ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES PRESENTES EN REDES SIN HILOS CORPORATIVAS

EDWIN ALFREDO MOLINA SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES PRESENTES EN REDES SIN HILOS CORPORATIVAS

EDWIN ALFREDO MOLINA SANCHEZ

Monografía como opción de grado para optar el título de
Esp. En Seguridad Informática

Director del proyecto:

EDILBERTO BERMUDEZ PENAGOS
Esp. Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 02 de noviembre del 2020.

DEDICATORIA

El presente documento es dedicado a Dios sobre todas las cosas y a mi familia de primer grado, conformada por mis padres, hermana, sobrina y pareja que son el eje y el apoyo incondicional para alcanzar todas mis metas propuestas, a nivel académico y personal. Igualmente, un agradecimiento especial a mis amigos, que han sido parte importante en dicho proceso, desde el aspecto motivacional y de apoyo.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AES: esquema de cifrado de bloques utilizado en la criptografía simétrica.

APs: puntos de acceso inalámbricos.

ARP: protocolo de resolución de direcciones, cuyo objetivo es determinar la dirección de Hardware *MAC* de una *IP* especifica.

BUGS: error de software que desencadena respuestas o resultados indeseados

CPU ACL: listas de control de acceso que contienen los permisos de tráfico de entrada o salida y almacenadas en una controladora inalámbrica.

CRC: son errores de comprobación de redundancia cíclica generados por la no coincidencia de los valores de un paquete.

DMZ: zona desmilitarizada, red ubicada entre la red interna y externa a una organización y que expone publicaciones o servicios de la red corporativa por medio de internet.

DOT1X/ 802.1X: es una norma de control de accesos que se basa en puertos y permite establecer una conexión punto a punto más segura a nivel de autenticación.

EAP: protocolo de autenticación extensible que trabaja bajo métodos arbitrarios como certificados, tarjetas inteligentes, etc.

EAP-MS-CHAP V2: método de autenticación mutua, basado en una contraseña.

EAP-TLS: tipo de protocolo *EAP* que utiliza certificados y proporciona métodos de autenticación y claves más robustas.

ESSID: servicio de identificador de red extendido, identificador de la red inalámbrica.

EXPLOITS: programa o código que se aprovecha de vulnerabilidades de seguridad sobre *software* o *hardware* para sacar algún beneficio.

FAST SSID: funcionalidad que permite movilidad entre redes inalámbricas de manera rápida, sin afectar disponibilidad de servicio.

FINGERPRINTING: etapa de *pentesting*, que consiste en recolectar información pública de una organización.

FOODPRINTING: etapa de *pentesting*, que consiste en recolectar información directa de una organización.

HALF-OPENING: método de escaneo utilizado por *zenmap* para determinar si un puerto está abierto, trabaja enviando paquetes de sincronización para iniciar una comunicación, sin necesidad de establecer la comunicación completa

HANDSHAKE: es un establecimiento de comunicación, denominado en el ámbito informático, como comunicación de las 3 vías, puesto que se envía una solicitud de sincronización, se responde, y el solicitante la establece.

HIJACKING: técnica en el ámbito informático utilizada por un atacante que consiste en robar.

HTTPS: es un protocolo de transferencia de hipertexto seguro.

IDS: sistema de sensores virtuales que permiten la detección de intrusiones.

IPS: sistema de sensores virtuales que permiten la prevención de intrusiones, bajo controles de accesos que se actualizan con una base de datos contra intrusos.

MAC: identificador de hardware único de un dispositivo de una red.

NPS: servidor de políticas de red.

NTP: protocolo de tiempo de red, que hace uso del internet para sincronizar los relojes de los sistemas informáticos.

PEAP: protocolo de autenticación extensible protegido, trabaja bajo la encapsulación del *EAP* sobre un túnel de capas.

PENTESTING: pruebas de penetración que se le realizan a los sistemas informáticos para identificar falencias de seguridad.

PHISHING: técnica de robo de información informática por medio de suplantación y engaño.

RADIUS: es un protocolo de autenticación y autorización remoto para permitir el acceso a aplicaciones de acceso a la red.

RC4: Sistema de cifrado de flujo bajo operaciones lógicas OR byte a byte

ROUTER: dispositivo encargado de establecer una ruta de los paquetes dentro de una red.

SWITCH: dispositivo de red que permite la interconexión de dispositivos permitiendo formar una red de área local.

SITE SURVEY: encuesta de sitio o inspecciones del área donde se va implementar una actividad para su posterior diseño u estimación.

SNMP: protocolo simple de red perteneciente a la capa de aplicación que permite mostrar información de administración entre dispositivos de red.

SSH/SECURE SHELL: programa y protocolo que implementa el acceso remoto seguro a un servidor o elemento de la red.

SSID: secuencia de octetos identificadores de una red inalámbrica.

TCP SYNC: peticiones de sincronización bajo paquetes *TCP.*

VULNERABILIDAD: debilidad de un sistema o tecnología informática que se puede explorar con deferentes fines de ataque, robo u extracción de información.

WARDRIVING: búsqueda de redes inalámbricas realizadas desde un vehículo en movimiento.

WIRESHARK: analizador de protocolos que permite dar identificación, análisis y solución a problemas en las redes de comunicaciones.

ZENMAP: herramienta que permite la exploración de una red determinando sus equipos y servicios ofrecidos.

RESUMEN

Se realizó un estudio que permitió determinar y analizar las diferentes vulnerabilidades de seguridad que se presentan sobre las redes sin hilos corporativas, con el objetivo de resaltar la importancia de realizar un buen aseguramiento en este tipo redes que hacen parte de la base que soporta la infraestructura tecnológica de una compañía.

Para la obtención de las vulnerabilidades de seguridad que amenazan a las redes sin hilos, se realizó una investigación sintética y se utilizó como evidencia un caso práctico empresarial, en el que se determinaron huecos de seguridad concurrentes en este tipo de redes inalámbricas, de manera adicional, este documento presentó un análisis de las diferentes redes sin hilos que se utilizan en las compañías, su composición, funcionamiento, diseños y mecanismos de seguridad.

Es importante resaltar que las redes inalámbricas facilitan las operaciones en las compañías respecto al uso de las redes locales cableadas, permitiendo la conectividad a usuarios y dispositivos que no disponen de un lugar fijo, pero dicha facilidad de conexión y su comunicación con las redes públicas, dan origen a vulnerabilidades en la seguridad que pueden ser aprovechadas por terceros, amenazando los pilares fundamentales de la seguridad informática y facilitando así: el acceso a información confidencial, accesos a dispositivos no autorizados e inclusive el robo y manipulación de información.

Es así que finalmente el documento incluye recomendaciones y alternativas para garantizar el aseguramiento sobre los dispositivos que administran e intervienen en las redes sin hilos corporativas con el objetivo de que las compañías no sean blanco fácil de las amenazas latentes y de terceros con objetivos malintencionados.

Palabras Clave: Vulnerabilidades, conectividad, redes sin hilos, aseguramiento, encriptación, suplantación, *MAC*, *Pentesting, test surveys,* Protocolos de Seguridad, *WMAN, WLAN*, Puntos de Acceso

ABSTRACT

A study was carried out that allowed determining and analyzing the different security vulnerabilities that arise on corporate wireless networks, with the aim of highlighting the importance of making a good assurance in this type of networks that are part of the base that supports the infrastructure technology of a company.

In order to obtain the security vulnerabilities that threaten wireless networks, a synthetic investigation was carried out and a business case study was used as evidence, in which concurrent security gaps in this type of wireless networks were determined, in addition This document presented an analysis of the different wireless networks used in companies, their composition, operation, designs and security mechanisms.

It is important to highlight that wireless networks facilitate operations in companies regarding the use of local networks, allowing connectivity to users and devices that do not have a fixed location, but such ease of connection and communication with public networks give rise to to security vulnerabilities that can be exploited by third parties, threatening the fundamental pillars of computer security and thus facilitating: access to confidential information, access to unauthorized devices and even theft and manipulation of information.

Thus, finally, the document includes recommendations and alternatives to guarantee the security of the devices that manage and intervene in corporate wireless networks so that companies are not easy targets of latent threats and third parties with malicious objectives.

Keywords: Vulnerabilities, connectivity, wireless networks, assurance, encryption, impersonation, MAC, Pentesting, test surveys, Security Protocols, WMAN, WLAN, Access Points.

INTRODUCCIÓN

La implementación de las redes inalámbricas en las empresas, nace de la necesidad inherente de permitir la conectividad a los usuarios sin acudir a gastos de recursos físicos adicionales en comparación con la implementación de una red cableada. El despliegue de dichas redes sin hilos en las compañías ha aumentado de manera considerable tras el lanzamiento de nuevos equipos y tecnologías inalámbricas que permiten alcanzar un rendimiento óptimo de conectividad, aun así, cabe destacar que estas redes cuentan con brechas diferenciales a nivel de conectividad y seguridad en comparación con las redes cableadas.

En el proceso de implementación de las redes sin hilos en las compañías, dado su enfoque y aparente facilidad de configuración inicial, se descuidan múltiples factores de *hardening* (endurecimiento de plataformas o sistemas informáticos) que debiesen ser garantizados con el objetivo de proteger los pilares fundamentales de la seguridad informática. Por consiguiente, la presente monografía “ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES PRESENTES EN LA REDES SIN HILOS CORPORATIVAS” permite concientizar a los administradores de telecomunicaciones acerca de la relevancia que tiene el aseguramiento de las redes en las organizaciones, así mismo, identificar aquellos aspectos que exponen la seguridad de una red sin hilos corporativa.

Para ello, la monografía se organiza de la siguiente manera: una primera parte con Conceptos y generalidades, en la que se documentan las diferentes estructuras que tienen las redes sin hilos corporativas, en cuanto a los elementos que la componen y los parámetros de seguridad establecidos para sus diferentes modos de operación. También se explican las diferentes tipologías de redes corporativas y las vulnerabilidades de seguridad más comunes presentadas por errores de diseño y fallas de aseguramiento.

Una segunda parte que cuenta con la Identificación de vulnerabilidades y un *Pentesting* (Pruebas de penetración) sobre un caso práctico**,** en la que se documentan las pruebas de vulnerabilidades realizadas sobre una red inalámbrica destinada a los invitados, esta red fue creada con el objetivo de dar acceso a internet al personal externo de una compañía. Implementada sobre una ***WMAN (Wireless***

Man Area Network- Red Inalámbrica de Área Metropolitana*)**, cuya composición de red fue diseñada y parametrizada bajo la unión de dos redes ***WLAN (Wireless Lan Area Network- Red Inalámbrica de Área Local) que proveen un clúster, permitiendo una alta disponibilidad de servicio y redundancia a fallas, asimismo la red corporativa de invitados se configuró sobre una controladora inalámbrica *WLC* (*Cisco Wireless Lan Controller* 2504).

La configuración realizada demuestra las falencias de aseguramiento que presenta una red sin hilos que carece en su diseño inicial de unos buenos parámetros de seguridad, encriptación, autenticación, conectividad y accesos. Finalmente, identificadas las falencias de seguridad, se generaron unas recomendaciones destacadas por *Best Practices* de *Cisco* y se activaron algunos mecanismos de seguridad que permitieron el aseguramiento de la plataforma inalámbrica. Dichas implementaciones y recomendaciones deben ser aplicadas al momento inicial del diseño y despliegue de las redes inalámbricas empresariales.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

Las redes inalámbricas facilitan la conectividad en el entorno empresarial, aun así, estas redes son el foco de una lucha incesante contra hackers y terceros mal intencionados que buscan de manera permanente escuchar, inspeccionar y descifrar los métodos de encriptación usados para obtener beneficios propios. Estos continuos ataques vectorizados hacia las redes inalámbricas y cuyo causante principal es el radio de propagación, permiten dejar al descubierto vulnerabilidades sobre los protocolos de seguridad, comprometiendo así la seguridad de las redes corporativas y llevando a la creación de protocolos y dispositivos más robustos para la comunicación y autenticación hacia la red.

Méndez[1] indica que, en el año 2001 *Fluhrer* investigadores y analistas de criptografía, descubrieron múltiples vulnerabilidades en el algoritmo *RC4* (*rivest cipher*), utilizado por el protocolo *WEP* (Wired Equivalent Privacy), que permitían el acceso rápido a las redes *WI-FI* (*Wireless Fidelity*), por consiguiente y de manera provisional en pro de dar respuesta a la inseguridad del protocolo *WEP*, nace en 2003 un protocolo de transición denominado *WPA* (*Wi-Fi Protected Access*), cuyo sistema de algoritmos brindó mayor seguridad en las empresas que hacían uso de las redes inalámbricas. A finales del año 2004 se estableció el protocolo *WPA* 2 cuyo algoritmo *AES* (*Advanced Encryption Standard*) proporciona robustez en la encriptación. En 2018 se da lanzamiento al protocolo *WPA3*.

Aunque se creen medidas de aseguramiento por parte de la *WI-FI Alliance,* organización encargada de promover las tecnologías inalámbricas mediante estándares con el objetivo de salvaguardar las redes, y a pesar de que son la vanguardia en la creación de los múltiples protocolos de encriptación lanzados para brindar mayor seguridad en las redes sin hilos, estos protocolos finalmente han sido vulnerados, incluyendo el protocolo mas reciente, *WPA3*.

[1] MENDEZ MORENO, Wilmer Antonio; MOSQUERA PALACIOS, Dairin y RIVAS TRUJILLO, Edwin. WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform. Tecnura, vol.19, n.spe, 2015, 9p. [En Linea]. [Consultado el 11, marzo, 2020]. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007&lng=en&nrm=iso.

De manera adicional, existen vulnerabilidades que se despliegan debido a las configuraciones creadas para activar funcionalidades de servicio. Una de las configuraciones existentes e inseguras de las redes corporativas se genera a la hora de activar los portales cautivos, puesto que los sistemas de portales creados por las organizaciones para permitir el acceso a internet a usuarios externos bajo una conexión regulada, pueden generar vulnerabilidades de seguridad explotables por falta de un buen diseño y robustecimiento de la configuración. En la creación de los portales se definen 2 partes diferenciadas que permiten el acceso y la navegación, una parte pública que permite a los nodos la conexión de cualquier terminal y una privada que debe ser regulada por un sistema de autenticación y aseguramiento que impide o no la navegación a internet y a la red corporativa.

Debido a las características de los portales cautivos, la conexión entre el *AP* y el cliente, no está cifrada, motivo por el cual existe la posibilidad de capturar el tráfico de las conexiones a la zona privada e implementar ataques de tipo *spoofing* (suplantación de identidad) o *hijacking* (secuestro informático), una vez conseguida la clave o *token* (firma cifrada) de ingreso.

1.2 FORMULACIÓN

Siendo identificadas las múltiples vulnerabilidades presentadas por los protocolos de encriptación en las redes sin hilos y en los sistemas de acceso cautivo, la pregunta central de esta monografía es ¿Cómo prevenir las vulnerabilidades de seguridad en una red corporativa sin hilos y asegurar las plataformas inalámbricas, minimizando futuros riesgos en las empresas que cuenten con estos sistemas de comunicación?

1.3 DESCRIPCIÓN

El despliegue de una red inalámbrica conlleva retos que inician desde la implementación de *test surveys* (estudios de sitio), elección de protocolos de encriptación seguros, canales de comunicación, bandas de frecuencia y mecanismos alternativos de protección contra intrusiones de usuarios mal intencionados, evitando así los accesos de *rogues (APs* no autorizados), intrusión

de terceros y explotación de vulnerabilidades cuyo objetivo final es el ingreso a la infraestructura tecnológica corporativa por medio de la ejecución de procesos de *hack* (alteración informática)*,* que se aprovechan de huecos de seguridad presentes en las plataformas inalámbricas mal configuradas y diseñadas.

En el contexto de comunicaciones empresariales se cuenta con diferentes alternativas que permiten la comunicación entre usuarios internos y, adicionalmente proporcionan conectividad a usuarios externos. El método más común de conectividad a una red es ejecutado por medio del cableado, pero existen las redes inalámbricas como alternativa de conexión para algunos usuarios internos. Para la conectividad de los usuarios externos, comúnmente se habilitan sobre las plataformas inalámbricas la funcionalidad de un portal cautivo. Este último sistema, permite la autenticación y accesibilidad limitada y controlada. Para la implementación del portal se despliega un proceso de configuración directamente sobre la controladora inalámbrica que, bajo algunas directrices configuradas por el administrador de la plataforma, ejecuta las restricciones de acceso pertinentes a cada usuario.

Para el proceso de implementación de las *WLAN* (*Wireless Lan Area Network*- Red inalámbrica de área local) y difusión de sus *SSID* (*Service Set Identifier*- identificador de servicio inalámbrico) se realizan estudios de *test survey* con el objetivo de determinar la ubicación de los diferentes puntos de acceso, sin embargo, en este proceso de instalación no es común que se ejecuten métodos de análisis de seguridad e implementación de esquemas de protección lógicos y físicos, generando así una configuración de encriptación básica. Estas fallas de análisis y de diseño conllevan asimismo a la instalación de los puntos de accesos con una ubicación aleatoria, fallas que igualmente se repiten a nivel de configuración con la controladora inalámbrica y, debido a la falta de fundamentación en seguridad y diseño, se facilitan la generación de vulnerabilidades a las redes corporativas inalámbricas.

Con base en las características descritas para el despliegue de una red *WLAN* corporativa, es importante considerar las vulnerabilidades de seguridad promovidas por la implementación de una red inalámbrica insegura. Esta identificación de vulnerabilidades permite fundamentar el objetivo de realizar y generar recomendaciones de seguridad que permitan minimizar riesgos de seguridad en las empresas.

2. JUSTIFICACIÓN

Las configuraciones básicas a nivel de seguridad, los errores de diseño en el despliegue e implementación de los dispositivos y las redes inalámbricas, exponen la red en general a diferentes tipos de ataques como lo son: *Arp Spoofing* (suplantación del protocolo de resolución de direcciones)*, Mac Spoofing* (suplantación del identificador de dispositivos)*, DDoS* (*Distributed Denial of Service*- Denegación de servicios distribuida), *Wardriving* (búsqueda de redes en vehículos)*, Acces Point Spoofing* (suplantación de puntos de acceso inalámbricos) y otras metodologías de intrusión, según la finalidad y objetivo del atacante, vulnerando así los pilares fundamentales de la seguridad informática.

Es por ello la importancia de validar las vulnerabilidades que puedan presentar las empresas en el momento de diseñar, implementar y configurar las redes *WLAN, WMAN o WWAN* (*Wireless Wide Area Network*- Red inalámbrica de área extensa), igualmente es relevante validar la robustez en los parámetros de seguridad, como los métodos de encriptación y autenticación adecuados para las redes sin hilos, evitando la mayor exposición a nivel de seguridad, aun así, las redes inalámbricas corporativas, aunque consideradas en la actualidad robustas, presentan diferentes tipos de falencias debido a su mal diseño y optimización.

Una de estas fallas de aseguramiento que se pretende identificar en el análisis de vulnerabilidades planteado, son las conexiones realizadas por medio de los portales cautivos, ya que estos portales se generan con el fin de permitir la navegación a los usuarios externos y su funcionamiento está basado en la petición realizada por la terminal al elemento autenticador y autorizador dispuesto en la controladora inalámbrica.

La realización de un análisis de seguridad permite identificar las fragilidades y fallas comunes presentes en las compañías a causa de un erróneo diseño e implementación de las redes sin hilos, dicho análisis posibilita así la generación de un plan de acción que ayude al fortalecimiento de las infraestructuras tecnológicas, mejorando la seguridad informática y seguridad de la información de las organizaciones, teniendo en cuenta la importancia que tiene la red y cuyo principal objetivo se basa en soportar la infraestructura tecnológica.

Cabe destacar que no se pretenden abarcar todos los tipos de ataques y variantes existentes, pero sí dar un repaso inicial al análisis de las vulnerabilidades de

seguridad presentes en las empresas y al fortalecimiento de la infraestructura tecnológica bajo algunas condiciones reales que se pueden presentar por intentos de intrusión o ataques malintencionados por parte de personal externo a las organizaciones.

Es por ello por lo que se observa alta viabilidad del desarrollo de la monografía, generando una base de conocimiento para el contexto de la seguridad en las redes inalámbricas corporativas. Igualmente, este documento pretende entregar bajo las evidencias y pruebas argumentadas, mecanismos a los administradores e implementadores de las rede, que, de manera posterior, les permita realizar actividades de *hardening* bajo las recomendaciones descritas, mejorando así las prácticas de seguridad en las redes sin hilos con la implementación de protocolos y el uso de elementos y configuraciones de aseguramiento que se permitan en el despliegue de estas tecnologías inalámbricas. De manera posterior, la documentación realizada se puede utilizar como elemento guía para la continuación de estudios sobre las diferentes vulnerabilidades de seguridad que afectan las infraestructuras inalámbricas organizacionales.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las vulnerabilidades de seguridad en redes inalámbricas corporativas bajo la metodología NIST (SP800-115), para la generación de recomendaciones en el aseguramiento y salvaguarda de la seguridad informática en las organizaciones.

3.2 OBJETIVOS ESPECÍFICOS

- Recolectar la Información referente a las redes Inalámbricas, identificando así las vulnerabilidades de seguridad más comunes en las redes sin hilos corporativas.

- Indagar acerca de los mecanismos de seguridad utilizados para la implementación de las redes inalámbricas corporativas.

- Corroborar, a través de un *Pentesting,* las vulnerabilidades de seguridad generadas por errores de diseño y configuración de los sistemas de acceso por medio de portales cautivos en las redes inalámbricas corporativas.

- Documentar las vulnerabilidades de Seguridad de las redes inalámbricas corporativas, generando las recomendaciones de seguridad e identificando los riesgos consecuentes de la no aplicación de un buen aseguramiento.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Introducción a las redes inalámbricas. El avance, evolución e innovación de los equipos tecnológicos de comunicaciones y la implementación de estos para la unificación de las comunicaciones por medio de las nuevas tecnologías en las redes de datos es exponencial. Como lo indica Baran[2], es de resaltar la importancia y el papel que juegan las redes inalámbricas como opción de los sistemas de comunicación corporativa, puesto que permite disminuir los costos de implementación de una red, que, a diferencia de la cableada, incurre con altos costos de instalación.

En gran porcentaje de las compañías, las comunicaciones son un tema de alta importancia y trascendencia, por ende, con el fin de facilitar la comunicación a la totalidad de empleados o si es el caso personal invitado, como se mencionó anteriormente sin incurrir en gastos locativos de cableado, se buscan alternativas que puedan facilitar esta conectividad y es ahí donde son implementadas las redes sin hilos.

Las redes sin hilos o denominadas inalámbricas son redes que utilizan el espectro radioeléctrico como medio de transmisión, generando ondas magnéticas desde el transmisor hasta un receptor que tiene la capacidad de interpretación de las señales. Según Varela[3], indica que, debido a su naturaleza de servicio, el despliegue y utilización de este tipo de tecnología ha tenido un crecimiento notable y trascendental para las redes de comunicaciones en el hogar y las empresas.

Villagómez[4], advierte que las redes inalámbricas cuentan con ciertas ventajas debido a su menor complejidad de instalación con respecto a una red cableada, aunque bajo las características de velocidad y seguridad aún no tienen la capacidad

[2] BARAN, Nicolas. Redes Inalámbricas. Redes (Vol. 2). 2012. [En Línea]. [Consultado el 12, noviembre, 2019] Disponible en: http://www3.uah.es/vivatacademia/ficheros/n54/redesinalam.PDF

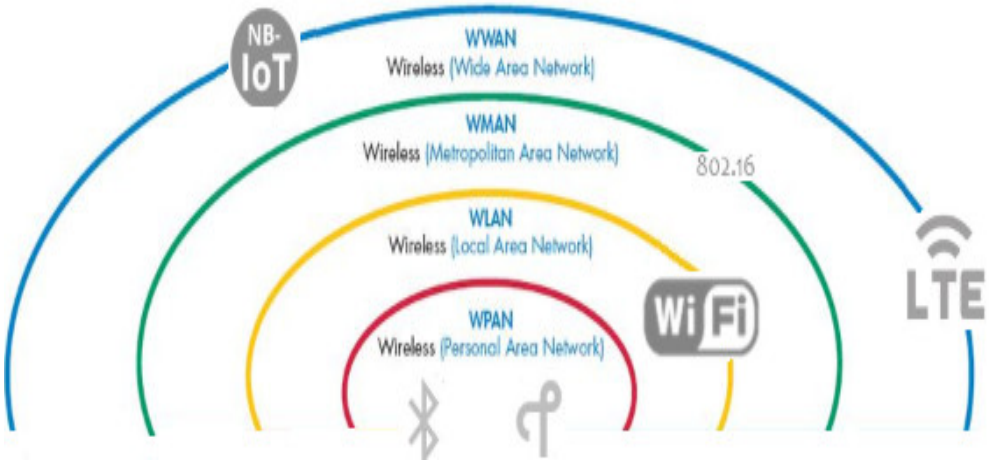
[3] VARELA, Carlos; DOMÍNGUEZ, Luis. Redes Inalámbricas. 2002. 18p. [En línea]. [Consultado el 25, junio, 2019]. Disponible en: http://www.blyx.com/public/wireless/redesInalambricas.pdf

[4] VILLAGÓMEZ, Carlos. Introducción a Wi-Fi (802.11 o WiFi). 2018. 8p. [En Línea]. [Consultado el 02, septiembre, 2019] Disponible en: http://es.ccm.net/contents/789-introduccion-awi-fi-802-11-o-wifi

de suplantar el rendimiento de una red de área local cableada *LAN*. Cardenas[5], destaca que las mayores ventajas cualitativas de las redes inalambricas se observan debido a sus características, que aumentan su importancia en el entorno corporativo y cambian las definiciones iniciales presentadas sobre una red, disminuyendo costos de movilización, implementación y administración centralizada.

Las redes sin hilos a nivel general son implementadas y categorizadas de acuerdo con múltiples factores en los que encontramos: objetivos, características, rangos de alcance, funcionalidades de uso y servicios a prestar. Baydal[6], indica que, dentro de las principales clasificaciones en el ámbito corporativo se destacan el cubrimiento y servicios que ellas prestan, por consiguiente, como se observa en la Figura 1, se realiza una descripción gráfica basada en sus alcances.

Figura 1. Clasificación de las Redes Inalámbricas



Fuente: El autor

[5] CARDENAS, Jose. Arquitectura de Redes Inalámbricas. 2019, 10p. [En Línea]. [Consultado el 17, agosto, 2019] Disponible en https://www.academia.edu/11940956/Arquitectura_de_Redes_Inalabricas

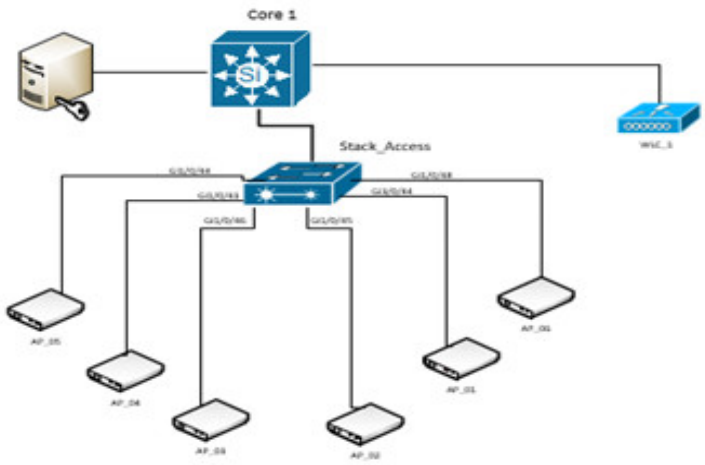
[6] BAYDAL CARDONA, María Elvira. Clasificación de las redes inalámbricas. 2018, 3p. [En línea]. [Consultado el 11, abril, 2019]. Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.4AAE4B49&lang=es&site=eds-live&scope=site

4.1.2 Clasificación de redes sin hilos corporativas según su cobertura y funcionalidades. Las redes sin hilos corporativas tienen diferentes clasificaciones y topologías según el uso específico y el área geográfica, comúnmente son categorizadas en base a la cobertura, en este sentido las describimos de la siguiente manera.

4.1.2.1 Red de Área Personal Inalámbrica - *WPAN.* Las coberturas de estas redes son bajas, por ende, son de uso personal comúnmente y tiene un alcance aproximado a los 10 metros. El *Bluetooth* o *RFID* (Radio Frequency Identification-Identificación por Radio Frecuencia), sin embargo, los sistemas de *RFID*, son utilizados en las organizaciones para el control y monitoreo industrial que, en conjunto con otras tecnologías de comunicación y transporte de datos, permiten aprovechar su uso en el sector industrial.

4.1.2.2 Red de Área Local Inalámbrica - *WLAN.* La red *WLAN* es un sistema de comunicación sin hilos flexible, siendo la principal alternativa para las redes de área local corporativa, dichas redes son descritas en la Figura 2. Según Arano[7], la tecnología *WLAN* tiene diferentes niveles de interoperabilidad, por los cuales los fabricantes de computadoras y dispositivos corporativos cuentan con tarjetas que tienen la capacidad de funcionar sobre con estas redes.

Figura 2. Red WLAN

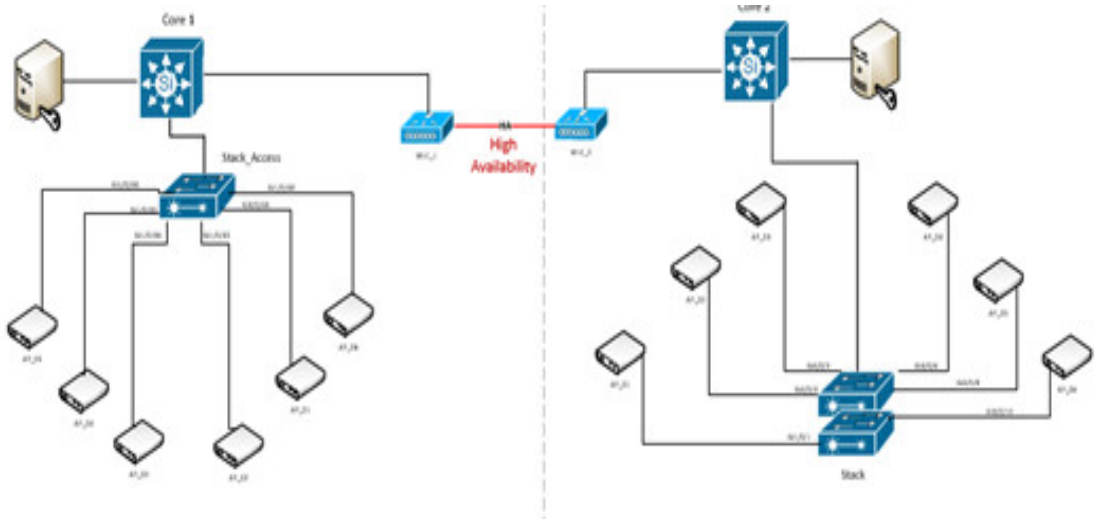


Fuente: El autor

[7] ARANO, Souta. Redes-inalambricas-lan. 2015, 12p. [En Línea]. [Consultado el 03, agosto, 2019] Disponible en: https://www.academia.edu/16611460/Redes-inalambricas-lan

4.1.2.3 Red de Área Metropolitana Inalámbrica – *WMAN*. La red *WMAN* es una red sin hilos que permite establecer conexiones entre distintas ubicaciones dentro de un área metropolitana. Además, es posible configurar las redundancias entre controladoras de tipo *WLAN* para generar un sistema *WMAN* de alta disponibilidad, Fan[8], describe como La principal tecnología de *WMAN*, *la WIMAX* (*Worldwide Interoperability for Microwave Access* - interoperabilidad mundial para acceso por microondas), sistema que presta servicios de altas velocidades repartidas en un rango de alrededor 50 kilómetros, es así que esta tecnología además de prestar servicios en grandes áreas, se caracteriza por conectar redes *WLAN* en grandes distancias. La Figura 3, ilustra la red *WMAN* utilizada en la monografía, bajo la configuración de dos redes de tipo *WLAN* que permiten crear alta redundancia y disponibilidad de servicio a la organización.

Figura 3. Red WMAN

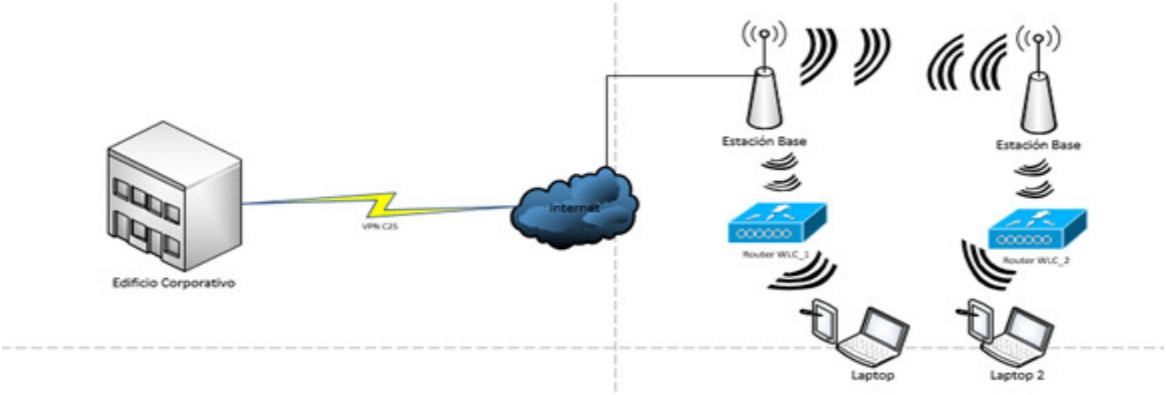


Fuente: El autor

[8] FAN, Yang; HUAIBEI, Zhou. An improved security scheme in WMAN based on IEEE standard 802.16. Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005, Wireless Communications, Networking and Mobile Computing, 1191. [2005. En línea]. [Consultado el 24, abril, 2019]. Disponible en https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/WCNM.2005.1544255

4.1.2.4 Red de Área Extendida Inalámbrica – *WWAN.* La red *WWAN* es un tipo de red sin hilos que permite una conexión inalámbrica a través de redes remotas públicas o privadas. Salazar[9], indica que su uso es muy común en proveedores de servicio bajo tecnología celular y satelital, por ende es muy poca su implementación para las empresas como red corporativa, sin embargo, con ayuda de otras herramientas como las *VPNs (Virtual Private Networks), C2S (Client to Site) y S2S (Site to Site)* se podría generar una conectividad completa a las compañías y hacer de estas un complemento para de la red de área local, la Figura 4, describe el uso de las redes *WWAN* para el uso corporativo.

Figura 4. Red WWAN



Fuente: El autor

4.1.3 Elementos que componen una red inalámbrica corporativa. Entre los cuales se encuentran los siguientes:

- ✓ **Adaptadores:** Marrugo[10], los define como los dispositivos encargados de interpretar la señal electromagnética generada por el transmisor inalámbrico. Teniendo como finalidad permitir la conexión a la red difundida, de manera transparente entre los puntos de accesos y el dispositivo final, la Figura 5, ilustra un adptador de red de una computadora.

[9] SALAZAR SOLER, Jordi. Redes inalámbricas. 2016, 3p. [En línea]. [Consultado el 23, abril, 2019]. Disponible en https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

[10] MARRUGO, Blanca; MARZOLA, Victor. REDES AD-HOC, INALÁMBRICAS Y SENSORIALES. 2008, 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0043203.pdf

Figura 5. Adaptador Inalámbrico

Fuente: PCCOMPONENTES. Startech Adaptador Tarjeta PCI Express PCIe de Red Inalámbrica N 802.11b/g/n 300Mbps, 2020, 1p. [En línea]. [Consultado el 23, abril, 2019]. Disponible en https://www.pccomponentes.com/startech-adaptador-tarjeta-pci-express-pcie-de-red-inalambrica-n-80211b-g-n-300mbps

- ✓ **Acces Points:** Los puntos de accesos son los encargados de retransmitir los datos entre la red cableada y administrada por las controladoras y soportan la conexión de los usuarios. Mena[11], documenta que en las redes inalámbricas corporativas se implementan múltiples *AP*s con la finalidad de realizar *handoff* (Traspaso de sistemas*)* al igual que lo realizan las celdas móviles, permitiendo movilización de usuarios sin perder la conectividad de un *AP* a otro, este dispositivo es ilustrado en la Figura 6.

Figura 6. Acces Point

Fuente: PCANDPARTS. Punto de acceso inalámbrico Cisco Aironet AP1815I. 2020, 1P. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://pcandparts.com/access-point/cisco-aironet-ap1815i-wireless-access-point/

[11] MENA. Network Components Wlan. 2018, 5p. [En línea]. [Consultado el 09, julio, 2019]. Disponible http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsgao&AN=edsgcl.553554213&lang=es&site=eds-live&scope=site

- ✓ **Controladora:** Dispositivo encargado de implementar y operar todos los elementos de la arquitectura de la red inalámbrica. Garg[12], documenta que este dispositivo además de almacenar la configuración de los puntos de acceso, en la actualidad cuenta con diferentes funcionalidades que permiten optimizar, analizar el tráfico, protegerlo antes amenazas y responder de manera inteligente a procesos de *handoff* y protección contra redes que se solapan y representan un problema de seguridad, la Figura 7 ilustra dos tipos de controladoras inalambricas comunes del fabricante CISCO.

Figura 7. Controladoras Inalámbricas

Fuente: CISCO. Cisco Access Point y selector de controlador inalámbrico. 2020, 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.cisco.com/c/en/us/products/wireless/access-point-controller-selector.htmlwireless

4.1.4 Seguridad de las redes inalámbricas corporativas. La facilidad de movilidad y difusión del *SSID* en las redes inalambircas, como lo indica Serrano[13], hace que las redes inalámbricas sean focos de ataques y posean mayor desventaja a nivel de control y seguridad con respecto a las redes cableadas. Al igual que en las redes cableadas se debe regular el uso al medio, evitando que más de un dispositivo realice envíos de *data* al mismo tiempo y produzca colisiones en la red, generando a su vez problemas de integridad y seguridad en las comunicaciónes.

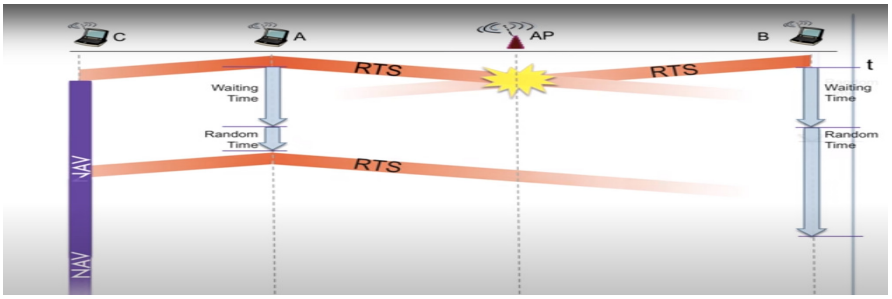
Con el objetivo de evitar estas fallas en la comunicación, se crearon los protocolos de acceso al medio. Para las redes inalámbricas se estableció el método *CSMA/CA* (acceso múltiple por detección de portadora y prevención de colisiones), cuya función es generar una contención basada en el acceso, controlando el acceso y

[12] GARG, Vijay K. Wireless Communications & Networking. Amsterdam: Morgan Kaufmann. 2007. [En línea]. [Consultado el 05, julio, 2019]. Disponible en https://www.academia.edu/19503445/Wireless_Communications_and_Networking

[13] SERRANO FLORES, Andrés Guillermo. Análisis de Vulnerabilidades de Seguridades en Redes Inalámbricas dentro un Entorno Empresarial que Utilizan Cifrado AES y TKIP, WPA y WPA2 Personal del DMQ, Quito, 2011, 3p. [En línea]. [Consultado el 14, julio, 2019]. Disponible en: http://repositorio.puce.edu.ec/bitstream/22000/4642/1/TESIS%20-%20PUCE%204479.pdf

envio de información desde los clientes hacia el punto de acceso, por medio de paquetes de control, que regulan el uso del canal como se evidencia en la Figura 8.

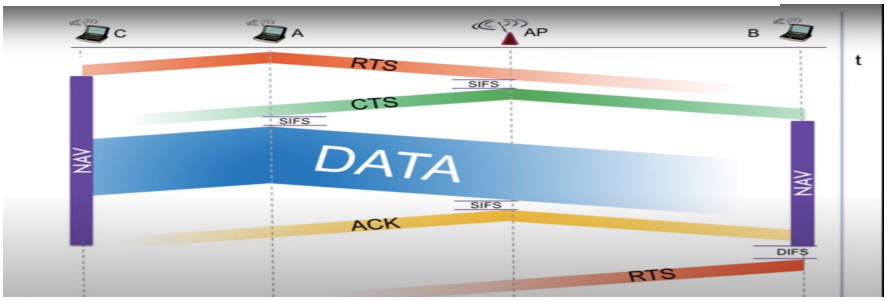
Figura 8. Inicio del protocolo *CSMA/CA*



Fuente: SLIDESERVE. Redes Inalámbricas Estándar 802.11. 2020, 27P. [En línea]. [Consultado el 30, octubre, 2020]. Disponible en https://www.slideserve.com/rad/redes-inal-mbricas-est-ndar-802-11

Debido a que los clientes envían los paquetes de requerimiento *RTS* y que pueden coindicidir en el mismo periodo de tiempo, el *AP* identifica este choque de solicitudes y no genera el *CTS* a los dispositivos, por consiguiente, los clientes esperan durante un periodo tiempo aleatorio y vuelven a intentar el envió del paquete *RTS*. Este proceso mencionado de evita las colisiones y continua con la generación de un paquete que confirma al primer cliente que realizo la solicitud, su disponibilidad. De manera posterior el cliente puede enviar la *data* y el punto de acceso confirma su recibido, este proceso se repite como se evidencia en la Figura 9.

Figura 9. Funcionamiento normal del *CSMA/CA*

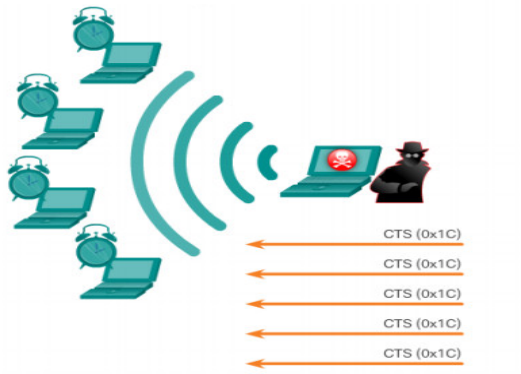


Fuente: SLIDESERVE. Redes Inalámbricas Estándar 802.11. 2020, 27P. [En línea]. [Consultado el 30, octubre, 2020]. Disponible en https://www.slideserve.com/rad/redes-inal-mbricas-est-ndar-802-11

En el ámbito de las redes corporativas, en donde las redes sin hilos en su gran mayoría hacen uso de un sistema controlador de los puntos de acceso, el flujo de control se repite, pero se añade a su escenario una capa de control entre la controladora inalámbrica y sus puntos de accesos, añadiendo así un estándar que permita realizar tunelización de la comunicación de manera ordenada, controlada y segura.

El uso de este protocolo de acceso al medio *CSMA/CA*, también es utilizado por atacantes malintencionados para volcar el objetivo inicial del protocolo a su favor, generando denegaciones de servicio bajo dos tipos de ataques conocidos y comunes de *DoS* como lo son: los ataques de des asociación de los clientes inalámbricos hacia una red que inducen al cliente a un intento de conexión cíclico sin éxito alguno. El otro ataque consta de una saturación de los mensajes de *CTS* hacia los clientes, Como es indicado por CAO[14], se da vía libre a todos los clientes inalámbricos para envíen sus transmisiones generando colisiones, que deniegan a su vez la comunicación como lo ilustra la Figura 10.

Figura 10. Ataque DoS con stauracion de CTS



Fuente: CCNA R&S. Seguridad en Redes Inalámbricas. 2019, 22P. [En línea]. [Consultado el 30, octubre, 2020]. Disponible en https://clementecervantesbustos.files.wordpress.com/2019/05/seguridad-en-redes-inalc3a1mbricas.pdf

[14] CAO, Bin; LI, Mengyang; ZHANG, Lei; LI, Yixin; PENG, Mugen. ¿Cómo afecta CSMA / CA el rendimiento y la seguridad en las redes inalámbricas de cadena de bloques, en *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, págs., 2020, doi: 10.1109 / TII.2019.2943694. [En Línea]. [Consultado el 30, octubre, 2020] Disponible en: https://www.researchgate.net/publication/336074053_How_Does_CSMACA_Affect_the_Performance_and_Security_in_Wireless_Blockchain_Networks

Para la mitigación de estos tipos de ataques existen estándares basados en la característica de protección de tramas de administración *MFP*, estándar originario del fabricante de CISCO, utilizado desde el IEEE 802.11i y la 802.11w, generando una protección completa control a la suplantación de las tramas, además existen algunos fabricantes como CISCO que bajo la firma de sus sistemas de *IPS* en las controladoras, permiten una detección anticipada, utilizando la comparación de firmas de los atacantes.

Con el objetivo de mitigar las fallas de seguridad de las redes inalambricas, relacionadas con integridad y confidencialidad, se crearon e implementaron los protocolos de seguridad *WEP, WPA/WPA2* y *WPA3* con algoritmos de encriptación que permiten cifrar la información y que en conjunto con cierto protocolos y estándares embedidos en los sistemas inalámbricos se salvaguardan las comunicaciones a nivel de autenticación, comunicación y acceso al medio.

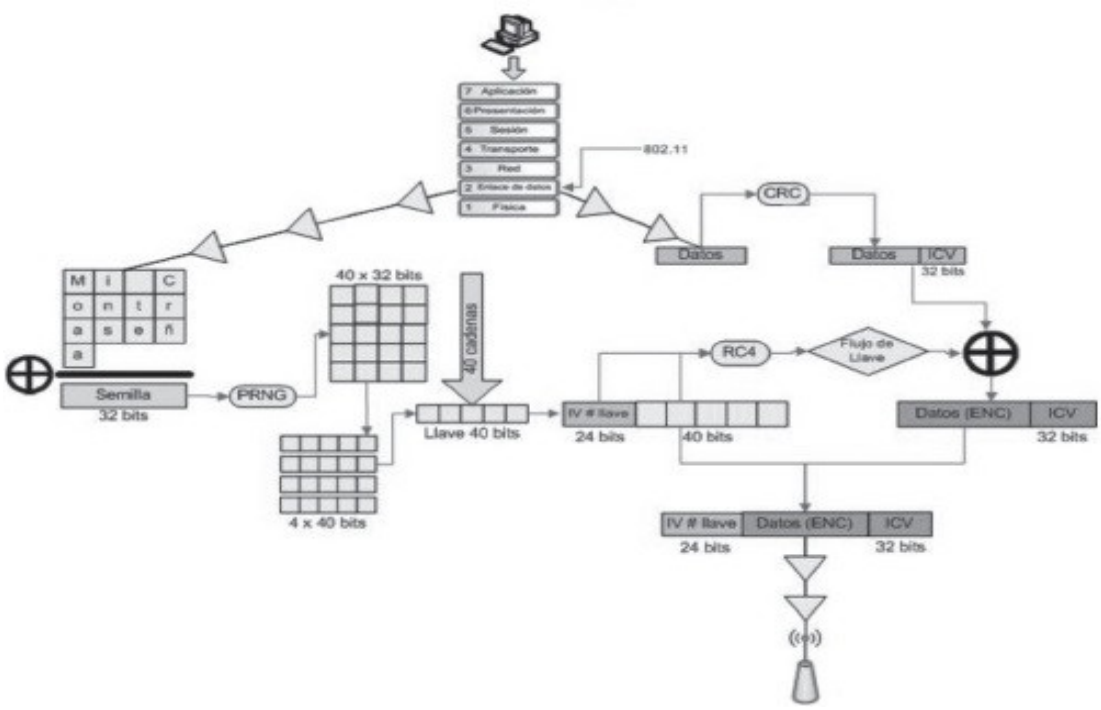
4.1.4.1 Protocolos de seguridad de las redes inalámbricas. Basado en la caracterización de amenazas y en la necesidad de cifrar los datos y las conexiones, la *IEEE* en conjunto con organizaciones como la *WIFI Alliance*, han desarrollado a través del tiempo los siguientes protocolos para redes inálambricas.

- ✓ ***WEP (Wired Equivalent Privacy).*** Protocolo de seguridad y encriptación de redes inalámbricas que debido a su vulnerabilidad a lo largo del tiempo se ha dejado de implementar, este protocolo genera un cifrado de un nivel bajo clasificado como 2, y se basa en un algoritmo *RC4*, su configuración utiliza claves de longitudes de 64 a 128 bits.

  Funcionamiento. Sistema de cifrado que trabaja mediante la autenticación del usuario con una contraseña. Lehembre[15], indica que su funcionamiento es aplicado sobre la capa *MAC* del sistema y utiliza el algoritmo *RC4+* la Clave Secreta, combinada con un vector de inicialización de 24 bits para encriptar el mensaje y el *checksum* (sumas de verificación). La Figura 11, describe paso a paso su proceso de funcionamiento.

[15] LEHEMBRE, Guillaume. Seguridad Wi-Fi – WEP, WPA y WPA2. 2006, 2p. [En Línea]. [Consultado el 29, octubre, 2019] Disponible en: http://index-of.co.uk/INFOSEC/Seguridad%20WiFi%20WEP%20WPA%20y%20WPA2.pdf

Figura 11. Proceso de funcionamiento WEP



Fuente: PAU OLIVA, Fora. Inseguridad en redes 802. 2003. 11p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://docplayer.es/9590765-In-seguridad-en-redes-802-11b-pau-oliva-pof-eslack-org-feb-2003.html

- ✓ ***WPA/WPA2 (Wireless Protected Access).*** Protocolo de seguridad robusto de redes sin hilos que surgió tras las vulnerabilidades presentadas por el *WEP.* Molina[16], indica que el protocolo *WPA* y *WPA2* en forma diferencial implementan el sistema *TKIP*, además de ser un protocolo que gestiona las claves dinámicas, permite diferentes sistemas de control como los son el *WPA-PSK (Wi-Fi Protected Access- Pre shared Key) y WPA Enterprise,* de manera adicional, como lo describe Filip[17], trabaja con el robusto algoritmo de cifrado *AES,* cuyo

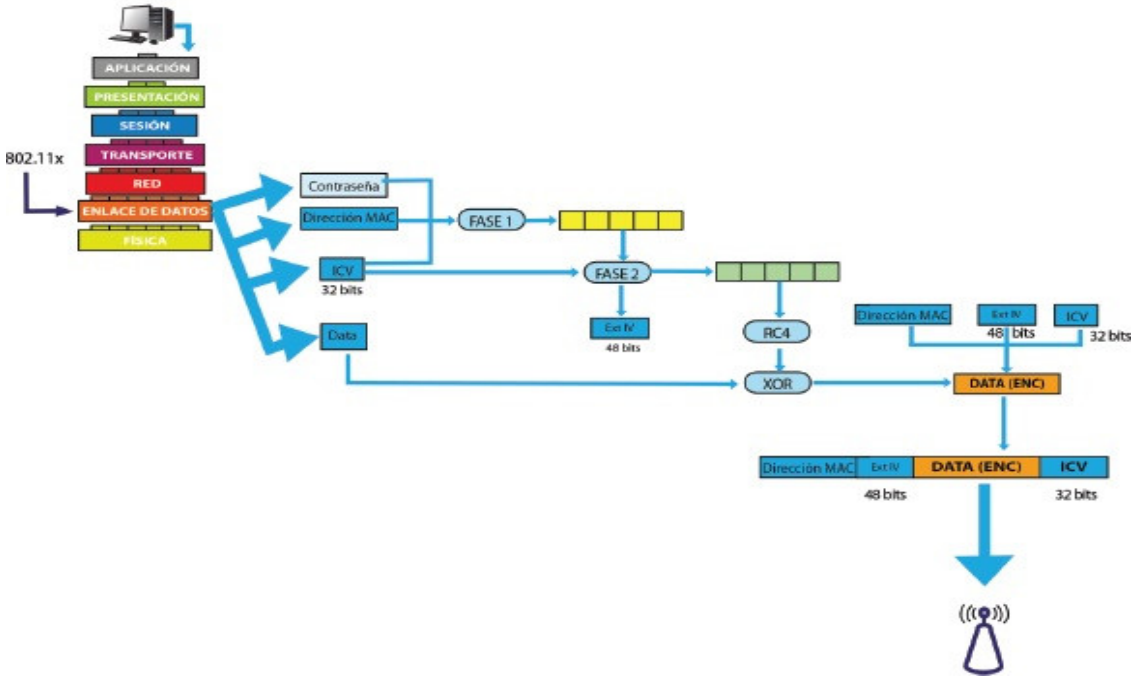
[16] MOLINA, Juan M. Seguridad en redes inalámbricas 802.11. Sistemas & Telemática, 1, 2006. pp. 13-28. [En Línea]. [Consultado el 10, enero, 2020] Disponible en: http://www.icesi.edu.co/contenido/pdfs/jamdrid-seguridad_redes_inalambricas.pdf

[17] FILIP, Andra; VÁZQUEZ TORRES, Estefania. Seguridad en redes WiFi Eduroam. 2010. 3p. [En Línea]. [Consultado el 15, noviembre, 2019] Disponible en: http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

esquema de seguridad esta basado en un cifrado en bloques que llego a ser adoptado por el gobierno americano

Funcionamiento. Este sistema trabaja mediante la autenticación del usuario con una contraseña, su funcionamiento es aplicado sobre la capa *MAC* del sistema. Panda Software[18], indica que el protocolo utiliza el algoritmo *AES* + la Clave Secreta combinada con un vector de inicialización de 24 bits, para encriptar el mensaje y el *checksum*. Cabe resaltar que *WPA2* a diferencia del protocolo *WPA*, contiene mejoras de los protocolos de 4 *way-handshake,* que permite que el punto de acceso, el elemento autrenticador, y el cliente puedan de manera independiente proporcionarse entre estos elementos la clave o la denominada *PSK* sin comprometer la confidencialidad de la misma, la Figura 12, describe paso a paso su proceso de funcionamiento.

Figura 12. Proceso de funcionamiento WPA y WPA2



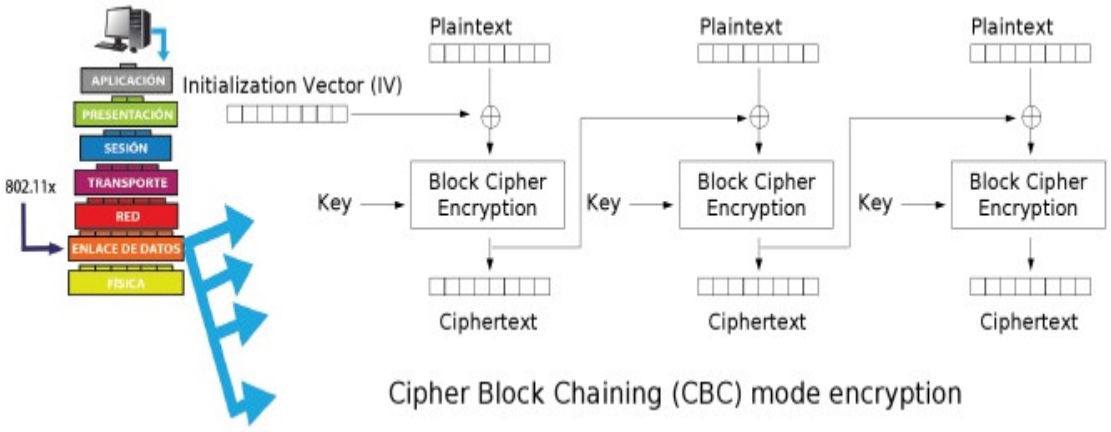
Fuente: PAU OLIVA, Fora. Inseguridad en redes 802. 2003. 11p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://docplayer.es/9590765-Inseguridad-en-redes-802-11b-pau-oliva-pof-eslack-org-feb-2003.html

[18] PANDA SOFTWARE INTERNATIONAL. Seguridad en Redes Inalámbricas. 2005, 5p. En línea]. [Consultado el 21, julio, 2019]. Disponible en: https://www.academia.edu/8604820/Seguridad_en_redes_Inal%C3%A1mbricas

- ✓ ***WPA3 (Wireless Protected Access).*** Es una tecnología sucesora de la *WPA2* y surgida en enero de 2018, desarrollada por la *Wi-Fi Alliance* como respuesta algunas vulnerabilidades identificadas y explotables en *WPA2* según indica Parras[19], *WPA3* surge como un protocolo de seguridad renovado que utiliza algunos algoritmos de encriptación más robustos, evitando facilidades en el criptoanálisis y ruptura de su seguridad.

  Funcionamiento. Esta nueva tecnología de seguridad inalámbrica cuenta con un cifrado de 128 bits en su versión *WPA3* Personal y de 192 bits en *Enterprise*, permitiendo así robustecerse ante los ataques de fuerza bruta, de manera adicional y entrando en el mundo del *IoT* (*Internet of Things* - Internet de las cosas), cuenta con sistemas de conexión llamados ***Wi-Fi Easy Connect*** permitiendo a dispositivos que no tienen la capacidad de digitar claves conectase por medio de los códigos *QR* (*Quick Response Code* - Código de rápida respuesta). la Figura 13, describe paso a paso su proceso de funcionamiento.

Figura 13. Funcionamiento WPA3



Fuente: Fuente: PAU OLIVA, Fora. Inseguridad en redes 802. 2003. 11p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://docplayer.es/9590765-In-seguridad-en-redes-802-11b-pau-oliva-pof-

[19] PARRAS CORRALIZA, Jose Luis. Redes WiFi: ¿realmente se pueden proteger?. 2018. 3p. [En línea]. [Consultado el 15, enero, 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73247/6/jcorralizaTFM0118memoria.pdf

4.1.5 Vulnerabilidades de redes inalámbricas corporativas. El concepto de vulnerabilidad en redes inalámbricas, como lo indica Chuquitarco[20], es determinado por las debilidades que el sistema presenta y la facilidad para violar los tres pilares fundamentales de la seguridad informática; Confidencialidad, integridad y disponibilidad, por medio de accesos no autorizados, modificación de datos e ingreso a aplicaciones.

Dichas vulnerabilidades son derivadas según Vallejo de León[21], de *bugs* (Errores de software) de los sistemas inalámbricos, así como fallos en el diseño e implementación de la tecnología, igualmente, existe el principio de que ningún sistema está al 100% seguro, debido algunas limitaciones de la misma tecnología. La Figura 14, presenta una descripción gráfica de un ataque a la red inalámbrica generada por vulnerabilidades de la tecnología.

Figura 14. Vulnerabilidad Inalámbrica

Fuente: TOOLWAR1. Kit de herramientas de análisis de implementaciones criptográficas: Framework.202. p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en http://toolwar1.rssing.com/chan-52947478/latest.php

[20] CHUQUITARCO, Mario; ROMERO, Mónica. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador Diagnosis of vulnerabilities in wireless networks at Ecuador, 3(2), 122–133. [En línea]. [Consultado el 11, enero, 2020]. Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3320/3/document%20%2811%29.pdf

[21] VALLEJO DE LEON, Tatiana. (2010). Vulnerabilidades Y Niveles De Seguridad De Redes WI-FI. Guatemala, 116p. Trabajo de grado (Ingeniera de Sistemas). Universidad de San Carlos. Facultad de Ingeniería. [En línea]. [Consultado el 27, julio 2019]. Disponible en: http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf

Por consiguiente, la definición de una red segura no existe, dado que no es posible garantizar la plena seguridad debido a las múltiples vulnerabilidades que trae consigo la evolución de la tecnología y actualizaciones de los servicios y plataformas, aun así, se pueden tomar precauciones que minimicen el impacto de las vulnerabilidades cuando se implementan dichas redes.

Según Ramirez[22], indica que las redes cableadas e inalámbricas son seguras o vulnerables de acuerdo al descuido o robustecimiento que se apliquen bajo los pilares establecidos de la seguridad informática, pilares definidos por la autenticidad, confidencialidad, disponibilidad e integridad de todos los elementos que componen la red.

No importa el tipo de configuración que se use hoy en día, existen herramientas que permiten el acceso a redes privadas por medio de *exploits* que permiten vulnerar los parámetros de seguridad implementados, encontrando así los agujeros que no hacen del todo robusta la seguridad de las plataformas, esto indica que ningún sistema ofrece confiabilidad frente a lo desplegado en el ámbito comercial y usado por la gran mayoría de usuarios convencionales (empresas, instituciones públicas y privadas)

4.1.6 Ataques comunes a las redes inalámbricas. Existen un abanico de técnicas de ataques a las redes corporativas con diferentes finalidades, que pueden incluso permitir interactuar directamente con los equipos de la red y derivar múltiples tipos de ataques que se categorizan a continuación. Las configuraciones básicas en los dispositivos inalámbricos exponen la red a diferentes tipos de ataques ya sean pasivos o activos. Cioperu[23], documenta algunos los tipos de ataques comunes en las redes inalambricas: ***Sniffing***, ***Arp Spoofing, Mac Spoofing, DDoS, AP Spoofing*****,** y otras metodologías de intrusión comunes utilizadas en las redes corporativas.

[22] RAMIREZ, Aydee. M. V. Identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting. 2016, 1p. [En Línea]. [Consultado el 01, febrero, 2020] Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12425/1/46646702.pdf

[23] CIOPERU. 5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos. 2015, 1p. [En Línea]. [Consultado el 13, septiembre, 2019] Disponible en: http://cioperu.pe/articulo/18229/5-ataques-comunes-a-las-redes-wifi-y-comodefenderse-de-ellos/.

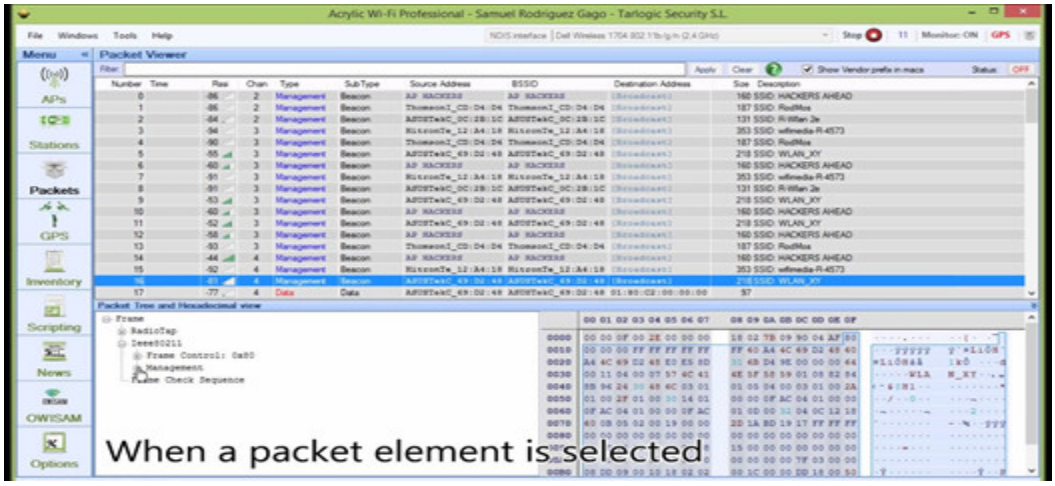
Igualmente, existen otros tipos de ataques que se generan debido al medio de transmisión utilizado en dicha tecnología. Las redes sin hilos generan una distribución de señales por ondas electromagnéticas que son irradiadas en diferentes direcciones dentro de un rango relativamente extenso, esto crea el problema de la propagación desmedida, por consiguiente, estas señales pueden ser identificadas por personas ajenas a la compañía y de esta manera se abre la posibilidad de ataques a la red, cuando estas no cuentan con una seguridad apropiada y robusta.

- ✓ ***Sniffing.*** Considerado un ataque de tipo pasivo que permite al atacante realizar captura de algunos datos que de manera posterior pueden ser útiles para un ataque más robusto a la red corporativa. Verbel[24], advierte que los *sniffer* tienden a ser más efectivos en las redes *LAN o WLAN* y pueden ser ejecutados bajo *software* o bajo puertos *mirrors* (espejos) en los dispositivos donde se pueda intervenir este tráfico.

  Consecuencias y solución: El husmear por medio de la técnica de *sniffining* permite al atacante capturar y sustraer información crítica de las organizaciones, igual que es de uso común tras realizar un ataque *MiTM* (*Man-in-The-Middle Attack- Ataque de hombre en el medio*), cuyo objetivo es capturar contraseñas de acceso e información relevante de una organización. Como solución y mecanismo de protección es importante contar con sistemas de análisis, monitoreo y reacción como los son los sistemas de *IPS* (Intrusion Prevention System – Sistema de Prevención de Intrusos). En la Figura 15, se realiza una descripcón gráfica del uso del analizador *Acrylic Wi-Fi Professional* utilizado para capturar paquetes en las redes inalambricas.

[24] VERBEL, Daniel; CANO, Hernan. (2016) ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS: APLICACIÓN DE BUENAS PRACTICAS EN PYMES Y USUARIOS FINALES [En Línea]. [Consultado el 02, febrero, 2020] Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf

Figura 15. Sniffing a una Red inalámbrica



Fuente: ACRYLICWIFI. Acrílico Wi-Fi Profesional - Analizador Wifi. 2020. 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wifi-analyzer-acrylic-professional/

- ✓ **Arp Spoofing y Mac Spoofing.** Indicados por Hao[25], como ataques realizados en la capa 2 del modelo *OSI* (*Open System Interconnection* - Modelo de interconexión de sistemas abiertos) en donde se tiene como finalidad enviar mensajes falsos de *ARP* (*Address Resolution Protocol* – Protocolo de Resolución de Direcciones) y utilizar una dirección y *MAC* de un dispositivo autorizado para ingresar a la red, llegando a modificar las tablas *ARP* de los equipos de la red y permitiendo conectar a la red a un equipo intruso enmascarado con información de un equipo legítimo.

  Consecuencias y solución: Estos tipos de ataques están relacionados igualmente con los ataques *MiTM*, puesto que, al suplantar un *host* en una organización, se tiene la capacidad de ingresar a sitios de confianza configurados bajos *MACs* o interceptar comunicaciones y permitir el despliegue de otras herramientas de *exploit.* La solución y el mecanismo de protección a dichos ataques se basa en un sistema de seguridad que impida la duplicación de *MAC* e *IPs*, por lo general esta actividad es controlada por sistemas de *IPS*

[25] HU, Hao; MYERS, Steven; COLIZZA, Vittoria; VESPIGNANI, Alessandro. WiFi networks and malware epidemiology. Proceedings of the National Academy of Sciences of the United States of America. 106. 1318-23. 10.1073/pnas.0811973106. 2009, 3p. [En Línea]. [Consultado el 11, febrero, 2020] Disponible en: https://www.pnas.org/content/pnas/106/5/1318.full.pdf

en las controladoras inalámbricas. La Figura 16, describe el principio del funcionamiento de un ataque de envenenamiento.

Figura 16. ARP y MAC Spoofing

Fuente: CAUSEYOURESTUCK. Envenenamiento por ARP - Hombre en el medio. 2020. 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://causeyourestuck.io/2016/01/07/arp-poisoning-man-in-the-middle/

- ✓ ***DDoS.*** Los ataques de denegación de servicio distribuidos, segun Sanatinia[26], son muy fáciles de ejecutar a una red inalámbrica corporativa cuya configuración en la controladora no ha sido robustecida, siendo esta débil configuración el punto de partida para a través de un software y líneas de comando, en el que se generan de manera reiterativa indefinido número de tramas de des-autenticación imposibilitando el normal funcionamiento de la red inalámbrica.

  Consecuencias y solución: Estos ataques en las organizaciones son realizados para indisponer las plataformas o servicios, su objetivo es generar distracción para que se puedan realizar otras ejecuciones sin ser detectados. La mejor forma de prevenir estos eventos es evitar inicialmente la intrusión, así como un control de las conexiones, que permitan generar umbrales de monitoreo sobre los dispositivos, para así determinar si se sobrepasa el límite establecido y de esta manera reaccionar e identificar el origen del ataque y controlarlo. La

[26] SANATINIA, Amirali S; NOUBIR, G. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In IEEE Conference on Communications and Network Security (CNS) 2003, pp. 430–437. [En Línea]. [Consultado el 19, febrero, 2020]. Disponible en: https://doi.org/10.1109/CNS.2013.6682757

Figura 17, ilustra un ataque de denengación de servicio distribuido hacia una infraestructura inalámbrica.

Figura 17. Ataques DDoS WIFI

Fuente: HACKING ÉTICO. Ataque DoS WiFi. Blog de seguridad de la información.2013, 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://hacking-etico.com/2013/03/13/ataque-dos-wifi/

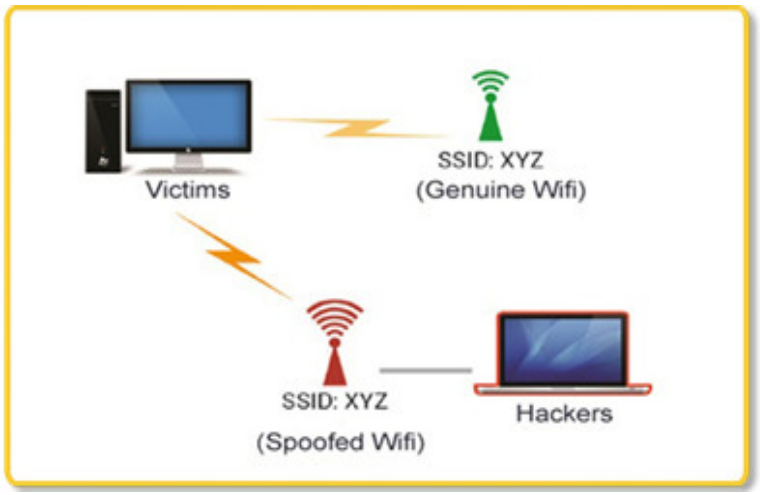
- ✓ ***Ap Spoofing.*** Como es indicado por Sanatinia[27], se determina como una técnica de ataque que combina métodos de *phishing* en el que se asume el *ESSID* (*Extended Service Set Identifier* - Identificador de de servicio extendido) de una red autentica y, a su vez, se realiza un ataque en el que se des-autentica algún usuario de la red para que cuando reactive su comunicación lo haga hacia el *ESSID* falso y posterior a esto se puedan capturar las credenciales de acceso reales.

  Consecuencias y solución: Son ataques de la categoría MiTM, en las organizaciones tienen como objetivo capturar información de un usuario activo, para de manera posterior utilizar esta información con el fin deseado o en su defecto realizar escalamiento y realizar un ataque de mayor impacto. Estos ataques pueden ser controlados con la activación de herramientas dentro de las

[27] SANATINIA, Amirali S; NOUBIR, G. (2013). Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In IEEE Conference on Communications and Network Security (CNS) (pp. 430–437). [En Línea]. [Consultado el 19, febrero, 2020]. Disponible en: https://doi.org/10.1109/CNS.2013.6682757

controladoras inalámbricas, que detecten, informen y tomen medidas con los *AP* y *SSID Rogues.* La Figura 18, describe el principio de funcionamiento de un ataque de tipo *AP Spoofing*.

Figura 18. AP Spoofing



Fuente: SHAJI. SSID SPOOFING conocido como puntos de acceso falsos, gemelos malvados o honeypots. 2020. 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en http://shaji-3848.herokuapp.com/

- ✓ **Errores de Configuración y mal diseño de la red.** La implementación de una red inalámbrica se torna sencilla, sin embargo, una buena configuración agrega complejidad y requiere sólidos conocimientos de seguridad como lo indica Alvarez[28], la vulnerabilidad más grande de una red, está en su errónea configuración, permitiendo abrir brechas de seguridad para múltiples intrusiones y ataques a quien tenga acceso a dicha red

  Consecuencias y solución: La principal consecuencia de un mal diseño y configuración es la exposición de la red a múltiples alternativas de *exploits*, la solución de esta vulnerabilidad está basada en la realización de un correcto diseño y *hardening* sobre las plataformas de red.

[28] ALVAREZ MENDEZ, Yelitza PASTORA. 2006. Seguridad Al Acceso De Información En La Implantación De Una Red Inalámbrica, Caracas. 98p. Trabajo de Grado (Especialista en Comunicaciones) Universidad Central de Venezuela. Facultad de Ingeniería. [En línea]. [Consultado el 14, julio, 2019]. Disponible en: http://saber.ucv.ve/xmlui/bitstream/123456789/2420/1/Tesis%20yelitza%20Alvare z.pdf

4.1.7 Clasificación de bandas de *RF* redes inalámbricas corporativas - *WLAN*. El diseño de los sistemas de redes inalámbricas corporativos a nivel latinoamericano trabajan en su gran mayoría bajo el estándar americano y son referenciados bajo el estándar 802.11 para *Wireless LAN,* 802.16 *WMAN* y normalizados por el *IEEE* (*Institute of Electrical and Electronics Engineers*), la normalización y regulación a nivel nacional está dirigida por la *CRC* (Comisión de Regulación de Comunicaciones)*,* instituto encargado de regular la implementación y la utilización de estas tecnologías de telecomunicaciones, aun así, en Colombia no existe una normativa clara relacionada con la implementación de servicios de redes inalámbricas locales y metropolitanas corporativas, pero si es considerado que los dispositivos adquiridos en Colombia deben estar adscritos al sistema de homologación internacional y nacional, por ende, dichos equipos están pre-configurados para difundir sus ondas bajo las frecuencias espectrales estandarizadas como públicas y permitidas sobre la banda de los 5GHZ, con todos sus canales frecuenciales, modos de usos y anchos de banda especificados en la Tabla 1.

Tabla 1. Frecuencia y canales de la banda de 5GHz

Canal	Frecuencia central	Modo de Uso	Ancho de Banda entre Canal
	GHz		MHz
36	5180	✓	Hasta 160
40	5200	✓	
44	5220	✓	
48	5240	✓	
52	5260	DFS	
56	5280	DFS	
60	5300	DFS	
64	5320	DFS	
100	5500	DFS	
104	5520	DFS	
108	5540	DFS	
112	5560	DFS	
116	5580	DFS	
132	5660	DFS	
136	5680	DFS	
140	5700	DFS	
149	5745	✓	
153	5765	✓	
157	5785	✓	
161	5805	✓	
165	5825	✓	

Fuente: IEEE 802.11 Standards, Facts & Channels

Para el rango de frecuencias en la banda de 2,4 GHz, se maneja la misma normalización indicada por la *IEEE* y regulada en el territorio nacional por la *CRC*, considerando así la relevancia el proceso de homologación que deben tener los dispositivos para el territorio colombiano, cabe resaltar que actualmente es la banda más común y utilizada a nivel comercial, La Tabla 2, representa el rango de frecuencias permitidas sobre la banda 2,4GHz, así como sus canales y anchos de banda entre canales

Tabla 2. Frecuencia y canales de la banda 2,4GHz

Canal	**Frecuencia central**	**Ancho del canal**	**Ancho de banda entre canal**
	GHz	**GHz**	**MHz**
1	2.412	2.401 - 2.423	22
2	2.417	2.406 - 2.428	
3	2.422	2.411 - 2.433	
4	2.427	2.416 - 2.438	
5	2.432	2.421 - 2.443	
6	2.437	2.426 - 2.448	
7	2.442	2.431 - 2.453	
8	2.447	2.436 - 2.458	
9	2.452	2.441 - 2.463	
10	2.457	2.446 - 2.468	
11	2.462	2.451 - 2.473	
12	2.467	2.456 - 2.478	
13	2.472	2.461 - 2.483	
14	2.484	2.473 - 2.495	

Fuente: IEEE 802.11 Standards, Facts & Channels

4.2 MARCO CONCEPTUAL

Las redes de computadoras en la actualidad son catalogadas como un ecosistema de múltiples dispositivos interconectados. Según el concepto de Tanebaum[29], las redes son un conjunto de computadoras conectadas entre sí, cuyo objetivo es el de intercambiar información. Existen múltiples métodos que permiten la comunicación de las computadoras, esta información puede ser transmitida por medios guiados o no guiados, categorizados bajo medios de transmisión como el cableado de cobre, fibra óptica, satelital, inalámbrico, infrarrojos y microondas.

Las redes inalámbricas son la composición de todos aquellos medios de comunicación que utilizan la propagación por medio de radio frecuencias con el objetivo de conectar computadoras, celulares o cualquier otro *host* (Anfitrión). Estas ondas de radio, según su frecuencia y potencia del dispositivo transmisor, permiten recorrer grandes distancias o penetrar diferentes barreras físicas. Algunos sistemas de radiofrecuencias como las utilizadas por las redes inalámbricas empresariales son omnidireccionales, sistema que permite dirigir sus ondas en todas las direcciones.

Debido a los alcances de conectividad que genera una red inalámbrica, Viloria[30], señala que estas son categorizadas según el rango que abarcan y sus servicios a prestar, indicando que existen las redes inalámbricas de menor alcance, nombradas como *WPAN* (Redes inalámbricas de área personal), mundialmente conocida como la tecnología *Bluetooth,* redes que permiten la conectividad entre dispositivos a una muy corta distancia, que por lo general son utilizadas por dispositivos de uso personal como las *PDA* (*Personal Development Analysis* - Ayudante personal digital), impresoras y teléfonos móviles.

Las redes inalámbricas más comunes a nivel comercial por su rango de trabajo y los servicios que pueden ser prestados sobre ellas son las redes *WLAN* (Redes inalámbricas de área local), estas redes permiten la conectividad entre

[29] TANEBAUM, Andrew; WETHERALL, David. Redes de computadoras. Quinta edición. México: PEARSON EDUCACIÓN, 2012. 791 p. ISBN: 978-607-32-0817-8

[30] VILORIA Núñez, César; CARDONA Peña, Jairo; LOZANO Garzón, Carlos. Análisis comparativo de tecnologías inalámbricas para una solución de servicios de telemedicina. En: Ingeniería y Desarrollo, núm. 25, enero-junio, 2009. pp. 200-217 Universidad del Norte. [En línea]. [Consultado el 25, marzo, 2020]. Disponible en: https://www.redalyc.org/pdf/852/85212371012.pdf

computadoras y diversos dispositivos que están diseñados para funcionar con esta tecnología, a nivel empresarial son el complemento y la alternativa perfecta de las redes locales cableadas.

Con un mayor rango de alcance a nivel de una metrópolis, están las redes *WMAN* (Redes inalámbricas de área metropolitana), también conocidas por la tecnología más común utilizada en estas redes, que es la *WIMAX* (*Worldwide Interoperability for Microwave Access* - Interoperabilidad mundial para acceso por microondas). Byeong[31] ,indica que este tipo de redes tiene un alcance que cubre hasta 70 km y permite en la gran mayoría de ocasiones brindar acceso a internet a lugares donde es de difícil contar con conectividad cableada por un *ISP* (*Internet Service Provider* - proveedor de servicio de internet).

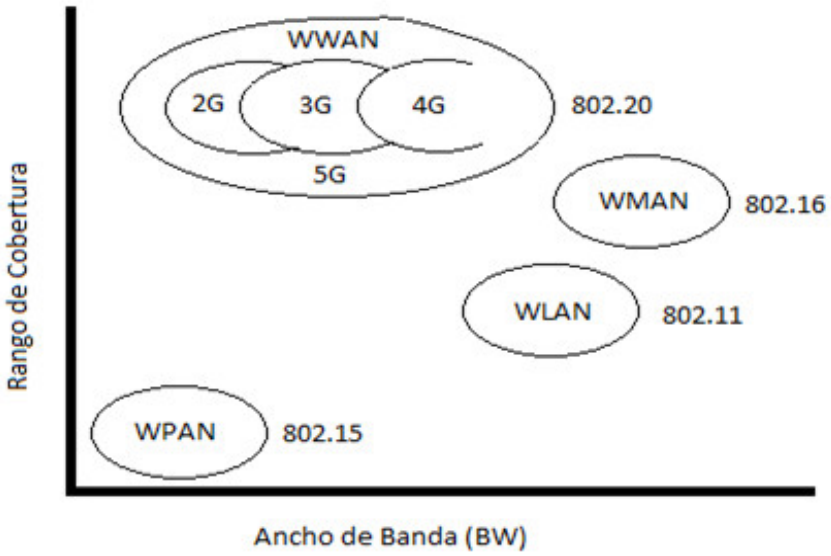
A mayor escala y mayor rango de cobertura se encuentran las redes *WWAN* (Redes inalámbricas de área amplia), descritas por Hu[32], como redes que comúnmente se ofrecen para nuestros dispositivos móviles y donde identificamos tecnologías de 2G,3G,4G y actualmente 5G, tecnologías que han estado en constante evolución ofreciendo así altas velocidades de conexión para la utilización de todo tipo de servicios que requieran buenas latencias y altos niveles de conectividad.

Descritas las diferentes redes inalámbricas, es directriz que se establezcan estándares que permitan definir como operaran estas tecnologías, bajo la estandarización americana diseñada por la *IEEE* (Instituto de Ingenieros Eléctricos y Electrónicos), las redes inalámbricas nombradas anteriormente son estandarizadas de la siguiente manera: *WPAN/IEEE* 802.15, *WLAN/IEEE* 802.11, *WMAN/IEEE* 802.16 y *WWAN/IEEE* 802.20. En la Figura 19, se realiza una descripción de las tecnologías inalambricas descritas anteriormente, caracterizando su alcance frente al ancho de banda alcanzado.

[31] BYEONG, Gi Lee; SUNGHYUN, Choi. Broadband Wireless Access and Local Networks: Mobile WiMax and WiFi. ARTECH HOUSE, 2008. 618 p. ISBN: 1596932945, 9781596932944

[32] HU, Fei. Cyber-Physical Systems: Integrated Computing and Engineering Design. CRC PRESS, 2013. 398 p. ISBN: 1466577010, 9781466577015

Figura 19. Comparación de Tecnologías Inalámbricas



Fuente: VILORIA Núñez, César; CARDONA Peña, Jairo; LOZANO Garzón, Carlos. Análisis comparativo de tecnologías inalámbricas para una solución de servicios de telemedicina. Universidad del Norte, Barranquilla, Colombia. Núm. 25, 2009, pp. 200-217. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.redalyc.org/pdf/852/85212371012.pdf

Estas estandarizaciones permiten que se cumpla con dichos lineamientos, salvaguardando la utilización del espectro, canales de frecuencia, calidad de señal, entre otras características importantes que permiten un uso eficiente, responsable y de calidad, para un uso seguro y eficiente de las tecnologías. En el ámbito informático y de redes es relevante término de *hardening*, cuyo concepto según Robayo[33], es el fortalecimiento de la seguridad con el objetivo de resistir los ataques o generar una línea de seguridad cerrándose a la exposición de vulnerabilidades que en las redes corporativas generan un alto impacto, debido a la criticidad de la información manejada por los sistemas informáticos, en cambio Mallery[34], conceptualiza el *hardening* como un compilado de actividades implementadas con

[33] ROBAYO LÓPEZ, Javier; RODRÍGUEZ RODRÍGUEZ, Richar. Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net". Repositorio Institucional UMNG. Universidad Militar Nueva Granada. 2015, 33p. [En línea]. [Consultado el 25, marzo, 2020]. Disponible en https://repository.unad.edu.co/handle/10596/3818

[34] MALLERY, Jhon; MCMULLIN, Robert; ZANN, Jason; LOVE, Paul. Hardening Network Security. MCGRAW-HILL OSBORNE MEDIA, 2005. 593 p. ISBN: 0072257032, 9780072257038

el objetivo de reforzar la seguridad de los dispositivos, llegando a dificultar las actividades realizadas por un atacante y así permitir ganar tiempo para remediar o minimizar las consecuencias de un incidente a nivel de seguridad.

La seguridad en las redes se define en su expresión más simple como el hecho garantizar que no sea lea, modifique o se acceda a un servicio sin ser autorizado, concepto que juega un papel relevante en las redes de comunicaciones. Debido a que la interconexión entre las diferentes tecnologías de comunicaciones requiere transportar de manera cifrada y segura la información, Tanebaum[35], indica que la seguridad favorece principalmente a las redes alámbricas, puesto que las ondas electromagnéticas sobrepasan paredes y facilitan la interceptación, aún asi existen múltiples mecanismos de seguridad encargados de transportas los *bits* de la comunicación de manera segura desde el emisor hasta el transmisor.

4.3 MARCO LEGAL

La ley 1581 de 2012 y el Decreto 1377 de 2013[36], consignado en el artículo 15 de la constitución política colombiana, garantiza la intimidad, los derechos a la privacidad, y el buen nombre de las personas, durante el proceso del tratamiento de datos personales, en todas las actividades, las cuales tendrán los principios de confidencialidad, seguridad, legalidad, acceso, libertad y transparencia.

Por consiguiente, esta reglamentación da orden expresa de no revelar la información que se digita en los portales cautivos, de acuerdo con las normas de la Ley 527 que reglamenta el Comercio Electrónico en Colombia y la Ley 1581 de 2012 sobre el uso de datos confidenciales. A través de la presente política de tratamiento y protección de datos personales se regula recolección de la información y la disposición que esta información pueda tener.

---

[35] TANEBAUM, Andrew; WETHERALL, David. Redes de computadoras. Quinta edición. México: PEARSON EDUCACIÓN, 2012. 791 p. ISBN: 978-607-32-0817-8

[36] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. MINTIC. Decreto 1311 (14, septiembre, 2013). por el que se establece el marco de actuación para conseguir un uso sostenible de los productos fitosanitarios. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2013. 5 p. [Consultado el 25, marzo, 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

La resolución derogada por el artículo 1 de la 963 de 2019 en Colombia estipulada por el *ANE* (Agencia Nacional del Espectro) y el *MINTIC* (Ministerio de las Tecnologías de la Información y las Comunicaciones)[37], declara las bandas libres las frecuencias las correspondientes a las frecuencias 915-924 MHz, de la frecuencia 2400 - 2483,5 MHz y de la 5150 - 5250 MHz para uso en dispositivos de telecomunicaciones inalámbricas.

La normativa establecida a nivel nacional por el *MINTIC*[38], bajo la LEY 1341 DEL 2009 proclama a la *ANE* ente regulador del espectro y donde especifica sus disposiciones. La *ANE* bajo la RESOLUCIÓN 711 DE 2016 estandariza las bandas de frecuencias libre para la utilización en el territorio nacional y establece los siguientes artículos para evitar infringir en lo reglamentado:

Artículo 5. Habla sobre las interferencias. La utilización del espectro no podrá causar interferencia a las estaciones de un servicio primario o secundario, quien cause interferencia perjudicial a una radiocomunicación autorizada a título primario o secundario deberá suspender la operación y no podrá reanudarla hasta que se haya subsanado el conflicto interferente, esto da cabida a la imposición de las sanciones previstas en la Ley 1341 de 2009.

Artículo 6. Las infracciones y sanciones estipuladas. El incumplimiento de lo dispuesto en la resolución constituye una violación al régimen de telecomunicaciones y genera las sanciones previstas en las normas legales, de conformidad con lo dispuesto en los artículos 64 y 65 de la Ley 1341 de 2009.

Artículo 11. Acceso al uso del espectro radioeléctrico. El uso del espectro Radioeléctrico sobre frecuencias no denominadas libres, requiere permiso previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las

---

[37] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. MINTIC. Resolucion 0963 (30, abril, 20193). Por la cual se derogan unas disposiciones en materia de planeación, atribución y asignación del espectro. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0963_2019.htm#1

[38] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. MINTIC. Ley 1341 (29, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0963_2019.htm#1

Comunicaciones.

Artículo 65. Categorización de Sanciones., la persona natural o jurídica que incurra en cualquiera de las infracciones de la presente ley, será sancionada, además de la orden de cesación inmediata de la conducta que sea contraria a las disposiciones previstas en esta ley, con:

- Amonestaciones.

- Multa hasta por el equivalente a dos mil (2.000) *SMMLV* (Salario mínimo mensual legal vigente) y hasta por el equivalente a quince mil (15.000) *SMMLV* para personas jurídicas.

- Suspensión de la operación que estén realizando hasta por dos (2) meses.

A nivel judicial en la categorización de delitos informáticos que se pueden cometer bajo el acceso abusivo, la interceptación de datos, hurtos y otras definiciones que están en los lineamientos y abarcan a las redes inalámbricas, se estableció por el Congreso de la Republica la Ley 1273 del 2009[39], que categoriza y penaliza las infracciones de la siguiente manera:

Acceso abusivo a sistemas informáticos: El ingresar a un sistema o tecnología informática sin autorización, para realizar actos ingeniería social, mantenerse dentro de él y obtener acceso a cuentas o uso de diccionarios para ataques de fuerza bruta, lo hace acreedor a una pena de 48 a 96 meses de prisión y sanción económica de 100 a 1000 SMMLV.

Hurto por medios informáticos: Cuando por medio del uso de las redes inalámbricas o cualquier medio electrónico se realicen robos de tarjetas, contraseñas, información o se realice suplantación, lo hace acreedor a una pena de 3 a 8 años.

[39] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05 – enero - 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. No. 47.223. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Daño informático: la persona que destruya, borre, deteriore o altere datos de un sistema o tecnología informática, lo hace acreedor a una pena de 48 a 96 meses de prisión y sanción económica de 100 a 1000 SMMLV.

Interceptación de datos: El uso de medios o plataformas tecnológicas con el objetivo de capturar e intervenir las señales electromagnéticas emitidas por una red inalámbrica, lo hace acreedor a una pena de 36 a 72 meses de prisión.

Obstaculización de sistema informático o red de telecomunicaciones: El impedir el normal acceso a los dispositivos o tecnologías informáticas bajo ataques *DoS* (Denial of Service – Denegación de Servicio), lo hace acreedor a una pena de 48 a 96 meses de prisión y sanción económica de 100 a 1000 SMMLV.

Suplantación de sitios web para captura de datos personales: El realizar suplantación *phising* (suplantación), un ejemplo específico puede ser una suplantación a un portal cautivo inalámbrico, sea cual sea su objetivo, lo hace acreedor a una pena de 48 a 96 meses de prisión y sanción económica de 100 a 1000 SMMLV.

Uso de software malicioso: Quien cree, distribuya o comercialice programas que afecten los servicios y tecnologías informáticas, en su ejemplo programas maliciosos*, trojans* (troyanos), bombas lógicas, *exploits* (elementos para explotar vulnerabilidades), etc. Lo hace acreedor a una pena de 48 a 96 meses de prisión y sanción económica de 100 a 1000 SMMLV.

5. RESULTADOS

5.1 TEORIA BÁSICA RELACIONADA CON LAS REDES INALÁMBRICAS.

Esta temática correspondiente a la resolución del primer obejtivo propuesto, que abarco la información referente a la documentación sobre las redes inalámbricas, las vulnerabilidades y ataques que estas presentan, fueron descritas en el marco referencial, bajo la categorización de las diferentes redes de uso común a nivel empresarial, e igualmente los elementos utilizados para su despliegue y funcionamiento. Asimismo, se documentó los protocolos de seguridad utilizados para cifrar las comunicaciones, las bandas de frecuencias utilizadas en los sistemas inalámbricos y los diferentes tipos de ataques que se pueden desplegar al identificar vulnerabilidades en la red.

5.2 MECANISMOS DE SEGURIDAD EN REDES SIN HILOS COPORATIVAS

En la actualidad, existen múltiples métodos de aseguramiento para las redes alámbricas e inalámbricas, basados en mecanismos de autenticación, políticas y cifrado. De igual manera existen diferentes tipos y metodologías de aseguramiento de las tecnologías sin hilos, cuyo objetivo común es salvaguardar los datos y las comunicaciones en general, esto a partir de los algoritmos de encriptación; que son los mecanismos de *front* en seguridad de una red inalámbrica.

Los algoritmos de encriptación tienen su clasificación basado en el método utilizado, ya sea asimétrico o simétrico, su diferencial está fundamentado en la cantidad de llaves utilizadas, puesto que el cifrado simétrico solo utiliza una misma clave para cifrar y descifrar la comunicación, algunos de sus algoritmos más comunes son *AES* (*Advanced Encryption Standard*), RC4 (Rivest *Cipher 4*), *DES* (*Data Encryption Standard*) *o 3DES* (*Triple Data Encryption Standard*), mientras que el modelo asimétrico utiliza el sistema de dos claves, en donde una es pública y la otra es una clave privada, algunos de sus algoritmos comunes son el *RSA* (*Rivest, Shamir y Adleman*) o *DSA* (*Digital Signature Algorithm*).

5.2.1 Categorización de mecanismos de seguridad en las redes inalámbricas. Los mecanismos de cifrado son un conjunto implementaciones a nivel de seguridad que permiten garantizar un minimo de seguridad en la conexión y transporte de datos. En los dispositivos inalámbricos son mayormente utilizados los cifrados simétricos. En las redes corporativas como *WLAN, WMAN y WWAN* el método más común utilizado para salvaguardar y mantener la privacidad en la comunicación es el cifrado simétrico, aun así, el cifrado hace parte de una configuración opcional y en caso de no configurar permite que se pueda escuchar y capturar todo el tráfico que se genere en la red.

Actualmente existen 4 generaciones de protocolos seguridad en las redes inalámbricas:

WEP (Wired Equivalent Privacy) / Norma 802.11b.
WPA (Wi-Fi Protected Access) / Norma 802.11g.
WPA2 (Wi-Fi Protected Access 2) / Norma 802.11ac.
WPA3 (Wi-Fi Protected Access 2) / Norma 802.11i.

- ✓ *WEP (Wired Equivalent Privacy) /* Norma 802.11b. Esta primera normativa de seguridad fue creada con el fin de proteger las redes inalámbricas, se denominó protocolo *WEP* y se implementó bajo el estándar 802.11b, este protocolo se basó en un algoritmo de tipo *RC4*, cuya ventaja inicial se debía a la eficiencia y rapidez de encriptación, no obstante este protocolo ya fue vulnerado y por consiguiente remplazado por su predecesor *WPA*, protocolo elaborado para realizar la transición a un sistema más seguro, *WPA* cubría las vulnerabilidades de privacidad identificadas sobre *WEP* bajo su novedosa utilización de las claves temporales *TKIP* (*Temporal Key Integrity Protocol*), que combinado con el algoritmo *RC4*, propuso un sistema de claves dinámicas que mejoro la privacidad y los sistemas de autenticación

- ✓ WPA (Wi-Fi Protected Access) / Norma 802.11g. Aun teniendo robustez, el protocolo *WPA* también logró ser violentado, habilitando la posibilidad de descubrir su clave de cifrado mediante métodos de ataque de fuerza bruta, cuyo procedimiento consiste en buscar coincidencias en un diccionario de las posibles claves que permitan el ingreso a la red, esta identificación de vulnerabilidades en dicho protocolo dio paso al lanzamiento en 2004 el protocolo *WPA2*, que en la actualidad es el método de encriptación más eficiente a pesar de tener un predecesor, el sistema WPA2 introdujo un sistema de cifrado por bloques *AES*

bajo el algoritmo *CCMP* (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) que remplazo la utilización de claves *TKIP*

- ✓ WPA2 (Wi-Fi Protected Access 2) / Norma 802.11ac. El sistema de cifrado en bloques utilizado por *WPA2*, permite unas longitudes variables en las claves que van desde 128,192 o 256 bits, cifrando así todos los bloques de datos, el cifrado *AES* además de ser rápido y flexible fue normalizado para su implementación en múltiples plataformas de comunicación inalámbrica, como tarjetas inteligentes y dispositivos pequeños, además, *AES* ha sido objeto de pruebas rigurosas que han demostrado robustez a nivel de seguridad.

  En 2017, bajo la identificación de una vulnerabilidad presentada en WPA2, donde se rompe la seguridad del protocolo con un ataque realizado con el software *KRACKs* (*Key Reinstallation Attacks*)*,* la *Wifi-Alliance*[40]*, se* dio a la tarea de crear un protocolo que salvaguardara las redes inalámbricas de los ataques y vulnerabilidades conocidas, por consiguiente, en enero del 2018 se dio a conocer *WPA3*, protocolo que asegura importantes mejoras a nivel de seguridad y conectividad.

- ✓ *WPA3* es un protocolo Desarrollado bajo la colaboración del sistema *Dragonfly Handshake* o denominado protocolo *SAE* (*Simultaneous Authentication of Equals*), cuya característica más relevante es que evita el descifrado de datos y robustece el sistema de contraseñas, por consiguiente brinda un paquete de seguridad de 192 bits, permitiendo que el sistema sea más robusto, brindando mayor seguridad a nivel empresarial, a pesar de estas características, en abril del 2019 se dieron a conocer 5 vulnerabilidades, según *Dragonblood*[41], cuyo impacto es directo a la seguridad y a la autenticación del protocolo *WPA3,* dichos ataques abren múltiples posibilidades de ofensivas de tipo de denegación de servicio, ataques de canal lateral, ataques de degradación de seguridad y *downgrade* (degradar) a *WPA2* que permite el ataque de diccionario.

Por consiguiente y a falta de una mayor maduración del protocolo *WPA3*, la seguridad basada en los sistemas *WPA2* siguen siendo la elegida por las

[40] Wi-FI Alliance. “WPA3™ Specification Version 2.0”. 2019. 3p. [En Línea]. [Consultado el 15, Marzo, 2020] Disponible en: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf

[41] DRAGONBLOOD. Analysing WPA3’s Dragonfly Handshake. 2019, 1p. [En Línea]. [Consultado el 01, abril, 2020] Disponible en: https://wpa3.mathyvanhoef.com/

organizaciones, aun así, al igual que la mayoría de protocolos, a medida que se identifiquen las vulnerabilidades se intentará solventarlas con actualizaciones. Igualmente es importante que los fabricantes de sistemas de comunicaciones inalámbricas adopten este protocolo, con el objetivo de robustecer su fuerza en el mercado, llevando así a fortalecer sus funcionalidades de servicio y de seguridad. La Tabla 3. representa los protocolos de seguridad en las redes inalámbricas, en conjunto con sus algoritmos, características, vulnerabilidades y ataques conocidos.

Tabla 3. Protocolos de encriptación *WI-FI* y sus Vulnerabilidades

Encriptación	**WEP**	**WPA**	**WPA2**	**WPA3**
Estándar	802.11b	802.11g	802.11i	802.11ax
Características	Protección básica a redes inalámbricas	Llaves dinámicas *TKIP*, incluye MAC del emisor	Algoritmo por medio de operaciones matriciales	*Handshake* más seguro, mejora en redes abiertas
Algoritmos	*RC4*	*RC4+TKIP*	*AES (Rijndael)*	*(CCMP/GCMP)*
Longitud de Claves	64 y 128 bits	128 a 256 bits	128 a 256 bits	192 a 384 bits
Vulnerabilidades	Llaves Cortas y estáticas	Llaves conocidas por medio de diccionarios de los atacantes, auditoria de *handshake*	Llaves conocidas por medio de diccionarios de los atacantes, auditoria de *handshake*	Opción de *downgrade* a WPA2, *spoofing*
Ataques Conocidos	FMS Ataque de Cifrado (2001)	Ataques de Fuerza Bruta, comparando claves de diccionarios (*krack*, 2007)	Ataques de Fuerza Bruta, comparando claves de diccionarios, debido a su algoritmo, muy poco éxito en descifrar (2017)	Ataques *Dragonblood*, contienen diversos ataques *DDoS* y *downgrade* (Agosto /2019)

Fuente: El autor

Igualmente, Identificados los principales protocolos de encriptación utilizados para las redes sin hilos corporativas, se pueden establecer mecanismos de seguridad aplicables en el diseño, que se integran con las características de los mecanismos

de cifrado *WEP, WPA, WPA2* y *WPA3* anteriormente nombrados, permitiendo generar robustecimiento de las plataformas inalámbricas.

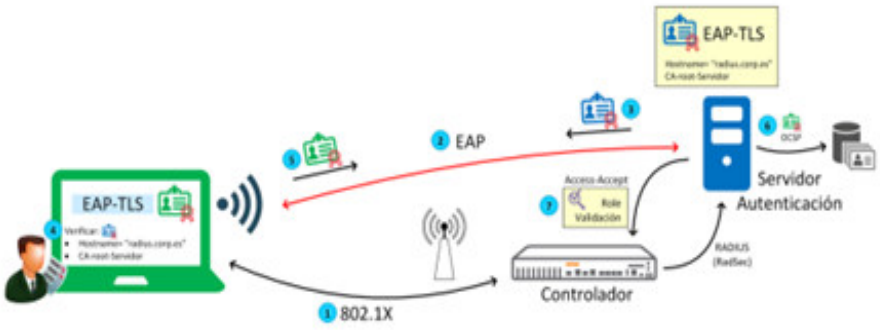
5.2.2 Mecanismos de Autenticación. Uno de los mecanismos de autenticación se realiza bajo el protocolo *802.1X*, donde se instaura una comunicación con el servidor de autenticación de tipo *EAP* que puede ser: *EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST*, este tipo de autenticación depende de la tecnología y fabricante de la controladora inalámbrica, como resultado se abre un puerto virtual que según la autorización da la fluidez en la comunicación, bajo esta implementación se mejora la seguridad a nivel de acceso, dicho protocolo es completamente funcional con *WEP, WPA, WPA2* y *WPA3*. La Figura 20, describe el principio de funcionamiento y cuya estructura se presenta de la siguiente manera:

Suplicante: El cliente *Wi-Fi.*

Autenticador: El *Ap Wi-Fi* o la Controladora inalámbrica.

Servidor de autenticación: Una base de datos de autenticación, generalmente un servidor *RADIUS*

Figura 20. Autenticación bajo el protocolo *802.1X*



Fuente: ESPAÑA. Recomendaciones de seguridad en redes Wi-Fi corporativas Centro Criptologico Nacional. 2020. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

5.2.3 Mecanismos basados en políticas. Gran cantidad de controles se pueden establecer bajo políticas de aseguramiento a partir de controles los cuales según el Centro Criptológico Nacional de España CCN-CERT[42], son los accesos basados en listas blancas o negras, como lo describe la Figura 21. En dicho proceso se crea una base de datos con las *MAC* de los dispositivos que se quiere permitir o bloquear, generando así un control inicial antes de entrar a un sistema de autenticación.

Figura 21.Acceso basado en la *MAC*

Fuente: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

Otro mecanismo basado en políticas es el utilizado bajo el agente *NAC* (*Network Admission Control*), quien define políticas de acceso bajo algunos atributos o requisitos a las terminales que deseen acceder a la red inalámbrica, asegurando así, por ejemplo, que se cuente con sistema de antivirus actualizado y cualquier política empresarial que se desee implementar para permitir el acceso a la red. La Figura 22, describe su principio de funcionamiento.

Figura 22. Acceso basado en políticas del *NAC*

Fuente: ESPAÑA. Recomendaciones de seguridad en redes Wi-Fi corporativas Centro Criptologico Nacional. 2020. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

[42] CCN-CERT BP/11. Recomendaciones de seguridad en redes Wi-Fi corporativas. 2020. 5p. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

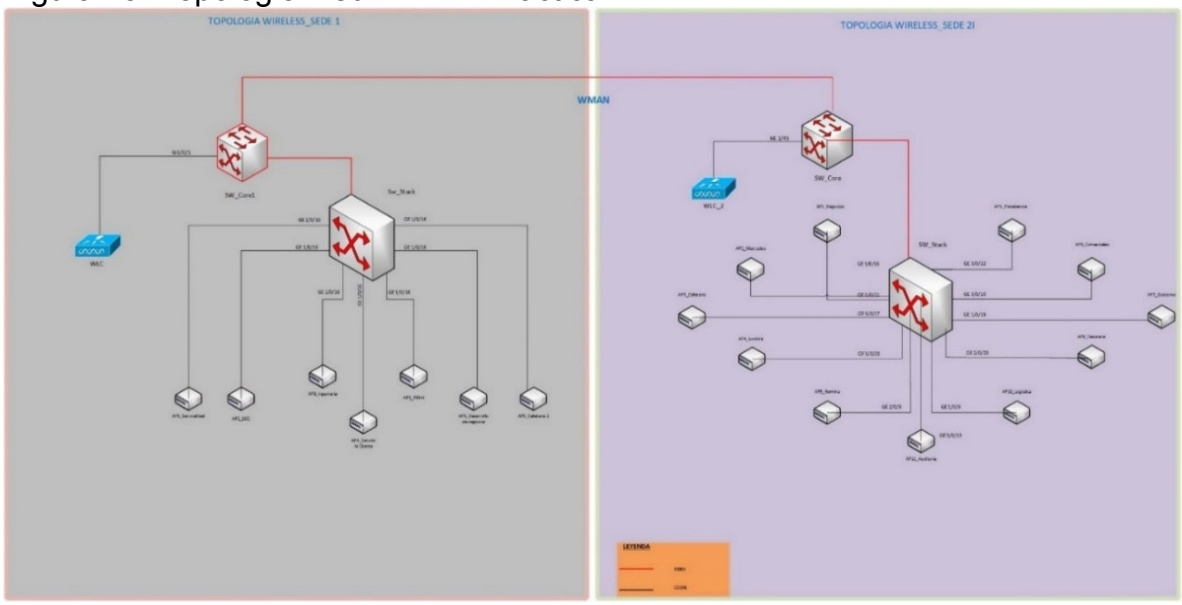
5.3 VULNERABILIDADES DE DISEÑO EN REDES INALÁMBRICAS (CASO PRÁCTICO SOBRE UN PORTAL CAUTIVO)

5.3.1 Análisis de vulnerabilidades. Este escenario propuesto es simulado de acuerdo con los errores más comunes de diseño y configuración de las plataformas inalámbricas administradas sobre una controladora inalámbrica, para dicha simulación se establece una red de tipo *WMAN* y dicha red está compuesta por dos Redes *WLAN* y por dos controladoras inalámbricas que tiene la capacidad de realizar *Failover* (Conmutación por errores) y un sistema de portal cautivo para el acceso de los invitados como se ilustra en la Figura 23. Cuya salida a internet del servicio es realizada por la misma *IP* pública.

5.3.2 Materiales a utilizar. El equipamiento utilizado para cumplir dichas actividades correspondientes al proyecto monográfico será descrito a continuación:

Software: *Nmap.* Navegador Web -Portal Web *Cisco Controller, VirtualBox, ettercap*, **O.S Atacante:** Kali Linux

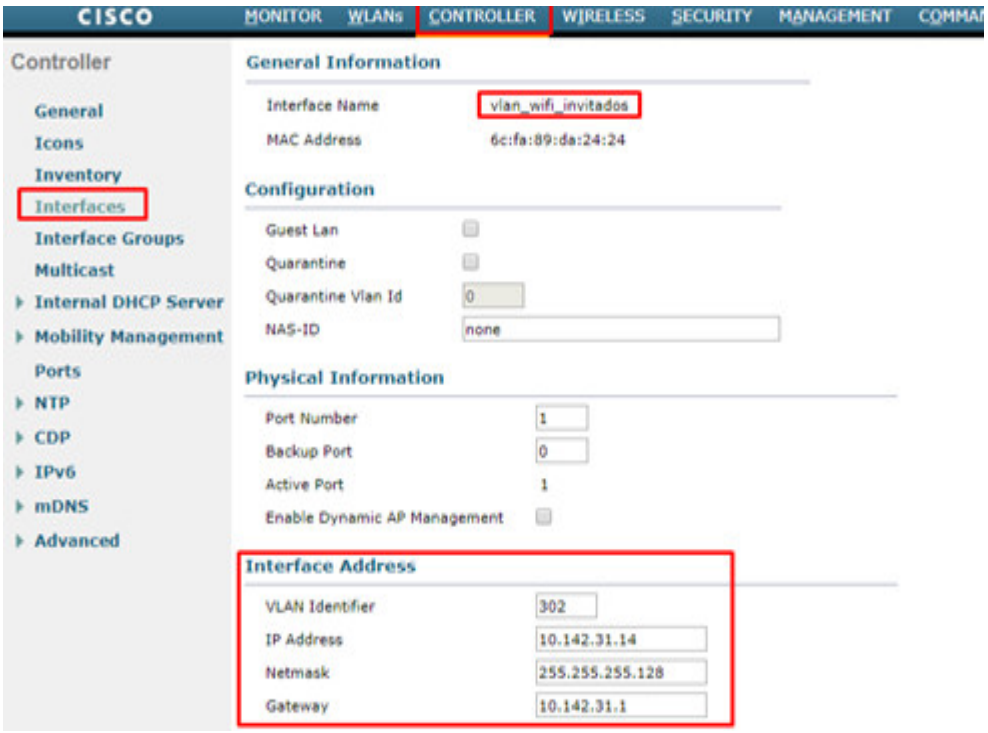
Figura 23. Topología Red WMAN Práctica



Fuente: El Autor

5.3.3 Proceso de Configuración de red de Invitados. Bajo la simulación se realiza la configuración rápida del portal cautivo sobre una de las 2 *WLC*, puesto que las configuraciones en las dos controladoras son de tipo *HA* (*High Availibity* – Alta Disponibilidad). Esta configuración realizada en el Portal *Web Cisco Controller*, puesto que la controladora es la que permite el acceso inalámbrico al personal invitado, para este proceso se debió crear una interfaz *VLAN* como lo ilustra la Figura 24, que en este caso particular se llama invitados.

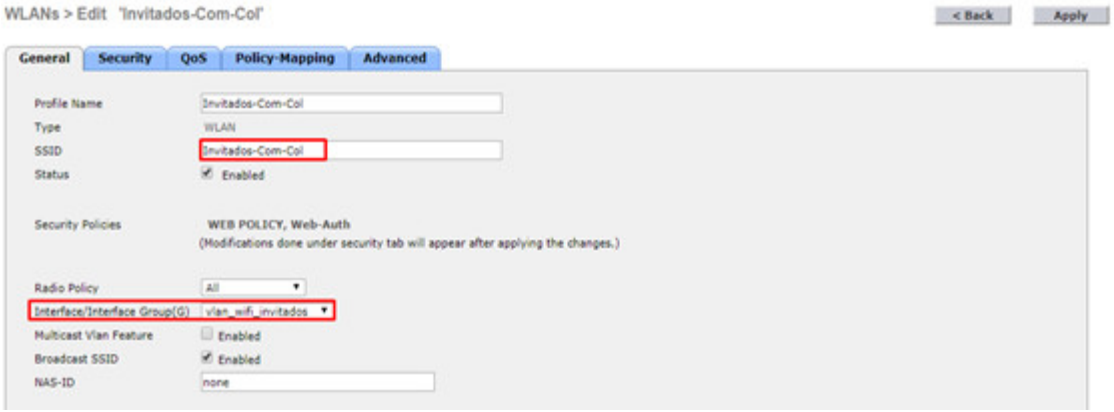
Figura 24. Creación de interface *Vlan* de invitados



Fuente: El autor.

Posterior a la creación de la interfaz *vlan* se procede asociarlo al *SSID* **Invitados-Com-Col** que va ser difundido, se habilita y se establece la *Web Auth* (Web de Autorización), que es el *front* (frente) hacia el usuario como se ilustra en la Figura 25, adicional a esta configuración se puede añadir al *SSID* algunos parámetros alternos de calidad de servicio y políticas de seguridad mapeadas, así como la cantidad de tiempo que un usuario puede estar activo en esta red difundida.

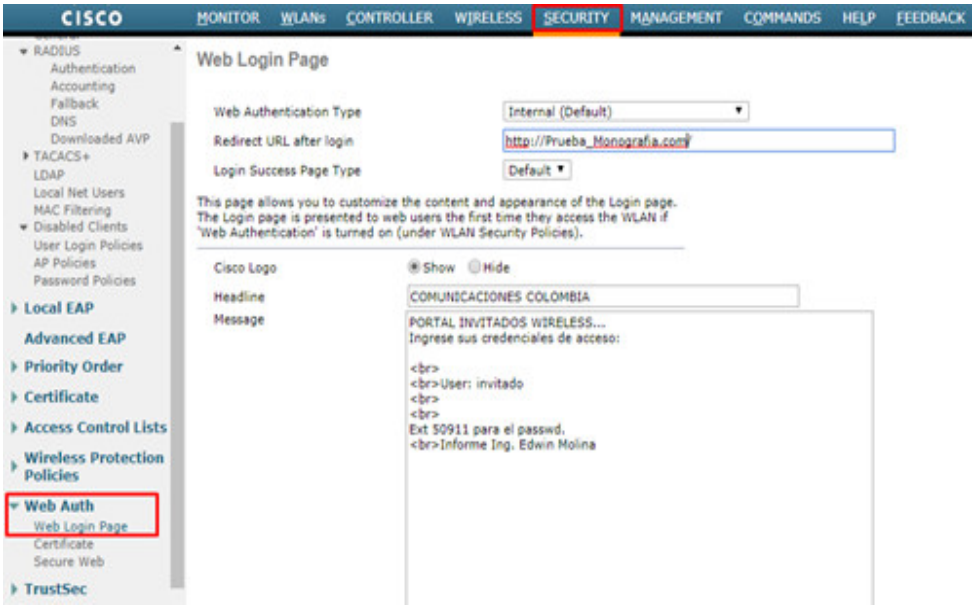
Figura 25. Asociación de *VLAN* Invitados al *SSID*



Fuente: El autor.

Una vez parametrizado la interfaz *vlan* y el *SSID* a difundir, se creó una *Web Auth* (Web de Autorización), que permitió ser el *front* al usuario, este frente es personalizable y re-direccionable a un segundo sistema de autenticación interno o externo, igualmente puede ser dirigido hacia a una página *Web*, una vez se comprueban las credenciales y es autenticado el usuario como lo ilustra la Figura 26.

Figura 26. Creación de Pagina de Autorización-*Front End*



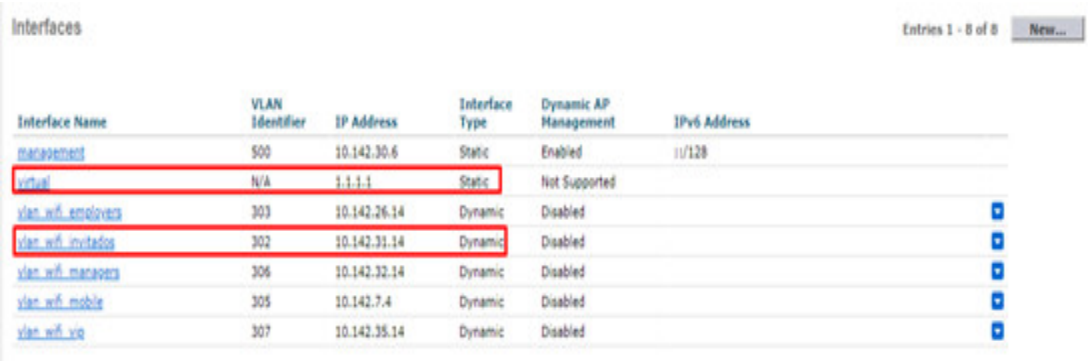
Fuente: El autor.

Como último paso, tras la configuración de las interfaces, la asociación con el *SSID* y la creación del portal Web que será el frente al usuario, se crea una interfaz virtual sobre un rango de *IPs* que no sea enrutable, esto para que permita a la controladora desplegar el menú hacia el usuario donde se carga dicho portal y en el que se muestran las opciones para ingresar las credenciales de autenticación, esto es ilustrado en la Figura 27. Mientras tanto la Figura 28, ilustra la interfaz virtual.

Figura 27. Sistema de Portal Cautivo

Fuente: El autor.

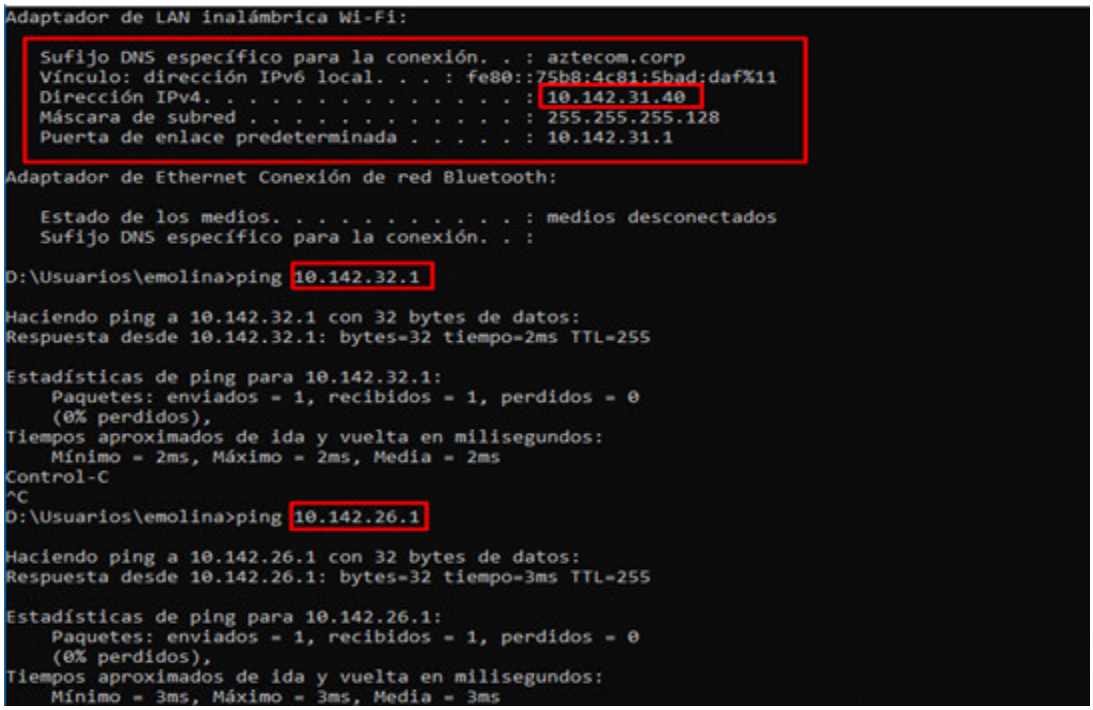
Figura 28. *VLAN* virtual y *VLAN* del Portal Cautivo



Fuente: El autor.

La configuración inicial se realizó sin ningún robustecimiento, para dejar expuesto los errores más comunes a nivel de diseño y seguridad cometidos por los administradores. A continuación, se observa el direccionamiento generado por la red al conectarse por medio del portal cautivo, la conexión a dicho portal permite el ingreso directo a una *VLAN* (*Virtual LAN*) creada en la red corporativa y esta tiene comunicación a otros segmentos de la red de la *LAN*, generando claramente una **falla de diseño y configuración**, que facilita a un atacante múltiples posibilidades de explotación, una vez conectado a la red corporativa. La Figura 29, ilustra el direccionamiento asignado a la red de invitados, asi como el alcance que tiene dicha red a los demás segmentos corporativos.

Figura 29. *DHCP* Asignado a la red Invitados y ping entre Segmentos



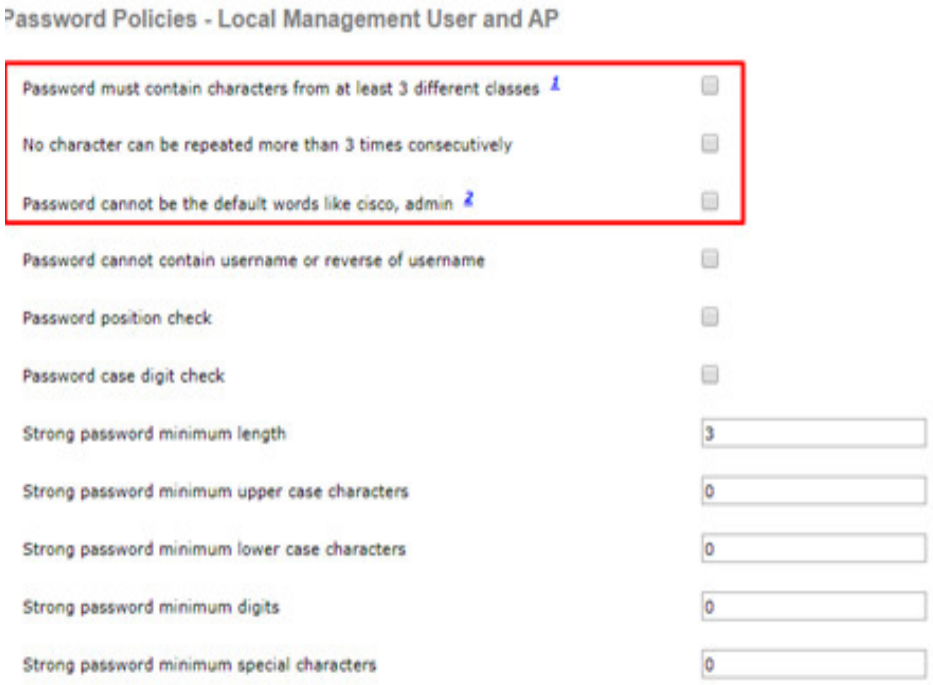
Fuente: El autor.

De manera adicional, Hernández[43], habla sobre la importancia de crear medidas de robustez para la autenticación hacia los dispositivos, en este caso práctico, en el

[43] HERNÁNDEZ Mendoza César Manuel; RODRÍGUEZ Vidal, Luz María; AGUILAR Almanza, Maricela. Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. 2017. 10p. [En línea]. [Consultado el 20, julio, 2019]. Disponible en: https://www.pag.org.mx/index.php/PAG/article/viewFile/647/793

proceso erróneo de configuración y diseño por parte del administrador, no se parametrizan las contraseñas de acceso a la administración de la controladora, *APs (Acces Points)* y a las redes inalámbricas difundidas. Dichas fragilidades de configuración que a su vez generan vulnerabilidades son ilustradas en la Figura 30.

Figura 30. Vulnerabilidad en la parametrización de contraseñas



Fuente: El autor.

La suma de todas las fallas estructurales de diseño de la red y de configuración en la controladora inalámbrica, permiten realizar un *pentesting* con objetivo sencillo, bajo técnicas de recolección pasiva y activa, demostrando así la información que es posible capturar y las diferentes posibilidades para violar la confidencialidad de la red, es de resaltar que la falta de robustecimiento abre las puertas para diferentes tipos de ataques hacia la red inalámbrica y su posterior escalamiento hacia la demás infraestructura de una organización.

5.3.4 Prueba de vulnerabilidades *(Pentesting)*. Para lograr este tipo de pruebas, se realiza una recolección desde la perspectiva de la red interna, como anteriormente es mencionado, el hecho de que la red de invitados permita la conexión a los demás dominios pertenecientes a la red corporativa, deja un abanico de vulnerabilidades que permite al atacante realizar diferentes tipos de ataque.

Se procedió con el *pentesting* basado en la metodología *NIST (SP 800-115)*[44], bajo esta metodología se simula un ataque real, aún así, generó como reto el tener que identificar la forma de evadir la seguridad de la red, aplicación o los servidores presentes en la infraestructura. Las pruebas involucran una explotación combinada de todas las vulnerabilidades, con el fin de ganar todos los privilegios posibles, el proceso fue realizado sobre las siguientes 4 fases:

- Planeación
- Descubrimiento
- Ataque
- Reportes

Para fines prácticos se realizaron las fases de planeación, descubrimiento y ataque, siendo suficiente para demostrar las vulnerabilidades presentes en la red inalámbrica corporativa. En el análisis inicial se determinó el fallo a nivel de red, por consiguiente, se tiene un objetivo claro que es: el acceso a las plataformas con vulnerabilidades de seguridad, una vez se realice la conexión por la red inalámbrica corporativa.

Para ello se realizó una planeación previa donde se reconocen estos objetivos, igualmente hubo un proceso de descubrimiento de los elementos de la infraestructura y los servicios publicados, este proceso fue ejecutado bajo las técnicas de recolección pasivas y activas, al obtener esta información se presentan las diferentes alternativas de ataque para lograr acceso a las plataformas, que en la práctica culminan con el proceso de obtención de credenciales de uno de los *Web Services* de la organización que es publicado bajo el protcolo *http* (Hypertext Transfer Protocol - Protocolo de transferencia de hipertexto), que en la actualidad es un protocolo categorizado como inseguro y reemplazado por su predecesor *https*.

[44] BEHIQUE DIGITAL. Metodología de Pruebas de Intrusión en la NIST SP 800-115, de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/. 2017. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/.

5.3.4.1 Planeación de las pruebas. Al ser un caso simulado, solo se indicó el proceso a seguir en esta fase, en la que debe establecerse una comunicación con el área directamente interesada en el proceso de *pentesting*, por lo tanto se procede a realizar un análisis documentado de los alcances, clarificación de objetivos y se establecen acuerdos de accesos y confidencialidad, lo anteriormente descrito, plasmado en un documento firmado por las partes, igualmente se define el horario de la ejecución de este proceso, bajo un cronograma establecido con fechas y franjas horarios teniendo en cuenta que siendo un procedimiento intrusivo puede afectar en cierta medida la operatividad.

5.3.4.2 Descubrimiento- Recolección de la información. En el proceso de obtención de información, una vez descrito el análisis inicial, se procede a utilizar las técnicas de recolección pasivas y activas, con el fin de extraer la mayor cantidad de información que permita el avance de las siguientes fases, se enmarca la fase 1 como clave para el desarrollo final de todas las pruebas realizadas, siendo así que, un alto porcentaje del éxito depende de una buena obtención de información.

Durante la recolección pasiva se utilizó la técnica de obtención *footprinting* (búsqueda de información pública) y en la activa se utilizó la obtención bajo *fingerprinting* (búsqueda de información privada e interna), de esta manera se logró obtener desde dos perspectivas diferentes la información, que permitió identificar vulnerabilidades expuestas en la red interna, como desde el lado externo a la red.

Recolección Pasiva - *Footprinting*, al ser un caso práctico y simulado, esta técnica indica que se debe realizar un análisis exhaustivo del *front-end* de las organizaciones expuesto en la red pública, precisando recopilar información pública en el internet

- Nombre de la Empresa, Redes Sociales, Teléfonos, Dominios de correo, Organigrama, *IPs* públicas, *DNS*, *URLs* publicadas

Como alternativa de recolección de información del *footprinting,* se puede asumir la utilización de técnicas de ingeniería social, para así lograr obtener la contraseña de acceso utilizada en el portal cautivo, por consiguiente, la búsqueda y el resultado más relevante de dicho proceso fue: **la obtención de la clave** que permitió la conexión a la red creada para los invitados**.**

Recolección Activa - *Fingertprinting*, bajo esta técnica, se realizó la conexión a la red de invitados y a partir de esto, se inició con un proceso de identificación de la infraestructura tecnológica de la organización. Teniendo conocimiento del alcance a las diferentes redes, por medio de la conexión de invitados, se procede con un escaneo de puertos con la herramienta ***Zenmap,*** que es una interfaz gráfica de ***Nmap***, enumerando en esta búsqueda los principales puertos de administración de los sistemas.

Para lograr el objetivo de poder saltar a multiples dispositivos como lo son: Access Points, controladora inalámbrica, servidores o cualquier elemento de la infraestructura, se hace un escaneo a la red **10.142.0.0/19** como se ilustra en la Figura 31, asumiendo que se deben encontrar varios dominios funcionales de la red sobre este rango, adicional a esto, el escaneo es realizo por los puertos comunes de administración **22 (ssh), 80 (http), 443 (https)**, demostrando así otra falencia de *hardening* sobre la red y es administrar los servicios por puertos bien conocidos.

Figura 31. Cálculo de alcance a los dominios de Red

Fuente: El autor.

Para el análisis con la herramienta ***Zenmap*** Se realiza un escaneo en modo *TCP sync (Transmission Control Protocol Synchronized)*, que tiene la capacidad de determinar si los puertos definidos como objetivos están escuchando bajo la técnica de escaneo *half-opening*. Puesto que su modo de funcionamiento inicia como una conexión normal, pero no llega a establecerse un *handshake* en ambas partes, solo se envia un único paquete *SYN* y se espera la respuesta, ***SYN/ACK* o *RST*** automáticamente se determina que el puerto está en escucha.

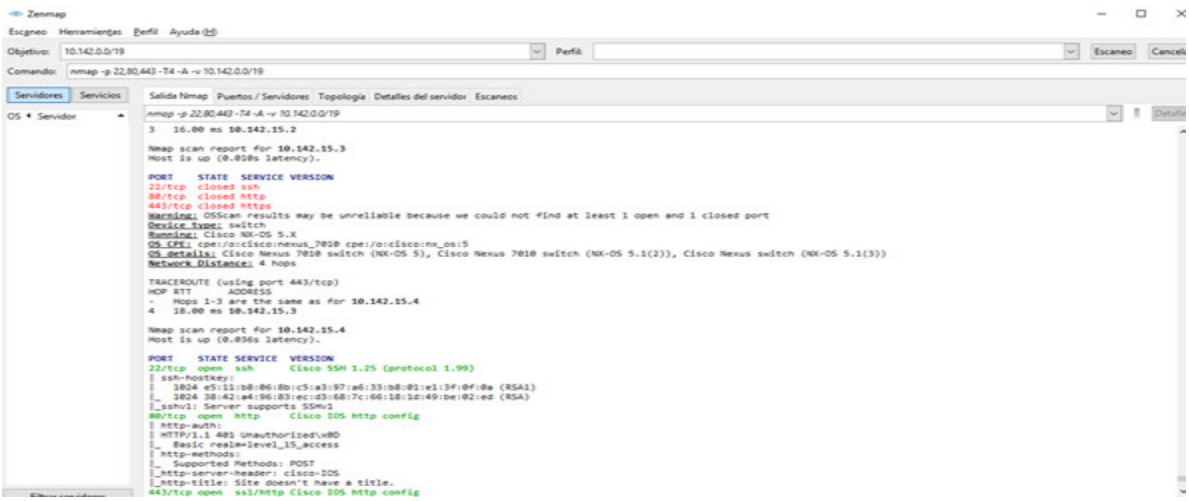
Para ello se escribe la siguiente línea de comandos:

Nmap –p (Puerto o puertos) **–T4**(Modo de escaneo agresivo) –**A** (Análisis agresivo) **-v** (Incrementar el nivel de detalle del escaneo) **10.142.0.0/19** (Red objetivo)

nmap -p 22,80,443 -T4 -A -v 10.142.0.0/19

Bajo este escaneo, se identificaron diferentes tipos de servidores, versiones de sistemas operativos y elementos de red, que pudiesen facilitar al atacante armar una topología e identificar qué equipos se utilizan en toda la infraestructura tecnológica. A partir de este escaneo uno de los ataques puede ser dirigido sobre los sistemas operativos que se encuentren con vulnerabilidades por versiones desactualizadas, así como también se puede vectorizar el ataque por puertos vulnerables. La técnica evidenciada a continuación es ilustrada en la Figura 32, y abre un abanico de oportunidades a los atacantes para determinar sus objetivos y técnicas de ataque a utilizar.

Figura 32. Escaneo sobre un rango de red calculado



Fuente: El autor

Dentro del escaneo, se pudo evidenciar un balanceador de carga, de marca de fábrica F5, con su *IP* de administración y los puertos por los cuales permite el ingreso, así como el sistema operativo y la versión en el cual está basado, de manera adicional en el escaneo se evidenciaron muchos dispositivos propios de la infraestructura TI, determinando que dicha prueba de escaneo resulto en una

intrusión total a la red empresarial, debido a las fallas de diseño y seguridad de la misma.

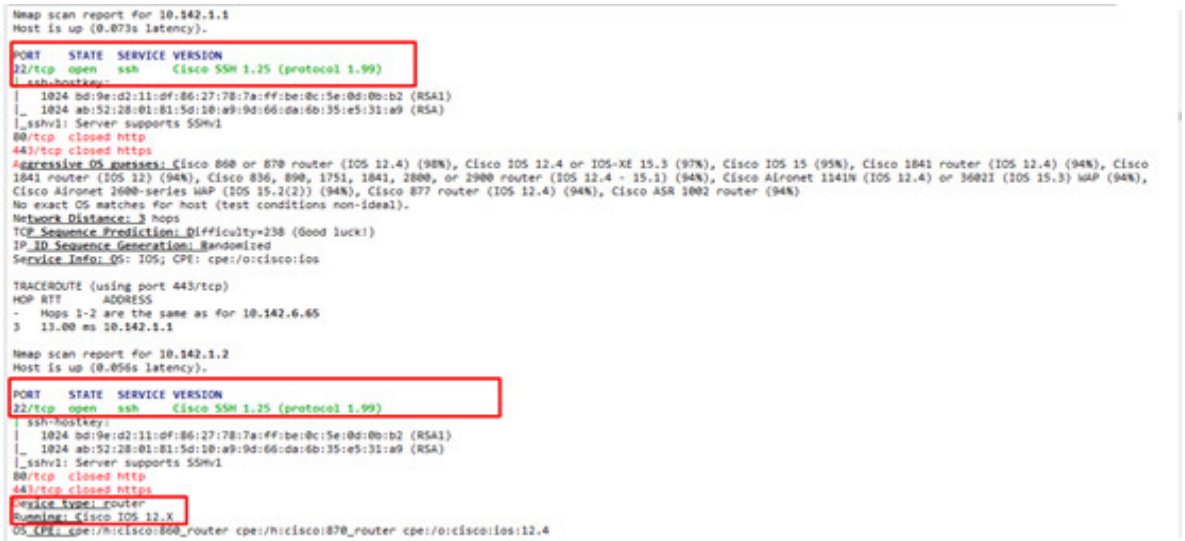
Como se evidencia en las Figura 33, quedaron al descubierto múltiples plataformas de la infraestructura de la organización en conjunto con nombres de fabricantes, tipo de equipos y puertos de servicio que pueden ser atacados con diferentes herramientas de *exploits* (Explotación de sistemas).

Figura 33. Escaneo y descubrimiento de infraestructura de la Red

Fuente: El autor.

El escaneo a la red bajo la herramienta *nmap* desde la conexión de invitados, permitió el reconocimiento de otros elementos de red, *routers* (enrutadores) *y switchs* (conmutadores), estos dispositivos fueron descubiertos bajo un escaneo a un rango que se consideró que la organización utiliza para segmentar su red corporativa, como lo evidencia la Figura 34.

Figura 34. Escaneo y descubrimiento de elementos de Red



Fuente: El autor.

Una de las evidencias más relevantes y sobre la cual se identificó una vulnerabilidad, es el alcance a un sistema de Energía *Liebert*, descrito en la Figura 35, cuya apertura del puerto 80 de la *ip* 10.142.1.100, es la que permite avanzar a la siguiente fase del *pentesting,* en la que se realiza un ataque pasivo, ya que el ingreso inicial al dispositivo no solicita ninguna contraseña, como se evidencia en la Figura 36.

Figura 35. Escaneo y descubrimiento de una plataforma insegura

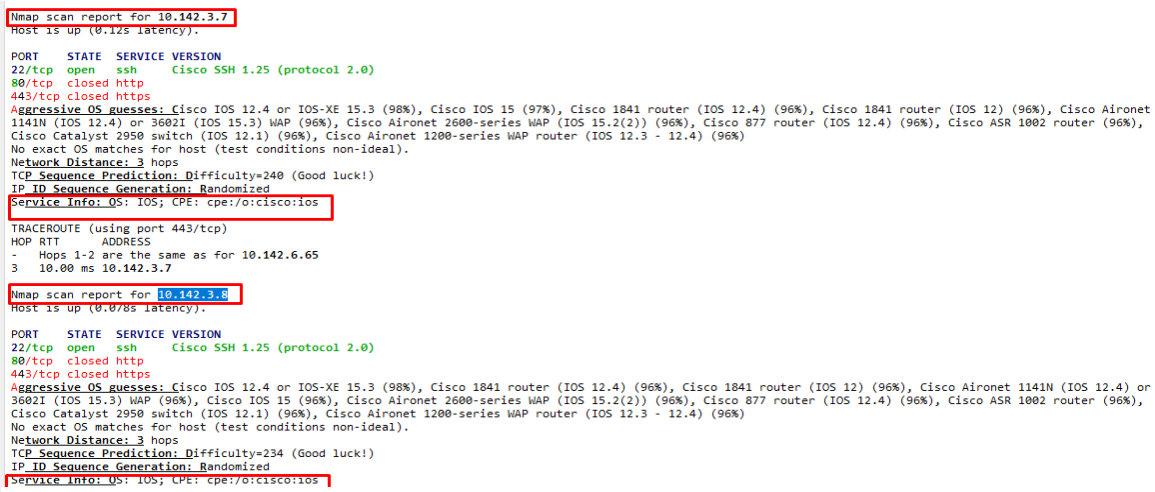
Fuente: El autor.

Figura 36. Acceso web a sistema de energía vulnerable

Fuente: El autor.

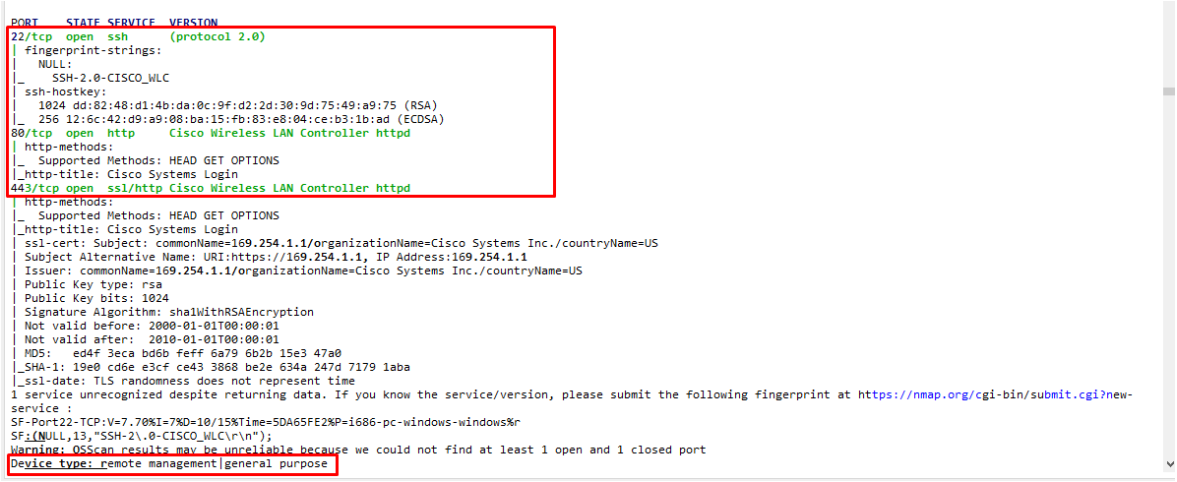
Finalmente, en el escaneo se logró la identificación de una controladora inalámbrica y a los puntos de accesos *APs*, que permiten la conexión a la red demostrando así, el hueco de seguridad empresarial que puede dejar un mal diseño y configuración de la red inalámbrica y la red en general, la Figura 37, ilustra las IPs de administración de los dispositivos inalámbricos, mientras que en la Figura 38 ilustra la IP de administración de la controladora inalámbrica.

Figura 37. Identificación de la IP de administración de los Acces Points



Fuente: El autor.

Figura 38. Identificación de la IP de administración de la WLC



Fuente: El autor.

Una vez escaneada, toda la red y conociendo la infraestructura tecnológica, es posible proceder con diferentes tipos de ataques ya sean pasivos o activos que permitan evadir los elementos de seguridad y los controles adicionales implementados en la red, como se evidencia en el *pentesting*, la infraestructura de red es el primer *front* y el más importante a nivel de seguridad y siendo este vulnerado, existe un mundo de posibilidades en cuanto ataques a cualquier elemento que se encuentre dentro de dicha red.

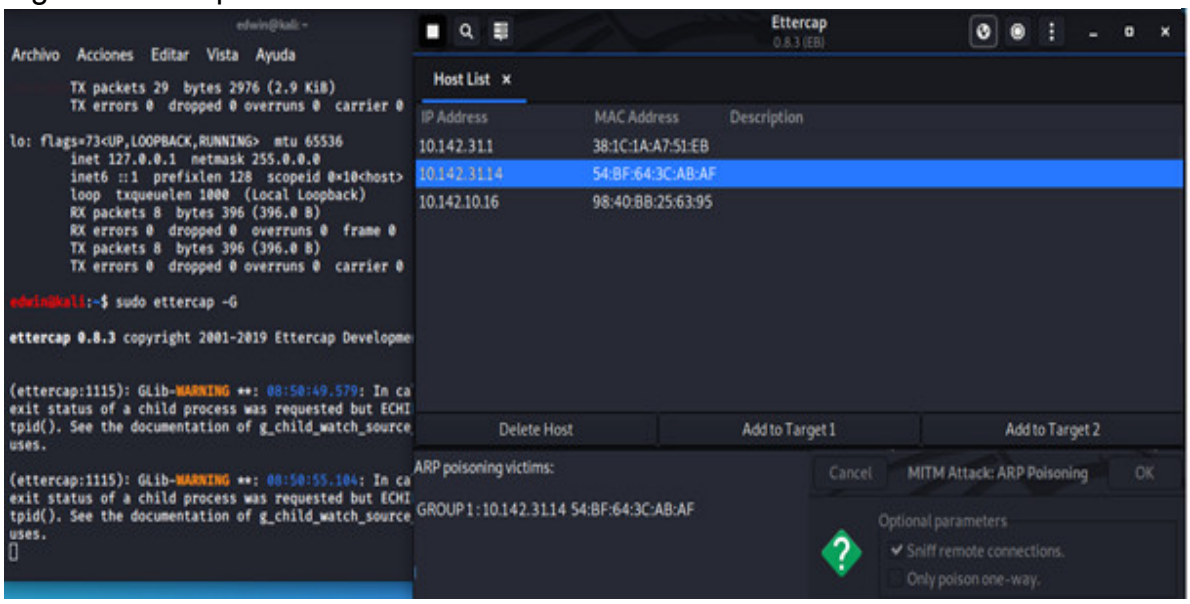
5.3.4.3 Ataque. Teniendo un conocimiento más amplio de la organización y de los objetivos a trabajar descritos en la planeación, se procedió con la vectorización de los ataques, para determinar más vulnerabilidades y generar el acceso a las plataformas. Para dicho fin fue de utilidad el escaneo realizado con *Zenmap*, que permitieron la identificación de los puertos de servicio de las aplicaciones, infraestructura, plataformas y *web services* (servicios web).

Al realizar la identificación de vulnerabilidades, a nivel de conectividad, escalamiento a diferentes segmentos de red, identificación de servicios expuestos sobre puertos inseguros como el *http* (Hypertext Transfer Protocol- Protocolo de Transferencia de Hipertexto), se realizó el ataque pasivo a la página Web del sistema de energía *Liebert* mencionado.

Para el ataque pasivo en el que se desea obtener la contraseña de acceso al *web service*, se utiliza el *software ettercap* (interceptador) que permite un ataque de tipo *MiTM* (*Man-in-The-Middle Attack- Ataque de hombre en el medio*). Para lograr dicho objetivo se realizó un envenenamiento *ARP*, haciendo creer a la maquina atacante es el *router*, por lo cual el trafico pasa directamente por la maquina atacante, permitiendo que en el momento que el *host* atacado dentro de la red ingrese al portal web del sistema de energía se realice la captura de la información en texto plano de la contraseña que digitó.

La Figura 39, evidencia el proceso de ataque *MiTM*, realizado bajo el software *ettercap* que funciona como programa de sniffing y que es de uso común en procesos de auditorías, por sus alternas funcionalidades de interceptación de protocolos *http*, *SSL* e incluso permite la inyección de caracteres. Para la ejecución del software se utilizó el virtualizador *VirtualBox* y sobre él se corrió el sistema operativo *Kali Linux,* mismo que contiene el software de ataque.

Figura 39. Ataque *MiTM* con Envenenamiento *ARP*

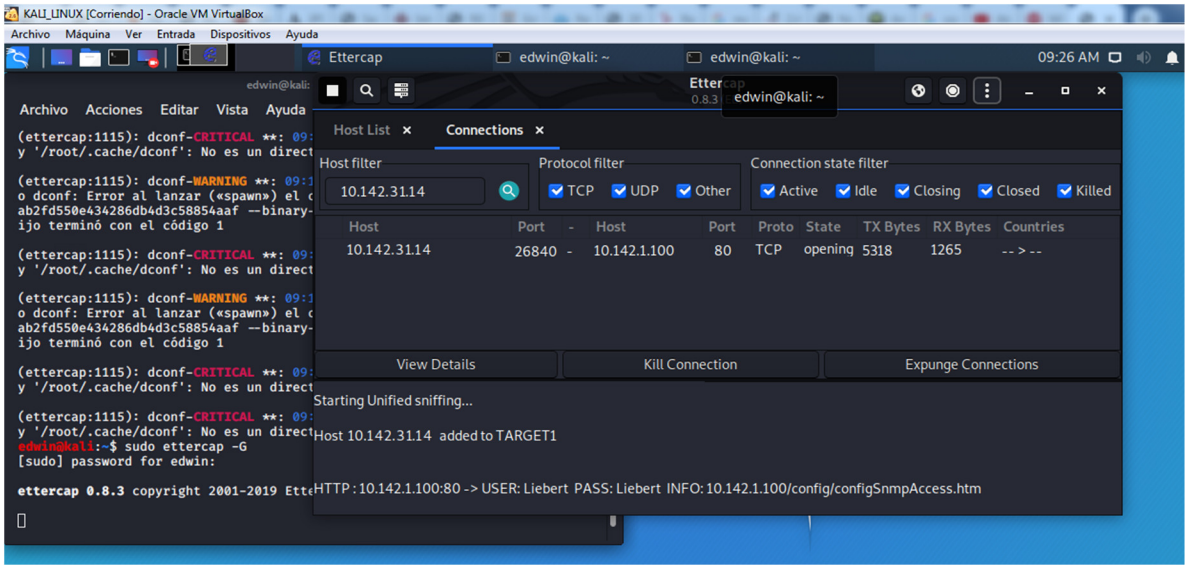


Fuente: El autor.

Como se evidencia a continuación, una vez envenenada la tabla *ARP,* se realizó escucha de las peticiones http realizadas por el host atacado, hacia el sistema de energía *Liebert*, obteniendo las credenciales de acceso y con esto se da por

finiquitado el ataque pasivo por medio de un *sniffing* hacia la plataforma como lo ilustra la Figura 40.

Figura 40. Ataque *MiTM* con *sniffing* exitoso



Fuente: El autor.

5.4 DOCUMENTACIÓN DE VULNERABILIDADES Y GENERACIÓN DE RECOMENDACIONES DE SEGURIDAD EN LAS REDES SIN HILOS COPORATIVAS

Dicha ofensiva como se describió anteriormente, fue realizada bajo algunas fases de la metodología *NIST (SP800-115)* indicadas por Scarfone[45], en donde existe una planeación del objetivo, una fase de descubrimiento de puertos, de servicios y *hosts*, toda esta técnica fue elaborada hasta llegar a la fase de ataque pasivo, que fácilmente como se evidencia en el *pentesting* puede convertirse en un ataque activo. Al obtener la conectividad, se puede no solo escuchar el trafico, cabe la posibilidad de vulnerar todos los pilares de la seguridad informática, por actos de manipulación de información o denegación servicios de toda la red.

[45] SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUGH, Angela. (Technical Guide to Information Security Testing and Assessment (No. NIST Special Publication (SP) 800-115). National Institute of Standards and Technology. 2008. 6p. En Línea]. [Consultado el 11, octubre, 2019] Disponible en https://doi.org/10.6028/NIST.SP.800-115

5.4.1 Vulnerabilidades identificadas. Bajo el caso práctico se identificaron: múltiples errores de configuración de plataformas, falta de robustecimiento sobre la red, vulnerabilidad de acceso a diferentes segmentos de red, servicios expuestos inseguros mostrados por lo puertos asignados por *default* (defecto), sistemas de contraseñas simples e inseguras, falta de herramientas de monitoreo y de prevención activa que detecten las intrusiones. De manera descriptiva se identificó:

- Facilidad en la ejecución de ingeniería social
- Fragilidad en contraseñas
- Falta de monitoreo sobre el comportamiento de la red
- Fallas de aseguramiento en la red, a pesar de existir una segmentación de la red, se evidencia que desde la *VLAN* de invitados se puede saltar a otros segmentos de la red corporativa
- La no existencia de un sistema IDS/IPS que evite el escaneo sobre la red y evitase los ataques de hombre en el medio

5.4.2 Consideraciones de seguridad. La implementación de toda tecnología debe llevar consigo un plan de protección y respaldo de la misma, no es la excepción para las redes inalámbricas corporativas. Monsalve[46], documenta que se debe contemplar la seguridad como un factor relevante, previo a la puesta en producción de servicios y tecnologías es importante realizar un análisis de las necesidades de dicha red en el ámbito empresarial y tomar en consideración factores de seguridad tales como:

- Segmentación de la red
- Controles de acceso
- Defensa Integral de la red

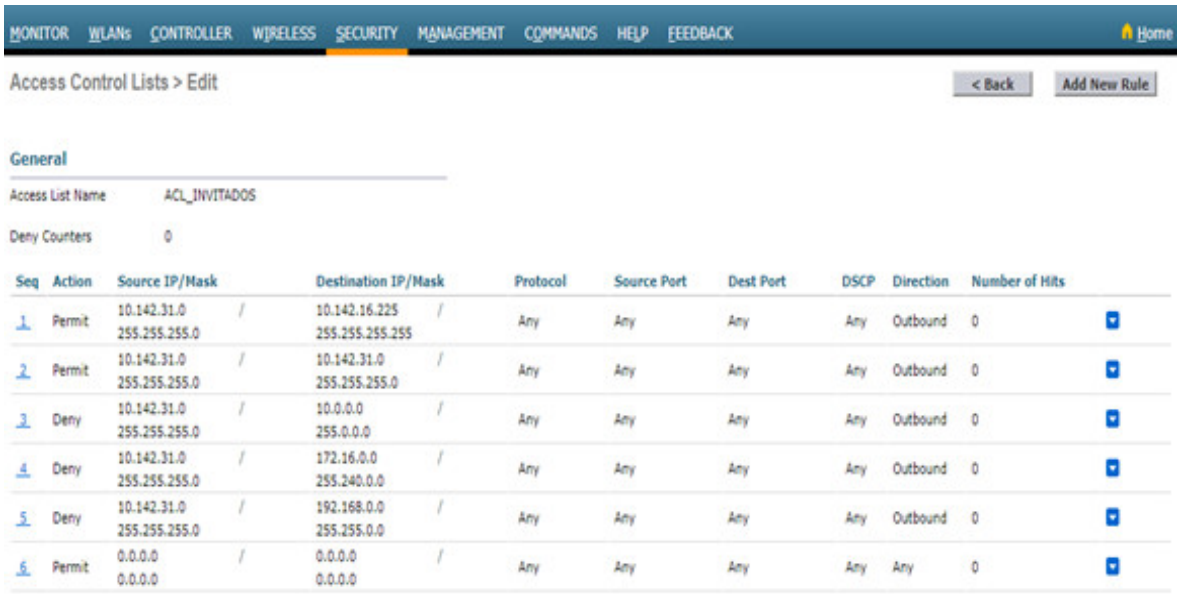
5.4.2.1 Segmentación de la red. Como regla general de las redes empresariales, estas deben ser segmentadas con el objetivo evitar puntos únicos de fallo, mejorando rendimientos a nivel de carga y tráfico. La segmentación permite garantizar una mayor seguridad y escalabilidad de la red y los servicios, permitiendo crear reglas de seguridad más específicas sobre cada subred y así aislar focos de

[46] MONSALVE Pulido, Julián. A.; APONTE Novoa, Fredy. A; CHAPARRO Becerra, Fabian. Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. Dyna, 82(189), 226– 232. 2015. [En Línea]. [Consultado el 02 noviembre, 2019] Disponible en: http://www.scielo.org.co/pdf/dyna/v82n189/v82n189a28.pdf

falla y por consiguiente mejorar el tiempo de respuesta a la solución de inconvenientes presentados

5.4.2.2 Controles de acceso sobre las controladoras inalámbricas. Para cubrir el acceso de los invitados o la red inalámbrica en general. García[47], indica que las redes inalámbricas en su diseño y configuración se deben contar con diferentes mecanismos de control de acceso, uno de los controles eficientes se basa en crear listas de control de acceso que impidan a dichos usuarios alcanzar dominios corporativos; En el caso práctico es la medida de seguridad más importante a considerar, sobre el sistema de *WLC Cisco,* como se ilutra en la Figura 41, aun así existen diversas herramientas a desplegar según sea el nivel de *hardening* deseado.

Figura 41. ACL sobre la WLC para evitar alcanzar dominios corporativos



Fuente: El autor, modificaciones bajo la palataforma *virtual cisco controller*.

[47] GARCÍA, Ruby R. Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central “Marta Abreu” de Las Villas. Santa Clara. 2011. 2p. [En Línea]. [Consultado el 07, noviembre, 2019] Disponible en: https://dspace.uclv.edu.cu/bitstream/handle/123456789/6853/Rubersy%20Ramos%20Garc%C3%ADa.pdf?sequence=1&isAllowed=y

5.4.2.3 Defensa integral de la red. La defensa integral de la red, como es indicado por Castro[48], está compuesta por múltiples configuraciones tanto en las controladoras inalámbricas, como en todos los elementos que componen la red local o metropolitana, según sea el caso. Una de estas configuraciones es la aplicación de firmas estandarizadas de tipo *IDS* (Intrusion Detection System – Sistemas de Detección de Intrusos) con la que cuenta la *WLC de Cisco*[49], cuyo objetivo es el de monitorear e informar eventos anómalos del tráfico que atraviesa por la red inalámbrica y basado en las firmas y actualizaciones de la controladora permita mantener otro frente de protección y aseguramiento.

Actualmente las plataformas inalámbricas de Cisco cuentan con mecanismos más avanzados de proteccion y prevención, anteriormente esta plataforma contaba con sistemas de IDS (Intrusion Detection System – Sistema de Prevención de Intrusos), en la actualidad la plataforma inalámbrica cuenta con un sistema de *IPS* (Intrusion Prevention System – Sistema de Prevención de Intrusos) en constante actualización de firmas, permitiendo así que no solo sean reportadas las amenazas detectadas, sino que se realice una acción que permita evitarlas

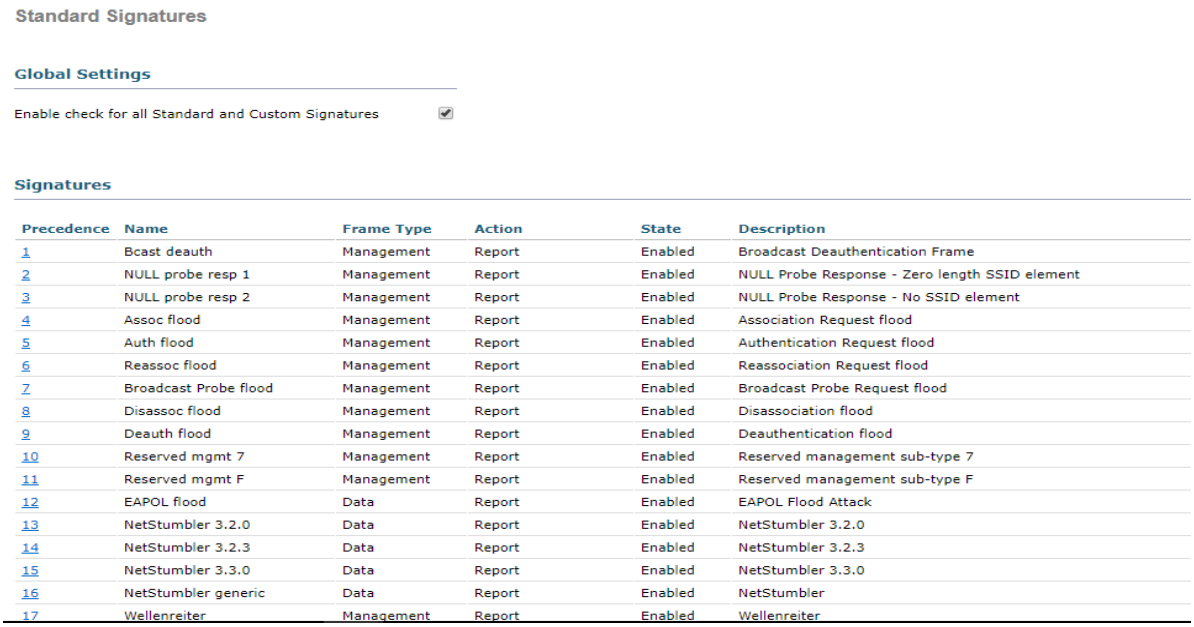
Cisco[50], de manera adicional, recomienda y enfatiza en la importancia de que los dispositivos cuenten con la última actualización estable del sistema operativo recomendada por el fabricante, con el objetivo de actualizar funcionalidades, servicios y a su vez eliminar *bugs* y vulnerabilidades identificadas y resueltas en la liberación de las actualizaciones, la Figura 42, ilustra algunas de las firmas de *IDS/IPS* por defecto con que cuenta la plataforma de la controladora inalámbrica, para la cual se tiene la opción de detectar y reportas o sea la conveniencia tomar acciones.

[48] CASTRO, Rodrigo. (Avanzando en la seguridad de las redes Wifi. Enfoques 73. 2005. , pp. 23-32 [En Línea]. [Consultado el 24, noviembre, 2019]. Disponible en: http://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

[49] CISCO. Guía de despliegue inalámbrico del regulador de las Cisco 2500 Series. 2016, 1p. [En Línea]. [Consultado el 02, octubre, 2019] Disponible en: https://www.cisco.com/c/es_mx/support/docs/wireless/2500-series-wireless-controllers/113034-2500-deploy-guide-00.html

[50] CISCO. (2019). Wireless LAN Controller (WLC) Software Upgrade - [En Línea]. [Consultado el 22, noviembre, 2019] Disponible en: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/68835-wlc-upgrade.html

Figura 42. Implementación de firmas de IDS en WLC



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Management	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Management	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Management	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Management	Report	Enabled	Association Request flood
5	Auth flood	Management	Report	Enabled	Authentication Request flood
6	Reassoc flood	Management	Report	Enabled	Reassociation Request flood
7	Broadcast Probe flood	Management	Report	Enabled	Broadcast Probe Request flood
8	Disassoc flood	Management	Report	Enabled	Disassociation flood
9	Deauth flood	Management	Report	Enabled	Deauthentication flood
10	Reserved mgmt 7	Management	Report	Enabled	Reserved management sub-type 7
11	Reserved mgmt F	Management	Report	Enabled	Reserved management sub-type F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Management	Report	Enabled	Wellenreiter

Fuente: El autor, bajo la palataforma *virtual cisco controller*

Sabogal[51], advierte que los equipos (Computadoras) corporativos deben estar bajo las políticas de seguridad de organizacional creadas bajo el criterio del área encargada de la seguridad informática de la compañía. Los dispositivos externos que se conecten a la red inalámbrica, como no tienen aseguramiento e incluso ninguna política de control, deberán tener conectividad aislada de los dominios corporativos, sin permitir interactuar entre ellos.

Pastor[52], indica la importancia de habilitar en las controladoras un mecanismo de protección que impida las conexiones duales, de esta manera se evitan la reutilización de conexiones, que dan cabida a los ataques de suplantación por *MAC*. Es importante realizar un proceso de *hardening* sobre los elementos de red, en mayor medida este aseguramiento debe ser realizado antes de desplegarlo sobre la misma red, evitando que el dispositivo una vez se encuentre en producción presente falencias de seguridad que permitan al intruso realizar manipulación de

[51] SABOGAL ROZO, Esther Angélica. Proyecto de Seguridad Informática I. Bogotá: Universidad Nacional Abierta y A Distancia, 2013. 54-56p. [En Línea]. [Consultado el 02, diciembre 2019] Disponible en: https://www.academia.edu/6240795/

[52] PASTOR SATORRAS, Romualdo; VESPIGNANI, Alessandro. Epidemic spreading in scale-free networks. Phys. Rev. Lett. 2001, 21p. [En Línea]. [Consultado el 06, diciembre 2019] Disponible en: https://www.cs.princeton.edu/courses/archive/fall03/cs323/links/pastor-satorras.pdf

elementos de la infraestructura y violar los pilares fundamentales de la seguridad informática.

Es de relevancia utilizar las funcionalidades de seguridad de las plataformas e implementar sistemas de *IDS/IPS*, que realicen análisis constante sobre el comportamiento del tráfico y que permitan identificar y bloquear los análisis persistentes que realizan herramientas como el *Zenmap, Wireshark*, entre otras. Igualmente, el habilitar sistemas de monitoreo propios de las controladoras basados en firmas de *IDS o IPS,* permiten localizar o bloquear usuarios infractores bajo los diferentes tipos de ataques que puedan experimentar una red sin hilos corporativa.

Se deben establecer políticas de seguridad que controlen la navegación de los visitantes, igualmente es importante generar un monitoreo sobre las conexiones del personal externo a la compañía, esta configuración debe ser realizada teniendo en cuenta algunas características correspondientes al servicio que desee prestar la compañía a los visitantes, ya que a nivel general no se requieren altas velocidades o conectividad específica a segmentos de la red corporativa.

Parametrizar las configuraciones en las redes inalámbricas sobre los canales, frecuencias, encriptación, colocación y servicios a prestar por la red corporativa inalámbrica, todo esto basado en el análisis de seguridad específico para las organizaciones. Según Gareth[53], se debe realizar un *site survey* con la finalidad de tener éxito en el proceso de despliegue de los puntos de acceso y cubrimiento correcto, ofreciendo la cobertura estrictamente necesaria, evitando que se pueda prestar conectividad en áreas que no pertenecen a la organización corporativa.

En el proceso de *hardening* de la red corporativa se debe implementar aislamiento lógico de la red inalámbrica, evitando un escalamiento en caso de que se obtenga acceso mal intencionado, por consiguiente, se deben definir los accesos específicos a las redes externas, a la *DMZ* (Demilitarized Zone - Zona Desmilitarizada) y el acceso controlado a las demás redes internas y de servidores si esto lo requiere, es recomendable implementar un *SSID* no descriptivo, la exposición del nombre de la compañía por temas de seguridad informática no es recomendable, validar el

[53] GARETH, Owen; MO, Adda. SOLS: Self Organising Distributed Location Server for Wireless Ad Hoc Networks. 2009, 1p. [En Línea]. [Consultado el 03, agosto, 2020] Disponible en: https://www.academia.edu/33094804/SOLS_Self_Organising_Distributed_Location_Server_for_Wireless_Ad_Hoc_Networks

ocultamiento del *SSID* es una buena práctica, de tal manera que sea visible a los ataques y conforme otra barrera de seguridad a la red corporativa.

Según Astaiza[54], se debe contar con un proceso de selección dispositivos inalámbricos, dicha elección debe estar basada en su robustez de funcionamiento, seguridad, reconocimiento en el mercado, y este mismo proceso se debe realizar con los *APs* que garanticen las necesidades del negocio y así mismo permitan un aseguramiento de la red y los servicios que exponen y propagan.

5.4.3 Recomendaciones de seguridad y mejores prácticas de configuración para plataformas inalámbricas WLC Cisco. Bajo la Plataforma *WLC CISCO* trabajada, existen múltiples recomendaciones de seguridad, indicadas por el fabricante Cisco[55], con el objetivo de salvaguardar la seguridad de la infraestructura de la red y la seguridad misma de los dispositivos, por ello es importante aplicar *hardening* de manera categorizada y según se ajuste a la compañía, dicho aseguramiento está basado en aspectos tales como: infraestructura, Seguridad y un motor de servicios de identidad.

5.4.3.1 Recomendaciones de Hardening a nivel de infraestructura. Se recomienda la utilización de un DHCP externo, puesto que en las *WLC CISCO* dicho servidor no es diseñado para despliegues a gran escala empresarial, se recomienda habilitar funcionalidades de visibilidad de usuarios y así permitir realizar un análisis de tiempo real de los usuarios conectados a la red inalámbrica y de las aplicaciones que el usuario utiliza, la Figura 43, ilustra el proceso de *hardening* a nivel de infraestructura que fue ejecutado en la controladora inalámbrica, basado en las recomendaciones de *cisco* descritas a continuación.

- ✓ Importante inhabilitar la administración y gestión de la controladora por vía inalámbrica y permitir su gestión por el sistema de web seguro *HTTPS*

[54] ASTAIZA HOYOS, Evelio; BERMUDEZ OROZCO, Hector; TRUJILLO DAVILA, Dora. 2014. Selección de access point en redes inalámbricas 802.11 garantizando mínima QoS. Ingeniería y Ciencia, 10(20), 115–137. [En Línea]. [Consultado el 21, agosto, 2019] Disponible en: http://www.academia.edu/7582669/Selecci%C3%B3n_de_Access_Point_en_Redes_Inal%C3%A1mbricas_802.11Garantizando_m%C3%ADnima_QoS

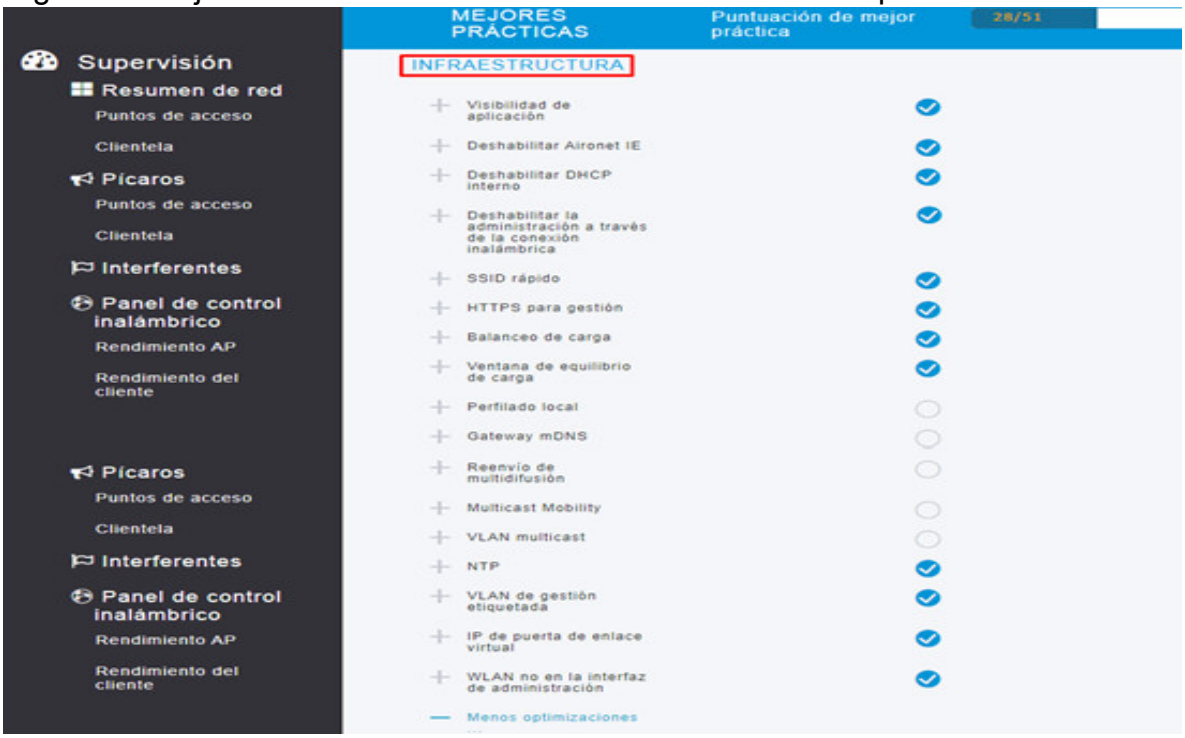
[55] CISCO. 2015. Cisco Wireless Controller Best Practices—RF Management [En Línea]. [Consultado el 19, abril, 2020] Disponible en https://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc/rfmgmt.html

(*HyperText Transfer Protocol Secure* - Protocolo de transferencia de hipertexto), adicional a esto se recomienda habilitar el sistema de balanceo de carga permite entre las redes inalámbricas creadas y sus *APs.*

- ✓ Habilitar el protocolo *NTP* (*Network Time Protocol* – Protocolo de Tiempo de Red), necesario para la sincronización de la *WLC* en procesos de autenticación y sincronización de *traps* (trampas) y *snmp* (*Simple Network Management Protocol* – Protocolo de Administración Simple de Red), igualmente se recomienda habilitar el *Fast SSID* permitiendo a los clientes moverse más rápido entre los *SSID* existentes, no menos importante es dividir el tráfico de administración con el de servicio.

- ✓ Configurar una puerta de enlace virtual que no estén sobre las redes asignadas a Internet en **RFC5737**, esta puerta de enlace será utilizada para re direccionar y permitir la autenticación de usuarios externos que se conectan por los portales cautivos.

Figura 43.Mejores Prácticas de Infraestructura recomendada por *WLC Cisco*



Fuente: El autor, modificaciones bajo la palataforma *virtual cisco controller*

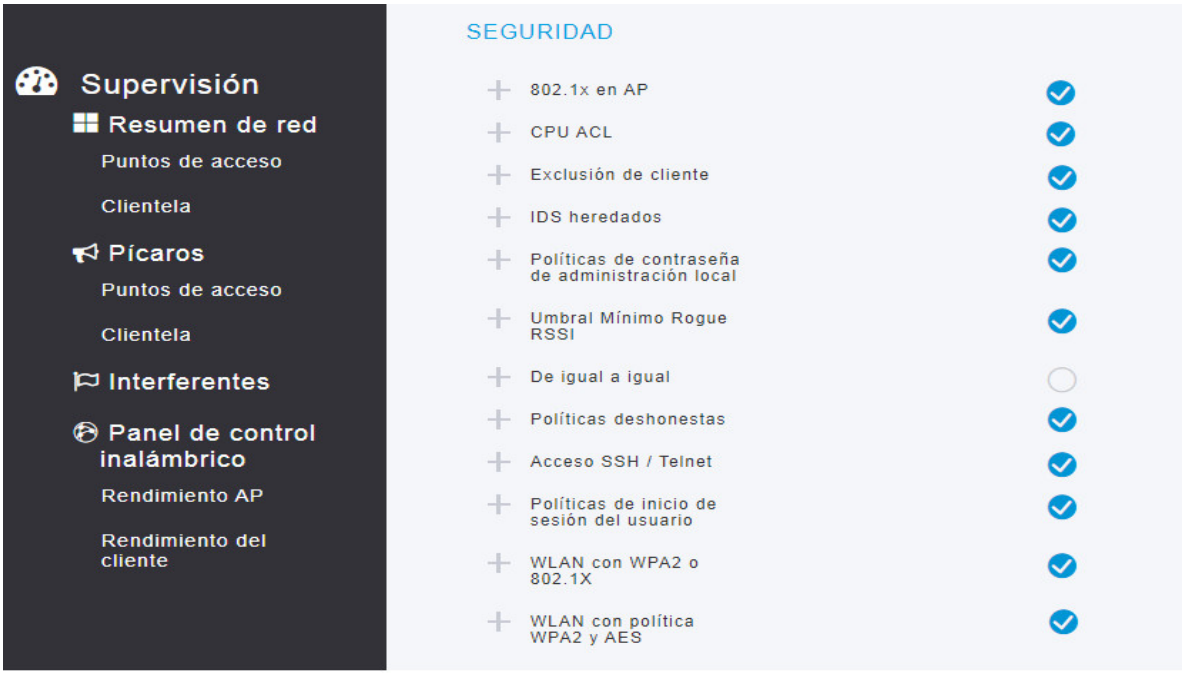
5.4.3.2 Recomendaciones de Hardening a nivel de seguridad. Se recomienda habilitar la autenticación dot1x contra los *APs* y así permitir que esta autenticación sea autorizada por un servidor *RADIUS (Remote Authentication Dial-In User Service)* y que se permita el control de los solicitantes de la conexión, igual de importante y recomendado es activar las *CPU ACL (Central Processing Unit / Acces Control List)*, controlando el acceso a la controladora por medio de protocolos de administración filtrados y específicos como *SNMP, SSH (Secure Shell),* etc. la Figura 44, ilustra el proceso de *hardening* a nivel de seguridad que fue ejecutado en la controladora inalámbrica, basado en las recomendaciones de *cisco* descritas a continuación.

- ✓ Habilitar las políticas de exclusión de clientes bajo algunas condiciones específicas y así evitar que la red sufra ataques de autenticación y asociación, igualmente habilitar las firmas de *IDS/IPS* que permiten su actualización constante con la *Cloud Cisco* y así evitar los múltiples ataques de intrusión. Cabe destacar que se deben contar con políticas de contraseñas seguras y políticas de control de autenticación local, limitando así conexiones paralelas e inicios de sesión simultáneos que accedan a la controladora inalámbrica, tarea que se realiza bajo una comprobación de autenticación consecutiva. Con lo referente a la política de credenciales se deben configurar contraseñas robustas y con parámetros de longitud y caracteres específicos.

- ✓ No se recomienda que se utilice el protocolo WPA por las vulnerabilidades indicadas y por su fragilidad a nivel de seguridad, recomendable habilitar WPA2 bajo el algoritmo *AES*. Existen buenas razones para utilizar el sistema de políticas no autorizadas, llevando así un control de acceso que permita minimizar los riesgos de seguridad a los que se exponen la compañía, por el mal uso del servicio de los mismos clientes internos.

- ✓ A nivel de autenticación, *Cisco* recomienda la utilización de un servidor *NPS (Network Policy Server* – Servidor de Políticas de Red), que permite establecer un mayor nivel de seguridad y monitoreo basado en una autenticación bajo directorio activo y así brindar seguridad al acceso a la *WLAN,* esta herramienta es complementada con un servidor *RADIUS* bajo métodos de *EAP, EAP-TLS, EAP-MS-CHAP v2 y PEAP.*

Figura 44. Mejores Prácticas de Seguridad recomendada por WLC Cisco

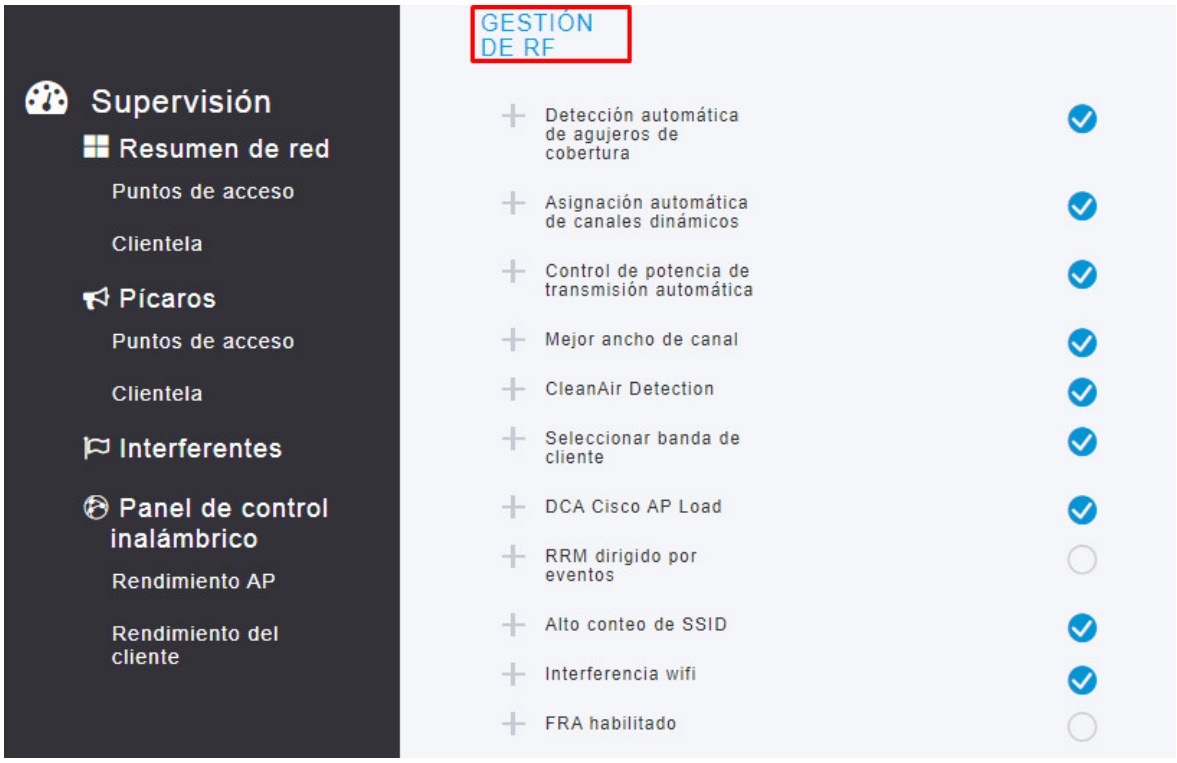


Fuente: El autor, modificaciones bajo la palataforma *virtual cisco controller*

5.4.3.3 Recomendaciones de Hardening a nivel de Gestión de las RF. Se recomienda la habilitación del sistema de detección de agujeros de cobertura para permitir a los APs aumentar o disminuir de manera automática sus niveles de potencia para optimizar la cobertura y señal de la red. Igualmente debe ser complementado con la asignación automática de canales en las diferentes bandas de frecuencia, así como el control de potencias de transmisión. Figura 45, ilustra el proceso de *hardening* a nivel de gestión de las *RF* que fue ejecutado en la controladora inalámbrica, basado en las recomendaciones de *cisco* descritas a continuación.

- ✓ Habilitar las mejoras del ancho del canal permitirá reducir todos aquellos errores de *CRC* (*Cyclic Redundancy Check*- Verificación de Redundancia Cíclica), dicha funcionalidad se complementa con el sistema de aire limpio, evitando interferencias y mejor calidad del aire, configuraciones que son acompañadas con el sistema de selección de banda por parte del cliente, el sistema de conteo de *SSID* y la funcionalidad de interferencia *WIFI.*

Figura 45. Mejores Prácticas de Gestión de RF recomendadas por WLC Cisco



Fuente: El autor, modificaciones bajo la palataforma *virtual cisco controller*

El no aplicar las recomendaciones de seguridad indicadas para la implementación, operación y robustecimiento de las redes sin hilos corporativas conlleva a la exposición de las diferentes vulnerabilidades presentadas anteriormente, e igualmente genera falencias generalizadas de seguridad que puede afectar a toda la red e infraestructura tecnológica de la empresa, vulnerando los pilares fundamentales de la seguridad informática.

Tomando como referencia las vulnerabilidades descritas anteriormente, la no aplicación de las recomendaciones puede generar un efecto adverso para una compañía y para la información manejada dentro de ella, llegando a exponer la totalidad de la infraestructura tecnológica, exponer la información, perder e incluso permitir que se manipule información vital del negocio.

6. CONCLUSIONES

En esta monografía se analizaron las múltiples vulnerabilidades de seguridad en las redes inalámbricas corporativas, llegando a recrear un escenario real de una organización, que, de manera posterior, bajo la identificación de vulnerabilidades de seguridad, admitió proceder con un ataque de tipo pasivo, este proceso se realizó bajo la metodología de pentesting NIST (SP800-115). Finalmente, el descubrimiento de las fallas de seguridad permitió generar recomendaciones para el aseguramiento y salvaguarda de la seguridad informática para las organizaciones, bajo el robustecimiento del diseño y configuración de las plataformas inalámbricas.

- ✓ En la monografía se recolectó la Información referente a las redes Inalámbricas utilizadas en el ámbito organizacional, la documentación recolectada fue estructurada y categorizada según la relevancia, permitiendo generar un conocimiento más amplio sobre las diferentes tecnologías, e identificar las principales vulnerabilidades de seguridad que afectan las redes sin hilos.

- ✓ En esta monografía se documentaron los múltiples mecanismos de seguridad utilizados para la implementación de las redes inalámbricas corporativas, determinando así los protocolos y elementos que utilizan las tecnologías inalámbricas para robustecer la seguridad a nivel de acceso, transporte de datos y manipulación de la información, teniendo en cuenta que es común que los administradores de red en primera instancia, no implementen o desplieguen un fuerte robustecimiento de seguridad, pero si hace parte de sus labores, realizar aseguramiento de las plataformas que administran.

- ✓ Se corroboró a través de un Pentesting las vulnerabilidades de seguridad generadas por los errores de diseño y configuración de los sistemas de acceso en una organización. La prueba de penetración basada en la metodología NIST (SP800-115) vectorizó su ataque una vez se identificaron las fallas en el equívoco despliegue y configuración de los portales cautivos en la red.

- ✓ En la monografía se documentaron las vulnerabilidades de seguridad a las que se ven expuestas las redes inalámbricas corporativas por malas prácticas, que en su mayoría no son cubiertas, dejando las redes expuestas a diversos ataques y vulnerabilidades. De manera posterior, se generaron recomendaciones de seguridad e identificaron los riesgos consecuentes de la no aplicación de un buen aseguramiento en las plataformas.

BIBLIOGRAFÍA

ACRYLICWIFI. Acrílico Wi-Fi Profesional - Analizador Wifi. 2020. 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wifi-analyzer-acrylic-professional/

ALVAREZ MENDEZ, Yelitza Pastora. 2006. Seguridad Al Acceso De Información En La Implantación De Una Red Inalámbrica, Caracas. 98p. Trabajo de Grado (Especialista en Comunicaciones) Universidad Central de Venezuela. Facultad de Ingeniería. [En línea]. [Consultado el 14, julio, 2019]. Disponible en: http://saber.ucv.ve/xmlui/bitstream/123456789/2420/1/Tesis%20yelitza%20Alvarez.pdf

ARANO, Souta. Redes-inalambricas-lan. 2015, 12p. [En Línea]. [Consultado el 03, agosto, 2019] Disponible en: https://www.academia.edu/16611460/Redes-inalambricas-lan

ASTAIZA HOYOS, Evelio; BERMUDEZ OROZCO, Hector; TRUJILLO DAVILA, Dora. 2014. Selección de access point en redes inalámbricas 802.11 garantizando mínima QoS. Ingeniería y Ciencia, 10(20), 115–137. [En Línea]. [Consultado el 21, agosto, 2019] Disponible en: http://www.academia.edu/7582669/Selecci%C3%B3n_de_Access_Point_en_Redes_Inal%C3%A1mbricas_802.11Garantizando_m%C3%ADnima_QoS

BARAN, Nicolas. Redes Inalámbricas. Redes (Vol. 2). 2012. [En Línea]. [Consultado el 12, noviembre, 2019] Disponible en: http://www3.uah.es/vivatacademia/ficheros/n54/redesinalam.PDF

BAYDAL CARDONA, María Elvira. Clasificación de las redes inalámbricas. 2018, 3p. [En línea]. [Consultado el 11, abril, 2019]. Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.4AAE4B49&lang=es&site=eds-live&scope=site

BEHIQUE DIGITAL. Metodología de Pruebas de Intrusión en la NIST SP 800-115, de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/. 2017. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/.

BYEONG, Gi Lee; SUNGHYUN, Choi. Broadband Wireless Access and Local Networks: Mobile WiMax and WiFi. ARTECH HOUSE, 2008. 618 p. ISBN:1596932945, 9781596932944 páginas

CAO, Bin; LI, Mengyang; ZHANG, Lei; LI, Yixin; PENG, Mugen. ¿Cómo afecta CSMA / CA el rendimiento y la seguridad en las redes inalámbricas de cadena de bloques, en *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, págs., 2020, doi: 10.1109 / TII.2019.2943694. [En Línea]. [Consultado el 30, octubre, 2020] Disponible en: https://www.researchgate.net/publication/336074053_How_Does_CSMACA_Affect_the_Performance_and_Security_in_Wireless_Blockchain_Networks

CARDENAS, Jose. Arquitectura de Redes Inalámbricas. 2019, 10p. [En Línea]. [Consultado el 17, agosto, 2019] Disponible en https://www.academia.edu/11940956/Arquitectura_de_Redes_Inalabricas

CASTRO, Rodrigo. (Avanzando en la seguridad de las redes Wifi. Enfoques 73. 2005. pp. 23-32 [En Línea]. [Consultado el 24, noviembre, 2019]. Disponible en: http://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

CAUSEYOURESTUCK. Envenenamiento por ARP - Hombre en el medio. 2020. 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://causeyourestuck.io/2016/01/07/arp-poisoning-man-in-the-middle/

CCN-CERT BP/11. Recomendaciones de seguridad en redes Wi-Fi corporativas. 2020. 5p. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://www.ccn-

cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

CHUQUITARCO, Mario; ROMERO, Mónica. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador Diagnosis of vulnerabilities in wireless networks at Ecuador, 3(2), 122–133.[En línea]. [Consultado el 11, enero, 2020]. Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3320/3/document%20%2811%29.pdf

CIOPERU. 5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos. 2015, 1p. [En Línea]. [Consultado el 13, septiembre, 2019] Disponible en: http://cioperu.pe/articulo/18229/5-ataques-comunes-a-las-redes-wifi-y-comodefenderse-de-ellos/.

CISCO. Cisco Wireless Controller Best Practices—RF Management [En Línea]. [Consultado el 19, abril, 2020] Disponible en https://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc/rfmgmt.html

CISCO. Cisco Access Point y selector de controlador inalámbrico. 2020, 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.cisco.com/c/en/us/products/wireless/access-point-controller-selector.html?oid=caten019019&view=filter&wireless_controller_network_type_and_size_(small,_midsize,_or_large_networks)=more_than_1500_users_wireless|up_to_1500_users_wireless|up_to_500_users_wireless

CISCO. Guía de despliegue inalámbrico del regulador de las Cisco 2500 Series. 2016, 1p. [En Línea]. [Consultado el 02, octubre, 2019] Disponible en: https://www.cisco.com/c/es_mx/support/docs/wireless/2500-series-wireless-controllers/113034-2500-deploy-guide-00.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05 – enero - 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. No. 47.223. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. MINTIC. Resolucion 0963 (30, abril, 20193). Por la cual se derogan unas disposiciones en materia de planeación, atribución y asignación del espectro. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0963_2019.htm#1

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. MINTIC. Ley 1341 (29, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: El Ministerio, 2019. [Consultado el 25, marzo, 2020]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0963_2019.htm#1

DRAGONBLOOD. Analysing WPA3’s Dragonfly Handshake. 2019, 1p. [En Línea]. [Consultado el 01, abril, 2020] Disponible en: https://wpa3.mathyvanhoef.com/

ESPAÑA. Recomendaciones de seguridad en redes Wi-Fi corporativas Centro Criptologico Nacional. 2020. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

FAN, Yang; HUAIBEI, Zhou. An improved security scheme in WMAN based on IEEE standard 802.16. Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005. Wireless Communications, Networking and Mobile Computing, 1191. [En línea]. [Consultado el 24, abril, 2019]. Disponible en https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/WCNM.2005.1544255

FILIP, Andra; VÁZQUEZ TORRES, Estefania. Seguridad en redes WiFi Eduroam. 2010. 3p. [En Línea]. [Consultado el 15, noviembre, 2019] Disponible en: http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

GARCÍA, Ruby R. Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central “Marta Abreu” de Las Villas. Santa Clara. 2011. 2p. [En Línea]. [Consultado el 07, noviembre, 2019] Disponible en: https://dspace.uclv.edu.cu/bitstream/handle/123456789/6853/Rubersy%20Ramos%20Garc%C3%ADa.pdf?sequence=1&isAllowed=y

GARETH, Owen; MO, Adda. SOLS: Self Organising Distributed Location Server for Wireless Ad Hoc Networks. 2009, 1p. [En Línea]. [Consultado el 03, agosto, 2020] Disponible en: https://www.academia.edu/33094804/SOLS_Self_Organising_Distributed_Location_Server_for_Wireless_Ad_Hoc_Networks

GARG, Vijay K. Wireless Communications & Networking. Amsterdam: Morgan Kaufmann. 2007. [En línea]. [Consultado el 05, julio, 2019]. Disponible en https://www.academia.edu/19503445/Wireless_Communications_and_Networking

HACKING ÉTICO. Ataque DoS WiFi. Blog de seguridad de la información. 2013, 2p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://hacking-etico.com/2013/03/13/ataque-dos-wifi/

HERNÁNDEZ MENDOZA César Manuel; RODRÍGUEZ VIDAL, Luz María; AGUILAR ALAMANZA, Maricela. Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. 2017. 10p. [En línea]. [Consultado el 20, julio, 2019]. Disponible en: https://www.pag.org.mx/index.php/PAG/article/viewFile/647/793

HU, Fei. Cyber-Physical Systems: Integrated Computing and Engineering Design. CRC PRESS, 2013. 398 p. ISBN: 1466577010, 9781466577015

HU, Hao; MYERS, Steven; COLIZZA, Vittoria; VESPIGNANI, Alessandro. WiFi networks and malware epidemiology. Proceedings of the National Academy of Sciences of the United States of America. 106. 1318-23. 10.1073/pnas.0811973106. 2009, 3p. [En Línea]. [Consultado el 11, febrero, 2020] Disponible en: https://www.pnas.org/content/pnas/106/5/1318.full.pdf

LEHEMBRE, Guillaume. Seguridad Wi-Fi – WEP, WPA y WPA2. 2006, 2p. [En Línea]. [Consultado el 29, octubre, 2019] Disponible en: http://index-of.co.uk/INFOSEC/Seguridad%20WiFi%20WEP%20WPA%20y%20WPA2.pdf

MARRUGO, Blanca; MARZOLA, Victor. REDES AD-HOC, INALÁMBRICAS Y SENSORIALES. 2008, 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0043203.pdf

MENA. Network Components Wlan. 2018, 5p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsgao&AN=edsgcl.553554213&lang=es&site=eds-live&scope=site

MENDEZ MORENO, Wilmer Antonio; MOSQUERA PALACIOS, DAIRIN, Jairo y RIVAS TRUJILLO, Edwin. WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform. Tecnura, vol.19, n.spe, 2015, 9p. [En Linea]. [Consultado el 11, marzo, 2020]. Disponible en

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007&lng=en&nrm=iso.

MOLINA, Juan M. Seguridad en redes inalámbricas 802.11. Sistemas & Telemática, 1, 2006. pp. 13-28. [En Línea]. [Consultado el 10, enero, 2020] Disponible en: http://www.icesi.edu.co/contenido/pdfs/jamdrid-seguridad_redes_inalambricas.pdf

MONSALVE PULIDO, Julián. A.; APONTE NOVOA, Fredy. A; CHAPARRO BECERRA, Fabian. Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. Dyna, 82(189), 226– 232. 2015. [En Línea]. [Consultado el 02 noviembre, 2019] Disponible en: http://www.scielo.org.co/pdf/dyna/v82n189/v82n189a28.pdf

PANDA SOFTWARE INTERNATIONAL. Seguridad en Redes Inalámbricas. 2005, 5p. En línea]. [Consultado el 21, julio, 2019]. Disponible en: https://www.academia.edu/8604820/Seguridad_en_redes_Inal%C3%A1mbricas

PARRAS CORRALIZA, Jose Luis. Redes WiFi: ¿realmente se pueden proteger?. 2018. 3p. [En línea]. [Consultado el 15, enero, 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73247/6/jcorralizaTFM0118memoria.pdf

PASTOR SATORRAS, Romualdo; VESPIGNANI, Alessandro. Epidemic spreading in scale-free networks. Phys. Rev. Lett. 2001, 21p. [En Línea]. [Consultado el 06, diciembre 2019] Disponible en: https://www.cs.princeton.edu/courses/archive/fall03/cs323/links/pastor-satorras.pdf

PAU OLIVA, Fora. Inseguridad en redes 802. 2003. 11p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://docplayer.es/9590765-In-seguridad-en-redes-802-11b-pau-oliva-pof-eslack-org-feb-2003.html

PCANDPARTS. Punto de acceso inalámbrico Cisco Aironet AP1815I. 2020, 1P. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://pcandparts.com/access-point/cisco-aironet-ap1815i-wireless-access-point/

PCCOMPONENTES. Startech Adaptador Tarjeta PCI Express PCIe de Red Inalámbrica N 802.11b/g/n 300Mbps https://www.pccomponentes.com/startech-adaptador-tarjeta-pci-express-pcie-de-red-inalambrica-n-80211b-g-n-300mbps

RAMIREZ, Aydee. M. V. Identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting. 2016, 1p. [En Línea]. [Consultado el 01, febrero, 2020] Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12425/1/46646702.pdf

ROBAYO LÓPEZ, Javier; RODRÍGUEZ RODRÍGUEZ, Richar. Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net". Repositorio Institucional UMNG. Universidad Militar Nueva Granada. 2015, 33p. [En línea]. [Consultado el 25, marzo, 2020]. Disponible en https://repository.unad.edu.co/handle/10596/3818

SABOGAL ROZO, Esther Angélica. Proyecto de Seguridad Informática I. Bogotá: Universidad Nacional Abierta y A Distancia, 2013. 54-56p. [En Línea]. [Consultado el 02, diciembre 2019] Disponible en: https://www.academia.edu/6240795/

SALAZAR SOLER, Jordi. (Redes inalámbricas. 2016, 3p. [En línea]. [Consultado el 23, abril, 2019]. Disponible en https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

SANATINIA, Amirali S; NOUBIR, G. (2013). Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In IEEE Conference on Communications and Network Security (CNS) (pp. 430–437). [En Línea]. [Consultado el 19, febrero, 2020]. Disponible en: https://doi.org/10.1109/CNS.2013.6682757

SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUGH, Angela. (Technical Guide to Information Security Testing and Assessment (No. NIST Special Publication (SP) 800-115). National Institute of Standards and Technology. 2008. 6p. En Línea]. [Consultado el 11, octubre, 2019] Disponible en https://doi.org/10.6028/NIST.SP.800-115

SERRANO FLORES, Andrés Guillermo. Análisis de Vulnerabilidades de Seguridades en Redes Inalámbricas dentro un Entorno Empresarial que Utilizan Cifrado AES y TKIP, WPA y WPA2 Personal del DMQ, Quito, 2011, 3p. [En línea]. [Consultado el 14, julio, 2019]. Disponible en: http://repositorio.puce.edu.ec/bitstream/22000/4642/1/TESIS%20-%20PUCE%204479.pdf

SHAJI. SSID SPOOFING conocido como puntos de acceso falsos, gemelos malvados o honeypots. 2020. 1p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en http://shaji-3848.herokuapp.com/

TANEBAUM, Andrew; WETHERALL, David. Redes de computadoras. Quinta edición. México: PEARSON EDUCACIÓN, 2012. 791 p. ISBN: 978-607-32-0817-8

TOOLWAR1. Kit de herramientas de análisis de implementaciones criptográficas: Framework.202. p. [En línea]. [Consultado el 09, julio, 2019]. Disponible en http://toolwar1.rssing.com/chan-52947478/latest.php

VALLEJO DE LEON, Tatiana. (2010). Vulnerabilidades Y Niveles De Seguridad De Redes WI-FI. Guatemala, 116p. Trabajo de grado (Ingeniera de Sistemas). Universidad de San Carlos. Facultad de Ingeniería. [En línea]. [Consultado el 27, julio 2019]. Disponible en: http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf

VARELA, Carlos; DOMÍNGUEZ, Luis. Redes Inalámbricas. 2002. 5p. [En línea]. [Consultado el 25, junio, 2019]. Disponible en: http://www.blyx.com/public/wireless/redesInalambricas.pdf

VERBEL, Daniel; CANO, Hernan. (2016) ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS: APLICACIÓN DE BUENAS PRACTICAS EN PYMES Y USUARIOS FINALES [En Línea]. [Consultado el 02, febrero, 2020] Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf

VILLAGÓMEZ, Carlos. Introducción a Wi-Fi (802.11 o WiFi). 2018. 8p. [En Línea]. [Consultado el 02, septiembre, 2019] Disponible en: http://es.ccm.net/contents/789-introduccion-awi-fi-802-11-o-wifi

VILORIA NUÑEZ, César; CARDONA PEÑA, Jairo; LOZANO GARZÓN, Carlos. Análisis comparativo de tecnologías inalámbricas para una solución de servicios de telemedicina. Universidad del Norte, Barranquilla, Colombia. Núm. 25, 2009, pp. 200-217. [En línea]. [Consultado el 09, julio, 2019]. Disponible en https://www.redalyc.org/pdf/852/85212371012.pdf

Wi-FI Alliance. “WPA3™ Specification Version 2.0”. 2019. 3p. [En Línea]. [Consultado el 15, marzo, 2020] Disponible en: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf

ANEXOS

ANEXO A - DIVULGACIÓN DE RESULTADOS

Se anexa video explicativo evidenciando el problema de vulnerabilidad planteado sobre algunas redes inalámbricas corporativas mal administradas y configuradas, bajo la plataforma de CISCO WLC, de manera posterior se demuestra múltiples implementaciones de seguridad, algunas medidas y recomendaciones que ayudan a mitigar las brechas mencionadas

https://vimeo.com/user105700851/review/376292703/459791ae94

Igualmente, el documento estará disponible en el repositorio de la UNAD para su posterior revisión si es necesario y así dar continuidad en el proceso de identificación de vulnerabilidades presentes en las redes inalámbricas corporativas sobre las diferentes plataformas.

ANEXO B - RESUMEN ANALÍTICO RAE

Fecha de Realización: 08/08/2020
Título: ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES PRESENTES EN REDES SIN HILOS CORPORATIVAS
Autor: MOLINA, Edwin
Palabras Claves: Vulnerabilidades, conectividad, redes sin hilos, aseguramiento, encriptación, suplantación, *MAC*, *Pentesting, test surveys,* Protocolos de Seguridad, *WMAN, WLAN*, Puntos de Acceso
Descripción: El trabajo monografico está focalizado en las redes sin hilos corporativas bajo plataformas WLC Cisco, a través de un ambiente controlado, en el que se realizan un análisis de vulnerabilidades presentes y se exponen los riesgos que generan el mal aseguramiento de las plataformas WMAN corporativas, adicional esto se generan recomendaciones de seguridad aplicables y de fortalecimiento. Para dar el cumplimiento a los objetivos propuestos se implementó una metodología sintética, bajo diferentes análisis de los componentes de una red inalámbrica y su seguridad, para posteriormente profundizar en ellos y proceder a ejecutar un análisis de las falencias y vulnerabilidades presentadas. Las pruebas de pentesting se realizan sobre una plataforma de Cisco, a la que se le realiza conexión por medio de la red de invitados y se procede a ejecutar una resolución ARP y un escaneo de puertos identificando fallas de seguridad por el mal diseño de la red y permitiendo alcances a las diferentes subredes y equipos propios de la compañía, de manera adicional se vulnera un web services de un sistema de energía de la compañía que no cuenta con un protocolo de protección de acceso seguro. Los resultados de las pruebas demostraron que el mal diseño estructural físico, lógico y de hardening de las redes puede facilitar el trabajo de un atacante y de manera posterior permitir vectorizar el ataque.
ASTAIZA HOYOS, Evelio; BERMUDEZ OROZCO, Hector; TRUJILLO DAVILA, Dora. 2014. Selección de access point en redes inalámbricas 802.11 garantizando mínima QoS. Ingeniería y Ciencia, 10(20), 115–137. [En Línea]. [Consultado el 21, agosto, 2019] Disponible en: http://www.academia.edu/7582669/Selecci%C3%B3n_de_Access_Point_en_Redes_Inal%C3%A1mbricas_802.11Garantizando_m%C3%ADnima_QoS BAYDAL CARDONA, María Elvira. Clasificación de las redes inalámbricas. 2018, 3p. [En línea]. [Consultado el 11, abril, 2019]. Disponible en

http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.4AAE4B49&lang=es&site=eds-live&scope=site

BEHIQUE DIGITAL. Metodología de Pruebas de Intrusión en la NIST SP 800-115, de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/. 2017. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/.

CCN-CERT BP/11. Recomendaciones de seguridad en redes Wi-Fi corporativas. 2020. 5p. [En Línea]. [Consultado el 20, abril, 2020] Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html

CHUQUITARCO, Mario; ROMERO, Mónica. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador Diagnosis of vulnerabilities in wireless networks at Ecuador, 3(2), 122–133. [En línea]. [Consultado el 11, enero, 2020]. Disponible en: https://repositorio.uide.edu.ec/bitstream/37000/3320/3/document%20%2811%29.pdf

CISCO. Cisco Wireless Controller Best Practices—RF Management [En Línea]. [Consultado el 19, abril, 2020] Disponible en https://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc/rfmgmt.html

CISCO. Guía de despliegue inalámbrico del regulador de las Cisco 2500 Series. 2016, 1p. [En Línea]. [Consultado el 02, octubre, 2019] Disponible en: https://www.cisco.com/c/es_mx/support/docs/wireless/2500-series-wireless-controllers/113034-2500-deploy-guide-00.html

FILIP, Andra; VÁZQUEZ TORRES, Estefania. Seguridad en redes WiFi Eduroam. 2010. 3p. [En Línea]. [Consultado el 15, noviembre, 2019] Disponible en: http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

GARCÍA, Ruby R. Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central “Marta Abreu” de Las Villas. Santa Clara. 2011. 2p. [En Línea]. [Consultado el 07, noviembre, 2019] Disponible en:

https://dspace.uclv.edu.cu/bitstream/handle/123456789/6853/Rubersy%20Ramos%20Garc%C3%ADa.pdf?sequence=1&isAllowed=y

MENDEZ MORENO, Wilmer Antonio; MOSQUERA PALACIOS, DAIRIN, Jairo y RIVAS TRUJILLO, Edwin. WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform. Tecnura, vol.19, n.spe, 2015, 1p. [En Linea]. [Consultado el 11, marzo, 2020]. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007&lng=en&nrm=iso.

MONSALVE PULIDO, Julián. A.; APONTE NOVOA, Fredy. A; CHAPARRO BECERRA, Fabian. Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. Dyna, 82(189), 226– 232. 2015. [En Línea]. [Consultado el 02 noviembre, 2019] Disponible en: http://www.scielo.org.co/pdf/dyna/v82n189/v82n189a28.pdf

PARRAS CORRALIZA, Jose Luis. Redes WiFi: ¿realmente se pueden proteger?. 2018. 3p. [En línea]. [Consultado el 15, enero, 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73247/6/jcorralizaTFM0118memoria.pdf

RAMIREZ, Aydee. M. V. Identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting. 2016, 1p. [En Línea]. [Consultado el 01, febrero, 2020] Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12425/1/46646702.pdf

ROBAYO LÓPEZ, Javier; RODRÍGUEZ RODRÍGUEZ, Richar. Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net". Repositorio Institucional UMNG. Universidad Militar Nueva Granada. 2015, 33p. [En línea]. [Consultado el 25, marzo, 2020]. Disponible en https://repository.unad.edu.co/handle/10596/3818

SALAZAR SOLER, Jordi. (Redes inalámbricas. 2016, 3p. [En línea]. [Consultado el 23, abril, 2019]. Disponible en https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUGH, Angela. (Technical Guide to Information Security Testing and Assessment (No. NIST Special Publication (SP) 800-115). National Institute of Standards and Technology. 2008. 6p. En Línea]. [Consultado el 11, octubre, 2019] Disponible en https://doi.org/10.6028/NIST.SP.800-115

SERRANO FLORES, Andrés Guillermo. Análisis de Vulnerabilidades de Seguridades en Redes Inalámbricas dentro un Entorno Empresarial que Utilizan Cifrado AES y TKIP, WPA y WPA2 Personal del DMQ, Quito, 2011, 3p. [En línea]. [Consultado el 14, julio, 2019]. Disponible en: http://repositorio.puce.edu.ec/bitstream/22000/4642/1/TESIS%20-%20PUCE%204479.pdf

VERBEL, Daniel; CANO, Hernan. (2016) ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS: APLICACIÓN DE BUENAS PRACTICAS EN PYMES Y USUARIOS FINALES [En Línea]. [Consultado el 02, febrero, 2020] Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/3360/1/Estudio_Esquemas_Seguridad_Verbel_2016.pdf

VILLAGÓMEZ, Carlos. Introducción a Wi-Fi (802.11 o WiFi). 2018. 8p. [En Línea]. [Consultado el 02, septiembre, 2019] Disponible en: http://es.ccm.net/contents/789-introduccion-awi-fi-802-11-o-wifi

Wi-FI Alliance. “WPA3™ Specification Version 2.0”. 2019. 3p. [En Línea]. [Consultado el 15, marzo, 2020] Disponible en: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf

Contenido del documento:

En el desarrollo e implementación de las tecnologías inalámbricas en el ámbito corporativo, que permiten brindar facilidades de implementación y configuración, se identifican vulnerabilidades de seguridad, debido a falencias de implementación y hardening

Por ende se debe tener en cuenta que el proceso de implementación de una red inalámbrica conlleva retos que inician desde los *test surveys*, protocolo de encriptación a utilizar, canales de comunicación, banda de frecuencia y mecanismos de protección contra intrusiones de usuarios, puntos de acceso

no autorizados y otras vulnerabilidades que son el objetivo final de los atacantes con la finalidad de realizar diferentes ataques remotos contra la infraestructura corporativa, esto bajo técnicas básicas como las de ejecutar procesos de escaneos y lograr identificar vulnerabilidades de la plataforma inalámbrica.

En el contexto de comunicaciones empresariales, se cuentan con diferentes alternativas que permiten la comunicación de los usuarios pertenecientes a la empresa y al personal externo, el método más común de conexión es realizado por medio de la red cableada y como alternativa de cubrimiento de la total capacidad de empleados y algunos externos, se implementan las redes inalámbricas, este sistema de comunicación es implementado directamente en las edificaciones donde la organización presenta sus oficinas, en el proceso de implementación se realizan un estudio de *test surveys* para determinar la ubicación de los diferentes puntos de acceso, sin embargo sobre las instalaciones no es común que se realicen procesos de análisis de seguridad e implementación de esquemas de protección, generando así una configuración de encriptación básica, que proporciona una instalación de los puntos de accesos con una ubicación aleatoria, proceso que igualmente se repite con la controladora inalámbrica, esta falta de fundamentación en seguridad proporciona vulnerabilidad a las redes corporativas inalámbricas.

Las configuraciones básicas a nivel de seguridad y el erróneo diseño e implementación en los dispositivos inalámbricos exponen la red a diferentes tipos de ataques como lo son: *Arp Spoofing, Mac Spoofing, DDoS, Wardriving, Acces Points Spoofing* y otras metodologías de intrusión, según la finalidad y objetivo del atacante.

El núcleo del proyecto es la identificación de vulnerabilidades bajo el uso de una plataforma Cisco WLC, en el que se simula una red de invitados, con alcances a las demás redes corporativas permitiendo generar un documento con evidencias significativas y que de manera posterior se pueda utilizar como elemento guía, para la continuación de investigación de vulnerabilidades en diferentes infraestructuras inalámbricas organizacionales

Cabe destacar que no se pretenden abarcar todos los tipos de ataques y variantes existentes, pero si dar un paso inicial al análisis de las vulnerabilidades de seguridad presentes en una compañía y al fortalecimiento de la infraestructura bajo algunas condiciones reales que se pueden presentar

por intentos de intrusión o ataques malintencionados por externos a la organización

Metodología:

El método empleado para desarrollar la monografía fue basado en una investigación, acerca de la categorización funcionamiento y vulnerabilidades de las redes sin hilos corporativas. De manera posterior, bajo la documentación obtenida, se realizó un *pentesting* simulado sobre un entorno empresarial, que permitió identificar y atacar las vulnerabilidades presentadas por la red, para finalmente proporcionar unas recomendadciones de *hardening* al implementar y desplegar redes inalambricas en las organizaciones.

METODOLOGÍA UTILIZADA

Para cumplir los objetivos las actividades desarrolladas se organizaron de la siguiente manera:

1. Estudio y recolección de información generalizada y específica sobre las redes sin hilos corporativas.
2. Descripción de mecanismos de seguridad implementados en las redes sin hilos corporativas.
3. Ejecución de *pentesting* para determinar falencias de seguridad en la *WMAN* corporativa.
4. Documentación las vulnerabilidades presentes en el ejercicio simulado sobre una organización.
5. Se generaron las recomendaciones para fortalecer las redes inalámbricas corporativas ante las diferentes vulnerabilidades.

Conceptos nuevos: *Hardening, ARP,partner, handoff, CCMP, AES, RIJNDAEL, RC4, Hijacking,CCMP,EAP, MiTM*

Conclusiones

En esta monografía se analizaron las múltiples vulnerabilidades de seguridad en las redes inalámbricas corporativas, llegando a recrear un escenario real de una organización, que, de manera posterior, bajo las vulnerabilidades de seguridad identificadas en su red fue atacada, este proceso se realizo bajo la metodología de pentesting NIST (SP800-115). Finalmente, el descubrimiento de las fallas de seguridad, permitió generar recomendaciones para el aseguramiento y

salvaguarda de la seguridad informática para las organizaciones, bajo el robustecimiento del diseño y configuración de las plataformas inalámbricas

En la monografía se recolectó la Información referente a las redes Inalámbricas utilizadas en el ámbito organizacional, la documentación recolectada fue estructurada y categorizada según la relevancia, permitiendo generar un conocimiento más amplio sobre las diferentes tecnologías e identificar las principales vulnerabilidades de seguridad que afectan las redes sin hilos.

En esta monografía se investigó los múltiples mecanismos de seguridad utilizados para la implementación de las redes inalámbricas corporativas, determinando así los protocolos y elementos que utilizan las tecnologías inalámbricas para robustecer la seguridad a nivel de acceso, transporte de datos y manipulación de la información.

Se corroboró a través de un Pentesting las vulnerabilidades de seguridad generadas por los errores de diseño y configuración de los sistemas de acceso en una organización, la prueba de penetración basada en la metodología NIST (SP800-115) vectorizó su ataque una vez se identificaron las fallas en el equívoco despliegue y configuración de los portales cautivos en la red inalámbrica corporativa.

En la monografía se documentó las vulnerabilidades de Seguridad a las que se ven expuestas las redes inalámbricas corporativas por malas prácticas, que en su mayoría no son cubiertas, dejando las redes expuestas a diversos ataques y vulnerabilidades, de manera posterior se generaron recomendaciones de seguridad e identificaron los riesgos consecuentes de la no aplicación de un buen aseguramiento en las plataformas.

AUTOR: EDWIN ALFREDO MOLINA SANCHEZ