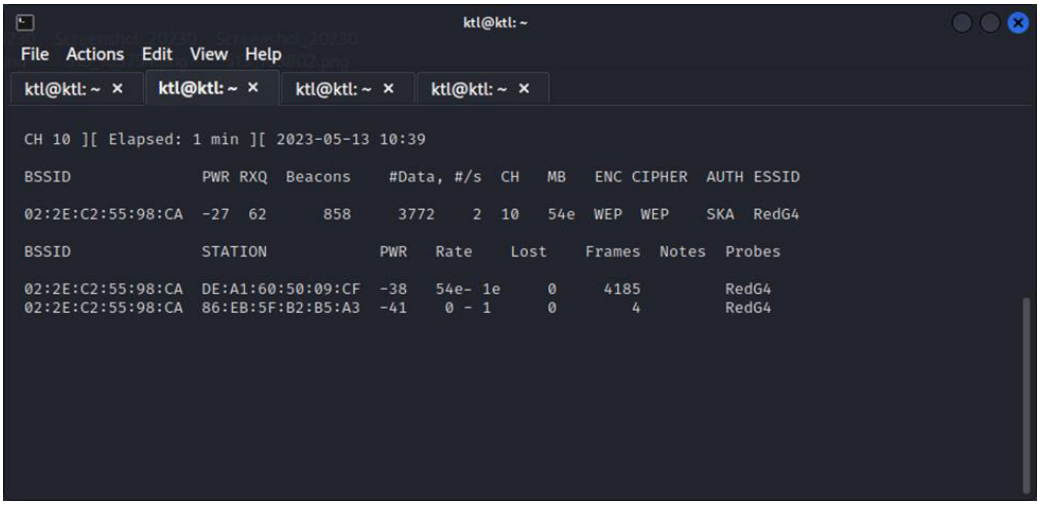
Ejecución de comando airodump-ng

A esta herramienta se le debe pasar los siguientes argumentos como:

- El canal de operación del AP víctima.
- La dirección física del Access Point.
- El argumento --write escribe en un archivo. pcap los datos capturados con el nombre que se le indique.
- El nombre de la interfaz inalámbrica que se utilizara.

Figura 34

Salida de comando airodump-ng

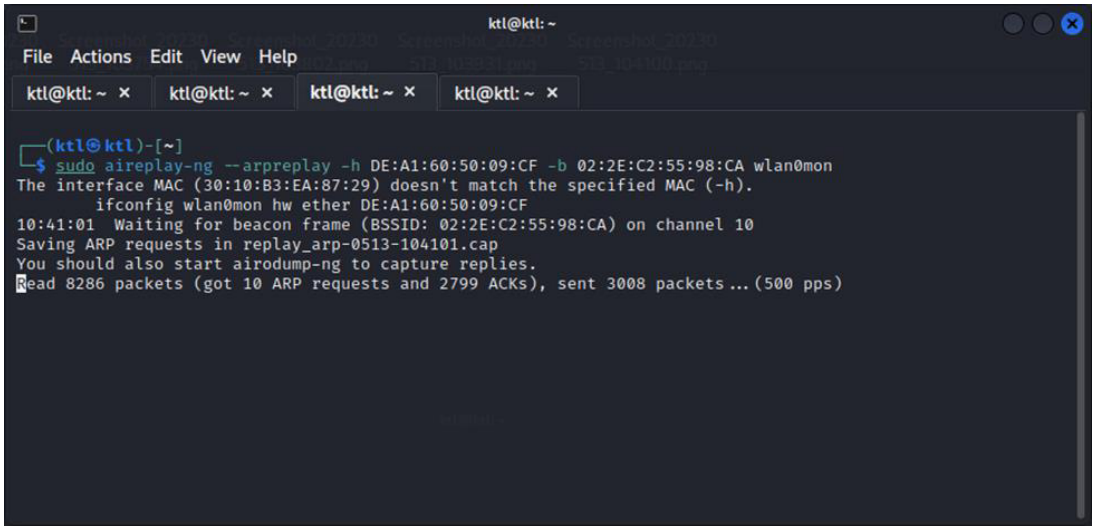


En la figura 34 podemos observar que existe un cliente conectado a nuestra red objetivo. A continuación, se usa la herramienta aireplay-ng que la utilizamos para inyectar tramas al punto de acceso y poder generar más tráfico. Para usar esta herramienta le debemos pasar los siguientes argumentos:

- El tipo de ataque que se va a realizar
- La dirección física de un cliente conectado
- La dirección física del Access Point
- La interfaz inalámbrica

Figura 35

Ejecución de comando aireplay-ng

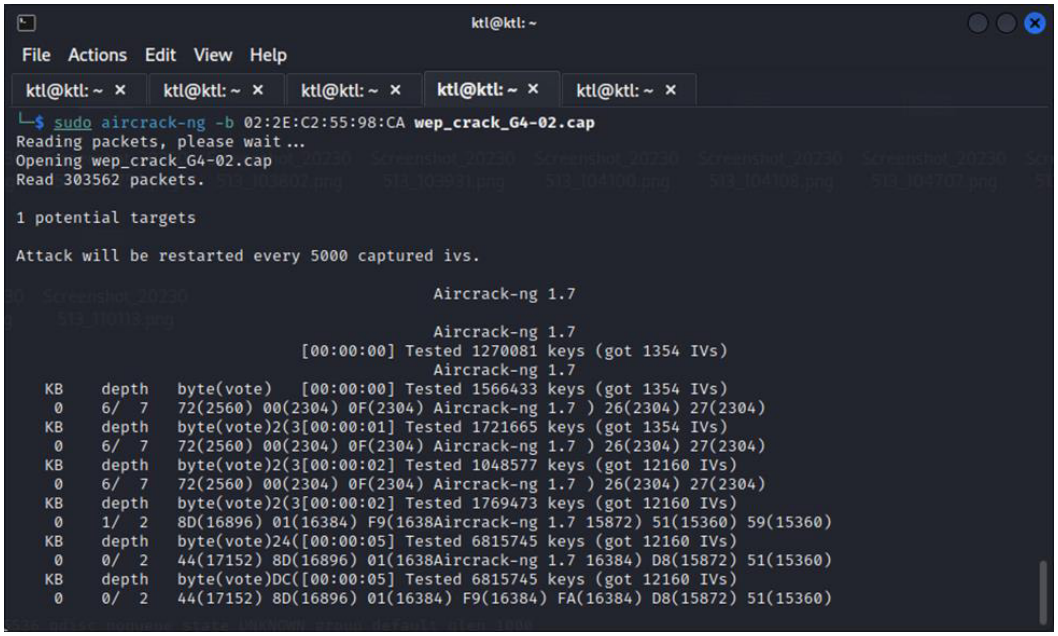


Una vez que hemos capturado el suficiente número de paquetes, se procede a tratar de romper la clave que está utilizando el protocolo WEP. Para este caso se utiliza la herramienta aircrack-ng.

Para comenzar el ataque procedemos a abrir una nueva terminal sin cerrar las que actualmente se están ejecutando y lanzamos el comando que observamos en la figura. A este comando se le pasa como argumentos la dirección física del punto de acceso y el nombre del archivo donde se están almacenando los paquetes.

Figura 36

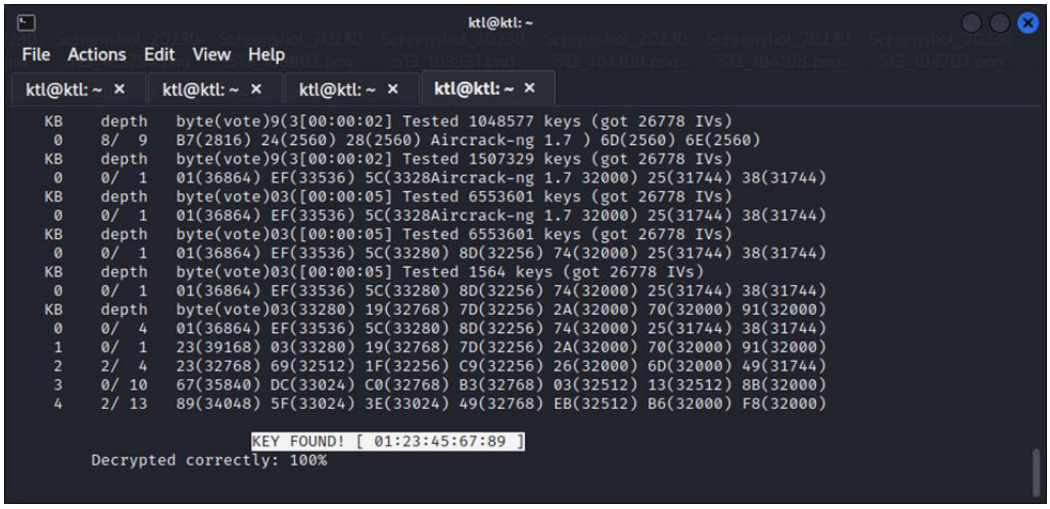
Ejecución del comando aircrack-ng



Para tener éxito en el ataque aircrack-ng se necesita obtener un número suficiente de IVs, por lo que si no se tiene éxito a la primera debemos esperar a recolectar más paquetes y volver a intentarlo. Después de realizar este proceso la herramienta nos indica que la contraseña fue obtenida con éxito y nos muestra en el apartado “KEY FOUND” como podemos observar en la figura 37.

Figura 37

Contraseña obtenida por la herramienta aicrack-ng

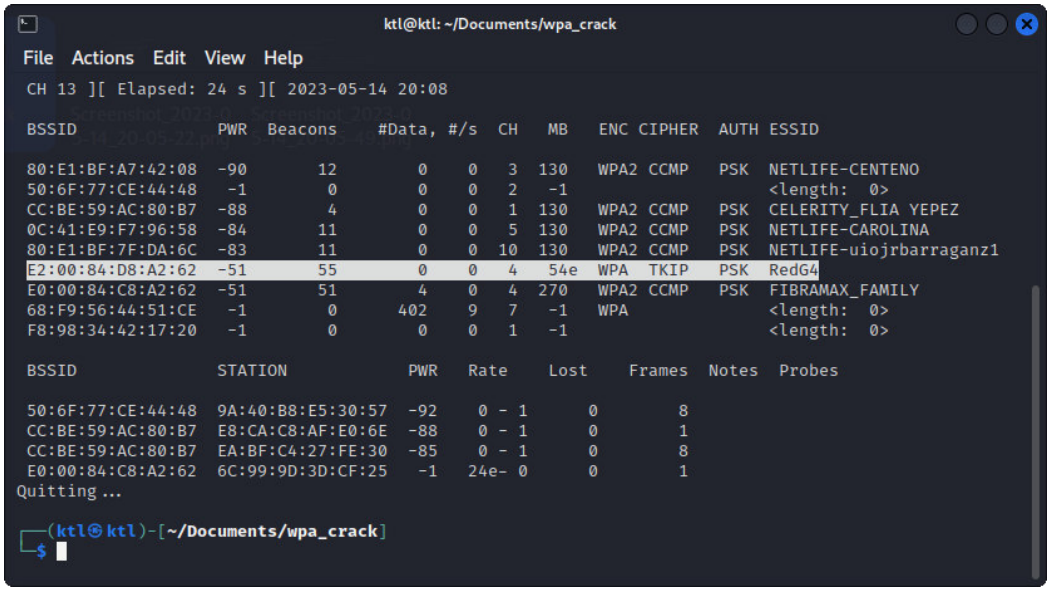


Ataque al protocolo WPA/WPA2:

De la misma manera que para WEP se procede a recopilar información de la red objetivo para lo que ejecutamos el comando “sudo airodump-ng wlan0mon” y verificamos que ahora nuestro SSID ahora está configurada con el protocolo WPA que se muestra en la figura 38**.**

Figura 38

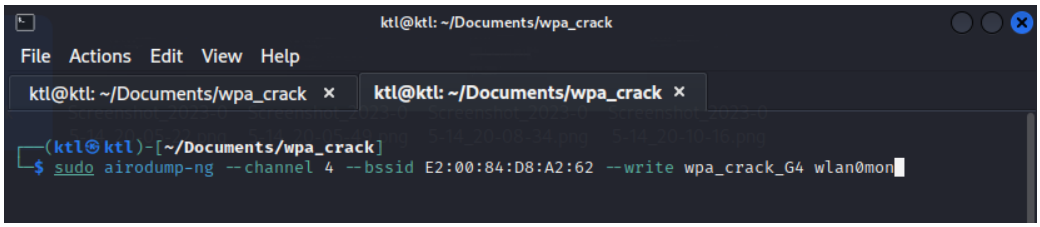
Salida del comando airodump-ng



A continuación, volvemos a utilizar la herramienta airodump-ng para la captura de tráfico con el comando que se indica en la figura 39. La herramienta de captura de paquetes monitorea el tráfico hasta que se autentique un cliente. En esta etapa, es posible que deba esperar hasta que algún cliente se conecte o realizar cualquier otra acción que inicie el proceso de autenticación.

Figura 39

Ejecución del comando airodump-ng

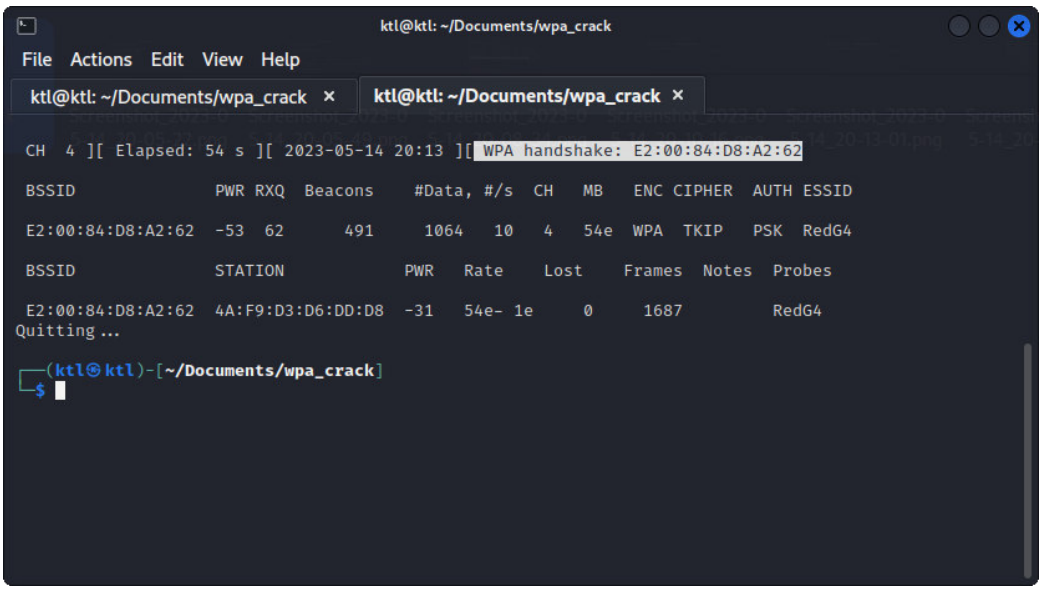


Aguirre (2019) indica que en la primera línea de salida de airodump-ng muestra el handshake WPA que se produce cuando un cliente se autentica con el AP, y airodump-ng almacena el handshake capturado en el archivo wpa_crack_G4.

Cuando el dispositivo cliente intenta autenticarse en la red inalámbrica, se produce el handshake. El cliente y el punto de acceso intercambian múltiples paquetes durante este proceso. Estos paquetes se registrarán con la herramienta airodump-ng y, una vez que se capturen todos los paquetes necesarios, se guardará en el archivo de salida especificado anteriormente. En la figura 40 se puede observar la captura del handshake.

Figura 40

Captura de handshake con la herramienta airodump-ng



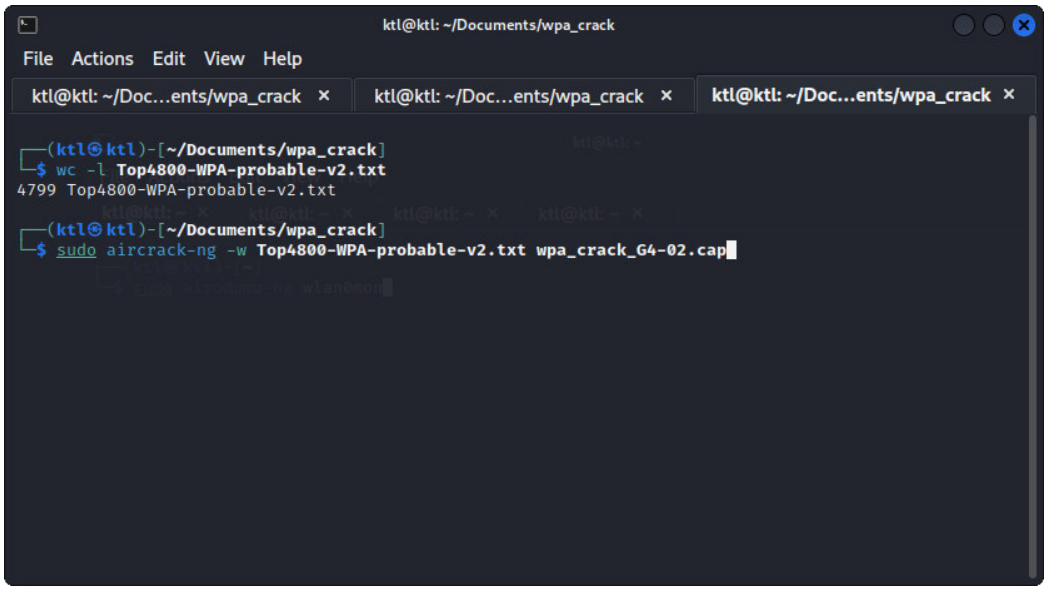
Puede detener la herramienta de captura de paquetes después de capturar el handshake y comenzar a realizar el ataque de diccionario para descifrar la clave WPA con el archivo de salida y la herramienta Aircrack-ng.

Antes de ejecutar el ataque, se debe obtener un diccionario de contraseñas para probar varias combinaciones de palabras y contraseñas. Se puede utilizar diccionarios preexistentes que contengan una lista de palabras comunes, contraseñas filtradas, combinaciones particulares, o puede crear su propio diccionario. Para este caso se utilizará un diccionario disponible en github: "https://github.com/berzerk0/Probable-Wordlists/blob/master/Real-Passwords/WPA-Length/Top4800-WPA-probable-v2.txt".

Ahora se debe ejecutar Aircrack-ng con los parámetros adecuados para iniciar el ataque como se indica en la figura 41. En donde el parámetro -w: Especifica la ruta al diccionario de contraseñas. El parámetro -b: Indica el BSSID (dirección MAC del punto de acceso) del objetivo. Y wpa_crack_G4-02.cap es el archivo de captura de paquetes de handshake obtenido anteriormente.

Figura 41

Ejecución de comando aircrack para ataque con diccionario

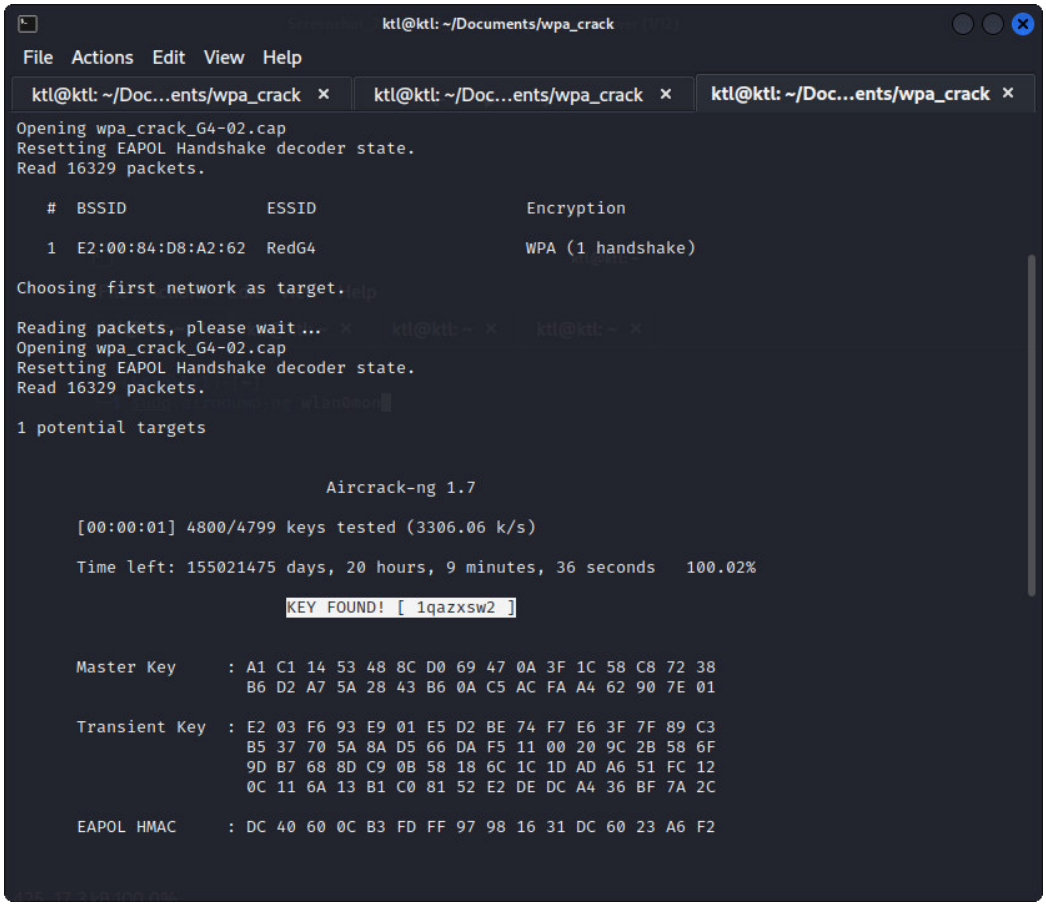


Aircrack-ng comenzará a probar las contraseñas del diccionario una por una en el archivo "wpa_crack_G4-02.cap" al ejecutar el comando. El programa mostrará los intentos realizados en tiempo real.

Dado que depende del tamaño y la complejidad del diccionario, así como del rendimiento del sistema, un ataque al diccionario puede llevar tiempo. Hasta que se encuentre una coincidencia exitosa en el archivo de captura de paquetes, aircrack-ng continuará probando contraseñas. La salida del programa mostrará como se indica en la figura 42 si se encuentra la clave correcta.

Figura 42

Obtención de contraseña por ataque a diccionario con aircrack-ng



Se debe seguir el mismo proceso para atacar el protocolo WPA2.

OWISAM-TR-005: Mecanismos de autenticación inseguros (LEAP, PEAP-MD5,)

Un problema del protocolo LEAP es que al momento de realizar la trama/handshake/comunicación entre cliente y servidor, la información no es cifrada enteramente por lo que con el uso/captura de las tramas mediante el uso como de wireshark se puede visualizar el nombre del usuario como veremos en el ejemplo:

Para realizar se deberá configurar un servicio de serverRadius, que servirá para realizar la autenticación/comparación entre las tablas de usuario/claves provistas por el cliente y aquellas guardadas en el servidor.

Figura 43

Diagrama de comunicación entre usuarios con servidor Radius/kerberos para autenticación.

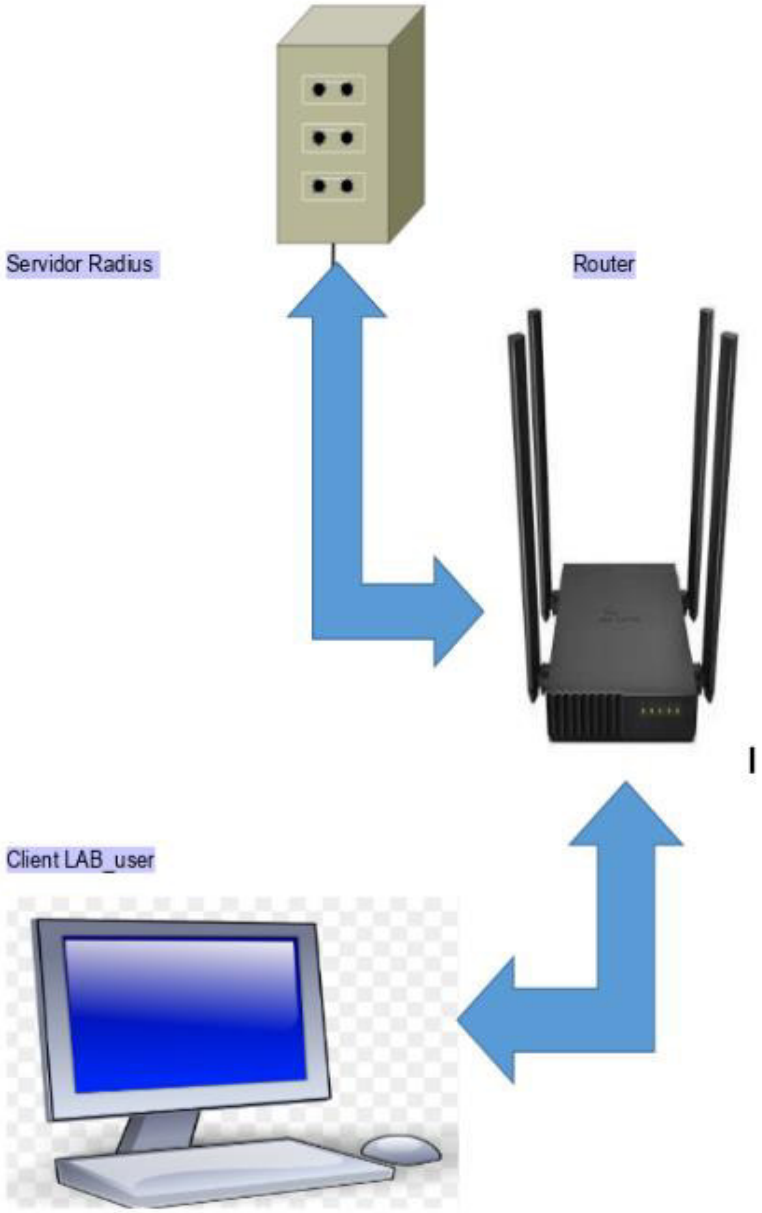


Figura 44

Configuración de usuarios dentro de la lista de usuarios en servidor de autenticación (usuario Grupo4).

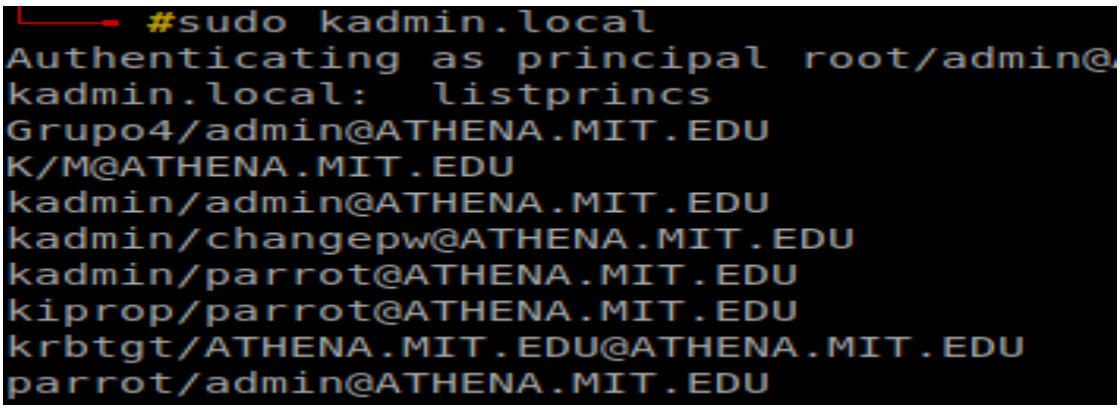
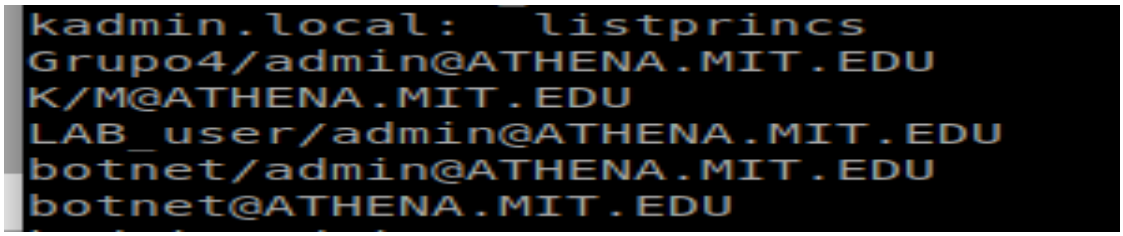


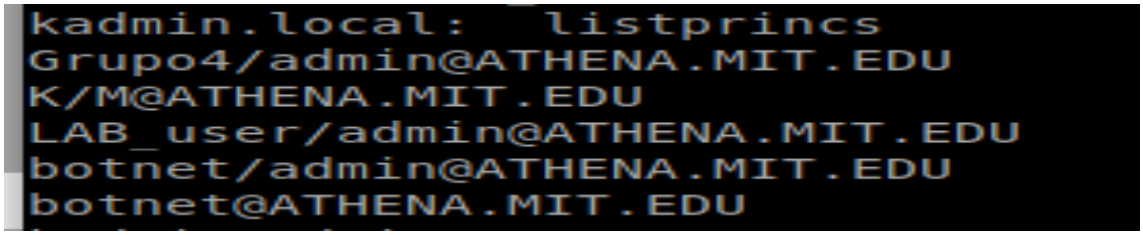
Figura 45



Nota. Configuración de usuarios dentro de la lista de usuarios en servidor de autenticación (usuario LAB_user).

Figura 46

Configuración de usuarios dentro de la lista de usuarios en servidor de autenticación.



Posterior configuramos la red a la cual deberemos acceder en donde deberemos ingresar usuario y clave para poder ser autenticados.

Figura 47

Modificación de base de datos/usuario clave.

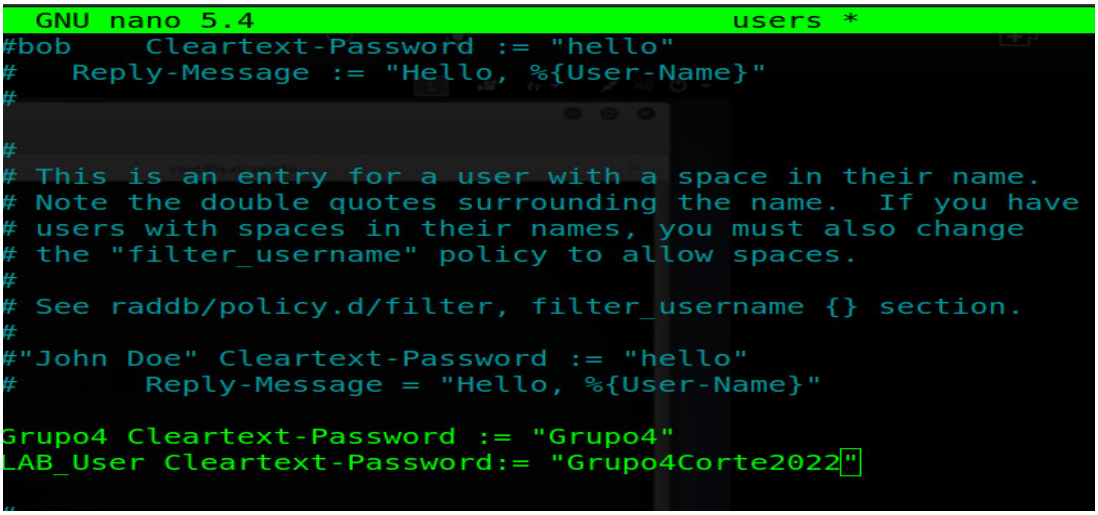


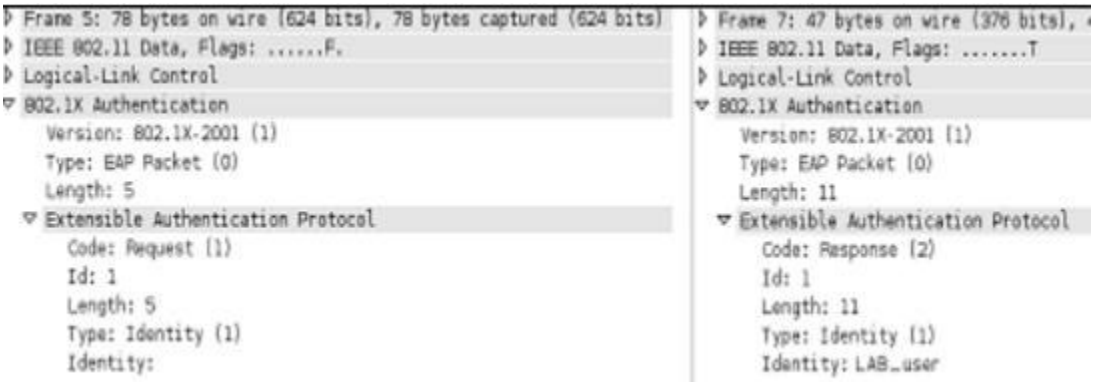
Figura 48

Configuración de red para acceso de usuario.

Antes de empezar la conexión abrimos la aplicación Wireshark en modo monitor, y empezamos a buscar la red, para poder ingresar y el tráfico/tramas empezaran a mostrarse dentro de los paquetes, en el cual nuestros intereses serán aquellos que contengan el protocolo EAP, y como podremos ver sin necesidad de ningún otro paso más que revisar la trama podremos visualizar el nombre del usuario.

Figura 49

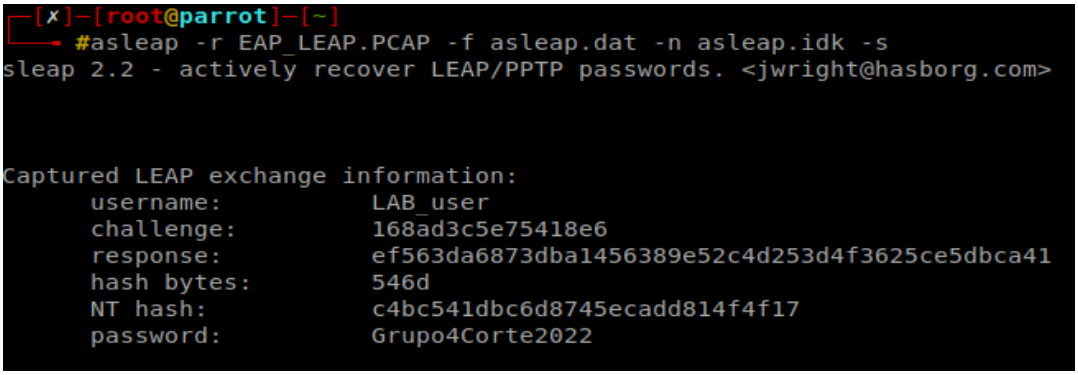
Porción de paquete Wireshark con nombre de usuario en cleartext.



De la misma manera una vez capturado el hash procedemos a intentar descifrar la clave del usuario, por lo que usamos asleap como base de ataque, y como resultado recibimos la clave de acceso de log in.

Figura 50

Cifrado de clave descubierta.



OWISAM-TR-006: Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).

Como es de común conocimiento mientras más fuerte es una clave toma más tiempo y recursos computacionales para romperla, y para que la clave sea eficiente deberá contener aparte de al menos 14 caracteres, números, letras mayúsculas y minúsculas juntamente con caracteres especiales.

WPS no permite más que el uso de números, con un máximo de (8-10) caracteres lo que hace muy fácil el poder vulnerarlo, sin importar si este número es aleatorio (creado por el servidor o cliente) los parámetros/complejidad serán los mismos, por lo que no será particularmente difícil que mediante un ataque obtener la clave de conexión. (Horowitz, 2021).

Como vimos en el apartado 3 (en el cual se logró vulnerar WPS) a continuación se intentó realizar el mismo proceso, pero esta vez con la opción de WiFi protected y los resultados después de varios intentos y técnicas, nos dio como negativo usando un router Tp-lin Archer c64, el cual previamente fue actualizado el firmware hasta la última versión (1.12.10 Build 230208 Rel.38878n (5553), este router también tiene habilitada WPA3.

Figura 51

Configuración de Router WPS.

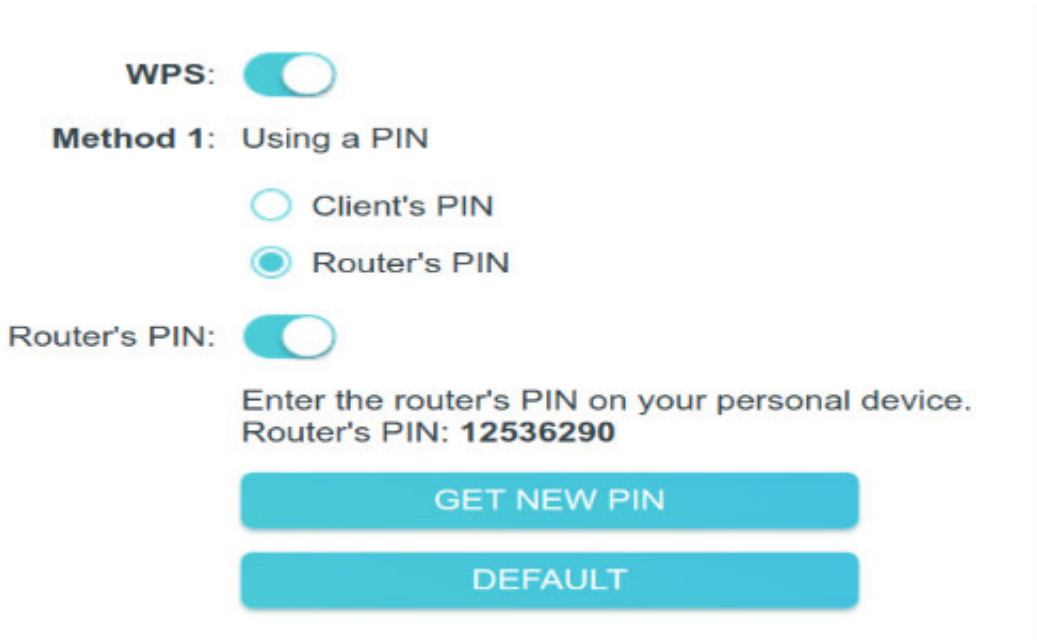


Figura 52

Configuración de Router WPS

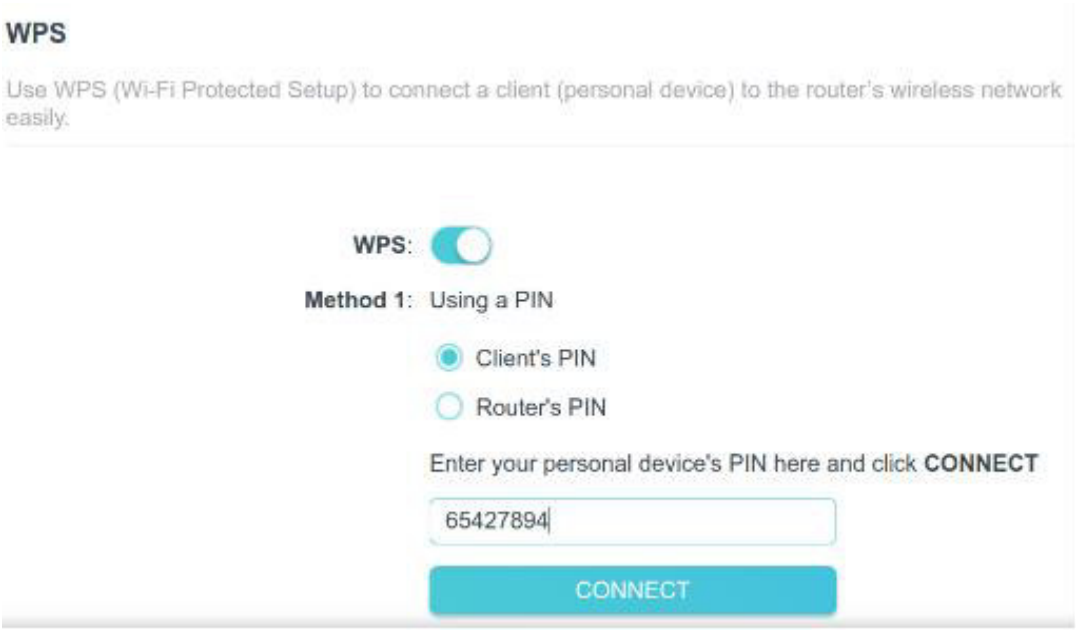


Figura 53

Escaneo de Routers con WPS activada.

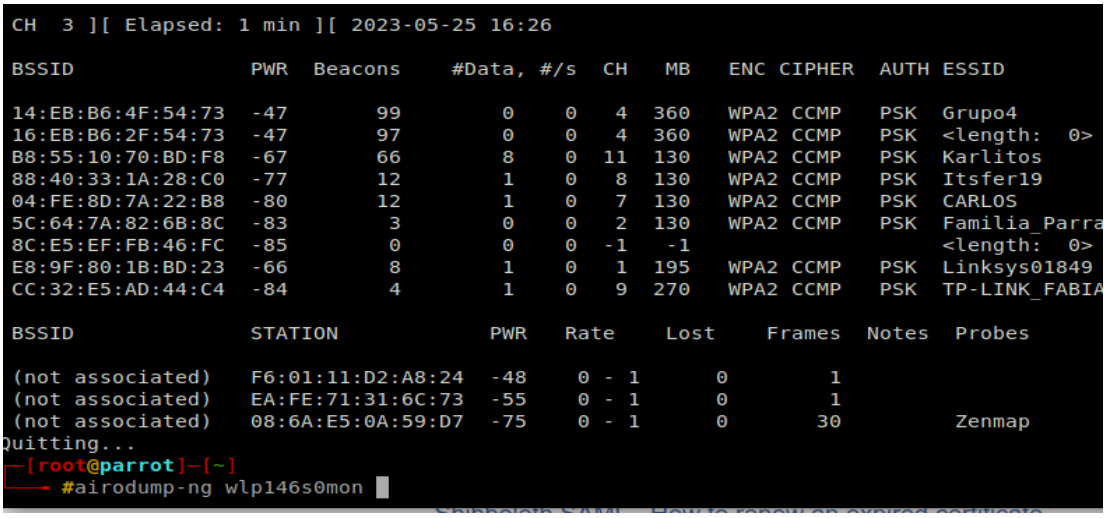


Figura 54

Pantalla de intento de fuerza bruta a WPS numero PIN.

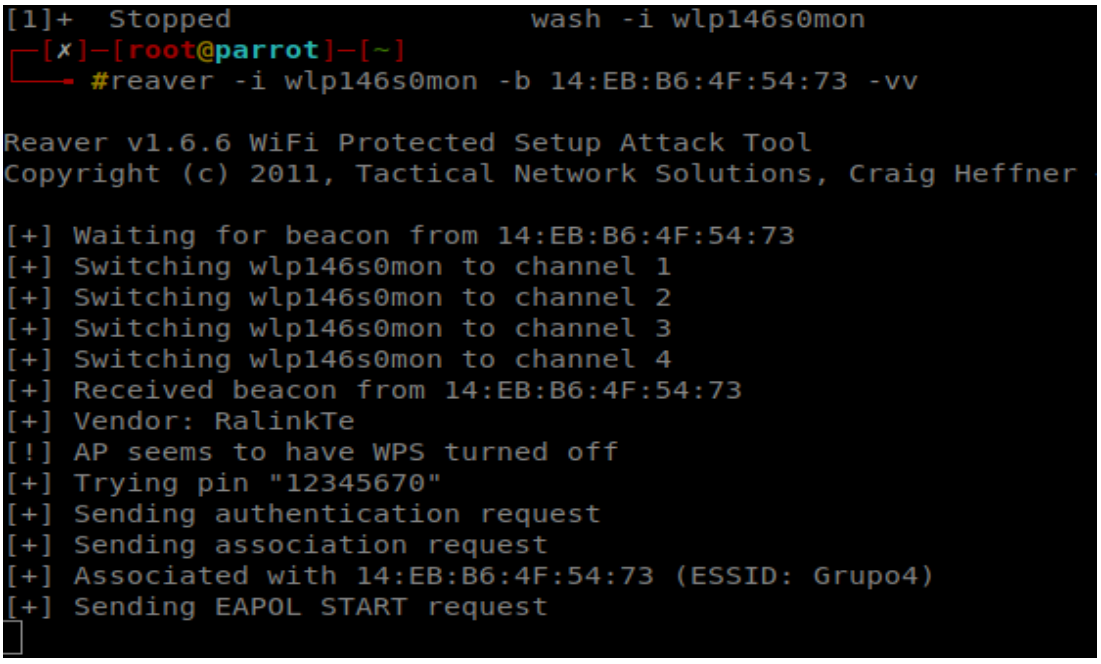
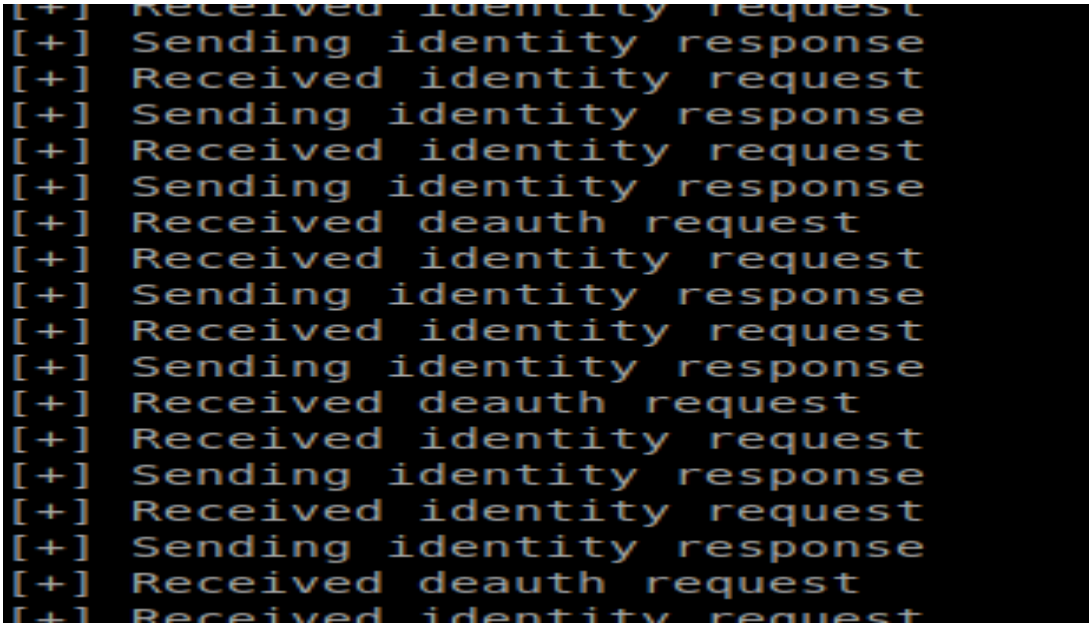


Figura 55

Pantalla de respuesta/pedido de intento de fuerza bruta a WPS numero PIN.



Como podemos observar después de determinados intentos de (9-15 identity request) por parte del cliente, el router envía un paquete (des autenticación) similar a un timeout, si ocurren 10 timeouts seguidos el router simplemente para el (broadcasting) y apaga/deshabilita WPS.

Figura 56

Pantalla de respuesta/pedido de intento de fuerza bruta a WPS numero PIN.

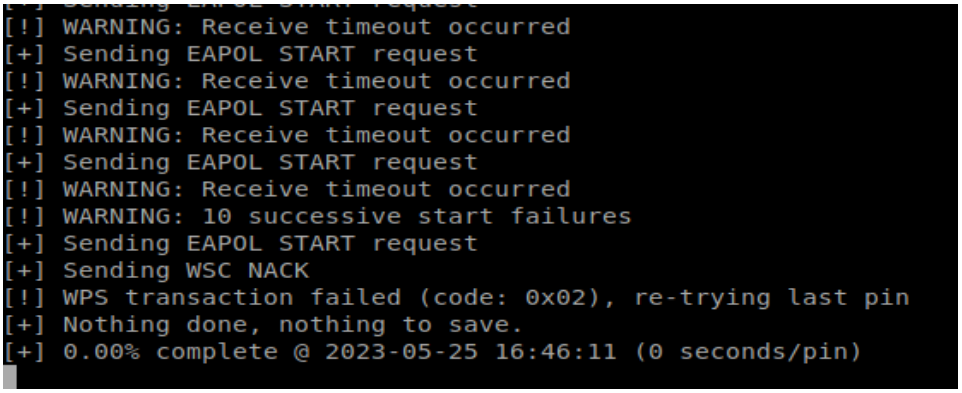
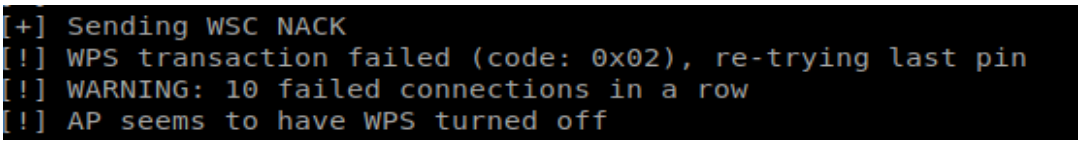


Figura 57

Pantalla de respuesta/pedido de intento de fuerza bruta a WPS numero PIN.



OWISAM-TR-007: Red Wi-Fi no autorizada por la organización.

Planificación:

Crear 3 ejemplos de redes no autorizadas

- Implementar un AP a través de una computadora por CMD
- Implementar un AP a través de un celular
- Implementar una AP a través de una computadora como un usuario común, y realizar un ataque de MitM para demostrar su vulnerabilidad

Implementar un AP a través de una computadora por CMD

compilación de información:

Se trabaja en un entorno controlado para realizar las pruebas de acceso a la red

Identificación de dispositivos:

Los dispositivos están en un entorno controlado y no necesitan ser identificados

Ataques:

Implementar un AP a través de una computadora por CMD

Pasos:

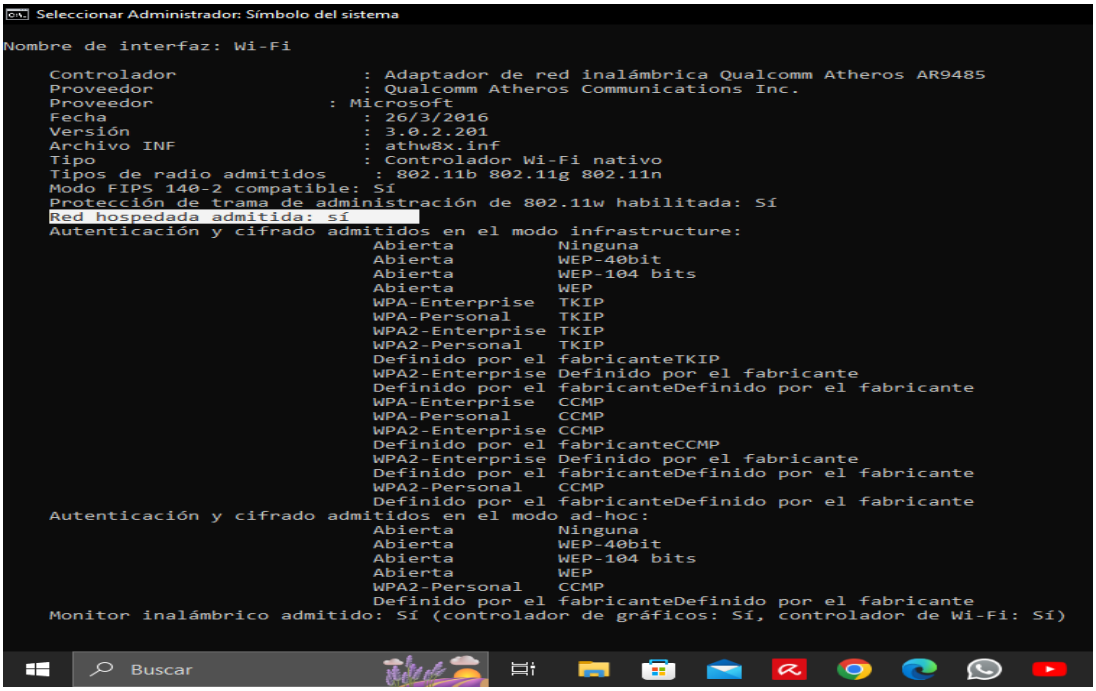
Abrir el símbolo del sistema con permisos de administrador. Para ello, haz clic con el botón derecho del ratón en el menú Inicio de Windows y selecciona "Símbolo del sistema (Admin)" en el menú contextual.

Escribir el siguiente comando para ver si tu adaptador de red admite la creación de un punto de acceso virtual: netsh wlan show drivers

Busca la línea "Hosted network supported" en los resultados. Si esta línea muestra "Si", entonces tu adaptador de red es compatible con la creación de un punto de acceso virtual tal como se muestra en la figura

Figura 58

Propiedades del controlador wifi.

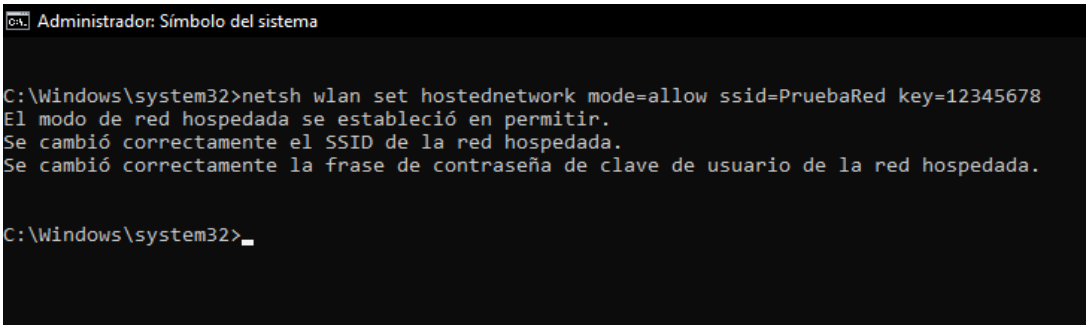


Nota. El controlador wifi corresponde a un laptop Toshiba Satellite C55-B5213K2. Tomado de laptop del autor

Configura tu punto de acceso virtual con el siguiente comando: netsh wlan set hostednetwork mode=allow ssid=PruebaRed key=12345678 tal como se muestra en la figura

Figura 59

Configuración de punto de acceso

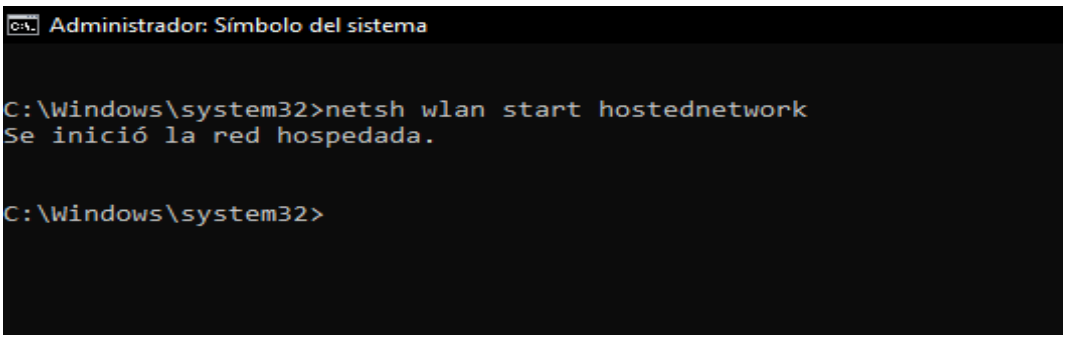


Nota. El controlador wifi corresponde a un laptop Toshiba Satellite C55-B5213K2. Tomado de laptop del autor

Inicia tu punto de acceso virtual con el siguiente comando: netsh wlan start hostednetwork, tal como se muestra en la figura 55.

Figura 60

Inicio de red Hospedada

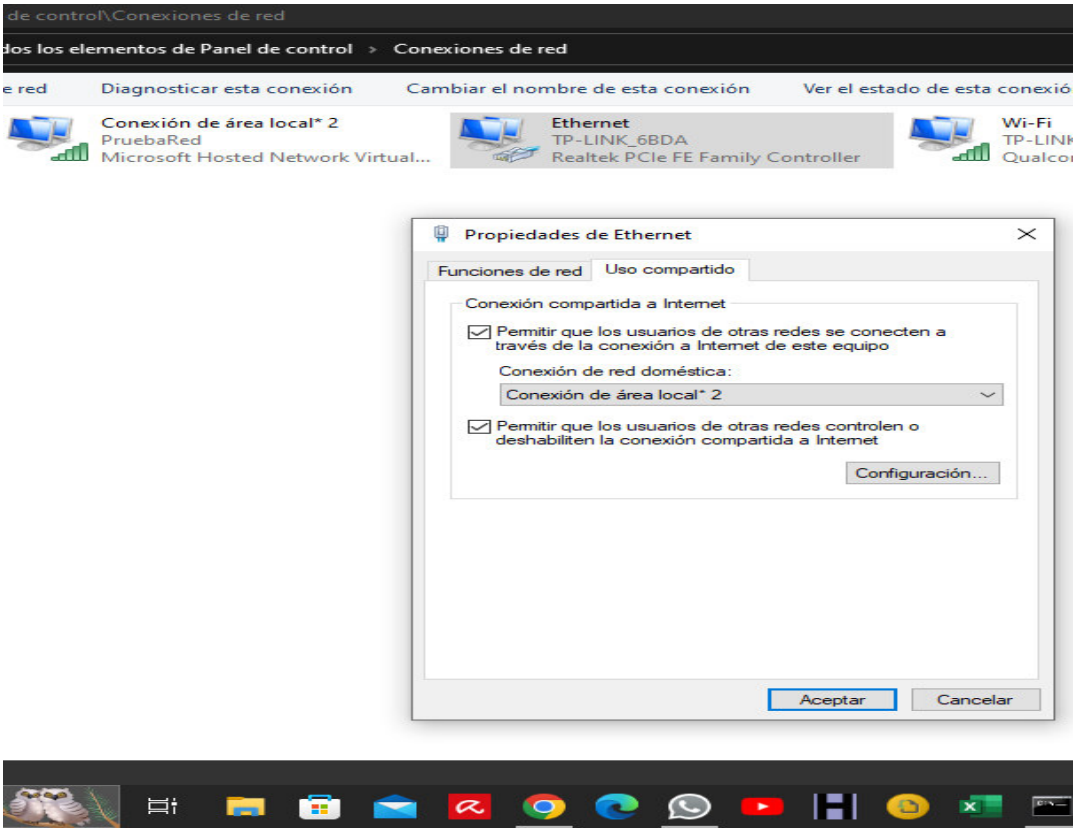


Nota. El controlador wifi corresponde a un laptop Toshiba Satellite C55-B5213K2. Tomado de laptop del autor

Se activa la conexión compartida con el nombre del AP: PruebaRed tal como se muestra en la figura

Figura 61

Activación de la conexión compartida

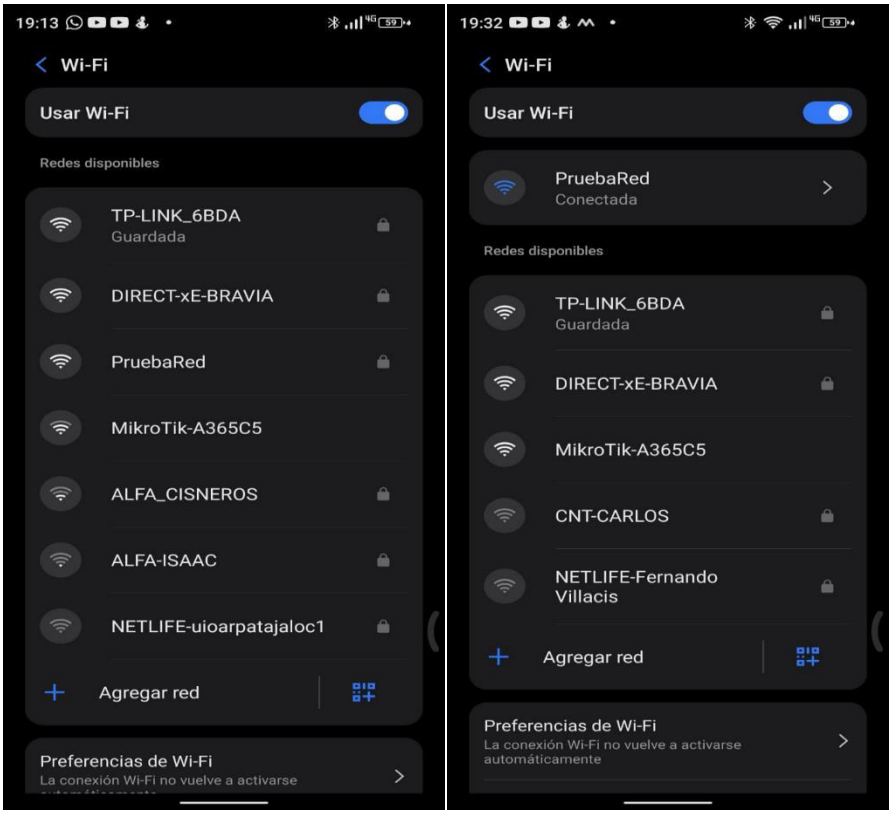


Nota. El controlador wifi corresponde a un laptop Toshiba Satellite C55-B5213K2. Tomado de laptop del autor

Red detectada y con acceso a internet mediante móvil Se activa la conexión compartida con el nombre de AP: PruebaRed tal como se muestra en la figura

Figura 62

Ingreso mediante celular del AP: PruebaRed



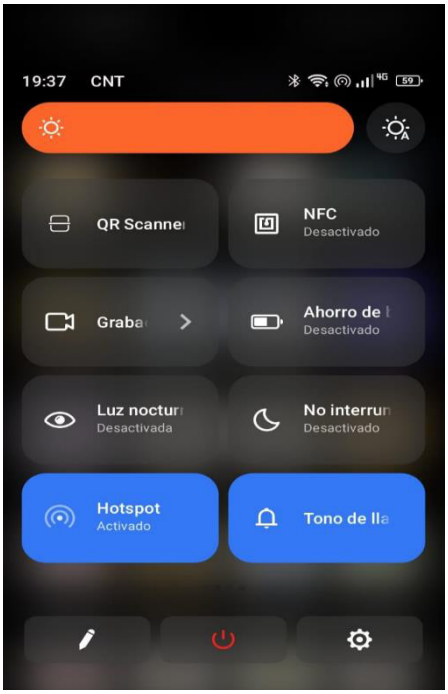
Nota. El celular empleado es un Doogee S98 Pro. Tomado del celular del autor

Implementar un AP a través de un celular

El AP se implementó a través de un celular Doogee S98 Pro con la versión 12 de Android, Deslizar el dedo hacia abajo desde la parte superior de la pantalla, Mantener presionado el ícono de Hotspot, Activa Hotspot de Wi-Fi, tal como se muestra en la figura

Figura 63

Activación de Hotspot

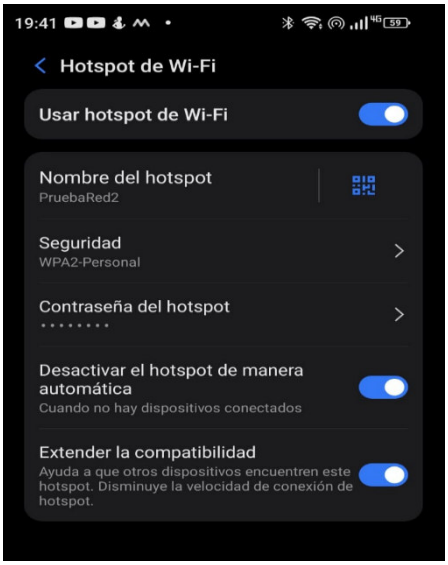


Nota. El celular empleado es un Doogee S98 Pro. Tomado del celular del autor

Configurar el nombre de hotspot que es PruebaRed2, contraseña es 12345678 y el tipo de seguridad WPA2 tal como se muestra en la figura.

Figura 64

Configuración del hotspot

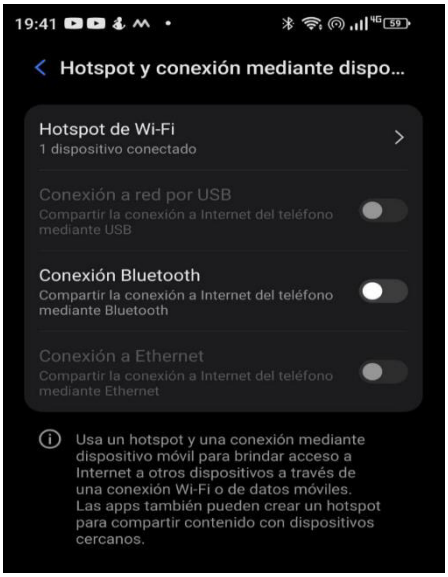


Nota. El celular empleado es un Doogee S98 Pro. Tomado del celular del autor

Ya configurada, ingresamos a través de un dispositivo, tal como se muestra en la figura:

Figura 65

Punto de acceso con un dispositivo conectado



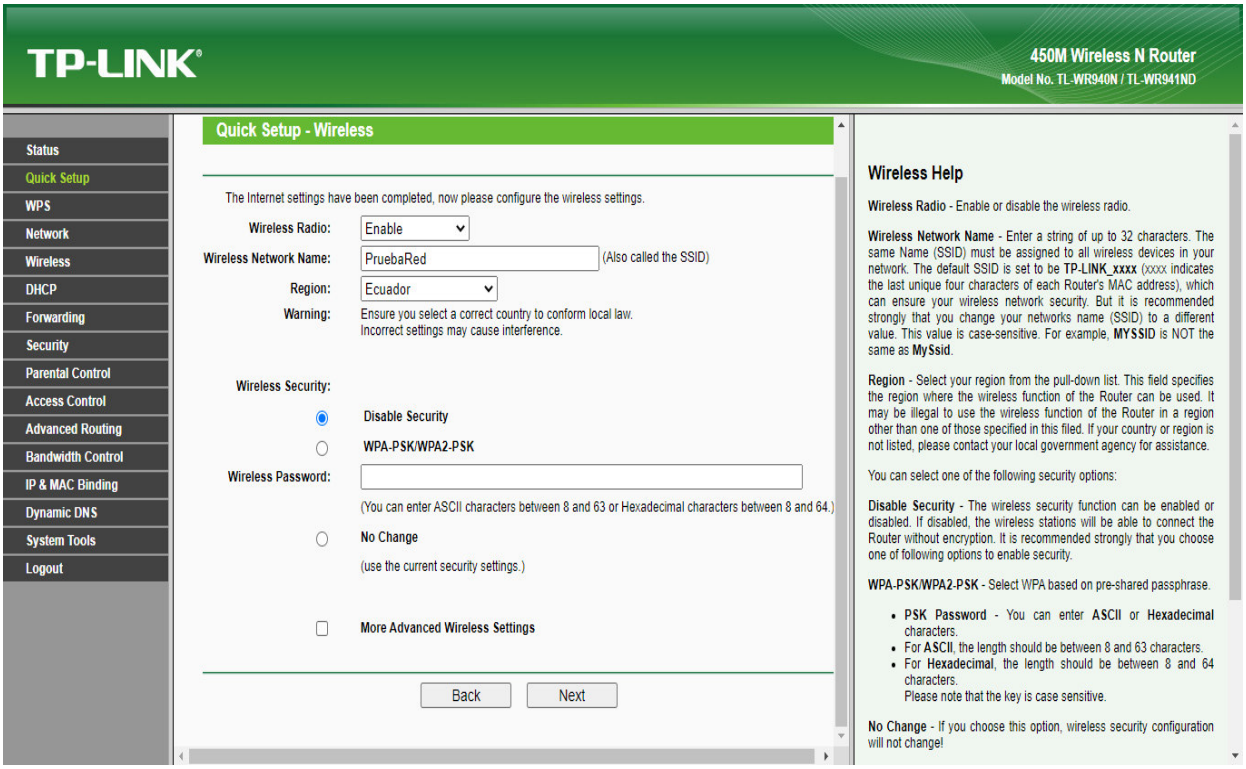
Nota. El celular empleado es un Doogee S98 Pro. Tomado del celular del autor

Implementar una AP a través de una computadora mediante dispositivo de red, y realizar un ataque para demostrar su vulnerabilidad:

Se establece un AP con el enrutador TP-Link WR940N, sin contraseña en este caso, para poder demostrar el ataque Man-in-the-Middle (MiTM), tal como se muestra en la figura

Figura 66

Configuración de Router

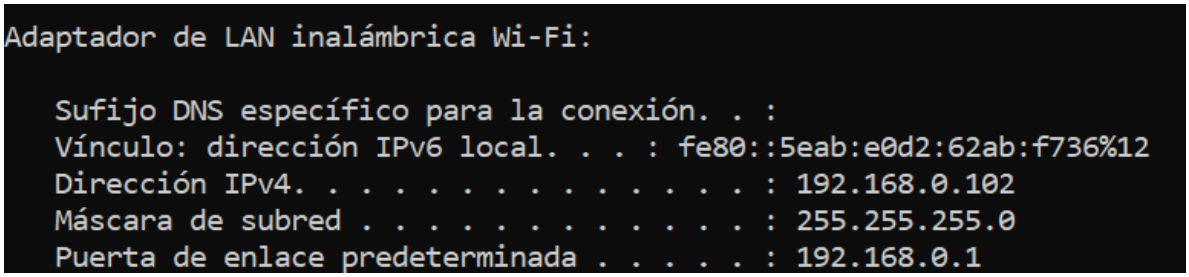


Nota. El router empleado es un TP-Link WR940N. Tomado de la laptop del autor

Busco el IP de la máquina que se realizara el ataque mediante CMD de Windows y escribir ipconfig la cual es 192.168.0.102, tal como se muestra en la figura

Figura 67

Verificar el IP

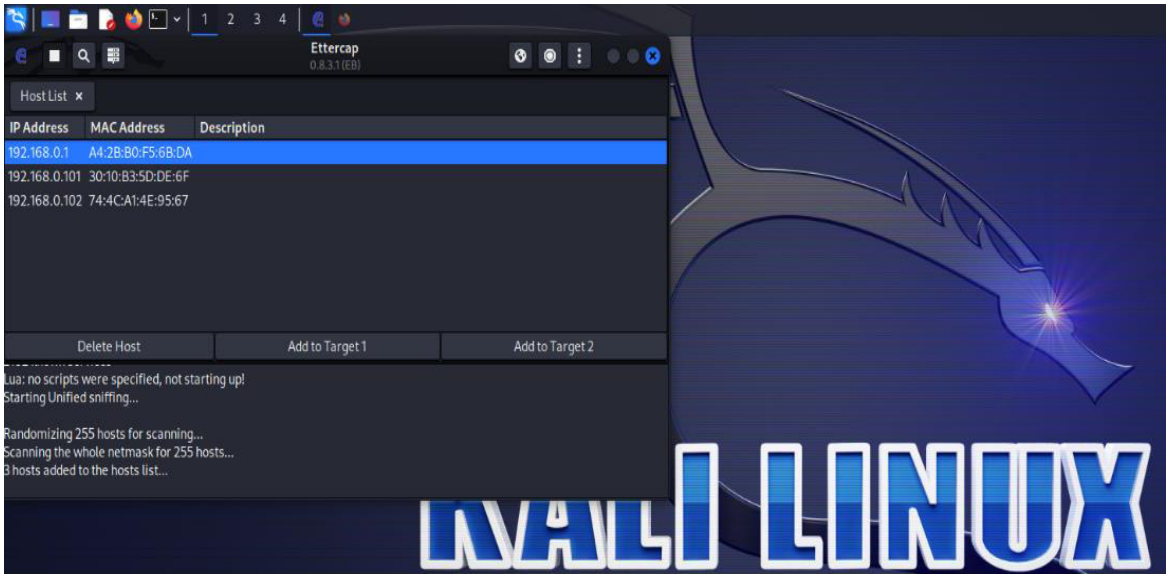


Nota. Obtenemos el IP de nuestra máquina. Tomado de la laptop del autor

Establecer una búsqueda de equipos con ettercap, tal como se muestra en la figura.

Figura 68

Verificación de IPs en la Red



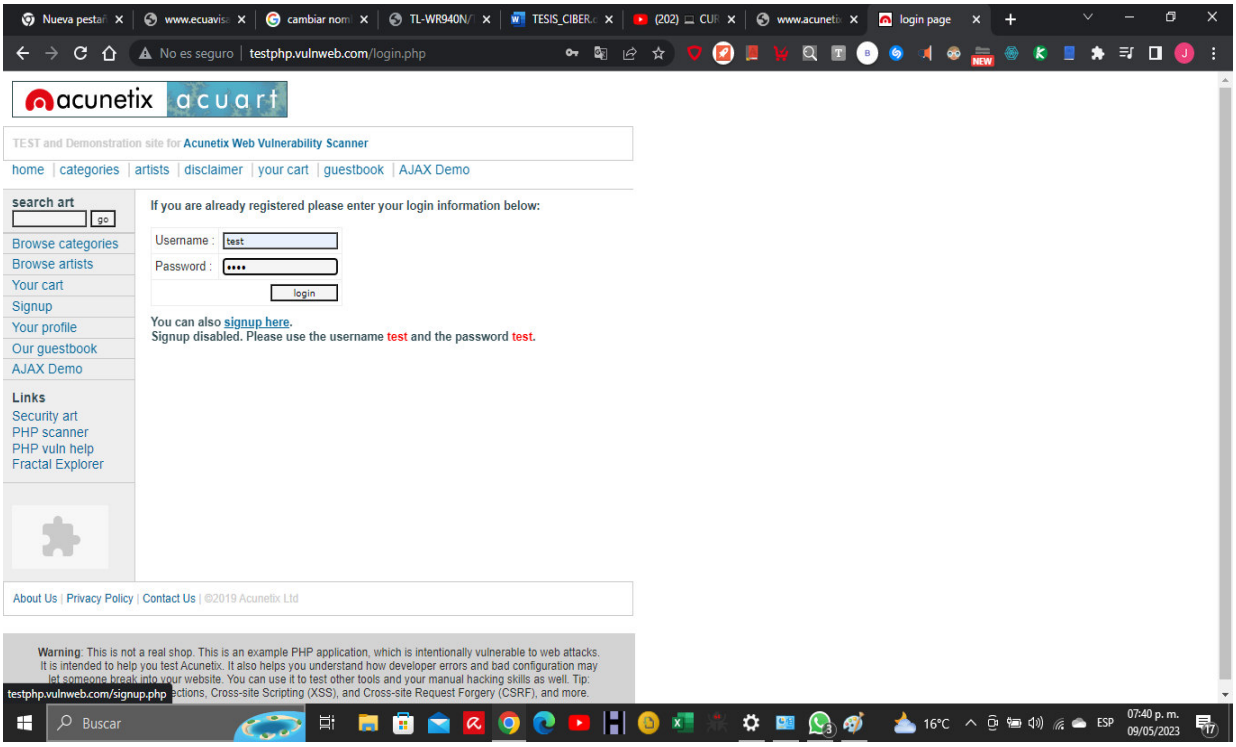
Nota. Obtenemos el IPs; de la máquina que atacamos y el router. Tomado de la laptop del autor.

La dirección de la máquina que vamos a atacar es: 192.168.0.101 y la dirección del router es 192.168.0.1 Realizamos un ataque con ettercap, tal como se muestra en la figura. anterior

Ingresamos a una página web: http://testphp.vulnweb.com/login.php para log in tal como se muestra en la figura

Figura 69

Ingreso a http://testphp.vulnweb.com/login.

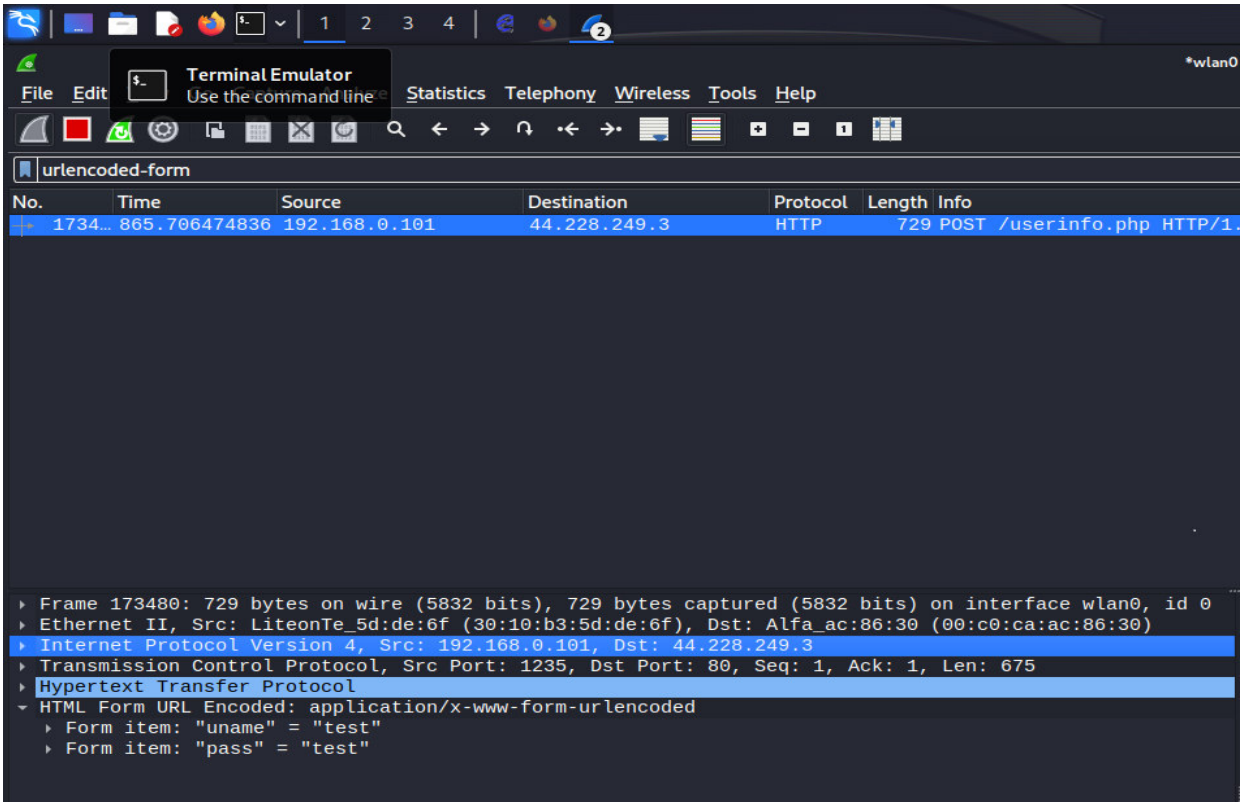


Nota. Ingreso de usuario y contraseña. Tomado de la laptop del autor

Con wireshark mediante el ataque Man-in-the-Middle (MiTM), capturamos el usuario: test y su contraseña: test, tal como se muestra en la figura.

Figura 70

Análisis de tráfico



Nota. Mediante Wireshark obtenemos las credenciales. Tomado de la laptop del autor

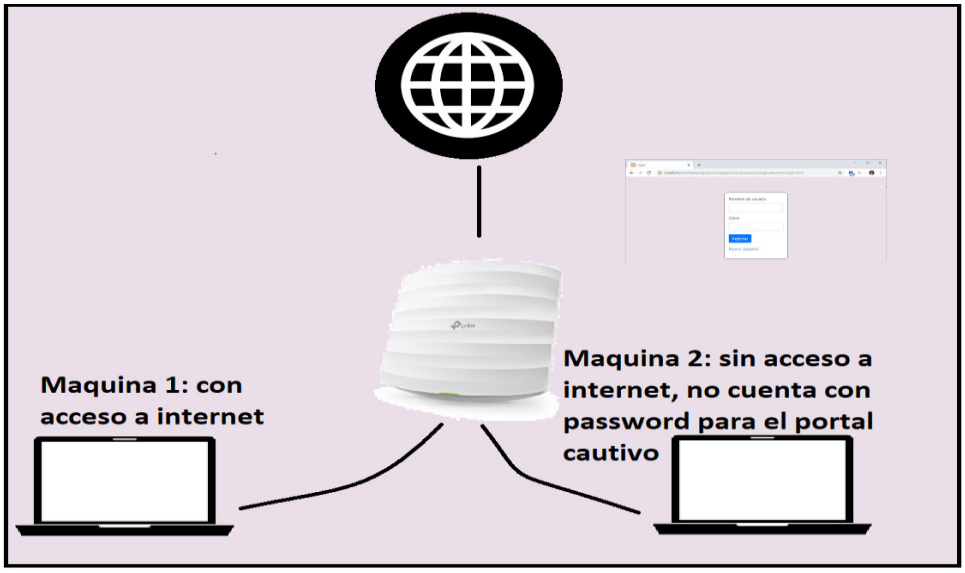
OWISAM-TR-008: Portal hotspot inseguro.

Planificación:

Crear un portal cautivo mediante punto de acceso Tp-link EAP115, crear el AP: PruebaRed3 y demostrar que pueden ser vulnerado y acceder al internet, al clonar la MAC de algún equipo que ya este registrado en la Red.

Figura 71

Red a implementarse

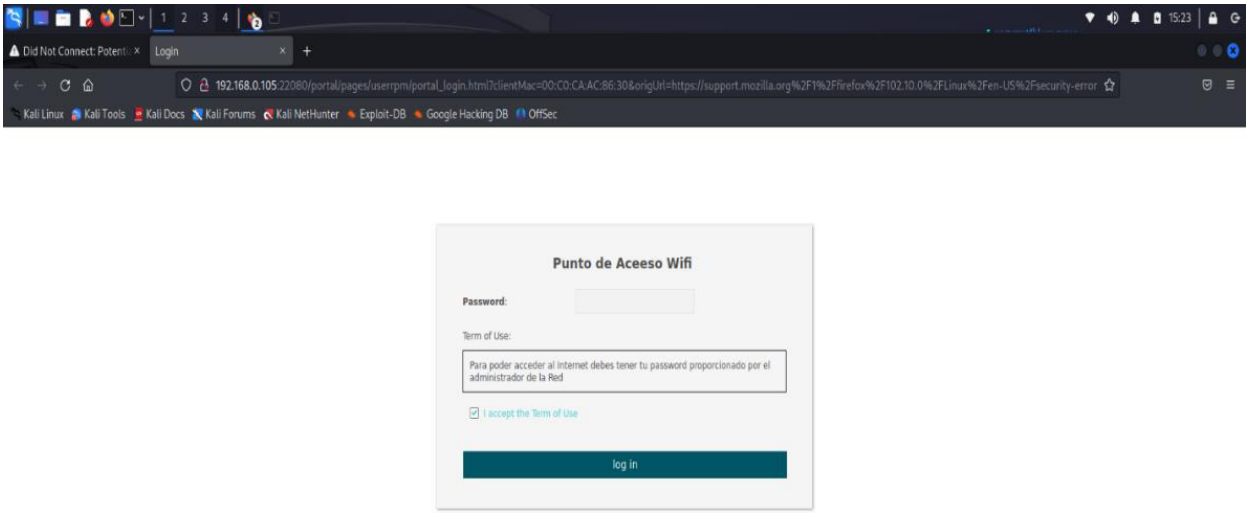


Nota. Se emplea un Access Point Tplink EAP115 el AP: PruebaRed3, la maquina 1 corresponde al equipo Toshiba Satellite C55-B5213K2 y la maquina 2 corresponde al equipo Acer Swift 3 N20C12. Tomado de la laptop del autor

En la máquina 2, saldrá el siguiente portal para poder acceder al Internet, como se muestra en la siguiente figura:

Figura 72

Portal Cautivo

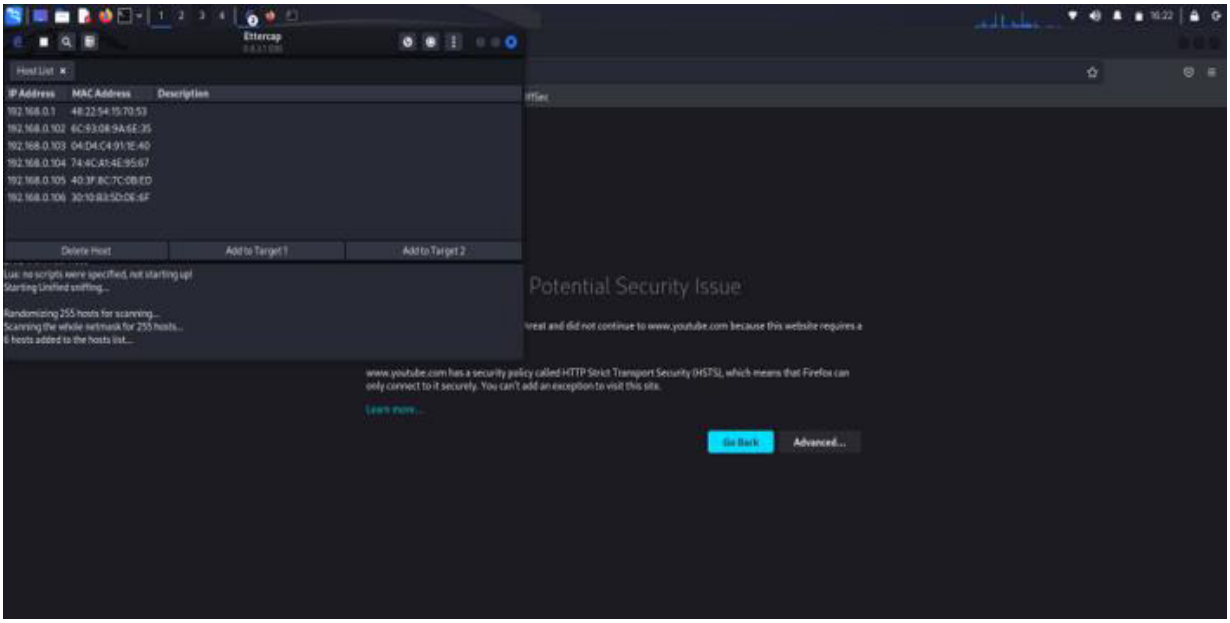


Nota. El portal cautivo se configura dentro del Access Point Tplink EAP115. Tomado de la laptop del autor

En este caso para poder acceder al internet, y saltarnos el portal cautivo lo que debemos hacer es ver que equipos se encuentran en la red, para ello podemos usar ettercap.

Figura 73

Identificación de IP



Nota. Identificamos a la Maquina 1, su Ip es 192.168.0.106 y su MAC es 30:10:b3:5d:de:6f. Tomado de la laptop del autor

Luego procedemos a clonar la Mac del equipo en nuestra máquina virtual Kali mediante los siguientes comandos:

Figura 74

Pasos para la clonación de MAC a través de Linux

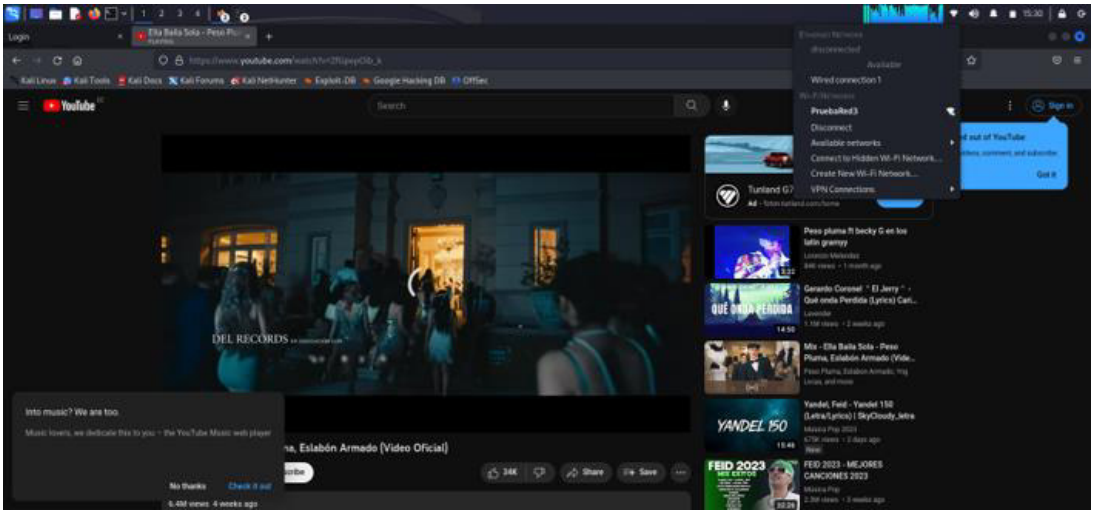
Nota. Detenemos la interfaz inalámbrica, clonamos el MAC y Reanudamos la interfaz inalámbrica.

Tomado de la laptop del autor

Verificamos que ya podemos acceder a internet:

Figura 75

Constatación de acceso a internet



Nota. Se accede al AP: PruebaRed3 y se abre la página web YouTube sin necesidad de loguearse. Tomado de la laptop del autor

Como podemos observar estamos conectados a Internet y reproducimos un video.

OWISAM-TR-009: Cliente intentando conectar a red insegura.

Planificación:

Crear una SSID: wifigratis para que la víctima acceda a esta red insegura y mediante wifpumpkin3 revisar su tráfico.

Compilación de información:

Se trabaja en un entorno controlado para realizar las pruebas de acceso a la red

Identificación de dispositivos:

Los dispositivos están en un entorno controlado y no necesitan ser identificados

Ataques:

Implementar un SSID y ejecutar wifipumpkin3

Pasos:

Implementar la máquina virtual Kali y conectar un adaptador wifi en nuestro caso utilizamos Alfa awus 1900, revisar que sea reconocida por sistema operativo como se muestra en el siguiente gráfico.

Figura 76

Instalación de adaptador wifi Alfa awus 1900

Nota. Se escribe el comando ifconfig y se visualiza el adaptador wifi. Tomado de la laptop del autor

Se procede a acceder a la aplicación wifipumpkin3 y se configurar la interface y el SSID como se muestra a continuación:

Figura 77

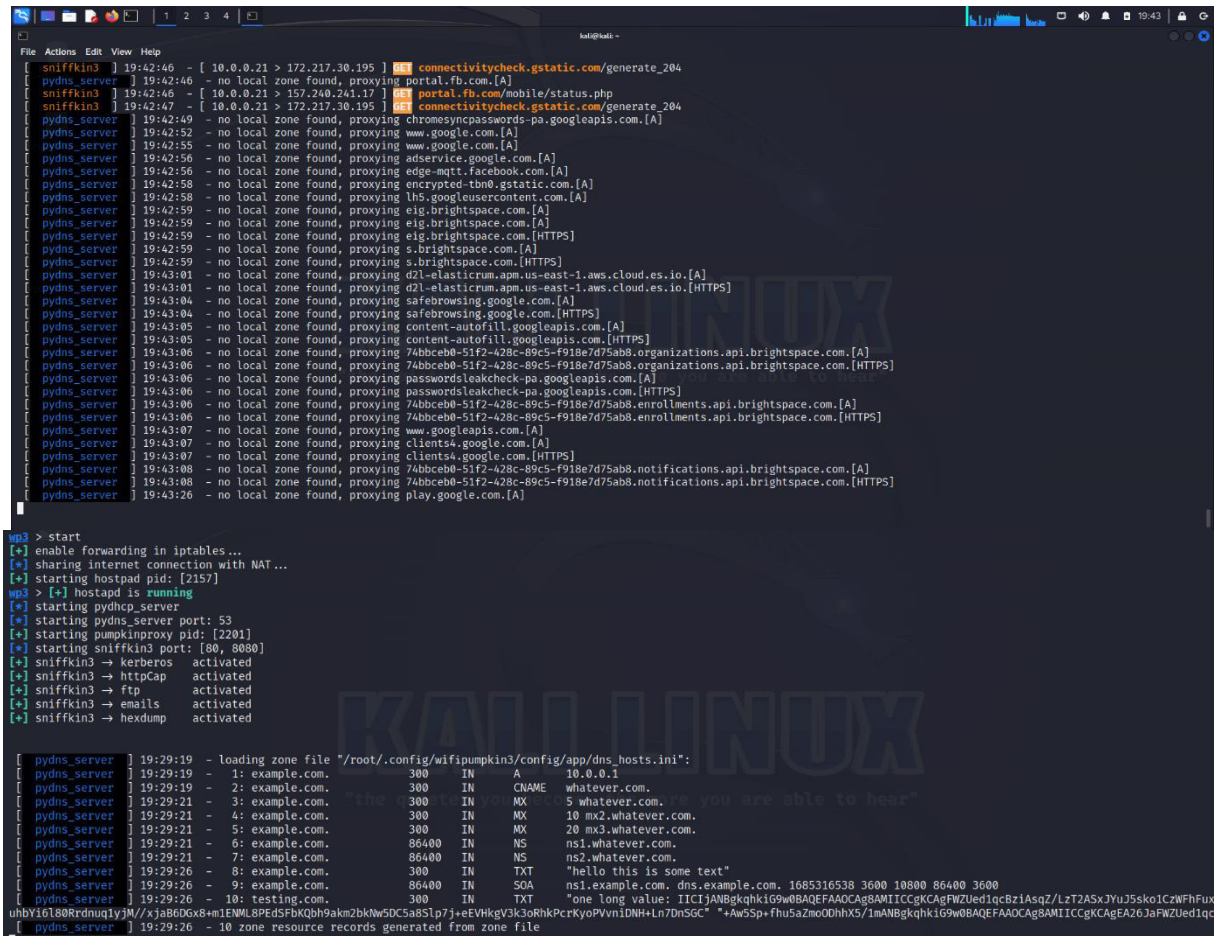
Configuración del AP

Nota. Se escribe el comando: set interface wlan0 y set ssid wifigratis tomado de la laptop del autor

Después iniciamos el punto de acceso y empieza a capturar tráfico de los clientes que se conecten a él tal como se muestra a continuación.

Figura 78

Puesta en marcha del AP y captura de trafico



Nota. Se escribe el comando: start y el AP se inicia, el tráfico capturado es del acceso de un dispositivo móvil. Tomado de la laptop del autor

Como se puede observar en la captura anterior, ya empezó a funcionar el AP y captura los paginas en la que navega el móvil Doogee S98 Pro.

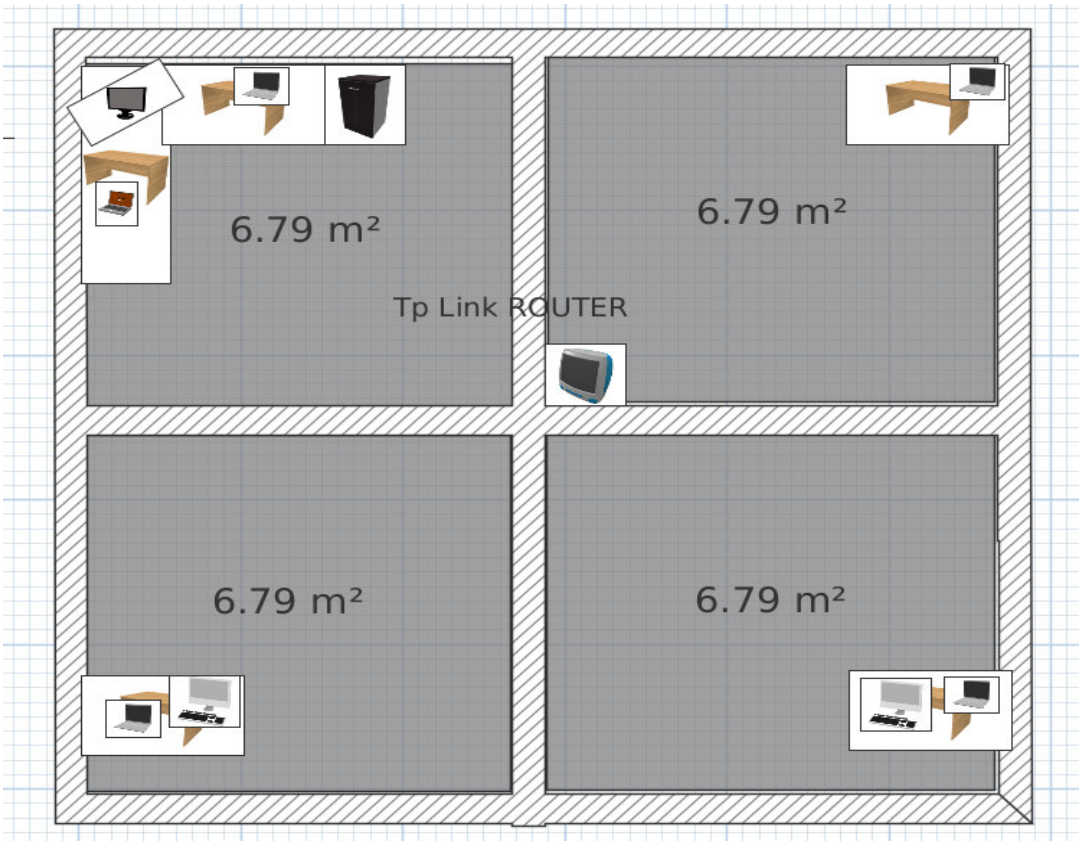
OWISAM-TR-010: Rango de cobertura de la red demasiado extenso.

Como se mencionó el estudio de la área a cubrir es crucial para saber exactamente la distancia que debería tener cobertura/señal y el número de dispositivos con sus respectivos

parámetros que debemos implementar, en la Figura de Abajo (oficinas de 4 ambientes) podemos observar que con un dispositivo (Router) es suficiente para cubrir los cuatros ambientes (siempre que este en centro), y mucho mejor si este dispositivo es colócalo en el techo para evitar entre otras cosas interferencias como electrodomésticos (teléfonos inalámbricos, microondas) y otro aspecto muy importante evitar el acceso físico al dispositivo y no permitir manipulaciones no autorizadas a el Router(s).

Figura 79

Diagrama de espacios con dispositivos interconectados mediante red inalámbrica.



Tomando en cuenta el ejemplo de 4 ambientes los parámetros ideales de configuración del único dispositivo/router seria de la siguiente manera:

Espectros: 2.4GHZ y 5GHZ (este segundo mayormente para evitar colisión con otros dispositivos/electrodomésticos).

Transmisión de Poder: Middle/Mediano, debido a que es un ambiente relativamente pequeño no se requerirá de un alto poder para cubrir/proveer la señal.

Anchura de canal: 40MHz también es una medida mediana/adecuada para suplir las necesidades sin necesidad de sobrealimentar la banda de flujo.

Canal de transmisión: Como sabemos en su mayoría los dispositivos trabajan en el rango de canales 1-13(2.4 GHz) y 24-161(5 GHz), entonces con la necesidad de evitar el overlaping y la colisión con el espectro de los otros canales y es mucho más factible utilizar un canal en el extremo del espectro (161 en este caso).

Modo: 802.11a/n/ac para permitir mayor compatibilidad de asociación incluso con dispositivos con tecnologías antiguas como son (a o n) velocidades.

Figura 80

Configuración de Router (TP-Link Archer 64) espectro 2.4GHZ.

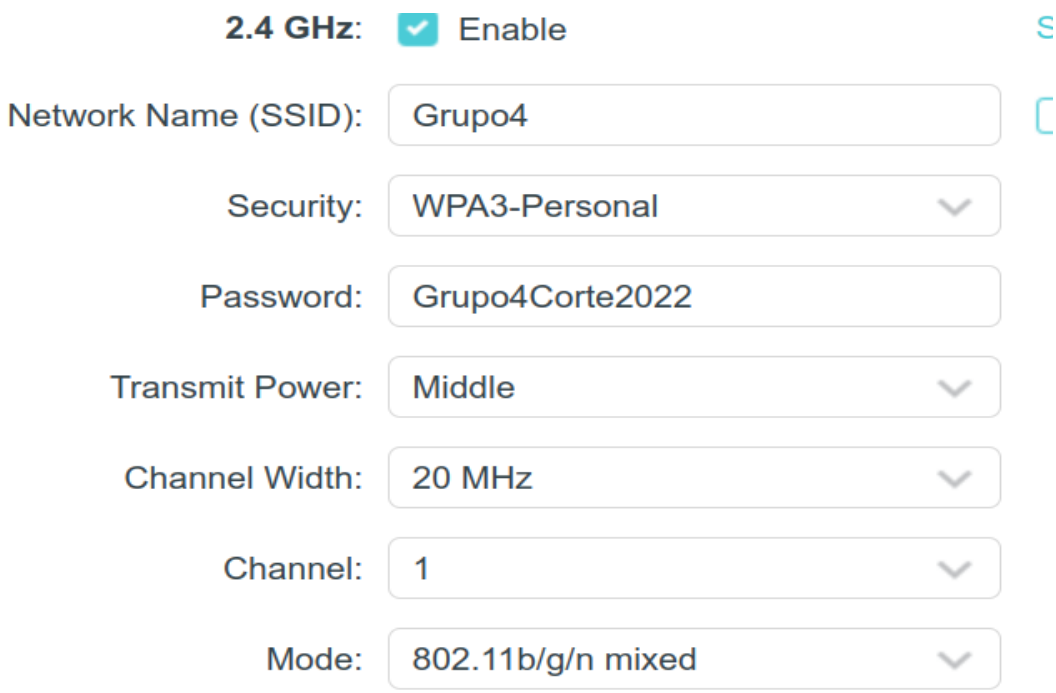
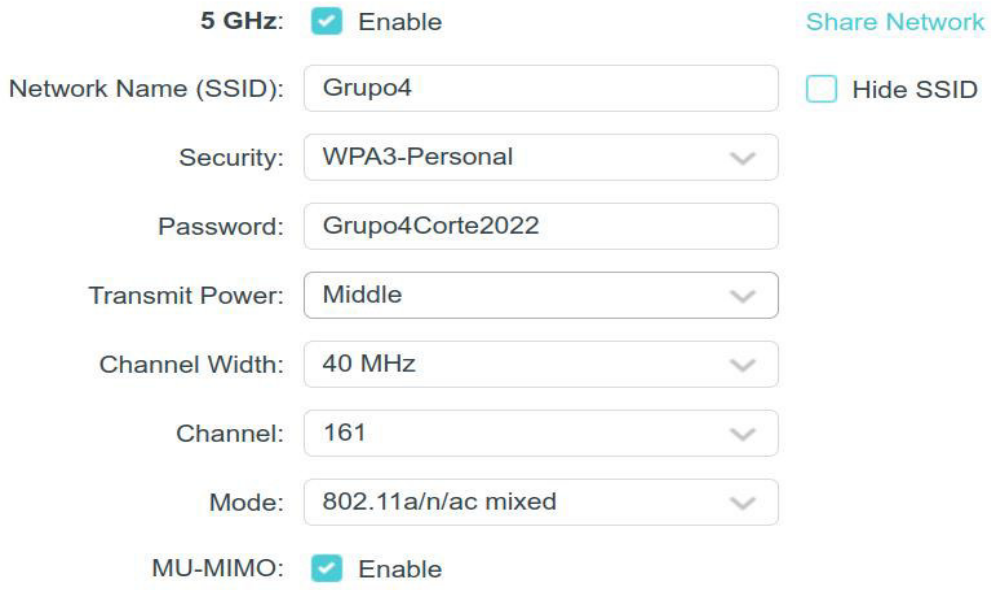


Figura 81

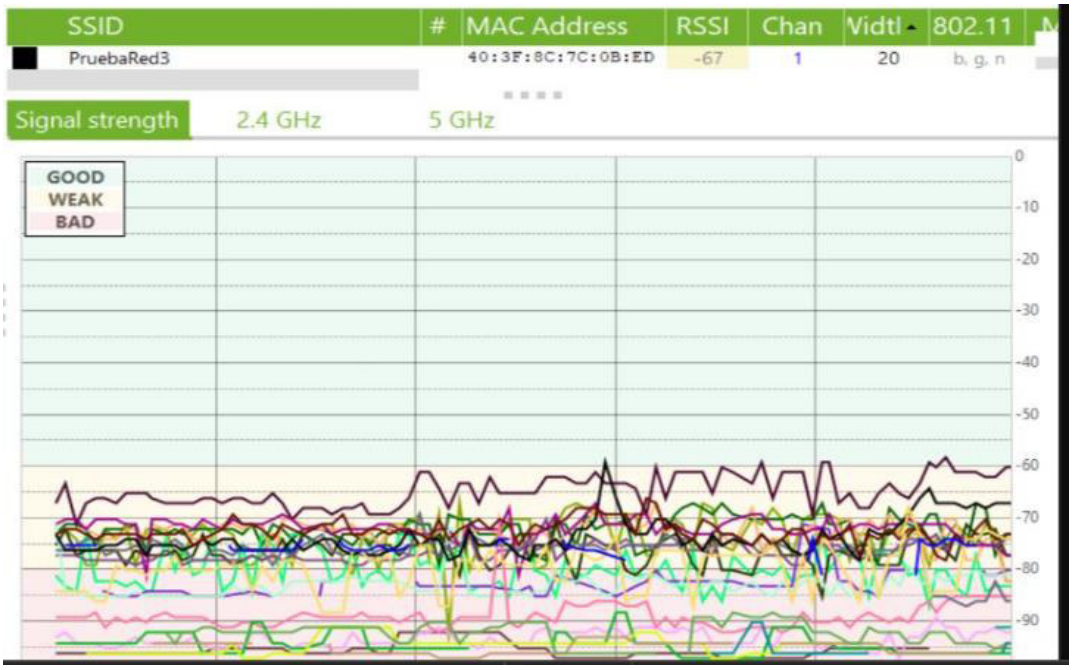
Configuración de Router (TP-Link Archer 64) espectro 5GHZ.



Una vez realizado la distribución corroboramos con un WIFI Analyzer (Acrylic) y nos da como resultado el siguiente diagrama de abajo: En el cual se observa que la señal tanto en el 4GHz como en el 5GHz es bastante buena para los 4 ambientes.

Figura 82

Mapa de calor de señales inalámbricas 2.4GHz y 5GHz.



Después de la implementación adecuada y la configuración apropiada de los dispositivos/AP, no solo con los valores más adecuados tanto en temas como poder, espectro etc. sino también en cuanto a la seguridad (como lo es el uso de protocolos más recientes WPA3), se realizó un escaneo del dispositivo implementado para saber cómo se compara en relación con protocolos anteriores y poder tener una idea clara de que tan protegida esta las tramas que viajan desde y hacia el router, y los hallazgos no fueron de lo mejor, es más deja muchas dudas acerca de la “supuesta protección mejorada” que tanto ofrecía y también nos lleva a reconsiderar el principio básico de la seguridad “mientras más fuerte/compleja es la clave tomara mucho más tiempo el poder romper la misma”.

Figura 83

Pantalla de escaneo de Routers disponibles/broacasting.

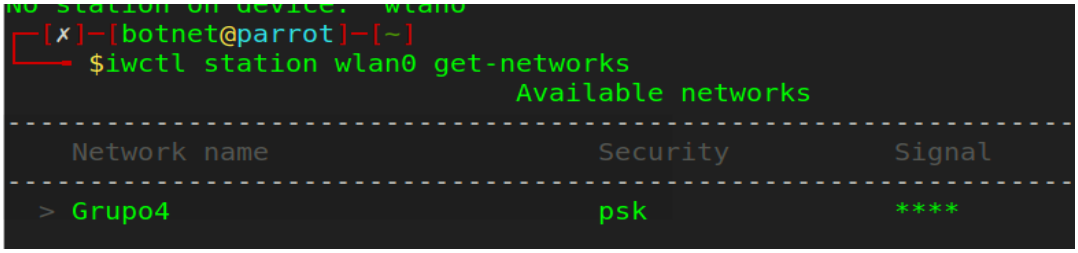
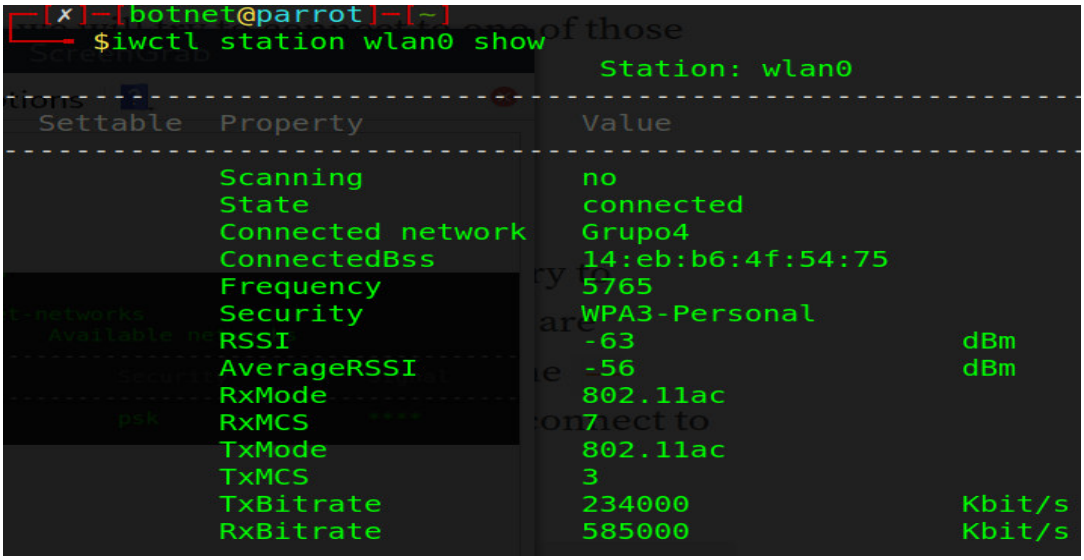


Figura 84

Pantalla con presencia de Router con WPA3 presente.

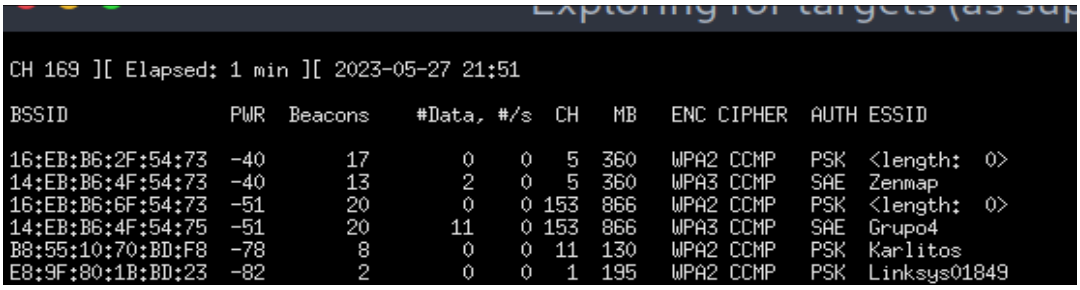


Como podemos observar en las imágenes superiores, las redes están configuradas con el protocolo WPA3- Personal, lo que demuestra en un escaneo de estaciones APs. Pero si miramos las tramas usando Wireshark nos daremos en cuenta que por algún motivo también está habilitada WPA2-PSK con la excepción que esta no hace broadcasting el nombre de la red sino más bien la pone como escondida, como aparece en la Figura 84 (WPA3 supuestamente evitaría que se pudiera

realizar ataques de diccionario), pero al incluir WPA handshake nos permite volver a intentar atacar esta parte del handshake que tan buenos resultados ha dado.

Figura 85

Escaneo de Red hacia routers.



Al revisar las tramas del wireshar y su posterior escaneo vemos que efectivamente se puede lanzar un intento de robo de handshake, como vemos en las imágenes después de recibir las 4 tramas de autenticación, hay una trama (Beacon) recibida donde nos muestra que tanto AES como la PSK han sido recibidas/interceptadas.

Figura 86

Porción de paquete de wireshar con (4) paquetes de autenticación de protocolo WPA3.

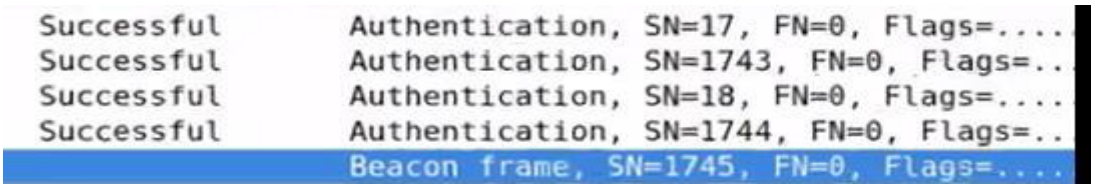
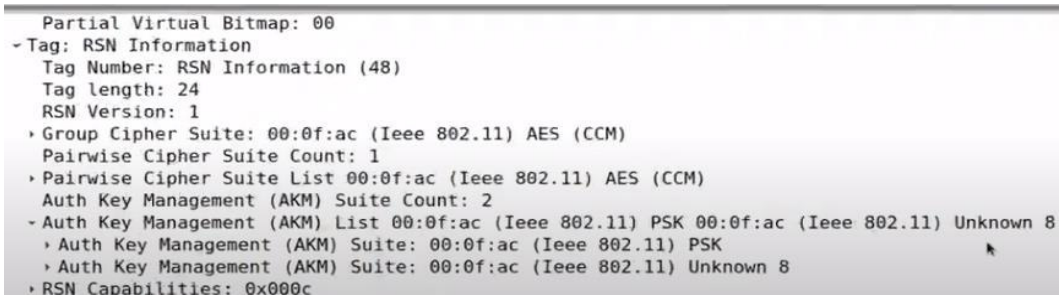


Figura 87

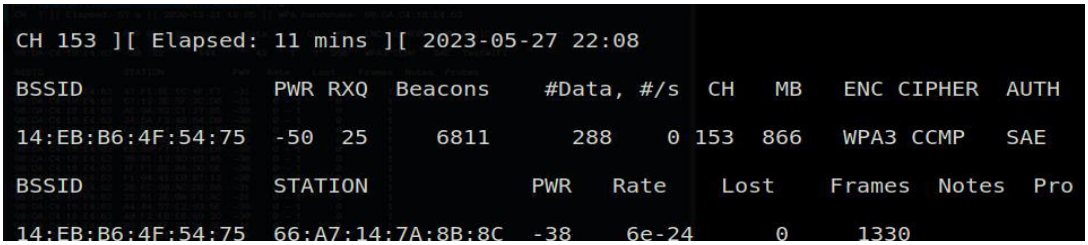
Porción de paquete de wireshar con presencia de PSK (pre shared key).



Al final se pudo intentar (sin éxito aparente) poder rescatar el handshake, con lo que demuestra que, aunque WPA3 al utilizar una nueva técnica para que el handshake no pueda ser utilizado en un ataque diccionario, debido a la compatibilidad con dispositivos antiguos también ofrece el mismo mecanismo WPA2, a este se tipo de vulnerabilidad se le conoce como ataque Downgrade, en la que se toma ventaja de una antigua tecnología vulnerable como lo es WPA2.

Figura 88

Escaneo para obtener el handshake.



CAPÍTULO 3

Análisis de resultados

Red de comunicaciones Wi-Fi abierta:

Luego de recrear en ambientes controlados los principales ataques que se pueden realizar en redes de comunicaciones Wi-Fi abiertas, se demostró la facilidad con la que el atacante puede hacerse de los datos de la víctima, es imperioso seguir las recomendaciones que se presentarán a continuación para evitar caer en estos ataques. Una red wifi abierta le proporciona al atacante un campo de acción que no podría obtener en una red protegido con contraseña. También se pudo verificar luego de las pruebas realizadas, tanto los navegadores como los desarrolladores de páginas web están al tanto de las vulnerabilidades existentes y han implementado una gran cantidad de filtros y protecciones para alertar y defender al usuario, de ahí la importancia de siempre mantener el software al día y así poder aprovechar de estas actualizaciones que se lanzan al mercado todos los días.

Presencia de cifrado WEP en redes de comunicaciones

El cifrado WEP ha sido objeto de numerosos estudios y análisis que han revelado varias debilidades y vulnerabilidades. Por ejemplo, el artículo "Weaknesses in the Key Scheduling Algorithm of RC4" mostró la existencia de problemas graves en el algoritmo RC4 utilizado por WEP, lo que permite a los atacantes recuperar la clave de cifrado. (Fluhrer, 2001). Se han desarrollado y demostrado varios ataques prácticos contra WEP. El artículo "Breaking 104 bit WEP in less than 60 seconds" describe un método para recuperar una clave WEP de 104 bits en menos de un minuto utilizando una técnica de inyección de paquetes (Tews, 2007).

WEP requiere que todos los dispositivos de la red compartan la misma clave de cifrado, lo que puede ser problemático en entornos donde se necesita compartir el acceso con múltiples usuarios o invitados. Además, cambiar las claves de cifrado en una red WEP puede ser complicado y propenso a errores. Diversas organizaciones de seguridad y estándares, como el Instituto Nacional de Estándares y Tecnología (NIST) y el Grupo de Trabajo de Ingeniería de Seguridad (IETF), desaconsejan el uso de WEP y recomiendan utilizar protocolos de seguridad más sólidos, como WPA2.

Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS)

Debido a sus fallos de seguridad, el protocolo Wi-Fi Protected Setup (WPS) ha suscitado críticas. Aunque su objetivo era facilitar la configuración de los dispositivos Wi-Fi, su aplicación ha mostrado graves fallos que podrían poner en peligro la seguridad de la red.

Numerosos ataques y debilidades conocidos, como el ataque por fuerza bruta al PIN de WPS se han dirigido al protocolo WPS. El PIN WPS de 8 dígitos utilizado en muchos dispositivos es vulnerable a estos ataques, ya que la combinación de 8 dígitos proporciona un campo de búsqueda relativamente pequeño, lo que hace posible que un atacante adivine o fuerce el PIN WPS y obtenga acceso ilegal a la red Wi-Fi. Debido a esto, es sencillo para los atacantes adivinar el PIN WPS o romperlo mediante estos tipos de ataques.

Clave WEP/WPA/WPA2 basada en diccionario

La eficacia de estos ataques demuestra lo débiles que son los protocolos WEP, WPA y WPA2 basados en diccionarios. Debido a las restricciones de estos protocolos en materia de

cifrado y autenticación, se ha demostrado que no son seguros. Sin embargo, el éxito del asalto subraya la importancia de emplear claves de seguridad robustas y distintivas. La seguridad de las redes inalámbricas es una actividad continua más que un acontecimiento puntual. Es esencial realizar auditorías de seguridad periódicas, vigilar la red en busca de actividades sospechosas y parchear los dispositivos con los parches de seguridad más recientes.

Es bien sabido que el protocolo WEP es poco seguro. Su método de cifrado RC4 y su implementación subyacente exponen una serie de puntos débiles que pueden ser explotados por los atacantes. La clave de cifrado puede descifrarse rápidamente mediante ataques basados en diccionario y fuerza bruta, lo que puede dar a los atacantes acceso ilimitado a la red.

El uso de WPA/WPA2 constituye una mejora sustancial de la seguridad con respecto al protocolo WEP. Estos protocolos hacen más difícil para los atacantes comprometer la red al utilizar técnicas de cifrado y autenticaciones más potentes. Aunque el uso de contraseñas débiles puede facilitar los intentos de piratear una red WPA/WPA2, sigue siendo crucial utilizar contraseñas fuertes y seguras. Las combinaciones cortas y las palabras frecuentes son ejemplos de contraseñas débiles más vulnerables a los ataques de diccionario.

Aunque WPA/WPA2 es más resistente a los ataques de fuerza bruta y a los ataques de diccionario que WEP los atacantes podrían seguir utilizando diccionarios de contraseñas débiles para acceder a la red. Sin embargo, gracias al aumento de los mecanismos de seguridad incluidos en WPA/WPA2, estos ataques podrían ser considerablemente más lentos y menos eficaces.

Mecanismos de autenticación inseguros (LEAP, PEAP-MD5,)

Mediante la configuración de servidores de autenticación que usan los protocolos LEAP, PEAP y MD5, se realizaron pruebas/ataques a las tramas emitidas durante la comunicación para la autenticación y posterior autorización de un usuario/dispositivo, y como se puede ver mediante el uso de herramientas con muy poca necesidad de configuración como Wireshark, se pudo no solo capturar la trama/handshake, sino que también poder leer la misma y descubrir que los datos del usuario no estaban cifrados.

Y en caso de que estos estuviesen cifrados no es difícil romper/descifrar los mismos con ataques offline debido al pobre mecanismo de cifrado que se usa, los detalles descubiertos en las tramas como son el checksum no solo que indican el tipo de algoritmo que usa, sino sirve para saber el mecanismo de ataque como (fuerza bruta) para poder obtener las claves que se encuentran establecidas en la comunicación.

Dispositivo con soporte de Wi-Fi protected setup PIN activo (WPS).

Durante las pruebas realizadas a la configuración de PIN activo WPS, se pudo observar que, aunque la extensión de las claves numerales (8 o 10 dígitos) no es lo mejor, se pueden realizar modificaciones en cuanto a los métodos para la sincronización/pairing entre el router y el cliente, lo cual permite tener 3 diferentes métodos de control (PIN Router, PIN Dispositivo y por descubrimiento), esto ayuda a que si algún atacante desea ingresar/ser parte de una red deberá al menos intentar una des autenticación previa (en modo PIN Router) para intentar obtener el código correcto.

En las pruebas también se observó que el router cuando descubre intentos de ataque como des autenticación, corta/rechaza el flujo cada 9-14 intentos de dar con el código correcto, este mecanismo de protección también deshabilita WPS y solo puede volver a ser habilitado mediante un login al router IP, entre los parámetros de (hardening) en este router tiene activado cifrado WPA3, lo que impediría que el atacante pudiera realizar un ataque de fuerza bruta y en el caso de ser éxito el robo de la trama/handshake vendría el dilema de intentar descifrar el cifrado WPA3 lo que en si trae un reto más grande.

Un descubrimiento que se dio es que el router que se usó para las pruebas de WPS (Tp-linkArcher c64) asignado como (Grupo4) una vez habilitado el cifrado WPA3, no fue posible vulnerar este dispositivo incluso durante la búsqueda de "escaneo de víctimas con WPS" (la única explicación para esto ha sido la activación de WPA3).

Red Wi-Fi no autorizada por la organización.

Durante la prueba se puede evidenciar lo fácil que se puede capturar información en este caso usuario y password, mediante wireshark y ettercap, se puede realizar estas mismas pruebas como bettercap, wifipumpkin3 entre otras.

Portal hotspot inseguro

Durante la prueba se pudo acceder al portal cautivo, pero la velocidad de conexión es menor, también pude constatar que el procesador empieza a trabajar más y la pagina se empieza a cargar más lento. Tal vez el que en la red se encuentre duplicado dos Mac crea estos inconvenientes en conexión.

Cliente intentando conectar a red insegura.

Este tipo de ataque se debe emplear un adaptador wifi adicional para poder crear el AP que tenga las características adecuadas para poder configurarlo, así también el uso de la herramienta wifipumpkn3, requiere una cierta de curva de aprendizaje ya que permitía acceder a móviles al AP creado, pero, no a la laptop que empleamos para hacer ataques en ejercicios anteriores

Rango de cobertura de la red demasiado extenso.

Ciertamente la implementación de una red/dispositivos requiere un estudio complejo no solo en el tema del espacio a cubrir sino también las tecnologías a usar, y en la gran mayoría de los casos por falta de un mapa de calor en cuanto al alcance de las señales (mayormente de APs) se comete el error de implementar demasiados dispositivos o muy cercanos el uno del otro, lo que puede crear overlaping de canales si estos son muy continuos, pero como se ha realizado en el pequeño ambiente se puede usar un solo dispositivo con 2 bandas, para crear 2 señales distintas que trabajaran en canales diferentes evitando la colisión y al mismo tiempo ofrecerán velocidades distintas para que el dispositivo de acuerdo a la necesidad del contenido, pueda elegir entre estar en una robusta pero no muy larga como 5GHz, o no muy robusta pero de mayor alcance como la 2.4GHz.

Durante la implementación de los protocolos de seguridad pudimos descubrir también que, aunque prioricemos el protocolo (WPA3) algunos dispositivos (debido a la incompatibilidad) harán uso de un protocolo mucho más familiar/sencillo e inseguro como lo es (WPA2), esto lleva a replantearnos e intentar vulnerar este “nuevo protocolo” para saber si es tan seguro como lo mencionaron, lo cual no es totalidad cierto en cuanto al tema de no permitir vulnerabilidades conocidas, por lo que se requiere que después de la implementación de una red un extenso

análisis/pentest de la misma. Ya que si en el handshake existen tramas de WPA2 estas son susceptibles a ataques de diccionario.

CAPÍTULO 4

Conclusiones y Recomendaciones

Al conectarse a una red de comunicaciones Wi-Fi abierta

Ante esta vulnerabilidad las recomendaciones que podemos aportar luego del trabajo realizado son: Siempre verificar la autenticidad de la red a la que nos vamos a conectar, es importante asegurarnos de que la red Wi-Fi abierta a la que nos pretendemos conectar sea legítima. De ser posible preguntar al encargado del lugar el nombre exacto de la red y en qué sector se encuentra el AP que la distribuye.

En lo posible utilizar siempre una VPN, esto a fin de cifrar todo tipo de dato que se vaya a transmitir dentro de nuestra red inalámbrica y así proteger la privacidad de la información. Las VPN (Redes Privadas Virtuales) cifran los datos transmitidos, lo que dificulta a los atacantes espiar la información enviada o recibida

Al estar conectados en una red abierta es de suma importancia evitar visitar sitios web que nos soliciten credenciales o información confidencial, como pueden ser contraseñas, números de tarjetas de crédito o cualquier otra información sensible. Lo recomendable es esperar a conectarnos en una red segura para acceder a estos sitios.

Mantener los dispositivos siempre actualizados nos mantendrá alejados de las últimas amenazas de seguridad detectadas, evitando ser víctimas de vulnerabilidades que ya tienen parches y que los cibercriminales pudieran intentar aprovechar.

En muchas ocasiones los dispositivos se conectan a estas redes abiertas sin que el usuario se dé cuenta, es importante desactivar la opción de conexión automática en todos nuestros equipos.

Adicional a estas recomendaciones, se pueden agregar las siguientes enfocadas en evitar ser víctimas del SSL Stripping:

Asegurarse que los sitios web que se visita utilicen HTTPS y no HTTP, ya que como se demostró HTTPS cifra la información y es más segura la transmisión de datos. Se debe en lo posible mantener todos los navegadores actualizados y con los parches de seguridad al día, ya que estos suelen detectar ataques de SSL Stripping y los bloquean.

Tal y como se mencionó en el apartado anterior el uso de VPN es imprescindible para mantener la privacidad del tráfico enviando desde y hacia nuestros equipos, contar con una VPN dificulta la tarea de los atacantes y protege nuestra información.

Existen extensiones de seguridad propias de los navegadores que nos alertan cuando una conexión no es segura o incluso la bloquean para evitar que caigamos en este tipo de ataques. Y como recomendación final, en lo posible evitar conectarse en redes libres al menos que sea una emergencia.

Presencia de cifrado WEP en redes de comunicaciones

Aunque el cifrado WEP se creó en busca de aportar seguridad a las comunicaciones inalámbricas, hoy en día está obsoleto y es muy peligrosos confiar en este tipo de cifrado para proteger nuestras redes. Por lo antes expuesto ya son pocos los equipos que permiten asociarse a una red Wi-fi que implemente el cifrado WEP y es mucho más difícil encontrar en el mercado equipos que difundan redes inalámbricas protegidas con él. En todo caso si por algún motivo se debe establecer una conexión por medio de cifrado WEP es importante mantener cualquier comunicación sensible a través de una VPN, así con esta protección adicional del tráfico generado y recibido, será mucho más difícil para un atacante hacerse con nuestra información.

Algoritmo de generación de claves del dispositivo inseguro (contraseñas y WPS).

Se desaconseja utilizar el protocolo WPS al configurar redes Wi-Fi debido a los fallos conocidos y a la sencillez de los ataques de fuerza bruta al PIN WPS. Para proteger eficazmente la red Wi-Fi y evitar accesos ilegales, es importante desactivar WPS en los dispositivos y elegir medidas de seguridad más robustas, como WPA2-PSK o WPA3.

Clave WEP/WPA/WPA2 basada en diccionario.

Debido a su enorme debilidad y a la facilidad con la que se vulnera, el protocolo WEP supone un riesgo importante para la seguridad de la red inalámbrica. Para garantizar la confidencialidad de los datos transmitidos y defender la red de posibles ataques, se recomienda encarecidamente no utilizar WEP y adoptar protocolos más seguros. Dado el alto nivel de vulnerabilidad del protocolo WEP, varios expertos y organizaciones de seguridad desaconsejan encarecidamente su uso. Por ejemplo, la Wi-Fi Alliance ya no certifica los aparatos que sólo admiten WEP.

Para proteger las redes contra los ataques de diccionario y garantizar la seguridad, una clave segura debe tener una mezcla aleatoria de caracteres y la longitud adecuada. La sugerencia clave es utilizar protocolos más seguros como WPA2 o WPA3. Es mucho menos probable que se produzcan ataques basados en diccionarios gracias a las técnicas superiores de cifrado y a los procedimientos de autenticación que ofrecen estos protocolos.

Para reforzar aún más la seguridad de la red, además de utilizar contraseñas seguras, se aconseja aplicar medidas de seguridad adicionales, como el filtrado de direcciones MAC o el uso de redes privadas virtuales (VPN).

Mecanismos de autenticación inseguros (LEAP, PEAP-MD5)

Independientemente del tipo de cifrado que se use, de no ser posible abandonar los protocolos vulnerables/débiles (en muchos casos por la compatibilidad con dispositivos antiguos), se debería (hardenizar) los contenidos de (mschap.conf) recomendado para crear una política de enforzar la validación del certificado no solo en los usuarios sino que también los dispositivos (MAC address) deberían tener su certificado asociado a esta con los parámetros enlazados como (IP address y VLAN) de esta manera el dispositivo no solo deberá poseer el certificado asignado sino también debería estar dentro de la segmentación autorizada, esto con la finalidad de que el atacante incluso si es capaz de descubrir la clave, la base al revisar el certificado deberá cumplir con los mecanismos implementados dentro de (mschap.conf), dentro de este apartado (mschap.conf) se recomienda también configurar para evitar (MD5, LEAP) por completo y enforzar (strong encryption), por lo que nos daría un mecanismo más de protección.

Como se menciona el énfasis deberá estar en proteger y enforzar el uso de certificados asociados a cada usuario/dispositivo mediante la asociación, de esta manera un mismo certificado no pueda ser utilizado en un dispositivo diferente.

Dispositivo con soporte de Wi-Fi Protected Setup PIN activo (WPS).

Aunque los routers ahora vienen con capacidad WPS para una “facilidad de configuración” no se debería habilitar la misma, y si existiera una exigencia de así hacerlo, se debería recurrir al método de (PIN Dispositivo) de esta manera será el dispositivo del usuario el que deberá proveer el código correcto para la asociación.

Hoy en día incluso hay routers que vienen con un botón/manual para desactivación, activación y sincronización de WPS lo que da el mejor control al momento de configurar, ya que incluso con intento de fuerza bruta no se podría vulnerar el protocolo ya que se debería activar/presionar manualmente (acceso físico) el protocolo WPS.

Actualizar el firmware: Tener la última versión del firmware del enrutador instalada. Los fabricantes a menudo lanzan actualizaciones para abordar vulnerabilidades y mejorar la seguridad. Revisar el sitio web del fabricante del enrutador para obtener las actualizaciones más recientes ya que al momento de la actualización las vulnerabilidades antiguas/descubiertas no surtan efecto en el dispositivo.

Contraseñas seguras: Asegurarse de que la red Wi-Fi esté protegida con una contraseña fuerte y única. Utilizar una combinación de letras mayúsculas y minúsculas, números y símbolos para crear una contraseña segura. Evitar usar contraseñas predecibles o fáciles de adivinar.

Cambiar la contraseña predeterminada del enrutador: Muchos enrutadores vienen con una contraseña predeterminada que es conocida por los atacantes. Cambiar la contraseña predeterminada del enrutador por una contraseña única y segura.

Filtrado de direcciones MAC: El filtrado de direcciones MAC permite que solo los dispositivos con direcciones MAC específicas se conecten a tu red. Se puede agregar las direcciones MAC de los dispositivos permitidos en la configuración del enrutador. Esto añade una capa adicional de seguridad.

Cortafuegos activado: Asegurarse de que el cortafuegos del enrutador esté activado. Un cortafuegos ayuda a proteger la red bloqueando el tráfico no autorizado y los intentos de intrusión.

Red privada virtual (VPN): Si se desea una capa adicional de seguridad al usar Wi-Fi público o cuando se conecta a una red doméstica desde lugares remotos, considera utilizar una red privada virtual (VPN). Una VPN encripta la conexión y protege los datos de posibles amenazas.

En último caso si el uso de WPS no justifica los riesgos/vulnerabilidades que trae se debería: Desactivar WPS: Aunque WPS fue diseñado para facilitar la conexión de dispositivos a la red Wi-Fi, también puede ser una vulnerabilidad de seguridad. Es recomendable desactivar la función WPS en el enrutador para evitar posibles ataques, o en su defecto usar WPA3 en los canales de comunicación y con esto se deshabilitará WPS automáticamente.

Red Wi-Fi no autorizada por la organización.

Para evitar que se establezcan redes Wi-Fi no autorizadas en una organización, puede tomar las siguientes medidas:

- **I**mplementa una política clara: Establece una política de uso de redes Wi-Fi en la organización y comunícala a todos los empleados. Debe dejar en claro que solo se permite el uso de redes Wi-Fi autorizadas y que la creación de redes personales no está permitida.

- Configura un punto de acceso centralizado: Configura un punto de acceso Wi-Fi centralizado y controlado por el departamento de TI de la organización. Esto permite tener un control total sobre la infraestructura de Wi-Fi y evita que los empleados configuren redes no autorizadas.
- Utilice medidas de seguridad adecuadas: Asegúrese de que la red Wi-Fi autorizada esté protegida con medidas de seguridad robustas, como el cifrado WPA2 o WPA3, contraseñas seguras y actualizaciones regulares de firmware. Esto dificultará que los empleados busquen alternativas no autorizadas.
- Supervisa la red: Realiza un monitoreo regular de la red Wi-Fi para detectar cualquier actividad no autorizada. Puede utilizar herramientas de monitoreo de red para identificar redes no autorizadas y tomar medidas en consecuencia.
- Educa a los empleados: Realiza programas de capacitación y concientización para educar a los empleados sobre los riesgos asociados con el uso de redes Wi-Fi no autorizadas. Explícales las políticas de seguridad y las razones por las que es importante evitar el uso de redes no autorizadas.
- Bloquea el acceso físico: Limita el acceso físico a los puntos de conexión de red para evitar que los empleados conecten dispositivos no autorizados a la infraestructura de red.

- Mantén actualizados los dispositivos: Asegúrate de que los dispositivos de red, como enrutadores y puntos de acceso, estén actualizados con los últimos parches

de seguridad. Esto ayuda a prevenir vulnerabilidades conocidas que podrían ser explotadas para configurar redes no autorizadas.

- Realice auditorías de seguridad: Realice auditorías periódicas de seguridad de la red para identificar posibles vulnerabilidades y asegurarte de que se están siguiendo las políticas establecidas.

Al implementar estas medidas, puede reducir significativamente el riesgo de que se establezcan redes Wi-Fi no autorizadas en su organización y mantener un entorno de red más seguro.

Portal hotspot inseguro.

Para configurar un punto de acceso EAP115 para que no permita clonadas de MAC, siga estos pasos:

- Conecta tu computadora al EAP115 usando un cable Ethernet.
- Asegúrese de que su computadora esté configurada para obtener una dirección IP automáticamente a través del protocolo DHCP.
- Abre un navegador web en tu computadora e ingresa la dirección IP predeterminada del EAP115 en la barra de direcciones. Por lo general, la dirección IP predeterminada es 192.168.0.1, pero verifique el manual del EAP115 por si hay alguna diferencia.
- Inicia sesión en la interfaz de administración del EAP115 utilizando las credenciales de administrador. Si no ha cambiado las credenciales, es posible que encuentre la información predeterminada en el manual del dispositivo.

- Una vez que haya iniciado sesión, busque la configuración de seguridad inalámbrica o la configuración de control de acceso inalámbrico.
- En esta configuración, busca la opción "Filtrado de direcciones MAC" o algo similar.
- Habilita el filtrado de direcciones MAC.
- Ahora, debe configurar la lista blanca de direcciones MAC permitidas. Ingresa las direcciones MAC de los dispositivos que deseas permitir que se conecten al EAP115.
- Guarde los cambios realizados en la configuración.
- Desconecta el cable Ethernet que conecta tu computadora al EAP115 y reinicia el dispositivo.
- A partir de este punto, el EAP115 solo permitirá que los dispositivos con direcciones MAC se especifiquen en la lista blanca se conecten a él. Las direcciones MAC no autorizadas estarán bloqueadas.

Hay que tener en cuenta que los pasos pueden variar ligeramente según el firmware o la versión del dispositivo. Siempre es recomendable consultar el manual del usuario o ponerse en contacto con el soporte técnico del fabricante si tiene alguna duda específica sobre la configuración de su punto de acceso EAP115.

Cliente intentando conectar a red insegura.

Evitar redes Wi-Fi abiertas y desconocidas: Las redes Wi-Fi abiertas y no seguras, como las que se encuentran en cafeterías, aeropuertos o lugares públicos, suelen ser un objetivo fácil

para los ciberdelincuentes. Intente utilizar siempre redes Wi-Fi seguras y confiables, preferentemente protegidas con cifrado WPA2 o superior.

Uso de una conexión VPN: Si necesita acceder a una red no segura, es altamente recomendable utilizar una conexión VPN (Red Privada Virtual). Una VPN cifrará tu tráfico y establecerá una conexión segura entre tu dispositivo y el servidor VPN, protegiendo así tus datos de posibles interceptaciones.

Actualizar y proteger tus dispositivos: Mantén tus dispositivos (teléfonos, computadoras portátiles, tabletas, etc.) actualizados con las últimas actualizaciones de software y parches de seguridad. También asegúrese de tener un software de seguridad confiable instalado, como un antivirus o un firewall personal.

Evite introducir información confidencial: No ingreses confidencial, como contraseñas, números de tarjetas de crédito u otra información sensible, mientras estés conectado a una red no segura. Si es absolutamente necesario, utilice una conexión segura a través de HTTPS o una red de confianza.

Configurar conexiones automáticas: Deshabilita la configuración de conexión automática en tus dispositivos para evitar que se conecten automáticamente a redes no seguras sin tu conocimiento. Esto te dará mayor control sobre las redes a las que te conectas.

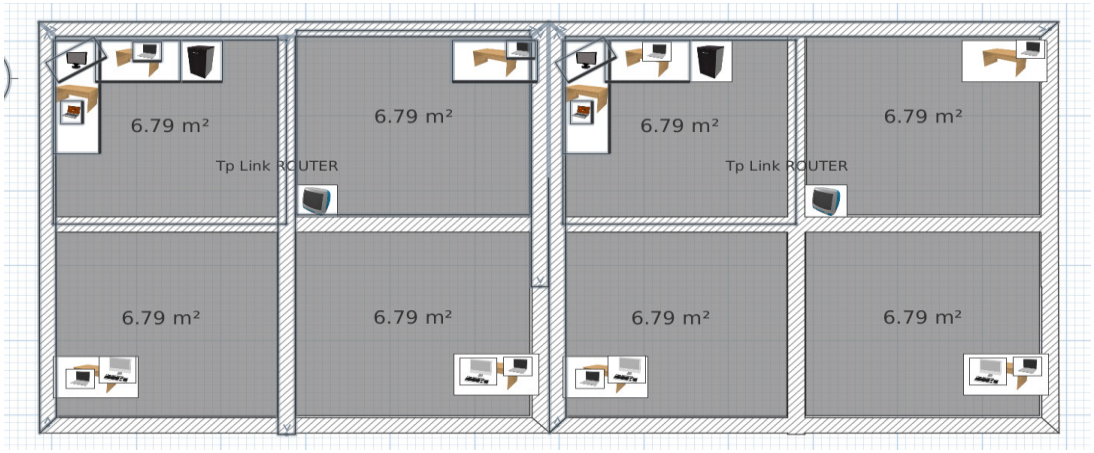
Utilizar autenticación de dos factores (2FA): Donde sea posible, habilita la autenticación de dos factores en tus cuentas en línea. Esto tendrá una capa adicional de seguridad y dificultará que los atacantes accedan a tus cuentas incluso si obtienen tu contraseña.

Rango de cobertura de la red demasiado extenso.

En caso de que se duplicara el espacio/dispositivos a los cuales se debería proveer con servicios/señal, considerando el material de las paredes (que en Ecuador por lo general son sólidas ladrillo/concreto), lo más recomendable seria instalar dos (2) dispositivos/routers con parámetros muy similares al primer caso, pero con 2 canales distintos bajo el mismo (con el fin de garantizar conectividad) automática en caso de que los dispositivos se muevan de un extremo a otro/cobertura.

Figura 89

Diagrama de espacios con dispositivos interconectados mediante red inalámbrica.



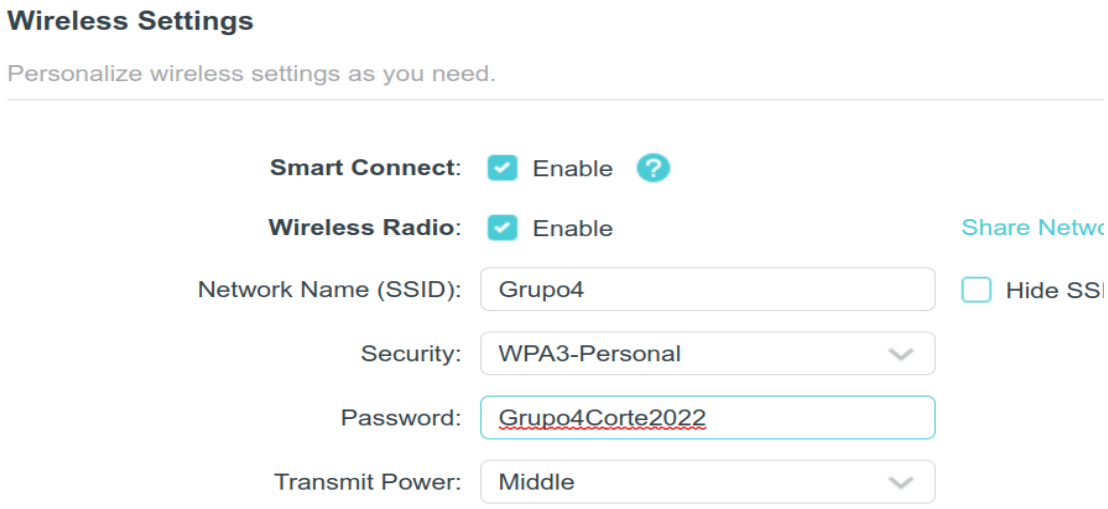
Como podemos observar para mejorar el servicio/cobertura sin necesidad de overlaping o demasiada cobertura, se puede configurar 2 dispositivos, pero en los dos realizar los siguientes cambios:

- Activar Smart Connect**:** Esto permite que la conexión entre dispositivos no sea notoria (no se interrumpa la conexión) y permite que tanto las bandas 2.4GHz & 5GHz trabajen/broadcasting de manera independiente, pero bajo un mismo nombre, por lo que no se necesita 2 claves diferentes.

- Wireless Radio: Activo lo que hace es que permite al dispositivo conectarse/computador a la señal más rápida (por lo general más cercana) con el afán de que la velocidad de los servicios sea la más optima.
- Seguridad: WPA3-Personal para evitar los ataques de diccionario que tan eficaces son con los protocolos WPA & WPA2, WPA3 debido a la implementación de dragonfly handshake este tipo de ataques no resultaría efectivo en WPA3, pero en caso de que un router utilice una combinación de (WPA3 & WPA2) sería posible realizar un ataque de downgrade, en cual se fuerza al router a utilizar WPA2 únicamente (como quedó demostrado).
- Algo que debemos observar muy detalladamente es la utilización de claves muy complejas (y cambiarlas frecuentemente) ya que con esto estaríamos haciendo el trabajo de un atacante más demandante/largo para romper/hallar la clave correcta.

Figura 90

Configuración de Router (TP-Link) con modo Wireless Radio.



Finalmente, lo más común/frecuente es utilizar un inhibidor de señales en ciertos puntos, como perímetros físicos/limítrofes para evitar que las señales sean absorbidas por dispositivos fuera del perímetro, pero esta idea no siempre es la mejor ya que al suprimir una de las frecuencias o las dos (2.4GHz & 5GHz), estaremos invalidando otros servicios como lo son la apertura de autos atreves del control remoto (ya que esta viaja por frecuencias generalmente dentro del espectro 2.4GHz también), controles remotos, teléfonos inalámbricos etc.

BIBLIOGRAFÍA

Airmon-ng [Aircrack-ng]. (9 de febrero de 2022). Recuperado el 28 de mayo de 2023, de aircrack-ng.org: https://www.aircrack-ng.org/doku.php?id=airmon-ng

Andrews, L. (4 de Noviembre de 2019). *Domain 3 - Security Engineering and Architecting*. Recuperado el 28 de mayo de 2023, de infosectests: https://infosectests.com/cissp-study-references/domain-3-security-engineering-and-architecting/

Berghel, H., y Uecker, J. (2005). WiFi attack vectors. *Communications of the ACM*, 21-28.

CISCO. (8 de Julio de 2021). *What is Wi-Fi Security? Cisco*. Obtenido de CISCO: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html

Crespo, J. P. (2005). Envenenamiento ARP. *blackspiral.org*, 1-4.

Fernández-Oliva Madrigal, M. E. (2020). Vulnerabilidades en redes Wifi.

Fluhrer, S. M. (2001). Weaknesses in the key scheduling algorithm of RC4. *Selected Areas in Cryptography: 8th Annual International Workshop*, 1-24.

Garcoaz, M. (9 de Marzo de 2019). *EAP-PEAP with Mschapv2: Decrypted and Decoded - Cisco*. Recuperado el 28 de mayo de 2023, de community cisco: https://community.cisco.com/t5/security-blogs/eap-peap-with-mschapv2-decrypted-and-decoded/ba-p/3106761

Ghimiray, D. (26 de Agosto de 2022). *¿Qué es el WPA2 (Acceso Protegido inalámbrico 2)?* Obtenido de AVG: https://www.avg.com/es/signal/what-is-wpa2

Guia de seguridad en redes wifi. (2019). Recuperado el 28 de mayo de 2023, de incibe: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

Hadi, T. H. (2022). Types of Attacks in Wireless Communication Networks. *Webology*, 718-728.

Horowitz, M. (2021). *WPS - WiFi Protected Setup*. Recuperado el 28 de mayo de 2023, de RouterSecurity.org: https://routersecurity.org/wps.php

Is WPA2 Security Broken Due to Defcon MS. (s.f.). Recuperado el 28 de mayo de 2023, de Revolution Wi-Fi: http://revolutionwifi.blogspot.com/2012/07/is-wpa2-security-broken-due-to-defcon.html

MS-chapv2, widely used in WPA2 enterprise, broken (more so than we thought)? (1 de agosto de 2012). Obtenido de wire.less: https://wire.less.dk/?p=190

Neagu, C. (20 de Enero de 2020). *How to use WPS in Windows 10 to connect to Wi-Fi Networks*. Obtenido de Digital Citizen: https://www.digitalcitizen.life/how-connect-windows-10-devices-wireless-networks-using-wps/

Paspuel, M. (28 de Diciembre de 2018). *Hack de Redes Wireless con Aircrack-ng*. Obtenido de nexoscientificos.vidanueva.edu.ec: https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/20

Security | Wi-Fi Alliance. (s.f.). Recuperado el 28 de Mayo de 2023, de wi-fi.org: https://www.wi-fi.org/discover-wi-fi/security

Tafur Bardales, C. L. (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.

Tews, E. W. (2007). Breaking 104 bit WEP in less than 60 seconds. *Information Security Applications: 8th International Workshop*, 188-202.

WeLiveSecurity. (16 de octubre de 2017). *WPA2 security issues pose serious wi-fi safety questions*. Obtenido de welivesecurity: https://www.welivesecurity.com/2017/10/16/wpa2-security-issues-pose-serious-wi-fi-safety-questions/

What is a captive portal and why is it essential for your network. (s.f.). Recuperado el 28 de mayo de 2023, de tp-link.com: https://www.tp-link.com/ca/blog/417/what-is-a-captive-portal-and-why-is-it-essential-for-your-network-structure-/

What Is a Hotspot? - WiFi Hotspot Definitions and Details. (s.f.). Recuperado el 28 de mayo de 2023, de Intel: https://www.intel.com/content/www/us/en/tech-tips-and-tricks/what-is-a-hotspot.html

What Is DNS Tunneling? (s.f.). Recuperado el 28 de Mayo de 2023, de Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Wind River Software | Safe, Secure, Reliable. (s.f.). Recuperado el 28 de mayo de 2023, de windriver: https://www.windriver.com/