ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO, REDES Y COMUNICACIÓN DE DATOS

AUTOR: YACCHIREMA ESPÍN, ANA MARIVEL

TEMA: ANÁLISIS DE LOS SISTEMAS DE ATAQUE Y PROTECCIÓN EN REDES INALÁMBRICAS WIFI, BAJO EL SISTEMA OPERATIVO LINUX

DIRECTOR: MSC. ING. ABG. ALULEMA, DARWIN

CODIRECTOR: MSC. ING. AGUILAR, DARWIN

SANGOLQUÍ, MARZO 2014

CERTIFICACIÓN

Certificamos que el presente proyecto titulado:

"ANÁLISIS DE LOS SISTEMAS DE ATAQUE Y PROTECCIÓN EN REDES INALÁMBRICAS WI FI, BAJO EL SISTEMA OPERATIVO LINUX".

Ha sido desarrollado en su totalidad, por la Señorita: Ana Marivel Yacchirema Espín con CI 1718555616, bajo la dirección de:

Msc. Ing. Abg. Darwin Alulema	Msc. Ing. Darwin Aguilar
DIRECTOR	CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

DECLARACIÓN DE RESPONSABILIDAD

ANA MARIVEL YACCHIREMA ESPÍN

DECLARO QUE:

El proyecto de grado titulado ***"ANÁLISIS DE LOS SISTEMAS DE ATAQUE Y PROTECCIÓN EN REDES INALÁMBRICAS WI FI, BAJO EL SISTEMA OPERATIVO LINUX"***, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme sus respectivas citas y referencias bibliográficas.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 28 de marzo del 2014

Ana Marivel Yacchirema Espín

1718555616

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, ANA MARIVEL YACCHIREMA ESPÍN

Autorizo a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución del trabajo ***"ANÁLISIS DE LOS SISTEMAS DE ATAQUE Y PROTECCIÓN EN REDES INALÁMBRICAS WI FI, BAJO EL SISTEMA OPERATIVO LINUX"***, cuyo contenido, ideas y criterios con de mi exclusiva responsabilidad y autoría.

Sangolquí, 28 de marzo del 2014

Ana Marivel Yacchirema Espín

1718555616

DEDICATORIA

Este trabajo junto con todo el esfuerzo y esmero que requirió de mi persona, queda especialmente dedicado a mis padres a quienes les debo vida, paciencia y amor.

También quiero dedicarlo a todas aquellas personas quienes puedan beneficiarse de este contenido.

AGRADECIMIENTO

Quiero agradecer de la manera más profunda y de todo corazón a mis padres, por ser quienes han dedicado su vida entera de la manera más desinteresada y amorosa a forjar la mujer que soy ahora. Lucharon sobre todas las cosas y necesidades, para que sus hijos tomen rumbos fructíferos.

Agradezco a mis hermanos Soledad y Luis, que desde mi infancia han sido los amigos más fieles y cariñosos, que no dudan en dar una mano sino las dos cuando más lo necesito.

A todos los maestros y maestras que durante toda mi vida estudiantil brindaron con empeño sus conocimientos, permitiendo que peldaño a peldaño me encuentre más cerca de mis sueños profesionales. Incluyo con gran aprecio a mi hermano Luis en esta mención, quien también se convirtió en gran maestro, cuando las dudas acechaban; admirable Ingeniero.

A mis maestros Darwin Alulema y Darwin Aguilar, director y codirector respectivamente de este proyecto, por su sabia guía durante la realización de este trabajo.

Finalmente agradezco a mi amor Wilson y a todas las bellas personas que conocí a lo largo de mi vida y tengo el gusto de llamarlos amigos.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Wi Fi es una tecnología que ha ido fascinando y consolidándose en las infraestructuras de red; pero su seguridad fue y sigue siendo una debilidad para las redes inalámbricas; porque el medio inclina la balanza hacia los atacantes. Mucho antes de su primer paso; a WEP, ya se le presentaban sus opositores, luego en la lucha por mejorar esta situación nacen consecuentemente WPA y WPA2. No obstante no sólo los protocolos iban evolucionando también las habilidades y herramientas de los hackers toman fuerza; inclusive la gran herramienta llamada Internet permitió que no sólo personas con gran conocimiento lograran sus ataques, ahora cualquiera con acceso a Internet puede adquirir herramientas tan fascinantes y efectivas en la realización de ataques. Pero también surgen y van madurando, herramientas tan valiosas como los IDSs, permitiendo no sólo dar un plus más de seguridad con la emisión de sus alertas; también brindan una forma de aprendizaje de la ejecución de un ataque. Cabe la necesidad de una evaluación de las mismas para determinar que tan desarrolladas están en el tema de Seguridad Inalámbrica, así los Benchmarks, agrupados en las herramientas de ataque de Backtrack ayudan a medir la efectividad de los sistemas Kismet y Snort, popularmente conocidos, para así dejar al descubierto fortalezas y debilidades de los IDSs; en el importante campo de la tecnología Wi Fi.

Palabras clave:

Wi Fi, Ataques, Backtrack, Snort, Kismet.

Abstract

Wi Fi is a technology that has been fascinating and consolidating in network infrastructure, but their safety was and remains a weakness for wireless networks, because the media tilt the balance towards the attackers. Long before its first step, WEP, already presented its opponents, then in the struggle to improve this situation arise consequently WPA and WPA2. However not only the protocols were also evolving the skills and tools of hackers are becoming stronger , even great tool called the Internet not only allowed people with great knowledge to achieve their attacks, now anyone with Internet access can get as fascinating and effective tools in performing attacks. But also emerge and mature, as valuable as tools IDS , allowing not only give more security plus issuing their alerts; also provide a way of learning about execution of an attack. There is the need for evaluating them to determine how developed are in the subject of Wireless Security and the Benchmarks grouped in Backtrack´s attack tools help measure the effectiveness of Kismet and Snort systems , popularly known for thus exposing the strengths and weaknesses of IDSs , in the important field of Wi Fi technology.

Key Words

Wi Fi, Attacks, Backtrack, Snort, Kismet.

CAPÍTULO 1

INTRODUCCIÓN

Las redes inalámbricas están formando parte de la actualidad de las redes de muchas organizaciones, negocios, campus, hogares, entre otros; por tal motivo la comunidad tecnológica se ha preocupado por su desarrollo y obtener cada vez mejores características, para sobrellevar sus puntos débiles, entre ellos velocidad y seguridad.

Aunque el punto velocidad fascinantemente se ha desarrollado en los últimos años a grandes pasos, la seguridad es un punto de gran debate entre hackers que han logrado desarrollar herramientas, que han permitido apreciar las falencias de los desarrolladores de los protocolos que intentan mantener protegida la información.

Los algoritmos criptográficos tienen la lucha constante no sólo por brindar más seguridad y ser más robustos, al mismo tiempo tienen que lograrlo con un consumo de procesamiento y tiempo óptimos; tan importantes en las comunicaciones, sobretodo en la actualidad con el mundo de las aplicaciones en tiempo real y QoS.

1.1. Wi Fi 802.11

El estándar 802.11 define las especificaciones de la capa física y el control de acceso al medio MAC para las LAN inalámbricas, fue desarrollado por el

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), en un comienzo permitió velocidades de 1 a 2 Mbps en la frecuencia de 2,4 GHz (1997) (Caizapanta, 2013), desde entonces se mantiene en constantes revisiones, enmiendas y cambios que permitan mejorar el ancho de banda, compatibilidad y seguridad conforme sigue evolucionando hacia las nuevas tecnologías.

1.1.1. Arquitectura

La arquitectura IEEE 802.11consiste de distintos componentes, que interactúan para proveer una WLAN que soporta una movilidad transparente, para las capas superiores como lo indica (IEEE802.11, 2012):

a. BSS

Una parte fundamental de una LAN 802.11 es el conjunto de servicio básico (BSS), que consiste de dos o más estaciones inalámbricas que se comunican dentro de un área delimitada denominada área de servicio básico (BSA).

b. IBSS

Cuando se trata de comunicación entre STAs sin la necesidad de otro dispositivo como un punto de acceso AP, esta se denomina BSS independiente (IBSS) ó también denominado como red ad- hoc. A continuación una representación gráfica de un IBSS y un BSS.

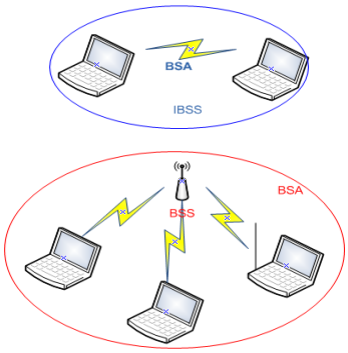


Figura 1. Representación gráfica de un IBSS y un BSS con su respectiva BSA

Elaborado por: Autora del Proyecto

c. ESS.

Cuando se desea una mayor cobertura de la red, se forma un conjunto de servicio extendido (ESS); mediante la interconexión a través de un sistema de distribución (DS), de varios BSSs, que poseen el mismo identificador de servicio compartido (SSID); siendo este un distintivo único que permite a los STAs, identificar entre varias redes. El AP es quien posee la funcionalidad de habilitar el acceso al DS para todas las STAs asociadas, figura 2.

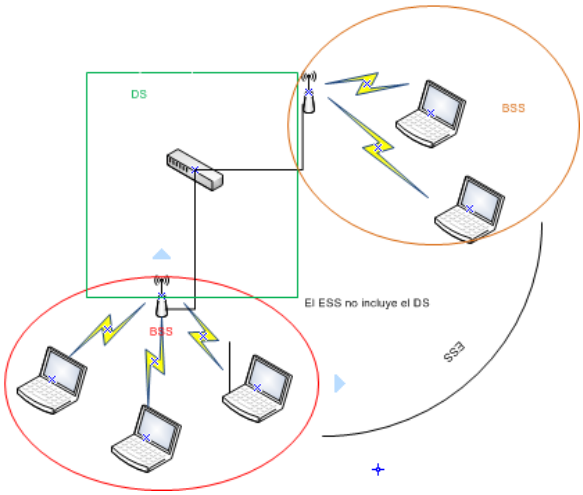


Figura 2. ESS formado por dos BSSs

Elaborado por: Autora del Proyecto

El área de cobertura que cubre un ESS se denomina área de servicio extendido (ESA) y los dispositivos que se mueven dentro de esta área pueden moverse de BSS a otro; siendo esto trasparente para la capa LLC, pues un ESS aparece como un simple IBSS para dicha capa.

1.1.2. Estándares

El IEEE formó grupos de trabajo que se encargarían de mejorar el estándar base 802.11 ratificado en 1997, existiendo un desarrollo continuo en torno a las necesidades que se han presentado conforme el paso del tiempo, principalmente la velocidad de datos para las aplicaciones que demandan mayor ancho de banda, la seguridad que requiere la información que circula en la red inalámbrica, la compatibilidad, debido a la gran cantidad de marcas existentes en el mercado, etc.

Los estándares se desarrollan bajo el uso de las frecuencias no licenciadas ISM (médica, científica e investigación) (IEEE802.11, 2012).

a. 802.11 a

Es una extensión del 802.11 ratificada en 1999 también conocido como “Wi-Fi5” (Ochoa, 2011), utiliza el mismo juego de protocolos de base que el estándar original, pero con las siguientes características:

- Trabaja en la frecuencia de 5 GHZ, con multiplexación ortogonal por división de frecuencia (OFDM) y utiliza 52 subportadoras.
- Velocidad máxima de 54Mbps
- No es compatible con 802.11b y 802.11g debido a que trabajan en distintas frecuencias.

- Existe un menor alcance, porque a mayor frecuencia hay una mayor absorción por parte del ambiente.
- Hay menos interferencias por ser una banda no tan utilizada, todo lo contrario a la banda de 2,4GHz que usan artefactos como el teléfono inalámbrico, monitor de bebé, horno microondas, etc.
- Estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20Mbps.
- 802.11a define 12 canales no solapados.

En la tabla 1 se indica la disminución de la velocidad de datos en ambientes interiores y exteriores, con respecto a la distancia a la que se encuentra el dispositivo cliente:

Tabla 1. Velocidad teórica según el ambiente y distancias para 802.11a

Transmisión Exterior	***Valor Máx. 30m***	54Mbps
	Valor Mín. 300m	6Mbps
Transmisión Interior	***Valor Máx. 12m***	54Mbps
	Valor Mín. 90m	6Mbps

Fuente: (Ochoa, 2011)

b. 802.11 b

Es una extensión del 802.11 que fue ratificada en el año de 1999 y consta de las siguientes características:

- Utiliza la frecuencia de 2,4GHz con una modulación de espectro de difusión de secuencia directa (DSSS), pero que permite más velocidad de datos que

el IEEE802.11 de 1997; porque utiliza una clave de código complementaria CCK., que permite enviar los bits de datos en palabra código, a través del aire, para ser recibidos y comparados con las posibles palabras código que corresponda.

- Velocidad máxima de 11Mbps.
- Vulnerable a interferencias sobre todo por la gran cantidad de artefactos que usan su misma banda de frecuencia libre.
- Define 14 canales de 22MHz parcialmente solapados.

A continuación la tabla 2 muestra las velocidades teóricas en ambientes externos e internos:

Tabla 2. Velocidad teórica según el ambiente y distancias para 802.11b

Transmisión Exterior	***Valor Máx. 200m***	11 Mbps
	Valor Mín. 500m	1 Mbps
Transmisión Interior	***Valor Máx. 50m***	11 Mbps
	Valor Mín. 150m	1Mbps

Fuente: (Ochoa, 2011)

c. 802.11e.

Fue aprobado en el 2005 y define la calidad de servicio en redes QoS inalámbricas, para permitir una mayor rapidez en la transmisión de datos, voz y video; evitando el menor retraso posible, para ello hace uso de dos mecanismos: el primero es el acceso al canal distribuido mejorado (EDCA), que entrega tráfico según las prioridades de usuario (UP), el segundo mecanismo es a través de la función de coordinación híbrida (HCF), con el

acceso al canal controlado(HCCA), que permite reservar las oportunidades de transmisión.

EDCA define ocho prioridades de usuario y cuatro categorías de acceso; tabla 3, estas últimas proveen soporte a las STAs en la entrega del tráfico con prioridades UPs.

Tabla 3. Mapa de relación prioridad de usuario y categoría de acceso

Prioridad	UP(Prioridad de usuario igual al 802.11 d)	Designación 802.11 d	AC (Categoría de Acceso)	Designación (informativo)
Lowest	1	BK	AC_BK	segundo plano
	2	-	AC_BK	segundo plano
	0	BE	AC_BE	mejor esfuerzo
	3	EE	AC_BE	mejor esfuerzo
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
Highest	6	VO	AC_VO	Voz
	7	NC	AC_VO	Voz

Fuente: (IEEE802.11, 2012)

d. 802.11 g.

Estándar publicado en el 2003, define las siguientes características:

- Velocidad teórica máxima de 54Mbps.
- Opera en la banda de frecuencia libre de 2,4GHz, por lo que es sensible a interferencias.
- Multiplexación OFDM, aunque también especifica el DSSS que permite una compatibilidad retrospectiva con 802.11b, ya que trabajan en la misma banda de frecuencia.

- Con este estándar se puede llegar a una velocidad real de transferencia de 24,7Mbps muy similar al 802.11a.

En la tabla 4 se describe las velocidades teóricas según el ambiente en el que se da la comunicación.

Tabla 4. Velocidad teórica según el ambiente y distancias para 802.11g

Transmisión Exterior	***Valor Máx. 75m***	54 Mbps
	Valor Mín. 350m	9 Mbps
Transmisión Interior	***Valor Máx. 27m***	54 Mbps
	Valor Mín. 75m	9 Mbps

Fuente: (Ochoa, 2011)

e. 802.11i.

Es el estándar que define la seguridad en las WLAN publicado en el 2004, para ello determina la autenticación y encriptación (IEEE802.11, 2012), como métodos para proteger la red de intrusos. El acceso a la red debe determinar si el dispositivo es realmente un cliente autorizado; así como la certeza de que está ingresando a la red correcta y no a un punto de acceso ilegal.

En un comienzo se trató de mejorar la seguridad con Privacidad Equivalente a Cable (WEP), al poseer fallas notorias en el cifrado de la clave, la alianza Wi-Fi desarrolla el Acceso Protegido Wi-Fi (WPA), que introduce el protocolo de integración de clave temporal (TKIP) y la autenticación con el protocolo de autenticación extendido (EAP); pero el cifrado RC4 hace que siga teniendo falencias. El IEEE802.11i finalmente se implementa en su totalidad en WPA2.

Este estándar define dos clases de algoritmos de seguridad para las redes IEEE 802.11: los algoritmos de creación y uso RSNA (Asociación de Red de Seguridad Robusta), y los pre-RSNA, además indica como obsoleto el uso de WEP y TKIP (IEEE802.11, 2012, pág. 94).

f. 802.11n.

Estándar inalámbrico que permite un notable mejoramiento en rendimiento de la velocidad de transferencia de datos con respecto a las versiones a, b y g; fue un borrador desarrollado en el 2007 y finalmente ratificado en el 2009, presenta las siguientes características (IEEE802.11, 2012):

- Velocidad máxima teórica de 600Mbps.
- Puede trabajar tanto en la banda de 2,4GHz como en la de 5GHz; ó simplemente trabajar en ambas.
- Tiene compatibilidad con los dispositivos que operan con 802.11a, b y g; aunque esto disminuya el rendimiento del equipo pues tiene que sujetarse al rendimiento lento de las versiones anteriores.
- Utiliza la técnica de multiplexación espacial que consiste en dividir en partes un flujo de datos y codificarlo individualmente, para así enviar las partes en diferentes canales espaciales pero en la misma frecuencia (802.11n especifica hasta cuatro flujos espaciales). Para enviar estos flujos de datos en paralelo se usa múltiples antenas de transmisión, que son recibidos por múltiples antenas receptoras en el receptor quien será el encargado de

obtener la estructura de datos original; a esta tecnología se le denomina MIMO (Múltiple Entrada Múltiple Salida).

- Usa la multiplexación de alto rendimiento (HT) ortogonal por división de frecuencia, por tratarse con flujos espaciales.
- Usa la técnica de unión de canales o canalización de 40 MHZ, que consiste en unir dos canales adyacentes de 20MHz para obtener uno de 40MHz; para el caso de 2,4GHz solo existen tres canales no solapados (1,6 y 11) con los que sólo se podría formar un solo canal de 40MHz con dos de ellos; para el caso de 5GHz se puede obtener una mejor canalización por poseer 23 canales no solapados.
- Define la técnica de agregación de tramas con subcapa MAC compartida, que permite enviar varias tramas como si fuese una sola trama y los equipos receptores realizan un “Reconocimiento de Bloque”, mediante el cual identifican que se trata de un grupo de tramas en vez de una sola trama.

La tabla 5 resume los resultados de los grupos de trabajo, por mejorar el funcionamiento de las redes inalámbricas.

Tabla 5. Estándares de la familia 802.11

Estándar	Año	Define
802.11c	2003	Información sobre el funcionamiento del puenteo en la capa MAC802.11. Fue tomado para desarrollar el estándar 802.11d.
802.11d	2001	Mejoramiento de la capa física y subcapa MAC conforme las regulaciones de cada país para evitar problemas con los canales. Llamado también “Método Mundial”.
802.11f	2003	Interoperabilidad entre APs de distintas marcas y facilidad de roaming; gracias al protocolo IAPP (Protocolo Inter Puntos de Acceso).
802.11h	2003	Hace que el 802.11a cumpla con las regulaciones de la Unión Europea; ya que la frecuencia de 5GHz es de uso militar.
802.11j	2004	Funcionamiento de las WLAN en frecuencias 4.9GHz y 5 GHz para las regulaciones japonesas.
802.11k	2008	Proveer a las capas superiores a la física, los mecanismos de medición de recurso de radio y definición de la información que debe estar disponible en la administración y mantenimiento de una WLAN móvil como: reportes de roaming, información de STAs asociadas, datos estadísticos del flujo de paquetes en el AP, etc.
802.11p	2010	Acceso inalámbrico en vehículos, como las comunicaciones dedicadas de rango corto DSRC entre vehículos en EEUU, con el fin de ofrecer seguridad vial, pago de peajes, prevención de colisiones, etc.
802.11r	2008	Transición rápida en el BSS, para reducir tiempo de desconexión entre el STA y el DS, cuando se conecta a otro AP, con uso de protocolos FT(transición rápida).Cuando se produce el proceso de unión de un STA a una red inalámbrica a través de un AP, proceso que se denomina “asociación”, se intercambia información conocida como Origen FT(FTO), con la que se puede agilitar la asociación o re asociación con otro AP en la red; porque se puede autenticar al STA antes de que abandone el actual.
802.11s	2011	Funcionamiento de redes inalámbricas en malla.
802.11u	2011	Inter-funcionamiento con redes externas.
802.11v	2011	Administración de red inalámbrica, para configuración o administración remota de estaciones cliente.
802.11w	2009	Establece tramas de gestión protegidas para darle aún más seguridad a la red inalámbrica, pues el 802.11 i sólo trata la seguridad de las tramas de datos; siendo las de gestión parte importante en las operaciones de la red, en las cuales dispositivos maliciosos pueden interferir.
802.11y	2009	Operación en las bandas de frecuencia 3650–3700 MHz en los Estados Unidos según sus regulaciones.
802.11z	2010	Configuración de DLS (Enlace-Directo a Extensiones); en el cual una estación cliente puede conectarse directamente con otra manteniendo la conexión con su AP; a través del mecanismo de túnel de enlace directo (TDLS).El enlace directo se establece sin la intervención del usuario.

Elaborado por: Autora del Proyecto

1.1.3. Capa MAC

a. Funciones

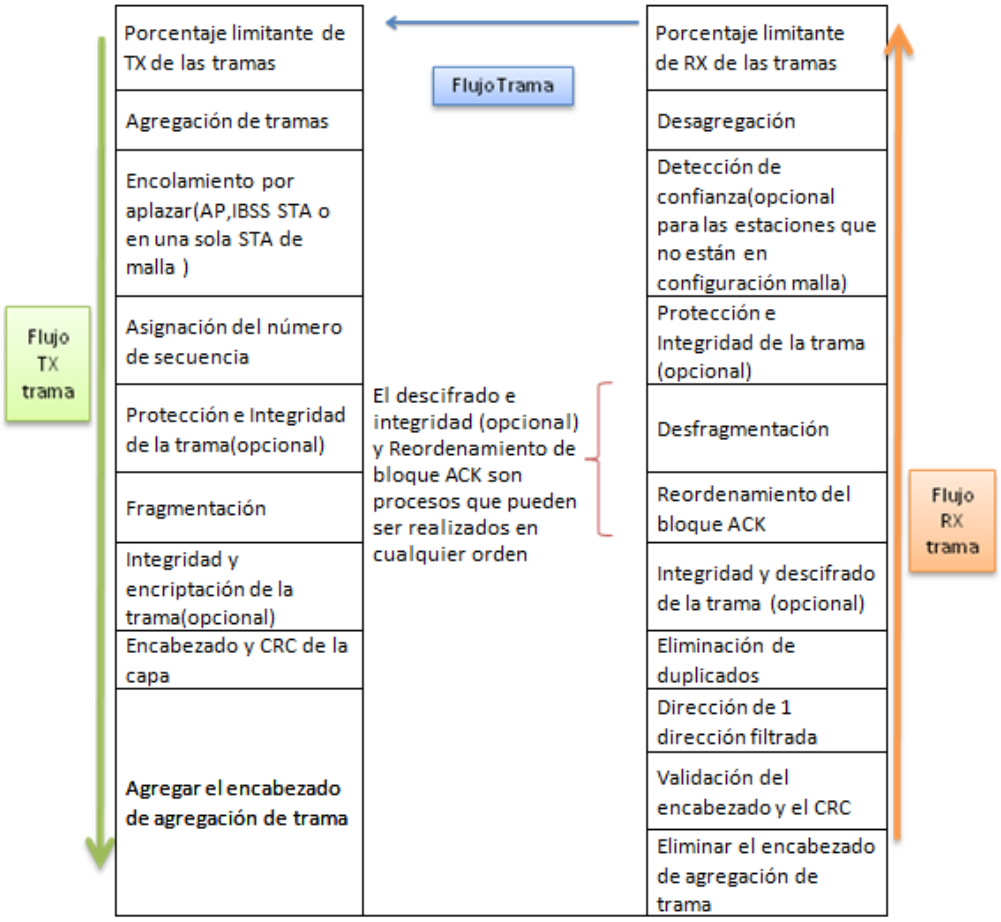
Cabe destacar a continuación funciones importantes que realiza esta subcapa (IEEE802.11, 2012):

- ***Calidad de Servicio:*** a través de la utilización de prioridades de usuario, que definen la categoría de tráfico; lo que permite dar prioridad a las MSDU[1]s que así lo requieran en una QoS STA (tabla.3.).
- ***Seguridad:*** principalmente enfocado en el servicio de autenticación y confidencialidad de los datos, por lo que se han venido desarrollando varios protocolos de seguridad que permitan brindar dichos servicios.
- ***Ordenamiento de las tramas (agregación de tramas)*****,** por el cual se puede mejorar la probabilidad de éxito de la transmisión de tramas, cuando se trabaja con gestión de la potencia tanto FMS (servicio multicast[2] flexible, el cliente inalámbrico solicita al AP el envío de varios grupos direccionados de tramas) como DMS (servicio de multicast dirigido, el cliente inalámbrico solicita al AP el envío de un grupo direccionado de tramas), es decir se puede agrupar varias tramas como si fuera una sola y el receptor estaría en capacidad de volver a obtener cada trama individual.
- ***Servicio de datos de la MAC***, esta subcapa maneja una arquitectura de manejo de las tramas tanto en su recepción como transmisión, que corresponden a etapas de un proceso por las cuales en su mayoría atraviesan las tramas. En la transmisión pueden atravesar, por un

[1] **MSDU:** Unidad de Datos de Servicio MAC
[2] **Multicast:** un origen que envía información a un grupo de destinatarios.

porcentaje limitante de tramas, agregación de tramas, aplazamiento de la transmisión de los datos en modo de ahorro de potencia, asignación de número de secuencia, fragmentación, etc; tal cual se observa en el Flujo Tx de Trama de la tabla 1.6. Para la recepción corresponden a los procesos inversos de las mencionadas etapas de la transmisión, Flujo Rx.

Tabla 6. Arquitectura plana del servicio de datos de MAC



Fuente: (IEEE802.11, 2012)

Formato de la Trama: existen tres tipos de tramas que son la de administración, control y datos. La primera tiene que ver con las tramas que se

intercambian en los procesos de asociación, reasociación, autenticación, la segunda tiene que ver con procesos que velan el intercambio correcto de las tramas de datos como son el reconocimiento ACK, las tramas para evitar problemas de STA oculta (RTS y CTS), y por último están las tramas que contienen los datos en sí.

El formato que tiene la trama, figura 3 consta de:

-El encabezado MAC que contiene información de control, duración, direcciones (corresponden al transmisor, receptor, destino, origen; según el tipo de trama y diseño de WLAN), información del control de secuencia y campos opcionales como QoS si se trata de QoS STA y HT si se trata con 802.11n.

-El cuerpo de la trama de máximo 2304 octetos

-Un campo de chequeo del frame FCS.

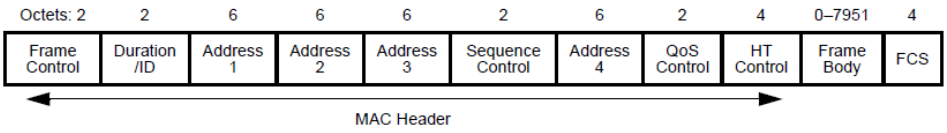


Figura 3. Formato General de la Trama 802.11

Fuente: (IEEE802.11, 2012)

b. Arquitectura

Para llevar a cabo sus servicios la subcapa MAC está construida bajo las denominadas funciones de coordinación que son: DCF (función de coordinación distribuida), PCF (función d2e coordinación de punto) y HCF (función de coordinación híbrida) (Hsiao & Mohsen, 2006):

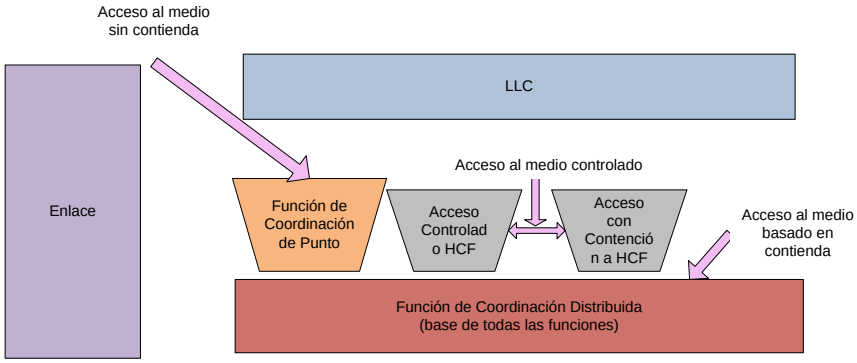


Figura 4. Arquitectura MAC

Elaborado por: Autora del Proyecto

❖ **DCF**

Esta es la función base de la subcapa MAC, la cual trabaja bajo la modalidad "escucha antes de hablar", a través del CSMA[3]. Cuando las STAs desean transmitir sus tramas censan el medio para determinar si hay una transmisión en tránsito, en el caso de que esté libre procede a enviar; esta función de censado es denominada CCA (Evaluación de Canal Libre), por medio de una potencia de umbral la estación compara, si es mayor en el medio hay una trasmisión y si es menor está libre.

Además del CCA existe un temporizador denominado NAV[4], que también permite la protección de la transmisión de la trama, porque la STA activa este temporizador cuando recibe una trama que contiene un estimado de duración de la siguiente trama. Mientras el CCA y el NAV estén activos las STAs no pueden transmitir.

[3] **CSMA:** Acceso múltiple por detección de portadora.
[4] **NAV:** Vector de distribución de red

- **Prevención de colisión (CA)**

Este es un mecanismo para evitar que las tramas de las estaciones que trasmiten colisionen, debido a que detectaron al mismo tiempo el medio como libre, por lo tanto se establece un tiempo randómico adicional que debe esperar la estación transmisora después de detectar el medio desocupado, si transcurrido el mismo sigue libre se puede transmitir.

Cada STA posee una denominada Ventana de contención (CW) con el que se determina los espacios de tiempo que se debe esperar, mientras existan fallos en la transmisión esta ventana crecerá al doble. Por otro lado las STAs que detectan el medio ocupado difieren el acceso al medio con la cuenta hacia atrás del tiempo de espera; así cuando esté libre quien tenga el tiempo más corto tendrá mayor prioridad para enviar.

- **Estación oculta RTS/CTS**

La estación oculta es un problema que puede ocurrir en la transmisión de tramas debido a la ubicación de las STAs, cuando estas pueden detectar la presencia de algunas pero no así de otras que se denominan ocultas, por lo que se puede determinar el medio como libre mientras las ocultas están transmitiendo; para esto se creó las tramas RTS (Solicitud para Envío) y CTS (Libre para Envío).

Cuando la estación desea transmitir envía un RTS al AP, si le responden con un CTS se puede transmitir las tramas de datos, caso contrario no lo puede realizar.

❖ **PCF**

Esta función usa un PC (punto coordinador) que generalmente es un AP y funciona dentro de un BSS, este coordinador se encarga de establecer prioridad en el acceso al medio de las STAs clientes, pues establece un mecanismo libre de contención; es decir el dispositivo realiza un escaneo de las estaciones clientes (usando tramas de gestión "beacon[5]") y les determina un NAV(esta asignación de NAV se le denomina como mecanismo de detección de portadora virtual), por lo tanto controla las transmisiones de las estaciones, mismas que usan DCF. El PC actúa solicitando y enviando tramas de las STAs clientes.

Para tener prioridad frente al DCF, usa IFSs (espacios de tiempo entre tramas) más pequeños, por lo que se establece un CFP (periodo libre de contención) en el que el PC accede al medio y luego un CP (periodo de contención) mediante el cual se utiliza DCF.

❖ **HCF**

Esta función es utilizada con STAs que requieren calidad de servicio QoS, para esto utilizan dos mecanismos: un control de acceso al canal distribuido mejorado EDCA, y un acceso al canal controlado HCCA.

- **EDCA (Enhanced Distributed Control Access)**

Cuando existe un periodo de contención las estaciones compiten por una TXOP (oportunidad para transmitir), que se logra gracias a parámetros como son las prioridades de usuario UPs, que definen categorías de acceso AC que

[5] **Beacon:** son tramas que contienen información sobre la red inalámbrica y son transmitidos periódicamente para anunciar la presencia de la red WLAN.

se pueden observar en la tabla 3 Tanto UPs como ACs permiten categorizar y priorizar el tráfico, así como también obtener un conjunto de parámetros como son: tamaño mínimo y máximo de la CW, tiempos entre tramas, límites de las oportunidades de transmisión a través de las ACs. Estos parámetros se conocen a través de las tramas beacon.

- **HCCA (Controlled Channel Access)**

Este mecanismo utiliza un HC (coordinador híbrido), que se ubica en un AP dentro del BSS, este empieza la transmisión de las tramas colocándose la más alta prioridad, define las TXOPs de las STAs clientes y para sí mismo, cuando está transcurriendo un periodo libre de contención. Pero también se puede programar la asignación de TXOPs durante el CP.

1.2. Protocolos de Seguridad Wi-Fi

Según el estándar 802.11 (IEEE802.11, 2012) existen dos tipos de algoritmos: los algoritmos en RSNA (Asociación de red seguridad robusta) y los previos a la RSNA.

- ***Pre-RSNA***, comprendido por: Autenticación previo a RSNA y WEP.
- ***RSNA***, comprendido por: TKIP, CCMP, BIP, SAE Autenticación, inicialización y terminación de RSNA, procedimientos de administración de clave y autenticación 802.1x.

Aunque por su lado Wi Fi con cooperación de la IEEE formó los protocolos de seguridad WPA, como intento desesperado por brindar seguridad hasta que se desarrolle por completo la 802.11i.

1.2.1. Autenticación previo RSNA

Se definen dos tipos de autenticación previo a RSNA (IEEE802.11, 2012):

a. Autenticación de Sistema Abierto

Simplemente corresponde a una nula autenticación, pues una STA puede solicitar autenticarse y simplemente se le permite la conexión; aunque la STA a la que se solicita puede reusarse a dar conexión. Con este tipo de autenticación existen dos tipos de mensajes: solicitud de conexión y permiso de conexión.

b. Autenticación de Clave Compartida

Se usa en WEP y consiste en que el AP transmite a las STAs clientes una clave compartida por un canal seguro independiente de 802.11, por su parte las STAs validan si los parámetros recibidos son válidos y si lo son proceden armar la trama de solicitud de autenticación de clave compartida.

Cuando el AP recibe la solicitud, genera una cadena de octetos para el desafío de autenticación de texto, si es exitosa la autenticación genera una trama de respuesta en la que incluye campos de una respuesta de asociación (porcentajes soportados, capacidad, dominio de movilidad, tiempo de asociación agotado, etc.) y los campos de códigos de estado (exitoso, negado, negado por desajuste de capacidades, parámetros inválidos, etc.), que son los estados de una operación solicitada.

1.2.2. WEP

El algoritmo WEP (Privacidad Equivalente a Cable), fue creado con la intención de proveer confidencialidad al intercambio de tramas, usa clave de 40bit aunque existen implementaciones de 104bits. El formato de la trama que

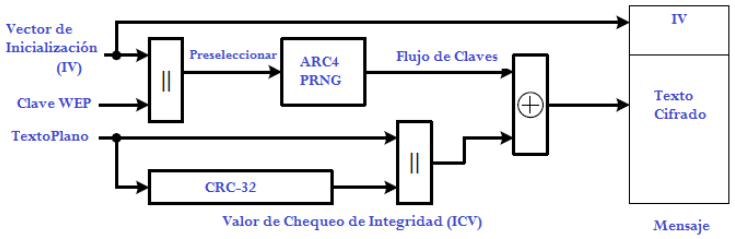
utiliza es un vector de inicialización IV de 32 bits, que corresponde a 3 octetos que contienen el vector en sí, 6 bits de relleno y 2 bits del ID de la clave, un campo de datos mayor o igual a un 1 octeto y un campo de verificación de chequeo de integridad (IEEE802.11, 2012). En la tabla 7 se presenta sus características relevantes:

Tabla 7. Características de WEP

Características de WEP	WEP solo cifra claves y no realiza autenticación de las tramas de datos, no tiene claves de integridad de datos.
	En la encriptación de claves usa claves mapeadas o por defecto. Es decir en el primer caso existe una clave configurada en el transmisor y receptor para encapsulación y desencapsulación; en el segundo no se ha configurado y debe generarse una por defecto.
	El valor de chequeo de integridad (ICV) se calcula con el algoritmo CRC32 en texto plano.
	Para cifrar o descifrar usa el algoritmo RC4[6], con un generador de números pseudoaleatorios PRNG[7] se realiza la operación XOR con el texto plano para obtener un texto cifrado, ó para recuperar un texto plano desde un cifrado

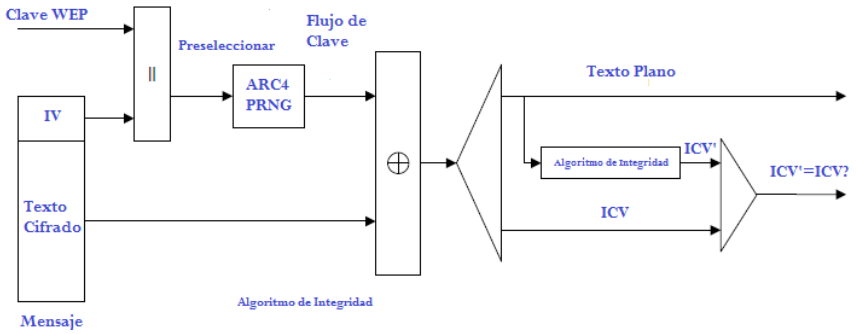
Elaborado por: Autora del Proyecto

La figura 5, indica el esquema del proceso de encriptación y descifrado para obtener las tramas encapsuladas ó desencapsularlas.



(a)

[6] **RC4:** algoritmo Rivest Cipher 4, diseñado por Ron Rivest de la RSA Security en el año 1987.
[7] **PRNG:** números que parecen ser obtenidos al azar pero siguen algún proceso determinístico



(b)

Figura 5. (a) Diagrama del proceso de encapsulación y (b) Desencapsulación WEP

Fuente: (IEEE802.11, 2012)

1.2.3. TKIP

El protocolo de integridad de clave temporal TKIP, es un protocolo que se encarga de la confidencialidad e integridad en lo que respecta a las tramas de datos tratando de mejorar WEP, para ello posee las siguientes características (IEEE802.11, 2012), tabla 8:

Tabla 8. Características de TKIP

Características de TKIP	Se incrementa el IV de 32 bits a 48 bits obteniendo un IV mejorado.
	Usa un MIC[8] para evitar ataques de falsificación, el transmisor lo calcula con las direcciones MAC, la prioridad y el texto plano de la trama, luego se añade la MIC a la trama(antes de fragmentarse), el receptor descifra, chequea el ICV, desfragmenta y entonces revisa la MIC.
	Usa un contador de secuencia TKIP (TSC) codificado en el IV, para descartar tramas que no llegan en el orden correcto ó con un valor de secuencia que no les correspondía.
	TKIP posee una función de mezclado de claves, en la que entran la clave temporal, la dirección del transmisor y el TSC, para mejorar la preselección WEP.

Elaborado por: Autora del Proyecto

[8] **MIC:** código de integridad de datos.

1.2.4. CCMP

CCMP (protocolo en modo CCM) provee confidencialidad, integridad, autenticación en tramas de datos; según la 802.11i es obligatorio su uso en seguridad inalámbrica y presenta las siguientes características, tabla 9:

Tabla 9. Características de CCMP

Características de CCMP(Modo Contador con CBC-MAC)	Es un algoritmo simétrico[9] que usa AES (Estándar de Encriptación Avanzado), en un procesamiento que maneja clave y bloque de datos de 128 bits.
	El modo contador es usado para obtener privacidad en los datos y CBC-MAC[10] para la integridad y autenticación.
	Requiere una nueva clave temporal por cada sesión, es decir para cada trama protegida existe un único valor dado por la clave temporal, a través de un PN (Número de Paquete) de 48 bits.
	Extiende la trama en 16 octetos, 8 de la MIC y 8 para su encabezado; en este último se encuentra el campo de ID de clave y el PN; cabe notar que no existe un campo ICV como en WEP.

Elaborado por: Autora del Proyecto

Para encapsular una trama se sigue el siguiente proceso: 1) se cifra la carga útil del texto plano, con este resultado se procede a incrementar el PN para asignar siempre uno nuevo y no se repita para la misma clave temporal, 2) se construye una autenticación de datos adicional (AAD), 3) se forma un bloque denominado Nonce con el PN, con la dirección A2 y prioridad de la MAC, 4) se coloca el nuevo PN y el ID de clave dentro de lo que será el encabezado de CCMP, 5) con la clave temporal, el AAD, el bloque Nonce y los datos de la trama se procede a obtener el texto cifrado y la MIC . 6) Por último se encapsula la trama con el encabezado original de la trama, el encabezado

[9] **Algoritmo simétrico:** significa que la misma clave que usa el transmisor para cifrar usa el receptor para descifrar.
[10] **CBC-MAC:** significa encadenamiento de bloque cifrado-código de autenticación de mensaje.

CCMP, los datos encriptados y la MIC. La desencapsulación es el proceso inverso a lo anteriormente mencionado, figura 6.

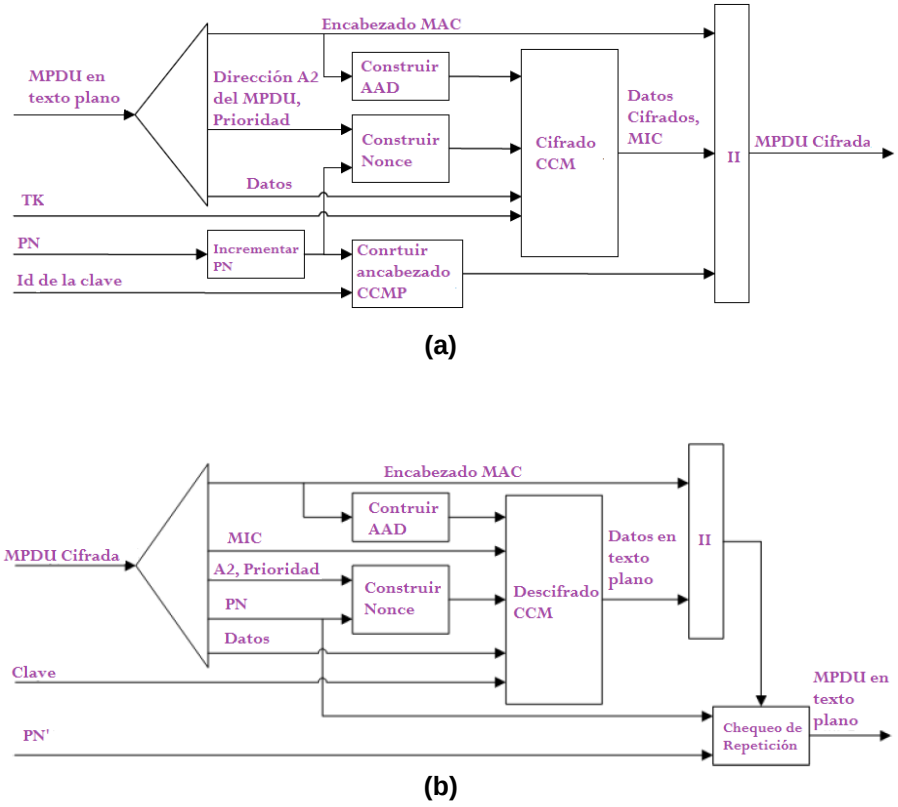


Figura 6. (a) Diagrama del proceso de encapsulación y (b) Desencapsulación CCMP

Fuente: (IEEE802.11, 2012)

1.2.5. BIP

El protocolo de integridad multicast/broadcast (BIP) está orientado a proporcionar protección a la integridad y evitar ataques replay (un atacante repite una trasmisión de un usuario válido hacia un receptor con el fin que a él le llegue la respuesta del receptor) en los grupos direccionados de tramas de

administración; para conseguir sus objetivos posee las siguientes características, tabla 10:

Tabla 10. Características de BIP

Características de BIP	Trabaja con el modo CMAC (Cifrado basado en MAC) de AES; que intenta dar mejoras a las deficiencias de CBC-MAC. Usa una clave temporal y bloques de 128 bits.
	La MIC se obtiene a través de una clave temporal de integridad de grupo (IGTK) para las tramas de administración, que se denomina elemento MIC de administración (MME).
	El formato de la trama consta del encabezado 802.11, el cuerpo de la trama de administración incluida la MME y un FCS.
	Usa una autenticación adicional de datos AAD, que debe ser obtenida a través del encabezado de la trama original.
	Para la protección contra ataques replay usa números de secuencia.
	En la transmisión de tramas de administración, el transmisor identifica el IGTK[11], obtiene el ADD, usa AES –CMAC para cifrar ADD, con el cuerpo de la trama y MME. Por último se forma la trama a enviar con el encabezado 802.11, el cuerpo cifrado y FCS.
	En la recepción de tramas de administración, el receptor identifica el IGTK, la MME, el ADD y por último recupera la trama original, si logra pasar todas las comprobaciones mencionadas.

Elaborado por: Autora del Proyecto

1.2.6. SAE

La autenticación entre STAs debe permitir una seguridad contra los ataques de diccionario, entre otros, un intento por asegurar este proceso es el protocolo de simultánea autenticación de iguales SAE, que posee las siguientes características, tabla 11:

[11] **IGTK:** Clave Temporal de Integridad de Grupo.

Tabla 11. Características de SAE

Características de SAE	El proceso de este protocolo define como exitoso, si al final de la autenticación; ambas estaciones posean una PMK (clave maestra de par sabio), a través de un generador de claves que usa el protocolo de autenticación extensible EAP ó a través de una clave pre compartida PSK.
	Funciona a través de 2 tipos de intercambios de frames: el de compromiso y confirmación; el primero permite un intercambio de una supuesta clave, mientras que el segundo una confirmación de la suposición. El proceso habrá terminado cuando ambas partes se comprometan y confirmen.
	Las claves son usadas en SAE para calcularse determinísticamente en un elemento secreto, dentro de un grupo negociado, denominado elemento de clave.

Elaborado por: Autora del Proyecto

1.2.7. Autenticación 802.1x

El 802.1x es un protocolo estándar de autenticación de red basado en puerto, a través del cual se autentifica a los clientes y se asigna las respectivas claves; que después se utilizarán en los algoritmos de encriptación. Define tres entidades que entran en el proceso de autenticación (Iniesta, 2010): solicitante, autenticador y el servidor de autenticación.

En un ambiente wireless el proceso de autenticación es el siguiente: un STA cliente solicita autenticarse (después de conectarse a un PAE-Entidad de Acceso de Puerto), el AP autenticador recibe y reenvía esta solicitud al servidor de autenticación, quien posee la información sobre los usuarios permitidos. El tráfico que se maneja en este proceso viaja a través de un canal seguro utilizando un protocolo de capa superior.

Si el proceso resulta exitoso el servidor envía un mensaje de autenticación correcta al AP, y este le permite el acceso al cliente; tomando en cuenta que

durante este proceso se generan las claves que se usarán en los procesos de encriptación, como se puede observar en la figura 7. En el caso de Wi Fi se generan dos tipos de claves; las que comparte el grupo de clientes con uso específico para tráfico multicast y la clave individual para tráfico unicast.

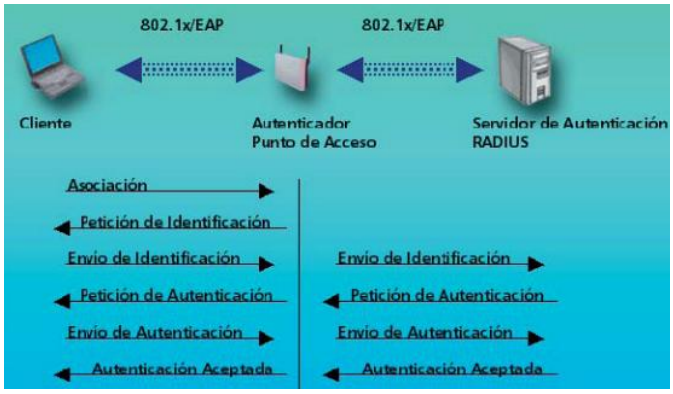


Figura 7. Proceso de autenticación 802.1x

Fuente: (Iniesta, 2010)

Los protocolos de capa superior relacionados con el proceso de autenticación son generalmente EAP y RADIUS (Iniesta, 2010):

a. **EAP:** protocolo que defina mensajes como son petición, respuesta, éxito o fallo que serán intercambiados entre cliente, autenticador y servidor; muchos protocolos de capa superior se basan en él como EAP- TLS (Seguridad de Capa de Transporte).

b. **RADIUS:** protocolo que trabaja en la conexión autenticador-servidor, ocupándose del intercambio de los mensajes EAP.

1.2.8. WPA

Frente a las debilidades que presenta WEP, la Alianza Wi Fi se vio en la necesidad de generar soluciones de seguridad hasta que la IEEE proporcionara

la 802.11i; para ello se tomó parte del estándar borrador para obtener la WPA (Acceso Protegido Wi Fi); a continuación características presentes en este protocolo:

Tabla 12. Características de WPA

Características de WPA	Utilización de claves dinámicas TK, a través del protocolo TKIP, para cada trama.
	Para el manejo de la autenticación y autorización, se basa en el uso de EAP.
	Uso de la MIC para poder revisar la integridad de los datos de las tramas.
	Se puede trabajar en dos tipos de modos: corporativo “enterprise” ó personal.
	El Modo Corporativo se basa en el uso de un servidor sea RADIUS o AAA, el cual tiene que manejar la autenticación y autorización de los clientes.
	El Modo Personal se basa en el uso de clave, que se tiene configurado tanto en el STA cliente como en el AP. A diferencia de WEP, esta clave solo se usa al iniciar la autenticación más no en el cifrado en sí.

Elaborado por: Autora del Proyecto

1.2.9. WPA2

La WPA versión 2 no es más que el 802.11i; las mejoras que implica son principalmente el uso del algoritmo AES para la encriptación, en lo que respecta al protocolo CCMP. También trabaja en los modos corporativo y personal, para los cuales es similar a WPA, uso de servidores de autenticación en el corporativo y PSK en el personal.

CAPÍTULO 2

ATAQUES EN LAS REDES INFORMÁTICAS

La seguridad informática es un tema que actualmente se convierte en prioritario, por ello se gasta en variedad de equipos y software, como firewalls, IDSs, IPSs, etc. Porque la información es un bien valioso que necesita cumplir con las tres características fundamentales, que son: confidencialidad, integridad y disponibilidad; para ello no basta con el elemento software y hardware, también se necesita de un factor humano bien preparado. Por su lado el personal técnico debe ser un hacker más, conocedor de las vulnerabilidades, ataques e intrusos que pueden atentar ó están atentando contra la organización; y los usuarios deben ser bien entrenados en las buenas prácticas de seguridad, para evitar que su desconocimiento sea el factor más potencial para los ataques.

Las redes inalámbricas son aún más sensibles a los atacantes por el mismo hecho que se encuentra en un medio libre como es el aire, pese a los esfuerzos de la IEEE y la Alianza Wi Fi, día con día sorprenden más las poderosas herramientas que se desarrollan para lograr vulnerar claves, suplantar identidades, descifrar contenidos, etc. Pero para todo lo expuesto anteriormente, sólo queda ser proactivos, conocer a fondo las amenazas, preparase contra ellas; siempre alertas, en conjunto de buenas prácticas y concientización.

2.1. Tipos de Ataques en las redes

Un **ataque** consiste en aprovechar la vulnerabilidad de un sistema informático y ejecutar una o varias **amenazas** existentes. Entendiéndose por amenaza, a todos los factores sean software, hardware, factor humano, que al existir la mínima oportunidad pueden causar daño tanto en la disponibilidad, integridad y confidencialidad de la información que viaja por la red; como por ejemplo desde un corte de luz eléctrica, destrucción o modificación de información, etc. Existen dos grupos en los que se dividen los ataques según el modo en el que trabaja el atacante ó también lo clasifican según las amenazas en las que se enfocan (Kimberly, 2010):

Tabla 13. Clasificación de Ataques

Ataques según el modo de operación del atacante	
Pasivo	Existe un acceso sin autorización a la información, se la monitorea pero no se realiza ninguna otra acción.
Activo	Cuando el atacante va más allá que simplemente observar la información, la modifica, daña, borra; ó también atenta contra los canales de comunicación ó servidores; saturándolos.
Ataques según las amenazas en las que se enfocan	
Ingeniería Social	Se enfocan en el factor humano, cuando este representa la debilidad de seguridad de la entidad, por desconocimiento. Un ejemplo común es el ataque conocido como phishing: se suplanta una página web, que por lo general pide ingreso de información; incluso tan delicada como números de cuenta; entre otros.
Escucha en la Red	Se enfocan en obtener información a través de la captura de tráfico, según las habilidades de interpretación de quienes observan, pueden determinar datos que les servirán para otros ataques.
Código Malicioso	Son código ó programas que penetran en el sistema para causar daños o anomalías. Para propagarse pueden se valen del factor humano, quien ejecuta algún instalador pirata, descarga y abre correos de desconocidos, usa memorias flash infectadas, etc. Ej.: virus, gusanos, backdoor[12],etc.
Explotación activa de vulnerabilidades	Los atacantes usan aplicativos para hacer un diagnóstico de la situación actual de la seguridad del sistema informático; por ejemplo un escaneo de puertos, luego procede de manera activa, modificando, borrando, cambiando ó robando la información. Las vulnerabilidades pueden causar ataques basados en los protocolos de red (ping de la muerte), ataques basados en el host (acceso remoto a través de un "backdoor") y basados en la capa de aplicación de red (comandos de depuración de envío de correos).

Fuente: (Kimberly, 2010)

[12] **Backdoor:** "puerta trasera",código malicioso que convierte al host en cliente de un servidor malicioso abriendo un acceso o puerto.

2.2. Tipos de Intrusos en las redes

Un intruso es aquella persona que sin autorización ingresa a un sistema informático; gracias a sus conocimientos, por ende para clasificarlo se lo realiza en base a su conocimiento en técnicas de hacking; y del beneficio que lo conlleva a su acción. En la tabla 14 se encuentran los distintos tipos de intrusos (Aguilera, 2010).

Tabla 14. Tipos de Intrusos

Intruso	Descripción	Objetivo
Hacker	Intruso que pone a prueba todos sus conocimientos sobre lenguajes de programación, arquitectura de los equipos, servicios, software, aplicaciones, sistemas operativos; entre otros, para descubrir accesos a los sistemas y su información.	Determinar las falencias de seguridad del sistema así como retarse a sí mismo. Generalmente este tipo de intruso tiene fines éticos denominado "hackeo ético".
Cracker	Es un hacker maligno.	Tiene fines económicos o simplemente el fin de causar daño motivado por razones políticas, sociales, religiosas, etc.
Pheaker	Intruso especializado en las redes telefónicas.	Obtener el servicio de manera ilícita y gratuita.
Newbie	Intruso que está aprendiendo técnicas de hacking, novato en el tema.	Fines educativos, convertirse ya sea en hacker o cracker.
Lamer	Intruso sin conocimiento de hacking, pero utiliza las aplicaciones, scripts, códigos y todas las herramientas que fueron generadas por verdaderos expertos en el tema; para efectuar los ataques.	Fines educativos, convertirse ya sea en hacker o cracker.
Spammer	Intruso que envía gran cantidad de correos, para saturar el buzón de correo de los usuarios y terminar saturando el servidor de correo.	Propagar código malicioso, realizar phishing.
Pirata informático	Intruso que roba aplicativos o contenido multimedia, infringiendo los derechos de autor y propiedad intelectual.	Propagar código malicioso, obtener beneficios económicos, etc.

Fuente: (Aguilera, 2010)

2.3. Técnicas de Ataque

Los ataques se enfocan en varias zonas donde se ha encontrado una vulnerabilidad, pero principalmente en las redes inalámbricas por la inseguridad del medio; los atacantes trabajan preferentemente sobre la capa de enlace de datos; porque las tramas están viajando en el aire y son más asequibles. No obstante también existen ataques que afectan tanto a redes Ethernet como inalámbricas; principalmente aprovechando las vulnerabilidades de la arquitectura TCP/IP, tan ampliamente utilizada.

2.3.1. Principales Ataques en Ethernet

El cableado es el medio físico por el cual se interconectan los equipos en una red Ethernet, por esta razón limita físicamente al atacante; que trata de burlar las seguridades y lograr el acceso a la LAN, pero también existe la posibilidad más frecuente; que dentro de la misma organización, con toda intención o por ignorancia, los propios usuarios produzcan los ataques. Además existen descuidos en la red interna que pueden comprometer su seguridad como tener el cableado al intemperie, puntos de red expuestos; de ahí que se hace indispensable tener un buen cableado, conexiones privadas hacia equipos críticos, tener un filtrado de direcciones MAC, IP; entre otras medidas.

A continuación los ataques más comunes en una red LAN Ethernet:

a. Spoofing:

Es un ataque que consiste en tratar de suplantar a un equipo o usuario que tiene un acceso autorizado; existe diferentes tipos de suplantación enfocados a protocolos como: DNS, Web, Email, MAC (más común en ataques en redes inalámbricas), IP, ARP; entre otros. Por lo general se intenta dejar fuera de

operación al equipo que se está suplantando para evitar que interfiera, valiéndose de ataques como la denegación de servicio; y lo que realmente le representa un reto al hacker es la forma en la que consiga disfrazarse (Kimberly, 2010). Los más comunes ataques spoofing son, (Tabla 15):

Tabla 15. Tipos comunes del Ataque Spoofing

SPOOFING	***IP Spoofing***	Suplantación de IP legítima.
	SMTP Spoofing	Envío de spam, suplantando emisores.
	DNS Spoofing	Suplantación de entradas DNS.
	Web Spoofing	Suplantación de páginas web.
	MAC Spoofing	Suplantación de direcciones MAC legítimas

Fuente: (Kimberly, 2010)

❖ **IP Spoofing:** A través de un proceso de sniffing, el atacante puede llegar a determinar la IP del equipo que desea dejar fuera de servicio para hacerse pasar por él, entonces existe tres factores presentes en esta clase de ataque: el atacante, el atacado y el receptor, este último tiene una relación de confianza basado en IP con el atacado (Kimberly, 2010).

El atacante captura los paquetes de la comunicación legítima y modifica los campos del encabezado IP; colocando su dirección IP como origen del paquete, para que el receptor crea que es un usuario legítimo y empiece a recibir la información; obviamente dejando fuera de servicio al atacado con alguna técnica de ataque, caso contario él sería quien reciba la información.

Aquí cabe mencionar también el ataque **"Hijacking"**[13], que es común en comunicación con TCP/IP, pues cuando se va a comenzar la comunicación se realiza una negociación en tres pasos (figura 8): el cliente le envía al servidor su encabezado TCP con la bandera SYN activada e indicando el número de

[13] **Hijacking:** nombre de un ataque que traducido al español significa secuestro.

secuencia corresponde ”a”, cuando el servidor ha recibido el encabezado TCP correcto confirma la conexión que contiene la bandera SYN y ACK activada, indicando también su número de secuencia “b” y el acuse de recibo “a+1”, y finalmente el cliente le envía un ACK con acuse de recibo”b+1”(Ochoa,2011). Lo que hace el atacante es adivinar el número de secuencia correcto para realizar el primer paso del inicio de comunicación TCP/IP; si lo logra recibirá la confirmación del servidor y tranquilamente ha logrado suplantar al legítimo cliente; secuestrar la conexión, sin embargo si no envía el número de secuencia correcto se rechazará la negociación de la conexión.

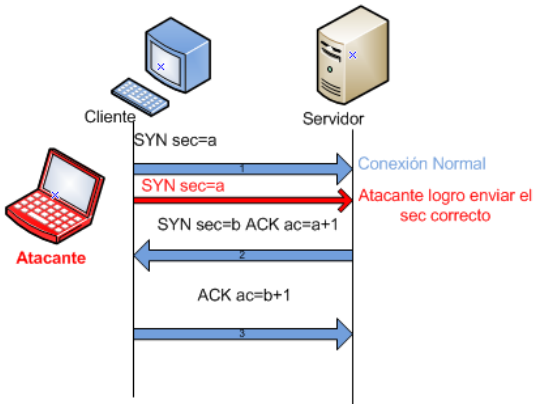


Figura 8. Proceso de conexión TCP/IP con un atacante

Elaborado por: Autora del Proyecto

- **SMTP Spoofing:** Este es otro tipo de suplantación, usado por los spammers para enviar correos con el objetivo de propagar código malicioso, ó realizar phishing; suplantando la dirección de correo legítima de un usuario afectando su reputación; pues figura como el emisor, ó simplemente usando una dirección de correo falsa.

Este ataque se desarrolla gracias a que el protocolo SMTP es vulnerable, porque no proporciona fuertes mecanismos de autenticación; y el puerto 25 se encuentra presto a establecer conexiones que no están restringidas sólo a la red interna; entonces si un hacker genera un telnet en el puerto 25, tranquilamente recibirá respuesta del servidor (Pandove, Jindal, & Kumar, 2010), lo que significa que se encuentra conectado al mismo. Dentro del servidor con el comando “rept”, se puede especificar a quienes se enviará el correo; a continuación simplemente se redacta el correo y se envía.

También se puede realizar este tipo de ataque a través de un servidor web, gracias al lenguaje php; que permite enviar correos falsos, como se muestra a continuación un ejemplo de (Pandove, et.al, 2010):

```
<?php
$toemail = $_POST['toemail'];
$fromname = $_POST['fromname'];
$fromid = $_POST['fromid'];
$subject = $_POST['subject'];
$message = $_POST['message'];
$headers = "From: $fromname <$fromid>";
mail($toemail,$subject,$message,$headers);
echo "Mail Sent!";
exit();
?>
```

Como se puede observar en el código se encuentra el receptor, el asunto, el mensaje, el emisor del correo y cuando se envía imprimirá “Mensaje Enviado”.

- **DNS Spoofing:** Este tipo de suplantación aprovecha vulnerabilidades de los servidores de DNS, que reciben entradas de DNS sin tener políticas correctamente predefinidas de seguridad, con las cuales tenga conocimiento

de los servidores DNS confiables para recibir información. Por consiguiente, el servidor guarda en su caché información corrupta que puede ocasionar los siguientes problemas (Kimberly, 2010):

- Si un usuario necesita acceder algún servidor; pedirá a su servidor DNS que tiene configurado, que le resuelva el nombre y le dé la respectiva IP para establecer la comunicación; pero el atacante habrá colocado las IPs corruptas según su conveniencia, a servidores que él tiene control para así generar otros ataques como el phishing, inyección de código malicioso, robo de información, etc.
- Se genera una denegación de servicio, porque se deja de lado los auténticos servicios.
- Los atacantes pueden leer, modificar o eliminar correos, con tan solo modificar el MX (Intercambio de correo), que es una entrada DNS que direcciona hacia un servidor de correo autorizado; pero si se corrompió esto se puede estar direccionando hacia un servidor de correo falso.

Tipos de DNS Spoofing según (Kimberly, 2010)

Tabla 16. Tipos de DNS Spoofing

Tipos DNS Spoofing	Descripción
Intranet Spoofing	Se da cuando se actúa como un equipo dentro de la misma red interna.
Internet Spoofing	Se da cuando actúa como un dispositivo en el internet.
Proxy Server DNS Poisoning	El envenenamiento de DNS del servidor proxy, es un ataque al servidor proxy de la organización, en el que se cambia las entradas que posee el proxy; lo que provoca que los usuarios sean re direccionados a otras redes.
DNS cache Poisoning	El envenenamiento de la cache DNS, es un ataque por el cual se modifica las entradas de la cache DNS, lo que resulta en direccionar incorrectamente a los usuarios a otros equipos.

Fuente: (Kimberly, 2010)

❖ **Web Spoofing:** consiste en la suplantación de un sitio web, que por lo general es de confianza del usuario y en el que suele ingresar información delicada, como claves o números de cuenta; independientemente de que exista una conexión TLS/SSL (Seguridad de capa de transporte/Seguridad de capa de sockets[14]) (Ochoa, 2011). Primero el atacante ha de insertar algún link falso en un correo a través de un ataque SMTP spoofing, o colocando el link en un buscador; para esto hace uso del ataque **"typehijacking"[15]**. Luego el hacker crea una réplica de la página real y lo coloca en un servidor web ilegítimo denominado SWS (Server Web Spoofing); principalmente enfocándose en el diseño para que la víctima no perciba nada extraño, obviamente modifica todo enlace que lleve al servidor confiable para que conduzca al del atacante y los formularios en los que el usuario ingresa su información, registren la misma en el SWS.

Proceso de un ataque Web Spoofing

1. El usuario atacado solicita a través de un URL al servidor SWS quien procesa la solicitud y hace petición al servidor confiable.
2. El Servidor confiable responde la petición al SWS, el cual modifica el contenido a su conveniencia y responde con la página falsa al usuario atacado.

[14] **Socket:** es una identificación que permite establecer conexión en la capa de transporte.
[15] **Typehijacking:** modificación leve del nombre de una página web real, para asignarle a una falsa para que exista una similitud que lleve a la confusión visual del atacado.

3. De ser el caso el usuario llena formularios con su información privada y envía al SWS.

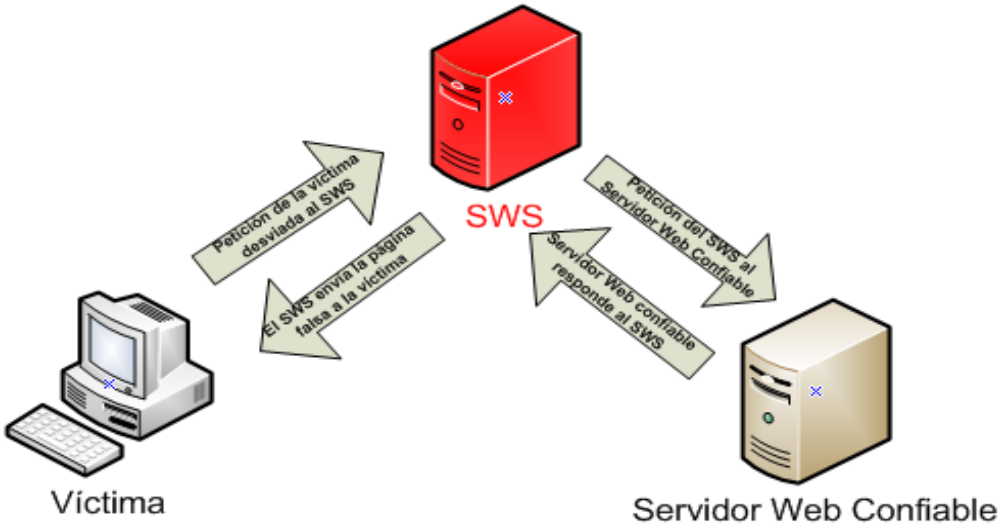


Figura 9. Proceso del Web Spoofing

Elaborado por: Autora del Proyecto

El **MAC Spoofing** es un ataque de suplantación más común en lo que son las redes inalámbricas por lo que se trata en los principales ataques a las redes inalámbricas, 2.4.3.

b. SPAM

El spam es todo tipo de mensaje no deseado que suele llegar de un emisor desconocido; este tipo de ataque es ampliamente difundido en el correo electrónico, posee las siguientes características, (Facua org, 2011):

- En su mayoría suele tener contenido publicitario, supuestas ofertas, venta de productos, inclusive ofertan pornografía.
- Este tipo de mensajes a menudo vienen acompañados de código malicioso, o phishing.

- El correo tiene un tipo de asunto llamativo, para captar la curiosidad del usuario.
- Tienen un remitente a menudo desconocido, aunque también suelen infiltrase y usar cuentas de otras personas, si se desea contestar este tipo de mensajes no lo permite.
- Existen algunas variantes de este tipo de ataque como son: **spam** propiamente dicho a través de correo electrónico, **spam SMS** cuando se recibe mensajes SMS en el dispositivo móvil no deseados, **spim** cuando se recibe mensajes instantáneos no deseados y **spit** que es spam hacia la telefonía IP (Facua org, 2011, pág. 10).

El spammer trata de conseguir la mayor cantidad de cuentas de correo válidas, en las cuales pueda cumplir su acometido para ello se une a los más conocidos servidores gratuitos de correo buscando contactos para añadirlos a su cuenta, usa programas que buscan en internet cuentas en páginas como blogs, compran ilícitamente bases de datos de organizaciones, ó simplemente trata de adivinar las cuentas de los destinatarios de un dominio.

Proceso del ataque (Ochoa, 2011)

1. El spammer genera el spam con un campo from[16] con direcciones que por lo general coloca al azar.

2. Se encuentra el servidor de correo que posee debilidades y se le inyectan los spam, que serán enviados a otros servidores de correo.

[16] **Campo from:** en un email corresponde al emisor, es decir “De:”.

3. Los servidores atacados y sobre todo vulnerables a este tipo de ataques, entregarán los correos a los destinatarios que si existan, pero tendrá que consumir sus recursos generando informes de error como respuesta a las direcciones de correo incorrectas.

c. Troyanos y Backdoors

El **troyano** es un programa malicioso que se oculta bajo alguna aplicación considerada buena por el usuario, causando pérdidas o robo de datos, caídas del sistema o lentitud en el mismo, inclusive apagar o reiniciar los equipos infectados (Kimberly, 2010). También pueden ser el comienzo de otros ataques como la denegación de servicio.

Generalmente viajan a través de un archivo compartido de NetBIOS[17], unido a un mensaje instantáneo ó un e-mail, un programa descargado de internet tal es el caso de software libre, imágenes, música, videos, protectores de pantalla, en la tabla 17 se presentan los más comunes troyanos.

Tabla 17. Programas Troyanos comunes

TROYANO	PROTOCOLO	PUERTO
Back Orifice	UDP	31337 ó 31338
Deep Throat	UDP	2140 y 3150
Netbus	TCP	12345 y 12346
Whack-a-Mole	TCP	12361 y 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Master's Paradise	TCP	3129, 40421, 40422, 40423 y 40426

Fuente: (Kimberly, 2010)

[17] **NetBIOS:** Network Basic Input/Output System, es una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

Los **Backdoors** son un programa o conjunto de programas que se instala en el equipo víctima con el objetivo de obtener un acceso a la máquina, en el momento que desee el hacker sin ser percibido. En ocasiones se encuentra unido a un troyano para lograr su acometido; por otro lado su acceso transparente como en el caso de los sistemas operativos Windows se logra disfrazándose, como un servicio; obviamente con un nombre discreto para evitar la atención del usuario.

Existen algunos backdoors avanzados que se disfrazan con nombres de otros servicios del mismo sistema, pero que se encuentran detenidos o son de inicio manual, el acceso que obtiene el hacker son de tipo administrador generalmente, para poder manejar el equipo a su antojo; como ejemplo de este tipo de backdoor existe RAT (Remote Access Troyan) (Kimberly, 2010, pág. 108), que permite a más del acceso al sistema la comodidad de ser remoto.

d. Virus y Gusanos

Los virus y gusanos son código malicioso (malware), son usados por el atacante para acceder al sistema y se esparcen como si en realidad fueran gérmenes; aprovechando vulnerabilidades. Tanto virus como gusanos pueden ser portadores de troyanos y backdoors; por lo tanto se podría decir que en muchas formas son similares; pero su principal diferencia radica en la forma en que se propagan, por un lado los virus necesitan de un programa portador, en el que ha sido inyectado previamente, provocando el contagio cuando este programa se ejecuta y así comienza la propagación en el sistema; los más comunes portadores son juegos, animaciones, sripts en visual basic,

dispositivos de almacenamiento portables , correo infectado que a su vez usa los contactos para seguirse propagando, etc.

En cambio los gusanos, no requieren de un programa portador así que se propagan a sí mismos; obviamente en ambos casos sin que el usuario se dé cuenta de que su equipo se ha convertido en portador de malware.

❖ **Tipos de Virus**

Se clasifican según lo que infectan y la manera en que infectan (Kimberly, 2010):

- **Según lo que infectan:** son virus que normalmente afectan sectores del sistema, archivos, macros (como Microsoft Macros), archivos complementarios (como los archivos INI y DLL), clusters del disco, archivos batch (archivos BAT), Código Fuente.
- **Según la manera en que infectan:** se puede apreciar los tipos en la tabla 18:

Tabla 18. Tipos de Virus

Virus	Descripción
Virus Polimórficos	Cada vez que infectan cifran su código de manera diferente; así van cambiando de forma para evadir su detección
Virus de Sigilo	Estos virus modifican sus características originales, tales como hora y fecha para que el sistema no los detecte como archivos nuevos
Agente de infección Rápidos y Lentos	Estos virus evaden la detección del antivirus, gracias a que infectan muy lentamente o muy rápido.
Virus Esparcido	Estos virus afectan a pocos sistemas o aplicaciones.
Virus Blindados	Cuando los virus se cifran para evitar ser detectados.
Virus Multipartito	Son virus que generan múltiples infecciones.
Virus de la Cavidad (Espacio Lleno)	Estos virus atacan espacios vacíos de archivos en el equipo
Virus de túnel	Estos virus son enviados a través de un protocolo diferente o encriptado para poder atravesar el firewall.
Virus camuflados	Son virus que aparentan ser otros programas.
Virus de NTFS y Directorio Activo	Virus que atacan los archivos NT y el Directorio Activo de los sistemas Windows.

Fuente: (Kimberly, 2010)

e. Sniffers

Un sniffer es un programa que permite monitorear, analizar y capturar el tráfico que fluye en la red. Para cumplir con este objetivo coloca la NIC de un host en modo promiscuo; esto significa que recibirá y enviará el tráfico sin necesidad que esté dirigido a él, las herramientas de hacking proporcionan un driver a la NIC que asegura el soporte en este modo (Kimberly, 2010). Adicional los hackers se aseguran de recibir el tráfico por lo general realizando ataques de ARP.

Los objetivos más comunes del sniffing son: conseguir claves y usuarios que no han sido correctamente encriptados (aunque actualmente los hackers más experimentados usan herramientas que pueden descifrar el tráfico encriptado), monitorear posibles fallos en la red como cuellos de botella,

monitorear la correcta comunicación servidor-cliente, incluso deja al descubierto tráfico malicioso.

Medio de comunicación y el sniffing

Para capturar el tráfico es indispensable ubicarse apropiadamente dentro de un medio compartido ya sea cableado o wireless (Kimberly, 2010).

- **Cableado:** en este caso se puede realizar un sniffing si se usa hubs en la red; que son significado de inseguridad, esto se soluciona con el uso de switches que usan sus tablas CAM (tabla que posee la relación puerto-MAC correspondiente). Pero si en un switch se ha configurado un replicado de puertos (port mirroring[18]); este puede ser usado para conectar el sniffer; por lo general el administrador de red realiza esta configuración con fines de monitoreo éticos.
- **Wireless:** el aire como medio compartido, obviamente es más inseguro, el sniffer simplemente necesita una tarjeta inalámbrica que tenga una buena recepción al objetivo.

f. Denegación de Servicio DoS

Un ataque de denegación de servicio es aquel que intenta dejar fuera de operación un host o sistema objetivo. También puede hacer que su rendimiento sea más lento, queden fuera algunos servicios ó que los usuarios legítimos del sistema no puedan acceder al mismo.

Para esto se basan en múltiples técnicas que se aprovechan de las debilidades de los equipos, protocolos; entre otros, para que así él o los equipos

[18] **Port mirroring:** configuración en un puerto de switch para que el tráfico que pasa por un puerto se refleje en otro puerto.

víctima sobrecarguen sus recursos como memoria y CPU. A continuación algunas formas como consiguen la saturación del objetivo:

Tabla 19. Formas de Saturar un Objetivo - DoS

Formas de Saturar un objetivo DoS	Inundan la red con tráfico basura, que evita el flujo del tráfico legítimo.
	Modifican los paquetes a su conveniencia y los envían masivamente, aprovechando la debilidad de protocolos que no están orientados a la conexión como UDP e ICMP. Incluso el protocolo orientado a la conexión TCP, enviando gran cantidad de requerimientos de conexión dejando varias conexiones semiabiertas que saturan a la víctima.
	Interrumpen una conexión o un servicio específico entre emisor y receptor legítimos.
	Aprovechan que algunos equipos no están preparados para tráfico inesperado.
	Envían tráfico incorrecto a equipos de comunicación legítimos; por ejemplo a un router, un equipo malicioso le envía información incorrecta a su tabla de enrutamiento
	Se valen de los recursos de otros sistemas (BOTNET) que son víctimas secundarias, para inundar con el tráfico de ataque.

Elaborado por: Autora del Proyecto

Clases de Denegación de Servicio (Kimberly, 2010)

- **Simple denegación de Servicio DoS**

Cuando un host envía el ataque a un objetivo.

- **Denegación de servicio distribuida DDoS**

Cuando múltiples sistemas envían el ataque a un objetivo, por consiguiente necesita primero comprometer a otros sistemas (BOTNET), para atacar. Dentro de este proceso se encuentran tres partes que entran en juego: el master, esclavo y víctima.

Fases DDoS

Este se basa en dos fases (Kimberly, 2010); primero la fase de intrusión, el hacker busca sistemas débiles e inyecta herramientas de DDoS para convertirlos en esclavos, también llamados zombis ó BOTs.

En la segunda fase el master; quien es la cabeza del ataque, dirige a los esclavos en el ataque al sistema víctima.

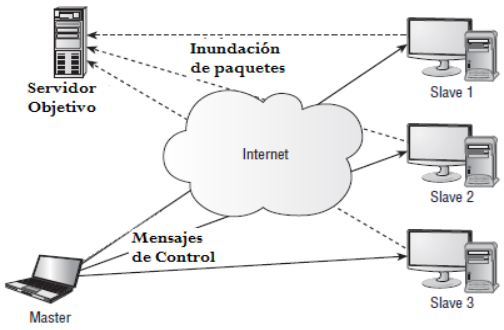


Figura 10. Anatomía de un Ataque Dos

Fuente: (Kimberly, 2010)

Claro está que esta clase de ataques; no tan elegantemente preparados, pueden no significar un robo de información o accesos, pero es enormemente perjudicial si se considera la indisponibilidad del negocio; adicional al desprestigio que genera en los consumidores.

Se puede generar un filtrado con ayuda de los proveedores de servicio de red; incluso los equipos de red nuevos tienen maravillosas herramientas que permiten el filtrado, protección contra algunos ataques como el ping de la muerte, incluso permiten la administración del ancho de banda según el tipo de tráfico; además existen los IDS, herramientas de rastreo muy útiles en caso de un ataque de este tipo ó también herramientas para auditar la red y los host;

para así evitar las BOTNETs. A continuación, en la tabla 20 se encuentran algunos ejemplos de ataque DoS.

Tabla 20. Ejemplos de Ataques de DoS

Ataque	Descripción
Ping de la Muerte	Se envía varios paquetes echo request (ping), de tamaño mucho más largo que lo normal; que necesitan fragmentarse y reensamblarse, lo que provoca saturación del equipo.
Ataque LAND	El atacante envía paquetes con la dirección IP del equipo atacado tanto en el destino como en el origen, como resultado genera un bucle que lleva al bloqueo del equipo
Ataque WinNuke	Es un programa de ataque DoS también denominado ataque de fuera de límite OOB(out-of-bound); que busca un sistema objetivo con el puerto 139 abierto para proceder a enviar tráfico IP basura en él.
Smurf	Se envía gran cantidad de paquetes ICMP echo request con la dirección IP de destino igual a la dirección broadcast y como origen la IP atacada, la cual se saturará cuando le respondan con echo reply.
SYN Flood	El atacante envía numerosos segmentos TCP con la bandera SYN activada, que indica el deseo de empezar una sesión, el equipo receptor enviará un SYN-ACK; como corresponde a una comunicación TCP de tres vías, pero el emisor no responderá con ACK dejando la sesión semiabierta; claro está que pasado un tiempo se cerrará la sesión por no existir respuesta, pero este tiempo tendrá su peso cuando se trate de varias conexiones.

Elaborado por: Autora del Proyecto

g. Escaneo de Puertos

Realizar un escaneo en la red se convierte en un primer paso para cualquier ataque más elaborado, existen varios tipos de escaneo como el de red, vulnerabilidades y puertos; este último es realizado por alguna herramienta que busca puertos TCP o UDP abiertos, para así documentarlos y usarlos en un siguiente ataque. Se apoyan en el conocimiento de los puertos bien conocidos 0-1023, en donde se encuentran los protocolos más usados como por ejemplo 80 HTTP, 23 TELNET, 110 POP3, etc.

Una herramienta muy conocida es NMAP; que permite realizar un escaneo de puertos, aunque para ello primero debe realizar un ping sweep, que no es

más que reconocer las direcciones IP, luego se vale de algunos tipos de escaneos propios (Kimberly, 2010), como son:

Tabla 21. Tipos de Escaneos con NMAP

Tipos de Escaneos con NMAP	Descripción
TCP connect	Abre conexiones full dúplex TCP en los puertos más conocidos, es muy seguro pero es muy detectable.
SYN stealth scan	El atacante solo envía un SYN, el objetivo responde con un SYN-ACK, pero no se responde con el ACK así se evita establecer una conexión full dúplex TCP y sobre todo ser detectado.
Null scan	Envía paquetes con todas las banderas apagadas y retorna cerrando los puertos, por ello el firewall puede pasar por alto este escaneo, es usado en sistemas Unix.

Fuente: (Kimberly, 2010)

2.3.2. Debilidades en Wi Fi

a. Debilidades en WEP

Para el año de 1999 con el surgimiento del 802.11b y la Wi Fi Alliance, surge también un interés enorme de la comunidad de hackers sobre la seguridad en las redes inalámbricas, que al cabo de muy poco tiempo WEP dejó mucho que desear, tanto así que el IEEE 802.11actual (IEEE802.11, 2012, pág. 94), ya lo determina como “deprecated” (fuera de uso).

Este hecho ocurre, porque en su diseño se da más prioridad a la necesidad de un rápido proceso de encriptación que evite la necesidad de mayor tiempo de procesamiento; y con ello dar menos velocidad a la comunicación; con esto RC4 encajó más que bien; por ser un algoritmo de encriptación de flujo en el cual resulta el mismo tamaño de texto a cifrar con el texto cifrado, a diferencia de los actuales algoritmos de bloque. A continuación se detalla las principales debilidades en WEP:

- Comenzando por el proceso de autenticación, tanto los clientes como el AP deben tener una misma contraseña compartida PSK, que en el protocolo se da por intercambiada entre los dispositivos por algún método seguro fuera de 802.11 (IEEE802.11, 2012, pág. 171), teniendo como consecuencia una clave estática y la confidencialidad a expectativa de que el usuario no vaya a compartir la clave con otros usuarios.
- Continuando con el proceso de autenticación el usuario envía un requerimiento al AP este le envía un texto de desafío ”challenge text” en texto plano; el cliente responde con el texto de desafío cifrado con la clave compartida y si corresponde a la que conoce el AP la autenticación es exitosa; pero cabe señalar que con una captura de tramas; a través de un sniffer, de los textos de desafío tanto en texto plano como cifrado, se puede obtener el flujo de clave (vector de inicialización IV más la PSK); adicional el vector de inicialización viaja en la comunicación en texto plano. En consecuencia se puede proceder a cifrar mensajes (Vladimirov, Gavrilenko, & Mikhailovsky, 2005).
- No se autentica el AP sólo el cliente, lo que da como resultado ataques con APs intrusos (Iniesta, 2010).
- La clave WEP solo está conformada por 40 bits ó 104 bits, más 24 bits que corresponden al IV (IEEE802.11, 2012), por lo tanto en el caso de los 40 bits es muy sensible a un ataque de fuerza bruta, que no demorará mucho en obtener la combinación de bits que corresponden a la clave, mientras que para el valor de IV se toma de un conjunto de valores predeterminados;

cayendo en la reutilización de los mencionados; que provocan ataques que aprovechan esta vulnerabilidad (Vladimirov, et.al, 2005).

- Se puede obtener la clave PSK, gracias a que se conoce que los primeros bytes del texto plano de la comunicación corresponde a la cabecera LLC, que para el caso de IP se activa SNAP(Subnetwork Access protocol) poniendo los campos SSAP y DSAP al valor hexadecimal predeterminado 0xAA; con esto puede determinar el primer byte de la clave, así sucesivamente se trabaja con los supuestos textos planos y el texto cifrado para seguir obteniendo el resto de bytes de la clave; como es un proceso mecánico y secuencial se han creado varias herramientas que realizan estos ataques como WEPCrack, inclusive si se aumenta el largo de la clave sólo se obtendrá un aumento de tiempo de crecimiento lineal, ni siquiera exponencial como se creería óptimo (Vladimirov, et.al, 2005).
- Tanto para autenticar y cifrar se usa la misma clave (IEEE802.11, 2012).
- En cuanto a la integridad usa CRC para verificar errores en la trama; introduciendo un ICV (Integrity Check Value) (IEEE802.11, 2012) que por ser un método lineal se puede determinar cuáles son los bits que producen una variación en los bits del ICV; a pesar de que viaja encriptado, porque la relación mencionada sobrevive a la operación XOR de la encriptación, así que se puede modificar los datos de las tramas y colocar un ICV logrando evitar que el receptor se dé cuenta. Es decir, lastimosamente el ICV no se basa en la clave PSK ni el IV, sino sólo en los datos (Hernando, 2007).

b. Debilidades de WPA

WPA posee mejoras en el manejo de claves, aparece ya un WPA corporativo con uso de un servidor RADIUS para la autenticación a través de 802.1x, pero aún se sigue basando en el algoritmo de encriptación RC4, con sus consecuentes debilidades ya presentadas, pero que con TKIP disminuyen considerablemente; a continuación se detalla sus vulnerabilidades (Rios, 2011):

- El proceso de autenticación es una etapa vulnerable; cuando se trata del modo WPA Personal, por el mismo hecho de tener una única clave compartida entre todos los dispositivos, que se espera no se filtre a terceros por falta de confidencialidad de un usuario legítimo; además las claves compartidas viajan en este proceso, de ahí que en una captura de paquetes se puede llegar a obtenerlas y se puede descifrarlas. Así el atacante puede autenticarse y generar las claves compartidas; es decir se logra vulnerar la seguridad si se conoce el contenido de la trama de autenticación y su valor cifrado.
- Es susceptible de ataques de diccionario sobretodo en el caso WPA Personal en el que existe una sola clave, pero en el corporativo esto se puede evitar con una configuración adecuada, por ejemplo permitiendo un determinado número de intentos de ingreso a la WLAN.

c. Debilidades de WPA2

Con WPA2, se disminuyó enormemente la brecha de inseguridad en lo que respecta a la encriptación gracias al algoritmo AES; a continuación se detalla algunas vulnerabilidades (Kimberly, 2010):

- El algoritmo AES requiere de un alto procesamiento por lo que algunos PDAs, necesitan trabajar en modo WPA2 mixto es decir usan TKIP para la encriptación.
- Es susceptible ataques de diccionario similar a WPA, en su modo personal; en el modo corporativo se logra evitar con una buena configuración de los equipos tanto autenticador (AP) y servidor de autenticación (servidor RADIUS).
- En el modo WPA2 Personal, se tiene que difundir la clave a todos los dispositivos por lo que si en el proceso un atacante logró obtener una clave, estaría al menos en la posibilidad de espiar el intercambio de claves entre un AP y un cliente.

2.3.3. Principales Ataques en Wi Fi

Los atacantes de las redes inalámbricas no necesitan subir más allá de la capa de enlace de datos para atacar, porque más allá de las vulnerabilidades que presentan los protocolos de seguridad de Wi Fi, su punto más débil es el medio de comunicación por el que viajan las tramas; aquí son capturadas, analizadas, modificadas según el objetivo final que necesite el atacante, que va desde simplemente denegar el servicio, modificar información, incluso poder seguir accediendo a la red y provocar mucho más daños. Los más comunes ataques son:

a. Craqueo de los Mecanismos de Encriptación y Autenticación

Este es un común ataque, los atacantes expertos a lo largo del tiempo desarrollaron técnicas e incluso las incorporaron en herramientas; con el objeto

de conectarse a la WLAN, robar credenciales, capturar datos, poder cifrar y descifrar, así lograron craquear WEP, como es el caso de:

- **Ataques FMS:** Es el más común ataque usado por las herramientas de craqueo de WEP, fue publicado en el 2001 en el documento titulado "Weaknesses in the Key Scheduling Algorithm of RC4" realizado por Scott Fluhrer, Itsik Mantin y Adi Shamir (FMS), y se basa en los siguientes principios (Vladimirov, et.al, 2005, p.220):

1. Algunos vectores de inicialización preparan el sistema de cifrado RC4 de tal forma que puede revelar información sobre la clave en sus bytes de salida.

2. La debilidad de invariancia permite utilizar los bytes de salida para determinar los bytes más probables de la clave.

3. Los primeros bytes de salida son predecibles siempre, ya que contienen la cabecera SNAP definida por la especificación IEEE.

Por lo tanto una clave de WEP se puede obtener, al capturar cierta cantidad considerable de tramas y con el texto plano de SNAP común poder obtener la clave, pues el resultado cifrado se obtiene de la operación XOR entre el texto plano y el flujo de clave; así sucesivamente en un tiempo considerable se puede obtener todos los bytes de la clave. Por ello se ha generado ataques FMS mejorados como por ejemplo el de H1kari de Dasb0den Labs. , que permite disminuir el tiempo y cantidad de paquetes a capturar, porque previo se realiza un análisis de la aparición de vectores de inicialización débiles y cómo se relacionan con los bytes de la clave, así obtienen algoritmos para filtrar IV

débiles a través de la clave secreta que puedan atacar. Así como también los **ataques PTW y Korek**, que simplemente juegan con los algoritmos para necesitar menos capturas de tramas y lograr romper la clave WEP.

b. Ataques de Vigilancia

Se refiere a los “scanners WLAN” mediante los cuales se realiza un barrido de la información que viaja por el aire en medio de una comunicación Wi Fi, entre un cliente y su correspondiente AP; es de tipo pasivo y le proporciona al atacante la información necesaria para prepararse para proceder con ataques más elaborados (Ochoa, 2011), por ejemplo:

- **Eavesdropping ó Sniffing:** este ataque consiste en estar monitoreando la red, para ello coloca la antena del atacante en modo monitor; así permanece capturando información que viaja en el medio de una WLAN, obtiene información para un futuro ataque más elaborado. Si se trata de una comunicación cifrada con algo de esfuerzo, conocimiento o simplemente fuentes de información como internet se obtendrá descifrar; imagínese un punto de acceso inalámbrico sin encriptación, resulta mucho más fácil para el atacante observar la información, por eso es importante que se use una VPN o cifrado a través de la capa de aplicación SSL.
- **Wardriving y Walkchalking:** Un atacante se mueve a través de un área en un vehículo, con un dispositivo con tarjeta inalámbrica y un GPS, en busca de redes inalámbricas abiertas, es decir sin protección. Luego de esto se produce el walkchalking, que no es más que la señalización con símbolos que describen el estado de la WLAN. Este ataque puede ser muy común

sobre todo por la irresponsabilidad de ciertos empleados en una organización que conectan APs no permitidos a la red para su comodidad, dejando una brecha en la seguridad de la red; ó simplemente hogares y pequeñas empresas u oficinas que dejan de lado el tema seguridad, conectan los equipos con configuraciones por defecto, que por lo general no incluyen ninguna seguridad.

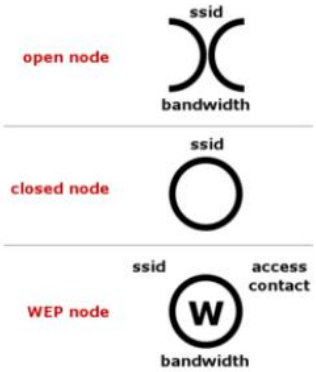


Figura 11. Simbología utilizada en el Walkchalking

Fuente: (Hernando, 2007)

c. Denegación de Servicio

Esta clase de ataque tiene lugar en la capa de enlace de datos, donde 802.11 es más vulnerable, es así que con una simple emisión de ruido RF se puede generar interferencia que deje fuera de operación a un AP permitido en la red, con ello dar lugar a que un **AP intruso** tome su lugar y se haga cargo de la comunicación con los clientes autorizados.

Con respecto a la Capa LLC se puede realizar un **ataque de DoS de desautenticación**, que no es más que el envío de tramas de desautenticación (DEAUTH), o simplemente enviando continuamente tramas falsas. Adicional

WPA es susceptible a un ataque de DoS, porque si un usuario está intentando autenticarse por lo menos dos veces fallidas en un segundo, asume que existe un ataque y se da de baja; esto supone una medida de seguridad pero que es aprovechado por los atacantes.

Se puede realizar un **ataque Queensland** (por ser descubierto en la universidad australiana de Queensland) ó también llamado **ataque CCA (Clear Channel Assessment)**, en el cuál el atacante envía constantemente CCAs; que son las tramas usadas por CSMA/CA para determinar si el canal está libre para usarse o no, entonces para este caso determinan el canal como ocupado.

Adicional se enfocaron en atacar la autenticación 802.1x en Cisco con el EAP-LEAP, logrando los siguientes tipos de DoS (Vladimirov et al., 2005):

- **Basados en el bombardeo con tramas EAPOL-start:** El EAPOLStart (Extensible Authentication Protocol) es la trama en la cual un cliente ó también llamado suplicante pide al autenticador en este caso el AP, autenticarse por consiguiente muchas peticiones de autenticación pueden saturar el equipo.

- **Basados en recorrer todo el espacio de identificadores EAP:** algunos puntos de acceso quedan fuera de servicio cuando un atacante ha consumido todo el espacio de identificadores EAP (0-255).

- **Basados en enviar tramas EAP de éxito prematuro:** un cliente puede conectarse con otro AP ilícito del que supone ya recibió el EAP de éxito de su autenticación.

- **Basados en la falsificación de tramas de EAP de fallo:** Un atacante envía a los clientes que falló su proceso de autenticación.

Una medida de seguridad que se puede tomar frente a estos ataques es el uso de IDS y asegurar el perímetro donde funcionará la WLAN removiendo toda fuente de DoS.

d. Ataque AP Masquerading ó Evil Twin

APs intrusos intentan hacerse pasar por APs legítimos, aplicando una configuración similar al permitido, como por ejemplo el mismo nombre de SSID, misma configuración de seguridad, entre otros. Clientes cercanos se unirán al AP intruso, creyendo que tienen una buena cobertura de la WLAN legítima (Kimberly, 2010)).

e. MAC Spoofing

Este es una forma en la que el atacante intenta hacerse pasar por un usuario legítimo, sobre todo en una WLAN que base la conexión de sus clientes en listas de filtrado MAC, entonces por el variado número de herramientas incluso gratuitas que existen en internet; disfrazan su MAC original y logran conectarse. Queda claro que este ataque se puede evitar si no se usa este tipo de filtrado y con un IDS inalámbrico adecuado.

f. ARP Poisoning/ Man in the middle

Este es un ataque en el cuál los APs que están trabajando en modo bridge son vulnerables, pues el atacante tiene que colocarse en la misma LAN lógica para lograr su cometido. ARP es el protocolo mediante el cual, a partir de una dirección IP se resuelve su correspondiente dirección MAC de un equipo destino; para así poder enviar las tramas; para ello usa un broadcast consultando la información (ARP request) a la espera de un unicast de

respuesta, ahora bien el gran inconveniente es que este protocolo no guarda estados, en consecuencia a una máquina que reciba una respuesta ARP colocará dicha información en su caché sin importar si es correcta o no; es ahí donde el atacante se aprovecha para enviar su MAC como la MAC de otro equipo.

Man in the middle es una consecuencia del ataque anteriormente mencionado, un intruso envía su MAC como si fuera el cliente al AP y el AP al cliente, para ello también hace uso de las tramas DEAUTH para desautenticar al cliente y cumplir el objetivo; así logra colocarse en la mitad de la comunicación, para realizar lo que requiere con la información; sea capturar, modificar, borrar, entre otros (Rios, 2011).

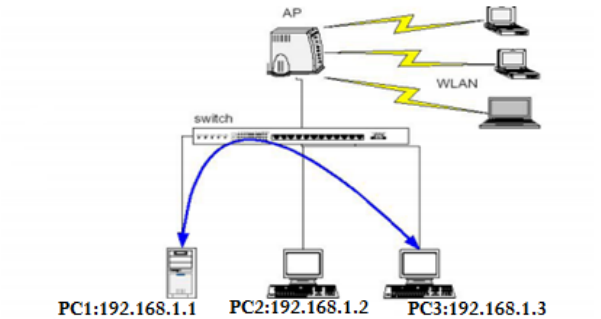


TABLA ARP PC1

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.3	3C:2A:4A:59:1A:7A

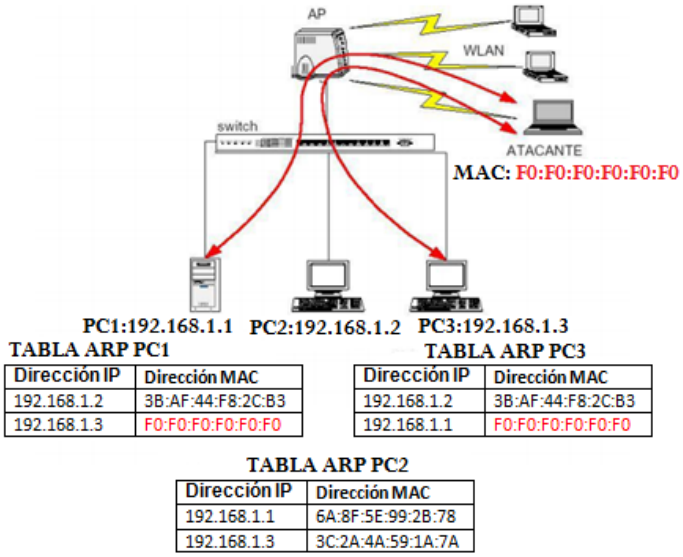
TABLA ARP PC3

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.1	6A:8F:5E:99:2B:78

TABLA ARP PC2

Dirección IP	Dirección MAC
192.168.1.1	6A:8F:5E:99:2B:78
192.168.1.3	3C:2A:4A:59:1A:7A

(a)



(b)

Figura 12. (a) Legítima comunicación inalámbrica (b) Atacante envenenando la caché ARP de los dispositivos y logrando colocarse en la mitad Man in the middle

Fuente: (Rios, 2011)

g. Ataques de fuerza bruta y diccionario

Este tipo de ataques usan la adivinanza de claves aprovechando la debilidad de las mismas que comúnmente usan los usuarios, apelando a su memoria débil.

- **Ataques de diccionario:** este es un ataque mediante el cual se intenta ingresar a la WLAN autenticándose como si se tratase de un usuario permitido, colocando contraseñas una y otra vez hasta llegar a la clave correcta; con el uso de un archivo que contienen las palabras comunes de un diccionario, que han sido sometidas al mismo proceso hashing[19] de autenticación que usa el sistema (Kimberly, 2010). Este es un tipo de

[19] **Hashing:** conjunto de algoritmos que una entrada se resuma en una salida (sólo la misma entrada generará la misma salida).

ataque muy débil, tranquilamente se lo puede evitar si se coloca claves con combinaciones de números, letras mayúsculas y minúsculas.

- **Ataques de fuerza bruta:** Este es un tipo de ataque que consume mucho tiempo, porque trabaja en todas las combinaciones posibles de números, letras mayúsculas o minúsculas y símbolos, hasta conseguir la clave verdadera. Cabe destacar que este tipo de ataque puede llegar a ser efectivo si tiene el tiempo que él requiera y un procesamiento muy alto (Kimberly, 2010).

Ambos ataques se pueden evitar si se da un considerable número exacto de intentos al usuario, para ingresar al sistema, antes declararlo bloqueado o simplemente cerrar la sesión, lo que a veces es aprovechado para realizar una DoS.

CAPÍTULO 3

SISTEMA DE DETECCIÓN DE INTRUSOS

Cuando se trata de aplicar seguridad más allá de que se trate de un sistema informático, se necesita un equipamiento para proteger o al menos identificar a los intrusos; como por ejemplo si se trata de un domicilio o negocio se pueden valer de cámaras de vigilancia y alarmas conectadas con la policía. Ahora bien para un sistema informático se han desarrollado los **IDS (Intrusion Detection System)**, que similar a nuestros ejemplos anteriores, ofrecen vigilancia y alertan al administrador de red a tomar acciones frente a un ataque en curso; gracias al sniffing del tráfico en la red que realiza y su análisis para determinar ataques.

Si bien se podría creer que es una herramienta poco útil porque el ataque ya está produciéndose, cabe recalcar que nada está escrito y definido inalterablemente, al menos el mundo de los ataques e intrusiones es muy cambiante y cada vez más sofisticado; si al menos nos permite identificar que algo anómalo ocurre es de gran ayuda. Además; a través de una honeynet[20] y un IDS se puede investigar, conocer y obtener un continuo proceso de aprendizaje tanto de intrusiones como ataques, que permitirán estar a la vanguardia de lo que ocurre en la red.

[20] **Honeynet:** red que simula una real para atraer atacantes.

3.1.1. Historia del IDS

En un principio todo tipo de análisis en los sistemas se propiciaba gracias a las auditorías de seguridad, que generaban eventos, almacenaban los logs generados, por último con toda la información recolectada se produce un análisis de resultados. Con el crecimiento exponencial de los equipos en la red surgió la necesidad de un análisis que evite informes manuales; que funcione un sistema automatizado de análisis de resultados, tanto de lo que se considera comportamiento normal y lo que se consideraría comportamiento anómalo.

Para los años 80 James Anderson; luego de un estudio para las fuerzas armadas estadounidenses, realiza un informe el cual se considera precursor en las investigaciones del IDS; que menciona la necesidad del desarrollo de un sistema de procesamiento de la información de seguridad, en el cual se pueda detectar como extraño toda conducta que se salga del registro de comportamiento común del usuario, que obtenga datos de todos los sistemas y suficiente como para que se logre encontrar el problema. Realizó un análisis estadístico, que fue gran idea para los posteriores estudios.

Luego en los años de 1986 y 1987 nace el modelo IDES (Intrusion Detection Expert System), que se basa en anomalías y abuso en los sistemas, con el aporte adicional del uso de perfiles que describen a los miembros del sistema y reglas de actividad de los mismos; que permiten determinar estadísticamente lo que se debe considerar anómalo. Para 1988 y 1990 se implementa la propuesta en un prototipo.

Por último en este resumen histórico, está el importantísimo aporte de la Universidad de California en 1990, con NSM (Network System Monitor); que ya realizaba un análisis de tráfico en la red; pues los antecesores utilizaban registros del sistema o pulsaciones del teclado. Así sucesivamente se desarrollaron varios proyectos y sistemas, con el fin de afrontar el creciente número de novedosos ataques.

3.2. Tipos de respuesta y Arquitectura

Cuando un IDS entra en funcionamiento debe responder frente a lo que su configuración y metodología determinen como intrusión, posible ataque, pero no siempre es así, siempre existirá un porcentaje de error, ya sea por falta de actualización, un mundo cambiante en técnicas de ataque, mala ubicación del IDS, etc. La figura 13 representa las respuestas que se obtiene en un IDS.

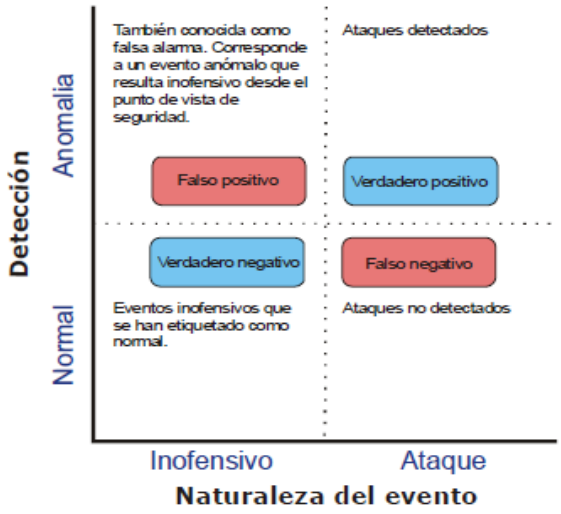


Figura 13. Posibles respuestas del IDS frente a eventos
Fuente: (Giménez, 2008)

3.2.1. Posibles respuestas frente a un ataque

a. Falso Positivo: son falsas alarmas que emite el IDS frente a tráfico inofensivo que lo confunde como ataque o intrusión. Lastimosamente este tipo de respuesta genera un gasto de recursos tanto del sistema como humano; esto puede generarse por una mala configuración o simplemente su metodología tiene fallas.

b. Falso Negativo: este es el peor de los casos porque el IDS no ha generado ningún tipo de respuesta frente a un ataque en proceso.

c. Verdadero Negativo: corresponde al tráfico común que se considera igualmente inofensivo en el IDS.

d. Verdadero Positivo: el IDS ha reconocido un ataque en su monitoreo.

Para evitar las malas respuestas como son los falsos positivos y negativos; sobre todo en un ambiente de producción, es necesario que se realicen pruebas y se mida la efectividad de los IDS a utilizar para evitar futuras sorpresas; adicional poseer una configuración, infraestructura y actualización conforme la evolución de la tecnología y el hackeo.

3.2.2. Arquitectura del IDS

Al existir gran cantidad de IDSs tanto propietarios como de software libre, cabe la necesidad de interoperabilidad entre las herramientas, además si existen ventajas, desventajas, características adicionales o áreas en las que han avanzado los desarrolladores; sería óptimo integrar algunos IDSs en producción para obtener mejores resultados.

Existen algunas organizaciones como CIDF, CISL, Aus CERT e incluso un grupo creado por la IETF (Internet Engineering Task Force) denominado IDWG; que se preocuparon del tema de comunicación entre los sistemas de detección de intrusos.

a. CIDF(Common Intrusion Detection Frameworks[21])

Este es un primer esfuerzo por estandarizar la arquitectura del IDS, especifica “cuatro cajas” (Mira, n.d.), que corresponden a las partes que debe tener el sistema de detección de intrusos:

- **Caja E-Generadores de Eventos:** su papel en el sistema es el de obtener los eventos, desde el ambiente en el que opera; es decir, viene a ser los sensores que al detectar algo fuera de lo común generan datos para el resto de las cajas del sistema (Mira).
- **Caja A-Analizadores de Eventos:** recibe el evento y realiza un análisis; como por ejemplo correlaciona eventos para determinar alguna relación, examina patrones para determinar un uso indebido, etc.
- **Caja D- Base de Datos de Eventos:** son los encargados de almacenar los eventos, dándoles persistencia de ser necesario; sobre todo cuando se necesite para un análisis posterior de pistas.
- **Caja R-Unidades de Respuesta:** son las encargadas de ejecutar una acción de acuerdo al comportamiento de los otros componentes o cajas; como por ejemplo detener procesos, alterar archivos de permisos, resetear conexiones, etc.

[21] **Framework:** en español marco de trabajo corresponde a un conjunto de estandarizado de conceptos, prácticas y criterios enfocados a resolver un problema.

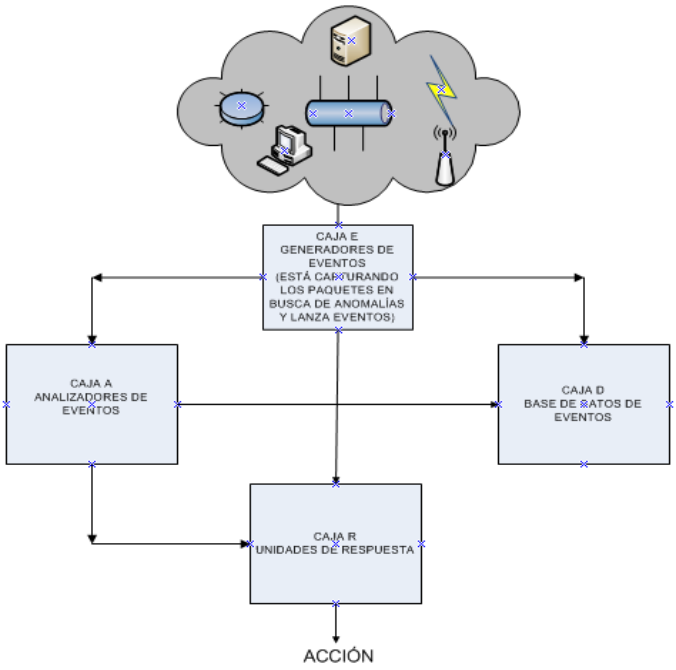


Figura 14. Modelo de Arquitectura de CIDF

Elaborado por: Autora del Proyecto

Pero como se puede observar es muy poca información; para lograr un análisis profundo de sucesos.

b. IDWG (Intrusion Detection Working Group)

La IETF crea el grupo IDWG con el afán de definir un formato de intercambio de detección de intrusos, para que los distintos sistemas puedan compartir información relevante. Según la IETF los resultados del grupo son:

- "Un documento de requerimientos, en el cual se describen los requerimientos de comunicación entre los sistemas de detección de intrusos y con sus sistemas de administración".
- "Especificación de un lenguaje común de intrusión; que describe los formatos de los datos, satisfaciendo los requerimientos".

- “Una estructura de trabajo que identifique los mejores protocolos que se pueden usar para la comunicación entre los IDSs y que defina como se mapean en éstos lo formatos de datos”.

Los resultados que se han obtenido aún están en estado borrador, como por ejemplo RFC 3620 “The Tunnel Profile”, RFC 4765 “The Intrusion Detection Message Exchange Format (IDMEF)”, RFC 4766 “Intrusion Detection Message Exchange Requirements”.

El modelo de RFC 4766, que se muestra en la figura 15 indica básicamente los elementos básicos que posee un IDS, destacando que el elemento analizador tendrá su propia estructura dependiendo del tipo de análisis que realice, además en algunos sistemas; varios de estos elementos se fusionan en un solo módulo.

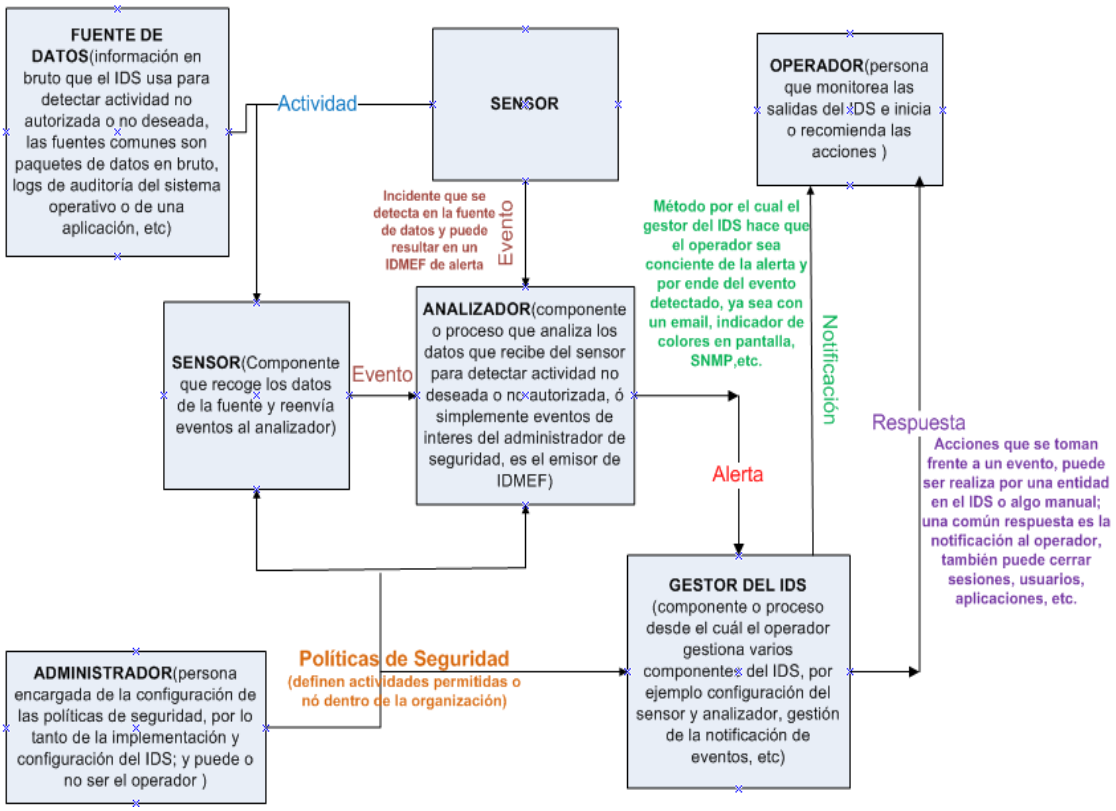


Figura 15. Componentes del IDS definidos según el RFC 4766
Fuente: (IEFT org, 2007)

3.3. Funciones del IDS

El IDS es un elemento que viene a complementar y fortalecer una estructura de seguridad de una organización, aunque algunos considerarían que es suficiente con un eficiente firewall u otros equipos, se hace necesario porque en la actualidad existen ataques que logran evadir los mismos, ó simplemente ocurren dentro de la misma organización.

Para que un IDS cumpla con sus funciones, muy aparte del software y/o hardware a usarse; se debe tener claramente definido en la organización sus políticas de seguridad; porque un IDS por defecto podría detectar actividades

legítimas como falsos positivos. Cómo podría el sistema alarmar sobre comportamiento no deseado si ni siquiera tiene definido qué lo es; aunque los mismos sistemas ayudan con esta tarea al administrador de red. Luego de una implementación y configuración adecuadas un IDS puede cumplir las siguientes funciones:

a. **Es una herramienta que ayuda en la determinación del diseño de la arquitectura y políticas de seguridad:** puesto que tras un previo análisis se podrá tener una visión mucho más clara de la situación en el sistema informático, las vulnerabilidades en los equipos y software del que se están aprovechando; para así poder tomar las medidas pertinentes, en cuanto a una implementación de seguridad e implementar nuevas políticas que se hayan pasado por alto.

b. **Realizar un control de calidad de las implementaciones de seguridad:** si ya se implemento una solución tecnológica, es de suma importancia que se evalúe su eficacia, con un IDS se observará si persisten las acciones anómalas que llevaron a esa adquisición.

c. **Determinar comportamientos en el sistema informático:** mediante las funciones estadísticas del módulo de análisis de un IDS se puede llegar a identificar valores mediante los cuales el comportamiento se considera normal, si existen variaciones quedará al descubierto que algo se está saliendo de lo establecido.

d. **Proporciona alerta al administrador:** poniéndole a su consideración los eventos que pueden afectar la disponibilidad, confidencialidad e integridad

de la información. Destacando los sistemas en tiempo real que permiten al administrador estar a tiempo para ejecutar acciones que logren salvar de las intrusiones, como por ejemplo sacar respaldos de información antes de que un ataque causa algún daño en la misma. Incluso algunos IDS poseen acciones mucho más proactivas como cierre de sesiones, modificación de accesos, etc; así nacen los sistemas IPS (Sistemas de Prevención de Intrusos).

e. Permite monitorear ataques conocidos y aprender de los nuevos: parecería ser que un IDS no es de gran ayuda si un ataque ya se está produciendo y ahí enciende la alarma; pero mucho más allá de esto; si se trata de algo desconocido cae en la desventaja de que no pueda reconocerlo si comparo con ataques conocidos, pero lejos de esto se puede automatizar el aprendizaje de nuevos patrones de ataque (que modifican ciertas partes de los conocidos), gracias a las herramientas estadísticas y análisis de tráfico anómalo. Los encargados de la seguridad tras un análisis pueden determinar nuevos patrones y actualizar la base de datos, por lo tanto un IDS es el arma de aprendizaje que permite ilustrar sobre ataques conocidos y descubrir nuevos.

f. Realizar un rastreo y análisis forense: con la información adquirida se puede realizar el rastreo del origen del ataque, sobre todo para tomar las medidas y sanciones necesarias, por esta razón son ampliamente utilizados en análisis forenses.

3.4. Desventajas en un IDS

Si bien existen varias razones por las cuáles un IDS es un sistema muy útil, existen sus desventajas:

a. Si un atacante ha conseguido el usuario y/o contraseñas de un usuario legítimo, podrá acceder al sistema y realizar las actividades a las que tiene acceso el atacado sin que el IDS pueda detectarlo; porque determina como legítimo el usuario y su comportamiento, salvo se registre otras acciones extrañas.

b. En una comunicación cifrada, no puede reconocer que se produce un ataque.

c. No puede automatizar la investigación de incidentes; pues se hace necesario un analista que defina si existe o no un nuevo patrón de comportamiento de un ataque.

d. No puede compensar malas configuraciones, con protocolos inseguros como Telnet, en el que puede existir robo de contraseñas, ó debilidades en los distintos niveles de protocolos, de los cuáles se aprovechan algunos atacantes mucho más profesionales, y realizan ataques a medida, que no podrán ser identificados por el IDS porque es desconocido para él.

3.5. Tipos de IDS

Muchos autores clasifican a los IDS de distintas maneras, ya sea sólo por su técnica de análisis, por su objetivo de análisis, etc, en la tabla 22 (Salinas, 2005), agrupa los tipos de clasificación posibles de los IDS:

Tabla 22. Posibles clasificaciones de los sistemas de Detección de Intrusos

Modo de análisis	Detección de usos indebidos	
	Detección de anomalías	
	Híbridos	
Tipo de sensores	De Red ó NIDS (WIDS)	
	De Máquina ó HIDS	Sistema Operativo De Aplicación Hardware
Tiempo de ejecución	Periódicos	
	De tiempo real	
Tiempo de Respuesta	Activos	
	Pasivos	
Arquitectura	Centralizados	
	Distribuidos	

Fuente: (Salinas, 2005)

3.5.1. Modo de análisis

Un evento puede ser analizado con los dos tipos de técnicas a continuación:

a. Detección de usos indebidos

Mediante esta técnica el tráfico se va comparando con una firma, que es una secuencia descriptiva de lo que ocurre cuando un ataque está en progreso; si resulta igual entonces se emite la alarma o acción pertinente. Las firmas son generadas por organizaciones como el CERT (Leading Computer Emergency Response Team), que realizan el trabajo de investigar los ataques y describirlos en la firma (para ello hacen uso de un lenguaje o modelo mediante el cual representar las técnicas utilizadas por los atacantes); es así que si desea un óptimo funcionamiento para este tipo de análisis se necesita tener actualizada la base de datos de firmas, porque lo que es desconocido simplemente pasará

desapercibido. Con este tipo de técnicas se genera pocos falsos positivos, pero existirán varios falsos negativos.

b. Detección de Anomalías

Se basa en la comparación del comportamiento que se ha definido como normal y el actual, cualquier variación que existe se define como una intrusión. El comportamiento normal o también llamado perfil se logra detallar después de colocar el sistema en las condiciones que se consideran comunes de operación; tras un determinado tiempo, almacenar la información en los registros de un historial que al ser revisado permitan determinar lo “normal”; es por esta razón que se debe definir un tiempo considerable y una calidad óptima en el aprendizaje; porque un aprendizaje muy general puede llevar a muchos falsos negativos ó un aprendizaje muy restringido puede llevar a muchos falsos positivos (Giménez, 2008).

El tráfico no es siempre estático en la red, claro que existirá ciertos valores que podrán ser definidos como número de intentos de acceso, porcentajes de procesamiento del CPU, etc. Por otro lado esta forma de análisis me permitirá observar acciones desconocidas que pueden llegar a ser ataques nuevos, e incluso ser una herramienta muy útil en la investigación de nuevas firmas para la base del análisis de uso indebido.

Existen distintas técnicas para que el comportamiento aprendido sea lo más óptimo para la detección de intrusiones, desde el hecho de definir perfiles de usuario, red; entre otros, se usan tanto técnicas estadísticas, como de prueba y error.

Una novedosa forma de detección de anomalías son las **redes neuronales**, que se basan en el aprendizaje que se logra a través de sus "unidades", que son elementos de procesamiento simple que tienen conexiones entre sí con peso, en analogía con nuestras neuronas cerebrales. En el proceso de aprendizaje se intercambia información a través de las conexiones priorizando la información de las unidades con mayor peso, se cambia pesos, y aumenta o disminuye conexiones.

También existen el método de detección de **sistema inmune**, que basa su técnica en el comportamiento de nuestro sistema inmunológico, determinar que es propio del sistema y todo lo ajeno como intrusión, con la operación de agentes T denominados así por los linfocitos T de nuestro cuerpo; en fin existen varias novedosas formas en el que se desea determinar lo normal y que viene a ser la intrusión.

c. Híbridos

Tanto en el análisis de detección de uso indebido y de anomalías; existen ventajas y desventajas, varios IDSs se complementan con ambas técnicas, si se produce un ataque conocido la comparación con firmas será enormemente eficaz, ó si es desconocido el comportamiento extraño puede ser detectado gracias al análisis de anomalías.

3.5.2. Tipo de sensores

a. De Red o NIDS

Los sistemas de detección de intrusos de red censan a través de una interfaz el medio de red, por lo general ésta se encuentra en modo promiscuo por el cual monitoriza el tráfico que existe, para ello se ubica en el segmento

deseado. Algunos NIDSs van más allá de ser sólo software, poseen hardware especializado con varias interfaces que le permiten ubicarse en varios segmentos de red, extendiendo más la vigilancia.

El NIDS debe poseer una clara visión del comportamiento de la red, porque está tratando con algunos o varios sistemas interconectados. Aunque por lo general los suelen ubicar en puntos estratégicos que complementen la seguridad con otros dispositivos como firewalls. Para su óptima operación necesita de un buen hardware con el que se pueda realizar un procesamiento rápido, así evitar que el NIDS descarte paquetes o simplemente colapse.

Un NIDS especial que cabe recalcar es el WIDS, que básicamente ubica su sensor inalámbrico en modo monitor para ubicarse en el medio inalámbrico a detectar intrusos.

- **WIDS**

En una WLAN puede ser mucho más complicado detectar un ataque, porque puede existir interferencia, dispersión, refracción y reflexión de la señal, que tal vez no se trate en sí de una intrusión intencionada como por ejemplo un microondas cerca del AP.

Eventos sospechosos en una WLAN

Si se ha determinado el comportamiento considerado normal en la WLAN y/o se posee una base de datos de firmas considerablemente buena, cabe el momento del WIDS entre a funcionar y busque eventos; pero estos a diferencia de una red cableada se han ensañado más en las capas inferiores del modelo OSI, como se ha mencionado en los ataques a las redes inalámbricas, a

continuación una clasificación de los más comunes eventos en los que debería reaccionar un buen WIDS según (Vladimirov et al., 2005):

Eventos en la capa física (eventos de radiofrecuencia)

Esta clase de eventos pueden ser; una señal de conectividad o red, dispositivos extraños a la red, ataques de hombre en el medio y distorsiones intencionadas, como el caso de: transmisores adicionales en el área, decaimiento de la calidad de señal, canales en uso que no lo han sido antes, cambio de canal o sobrelapamiento de ellos.

Eventos de las tramas de administración y control

Pueden ser el indicio de errores en la configuración de la red, problemas de conectividad, ataques de DoS u hombre en el medio en la capa de enlace de datos, wardrivers en el área que usan herramientas de barrido, MAC spoofing, etc. Por ejemplo: tramas que tienen modificado alguno de sus campos, frecuentes beacons, tramas con direcciones MAC duplicadas o no incluidas dentro de la lista que el administrador ha definido como permitidas.

Eventos de tramas 802.1x/EAP

Están enfocados en quebrantar la seguridad de la autenticación 802.1x, a través de ataques de fuerza bruta, AP intruso, DoS que deshabilite la autenticación, ó también pueden ser resultado de interferencias de radiofrecuencia u otros problemas de la capa física. Ejemplos de esta clase de eventos son: tramas 802.1x incompletas, corrompidas o mal formadas, avalanchas de tramas EAP (petición, respuesta, fallo, start, logoff, desafío), tramas EAP con tamaños inusuales, procesos de autenticación a medias.

Eventos relacionados con WEP

Estos eventos corresponden a la explotación de las vulnerabilidades del protocolo WEP, como por ejemplo: tráfico sin cifrar, tráfico cifrado con claves WEP desconocidas, de longitudes distintas, IV débiles, ausencia de cambios en el IV.

Eventos de conectividad general y de flujo de tráfico

Son eventos en los que se debe profundizar una investigación y determinar las causas del mismo, como el caso de: pérdida de conectividad, variaciones abruptas en el ancho de banda consumido, aumento de fragmentación de paquetes, retransmisiones frecuentes.

Eventos Varios

Esta clase puede ser consecuencia de ataques con o sin éxito, configuraciones defectuosas, uso de herramientas de inyección de tráfico, denegación de servicio de un AP por exceso de conexiones, aunque cualquier corrupción en las tramas ya son una señal de que algo anda mal en la capa física, ejemplo de estos eventos: máquinas no autenticadas pero que están asociadas, tramas con MIC corrompidos, avalancha de esfuerzos de asociación a la red.

b. De Host o HIDS

Es un IDS mucho más específico que se ubica en un equipo, en el cual analiza a profundidad, todos los eventos que en él se produce; tiene acceso a eventos que ni siquiera se observan en la red y son desapercibidos por los NIDS, como eventos en hardware, sistema operativo, memoria, e incluso observar la información en una comunicación cifrada (SSH, SSL) porque puede

apreciar la información antes de que sea cifrada en la fuente y descifrada en el destino; lo que da una mejor apreciación frente a un posible ataque. Existen algunas clases de HIDS:

c. HIDS de aplicación: se enfocan principalmente en el análisis de una aplicación, en el flujo de información que normalmente debería tener, como el caso de un servidor web, el HIDS sabrá monitorear lo que se considera un comportamiento normal desde el inicio a fin de una conexión con un cliente web.

d. HIDS de Sistema Operativo: monitorea en busca de eventos en el sistema operativo (acceso a ficheros, procesos desconocidos, etc), que indican al administrador la necesidad de actualizaciones o parches necesarios.

3.5.3. Tiempo de Ejecución

a. Periódicos o "Batch Mode"

El IDS realiza un análisis por bancos de datos recolectados, lo que representa mayor cantidad de tiempo en dar una respuesta. En la actualidad la prioridad está en detener a tiempo una intrusión por ello aparece el análisis en tiempo real.

b. Tiempo Real

Es un análisis rápido de la información de la fuente de datos, que permite con un mínimo retardo generar alarmas, en tanto detecta la intrusión.

3.5.4. Tiempo de Respuesta

a. Respuesta Pasiva

El IDS se limita simplemente a informar del ataque en curso que ha detectado al administrador de red, de seguridad, usuarios del sistema ó una base de firmas como un CERT.

b. Respuesta Activa

El IDS no sólo informa también está en la posibilidad de generar alguna acción adicional, como aumentar la sensibilidad del sensor y almacenar con más detalle información sobre el presunto ataque, e incluso cambiar su entorno, con un cierre de sesión, cambio de la configuración de accesos; entre otros, de ahí que nace los IPSs.

3.5.5. Arquitectura

a. Centralizados

Así comenzaron los primeros IDSs como el proyecto IDES, mediante el cual los sensores recolectan la información en un solo sistema central, lo que obviamente resulta en una degradación del rendimiento; dentro de la ubicación en la red del punto central.

b. Distribuidos(DIDS)

En este tipo de arquitectura existe varios agentes ubicados en puntos estratégicos, ya sea de red o host, incluso ambos, enviando la información a su correspondiente subsistema, luego la información que tiene relevancia se trasmite a un nodo central en el que se puede obtener una visión más amplia de

lo que ocurre en la organización. Los componentes que usa esta clase de estructura son (Giménez, 2008, pág. 18):

- Agentes que monitorizan la actividad (A).
- Transceptores que se encargan de la comunicación (T).
- Maestro/s que centralizan los datos (M).
- La consola de eventos, que es la interfaz con el operador (C)
- Otros componentes como: generadores, proxy, etc.

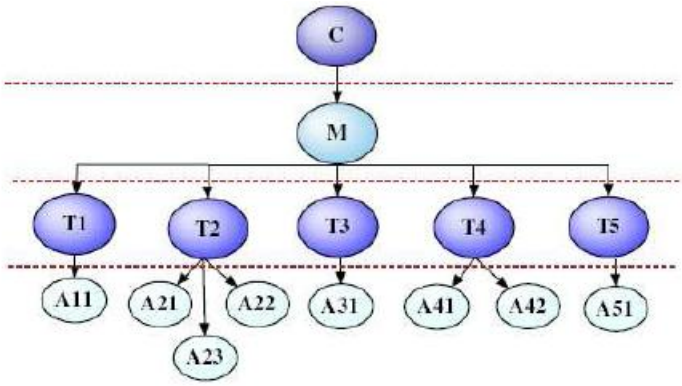


Figura 16. Esquema de un DIDS

Fuente: (Giménez, 2008)

3.6. Ubicación del IDS

La correcta ubicación de los IDSs, en conjunto con una buena configuración proporcionan gran ayuda al fortalecimiento de la seguridad en la red, colocando los HIDSs en los equipos críticos de la organización proporcionan un favorable complemento a los NIDSs colocados en los puntos estratégicos de la red; sobre todo por el hecho que no detecta ataques en las comunicaciones cifradas. En la figura 17 se puede observar las distintas ubicaciones que puede tomar un IDS.

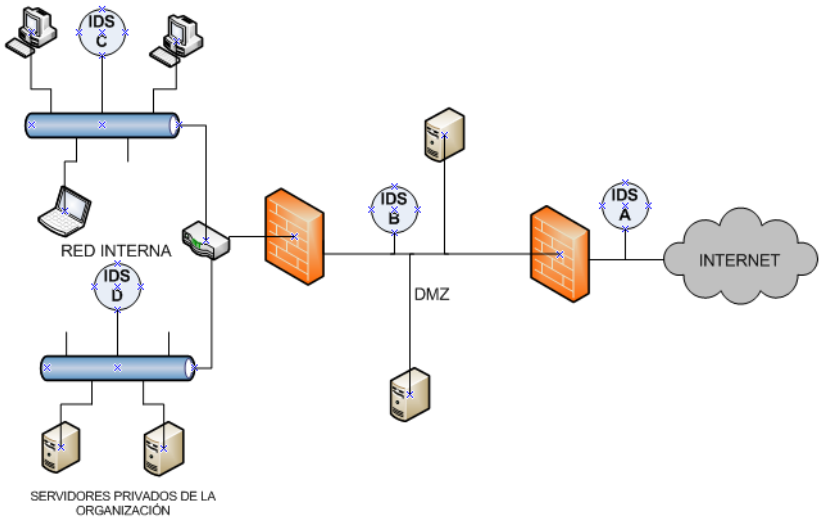


Figura 17. Posibles ubicaciones del NIDS

Elaborado por: Autora del Proyecto

3.6.1. Delante del Firewall que conecta a la organización con el Internet-IDS A

En esta ubicación existe una gran cantidad de tráfico pues en esta zona entra y sale todo el tráfico de la red, hacia el exterior (internet), es por esta razón que se necesita un IDS con un hardware que permita soportar todo este flujo, evitando que descarte información o simplemente deje inoperativo el sistema.

En esta zona el IDS permite apreciar el entorno, porque se observa los ataques que está recibiendo del exterior; por lo que en este punto, sirve como una herramienta que permite observar cómo se debe seguir armando la estructura de seguridad conforme lo que está ocurriendo en la actualidad en su ambiente.

Por otra parte, el sensor debe ser menos sensible para evitar gran cantidad de falsos positivos y logs que saturen el sistema, por la enorme carga de tráfico presente.

3.6.2. Detrás del firewall conectado a internet ó en la zona desmilitarizada (DMZ) - IDS B.

En este punto estratégico el IDS tiene la función principal de monitorear el tráfico que ha ingresado a la red de la organización tras pasar las políticas de filtrado del firewall, lo que permite observar las falencias de seguridad en el mismo; como políticas de seguridad mal implementadas y/o faltantes.

En esta zona existe gran cantidad de tráfico, claro está que mucho menos en comparación con el caso anterior, por el filtrado; pero aun así es necesario un IDS con hardware que soporte la carga de monitoreo, adicional con sensores mucho más sensibles que el análisis en la zona de internet, para tener un mejor soporte frente a los ataques que comprometan los servidores ahí conectados; que aunque posean menor seguridad en comparación con la red interna, siguen siendo de gran importancia para la organización.

3.6.3. En la red o subred Interna-IDS C.

La función del IDS en este punto radica en el análisis del tráfico interno en busca de ataques que han tenido como origen los propios usuarios legítimos, o simplemente un ataque externo ha logrado su objetivo y el acceso a la red interna, un ataque en esta zona es de carácter hostil, por ello el sensor debe ser

muy sensible, un mínimo aviso debe ser arduamente analizado y de ser el caso corregir cualquier novedad.

3.6.4. En la subred de servidores privados de la organización- IDS D.

Este es una ubicación especial de un IDS pues trata con la seguridad de los servidores delicados y de suma importancia en la organización; como es el caso de una base de datos.

3.7. SNORT

Según su página oficial (Sourcefire Team, 2013) a Snort lo definen como "un sistema de detección y prevención de intrusos de red (IDS/IPS) desarrollado por Sourcefire. Combinando los beneficios de la inspección basada en firmas, protocolo y anomalías, Snort es la tecnología IDS/IPS más ampliamente desplegada en el mundo. Con millones de descargas y cerca de 400000 usuarios registrados".

El equipo desarrollador Sourcefire fue fundado en el 2001 por Martin Roesch; quien fue el creador de Snort, en la actualidad es el director tecnológico del grupo. En un comienzo Roesch desarrolla en Linux el programa APE, que carecía de compatibilidad con otros sistemas operativos, un mes después (Diciembre de 1998), lanza la primera versión de Snort; que trabajaba simplemente como un sniffer, careciendo de características propias de un IDS, pero con una mejor portabilidad gracias a la inclusión de la librería libpcap[22].

[22] **Libpcap:** es una interfaz de programación de aplicaciones API para capturar tráfico de red.

Cabe destacar que Snort es de código abierto y se distribuye con Licencia Pública General (GPL); es gratuito y compatible con sistemas operativos como OSX[23], Windows, Centos, etc.

Snort es un sistema muy flexible, adaptable al entorno, configurable; es por esto que con conocimientos básicos de red y un buen manual se puede llegar a explotar enormemente sus características. Se puede configurar para que trabaje en tres modos:

- **Sniffer:** lee los paquetes de la red y los despliega en la consola.
- **Registro de paquetes:** se encuentra almacenando registros "logs" de paquetes en el disco.
- **NIDS:** realiza detección y análisis del tráfico, es su modo más complejo y configurable.

En su modo NIDS, puede trabajar en distintos modos que se pueden seleccionar y que se detallan en la tabla 23.

Tabla 23. Modos de operación de Snort como NIDS

Opción	*Descripción*
-A fast	Modo de alerta rápida. Escribe la alerta en un simple formato con una marca de tiempo, mensaje de alerta, fuente y destino IP/puertos.
-A full	Modo de alerta Full. Este es el modo de alerta por defecto y será usado automáticamente si no especifica un modo.
-A unsock	Envía alertas a UNIX socket que otro programa puede oír.
-A none	Apaga las alertas
-A console	Envía alertas de estilo rápido a la consola (pantalla).
-A cmg	Genera alertas de tipo cmg, despliega en pantalla la alerta en estilo full, pero se usa sólo en pruebas porque no guarda registros.

Elaborado por: Autora del Proyecto

[23] **OSX:** sistemas operativos basados en Unix, desarrollados y vendidos por Apple Inc.

3.7.1. Elementos del Sistema

Para el desarrollo de este trabajo interesa su modo de configuración NIDS, el cual consta de las siguientes partes:

a. Módulo de adquisición de datos.

Como se mencionó anteriormente Snort hace uso de una librería externa denominada libpcap para capturar el tráfico, pero a partir de la versión 2.9 (Roesch, Gree, & Sourcefire, 2013), se ha introducido la librería de Adquisición de Datos DAQ para los paquetes entrantes y salientes, que permite reemplazar las llamadas directas de las funciones de libpcap por una capa de abstracción (manera de ocultar los detalles de implementación de las funcionalidades), para poder trabajar independientemente del hardware y software, evitando cualquier cambio en Snort.

Existen otros métodos además de la libpcap para la captura de paquetes, en una tarjeta de red en modo promiscuo como el Filtro de Paquetes Berkeley BPF, que es una arquitectura diseñada para la captura de paquetes desarrollada por el Lawrence Berkeley National Laboratory, que proporciona una interfaz en bruto para la capa de enlace de datos.

b. Decodificador.

Este elemento de Snort consta de varios decodificadores que están organizados según las capas de los protocolos. Por lo tanto existen decodificadores de enlace de datos, decodificador de protocolos de red, así sucesivamente como se puede apreciar en la figura 18.

Una vez que se ha hecho la captura a través de libpcap, ingresa a los decodificadores que analizarán los elementos de cada protocolo que tenga introducido, almacenando así en una estructura de datos que será analizada por los preprocesadores y el motor de detección.

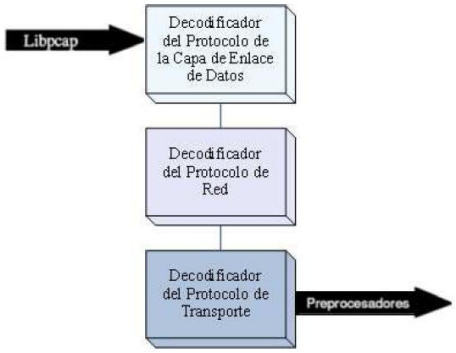


Figura 18. Flujo de datos del decodificador

Fuente: (Giménez, 2008)

c. Preprocesadores.

Estos componentes fueron introducidos a partir de la versión 1.5 y corresponden a programas encargados de tomar la información; que ha sido previamente decodificada e interpretarla dándole forma para que así pueda ser aplicada una regla que determine alguna intrusión en el motor de detección.

Los preprocesadores permiten introducir en Snort la funcionalidad de extenderse gracias a los usuarios y programadores que introducen interesantes y muy útiles módulos, incluso modificarlos; aunque una gran cantidad de módulos desencadena lentitud de procesamiento.

En la tabla 24 se muestra preprocesadores existentes con su respectiva función.

Tabla 24. Preprocesadores de Snort 2.9.5

Preprocesador	*Función*
Frag3	Tiene un módulo enfocado en la desfragmentación IP, para evitar la evasión del IDS y una rápida ejecución con poca complejidad en la gestión de datos.
Stream5	Está basado en un módulo de re ensamblaje de sesiones, es decir hace un seguimiento de las sesiones tanto para TCP como UDP.
sfPortscan	Está diseñado para detectar la primera fase de un ataque de reconocimiento (determinar protocolos y servicios del atacado).
RPC Decode	Permite normalizar múltiples registros Remote Procedure Call (RPC) fragmentados en un único registro.
Performance Monitor	Mide el desempeño máximo teórico de Snort con su desempeño en tiempo real.
HTTP Inspect	Es un decodificador HTTP de aplicaciones de usuario, que decodifica datos de un buffer[24] dado y normaliza los campos tanto en solicitudes del cliente y respuestas del servidor.
SMTP	Decodifica el buffer en búsqueda de comandos y respuestas SMTP, además se encarga de los procesos con y sin estado de este protocolo.
POP	Se encarga de decodificar el buffer en búsqueda de comandos y respuestas del protocolo POP3 y manejar los procesos con estado del mismo.
IMAP	Decodifica el buffer en busca de comandos y respuestas IMAP4, maneja los procesos con estado de este protocolo.
FTP/Telnet	Provee la capacidad de inspección con estado de los flujos de datos de FTP y Telnet.
SSH	Detecta las vulnerabilidades como: desbordamiento del buffer desafío-respuesta, CRC32, Seguridad CRT (certificados) y vulnerabilidades propias del protocolo.
DNS	Decodifica respuestas DNS y puede detectar desbordamiento de solicitudes DNS del cliente, tipos de registros obsoletos o experimentales.
SSL/TLS	Es un preprocesador dinámico que decodifica el tráfico SSL y TLS, adicionalmente puede determinar si debe parar el mismo.
ARP Spoof	Decodifica paquetes ARP y detecta ataques ARP, solicitudes unicast ARP, e inconsistencias en la tabla ARP.
DCE/RPC 2	Analiza el tráfico del protocolo Server Message Block que se usa para la compartición de carpetas y archivos en Windows.
Sensitive Data	Detecta y filtra información de identificación personal como números de tarjeta de crédito, dirección de correo electrónico, etc.
Normalizer	Normaliza los paquetes para ayudar a disminuir las oportunidades de evasión, esto se usa cuando Snort trabaja como IPS.
SIP	Analiza el tráfico del protocolo de inicio de sesión SIP, utilizado en llamadas en internet, distribución multimedia y conferencias multimedia.
Reputation	Permite bloquear, descartar ó permitir el tráfico dependiendo de una lista de direcciones IP.
GTP	Analiza los posibles intentos de intrusión en las redes a través de las redes de teléfonos móviles que usan GPRS; es decir análisis del tráfico del protocolo de túnel GPRS.
Modbus	Decodifica el protocolo Modbus, que se usa en la comunicación con equipos que usan controladores lógicos programables “PLC”.
DNP3	Analiza el tráfico usado en comunicaciones que usan el protocolo de red distribuido DNP, que utilizan equipos inteligentes y controladoras.

Elaborado por: Autora del Proyecto

[24] **Buffer:** ubicación en memoria reservada para almacenamiento temporal donde los datos esperan ser procesados.

d. Motor de Detección.

Es un componente muy importante de Snort, se encarga del análisis de reglas y detección de firmas, una vez que los paquetes ingresan a este módulo los compara con las reglas que se encuentran almacenadas en el archivo de configuración snort.conf, si encuentra una intrusión envía al módulo de salida; caso contrario se descartan los paquetes.

Snort usa un lenguaje simple, muy liviano, flexible para describir las reglas que constan de dos partes:

- **El encabezado de la regla:** contiene la acción de la regla, dirección IP origen, IP destino, puertos origen y destino, protocolos, máscaras de red. Las acciones por defecto de Snort como NIDS son alertar, registrar, pasar el paquete, activar (alertar y prender una regla dinámica) y dinámico; este último consiste en mantenerse inactivo hasta que una regla lo active y actúa como regla de registro.
- **Las opciones de la regla:** contiene mensajes de alerta y determinar en qué parte del paquete se debe examinar para tomar la acción de la regla.

El análisis de las reglas anteriormente se realizaba en un análisis de lista de enlazado 3D, este era un algoritmo de almacenamiento mediante el cual se almacenaban las reglas de Snort y sus opciones. Se buscaba una coincidencia con la lista enlazada de encabezado de regla llamado también Rule Tree Node (RTN), encontrada esta coincidencia se buscaba dentro de la RTN una

coincidencia con un patrón ó usando algún plugin[25] de detección denominado Opt Tree Node (OTN); es decir, las OTN son un conjunto de funciones que el motor de detección debe comprobar para disparar la alarma.

Pero con este tipo de análisis Snort era muy lento en procesar, ahora el motor de Snort agrupa las reglas por protocolo, luego por puertos, después por aquellas que tienen contenido y no lo tienen. Para las reglas con contenido usa un comparador multipatrón que selecciona las reglas que tienen oportunidad de coincidir, basado en un contenido singular. La selección de reglas para evaluar con este comparador incrementa el rendimiento, en especial cuando se trata con grupos de reglas grandes (Roesch et al., 2013).

e. Módulos de Salida

Estos módulos ó también llamados plugins fueron introducidos desde la versión 1.6 de Snort, ya que ofrecían mayor flexibilidad al momento de mostrar las salidas al usuario, tanto en formato como presentación. Estos son los encargados de generar las salidas dependiendo de lo que necesiten los subsistemas de registro y alerta de Snort, después que los paquetes han pasado por los preprocesadores y motor de detección.

Existen distintos módulos de salida que se pueden usar según lo que se necesite como se puede apreciar en la tabla 25 (Roesch et al., 2013):

[25] **Plugin:** módulo de hardware o software que añade una característica o servicio a un sistema más grande.

Tabla 25. Módulos de Salida de Snort

Módulo de Salida	Funcionamiento
alert-syslog	Este es un módulo que envía alertas al syslog[26], el usuario puede definir facilidades de registro así como prioridad en el archivo de configuración de Snort.
Alert-fast	Imprime alertas en formato de una línea, evitando las cabeceras de los paquetes porque sólo registra en un solo archivo.
Alert-unixsock:	Configura un socket en Unix que envía alertas; así otros programas o procesos externos pueden recibir de Snort sus alertas.
Log-tcpdump	Registra los paquetes en un formato tcpdump, de modo que pueda ser analizado posteriormente por otras herramientas que usen este formato.
Csv:	Los datos de alerta se generan en un formato que se puede importar a una base de datos; además se puede personalizar los campos y orden de la salida.
unified 2:	Este módulo puede trabajar en uno de tres modos que son: registro de paquetes, registro de alertas o registro unificado, este último unifica los dos tipos anteriores de registros en uno solo.
log null	Se introdujo desde Snort versión 1.8.2, genera alertas pero no causa entradas en el registro de paquetes.
log limits	Este módulo entra en acción cuando un determinado módulo ha excedido su límite especificado de registros; abriendo uno nuevo con marca de tiempo UNIX añadido al nombre del registro configurado.

Elaborado por: Autora del Proyecto

3.7.2. Instalación

Para la instalación tanto de Snort como Kismet se utilizará una máquina virtual con las siguientes características:

- Disco duro de 40 Gb
- 1500 Mb de RAM
- 1 Procesador
- Sistema Operativo Ubuntu 12.0.4 64 bits

[26] **Syslog:** aplicación o biblioteca que registra eventos de un sistema.

Procedimiento

1. Se debe cumplir con la instalación de requerimientos previos para el correcto funcionamiento de la herramienta, en la tabla 26. se detalla los paquetes y librerías necesarios; así como los comandos para proceder a su instalación, asumiendo que se encuentra como usuario privilegiado root.

Tabla 26. Librerías y paquetes necesarios para instalar Snort

Paquetes	Descripción	Comandos
nmap	Programa que sirve para realizar rastreo de puertos.	**# apt-get install nmap**
nbtscan	Escáner del servidor de nombres NetBIOS.	**# apt-get install nbtscan**
apache2	Servidor de páginas web.	**# apt-get install apache2**
php5	PHP es un lenguaje de secuencias de comandos del servidor, y es una herramienta para hacer páginas web.	**# apt-get install php5**
Php5-mysql	Proporciona los módulos para las conexiones de base de datos MySQL directamente desde scripts[27] PHP.	**# apt-get install php5-mysql**
Php5-gd	Librería gráfica gd para PHP.	**# apt-get install php5-gd**
Libpcap0.8-dev	API[28] de captura de tráfico.	**# apt-get install libpcap0.8-dev**
Libpcre3-dev	Librería de Expresiones Regulares Compatibles con Perl (PCRE).	**# apt-get install libpcre3-dev**
G++	Conjunto de compiladores de C++.	**# apt-get install g++**
Bison	Programa generador de analizadores sintácticos.	**# apt-get install bison**
Flex	Conjunto de librerías para el desarrollo de una interfaz gráfica.	**# apt-get install flex**
Libpcap-ruby	Proporciona una interfaz ruby (lenguaje de programación orientado a objetos) para libpcap.	**# apt-get install libpcap-ruby**
Make	Herramienta para dirigir la compilación.	**# apt-get install make**
Autoconf	Constructor automatizado de guiones de configuración (configure.in).	**# apt-get install autoconf**
Libtool	Herramienta de programación	**# apt-get install libtool**

[27] **Script:** programa simple escrito en texto plano.
[28] **API:** Interfaz de programación de aplicaciones.

CONTINUA=>

	GNU para crear bibliotecas de software portable.	
Mysql-server	Servidor de MySQL (base de datos de lenguaje de preguntas estructurado).	**# apt-get install mysql-server #colocar la clave del servidor, tenerla en cuenta para todo el proceso de instalación de Snort.**
Libmysqlclient -dev	Archivos de desarrollo de base de datos MySQL.	**# apt-get install libmysqlclient-dev**
DAQ	API de adquisición de datos que necesita Snort desde la versión 2.9.	Descargar DAQ de http://www.snort.org/start/requirements, se ingresa a la ubicación donde se guardó y se procede: **# tar zxvf daq-2.0.1.tar.gz** **# cd daq-2.0.1** **#./configure** **# make** **# make install**
libdnet	API genérico de red que provee acceso a distintos protocolos.	Descargar de la página https://libdnet.googlecode.com/files/libdnet-1.12.tgz, se ingresa en la ubicación guardada: **# tar zxvf libdnet-1.12.tgz** **# cd libdnet-1.12** **# ./configure** **# make** **# make install** **# ln –s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1**

Elaborado por: Autora del Proyecto

2. Actualizar el sistema operativo con los últimos parches de seguridad y reiniciar el PC.

   # *apt-get update*

   #*apt-get upgrade*

3. Para un despliegue de reportes se descarga y añade plugins; primero jpgraph que contiene librerías gráficas para una gráfica circular en la página principal de los reportes, luego snortreport-1.3.4 que generará los reportes.

   # wget http://hem.bredband.net/jpgraph/jpgraph-1.27.1.tar.gz

   # mkdir /var/www/jpgraph

tar zxvf jpgraph-1.27.1.tar.gz

cp –r jpgraph-1.27.1/src /var/www/jpgraph/

Ahora se descarga desde http://www.symmetrixtech.com, se ingresa al directorio de descarga, se descomprime y por último se configura el plugin snortreport a través de su archivo srconf.php figura 19 (UbK2013 es la clave del servidor MySQL).

 # tar zxvf snortreport-1.3.4.tar.gz –C /var/www/

 # gedit /var/www/snortreport-1.3.4/srconf.php

Se cambia $ pass= “YOURPASS”; por:

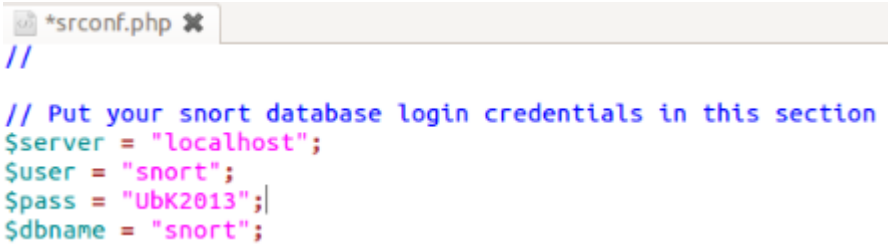


Figura 19. Archivo srconf.php modificado

Elaborado por: Autora del Proyecto

4. En la página web de Snort figura 20, se encuentra un botón de descarga de Snort que redirige a http://www.snort.org/snort-downloads donde se encuentra la última versión de Snort, al momento de este trabajo se encuentra en la 2.9.5.6; figura 21.

Figura 20. Botón de Descarga en la página oficial de Snort

Elaborado por: Autora del Proyecto

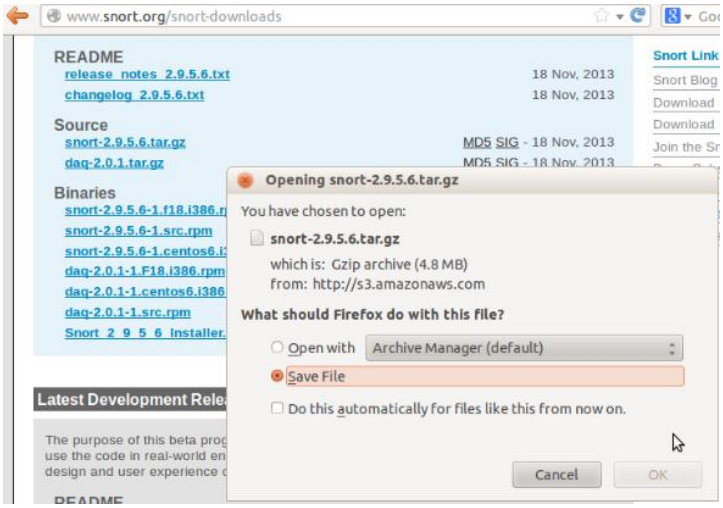


Figura 21. Descarga de Snort 2.9.5.6

Elaborado por: Autora del Proyecto

5. Se procede a la instalación con los siguientes comandos:

 # cd "Se ingresa al directorio donde se almacenó la descarga"

 # tar zxvf snort-2.9.5.6.tar.gz

 # cd snort-2.9.5.6

 # ./configure --prefix=/usr/local/snort --enable-sourcefire

 # make

 # make install

 # mkdir /var/log/snort

 # mkdir /var/snort

 # groupadd snort

 # useradd –g snort snort

 # chown snort:snort /var/log/snort

6. Se procede a descargar las reglas de Snort, igualmente en la página oficial existe el botón para redirigir a https://www.snort.org/snort-rules; aquí se encuentra tres maneras de obtener las reglas; la primera consiste en el grupo

de suscriptores que por una suma de dinero obtienen las más actuales reglas, ya sea uso personal o de empresa; el segundo obtienen las reglas como usuarios registrados a través de la página con un retardo de actualización de 30 días figura 22; por último las reglas de la comunidad que consisten en reglas gratuitas (licencia GPLv2 VRT), poseen su autor y permiten tener más actuales a los registrados. Se descarga las reglas como usuario registrado y se ejecuta los siguientes comandos una vez ingresado al directorio de la descarga:

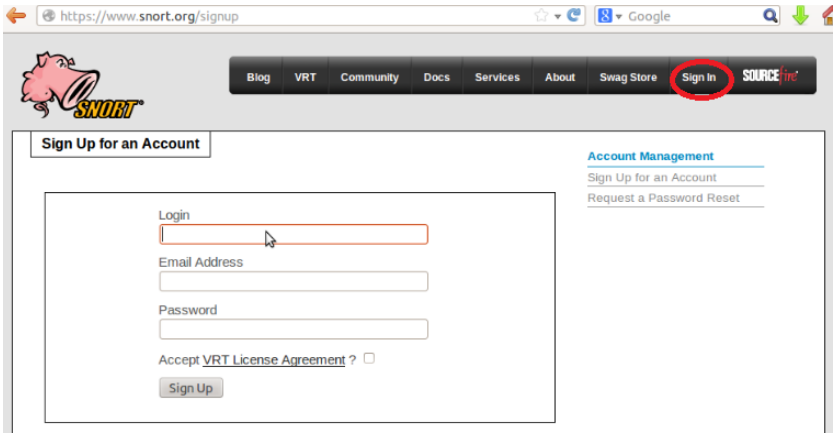


Figura 22. Formulario de registro de Snort

Elaborado por: Autora del Proyecto

 # tar zxvf snortrules-snapshot-2955.tar.gz –C /usr/local/snort

 # mkdir /usr/local/snort/lib/snort_dynamicrules

 # cp /usr/local/snort/so_rules/precompiled/Ubuntu-10-4/x86_64/2.9.5.6/ /usr/local/snort/lib/snort_dynamicrules*

 # touch /usr/local/snort/rules/white_list.rules

 # touch /usr/local/snort/rules/black_list.rules

 # ldconfig

7. Para actualizar aún más el estado de las reglas se descarga de https://www.snort.org/snort-rules, descomprimir, abrir la carpeta community-rules y copiar su contenido dentro de la carpeta rules de /usr/local/snort/rules.

3.7.3. Configuración

1. Ingresar al archivo snort.conf para colocar el directorio donde se encuentran las reglas, preprocesadores y motor de detección.

   # gedit /usr/local/snort/etc/snort.conf

   Cambiar *var WHITE_LIST_PATH ../rules*

   var BLACK_LIST_PATH ../rules

Por

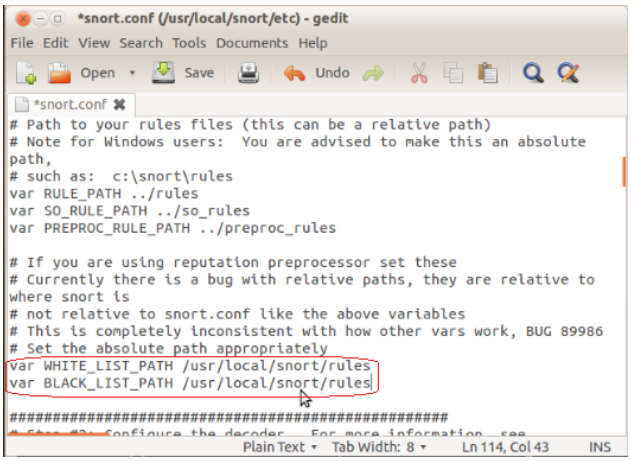


Figura 23. Edición snort.conf del directorio de reglas

Elaborado por: Autora del Proyecto

Cambiar

dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/

dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

dynamicdetection directory /usr/local/lib/snort_dynamicrules

Por

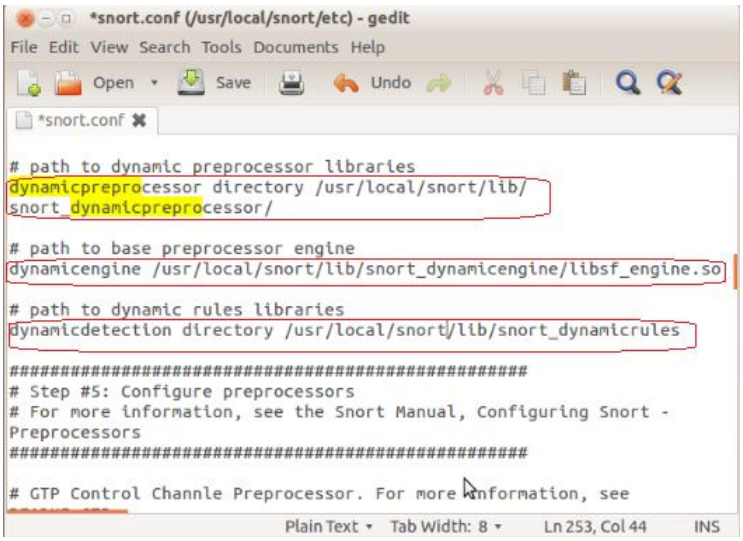


Figura 24. Edición snort.conf del directorio de preprocesadores y motor de detección

Elaborado por: Autora del Proyecto

2. Se configura la salida como unified2 porque se usará Barnyard para un mejor rendimiento de Snort, se coloca la línea encerrada en rojo bajo la línea de comando comentada encerrada en azul, figura 25.

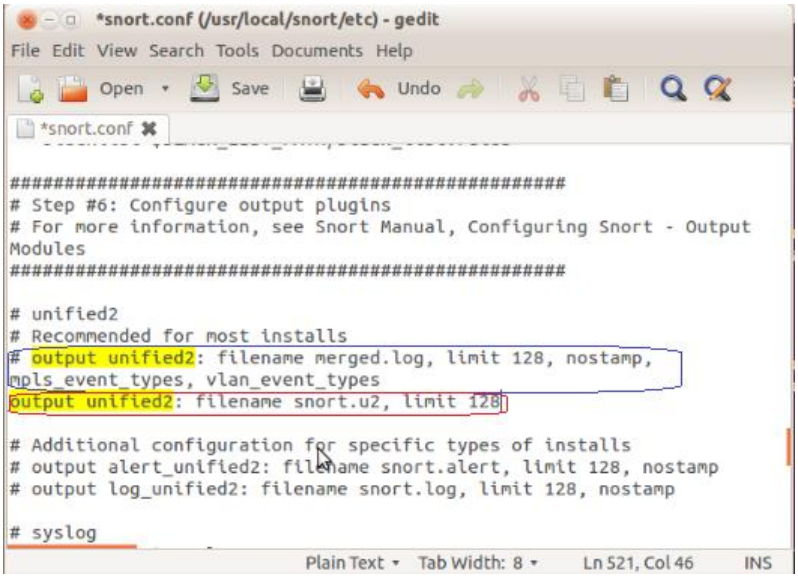


Figura 25. Configuración de salida unified2

Elaborado por: Autora del Proyecto

3. Se descarga Barnyard2 con el propósito de mejorar el rendimiento de Snort, por la disminución de carga en el motor de detección (Gullett, 2012) y se procede con los siguientes comandos para su instalación.

   # wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-1.13.tar.gz

   # tar zxvf barnyard2-1.13.tar.gz

   # barnyard2-master

   # autoreconf -fvi -I ./m4

   # ./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu

   # make

   # make install

   # cp etc/barnyard2.conf /usr/local/snort/etc

   # mkdir /var/log/barnyard2

   # chmod 666 /var/log/barnyard2

   # touch /var/log/snort/barnyard2.waldo

   # chown snort.snort /var/log/snort/barnyard2.waldo

4. Se crea la base de datos y su respectivo esquema, para manejar estas líneas de comando obviamente se pedirá ingresar la clave del servidor MySQL. El segundo comando contiene el directorio donde se encuentra el esquema, es decir dentro de la carpeta descomprimida de barnyard2.

   # echo "create database snort;" | mysql –u root –p

   # mysql –u root –p –D snort < /home/pcroot/Downloads/barnyard2-master/schemas/create_mysql

5. Se crea un usuario adicional para MySQL y evitar que el daemon[29] se encuentre como root; como medida de seguridad.

   # echo "grant create, insert, select, delete, update on snort. to snort@localhost identified by 'snort2013'" | mysql –u root –p*

   snort2013 corresponde a la clave del usuario que se está creando.

6. Se procede a editar el archivo barnyard2.conf como se indica a continuación:

   # gedit /usr/local/snort/etc/barnyard2.conf

   Cambiar

   config reference_file: /etc/snort/reference.config

   config classification_file: /etc/snort/classification.config

   config gen_file: /etc/snort/gen-msg.map

   config sid_file: /etc/snort/sid-msg.map

   # config hostname: thor

   #config interface: eth0

   #output database: log, mysql, user=root password=test dbname=db host=localhost

   Por

[29] **Daemon:** es u servicio o proceso que se inicia en segundo plano; es decir que por lo general no necesita de un usuario para su ejecución.

Figura 26. Partes de barnyard2.conf modificados

Elaborado por: Autora del Proyecto

7. Se ingresa a */etc/network/interfaces*, se cambia la configuración existente por las líneas siguientes y se reinicia los servicios de red a través de */etc/init.d/networking restart*.

   auto eth0

   iface eth0 inet manual

   ifconfig eth0 up

8. Para arrancar simplemente se digita el siguiente comando:

   # /usr/local/snort/bin/snort –u snort –g snort –c /usr/local/snort/etc/snort.conf –i eth0

3.8. KISMET

Es un detector de redes inalámbricas 802.11, sniffer e IDS que puede detectar ataques en la capa de enlace de datos y red, trabaja con tarjetas inalámbricas que soporten el modo de monitoreo para observar el tráfico 802.11 en sus estándares a, b, g y n, según permita el controlador y hardware de la tarjeta (Kershaw, 2011). En su comienzo esta era una herramienta de

wardriving, para seguir evolucionando hasta convertirse en un IDS cliente-servidor completo.

Permite capturar las tramas y colocarlas en el formato pcap, que permite realizar un análisis posterior en herramientas compatibles como Wireshark, tcpdump, etc. A continuación características de Kismet:

- Soporta el salto de canal, además de poder trabajar con múltiples tarjetas inalámbricas.
- Detección de ruido de radiofrecuencia excesivo y sondas de NetStumbler[30].
- Análisis de secuencias de tramas 802.11.
- Decodificación en tiempo de ejecución de WEP, además puede advertir sobre configuraciones vulnerables de este protocolo; contra ataques FMS.
- Se puede instalar en los sistemas operativos Linux, OSX, Windows y Berkeley Software Distribution BSD (sistema operativo derivado de Unix); según soporten el hardware y sus respectivos controladores.
- Se le puede agregar funcionalidades a través de herramientas como GPSDrive, que permitirán observar con mayor detalle la posición y áreas de cobertura de nuestra WLAN, también está Snort; con cuya unión se puede obtener un potente IDS a través de la generación de flujo de tramas en una cola FIFO[31].
- Puede detectar ataques de diccionario contra un ESSID a través de la herramienta Wellenreiter, así como también detecta bombardeos con tramas de desautenticación y disociación.

[30] **NetStumbler:** herramienta popular en la detección de redes inalámbricas.
[31] **FIFO:** de acuerdo a una estructura de datos en espera el primero que llega es el primero en salir; es decir ser procesado.

- Permite descubrir redes ocultas o camufladas, que son un intento de dar seguridad, evitando que el AP envíe beacons ó que no se coloque el SSID en la trama beacon, pero mientras existan sniffers pasivos como Kismet, que puedan entender el protocolo y escuchar la frecuencia; tranquilamente se pueden detectar las redes, sobre todo cuando un cliente legítimo se conecta.
- Utiliza controladores de red virtuales TUN/TAP para exportar paquetes en tiempo real, el controlador TUN simula un dispositivo que opera en la capa de enlace de datos y TAP simula un dispositivo que trabaja en la capa de red.
- Se puede realizar una captura de datos remota y distribuida, gracias a los "drones" de Kismet que son una versión muy simplificada del núcleo de Kismet que permiten la captura de datos desde el punto en el que se le instale, conectarse para reportar al registro de Kismet y el IDS.
- Puede generar registros en XML, lo que permite su integración con herramientas web, que permitan desplegar la información generada por Kismet de una manera visual más amigable.

3.8.1. Elementos del Sistema

Los elementos que componen la arquitectura del WIDS Kismet son:

a. Fuentes de Captura

Las fuentes de captura corresponde a los componentes que entregan la captura de información del medio a Kismet a través de la librería libpcap; principalmente las tarjetas inalámbricas que soportan el modo de operación monitor, que a diferencia del modo promiscuo; la captura de tramas no necesita

que el equipo este asociado a la WLAN. Adicional como fuentes de captura también se puede mencionar un drone de Kismet ó una fuente archivos previamente guardados, para que Kismet los procese.

Las fuentes de captura se las añade a través de la interfaz de usuario de Kismet, ó a través del archivo de configuración Kismet.conf (Kershaw, 2011).

Listas de captura: es una lista en la que se define los canales y patrones de cómo saltaran entre ellos, la fuente de captura. Se puede configurar manualmente, en caso de que no se auto detecte por la herramienta, ó simplemente se desea sobre escribir; aunque no es apropiado cambiar en la mayoría de casos. Las listas por defecto según (Kershaw, 2011) son IEEE80211b.IEEE80211a y IEEE80211ab.

b. Servidor

Este es un componente muy importante en la arquitectura de Kismet, pues el servidor es el encargado de recibir las capturas de la fuente, almacenar en registros “logging”, decodificar y realizar la comparación con firmas, para determinar alertas de intrusión. Este servidor por defecto trabaja en la dirección IP de loopback y en el puerto 2501 (Kershaw, 2011); aunque esto puede ser modificado; entre otras opciones.

- **Logging:** Kismet almacena los registros en archivos de tipo pcap, registros de GPS (Sistema de Posicionamiento Global), alertas y registros de red en XML y texto plano.

Kismet por defecto registra en archivos pcap con encabezados PPI, que son encabezados soportados por algunas herramientas como por ejemplo Wireshark.

- **Filtrado:** el servidor puede soportar un filtrado básico; en caso de que este sea configurado y activado por el administrador de la herramienta. Lo que se permite filtrar es: su seguimiento (tracking), registro pcap, o cualquier otro registro basado en BSSID, direcciones MAC fuente y destino.
- **Decodificación:** el servidor toma los datos ingresados y los decodifica para poder adquirir toda la información necesaria que le permita identificar SSID, clientes, resolver el cifrado como el caso de WEP, etc. Cuando no se instala Kismet como root (usuario privilegiado), la decodificación no sucede en el servidor, más bien en el cliente para evitar posibles ataques.
- **Alertas:** una vez decodificada la información de las tramas, realiza un seguimiento del intercambio que existe en la comunicación entre los clientes y el AP asociado, con esto se compara con firmas del WVE (Vulnerabilidades y Exploits[32] de las Redes Inalámbricas), adicional puede identificar ataques de comportamiento inusual, sondas inusuales o inundación de tramas de disociación; entre otros.

Esta funcionalidad es más efectiva mientras la fuente de captura se encuentre analizando un canal; si existe salto entre canales puede existir una menor precisión, porque se interrumpe el análisis continuo en un solo canal, puede existir un atacante en un determinado canal, pero se tardará en identificarlo si tiene que ir analizando canal por canal hasta llegar al atacado e

[32] **Exploit:** programa o código que explota una vulnerabilidad de un sistema.

incluso el análisis en este no será suficiente y tendrá que esperar hasta su siguiente turno.

Las alertas que se encuentran en el Kismet.conf, poseen dos parámetros que son su máximo número de detecciones por unidad de tiempo y cuántas alertas permite en un mínimo de tiempo. A continuación algunos ataques que pueden ser detectados:

Tabla 27. Alertas que posee Kismet según WVE

Nombre	Descripción	Tipo de análisis
AIRJACKSSID	Detección de la herramienta de hacking Airjack	Firma
APSPOOF	Detección de AP Spoof, conflicto de APs; a través de sondas y beacons sin MAC legítima.	Firma
BSSTIMESTAMP	Detección de marcas de tiempo BSS inválidos o fuera de secuencia, ataques spoofing o evil twin.	Anomalía
CHANCHANGE	Detección de cambio de canales, indica spoofing	Anomalía
CRYPTODROP	Detección de spoofing en un AP con poca seguridad.	Anomalía
DEAUTHFLOOD	Inundación de tramas de desautenticación.	Anomalía
BCASTDISCON	Detección de paquetes falsos de disociación y desautenticación, provocando DoS.	Anomalía
DHCPCLIENTID	Envío de paquetes DHCP Discover incorrectos buscando DoS, acabando con las direcciones disponibles.	Firma
DHCPCONFLICT	Clientes que reciben dirección IP por DHCP y usan otra, indicio de spoofing.	Anomalía
DISASSOCTRAFFIC	Detección de un cliente disociado que envía tramas de datos, indicio de un cliente falsificado o DoS al mismo.	Anomalía
DISCONCODEINVALID	Tramas de disociación con códigos inválidos, reservados ó desconocidos, indicio de DoS.	Firma
DEAUTHCODEINVALID	Tramas de desautenticación con códigos desconocidos, inválidos o reservados.	Firma
DHCPNAMECHANGE	Spoofing por clonación del cliente.	Anomalía
DHCPOSCHANGE	Spoofing por clonación del cliente.	Anomalía
LONGSSID	Detectar ataques que explotan la vulnerabilidad de algunos drivers a través de SSID de longitud mayor a la permitida (32 bytes) (IEEE802.11, 2012).	Firma
LUCENTTEST	Detección de paquetes de escaneo de tarjetas Lucent Orinoco.	Firma
MSFBCOMSSID	Detección campos SSID más largos que la especificación 802.11, causan problemas en drivers Broadcom en Windows.	Firma
MSFDLINKRATE	Detección de vulnerabilidad de drivers D-Link en manejo de largo porcentajes de campos 802.11.	Firma
MSFNETGEARBEACON	Detección de vulnerabilidad de drivers de Windows en el manejo de beacons sobre su largo normal.	Firma
NETSTUMBLER	Detección de Netstumbler	Firma
NULLPROBERESP	Detección de paquetes prueba-respuesta con longitud 0.	Firma
PROBENOJOIN	Detección de herramientas de escaneo de WLANs.	Anomalía

Elaborado por: Autora del Proyecto

c. Cliente

Corresponde a la interfaz gráfica (usa la librería ncurses), que se conecta al servidor para desplegar información como; los SSID de las WLAN que detecta la fuente de captura con su respectivo canal, información de GPS (si ha sido

configurado), errores, alertas, estadísticas del servidor; en fin todo lo que el servidor ha procesado y tiene listo para el despliegue visual del administrador de la herramienta. Al arrancar el servidor, arranca el cliente y permite que se configure su apariencia, arranque y apagado del servidor. Además el cliente se puede configurar muy amigable con sonidos .WAV[33], con el plugin Festival.

3.8.2. Instalación

1. Se comprueba que la tarjeta inalámbrica se encuentra en modo monitor con el comando *"iwconfig";* caso contrario se coloca en este modo; si existe algún inconveniente se debe revisar si el hardware y driver son compatibles con Kismet (información detallada en su página oficial):

   # ifconfig wlan0 down

   # iwconfig wlan0 mode monitor

   # ifconfig wlan0 up

2. Se descarga la herramienta de su página oficial (Kershaw, 2011), en la opción Donwload, figura 27; y se descomprime accediendo a la ubicación donde se guardó:

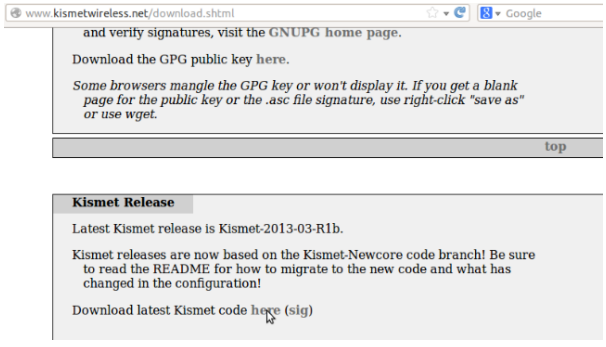


Figura 27. Sitio de descarga de Kismet
Elaborado por: Autora del Proyecto

[33] **Wav:** formato de audio digital normalmente sin compresión de datos.

 # cd <Ruta donde se guardó la descarga>

 # tar Jvxf kismet-2013-03-R1b.tar.xz

3. Se ingresa a la carpeta descomprimida, se ejecuta *./configure,* con esto nos indicará los paquetes que se necesitan instalar para el correcto funcionamiento de la herramienta, aunque cabe recalcar que la librería pcap ya fue instalada en la instalación de Snort (librería ncurses, nl):

   # cd Kismet-2013-03-R1b.tar.xz

   # ./configure

   # apt-get install libncurses.dev

   # apt-get install libnl.dev

4. Se instala Kismet:

   # make dep

   # make

   # make install

3.8.3. Configuración

Se ingresa a Kismet.conf, figura 28. para colocar la fuente de captura con las opciones que ameriten la necesidad del usuario; como se puede apreciar en la tabla 28:

 # gedit /usr/local/etc/kismet.conf

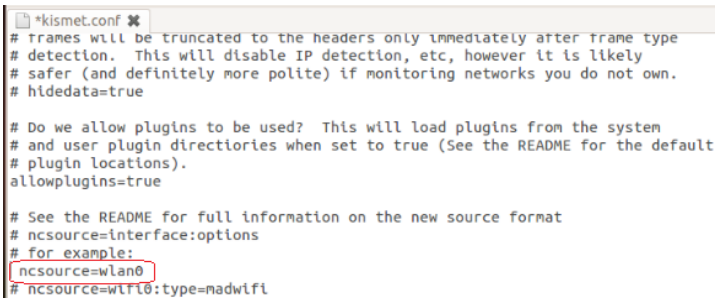


Figura 28. Archivo kismet.conf
Elaborado por: Autora del Proyecto

Tabla 28. Opciones configurables en las fuentes de captura en Kismet

Opción	Descripción
name=foo	Nombre que se le asigna a la fuente caso contrario toma el nombre de la interfaz de captura.
Type=foo	Permite definir el tipo de fuente cuando raramente la fuente no la autodetecta.
Uuid=foo	Permite a los usuarios definir un identificador único estático.
Hop=true | false	Deshabilita el salto de canales.
Velocity=#	Velocidad de salto de canal, Kismet puede saltar de 1 a 10 canales por segundo.
Dwell=#	Se define un tiempo de permanencia en el canal si el salto entre canales está habilitado. Kismet saltará en N segundos por canal en vez de N canales por segundo.
Channellist=name	Se puede usar una lista de canal alternativo en lugar de una lista auto detectada de canales soportadas por la interfaz.
Split =true|false	Se usa cuando existen varias fuentes que usan la misma lista de canales, Kismet los dividirá para que no cubran los mismos canales al mismo tiempo.
Retry=true|false	Kismet intentará reabrir una fuente de captura en la cual ha encontrado un error. Este comportamiento puede ser deshabilitado si el usuario quiere que la fuente permanezca cerrada.
Plcpfail=true	Forzar a que una VAP reporte paquetes que no pasan el chequeo PLCP[34].
Forcevap=t|f	Se puede forzar la inhabilitación de la creación de interfaces VAP colocando “false”, por defecto el comportamiento es “true”.
Wpa_scan=time	Esta opción permite definir el tiempo de exploración asistido por hardware que se dispara en una interfaz administrada utilizando suplicante-WPA de un VAP administrado. Tiempo sugerido 15 segundos
Validatefcs=t|f	Opción que se deshabilita por defecto debido a que los paquetes entrantes no se les revisa su FCS por parte de Kismet ya que se considera que los controladores por defecto solo reportan tramas válidas. Se activa si la fuente de captura reporta tramas inválidas.
Fcs=true|false	Permite forzar el manejo de los bytes FCS en la fuente de

[34] **PLCP:** encabezado de 144bits para sincronizar, determinar ganancia y estableces el CCA en la capa física de 802.11b.

CONTINUA=>

	paquetes.
Fcsfail=true	Forzar a que una VAP reporte paquetes con una conocida incorrecta FCS; solo funciona en Linux con controladores MAC802.11.
Vap=interface	Permite crear un punto de acceso virtual (VAP), para los usuarios que desean trabajar con Kismet+Administración ó Kismet + inyección de tramas. Sólo se permite en controladores que usan 802.11 en Linux.

Elaborado por: Autora del Proyecto

Se ejecuta kismet (# *kismet*) y se aprecia la ventana de la figura 29 en la que se puede acceder a personalizar la apariencia de kismet si se desea, en la figura 30 es la segunda ventana que aparece para que el usuario pueda cambiar las opciones de inicio del servidor. La siguiente ventana es la figura 31. en la que se advierte que el proceso se iniciará como root; es decir con privilegios de administrador.

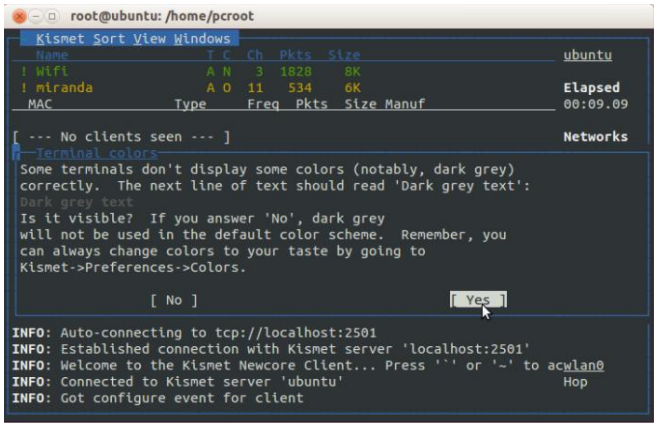


Figura 29. Ventana de inicio de Kismet interrogando preferencias de apariencia

Elaborado por: Autora del Proyecto

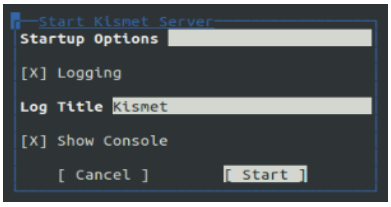


Figura 30. Ventana en la que se puede configurar arranque del servidor

Elaborado por: Autora del Proyecto

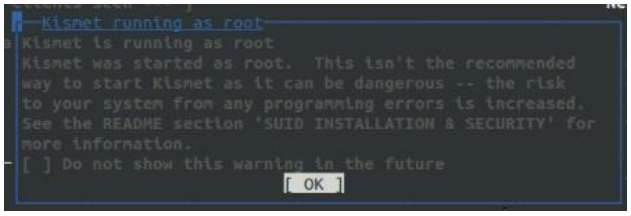


Figura 31. Advertencia que la herramienta se ha instalado como "root"

Elaborado por: Autora del Proyecto

Por último la figura 32 indica la ventana principal de Kismet funcionando, la tabla 29 presenta información detallada para entender esta interfaz de usuario.

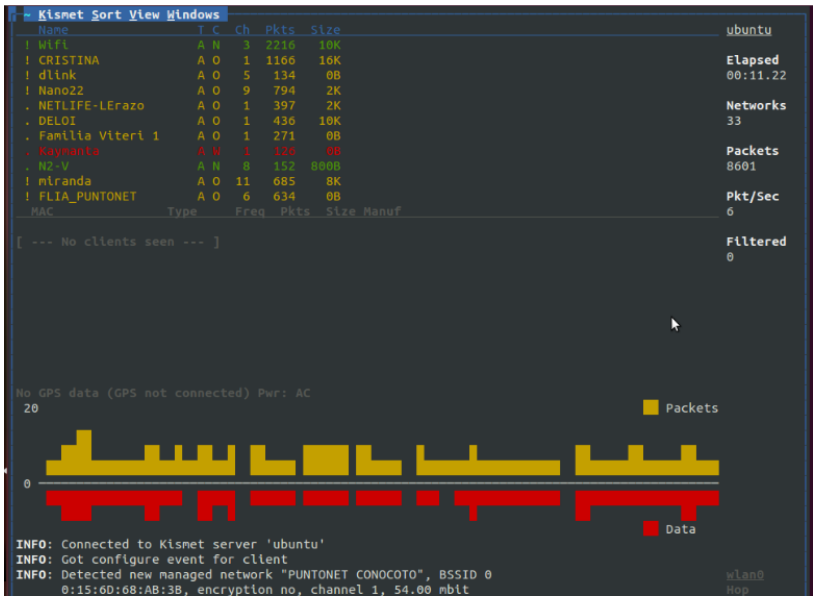


Figura 32. Ventana Principal de Kismet

Elaborado por: Autora del Proyecto

Tabla 29. Descripción de la Ventana Principal de Kismet

Componentes	Descripción	
Network List	Es la parte central de la interfaz en donde se despliegan las redes detectadas.	
Name: SSID de la redes detectadas	**Símbolo (!):** Ubicado en la columna de Name significa actividad de la red en los últimos 3 min.	
	Símbolo (.): Ubicado bajo la columna Name significa actividad detectada en los últimos 6 segundos.	
	Símbolo ( ): Si no aparece un símbolo significa nada de actividad.	
	Colores	**Verde:** con encriptación
		Amarillo: sin encriptación
		Rojo: usa su configuración por defecto.
		Azul: redes que ocultan su SSID.
T	Columna que corresponde al modo de funcionamiento del dispositivo WiFi detectado :(A)=modo AP, (H)=modo ad-hoc, (G)=grupo de redes wireless, (P)=modo “probe request”,(D)=red de datos: se aprecian tramas de datos pero kismet no ha capturado beacons o frames de gestión y aún no ha determinado el tipo de red.	
C	Existe encriptación WEP: (Y)=WEP, (N)=abierto, (O)=otro tipo de encriptación.	
Ch	Canal de operación.	
Rate	Velocidad máxima de operación.	
Packets	Número de paquetes capturados.	
Size	Tamaño de los paquetes capturados en cada red.	
PanelStatus	Proporciona información sobre las redes y clientes que se va detectando, alertas, problemas y hasta informa sobre batería baja..	
Panel Info	**Elapsed:** tiempo transcurrido desde que kismet arrancó. **Networks:**total de redes detectadas. **Packets:** total de tramas detectadas. **Pkt/sec:** tramas recolestadas por segundo. **Filtered:** tramas filtradas con filtros configurados en kismet.	

Elaborado por: Autora del Proyecto

CAPITULO 4

BENCHMARKS

Cuando existe un sistema de seguridad como por ejemplo un IDS; cabe la necesidad de evaluar cuan eficiente resulta; por el mismo hecho de cerciorar que no exista un desperdicio de recursos que desencadenen en vulnerabilidades y falta de protección de nuestra organización. Manteniendo una continua evaluación de cualquier sistema, se puede apreciar su actual operación, sus falencias y fortalezas; para obtener un aprendizaje y mejoramiento claves en su supervivencia.

Un **benchmark**, viene a ser la técnica con que se evalúa la función y rendimiento de un sistema, precisamente ayuda en la evaluación de los sistemas de detección de intrusos; permitiendo observar y determinar sus errores (falsos positivos y negativos), que conlleven a mejorar la configuración, implementación, incluso su desarrollo en sí, para obtener un porcentaje mínimo de error; porque es imposible alcanzar la perfección, mucho menos en un mundo en el que la base de datos de firmas o anomalías tenga actualizada las n modificaciones que podría tener un ataque, ó la infinita creatividad de los hackers desarrollando nuevos ataques.

4.1. Técnicas de Evaluación

Cuando se realiza una evaluación a un sistema de seguridad; este no solo se basa en la arquitectura tecnológica sino también, requisitos de seguridad

adecuados, la realización de análisis de riesgos, modelado de amenazas, revisiones de código y la medición de la seguridad ocupacional (Ali & Heriyanto, 2011).

Cuando se trata de evaluar la seguridad se puede realizar dos procesos; el análisis de vulnerabilidades y las pruebas de penetración; estas hacen uso de metodologías que permitan llevar su proceso, para poder comprender y analizar las defensas.

Las **pruebas de penetración** son un proceso de evaluación de seguridad; que realiza un conjunto de prácticas, como ataques para encontrar las debilidades; de modo más brusco que un análisis de vulnerabilidades, que simplemente enumera los puntos débiles, falencias, recomendaciones, entre otros. Existen tres tipos de pruebas de penetración (Ali & Heriyanto, 2011):

- **Black-box:** También conocido como external testing; corresponde a la evaluación remota que realizará el auditor, es decir externamente realizará las pruebas sin conocimiento de la infraestructura interna de la organización; como la situación de un hacker externo intentando vulnerar las seguridades perimetrales y lograr sus objetivos.
- **White-box:** También conocido como internal testing; trata la evaluación interna de la seguridad de la organización; el auditor tiene conocimiento de la infraestructura y tecnologías usadas, existiendo mayor facilidad en la determinación de problemas de seguridad.
- **Gray-box:** Combinación de la evaluación interna y externa, para una mejor visión de las vulnerabilidades de seguridad.

4.1.1. Metodologías de pruebas de seguridad

Las metodologías son las que permiten direccionar las necesidades de evaluación de seguridad, destacar las debilidades, definir características claves y beneficios de los sistemas. A continuación algunos benchmarks de evaluación de seguridad:

- **Construcción de modelos de datos:** modelos que recojan gran cantidad de información del comportamiento de un sistema; como el caso de la red; para con este proceder a evaluar la reacción de los mecanismos de seguridad. Un ejemplo de modelo de datos en el análisis de un IDS; es **DARPA** (Group Cyber System and Technology, 2013):

- Este es el primer modelo estándar para la evaluación de sistemas de detección de intrusos, sus datos fueron resultado de evaluaciones en los años 1998 y 1999; aunque en el 2000 se recolectaron tres adicionales conjuntos de datos de experimentos en escenarios específicos.
- Las pruebas fueron realizadas para medir probabilidad de falsa alarma y detección en una red local que simulaba una base de las fuerzas aéreas de EEUU; con exposición a conocidos y nuevos ataques.

Por otro lado existen metodologías de libre distribución que son muy utilizadas en la evaluación de los elementos de seguridad:

- **Open Source Security Testing Methodology Manual (OSSTMM)**

Esta metodología abierta fue desarrollada por el ISECOM (Instituto de Seguridad y Metodologías Abiertas); es ampliamente utilizada en pruebas y análisis de seguridad. Este tipo de metodología permite determinar el estado de

la seguridad operacional y sus costos, bajo los objetivos del negocio; por ello define cuatro grupos claves: **Alcance, Canal, Índice y Vector**.

El primero define el proceso de recolección de datos durante las pruebas, el segundo define la interacción según el tipo de comunicación en el que se llevará a cabo las pruebas (físico, espectro, etc.), el tercero es el método por el cual se clasifica las pruebas según la identificación de los objetivos como su dirección MAC e IP. Por último el vector concluye con la dirección que debe tomar el auditor para evaluar y analizar los objetivos.

Este proceso permite tener un mapa de rutas (conocido como Alcance de la Auditoría) para ubicarse mejor en una evaluación más completa.

Existen diferentes tipos de pruebas de seguridad que OSSTMM clasifica según lo presentado en la tabla 30.

Tabla 30. Tipos de pruebas de seguridad según OSSTMM

Tipos de pruebas de seguridad	Descripción	
	Auditor	**Sistema a Evaluar**
Blind("ciego")	No posee información del sistema.	Es informado acerca de las pruebas que se llevará a cabo.
Double blind ("doble ciego")	No posee información del sistema.	No ha sido informado de las pruebas.
Gray box ("caja gris")	Tiene un limitado conocimiento del sistema.	Es informado acerca de las pruebas que se llevará a cabo.
Double gray box ("caja gris doble")	Similar a gray box excepto que se define un plazo para la auditoría y no hay canales ni vectores siendo probados.	
Tandem	Posee un mínimo conocimiento del sistema.	Es informado acerca de las pruebas que se llevará a cabo.
Reversal("cambio completo")	Posee completo conocimiento del sistema.	No es informado de cuándo ni cómo se realizarán las pruebas

Elaborado por: Autora del Proyecto

Las principales características y beneficios de esta metodología se resumen en la tabla 31:

Tabla 31. Características y Beneficios Principales de OSSTMM

OSSTMM Características y Beneficios	Provee una exacta medición de seguridad.
	Su framework se adapta con muchos tipos de pruebas de seguridad.
	Asegura que se concluya a fondo la evaluación obteniendo resultados consistentes, cuantificables y confiables.
	La metodología sigue cuatro fases que son: la definición, información, regulación y control.
	El método RAV (Valores de Evaluación de Riesgo: análisis de resultados según la seguridad operacional, pérdida de control y limitaciones) puede lograr evaluar métricas de seguridad.
	Formalizar los reportes de la evaluación usando STAR (Reporte de Auditoría de Prueba de Seguridad).
	Es actualizada con nuevas tendencias de pruebas de seguridad, regulaciones y términos éticos.
	El proceso de OSSTMM puede coordinarse fácilmente con otras regulaciones como industriales, negocios, gubernamentales.

Elaborado por: Autora del Proyecto

- **Information Systems Security Assessment Framework (ISSAF)**

Fue Desarrollado por OISSG (Grupo de seguridad de Sistemas de Información Abierto), es un análisis de framework y prueba de seguridad; fue desarrollado con los dos enfoques de las evaluaciones de seguridad, lo técnico y lo administrativo. En el caso técnico se define un conjunto de reglas y procedimientos que se deben seguir para realizar una evaluación adecuada; el caso administrativo conseguir las mejores prácticas y compromiso administrativo a lo largo del proceso de pruebas.

ISSAF define la evaluación como proceso no como auditoría; además posee un conjunto de bases de evaluación técnicas que permiten probar gran cantidad

de diferentes tecnologías y procesos, en la tabla 32 se presenta las características y beneficios principales.

Tabla 32. Características y Beneficios Principales de ISSAF

ISSAF Características y Beneficios	Provee una propuesta para asegurar la infraestructura, evaluar los controles de seguridad críticos en contra de sus vulnerabilidades.
	Un framework direcciona diferentes áreas de información de seguridad como evaluación de riesgos, buenas prácticas, etc.
	El proceso de evaluación técnico de ISSAF consiste de: operaciones de gestión, evaluación de seguridad física, metodología de prueba de penetración, gestión de incidentes, gestión de cambio, gestión de continuidad del negocio, conciencia de seguridad, y conformidad legal y regulatoria.
	Examina la seguridad de una red, sistema o aplicación, porque el framework puede enfocarse transparentemente en tecnologías como firewalls, switches, IDSs, etc.
	Cierra la brecha entre lo técnico y lo administrativo de las pruebas de seguridad, porque implementa controles para manejar ambas áreas.
	Habilita la gestión para entender riesgos sobre las defensas perimetrales y poder reducirlos.

Elaborado por: Autora del Proyecto

Para evaluar un IDS, los modelos de datos y lo dos últimas metodologías de código abierto explicadas, son buenas estrategias; pero los benchmarks de seguridad también permiten evaluar el nivel de aplicación con enfoque en su seguridad como **Open Web Application Security Project (OWASP) top Ten**, con su lista de riesgos de seguridad principalmente enfocados en las aplicaciones web y bases de datos, por otro lado también está **Web Application Security Consortium Threat Classification (WASC-TC)**, con sus puntos de vista de ayuda a los desarrolladores y auditores de seguridad, en el entendimiento de las amenazas de una aplicación web.

4.2. Backtrack

Backtrack es una distribución basada en la distribución Debían GNU/Linux (Pritchett & De Smet, 2012, pág. 1), que está especializada en pruebas de

penetración y análisis forense; posee un arsenal de herramientas enfocadas en la evaluación de seguridad, por ello es una herramienta de benchmarking de seguridad muy completo. A continuación, algunas características:

- Se encuentra en la versión 5 cuyo lanzamiento lleva el nombre “Revolution”, al momento de la realización de este trabajo; se encuentra en la revisión R3; publicada el 13 de agosto del 2012, que a más de realizar correcciones a la revisión anterior adiciona más de 60 herramientas nuevas.
- Backtrack versión 5 provee soporte para arquitecturas de 32 y 64 bits; incluso para hacerlo más amigable puede usar como administrador de ventanas GNOME, KDE, aunque también se puede usar Fluxbox.
- Se puede realizar pruebas de seguridad tanto de Black-box como de tipo White-box.
- Es la primera versión que incluye código fuente completo dentro de sus repositorios, aclarando cualquier problema de licencia como se había dado con la versión 4 (Caizapanta, 2013).
- Se puede arrancar desde un DVD, USB, o estar instalado normalmente como un sistema operativo en el disco duro; incluso se puede descargar virtualizado desde su página oficial.
- El proceso de pruebas debe seguir una metodología escogida por el auditor que le permitan llevar un orden hacia una evaluación exitosa; el proceso incluye: alcance del objetivo, recopilación de información, descubrimiento del objetivo, enumeración de objetivos, mapeo de las vulnerabilidades, ingeniería social, escalada de privilegios, mantenimiento de accesos,

documentación y reportes. La figura 33 muestra el proceso de pruebas en Backtrack.

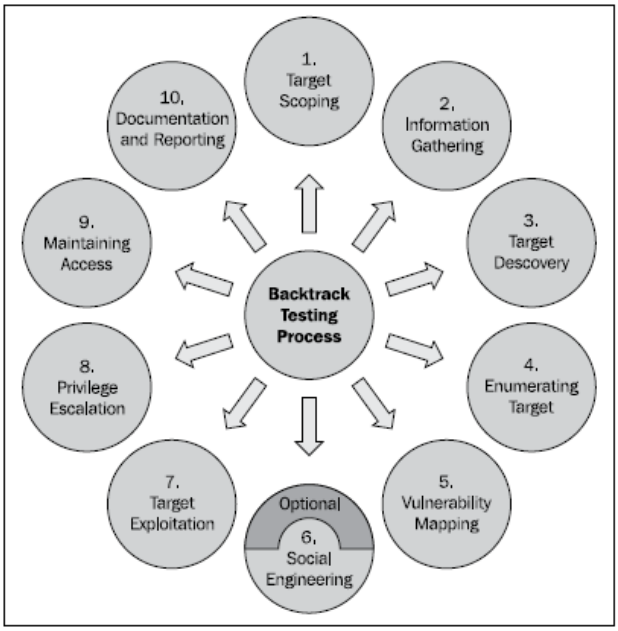


Figura 33. Proceso de pruebas de Backtrack

Fuente: (Ali & Heriyanto, 2011)

4.2.1. Herramientas en Backtrack

Posee gran cantidad de herramientas que se pueden clasificar en los siguientes grupos (Caizapanta, 2013):

- Recopilación de Información
- Mapeo de Puertos
- Identificación de Vulnerabilidades
- Análisis de Aplicaciones Web
- Análisis de Redes de Radio
- Penetración
- Escalado de Privilegios

- Mantenimiento de Accesos
- Forense
- Ingeniería Inversa
- Voz sobre IP

❖ **Herramientas para el análisis de redes 802.11**

Backtrack posee varias herramientas que permiten dejar al descubierto las inseguridades de una red Wi Fi; principalmente permiten realizar monitoreo de tráfico y los ataques comunes en Wi Fi anteriormente expuestos. En la tabla 33, se encuentra algunas herramientas que se usa en pruebas de seguridad para redes inalámbricas.

Tabla 33 . Herramientas de ataque a redes inalámbricas de Backtrack

Herramienta	Función
airbase-ng	Herramienta que realiza varios ataques enfocados a los clientes de la WLAN.
aircrack-ng	Herramienta de craqueo de claves WEP y WPA con una cantidad suficiente de paquetes capturados.
airdecap-ng	Descifrar archivos capturados que tengan encriptación WEP/WPA/WPA2.
airdecloak-ng	Remueve el encapsulado WEP desde un archivo pcap.
airdriver-ng	Provee información sobre el estado de los controladores inalámbricos, además permite descargar y cargar los mismos.
aireplay-ng	Permite realizar la inyección de tráfico para elevar la captura de vectores de inicio.
airmon-ng	Establece la tarjeta inalámbrica en modo monitor.
airodump-ng	Permite escanear redes (SSID) y capturar vectores de inicio.
airolib-ng	Almacenar y gestionar listas de ESSID y claves, cálculo de PMKs y craqueo WPA/WPA2.
airserv-ng	Servidor de tarjetas inalámbricas que permite usar múltiples aplicaciones y programas wireless independiente del controlador o tarjeta inalámbrica.
airtun-ng	Creador de interfaces de túnel virtuales, con el fin de monitoreo con un WIDS ó inyección de tráfico.
easside-ng	Permite la comunicación con un AP encriptado con WEP sin conocer la clave.
packetforge-ng	Crear paquetes encriptados para inyectarlos posteriormente.
tkiptun-ng	Permite inyectar pocas tramas dentro de una red WPA TKIP con QoS.
wesside-ng	Incorpora técnicas para obtener la clave WEP en minutos

Elaborado por: Autora del Proyecto

Adicional Backtrack, a través de su menú WLAN Exploitation en el directorio de la figura 34, permite acceder de una manera más cómoda a las más comunes y principales herramientas de pruebas de penetración inalámbricas; destacando fern-wifi-cracker y gerix-wifi-cracker-ng por sus interfaces gráficas mucho más cómodas para realizar los ataques; sin necesidad de ejecutar en el terminal un conjunto de comandos. En la tabla 34 se describe cada una de las herramientas que se despliegan en el menú WLAN Exploitation.

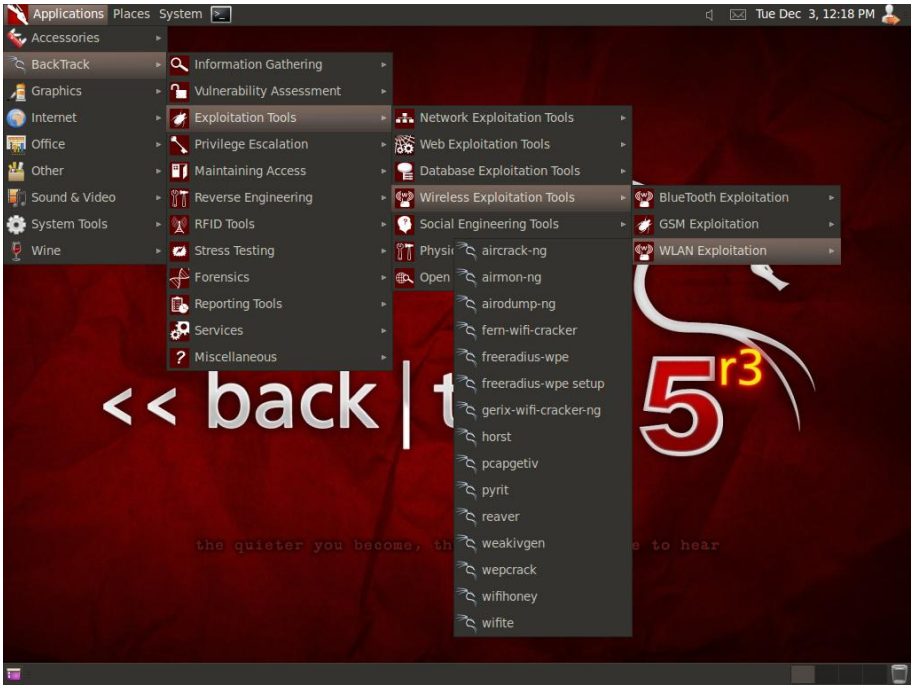


Figura 34. Directorio de Herramientas de WLAN Exploitation

Elaborado por: Autora del Proyecto

Tabla 34. Herramientas desplegadas en el menú WLAN Explotation de Backtrack 5 R3

Herramientas del menú WLAN Exploitation	Características
Aircrack-ng	- Herramienta de craqueo de claves WEP y WPA con una cantidad suficiente de paquetes capturados.
Airmon-ng	-Coloca las tarjetas inalámbricas en modo monitor.
Airodump-ng	-Permite capturar tráfico 802.11.
Fern-wifi-cracker	-Es una herramienta de auditoría wireless escrita en lenguaje Phyton y Qt GUI biblioteca Phyton, que permite realizar algunos tipos de ataques principalmente a WEP/WPA/Wi Fi Protected Setup (mecanismos que permiten una configuración sencilla en WPA en ambientes no empresariales); ó también ataques en Ethernet. -Funciona en sistemas operativos Ubuntu KDE/GNOME, Backtrack Linux y BackBox Linux. - Hace uso de otras herramientas de ataque inalámbrico como: aircrack-ng, reaver, macchanger.
Freeradius-wpe	-Da soporte y permite probar los métodos de autenticación EAP. -Proyecto desarrollado por Brad Antoniewicz y Josh Wright. - Permite demostrar a través de un servidor radius de código abierto las vulnerabilidades de suplantación.
Freeradius-wpe setup	-Permite configurar el servidor radius en Backtrack.
Gerix-wifi-cracker-ng	-Es la interfaz de usuario gráfica que automatiza los ataques de redes inalámbricas con aircrack. -Sus autores son: Emanuele Gentili y Emanuele Acri.
Horst	-Es un pequeño y liviano analizador de WLAN con una interface de texto; es decir su función es similar a los sniffers tcpdump, Wireshark ó Kismet.
Pcapgetiv	-Es un script que abre archivos pcap o un dispositivo en busca de IVs débiles.
Pyrit	Crea bases de datos analizando la parte de IEEE802.11 WPA/WPA-PSK en la fase de autenticación.
Reaver	-Implementa un ataque de fuerza bruta contra WPS.
Weakivgen	-Simulador de IVs que usa WEP, para poder conseguir la clave WEP.
Wepcrack	-Herramienta que permite quebrantar las claves secretas WEP.
Wifihoney	-Script que permite crear falsos APs para suplantar los legítimos.
Wifite	-Herramienta que permite realizar ataques a WEP, WPS y capturar el intercambio de información entre un AP y cliente WPA legítimos.

Elaborado por: Autora del Proyecto

CAPÍTULO 5

PRUEBAS Y RESULTADOS

Este capítulo contempla la preparación del escenario de pruebas en un ambiente de producción, y puesta en marcha de los ataques a través de Backtrack 5R3, para la obtención de un análisis de las respuestas obtenidas tanto en Snort como Kismet.

5.1. Escenario y Generación de Ataques a través de Bactrack5 R3

5.1.1. Escenario

La topología de pruebas se encuentra en producción según la topología de la figura 35, el FortiAP en rojo ha sido escogido para la generación de ataques. Para esto se configura un SSID "Pruebas", adicional se ha conectado un switch Catalyst 2960 (switch en color naranja) para configurar port mirroring y así tener operando Snort.

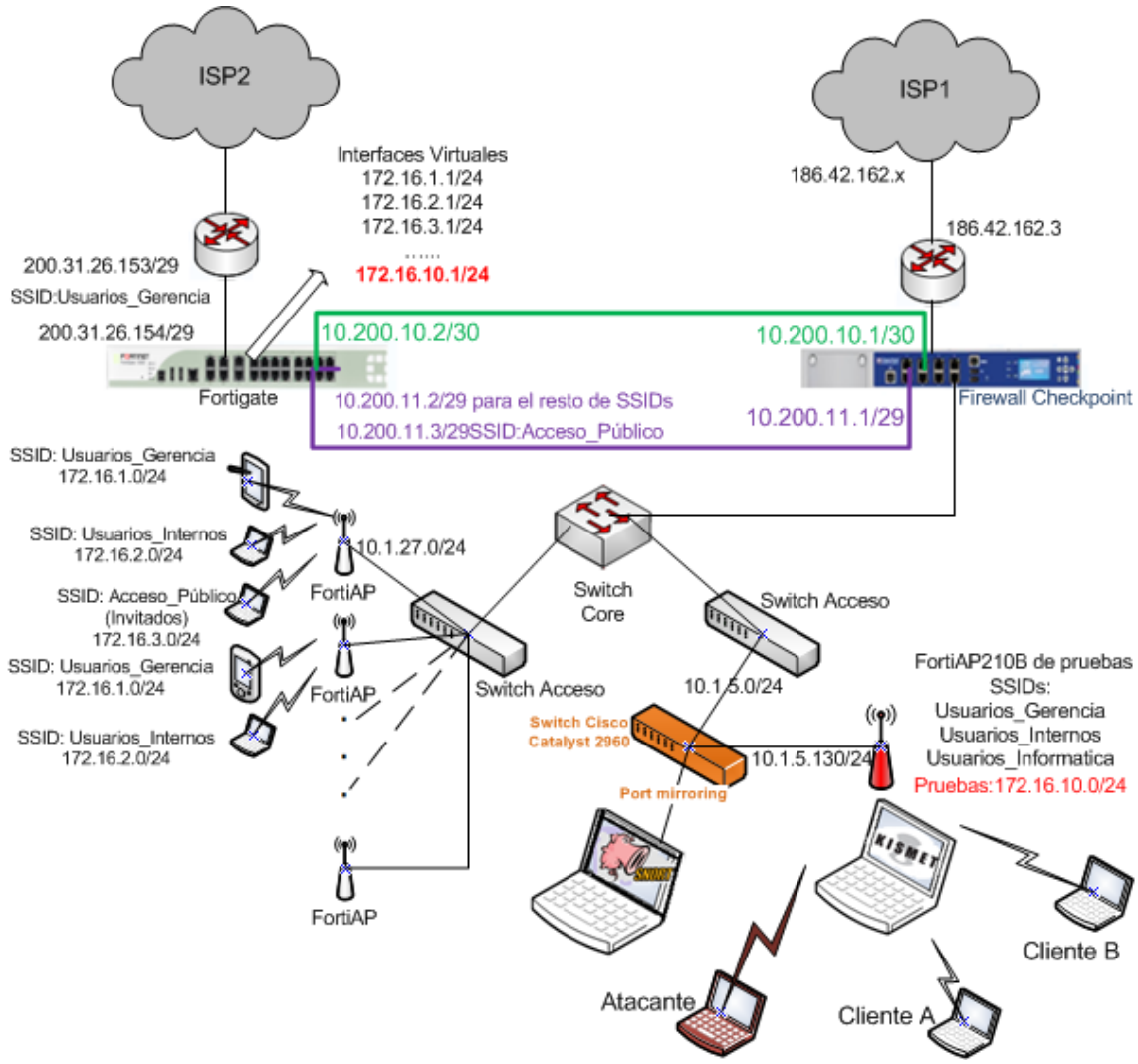


Figura 35. Topología en Producción que será utilizada en el análisis de Snort y Kismet

Elaborado por: Autora del Proyecto

A continuación se describen algunos de los componentes más importantes en la topología de la figura 35:

- **FortiGate 100D:** 22 puertos gigabit ethernet, transmisión de hasta 2,5 Gbps en el firewall, posee control de aplicaciones, protección avanzada contra amenazas, controlador inalámbrico, conmutación integrada, aplicación de

políticas de punto final; sistema operativo FortiOS 5, uso de tecnología ASIC (circuito integrado de aplicación específica).

Al momento de las pruebas posee 21 FortiAPs tanto del modelo 210B y el 220B, además de 11 interfaces virtuales que corresponden a los SSIDs; que se crean según el perfil y permisos que determine el administrador.

- **FortiAP-210B (características del AP de pruebas):** AP que posee 2 antenas internas con soporte IEEE802.11 a, b, g y n, ofrece hasta 300Mbps de rendimiento total, puede trabajar en la frecuencia de 2,5 y 5 GHZ, potencia de transmisión máxima de 17dBm (50mW), soporta 8 SSIDs (7 para acceso a clientes y 1 para monitoreo). En el momento de las pruebas posee 4 SSIDs, incluyendo el SSID “Pruebas”.
- **D-Link DWA-125 Wireless N 150 USB Adapter versión A2 (Tarjeta en el atacante):** chip Ralink RT3070, soporta los estándares IEEE802.11n y 802.11g, trabaja en las frecuencias 2,4 y 2,483 GHz, potencia de transmisión 17dBm, compatible con WPA/WPA2, 802.1x y WPS.
- **D-Link DWA-125 Wireless N 150 USB Adapter versión A3 (Tarjeta de trabajo para Kismet):** chip Ralink RT5370, soporta los estándares IEEE802.11n y 802.11g, trabaja en las frecuencias 2,4 y 2,483 GHz, potencia de transmisión 17dBm, compatible con WPA/WPA2, 802.1x y WPS.
- **Anera Wireless USB Adapter 802.11b/g/n 150 Mbps (Tarjeta conectada también en el atacante):** chip Realtek RTL8192CU, soporta WEP, WPA, WPA2, WPS y 802.1x, antena externa de 2dbi.

- **Switch Cisco Catalyst 2960:** 24 puertos.
- **Firewall Checkpoint:** a través de este equipo pasan las conexiones desde los FortiAPs hacia el FortiGate por su interfaz 10.200.10.1/30, y según se haya configurado en el FortiGate este decidirá si el tráfico hacia el internet, saldrá directo por su interfaz 200.31.26.153 ó a través del firewall por la 10.200.11.1/29.

❖ **Equipos en la WLAN de Pruebas:**

- **Máquina que hospeda los IDSs de pruebas:** máquina virtual con sistema operativo Ubuntu 12.0.4 64 bits, RAM de 1500Mb, 40 Gb de disco duro.
- **Dos Máquinas Clientes:** MAC cliente A igual a 70:F3:95:39:A4:97, MAC cliente B igual a 00:21:6B:32:DB:C2.
- **Máquina Atacante:** máquina virtual descargada desde la página oficial (Back|track-linux. org, 2013) de Backtrack con las características de la figura 36 al abrir la máquina a través de VMware Workstation 9.0.3 se aprecia que posee configurado una RAM de 768Mb y 20Gb de disco duro.

Figura 36. Descarga de la máquina virtual de Backtrack
Elaborado por: Autora del Proyecto

- **Configuración del SSID de Pruebas**

Se ingresa al FortiGate a través de su IP (10.200.10.2), un usuario y clave de administrador a través de un navegador con la dirección https://10.200.10.2.

Una vez dentro se procede a ingresar al menú *WiFi Controller*, luego WiFi *Network/SSID* y la opción *Create New*, luego se realiza el ingreso de la información en los campos que se puede observar en la figura 37 Cabe destacar que sólo está disponible como protocolo de seguridad WPA, WPA2, tanto enterprise como personal, WEP no se presenta como opción en estos equipos modernos.

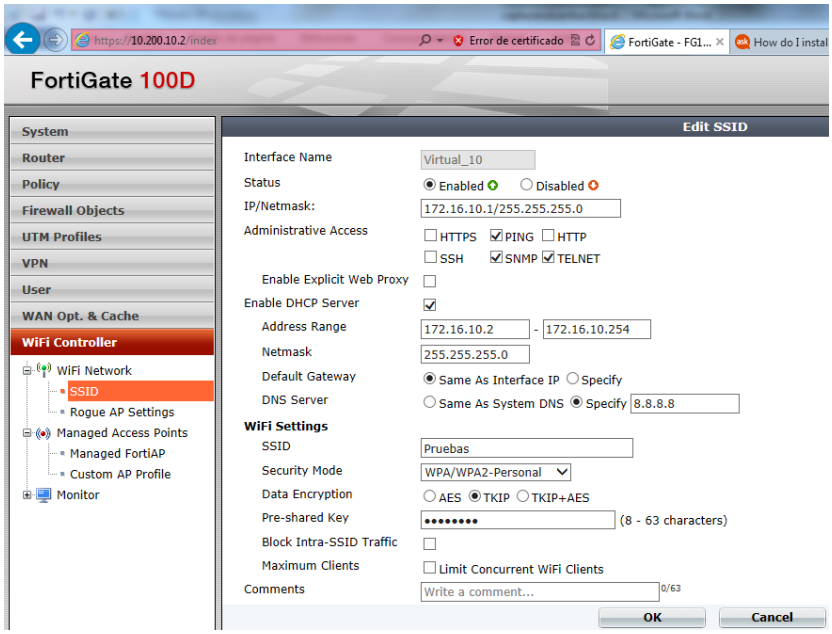


Figura 37. Configuración del SSID Pruebas
Elaborado por: Autora del Proyecto

Se necesita configurar las políticas (figura 38) para este SSID, con las que podrá tener acceso a internet, en este caso a través del firewall de la organización (10.200.11.1/29).

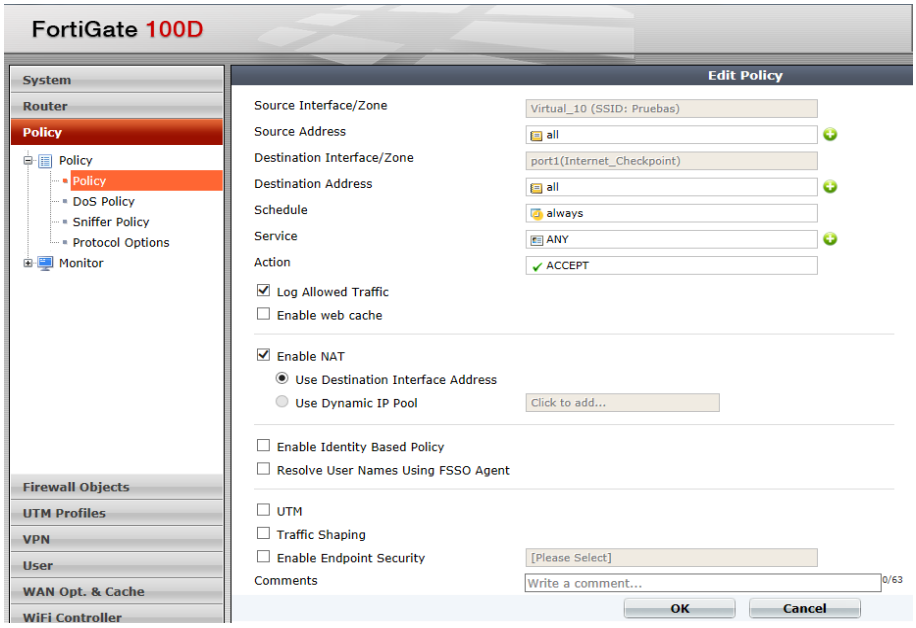


Figura 38. Configuración de Políticas para el SSID Pruebas

Elaborado por: Autora del Proyecto

Ahora se necesita configurar el FortiAP para que permita la conexión al SSID “Pruebas”; para ello se debe ingresar a *Wi Fi Controller/Managed Access Points/Managed FortiAP* y en el listado desplegado de APs conectados, escoger el que será objeto de las pruebas; en este caso el llamado Piso1_1, con doble clic se ingresa a su configuración y se escoge el SSID Pruebas; por último se da clic en ok quedando en el listado anterior como muestra la figura 39.

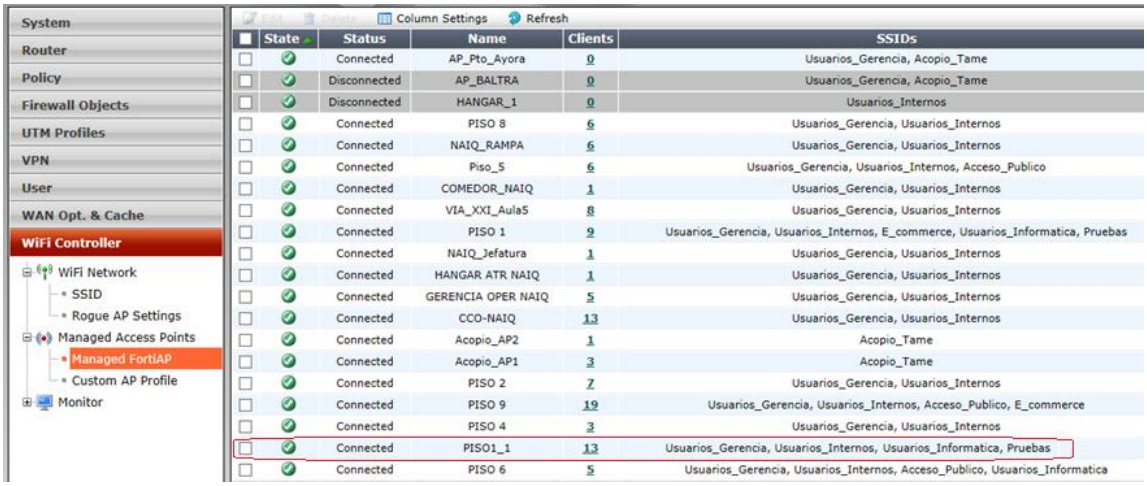


Figura 39. Listado de FortiAPs conectados al FortiGate

Elaborado por: Autora del Proyecto

- **Configuración del Switch Catalyst 2960**

Para las pruebas con Snort se necesita una interfaz Ethernet; ya que en el modo monitor de la tarjeta inalámbrica no reconoce el tipo de tráfico DLT_IEEE802_11_RADIO (127), que corresponde a la información de capa de

enlace Radiotap[35] seguido de un encabezado 802.11; porque Snort no provee un decodificador para ello (figura 40).

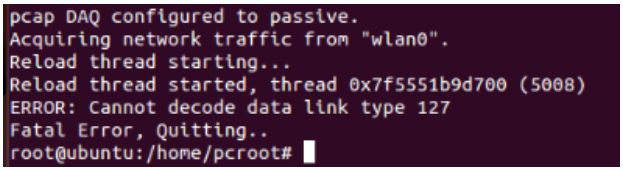


Figura 40. Problemas de decodificación en Snort con la tarjeta inalámbrica en modo monitor

Elaborado por: Autora del Proyecto

Por consiguiente su ubicación será entre el FortiAP y el FortiGate; para poder observar el tráfico que transita gracias al port mirroring. Se ejecutó los siguientes comandos para la generación del replicado de puertos:

Switch# configure terminal

Switch# monitor session 1 source interface Fa0/2

Switch# monitor session 1 destination interface Fa0/3

Para poder comprobar la configuración se ejecuta *show monitor* y desplegará un resultado similar a la figura 41.

[35] **Radiotap:** es un estándar de facto de frame 802.11 de inyección y recepción.

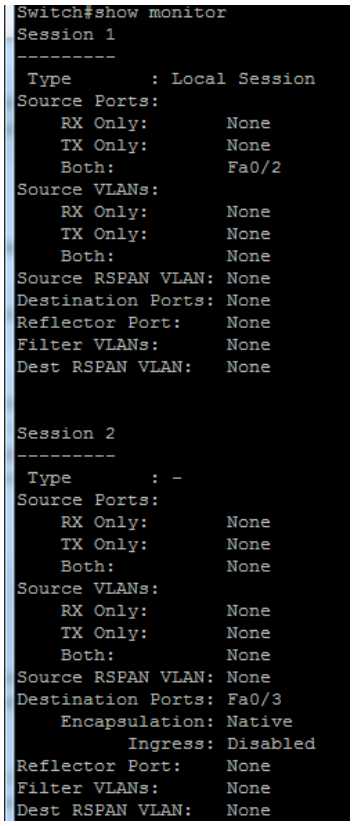


Figura 41. Comprobación de la configuración de Port Mirroring Switch Cisco

Elaborado por: Autora del Proyecto

Una vez culminada la preparación del escenario, se define las siguientes tablas con la información de direccionamiento:

Tabla 35. Direccionamiento IP del FortiGate

Direccionamiento IP del Fortigate		
Interfaz	**Dirección/Máscara**	**Descripción**
Wan1	200.31.26.154/255.255.255.248	Salida hacia el internet de la red de Gerencia.
port1	10.200.11.2/255.255.255.248	Salida hacia el internet controlada por el firewall checkpoint del resto de SSIDs.
port1 IP Secundaria	10.200.11.3/255.255.255.248	Salida hacia el internet controlada por el firewall checkpoint para la red acceso_invitados
port2	10.200.10.2/255.255.255.252	Puerto de acceso a la red LAN, para los SSIDs que así lo necesiten.
Virtual10	172.16.10.1 / 255.255.255.0	Acceso a la WLAN de Pruebas.
Otras Interfaces virtuales (TotalSSID=11)	172.16.0.1-172.16.0.9/255.255.255.0	Accesos a las diferentes WLANs configuradas según los perfiles y permisos necesarios solicitados; al fin de este proyecto existen 11 SSIDs.

Elaborado por: Autora del Proyecto

Tabla 36. Direccionamiento IP del FortiAP de Pruebas

Direccionamiento IP del FortiAP de pruebas		
Interfaz	**Dirección/Máscara**	**Descripción**
Eth0	10.1.5.130/255.255.255.0	IP asignada en la red 10.1.5.0/24 a través de la cual se une a la infraestructura de la red de la organización
SSID Pruebas	172.16.10.0/255.255.255.0	SSID Pruebas
Otros SSID	Usuarios _Gerencia 172.16.1.0/255.255.255.0 Usuarios_Informática 172.16.6.0/255.255.255.0 Usuarios_Internos 172.16.2.0/255.255.255.0	Otros SSIDs que también permiten el acceso autorizado el FortiAP de pruebas
Su Gateway en la red LAN		10.1.5.254
Su Fortigate configurado		10.200.10.2

Elaborado por: Autora del Proyecto

- **Generación de Ataques**

Para la generación de los ataques se utiliza Fern WiFi Cracker y Ettercap; el primero permite realizar varios ataques mencionados en el capítulo 2, con el objetivo principal de obtener las claves WPA y WEP; el segundo me permite realizar el ataque hombre en el medio con ARP Poisoning. En el siguiente proceso se describe la generación de ataques con Fern WiFi Cracker:

Se abre el terminal, se digita airmon-ng, a continuación se despliega las tarjetas inalámbricas que están conectadas y que permiten el funcionamiento en modo monitor; en este caso están las dos tarjetas descritas en los componentes de la topología. Aunque adicional se ejecutó un “iwlist wlan1scan” y un “iwlist wlan0 scan” para observar si salta algún problema adicional en las tarjetas (este comando hace un escaneo de redes con solicitudes probe).

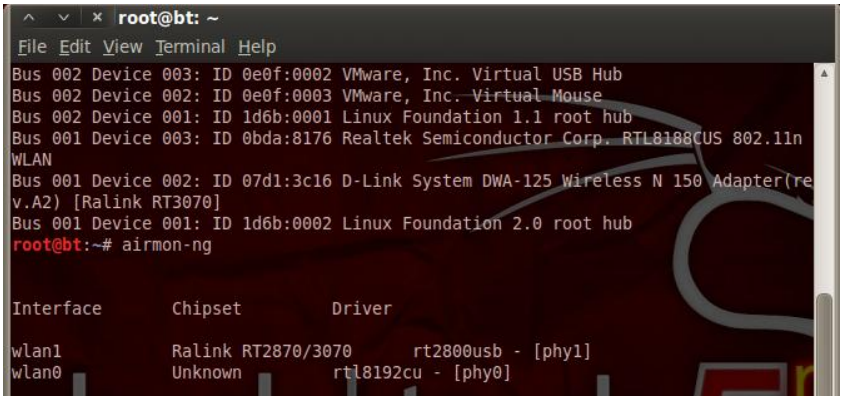


Figura 42. Ejecución del comando airmon-ng

Elaborado por: Autora del Proyecto

Se ingresa a *Applications/BackTrack/Exploitation Tools/Wireless Exploitation Tools/WLAN Exploitation/fern-wifi-cracker*; desplegando la ventana

principal de Fern WiFi Cracker en la cual se selecciona la tarjeta con la que se trabajará (wlan1), como muestra la figura 43.

Figura 43. Ventana Principal de Fern WiFi Cracker con la interfaz a trabajar
Elaborado por: Autora del Proyecto

Al seleccionar la interfaz la herramienta la coloca en modo monitor con airmon-ng, si es que aún no lo está; ahora se debe dar clic en el botón *Scan for Access points*; inmediatamente la herramienta procede a detectar los beacons de las WLAN cercanas (ataques de vigilancia-eavesdropping-sniffing).

Figura 44. Redes detectadas configuradas tanto con WEP como WPA

Elaborado por: Autora del Proyecto

Se da clic en el botón WiFi WPA para desplegar el listado de redes detectadas y seleccionar nuestro SSID de pruebas, figura 45.

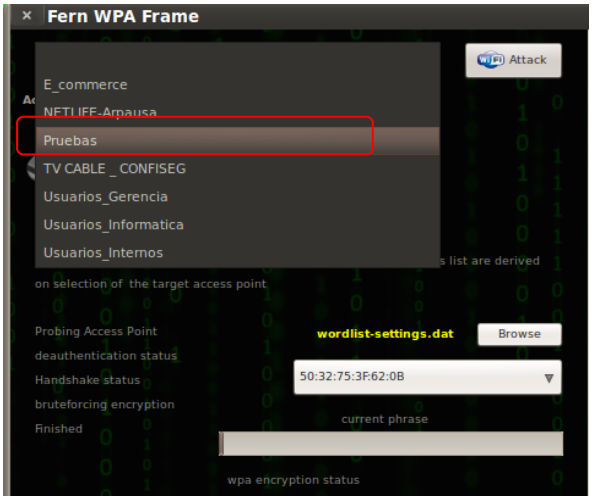


Figura 45. Selección del SSID de Pruebas dentro de la lista de SSIDs detectados por Fern WiFi Cracker

Elaborado por: Autora del Proyecto

Una vez que se ha seleccionado el SSID de pruebas, se despliega en la ventana información sobre el nombre de ESSID, la MAC del BSSID, el canal, potencia y tipo de cifrado (información encerrada en naranja en la figura 5.12); en la parte inferior de la ventana están paso a paso el proceso que la herramienta llevará a cabo para obtener la clave WPA. Se necesita seleccionar un diccionario con el que intentará adivinar la clave, en este caso se utiliza uno propio de la herramienta, dando clic en Browse (botón encerrado en color rojo de la figura 46) y se ingresa al directorio *Fyle System/pentest/passwords/wordlists/*, se escoge rockyou.txt y se da clic en open, figura 47.

Figura 46. Despliegue de la información del SSID Pruebas a través de Fern WiFi Cracker

Elaborado por: Autora del Proyecto

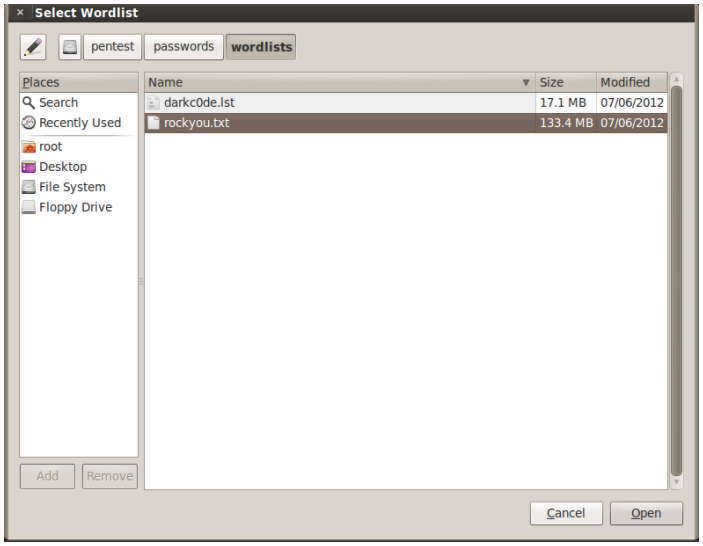


Figura 47. Selección de un diccionario en Fern WiFi Cracker

Elaborado por: Autora del Proyecto

Adicional la herramienta necesita al menos un cliente conectado al SSID objetivo, captura las tramas probe u otros tipos de tramas hacia el punto de acceso que le permita definir una víctima, procede a , desautenticarlo (DoS Deauth), esperar que nuevamente intente conectarse al SSID y así capturar el intercambio de información inicial entre el AP y el cliente “handshake”; por último con esta información proceder a enviar tramas de autenticación con claves provenientes del diccionario (ataque de diccionario), intentando adivinar la clave. En este caso se observa que usa al cliente B (00:21:6B:32:DB:C2).

Figura 48. Ataque de diccionario en proceso en Fern WiFi Cracker hacia la WLAN "Pruebas" a través del Cliente B

Elaborado por: Autora del Proyecto

Lastimosamente el ataque no pudo cumplir su acometido debido a que el diccionario que proporciona Backtrack no poseía la clave configurada; evidenciando la dependencia al uso de un potente diccionario; de preferencia armado a la medida con posibles claves afines (Nombre de la organización, fechas fines, etc).

Ahora se procede a detallar la generación de ataques con Ettercap:

Se ingresa al directorio *Applications/Privilege Escalation/Protocol Analysis/Network sniffers/Ettercap-gtk*; se ejecutará la ventana de Ettercap, se ingresa a la opción *Sniff/Unified Sniffing.*

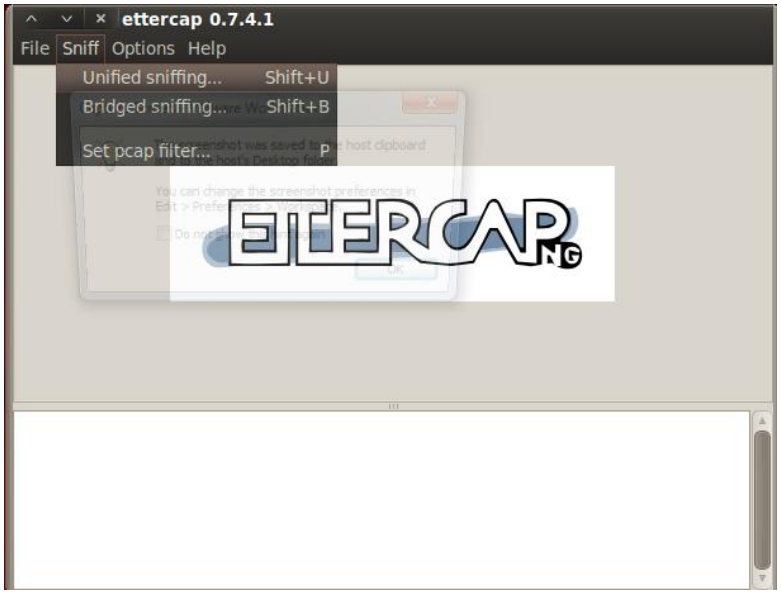


Figura 49. Ventana de Ettercap

Elaborado por: Autora del Proyecto

Luego se despliega un cuadro de diálogo que pide el ingreso de la interfaz de red con la que se trabajará, en este caso se hace uso de la wlan0 que corresponde a la tarjeta Realtek RTL8192CU, se procede a escanear los equipos en la red “host list” y se selecciona los objetivos para proceder con el menú *Mitm/Arp poisoning*.

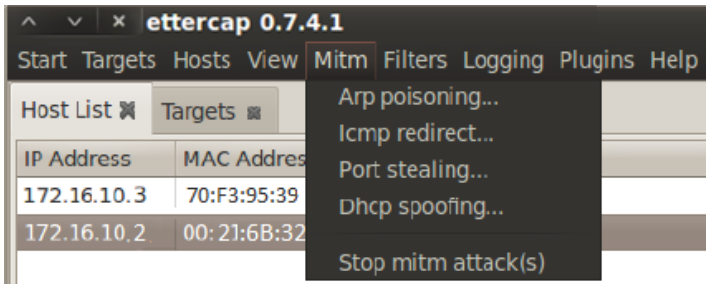


Figura 50. Ataque Hombre en el Medio a través de Ettercap

Elaborado por: Autora del Proyecto

Por último se puede comprobar el éxito del ataque a través de la revisión de las tablas ARP del cliente A (IP=172.16.10.2, MAC=70:F3:95:39:A4:97) y B (IP=172.16.10.3, MAC=00:21:6B:32:DB:C2); que deben tener respectivamente la MAC del atacante (48:02:2A:6F:FE:B5).

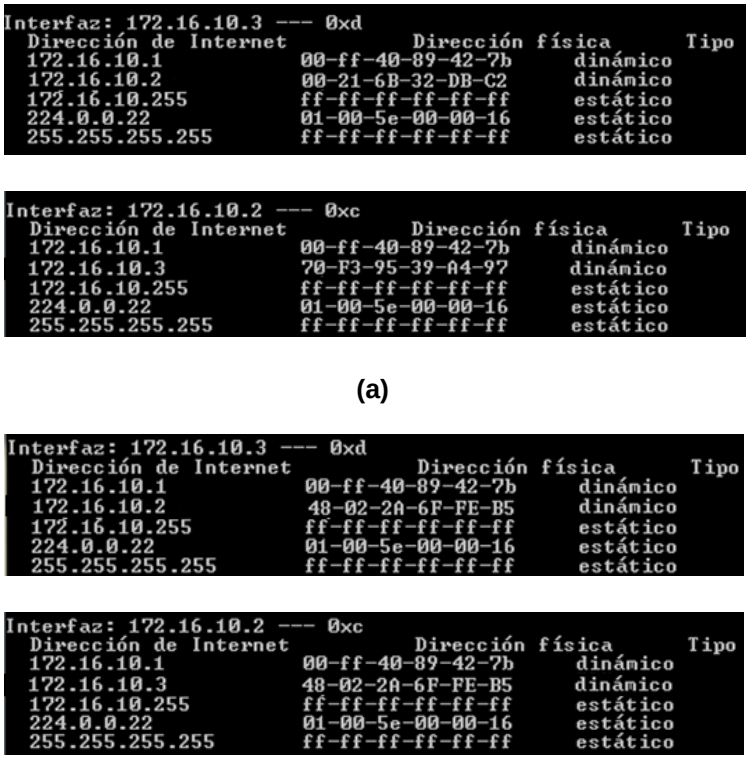


Figura 51. (a) Tabla ARP Cliente A y B antes del ataque MITM (b) Tablas ARP Cliente Ay B después del ataque MITM

Elaborado por: Autora del Proyecto

5.1.2. Resultados y Alarmas emitidas en Snort

Al ingresar a la página de snortreport lastimosamente no se generó ningún tipo de alerta durante la realización de los ataques, en la figura 52 se refleja el reporte vacío, y no existe ninguna gráfica a través de jpgraph (No Data), pues

no existe ninguna alerta como para un análisis de porcentajes en un gráfico circular.

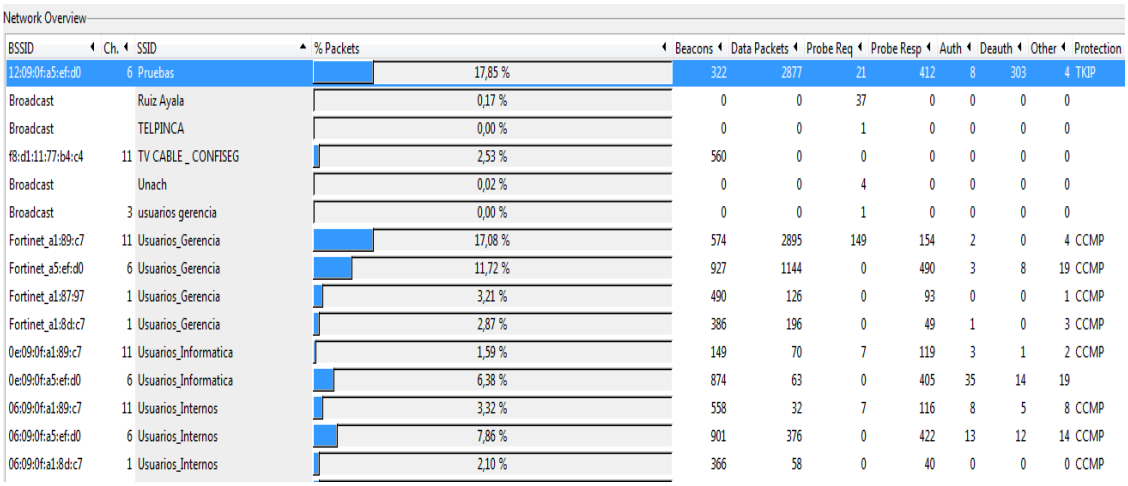
Figura 52. Página de SnortReport

Elaborado por: Autora del Proyecto

5.1.3. Resultados y Alarmas emitidas en Kismet

- **Frente a los ataques con Fern WiFi Cracker**

Kismet en ejecución genera archivos .pcapdump, .alert, .gpsxml, .nettxt, y .netxml, de los cuales principalmente de los tipos alert y pcapdump; se puede apreciar la reacción de la herramienta. Del archivo generado por la herramienta con el nombre Kismet-2013-12-04-09-59-09-1.pcapdump (11.7Mb) se obtiene los siguientes resultados:

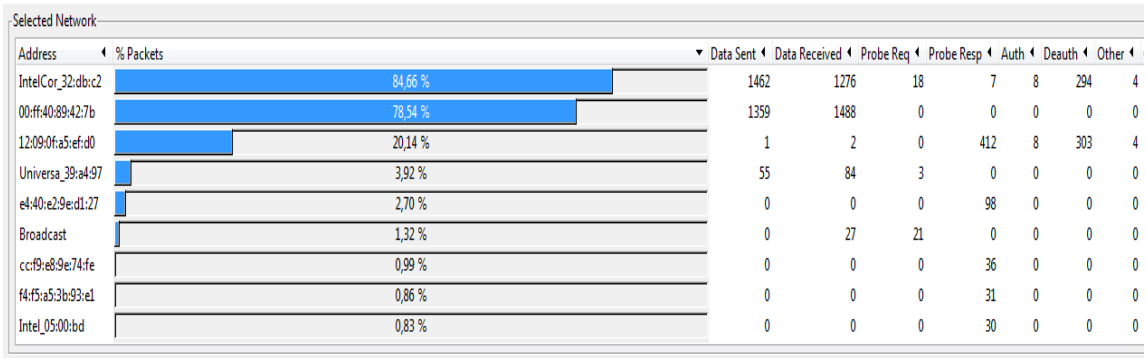


Network Overview

BSSID	Ch.	SSID	% Packets	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other	Protection
12:09:0f:a5:ef:d0	6	Pruebas	17,85 %	322	2877	21	412	8	303	4	TKIP
Broadcast		Ruiz Ayala	0,17 %	0	0	37	0	0	0	0	
Broadcast		TELPINCA	0,00 %	0	0	1	0	0	0	0	
f8:d1:11:77:b4:c4	11	TV CABLE _ CONFISEG	2,53 %	560	0	0	0	0	0	0	
Broadcast		Unach	0,02 %	0	0	4	0	0	0	0	
Broadcast	3	usuarios gerencia	0,00 %	0	0	1	0	0	0	0	
Fortinet_a1:89:c7	11	Usuarios_Gerencia	17,08 %	574	2895	149	154	2	0	4	CCMP
Fortinet_a5:ef:d0	6	Usuarios_Gerencia	11,72 %	927	1144	0	490	3	8	19	CCMP
Fortinet_a1:87:97	1	Usuarios_Gerencia	3,21 %	490	126	0	93	0	0	1	CCMP
Fortinet_a1:8d:c7	1	Usuarios_Gerencia	2,87 %	386	196	0	49	1	0	3	CCMP
0e:09:0f:a1:89:c7	11	Usuarios_Informatica	1,59 %	149	70	7	119	3	1	2	CCMP
0e:09:0f:a5:ef:d0	6	Usuarios_Informatica	6,38 %	874	63	0	405	35	14	19	
06:09:0f:a1:89:c7	11	Usuarios_Internos	3,32 %	558	32	7	116	8	5	8	CCMP
06:09:0f:a5:ef:d0	6	Usuarios_Internos	7,86 %	901	376	0	422	13	12	14	CCMP
06:09:0f:a1:8d:c7	1	Usuarios_Internos	2,10 %	366	58	0	40	0	0	0	CCMP

Figura 53. Porcentajes del tráfico total recolectado en el archivo pcapdump correspondientes a cada SSID en el medio

Elaborado por: Autora del Proyecto



Selected Network

Address	% Packets	Data Sent	Data Received	Probe Req	Probe Resp	Auth	Deauth	Other
IntelCor_32:db:c2	84,66 %	1462	1276	18	7	8	294	4
00:ff:40:89:42:7b	78,54 %	1359	1488	0	0	0	0	0
12:09:0f:a5:ef:d0	20,14 %	1	2	0	412	8	303	4
Universa_39:a4:97	3,92 %	55	84	3	0	0	0	0
e4:40:e2:9e:d1:27	2,70 %	0	0	0	98	0	0	0
Broadcast	1,32 %	0	27	21	0	0	0	0
cc:f9:e8:9e:74:fe	0,99 %	0	0	0	36	0	0	0
f4:f5:a5:3b:93:e1	0,86 %	0	0	0	31	0	0	0
Intel_05:00:bd	0,83 %	0	0	0	30	0	0	0

Figura 54. Porcentajes de tráfico generados dentro de la WLAN "Pruebas" según participación de los clientes

Elaborado por: Autora del Proyecto

Gracias a Wireshark en su opción *Statistics/WLAN Traffic*, se puede apreciar los porcentajes de tráfico recolectados en un intervalo de ocho minutos, en la figura 53 se puede observar que un 17,85% del tráfico pertenece al SSID de pruebas, destacando la gran cantidad de tramas de desautenticación (303), que resalta frente al resto de SSIDs. Por otro lado se puede apreciar que dentro del SSID de interés (figura 54) los que generan

mayor tráfico son la MAC del AP (00:FF:40:89:42:7B) con un 78,54%, la MAC del BSSID(12:09:0F:A5:EF:D0) con un 20,14% y la MAC de nuestro cliente B atacado(00:21:6B:32:DB:C2) con un 84,66%; porcentajes que pertenecen a su partición en los diferentes tipos de tramas de datos (tomando el papel de destino u origen). Adicional se generó un archivo .alert con un total de 11 alertas, de las cuales 5 corresponden a nuestro SSID Pruebas (color celeste), como se indica en la tabla 37.

Tabla 37. Alertas generadas por Kismet

Día	Hora	Año	Descripción de la alerta
Wed Dec 4	09:59:02	2013	PROBENOJOIN Suspicious client 1C:AF:F7:73:C7:6D probing networks but never joining
Wed Dec 4	10:00:20	2013	DEAUTHFLOOD 0 12:09:0F:A5:EF:D0 00:21:6B:32:DB:C2 12:09:0F:A5:EF:D0 Deauthenticate flood on Network BSSID 12:09:0F:A5:EF:D0
Wed Dec 4	10:00:27	2013	ADHOCCONFLICT 0 0E:09:0F:A5:EF:D0 00:19:D2:05:00:BD 0E:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 0E:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:00:43	2013	ADHOCCONFLICT 0 0E:09:0F:A5:EF:D0 00:19:D2:05:00:BD 0E:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 0E:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:01:00	2013	ADHOCCONFLICT 0 0E:09:0F:A5:EF:D0 00:19:D2:05:00:BD 0E:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 0E:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:03:12	2013	ADHOCCONFLICT 0 06:09:0F:A1:89:C7 00:19:D2:05:00:BD 06:09:0F:A1:89:C7 00:00:00:00:00:00 Network BSSID 06:09:0F:A1:89:C7 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:03:29	2013	ADHOCCONFLICT 0 0E:09:0F:A1:89:C7 00:19:D2:05:00:BD 0E:09:0F:A1:89:C7 00:00:00:00:00:00 Network BSSID 0E:09:0F:A1:89:C7 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:04:02	2013	ADHOCCONFLICT 0 06:09:0F:A5:EF:D0 00:19:D2:05:00:BD 06:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 06:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:05:02	2013	ADHOCCONFLICT 0 12:09:0F:A5:EF:D0 00:21:6B:32:DB:C2 12:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 12:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:05:32	2013	ADHOCCONFLICT 0 12:09:0F:A5:EF:D0 00:21:6B:32:DB:C2 12:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 12:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	10:05:33	2013	DEAUTHFLOOD 0 12:09:0F:A5:EF:D0 00:21:6B:32:DB:C2 12:09:0F:A5:EF:D0 Deauthenticate flood on Network BSSID 12:09:0F:A5:EF:D0

Elaborado por: Autora del Proyecto

Debido a que la NIC inalámbrica que usa Kismet no permite la eliminación de salto de canal para que solo trabaje en el canal de “Pruebas”, el IDS evalúa el tráfico que pasa por los SSIDs que están bajo su alcance.

- **Frente a los ataques con Ettercap**

Lastimosamente no existió evidencia ni en la captura de tráfico ni alerta acerca del ataque provocado por Ettercap; adicional sólo generó alertas con respecto a otros SSIDs.

Tabla 38. Alertas Generadas mientras Ettercap atacaba

Día	Hora	Año	Descripción de la alerta
Wed Dec 4	14:00:57	2013	ADHOCCONFLICT 0 06:09:0F:A5:EF:D0 00:19:D2:05:00:BD 06:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 06:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	14:03:23	2013	ADHOCCONFLICT 0 0E:09:0F:A5:EF:D0 00:19:D2:05:00:BD 0E:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 0E:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	14:07:02	2013	ADHOCCONFLICT 0 06:09:0F:A5:EF:D0 00:19:D2:05:00:BD 06:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 06:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation
Wed Dec 4	14:38:39	2013	ADHOCCONFLICT 0 06:09:0F:A5:EF:D0 00:19:D2:05:00:BD 06:09:0F:A5:EF:D0 00:00:00:00:00:00 Network BSSID 06:09:0F:A5:EF:D0 advertised as AP network, now advertising as Ad-Hoc IBSS, which may indicate AP spoofing/impersonation

Elaborado por: Autora del Proyecto

5.2. Análisis de Resultados

5.2.1. Análisis de Datos Obtenidos a través de Snort

Lastimosamente Snort se encuentra en una posición dificultosa para observar los ataques generados en el medio inalámbrico; en los casos como detección de tarjetas inalámbricas intrusas en modo monitor, no puede apreciar el ataque con flujo de desautenticación, ni mucho menos el ataque ARP Poisoning para obtener una posición man in the middle del atacante con Ettercap, debido a que el envenenamiento se realiza a los clientes, en ningún momento pasa por el enlace entre el FortiAP y el FortiGate. Lastimosamente

este IDS solo puede trabajar en esta posición que dificulta la detección de ataques en las capas física y de enlace de datos.

5.2.2. Análisis de Datos Obtenidos a través de Kismet

❖ **Análisis frente a los ataques con Fern WiFi Cracker**

En este punto es importante analizar las alertas que se han desprendido de la examinación de Kismet y el correspondiente tráfico generado:

- Como primer alerta corresponde un PROBENOJOIN, que indica la existencia de una NIC inalámbrica con comportamiento sospechoso por enviar constantemente “solicitudes Probe” y no se une a ningún SSID, cuya MAC corresponde a la utilizada en el ataque (1C:AF:F7:73:C7:6D); así se ubica como el primer verdadero positivo que emitió Kismet, que salta debido al iwlist que se ejecutó para comprobar la ejecución de la tarjeta.
- Como segunda alerta envía un DEAUTHFLOOD cuyo BSSID objetivo corresponde a Pruebas (12:09:0F:A5:EF:D0); la supuesta fuente el BSSID y el supuesto origen el cliente B. Bajo un análisis del tráfico con Wireshark se puede apreciar como la herramienta de ataque hace una DoS al cliente legítimo para poder capturar el handshake y mantenerlo desconectado; evitando interferencia del cliente legítimo. Pero no sólo envía desautenticación con origen el BSSID, también como origen el cliente B así se asegura aún más que cumplirá su acometido, ataque por el cual Kismet también emitió una alerta (tabla 37, última fila). En las figuras 55 y 56 se evidencia claramente lo mencionado gracias al flujo de comunicación,

incluso gracias a los porcentajes obtenidos en los resultados ya se apreciaba una gran cantidad de tráfico de tramas de desautenticación que daban sospecha de ataque (303 tramas deauth capturadas en el BSSID y 294 en el cliente B, de la información obtenida en la figura 54).

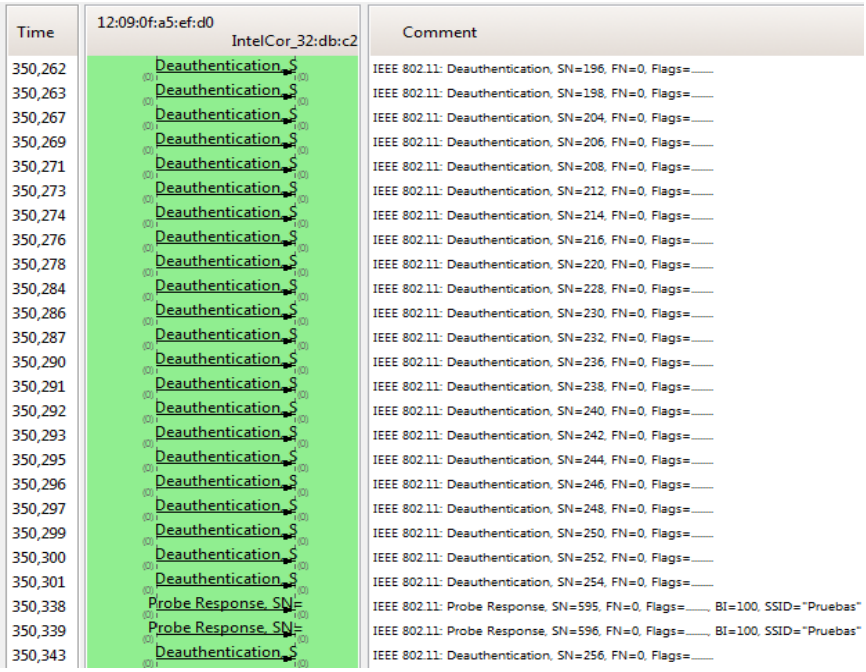
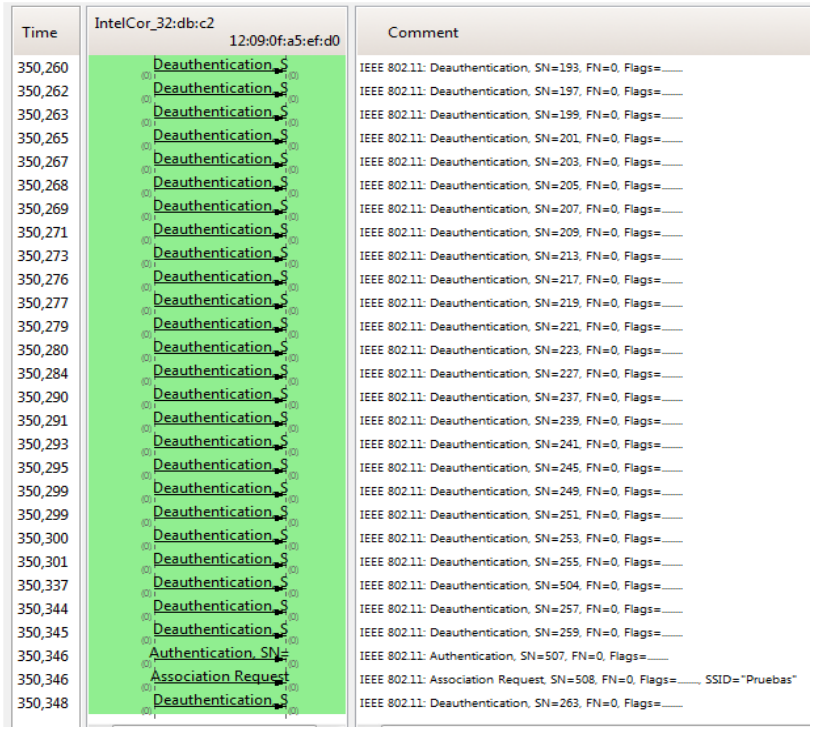


Figura 55. Flujo de Tramas desde el BSSID hacia el cliente B

Elaborado por: Autora del Proyecto



Time	IntelCor_32:db:c2 12:09:0f:a5:ef:d0	Comment
350,260	Deauthentication, S	IEEE 802.11: Deauthentication, SN=193, FN=0, Flags=.....
350,262	Deauthentication, S	IEEE 802.11: Deauthentication, SN=197, FN=0, Flags=.....
350,263	Deauthentication, S	IEEE 802.11: Deauthentication, SN=199, FN=0, Flags=.....
350,265	Deauthentication, S	IEEE 802.11: Deauthentication, SN=201, FN=0, Flags=.....
350,267	Deauthentication, S	IEEE 802.11: Deauthentication, SN=203, FN=0, Flags=.....
350,268	Deauthentication, S	IEEE 802.11: Deauthentication, SN=205, FN=0, Flags=.....
350,269	Deauthentication, S	IEEE 802.11: Deauthentication, SN=207, FN=0, Flags=.....
350,271	Deauthentication, S	IEEE 802.11: Deauthentication, SN=209, FN=0, Flags=.....
350,273	Deauthentication, S	IEEE 802.11: Deauthentication, SN=213, FN=0, Flags=.....
350,276	Deauthentication, S	IEEE 802.11: Deauthentication, SN=217, FN=0, Flags=.....
350,277	Deauthentication, S	IEEE 802.11: Deauthentication, SN=219, FN=0, Flags=.....
350,279	Deauthentication, S	IEEE 802.11: Deauthentication, SN=221, FN=0, Flags=.....
350,280	Deauthentication, S	IEEE 802.11: Deauthentication, SN=223, FN=0, Flags=.....
350,284	Deauthentication, S	IEEE 802.11: Deauthentication, SN=227, FN=0, Flags=.....
350,290	Deauthentication, S	IEEE 802.11: Deauthentication, SN=237, FN=0, Flags=.....
350,291	Deauthentication, S	IEEE 802.11: Deauthentication, SN=239, FN=0, Flags=.....
350,293	Deauthentication, S	IEEE 802.11: Deauthentication, SN=241, FN=0, Flags=.....
350,295	Deauthentication, S	IEEE 802.11: Deauthentication, SN=245, FN=0, Flags=.....
350,299	Deauthentication, S	IEEE 802.11: Deauthentication, SN=249, FN=0, Flags=.....
350,299	Deauthentication, S	IEEE 802.11: Deauthentication, SN=251, FN=0, Flags=.....
350,300	Deauthentication, S	IEEE 802.11: Deauthentication, SN=253, FN=0, Flags=.....
350,301	Deauthentication, S	IEEE 802.11: Deauthentication, SN=255, FN=0, Flags=.....
350,337	Deauthentication, S	IEEE 802.11: Deauthentication, SN=504, FN=0, Flags=.....
350,344	Deauthentication, S	IEEE 802.11: Deauthentication, SN=257, FN=0, Flags=.....
350,345	Deauthentication, S	IEEE 802.11: Deauthentication, SN=259, FN=0, Flags=.....
350,346	Authentication, SN=	IEEE 802.11: Authentication, SN=507, FN=0, Flags=.....
350,346	Association Request	IEEE 802.11: Association Request, SN=508, FN=0, Flags=....., SSID="Pruebas"
350,348	Deauthentication, S	IEEE 802.11: Deauthentication, SN=263, FN=0, Flags=.....

Figura 56. Flujo de tramas de desautenticación desde el cliente B hacia el BSSID y uno de los intentos de autenticación frente a los ataques de diccionario

Elaborado por: Autora del Proyecto

- Cuando logra desautenticar al cliente comienza el proceso del ataque de diccionario, mientras no logra autenticarse, mantiene desautenticado al cliente B originando tramas como las desglosadas en las figuras 57 y 58 (trama deauth por el valor hexadecimal 0x0C y tipo=0 que significa trama de control), tanto en el caso en que BSSID es fuente, el cliente B es destino y viceversa; expresando el mismo motivo de desautenticación (Reason Code: Class 3).

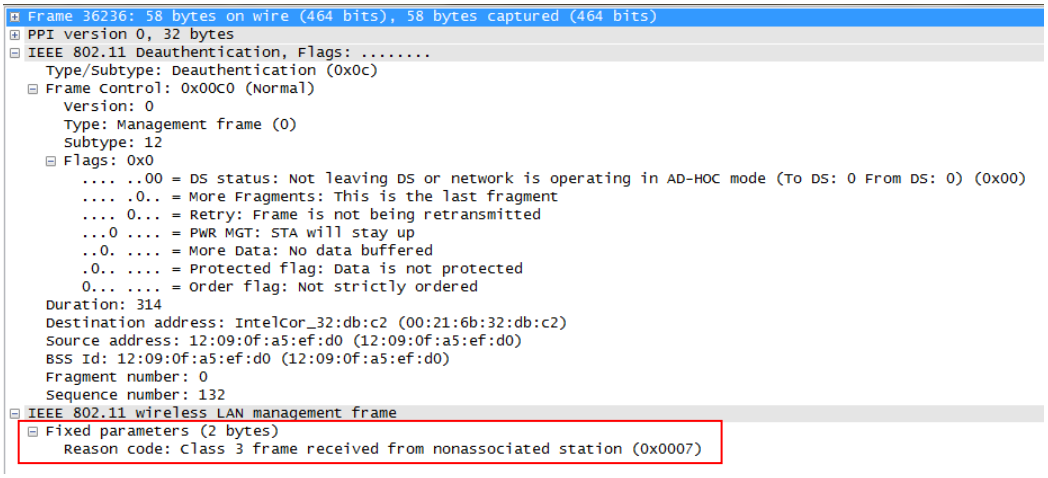


Figura 57. Trama DEAUTH desglosada con fuente BSSID y destino el cliente B

Elaborado por: Autora del Proyecto

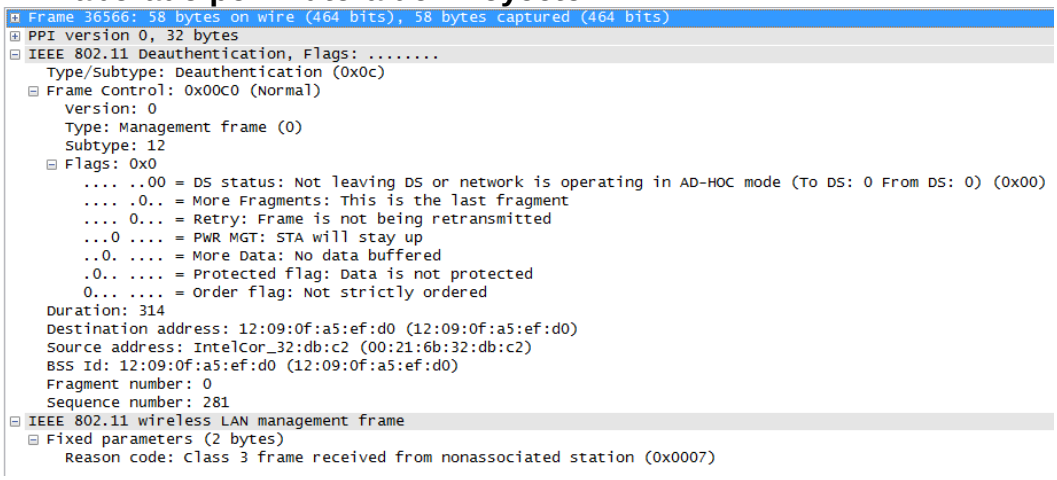


Figura 58. Trama DEAUTH desglosada con fuente cliente B y destino el BSSID

Elaborado por: Autora del Proyecto

- En cuestión de segundos se capturó tres intentos de autenticación que lastimosamente no provocaron algún tipo de alerta, específicamente indicando que se trata de un ataque de diccionario.

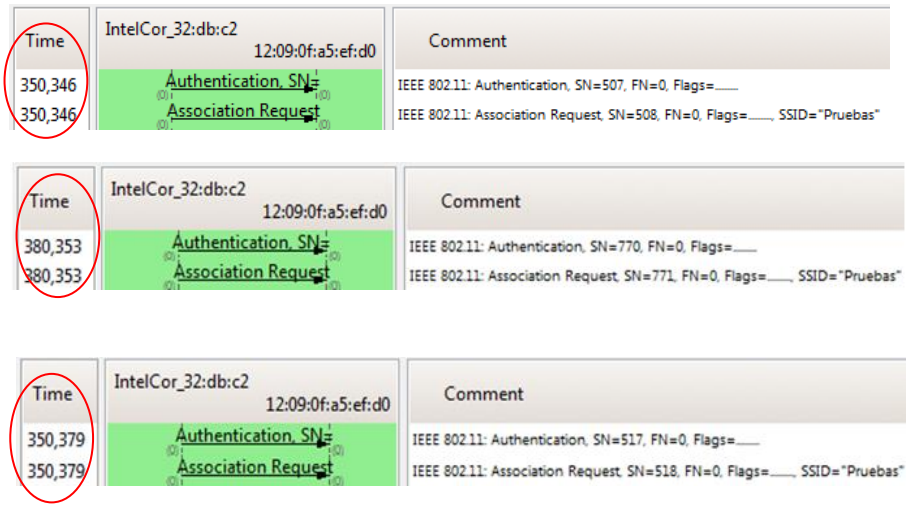


Figura 59. Intentos de autenticación durante el ataque de diccionario
Elaborado por: Autora del Proyecto

- Por último las dos alarmas correspondientes al SSID analizado, corresponde a una ADHOCCONFLICT, analizando la tramas a través de Wireshark se puede apreciar que el BSSID Pruebas envía “beacons” y “probe responses” con MAC del AP; pero al mismo tiempo en las banderas “To DS” y “From DS” poseen el valor 0, que significa una comunicación en red IBSS, pero esto es resultado de la existencia de un wireless controller; que posee las interfaces virtuales que corresponden a los SSIDs, proporcionando la verdadera conexión al DS y los FortiAP simplemente proporcionan la interfaz física.

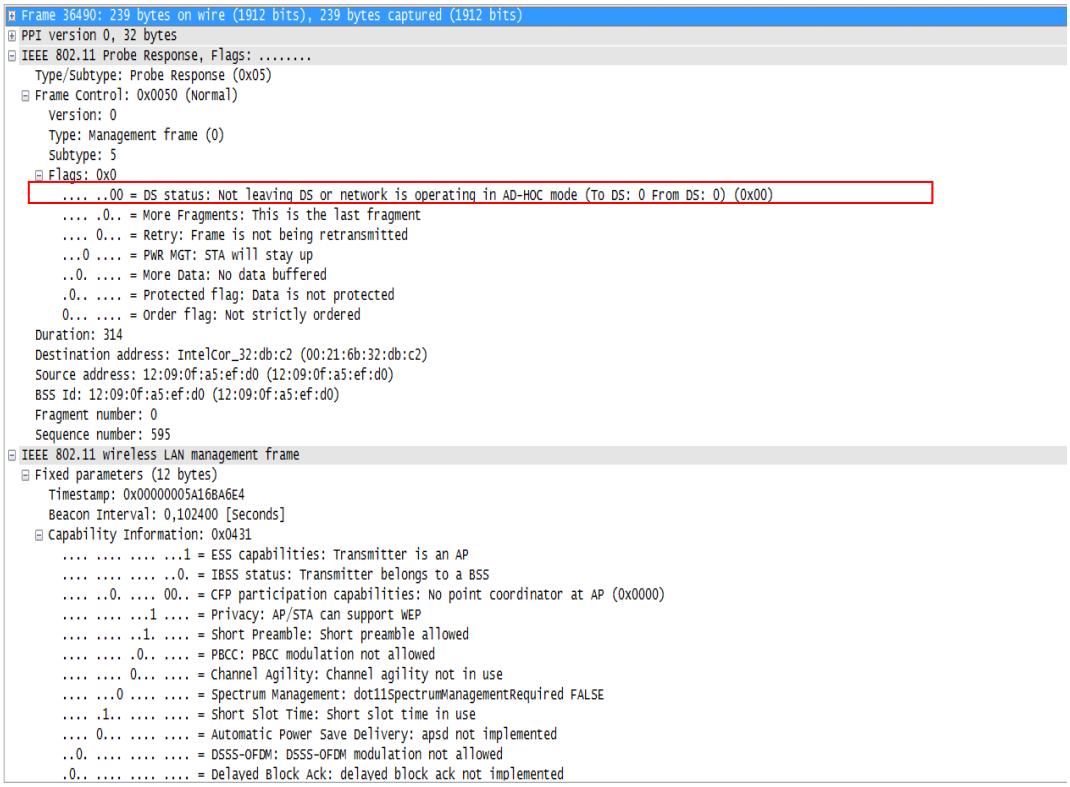


Figura 60. Probe Response enviado por el BSSID Pruebas

Elaborado por: Autora del Proyecto

- Por lo expuesto en el anterior párrafo, las alarmas emitidas en los demás SSIDs (tabla 38 y filas blancas en la tabla 37) se originan por el mismo hecho.

5.3. Determinación de Características de Respuesta de los IDSs

5.3.1. SNORT

A pesar de ser una herramienta ampliamente conocida, con numerosos preprocesadores y un motor de detección con una importante cantidad de firmas; ha llegado a especializarse más en los ataques en capas superiores; dejando de lado esta importante área como son las redes inalámbricas, para las cuales según los resultados y su respectivo análisis permiten determinar que la

calidad de respuesta frente ataques en WLANs es pésimo (no generó ninguna alarma).

5.3.2. KISMET

De un total de 15 alarmas emitidas que se puede apreciar en los resultados; 5 correspondieron al SSID Pruebas; luego del análisis se determinó que 3 alertaron según los ataques que se realizaron (DEAUTHFLOOD y PROBENOJOIN), lo que viene a ser los verdaderos positivos y 2 alertaron sobre un posible AP Spoofing, que más bien corresponde al comportamiento normal de la comunicación usando el FortiGate como controlador inalámbrico, por lo tanto representa 2 falsos positivos. En consecuencia se determina que un 60% de las alertas emitidas son acertadas y un 40% falsas alertas, porcentajes aceptables de respuesta.

- Kismet lastimosamente no emitió reacción alguna frente a los ataques de ARP Poisoning que se llevaron a cabo con objeto de obtener un ataque Man in the Middle con Ettercap, lastimosamente cae en falsos negativos.
- Según se puede apreciar en los tiempos de emisión de las alarmas existió una respuesta rápida, los ataques se llevaban a cabo y casi inmediatamente alertó sobre lo que consideró como ataque.
- Kismet adicional a la generación de alarmas aporta con archivos .pcapdump, en donde claramente se aprecia; correlacionando según el tiempo indicado en las tramas capturadas y la hora indicada en las alertas en el archivo .alert, el tráfico anómalo.
- Las alertas tienen un formato claro y muy conciso de lo que está ocurriendo, lo que proporciona una visión clara (Hora, Día, Año, BSSID, Tipo de Alerta,

Dirección MAC Destino, Dirección MAC Fuente y una corta descripción de lo que supuestamente puede estar sucediendo) al administrador de la herramienta, se puede obtener una visión más profunda tras el análisis del tráfico.

CAPÍTULO 6

MEDIDAS MÍNIMAS DE SEGURIDAD EN WI FI

Gracias a las pruebas realizadas en aquel escenario en producción, se deja al descubierto ciertas vulnerabilidades que se debe tomar en cuenta al momento de trabajar con redes inalámbricas 802.11, de ahí que se obtuvo importantes recomendaciones de seguridad que permitan lograr un entorno seguro.

Mientras los miembros de una organización no procuren desarrollar un conjunto de políticas de seguridad inalámbrica, capacitaciones del buen uso de una WLAN; no sólo a nivel cliente sino también administrativo de la red; seguirán apareciendo falencias en cualquier tipo de auditoría, adicional a ser fáciles víctimas frente a los ataques informáticos.

En ciertos ambientes laborales lo que antes era una recomendación de seguridad ahora se ha convertido en una obligación para todos quienes conforman el mismo, conscientes de que la seguridad de la información es un tema en el que están involucrados todos.

5.1. Medidas mínimas de seguridad recomendadas gracias a los resultados obtenidos en el transcurso del proyecto.

5.1.1. Recomendaciones para los Clientes de la WLAN

Los clientes de la WLAN como beneficiados de la comodidad de la misma, tienen que tomar conciencia que una mala práctica suya puede ser aprovechada en contra de la seguridad de la organización:

- Es importante que el cliente tenga un antivirus y firewall, debidamente instalados y actualizados.
- Tener un usuario y contraseña de ingreso a su sesión en cualquier sistema operativo; por ejemplo en el caso de Windows, si alguien ajeno logra acceder a una sesión legítima puede observar en la ventana de “Administrar Redes Inalámbricas”, todas los SSIDs y claves a los que tiene acceso, incluso no sólo esa información sino cualquier otra información y más crítica.

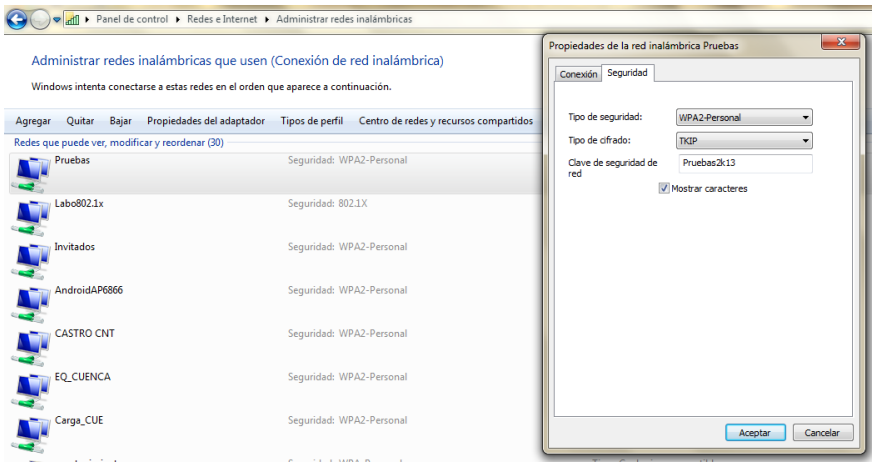


Figura 61. Administrador de Redes Inalámbricas de Windows7

Elaborado por: Autora del Proyecto

- Si presenta algún tipo de intermitencia en la conexión o desconexión total de la WLAN, en una ubicación donde antes si tenía el servicio sin inconvenientes reportar brevemente al área de soporte, para que revisen si no está siendo víctima de algún ataque.
- No tener anotado en lugares visibles para los ajenos la clave de acceso inalámbrico; es recomendable memorizarla, aunque en los actuales sistemas operativos las claves quedan almacenadas.

5.1.2. Recomendaciones para los AP

La configuración, ubicación y mantenimiento de estos equipos es un factor muy importante; porque ellos son la interfaz hacia el DS y con esto los hackers se darán la manera de seguir escalando privilegios dentro de la red:

- Deben ubicarse en un sitio donde no se encuentre algún tipo de equipo que sea fuente de interferencia. Si en su ubicación de siempre está presentando problemas de cobertura revisar nuevas fuentes de interferencia, el hardware del equipo ó simplemente es víctima de una ataque de interferencia.
- El AP debe encontrarse fuera del alcance de los usuarios, para evitar movimiento accidental o provocado de cables, desconexiones, etc. Además algunos modelos de estos equipos poseen puertos de administración (como el puerto de consola en los FortiAPs), en los que un descuido se pueden conectar los atacantes.

5.1.3. Recomendaciones para el Controlador Inalámbrico

Es importante tomar en cuenta las siguientes recomendaciones, principalmente porque aquí radica la configuración de los SSIDs y las distintas rutas a las que se podrán administrar el acceso:

- Cuando se posee este tipo de topología se posee un importante agregado de seguridad, no cualquier AP se podrá conectar a la red, porque primero debe ser autorizado, registrado y configurado en el controlador. Es por esto que cabe recomendar que la configuración en este equipo deba ser muy cautelosa y sobre todo conforme a las políticas de seguridad y acceso de la organización.
- Es recomendable que en la configuración del protocolo de seguridad, mínimo se use WPA; aunque en el FortiGate, simplemente WEP ya si siquiera se incluye como opción; adicional para el caso particular de WPA TKIP se use una clave de mínimo unos 10 a 15 caracteres alfanuméricos, entre mayúsculas y minúsculas; incluso en otros manuales de recomendaciones indican 20 caracteres (Telefonía Movistar).
- Es recomendable configurar un número máximo de intentos de autenticación, mínimo tres; para así conseguir que los ataques de diccionario tengan menos probabilidad de obtener su objetivo; para el caso específico del escenario de pruebas quedó al descubierto esta vulnerabilidad.
- Implementar filtrado por MAC, evitando DHCP; aunque existen ataques contra esta medida, le dará un obstáculo más al atacante; en los casos

como el escenario de pruebas la gran cantidad de usuarios y cambio en sus equipos dificulta este tipo de implementación, por lo que se recomienda la entrega de claves con acuerdo de confidencialidad con los clientes y de ser posible implementar un servidor RADIUS.

- Es recomendable cambiar constantemente la clave compartida y para este caso informar a los usuarios involucrados.

CAPÍTULO 7

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Los protocolos de Seguridad Wi Fi, intentan solventar las falencias que aprovechan los atacantes; enfocando sus esfuerzos principalmente: en una autenticación segura tanto para el autenticador como el autenticado, comprobar si verdaderamente la información no ha sido falsificada, alterada ó cambiada, a través de métodos de chequeo de integridad y finalmente obtener un cifrado fuerte; para que a pesar de transportarse por un medio sensible a espías, no les sirva de mucho interceptar el tráfico.
- Las técnicas de ataque enfocadas hacia las redes inalámbricas, apuntan sus esfuerzos principalmente a la capa física y de enlace de datos, porque las circunstancias favorecen este hecho; los atacantes no van más allá en las capas superiores de la arquitectura de red, si pueden aprovechar capas inferiores frágiles.
- La efectividad del ataque está principalmente en la cantidad y calidad de tráfico que se ha logrado capturar, y los campos clave en las tramas que se consigue interpretar y descifrar.
- Los Benchmarks han venido a ser parte importante de la seguridad informática, porque sin sus metodologías no se hubiera logrado elaborar

las grandes herramientas que permiten evaluar la efectividad de los sistemas; principalmente en este proyecto permitieron dejar al descubierto una importante cantidad de resultados por parte de los IDSs, facilitando una visión más clara de la calidad de reacción.

- Tanto el instrumento de evaluación Backtrack; como los evaluados sistemas de detección de intrusos principalmente kismet, presentaron ventajas y desventajas que destacaron a la vista de este proyecto, por su lado Backtrack es un sistema con un importante número de herramientas de ataque en redes inalámbricas; incluso con amigables interfaces como Fern WiFi Cracker y Ettercap, que facilitan aún más el accionar de los atacantes; claro que con un punto débil en el primero; porque está atado a un buen diccionario para conseguir la obtención de la clave WPA, por su lado kismet alertó del comportamiento anómalo que se generaba con Fern casi en el acto; pero lamentablemente no pudo definir alertas para el resto de ataques efectuados (ataques con Ettercap y diccionario).
- Kismet generó algunos tipos de archivos durante su ejecución, pero principalmente generó un importante cantidad de alertas y captura de tráfico, así se obtuvo un 60% de verdaderos positivos y un 40% de falsos negativos, porcentaje aceptable de detección.
- Snort lastimosamente no presentó reacción alguna frente a los ataques, la falta de un procesador adecuado para la interpretación de la información proporcionada por la NIC inalámbrica en modo monitor, determinó su posición entre el fortiAP y el Wireless Controller para la

intercepción del tráfico, incluso en esa posición no logró resultados; justificable en los ataques que no necesariamente iban dirigidos al FortiAP; pero en el caso del ataque de diccionario debía al menos identificar, que existía un exceso de peticiones de autenticación hacia el controlador.

- Existió una rápida respuesta en ejecución por parte de Kismet, reacción que claramente se puede apreciar después del posterior análisis del tráfico capturado y las alertas; de lo cual se puede determinar que la cantidad de preprocesadores y firmas dificulta el rendimiento de un IDS por el consumo de procesamiento que conlleva; pues Kismet no se compara con la gran cantidad de los mismos que posee Snort, es más liviano y de rápida reacción frente a lo que reconoce como anómalo.

6.2. RECOMENDACIONES

- Es recomendable tener definido políticas de seguridad relacionadas con el área inalámbrica, sea cual sea la organización, desde un hogar hasta una multinacional; un uso responsable de las mismas permitirá seguir disfrutando de la comodidad de las redes inalámbricas de una manera segura.
- Es recomendable trabajar con tarjetas inalámbricas que permitan la inhabilitación del salto canal; para así evitar que en el caso del IDS, tenga que ir analizando canal por canal; cuando puede enfocarse de mejor manera en un solo objetivo y no demorar la detección.

- A pesar de poseer una topología de red Controlador inalámbrico más APs legítimos, es recomendable analizar, revisar y ejecutar pruebas de la configuración. En el escenario quedó claramente al descubierto la falta de un número de intentos de autenticación; que eviten los ataques de fuerza bruta ó de diccionario.
- Un filtrado MAC en organizaciones como las del escenario de pruebas; no es una medida óptima por la cantidad de usuarios y cambios que podrían suscitarse, por esto se recomienda el uso de un servidor de autenticación como el caso de RADIUS.
- Es recomendable utilizar un equipo con excelentes características de hardware para contener un IDS; no es suficiente con los requisitos mínimos de la herramienta, pues con un escenario con una alta densidad de tráfico fluyendo, genera gran cantidad de información; que necesita ser procesada para determinar alarmas, por esta razón podría generarse inhibición y obstrucción de servicio del IDS; ó simplemente descarte de paquetes.
- Se recomienda la utilización de Snort y Kismet, cooperando mutuamente gracias a las interfaces virtuales TUN/TAP presentes en Kismet, en pruebas futuras, para así fusionar características, que permitirán a Kismet aumentar su detección de ataques en capas superiores de la arquitectura de red, y a Snort solventar sus falencias en detección de ataques en el medio inalámbrico.

- Se recomienda la ejecución de pruebas con las múltiples herramientas existentes, principalmente de software libre; para poder determinar tanto la eficiencia del funcionamiento de los sistemas de ataque y seguir dejando al descubierto más vulnerabilidades de los IDSs usados en este proyecto; para así contribuir a su mejora continua para que sigan manteniéndose dentro de las herramientas reconocidas de seguridad informática.

BIBLIOGRAFÍA

- Aguilera, P. (2010). *Seguridad Informática.* España: Editex S.A.
- Ali, S., & Heriyanto, T. (2011). *Backtrack 4: Assuring Security by Penetration Testing. .* Reino Unido: Packt Publishing Ltd.
- Back|track-linux. org. (2013). *BackTrack Linux-Pentration Testing Distribution*. Recuperado el 31 de noviembre de 2013, de http://www.backtrack-linux.org/.
- Caizapanta, A. (2013). Implementación de un escenario de prueba para el análisis de vulnerabilidad en redes (Tesis de grado). *Escuela Politeécnica del Ejército*. Sangolquí, Ecuador.
- Facua org. (2011). *SPAN qué es y cómo efrentrte a él*. Recuperado el 23 de septiembre de 2013, de http://www.facua.org/es/guias/guia141.pdf
- Giménez, M. (2008). *Utilización de Siatemas de Detéccion de Intrusos como elemento de seguridad perimetral*. Recuperado el 7 de septiembre de 2013, de http://www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf
- Group Cyber System and Technology. (2013). *DARP Intrusion Detection Data Sets*. Recuperado el 16 de noviembre de 2013, de Lincoln Laboratory of Massachusetts Institute of Technology: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html
- GSyC. (2012). *IEE 802.11.* Recuperado el 4 de febrero de 2013, de http://gsyc.es/~mortuno/rom/02-802.11.pdf
- Gullett. (2012). *Snort 2.9.3 and Snort Repot 1.3.3 on Ubunto12.04 LTS Installation Guide*. Recuperado el 24 de noviembre de 2013, de http://www.snort.org/docs.
- Hernando, R. (2007). *Seguridad en Redes Inalámbricas*. Recuperado el septiembre30 de 2013, de http://www2.rhernando.net/modules/tutorials/doc/redes/seg-wifi.pdf
- Hsiao, H., & Mohsen, G. (2006). *Next Generation Wireless Systems and Networks.* Estados Unidos: John Wiley & Sons, Ltd.

- IEEE802.11. (2012). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Recuperado el 1 de febrero de 2013, de http://standards.ieee.org/getieee802/download/802.11-2012.pdf
- IEFT org. (2007). *RFC4766*. Recuperado el 10 de octubre de 2013, de http://datatracker.ietf.org/doc/rfc4766/?include_text=1
- IETF org. (s.f.). *Instrution Detection Exchange Format*. Recuperado el 10 de octubre de 2013, de http://datatracker.ietf.org/wg/idwg/charter/
- Iniesta, M. (2010). Seguridad WIFI. Agresiones posibles (Proyecto de fin de carrera). *Universidad de Valencia*. Valencia, España.
- Kershaw, M. (2011). *Kismet*. Recuperado el 15 de octubre de 2013, de http://www.kismetwireless.net/documentation.shtml
- Kimberly, G. (2010). *Certified Ethical Hacker Study Guide. .* Estados Unidos: Wiley Publishing Inc.
- Mira, A. (s.f.). *Implantación de un Sistemas de Detección de Intrusos en la Universidad de Valencia*. Recuperado el 1 de octubre de 2013, de http://www.rediris.es/cert/doc/pdf/ids-uv.pdf
- Ochoa, V. (2011). Análisis de tráfico de datos en la capa de enlace de una red LAN, para la detección de posibles ataques o intrusiones sobre tecnologías Ethernet y Wi-Fi 802.11. (Tesis de grado). *Escuela Politécnica del Ejército*. Sangolquí, Ecuador.
- Pandove, K., Jindal, A., & Kumar, R. (2010). *Lauching Email Spoofing Attacks*. Recuperado el 20 de junio de 2013, de http://www.ijcaonline.org/volume5/number1/pxc3871254.pdf
- Pritchett, W., & De Smet, D. (2012). *Bactrack 5 Cookbook.* Reino Unido: Pack Publishing Ltd.
- Rios, D. (2011). *Seguridad en Redes Wi Fi*. Recuperado el 1 de octubre de 2013, de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MONOGRAFIA_DE_SEGURIDAD_EN_%20REDES_WIFI.pdf
- Roesch, M., Gree, C., & Sourcefire. (2013). *Snort's User Guide 2.9.5.* Recuperado el 1 de noviembre de 2013, de http://www.snort.org.

- Salinas, R. (2005). *Sistemas de Detección de Intrusos*. Recuperado el 12 de octubre de 2013, de http://www.iti.es/media/about/docs/tic/06/2005-02-intrusos.pdf
- Siguenza, H., & Léon, E. (2006). *Normas IEE801.11a, 802.11b y 802.11g*. Recuperado el 4 de febrero de 2013, de http://dspace.ups.edu.ec/bitstream/123456789/221/4/Capitulo%203.pdf
- Sourcefire Team. (2013). *Snort*. Recuperado el 1 de noviembre de 2013, de http://www.snort.org.
- Telefonía Movistar. (s.f.). *Recomendaciones para Redes Inalámbricas*. Recuperado el 4 de febrero de 2013, de http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/modem-router-inalambricos-adsl/guia-recomendaciones-para-redes-inalambricas.pdf
- Vladimirov, A., Gavrilenko, K., & Mikhailovsky, A. (2005). *Hacking Wireless Seguridad de Redes Inalámbricas.* España: ANAYA multimedia.

Sangolquí, 28 de Marzo del 2013

ELABORADO POR:

_____

Srta. Ana Marivel Yacchirema Espín

DIRECTOR DE LA CARRERA DE ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS:

_____

Ph.D. Ing. Nikolai Daniel Espinosa Ortiz