DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD EN REDES DE COMUNICACIÓN INALÁMBRICAS APLICADO A PEQUEÑAS EMPRESAS DEL SECTOR PRIVADO DE LA CIUDAD BOGOTÁ

JENNIFER JOHANA CIFUENTES RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
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

JENNIFER JOHANA CIFUENTES RODRÍGUEZ

Informe de trabajo de grado para optar al título de
Especialista en Seguridad Informática

Asesor:
Hernando José Peña
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, fecha

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

INTRODUCCIÓN

Actualmente los avances en las tecnologías de información y en las telecomunicaciones demandan de medidas de seguridad para salvaguardar el recurso más importante de toda organización, entidad o negocio, la información.

La falta de medidas de seguridad en las redes es un problema de gran impacto, ya que los riesgos, ataques y amenazas permanecen latentes en la sociedad, día a día la vulnerabilidad de los sistemas de información es mayor, ya que a medida que crecen los mecanismos de seguridad, nacen nuevos y más especializados ataques y amenazas, obligando a buscar mecanismos mayores que permitan satisfacer los servicios de protección de componentes y comunicaciones en la red.

La seguridad es un tema amplio y se ocupa de garantizar que la curiosidad, competitividad, y demás factores que implique vulnerar la información, no lleguen a su objetivo. Como consecuencia nace la necesidad de implantar medidas, procesos y procedimientos que velen por la integridad, disponibilidad y confidencialidad de la información.

Para establecer una guía, que permita mantener la seguridad de las redes inalámbricas, y garantizar a las pequeñas empresas, el salvaguardar la información. Es necesario realizar una investigación sobre los diferentes ataques que se presentan en el tiempo actual, así mismo identificar los riesgos

y vulnerabilidades a los que se encuentran expuestas las redes, localizar las falencias de la red o de las personas o sistemas informáticos que interactúan en esta.

El uso de herramientas de pruebas, ayuda a evaluar diferentes escenarios que se pueden presentar en la realidad, ejecutar pruebas de seguridad en una red inalámbrica tiene el propósito de mejorar la calidad de los servicios de la red, encontrar huecos de seguridad a tiempo, realizar mantenimientos preventivos y no correctivos, igualmente encontrar soluciones de seguridad antes de perjudicar la información de un negocio.

Por último especificar medidas o estrategias de seguridad, de acuerdo a un nivel de protección, y establecer protocolos, estándares, configuraciones y políticas de seguridad, basados en estudios prácticos demostrativos, confirmando la experiencia y utilidad de los mismos.

Una guía que dirige a los usuarios de las redes inalámbricas de las pequeñas entidades, para mantener la seguridad en la información.

1. PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCION

La seguridad en redes surge como consecuencia de la necesidad de utilizar medios y procedimientos para reducir riesgos debidos a las posibles amenazas y vulnerabilidades sobre la red inalámbrica. Para las empresas es de vital importancia dar un buen manejo y seguridad a la información, razón por la cual, es importante hacer uso de una metodología adecuada.

Actualmente la utilización e implementación de redes inalámbricas en las empresas de la ciudad de Bogotá es más frecuente, por tanto, es necesario a través de este proyecto de investigación identificar las amenazas y procedimientos que permitan controlar los riesgos a los que está expuesta la información como principal activo de las empresas mediante un modelo de gestión de seguridad adecuado.

Toda organización que maneje sistemas de información está expuesta a amenazas y ataques que ponen en riesgo su permanencia, más aún cuando hablamos de conexiones inalámbricas en donde son accedidas por diferentes personas desde diferentes medios como celulares, portátiles, servidores, *tablets*, impresoras etc.

Las empresas que utilizan redes inalámbricas se encuentran más expuestas a ataques que puedan generar la pérdida o robo de información, entre las que se encuentran: *Access Point Spoofing*, *MAC Spoofing*, *ARP Poisoning, Denial of*

service, WLAN escaners, Wardriving, entre otras como intercepción, intrusión e interferencia de datos; razón por la cual, el propósito de este proyecto es realizar una investigación a fondo sobre las vulnerabilidades de las diferentes redes de información inalámbricas, con esto encontrar que medidas de seguridad se pueden implantar para eliminar o reducir cualquier riesgo, que metodologías se pueden utilizar de acuerdo a cada uno de los protocolos utilizados en las redes de informática para garantizar la seguridad de cualquier empresa u organización, basados en normas o estándares internacionales que aporten a la misma. Lo anterior, enfocado al mejoramiento del negocio y a la seguridad de la información.

1.2 FORMULACION

¿Cómo el diseño de un modelo de gestión de seguridad en redes ayudará a disminuir los riesgos potenciales en las redes inalámbricas de las pequeñas empresas del sector privado de la ciudad Bogotá?

1.3 OBJETIVOS

1.3.1 General

Diseñar un modelo de gestión de seguridad en redes de comunicación inalámbricas para disminuir los riesgos potenciales en las pequeñas empresas del sector privado de la ciudad Bogotá.

1.3.2 Específicos

- Identificar las diferentes vulnerabilidades, amenazas y riesgos a que se ven expuestos los usuarios al conectarse a las redes inalámbricas de las pequeñas empresas del sector privado de Bogotá.
- Evaluar la seguridad mediante pruebas sobre las redes inalámbricas.
- Especificar medidas de seguridad de acuerdo a su función y grado de protección para establecer redes seguras.
- Elaborar un manual o guía de la implementación del modelo de gestión de la seguridad en las redes inalámbricas aplicado a las pequeñas empresas del sector privado de la ciudad de Bogotá.

1.4 JUSTIFICACIÓN

El propósito de este proyecto es investigar a fondo las vulnerabilidades, amenazas y riesgos a los que se encuentran expuestas las redes inalámbricas de las grandes empresas y ayudar a contribuir a la seguridad de las redes inalámbricas, por medio del diseño y propuesta de implementación de mecanismos, metodologías y guías para establecer redes seguras; teniendo en cuenta que en la sociedad actual juegan un papel fundamental, siendo una de las redes más usadas en la comunicación, bien sea, para la descarga de información, el uso de mensajería, transferencia de datos, entre otras.

Se estudian las redes inalámbricas y como ha sido la evolución del uso malicioso de cada uno de estas redes, como un *hacker* o un atacante puede

dañar de manera significativa la información. Analizar los posibles ataques y su funcionamiento, los problemas que actualmente enfrentan como lo es la saturación del espectro debido a la masificación de usuarios que afecta las conexiones a larga distancia. Ya que en realidad las redes *Wi-Fi* están diseñadas para conectar dispositivos a distancias reducidas, y a un mayor alcance se expone a un riesgo mayor de interferencia.

Existe un elevado porcentaje de organizaciones que implementan sus redes de manera abierta, sin proteger la información que circula por ellas, permitiendo el acceso y control de sus dispositivos *Wi-fi* (de distribución y terminales).

Así mismo, como se ha acrecentado el número de redes inalámbricas, se dio una gran evolución en el estándar global de comunicaciones para redes de área local IEEE 802.11 que permite la transmisión de datos entre diferentes equipos móviles y estáticos, en un entorno donde se necesita mayor velocidad de transmisión, facilidad, portabilidad, y especialmente seguridad, se ve fuertemente impulsada la norma en dispositivos como ordenadores, consolas de videojuegos, móviles, entre otros. Igualmente no se ha tardado en encontrar vulnerabilidades a la norma siendo los principales perjudicados los propios usuarios de la tecnología, compañías grandes, medianas y pequeñas que pueden ver comprometidos sus datos confidenciales de gran valor, perdidas en el entorno empresarial, utilización ilícita de información o suplantación de identidades, son algunas de las consecuencias que se producen debido a los agujeros de seguridad. Es por esto que el desarrollo de este proyecto se centra

en el estudio de la tecnología y herramientas de protección, estudiando los niveles de seguridad alcanzables, métodos de ataque y soluciones para evitar las intrusiones, se realiza un recuento de los diferentes métodos de cifrado, las herramientas más comunes de ataque y los métodos de protección más utilizados. Realizar una descripción del estándar IEEE802.11 direccionado en un marco de diferentes tecnologías inalámbricas, exponer los diferentes protocolos de seguridad que se aplican a las redes, detallando sus funciones y vulnerabilidades; basados en estudios prácticos demostrativos, teniendo en cuenta las experiencias.

La finalidad de este proyecto es dirigir o guiar a los administradores de redes y seguridad de información para proveer y mantener redes inalámbricas seguras que garanticen la fiabilidad de la transmisión de los datos de las pequeñas empresas de la ciudad de Bogotá.

1.5 DELIMITACIÓN

El alcance de este proyecto es proporcionar una guía con un conjunto de medidas de seguridad que proporcionen redes de comunicación inalámbricas seguras, lo suficientemente fuertes para evitar infiltraciones, intrusiones, violaciones a la información o recursos vitales de una organización, para prevenir problemas grandes y desastrosos en algunos casos, de igual manera el de dar a conocer una serie de pautas para configurar los diferentes tipos de medidas de seguridad en redes inalámbricas, así como implementar estándares de un sistema de seguridad, entre los que se encuentran: *WEP, WPA, WPA2* basados en la norma IEEE802.11.

Este proyecto de investigación solo abarca fines informativos y demostrativos, proporcionar la información necesaria para que una organización adquiera los conocimientos de nuevas y mejores tecnologías que garanticen una amplia protección en la transmisión y seguridad de datos dentro de una red, igualmente crear conciencia acerca de la seguridad de la información, ante ataques y frecuentes vulnerabilidades a la que se ve expuesta.

Todo lo anterior con la finalidad de mantener la integridad, confidencialidad, disponibilidad y autenticidad de la información en una organización.

2. MARCO DE REFERENCIA

2.1 ANTECEDENTES

Título: IMPACTO DE LA SEGURIDAD EN REDES INALÁMBRICAS DE SENSORES IEEE 802.15.4

Autor: Carlos García Arano

Resumen: Este proyecto analiza el impacto que provoca el uso de las funcionalidades de seguridad descritas en el estándar IEEE 802.15.4 en las redes de sensores. Se han implementado los diferentes niveles de seguridad propuestos con la asistencia de un módulo hardware criptográfico y se han integrado en un desarrollo basado en *FreeRTOS*. Estas funcionalidades permiten garantizar la confidencialidad e integridad de las comunicaciones, pero suponen un coste en diferentes aspectos que se ha de cuantificar. Se han analizado los costes en el consumo de energía, ya que los recursos energéticos de los sensores son una de las principales limitaciones de este tipo de redes. Los resultados evidencian un aumento en el consumo, pero casi exclusivamente derivados de incremento del tiempo de transmisión. (García Arano Carlos, 2008)

Aporte: Proporciona una guía para el desarrollo del proyecto, ya que al igual se pretende identificar las funcionalidades de seguridad que otorga el estándar IEEE802 en las redes *Wi-fi*, en este proyecto presentan diferentes niveles de seguridad con el fin de garantizar la confidencialidad e integridad de la información transmitida.

Título: *Network Wireless Security*

Autor: Stephen Blair Mandeville Armería

Resumen: Teniendo en cuenta los problemas y necesidades actuales que se presentan a diario en el uso de redes inalámbricas, se han establecido diferentes proyectos de investigación asociados al caso.

Con los cambios y avances tecnológicos en el transporte de la información, se definen métricas, configuraciones, entre otras cosas para garantizar la protección en la transmisión de datos dentro de una red.

El proyecto de investigación presentado se basa en el estándar 802.11 y se centra en el análisis e implementación de la tecnología *WPA2* como una solución a los actuales problemas arriba citados. (Mandeville Stephen).

Aporte: Es un proyecto de investigación similar, ya que establece los problemas, ataques y vulnerabilidades a los que se encuentran expuestas las redes Wi-fi, pero así mismo proporciona y se enfatiza en un método de seguridad conocido como WPA2, ya que parece el más factible para el autor del mismo.

2.2 MARCO TEÓRICO

2.2.1 Protocolos de seguridad

Protocolo WEP: WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) Protocolo para resguardar las redes inalámbricas, por medio de un estándar de encriptación. Se presenta debido a que los canales de comunicación son inseguros y su objetivo principal es garantizar la confidencialidad y evitar que usuarios no autorizados puedan acceder a las redes WLAN, proporcionando autenticidad. [1]

Se destacan las siguientes ventajas:

- Permite utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida
- El protocolo WEP es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta.
- Proporciona niveles de seguridad altos.

Dentro de las desventajas se tienen:

- Existe una vulnerabilidad en la captura de paquetes de información por parte de terceros, donde pueden encontrar la contraseña de la red y acceder a ella, las claves de tipo WEP son relativamente fáciles de conseguir por este método.
- No implementa adecuadamente, el enfoque de incrementar el vector de un paquete a otro, en el tamaño de los paquetes de iniciación. Permitiendo que la cantidad de tramas que pasan a través de un punto

[1] NETSPOT, Protocolos de seguridad inalámbrica: WEP, WPA, y WPA2. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: https//www.netspotapp.com/es/wifi-encryption-and-security.html

sea grande, lo que hace que se encuentren dos mensajes con el mismo valor de iniciación

- Las claves de cifrado estáticas son pocas veces cambiadas.
- Existen varias herramientas que pueden permitir romper la clave secreta.

Protocolo WPA: WPA *(Wi-Fi Protected Access*) Su objetivo es cubrir todas las falencias de seguridad detectadas en el protocolo de seguridad WEP. Trabaja bajo un estándar de MAC, se encuentra orientado a pequeñas oficinas y usuario doméstico. Como indica Guillaume. [2]

Dentro de sus principales características se tienen:

- Distribución dinámica de claves
- Incremento de robustez del vector de inicio
- Nuevas técnicas de integridad y autenticación

Tiene las principales ventajas:

- Implementación del Protocolo de Integridad de Clave Temporal (*TKIP - Temporal Key Integrity Protocol*), permite cambiar las claves dinámicamente a medida que el sistema es utilizado.

  Evita ataques de recuperación de clave a los que es susceptible WEP.
- Contiene protección contra ataques de "repetición" (*replay attacks*), cuenta con un contador de tramas.
- Permite trabajar a nivel doméstico y empresarial

Se encuentran las siguientes desventajas:

[2] Guillaume Lehembre, Seguridad Wi-Fi – WEP, WPA y WPA2. [En línea]. 2006 [Citado: 25-May-2016] Disponible en internet: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

- No es soportado por muchos dispositivos de red antiguos.
- No todas las tarjetas inalámbricas son compatibles con este estándar.

Protocolo WPA2: Diseñado específicamente para cumplir requisitos de entornos empresariales. Como indica Escobar.[3] Es compatible con *WPA2*.

Entre las principales ventajas:

- Utilizado para redes grandes, dado que proporcionan muy buena seguridad.
- Puede trabajar con y sin un servidor de llaves, todas las estaciones de la red usan una llave de tipo PSK (*Pre-Shared-Key*), en caso contrario se usa habitualmente un servidor IEEE 802.1x.
- Incluye un algoritmo considerado criptográficamente seguro

Su principal vulnerabilidad es el ataque a la clave PSK, ya que toda la información de la red va en formato texto y se transmite cuando un usuario se autentifica. Teniendo en cuenta que la infraestructura de clave pública se compone de un número de elementos necesarios que garantizan la ejecución de operaciones criptográficas, por medio de una tecnología, que proporciona mayor seguridad de la información dentro de una organización.[4]

Protocolo EAP (*Extensible Authetication Protocol*): Se encarga de la autenticación y autorización, gestionando las contraseñas, capaz de trabajar con tecnología de llave pública.[5]

---

[3] Escobar Varas Angel, Maluenda Ruz Javier, Redes WPA/WPA2. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: http://profesores.elo.utfsm.cl/~agv/elo322/1s12/project/reports/RuzRiverosVaras.pdf

[4] Ibid, p. 25.

[5] TechNet, Protocolo de autenticación extensible (EAP) para la introducción de acceso de red. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: https://technet.microsoft.com/es-es/library/hh945105(v=ws.11).aspx

2.2.2 Red Inalámbrica

Concepto: conjunto de equipos comunicados por medio de una transmisión sin cables y ondas electromagnéticas y a través de antenas, las cuales pueden presentar interferencias y de acuerdo a la cobertura que ofrecen una medida de transmisión. [6]

Ventajas de las redes inalámbricas: Dentro de las ventajas que ofrecen las redes inalámbricas, se encuentran:

- *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.
- *Seguridad:* gestiona y controla el acceso a las redes inalámbricas por medio de protocolos y configuraciones de seguridad para lograr el éxito de la misma. [7]

Tipos de acuerdo a su cobertura: Teniendo en cuenta la cobertura de las redes WI-FI, se pueden clasificar en los diferentes tipos:

[6] CCM, Redes inalámbricas. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet:http://es.ccm.net/contents/818-redes-inalambricas
[7] Blogspot, Ventajas y Desventajas De Redes Inalambricas. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: http://redessincableado.blogspot.com.co/p/ventajas-las-redes-wifi-poseen-una.html

- ✓ *Wireless Personal Area Network*

  Es de cobertura personal, para hogares, para interconexión de teléfonos móviles y ordenadores personales, requiere tasas bajas de seguridad.

- ✓ *Wireless Local Area Network*

  Son de cobertura local, basadas en *HiperLAN* y siguen el estándar IEEE 802.11.

- ✓ *Wireless Metropolitan Area Network*

  Son de cobertura metropolitana, se encuentra basada en la tecnología *WiMAX*, es decir, que tiene más cobertura y ancho de banda.

- ✓ *Wirelees Wide Area Network*

- ✓ Su cobertura es mundial, más amplia y basada en la tecnología UMTS, permitiendo comunicaciones universales.[8]

Características: Estas redes se caracterizan de acuerdo al rango de frecuencia utilizado para transmitir y de acuerdo al medio en que se implementan:

- ❖ Ondas de radio: las ondas electromagnéticas son omnidireccionales, sus frecuencias no son altas, lo que hace que la transmisión no sea sensible a atenuaciones.
- ❖ Microondas terrestres: utiliza antenas parabólicas con diámetros de tres metros, su cobertura es a nivel de kilómetros, su gran falencia es que el emisor y el receptor deben estar alineados para la transmisión, el enlace debe ser punto a punto a una distancia corta.[9]

[8] CCM, Op. cit. p.26.
[9] Informaticamoderna, LAS REDES INALÁMBRICAS. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: http://www.informaticamoderna.com/Redes_inalam.htm

- Microondas por satélite: su comunicación es por estaciones bases. El satélite recibe la señal en una banda frecuencia, la amplifica y la retransmite. Pueden haber interferencias con las comunicaciones.
- Infrarrojos: su comunicación consiste en enlazar receptores y transmisores que modulan la luz infrarroja, debe ser alineada directamente, no puede atravesar las paredes. [10]

2.2.3 Ataques sobre las redes inalámbricas

Pérdida de equipo robado: Cuando se utiliza seguridad en modo WPA2, hay una sola contraseña general para la red inalámbrica, esta contraseña generalmente es guardada por los dispositivos conectados, lo que genera un problema al momento que ocurra un robo a alguno de los dispositivos.

Espionaje de usuario a usuario: Las amenazas no siempre ocurren desde afuera. Los mismos clientes pueden espiar el tráfico de la red para observar la información de otros usuarios, es de tener en cuenta que esta situación se puede presentar a nivel empresarial y se debe controlar. [11]

[10] Informaticamoderna, Op. cit. p.27.
[11] De Luz Sergio, Ataques a las redes: Listado de diferentes ataques a las redes de ordenadores. [En línea]. 2016 [Citado:25-May-2016] Disponible en internet: https://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/

Sesiones de cuentas de secuestro: Existen muchas herramientas que hacen secuestro de sesión que ayudan a tener acceso a la cuenta o sesión total sin tener que ingresar la contraseña, con el fin de husmear y tener control total sobre la sesión del usuario.

Puntos de acceso falso: Cualquier punto de acceso que no es seguro se puede catalogar como falso, encontrar puntos de acceso abiertos puede generar varios problemas en la información. [12]

***Malware* en Internet:** Consiste en *software* malicioso en una página web, que puede infectar de virus, gusanos o troyanos los equipos asociados a la red, con la finalidad de borrar datos y recopilar información (contraseñas, *emails*, entre otros).

***Access Point Spoofing*:** Este ataque funciona haciéndose pasar por un punto de acceso verdadero, con la finalidad de que la víctima se conecte a la red errónea y lograr capturar la información, y una vez cometido el objetivo volver a direccionar el tráfico al punto verdadero, pasando un ataque inadvertido.

ARP *Poisoning*: Este ataque se realiza al protocolo ARP, colocando en medio de la red un invasor de tal manera que la comunicación o envió de paquetes de un punto a otro tenga que pasar en medio del sujeto y así capturar o alterar los paquetes de información.

MAC *Spoofing*: Consiste en suplantar la dirección MAC de un cliente autorizado, esto ocurre por los permisos que existen para cambiar las MAC.[13]

[12] CALLES, Juan Antonio "Wi-Fis: Tipos de ataque y recomendaciones de seguridad" [En línea]. 2013 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html.
[13] Ibid, p. 29.

***Denial of Service* (DoS):** Consiste en saturar la red con peticiones, haciendo que el servicio no esté disponible para los verdaderos clientes. En las redes inalámbricas se satura con peticiones de segregación. [14]

Colapsar totalmente con la finalidad que la navegación sea lenta o imposible, es decir denegar el servicio, se encuentran tres categorías de denegación del servicio:

- Inundación de conexiones: propio del protocolo TCP, ya que este pide el reenvió de los paquetes perdidos, lo que establece cientos de conexiones hasta colapsa el servicio.
- Inundación de ancho de banda: un usuario malintencionado envía muchos paquetes, impidiendo el paso de los legítimos paquetes de envió. Peticiones distribuidas.
- Ataque de vulnerabilidad: el atacante se centra en enviar mensajes construidos específicamente para provocar un fallo. [15]

***Sniffing o Sniffers*:** Este ataque intercepta el tráfico en una red, para que se lleve a cabo este ataque la víctima y el atacante debe estar en la misma red y ocurre por redes inseguras, abiertas y públicas.

Consiste en analizar los paquetes enviados en la red, poder ver todo lo que circula en la red, inclusive crackeando las claves de cifrado inalámbrico.[16]

[14] INFORMÁTICA HOY "Vulnerabilidades de las redes" [En línea]. 2012 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php

[15] Ibid, p. 30.

[16] CIOPERU "5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos" [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: http://cioperu.pe/articulo/18229/5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos/.

WLAN escáner: Consiste en realizar un recorrido por una zona determinada con el objetivo de buscar y almacenar puntos de acceso a redes inalámbricas y poder extraer datos e información.

2.2.4 Esquemas de seguridad en redes inalámbricas

Esquema 1: Como esquema de seguridad que se debe tener en cuenta para la seguridad de una red inalámbrica, es necesario:

- Mantener actualizados los controladores de *Wi-fi*, así como el *firmware* del *router*
- Si no se utiliza la red Wi-fi, deshabilitarla
- Configurar la red como oculta, aplicar la técnica de cifrado correspondiente al uso de la red:
- WPA2 Personal o PSK con cifrado para hogares o pequeñas empresas puede ser una buena opción, con el uso de contraseñas de más de 20 caracteres y robustas

  WPA *Enterprise* recomendable para empresas y corporaciones, esta utiliza el cifrado AES (*Advanced Encryption Standard*) y para generar contraseñas aleatorias y robustas por medio del servidor RADIUS (*Remote Authentication Dial in User Service*), para la autenticación utiliza protocolos 802.1X y EAP de acuerdo al que se determine utilizar. [17]

[17] ADSLZONE, DIFERENCIAS ENTRE WEP Y WPA2-PSK ENTRE WEP Y WPA2-PSK. [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: https://www.adslzone.net/tutorial-44.18.html

- Evitar conectarse a redes Wi-fi o redes públicas, ya que estas son el entorno perfecto para los atacantes
- No utilizar redes ajenas, en primer lugar es un delito, y en segundo lugar se puede cambiar los papeles de ser un atacante a ser atacados
- Cambiar la clave por defecto del *router,* ya que existen diferentes herramientas que permiten descifrar esta. [18]
- Cambiar el nombre de red *SSID* que viene por defecto y la contraseña de administración
- Limitar el número de IP asignables, cuando se tiene configurado el *router* para que las asigne dinámicamente
- Desactivar del *router* tecnologías que no se utilicen

Esquema 2: Otra opción para dar solución al problema de la inseguridad de la red inalámbrica, se encuentra en la autenticación:

a. Autenticación de usuario

   Utilizar y trabajar bajo un protocolo de autenticación fuerte. El protocolo EAP que utiliza métodos de autenticación arbitrarios, sirve como soporte a protocolos propios de autenticación gestiona contraseñas y se trabaja la autenticación a través de certificados, tarjetas inteligentes o credenciales. Como indica Martin. [19] Diversos fabricantes que crearon varios métodos EAP, entre los que se encuentran:

   - EAP-LEAP (*Ligth EAP*) desarrollado por Cisco, provee un mecanismo de autenticación mutua en *password*, es decir, se requiere que la

[18] Jonnathan “Wireless Network” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: http://wagneredesinalambricas.blogspot.com.co/2009/10/marco-teorico.html.
[19] MARTIN, Alejandro “Redes Inalámbricas” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: http://inalambricas2009.blogspot.com.co/2009/10/marco-teorico.html.

estación del usuario se autentique con la red, al igual que la red se autentique con el usuario, de esta manera se asegura que los usuarios son los correctos. También usa claves dinámicamente por sesión.

- EAP- TLS (*Transport Layer Security EAP*) desarrollado por *Microsoft*, ofrece autenticación mutua, credenciales seguras, claves de encriptación dinámicas, requiere de distribución de certificados digitales.

- EAP – TTLS (*Tunneled TLS*) permite certificados de servidor y no de cliente, permite que los usuarios sean autenticados dentro de las WLANs, utilizando criptografía de clave pública/privada, es más sencillo de gestionar y económico.

RADIUS (*Remote Authentication Dial-UP User Service*): servidor de punto final, es responsable de recibir solicitudes de conexión y de la autenticación de los usuarios para luego retomar la información de configuración necesaria para el cliente. Su principal característica es la capacidad de manejar sesiones, notificando cuando inicia y termina una conexión, generando estadísticas.

b. Autenticación del equipo

Esta fase brinda más seguridad y robustez, configurar DHCP (Protocolo de configuración dinámica de *hosts*), controla y limita el acceso a la infraestructura de red inalámbrica a aquellos equipos que no pertenezcan a la red. [20]

[20] ZEROSHELL, Autenticación en redes inalámbricas con 802.1x, WPA y WPA2. [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.zeroshell.net/es/radiusdetails/

Esquema 3:

- Activar funciones de seguridad inherentes a los puntos de acceso y las tarjetas de interfaz. Esto se realiza normalmente ejecutando un programa suministrado con el equipo inalámbrico.
- Conocer la versión de *firmware* que utilizan los puntos de acceso y mantener la actualización de los mismos ya que esto los hace más seguros y confiables
- Comprobar los recursos de seguridad que ofrece el *hardware y software*, para mejorar la red inalámbrica y simplificar la administración de esta
- Implementar y mantener recursos que se encarguen de la asistencia de la seguridad inalámbrica [21]

2.2.5 Herramientas de pruebas de seguridad: De acuerdo a los principales riesgos de seguridad que tienen las redes inalámbricas, se definen los métodos de pruebas a realizar: [22]

Riesgos:

a) Red de comunicaciones Wi-fi abierta
b) Presencia de cifrado WEP en redes de comunicaciones
c) Algoritmos de generación de claves de dispositivos inseguros
d) Claves WEP básicas
e) Mecanismos de autenticación inseguros
f) Red Wi-fi no autorizada

[21] ZEROSHELL, Op. cit. p.33.
[22] SILVA, Felix "Penetration Testing". [En línea]. 2016 [Citado: 16 mayo de 2016 Disponible en Internet: https://docs.google.com/presentation/d/1e3-VDVAdiV4tb-lNQ-v7hv581rhZHHg8i8cJ5gETQCk/htmlpresent?hl=es

g) Portal *hostspot* inseguro

h) Cliente intentado conectar a red insegura

i) Rango de cobertura de red demasiado extenso

Pruebas:

a) Descubrimiento de dispositivos: selección de información sobre las redes inalámbricas

b) *Fingerprinting*: consiste en el análisis de las funcionalidades de los dispositivos de comunicaciones

c) Pruebas sobre la autenticación, es decir, examinar los mecanismos de autenticación [23]

d) Cifrado de las comunicaciones, vigilar los mecanismos de cifrado

e) Configuración de la plataforma, verificar la configuración de las redes

f) Pruebas de la infraestructura, comprobar los controles de seguridad sobre la infraestructura *Wireless*

g) Pruebas de denegación de servicio, validar los controles orientados a verificar la disponibilidad

h) Pruebas sobre directivas y normativa, analizar los aspectos normativos aplicados a las redes de Wi-fi

i) Pruebas sobre clientes inalámbricos, considerar ataques contra clientes inalámbricos

j) Pruebas sobre *hostspots* y portales cautivos, reconocer las debilidades que afectan al uso de portales cautivos

2.2.6 Software de aplicación de pruebas

[23] SILVA, Op. cit. p.34.

WEPCrack

Esta herramienta se basa en las debilidades del algoritmo clave RC64, basada en *Perl* se utiliza principalmente para romper los puntos de acceso 802.11, proporciona capacidades de fuerza bruta para capturar y decodificar el trafico WEP para un posterior análisis.[24]

Kismet

Trabaja como un detector de redes Wi-fi, detector de intrusos y como *sniffer*. Opera como un identificador de red pasivo, generalmente se utiliza para detectar el SSID de una red WLAN. Si en un primer sondeo no se logra identificar SSID, se puede realizar él envió de tramas de disociación forjadas para exponer el SSID con una solicitud.

WiFinder

Es una aplicación de fácil uso, ya que se puede utilizar en cualquier dispositivo con sistema operativo *Android* para detectar redes abiertas. También contiene una funcionalidad de escaneo automático. La información que se obtiene de esta aplicación incluye información básica de la red, método de cifrado, canal y fortaleza de la red.[25]

Airmagnet WiFi Analyzer

Herramienta diseñada para ser una solución de auditoria móvil y una solución corporativa estándar. Es de gran ayuda al personal de monitoreo para detectar varios problemas con la red Wi-Fi, tales como: problemas de conectividad, de señales de trayectoria múltiple y conflictos entre dispositivos. Es muy útil,

[24] KARTHIK R “10 herramientas de seguridad Wi-Fi para su arsenal” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: http://searchdatacenter.techtarget.com/es/foto-articulo/2240220535/10-herramientas-de-seguridad-Wi-Fi-para-su-arsenal/10/10-Xirrus-Wi-Fi-Inspector.
[25] Ibid., p. 36

gracias a la asignación automatizada de diversos problemas con cumplimientos y políticas.

Agente AirMobile para PDA

Se ejecuta silenciosamente en las PDA. Si la aplicación encuentra un punto de acceso dudoso, analiza el objeto y luego determina si hay amenazas. Se ejecuta como cliente-servidor. Sus características principales es asegurar que los informes se envíen por correo electrónico a las personas de seguridad. [26]

NetStumbler

Es una herramienta basada en Windows, utilizada generalmente para descubrir redes WLAN, ayuda a detectar otras redes que pueden causar interferencia y es muy útil para guerra de atacantes. También reconoce áreas de cobertura pobre en red WLAN proporcionando ayuda al administrador de la red.

Airpwn

Se utiliza para la inyección de paquetes a una red 802.11. Esta herramienta escucha los paquetes Wi-Fi entrantes e inyecta paquetes personalizados a partir de puntos de acceso inalámbrico falsificados, contiene siete modos diferentes de operación y función. Esta herramienta es potencial para realizar *DoS* en toda una red WLAN.

AirCrack – ng

Útil para auditoria de red inalámbrica, ya que optimiza el ataque *WEPCrack*, incluye ataques *KoreK* y *PTW*, es más rápida y eficaz

Aircheck Wi-Fi Tester

[26] KARTHIK. Op. cit. p.36.

Comprueba problemas con redes 802.11, ya que incluye varias funcionalidades, como pruebas de exploración automática, proporciona análisis *pass/fail* de las redes. Es un dispositivo fácil de usar para encontrar accesos o dispositivos falsos, configurar la seguridad y detectar interferencias. [27]

Xirrus Wi-Fi Inspector

Herramienta muy poderosa para gestionar y solucionar problemas de redes Wi-Fi, contiene pruebas incorporadas para ejecutar automáticamente: pruebas de rendimiento sin interrupciones manuales. Ayuda a detectar puntos de acceso maliciosos, verifica la cobertura y localiza dispositivos Wi-Fi.

Pruebas de penetración y hacking

Se suele concentrar en descubrir la contraseña o en un acceso forzado a la infraestructura de la red, al igual que pruebas como identificación de redes ocultas, geo localización, falso punto de acceso, hombre en el medio, denegación de servicio, suplantación de sitios de autenticación, cobertura de señal, código malicioso e Ingeniería Social. [28]

[27] KARTHIK. Op. cit. p.36.
[28] Ibid,. p.36.

2.2.7 WiMax: Traduce Interoperabilidad mundial para acceso por microondas, es una tecnología que ofrece conexión a Internet súper rápida con amplia cobertura, útil para entornos exteriores, permitiendo construir una infraestructura a zonas de difícil acceso. Se está utilizando actualmente en empresas que ofrecen servicios a consumidores finales a precios y velocidades atractivos.[29] Se ha convertido en una red de gran utilidad para diferentes entidades y negocios:

- Permite crear una red empresarial y acceder desde cualquier punto
- Acceder a Internet a grandes velocidades
- Permite conexión de diferentes dispositivos sin necesidad de cables
- Accede a servicios de *VoIP* sin cables
- Se pueden añadir más canales con facilidad dependiendo de la regulación del país
- Posee anchos de banda configurables
- Se adapta a diferentes tipologías: Punto-Punto, Punto-Multipunto, etc
- Soporta gran número de usuarios

Tipos de redes WiMAX

- **WiMAX Fijo:** Fue diseñado para acceso fijo, es decir, se coloca una antena en un lugar estratégico para los abonados. Basado en el estándar IEEE 802.16 proporcionando una solución inalámbrica de acceso a internet de banda ancha, como alternativa inalámbrica al modem cable y ADSL.

[29] POLANCO, Juan José "WiMAX que es y para qué sirve?" [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: https://hackinglinux.wordpress.com/2009/04/09/wimax-que-es-y-para-que-sirve/.

- **WiMAX Móvil:** Se enfoca hacia el mercado móvil, proporcionando portabilidad y mayor capacidad, basado en el estándar IEEE 802.16, agrupa subportadores en diferentes subcanales, es decir, en una sola estación cliente pueden acceder todos los subcanales dentro de la transmisión. [30]

2.2.8 Estándares y especificaciones que influyen en el funcionamiento

Evolución del estándar

La norma 802.11 se encuentra conformada por una serie de grupos, dedicados cada uno a un desarrollo particular en el ámbito de la tecnología inalámbrica.

Estándares de las redes.

IEEE 802.11b *legancy* funciona en 2.4 Ghz y tiene una velocidad de 11 Mbps método de acceso definido en el estándar CSMA/CA (*Carrier Sense Multiple Acces wiht Avoidance*) lo cual se traduce al acceso múltiple con escucha de portadora y evasión de colisiones, protocolo para el control de acceso a redes de bajo nivel que permite que múltiple estaciones utilicen el mismo medio de trasmisión. [31]

IEEE 802.11a tiene una velocidad máxima de trasmisión de 54Mbps y funciona en 5Ghz es más rápida y define el uso de los niveles inferiores de arquitectura OSI en la capa física y en el enlace de datos, especifica normas de

[30] Ibid,. p.39..
[31] CCM "Introducción a Wi-Fi (802.11 o WiFi)" [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi

funcionamiento a las redes de área local y redes de área metropolitana, utiliza 52 subportadoras (*ortogonal frequency – división multiplexing*) OFCDM, tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto.

IEEE 802.11c Es la mejora del IEEE 802.d el cual permite combinar el 802.11d con dispositivos compatibles con 802.11 y es en el nivel de enlace de datos capa 2 modelo OSI.

IEEE 802.11d Es un complemento al estándar 802.11 el cual está diseñado para permitir el uso internacional de redes 802.11 locales, esto significa que diferentes dispositivos intercambien información en rangos de frecuencia según lo estipulado por cada país.

IEEE 802.11e Es un estándar para las redes inalámbrica que permite inter operar entre entornos públicos, de negocios y usuarios residenciales, se considera como el primer estándar inalámbrico que permite trabajar en entornos domésticos y empresariales, añadiendo características QoS (*quality of Service* -- es el rendimiento de la red), de soporte multimedia, he introduce el HCF con dos tipos de acceso: De acuerdo a Escudero. [32]

- (EDCA) *Enhanced Distributes Channes Access* o DCF conocida como la función de coordinación distribuida, la cual es una técnica fundamental

[32] ESCUDERO Alberto "Unidad 02: Estándares en Tecnologías Inalámbricas" [En línea]. 2007 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

para el control de acceso al medio para la redes de área local inalámbricas empleando el método CSMA/CA

- (HCCA) *Controlled Acces* o PCF conocida por la coordinación puntual, el cual una estación tienen autoridad para decir que estación puede trasmitir en cada momento

La incorporación de cuatro nuevas categorías de acceso al medio

- *Background* **(AC_BK)**
- *Best Effort* **(AC_BE)** Mecanismo que designa un tipo de servicio de red en el que la red no puede garantizar que los datos lleguen a su destino.
- Video (**AC_VI)**
- *Voice* (**AC_VO)** estas cuatro categorías se crean para diferenciar el tráfico y dan diferentes tiempos de acceso.

IEEE 802.11 f Se aplica a los proveedores de puntos de acceso permitiendo que los productos sean compatibles utilizando el protocolo IAPP el cual permite que el usuario itinerante cambie de un punto de acceso a otro.

IEEE 802.11g velocidad de trasmisión de 54Mbps pero funciona en 2.4Ghz es la interacción de 802.11g y 802.11b, esto permite operar con las tecnologías RF, DSSSS, OFDM, ofreciendo que las tramas den información acerca del punto de acceso y de la celda inalámbrica sin el cliente 802.11b[33]

[33] LÓPEZ Juan Miguel, DOMÍNGUEZ Roció, BENÍTEZ Rubén "Seguridad en redes Inalámbricas" [En línea]. 2010 [Citado: 16 mayo de 2016] Disponible en Internet: http://informatica.gonzalonazareno.org/plataforma/file.php/7/G21.pdf

IEEE 802.11h Modificación del estándar 802.11 para WLAN, el cual intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radar, para minimizar el impacto de abrir la banda 5Ghz la cual es utilizada por sistemas militares, que permite la selección de frecuencias y control de potencia **DFS** función requerida por la WLAN que operan en la banda de 5 GHZ con el fin de evitar, interferencias con sistemas de radar, **TPC** Función requerida por la **WLAN para** asegurar que se respeten las limitaciones de potencia trasmitida en los diferentes canales.

IEEE 802.11i Trata sobre la vulnerabilidad en los protocolos de autenticación y de codificación **TKIP** (protocolo de claves integra, segura-temporal) **AES** (cifrado avanzado) WPA2[34]

IEEE 802.11k Permite a los conmutadores y puntos de acceso **inalámbricos** calcular y valorar los recursos de radiofrecuencia de los cliente WLAN.

IEEE 802.11n velocidad máxima de trasmisión hasta de 600Mbps se puede emplear a 2 bandas 2.4 o 5 Ghz al mismo tiempo, empleando el cable UTP categoría 5° permite velocidades hasta de 1000Mbps, es una nueva revisión al estándar 802.11 sobre la velocidad real de trasmisión aplicado en tecnologías LTE, UMTS, *Wimax* y con soporte en ADLS que trae esta tecnología.

IEEE 802.11v permite la configuración remota de los dispositivos, cliente, lo cual permite una gestión de las estaciones de forma centralizada[35]

[34] ESCUDERO Op. cit. p.41.
[35] Ibid,. p.41.

2.3 MARCO CONCEPTUAL

2.3.1 Falta de seguridad: La principal consecuencia de la llamada "propagación desmedida" de ondas radiales es que personas no autorizadas pueden escuchar la red, logrando a acceder a información que transita por la red, de tal forma que se altere o hurte información vital para una persona u organización, afectando latentemente la disponibilidad, confidencialidad e integridad de la misma.

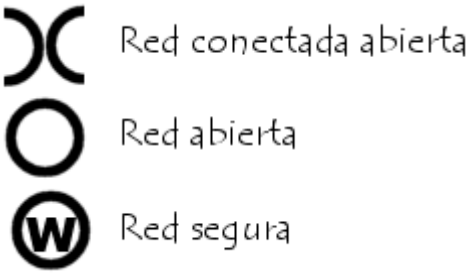
2.3.2 *War-driving:* Debido a lo fácil que es "escuchar" redes inalámbricas, algunas personas recorren la ciudad con un ordenador portátil (o PDA) compatible con la tecnología inalámbrica en busca de redes inalámbricas. Esta práctica se denomina *war driving* (a veces se escribe *wardriving o war-Xing*). *Software* especializado en "*war-driving*" permiten hacer un mapa exacto de la ubicación de estos puntos de acceso abiertos con la ayuda de un sistema de posicionamiento global (GPS).[36]

Estos mapas pueden revelar las redes inalámbricas inseguras que están disponibles y a veces permiten que las personas accedan a Internet. De hecho, en 2002 unos estudiantes londinenses inventaron una especie de "lenguaje de signos" para mostrar dónde están las redes inalámbricas al indicar su presencia con símbolos dibujados con tiza en las veredas. Esto se denomina "*warchalking*". Dos semicírculos opuestos significa que el área está cubierta por una red abierta que provee acceso a Internet, un círculo indica la presencia de

[36] CCM, Los riesgos relacionados con las redes inalámbricas (802.11 o Wi). [En linea]. 2016 [Citado: 25-May-2016] Disponible en internet: http://es.ccm.net/contents/792-los-riesgos-relacionados-con-las-redes-inalambricas-802-11-o-wi

una red inalámbrica abierta sin acceso a una red conectada y una W dentro de un círculo revela que es una red inalámbrica adecuadamente segura.

Figura 1. Símbolos para revelar redes inalámbricas inseguras



(CCM, 2016)

2.3.3 Riesgos de seguridad: Existen muchos riesgos que surgen de no asegurar una red inalámbrica de manera adecuada:

- La intercepción de datos es la práctica que consiste en escuchar las transmisiones de varios usuarios de una red inalámbrica.
- El *crackeo* es un intento de acceder a la red local o a Internet.
- La interferencia de transmisión significa enviar señales radiales para interferir con tráfico.
- Los ataques de denegación de servicio inutilizan la red al enviar solicitudes falsas.

2.3.4 Intercepción de datos*:* Una red inalámbrica es insegura de manera predeterminada. Esto significa que está abierta a todos y cualquier persona dentro del área de cobertura del punto de acceso puede potencialmente escuchar las comunicaciones que se envían en la red. En el caso de un individuo, la amenaza no es grande ya que los datos raramente son confidenciales, a menos que se trate de datos personales. Sin embargo, si se trata de una compañía, esto puede plantear un problema serio.[37]

2.3.5 Intrusión de red*:* Es por esto que una red inalámbrica insegura les ofrece a los *hackers* la puerta de acceso perfecta a la red interna de una compañía u organización.

Permitiendo al *hacker* robar o destruir información de la red y de darle acceso a Internet gratuito, la red inalámbrica también puede inducirlo a llevar a cabo ataques cibernéticos. Como no existe manera de identificar al *hacker* en una red, puede que se responsabilice del ataque a la compañía que instaló la red inalámbrica.[38]

[37] CCM, Op. cit. p.44.
[38] Ibid,. p.44.

2.3.6 Interferencia radial: Una señal se puede interferir fácilmente con una transmisión de radio que tenga una frecuencia cercana a la utilizada por la red inalámbrica.

2.3.7 Denegación de servicio*:* Consiste en esperar hasta que la red este libre antes de transmitir las tramas de datos. Una vez que se establece la conexión, una estación se debe vincular a un punto de acceso para poder enviarle paquetes. Debido a que los métodos para acceder a la red y asociarse a ella son conocidos, un *hacker* puede fácilmente enviar paquetes a una estación solicitándole que se desvincule de una red. El envío de información para afectar una red inalámbrica se conoce como ataque de denegación de servicio.[39]

2.4 MARCO LEGAL

2.4.1 Ley de delitos informáticos en Colombia: Ley 1273 de 2009

Se modificó el Código Penal, donde se creó un nuevo bien jurídico que se llamó: "De la protección de la información y de los datos", preservando los sistemas que utilizan tecnologías de información y comunicación. Esta ley plasmo una serie de delitos como conductas inapropiadas en el manejo de los datos personales, esto aplica principalmente para que las empresas se protejan de llegar a cometer delitos penales. [40]

[39] CCM, Op. cit. p.44.
[40] DIARIO Oficial, Ley 1273 de 2009 [En Línea]. 2009 [Citado: 10 noviembre de 2016] Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Esto con el fin de proteger la información importante y más vulnerable que día a día se transmite por las diferentes redes de comunicación, para preservar la confidencialidad, integridad y disponibilidad.

A continuación se enuncian los artículos de dicha la Ley que aplican para el proyecto:

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTICULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[41]

ARTICULO 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

[41] DIARIO Oficial, Op. cit. p.47.

ARTICULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

ARTICULO 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[42]

ARTICULO 269E: USO DE *SOFTWARE* MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional *software* malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTICULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100

[42] DIARIO Oficial, Op. cit. p.47.

a 1000 salarios mínimos legales mensuales vigentes.

ARTICULO 269G: SUPLANTACIÓN DE SITIOS *WEB* PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.[43]

ARTICULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

[43] DIARIO Oficial, Op. cit. p.47.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.[44]

CAPITULO SEGUNDO

De las atentados informáticos y otras infracciones

ARTICULO 2691: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. [45]

ARTICULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito

[44] DIARIO Oficial, Op. cit. p.47.
[45] Ibid,. p.47.

sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[46]

[46] DIARIO Oficial, Op. cit. p.47.

3. MARCO METODOLÓGICO

Define la manera como se realiza el estudio de una investigación, los pasos y métodos a seguir.

3.1 Metodología de la investigación

El propósito de esta metodología es definir o encontrar el significado de los hechos o fenómenos, con el fin de dirigir una investigación científica, y a partir de ella encontrar, demostrar, refutar y aportar un conocimiento. Su principal característica es elegir diferentes datos, sistematizarlos y obtener nuevos conocimientos.

Su visión debe ser objetiva y buscar la información necesaria para confirmar, demostrar y aportar nuevos conocimientos, por medio de validaciones que comprueben cada uno de los conocimientos.

Este tipo de metodología es descriptiva, basada en explicar las características más importantes de un fenómeno, en cuento a por que ocurren, con qué frecuencia ocurren y como se desarrollan. [47]

3.2 Investigación Cuantitativa: Se requiere conocer que conforma el problema, como limitarlo, en qué dirección va, que incidencia tiene entre sus elementos y hasta dónde puede llegar y terminar.

Se establece que el tipo de metodología que se maneja en este proyecto es investigativa con enfoque cuantitativo, ya que se expone la manera como se va

[47] GALÁN Manuel "Guía Metodológica" [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: http://manuelgalan.blogspot.com.co/p/guia-metodologica-para-investigacion.html.

a realizar el estudio, los pasos para realizarlo y su método. Donde es posible hablar de una metodología aplicada a todos los campos, que recoge las pautas presentes en cualquier proceder con el aumento del conocimiento y solución de problemas.

4. RESULTADOS

Una guía que brinde a los lectores conocimientos en cuanto a vulnerabilidades, riesgos y amenazas en las redes inalámbricas, con estrategias, mecanismos o esquemas de seguridad que permitan trabajar con redes inalámbricas seguras.

Teniendo en cuenta los protocolos de cifrado analizados, la combinación del protocolo WPA2 y el cifrado AES, lo que hace fuerte una red Wi-Fi, debido a que son redes vulnerables, de fácil acceso y están en permanente actividad lo que mantiene a los *hackers* en alerta para asechar, obtener información muy valiosa provocando daños contundentes, y conociendo que existe una cantidad de formas de *hackear* las redes.

Por lo tanto sea la red inalámbrica que se esté utilizando, debe tener en cuenta que procedimientos de seguridad seguir, teniendo en cuenta la configuración de red segura, conforme a lo visto en el proyecto y utilizarlo de manera correcta.

4.1 Identificación de vulnerabilidades, amenazas y riesgos

4.1.1 Riesgos Pasivos : Ocurren cuando un usuario no autorizado accede a la red para espiar o robar información, con la finalidad de analizarla y en el momento justo realizar un ataque, estos son un poco difíciles de detectar, ya que en el momento de robar la información no se efectúan alteración de datos. Entre los ataques pasivos se encuentran: Como indica Ruiz. [48]

***Warchalking / Wardriving*:** Consiste en recorrer diferentes lugares con una computadora portátil con la finalidad de buscar puntos de acceso inseguros y al encontrarlos son marcados con símbolos, esto ocurre igualmente, desde un automóvil y por medio de un GPS y obtener las coordenadas de los puntos de acceso.

Existe un *software* libre muy popular para ejecutar *warchalking y wardriving* llamado *NETSTUMBLER*.

***Sniffing* o Intercepción de datos:** Consiste en conocer las transmisiones de los usuarios en una red. Son programas que permiten capturar, interpretar y almacenar paquetes de datos, con la finalidad de obtener contraseñas, usuarios, direcciones electrónicas, información financiera, entre otras.

[48] JULIO RUIZ, José "Seguridad en redes Wi-Fi inalámbricas" [En línea]. 2004 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml.

4.1.2 Riesgos Activos: Estos ocurren cuando un usuario no autorizado modifica o altera el contenido de la información o impide el acceso a ella, entre los más comunes se encuentran: [49]

Enmascaramiento o Suplantación: Es conocido como robo de identidad, imitación o falsificación. Consiste en suplantar un usuario e intervenir en el momento que este no se encuentre conectado.

También se puede reemplazar un punto de acceso. Se presentan diferentes tipos de enmascaramiento o suplantación:

- *Secuestro de Sesión:* El atacante monitorea la red e inicia a recopilar usuarios, claves, direcciones MAC, SSID, y envía un ataque denegando el servicio, para el poder acceder a la red y utilizar la información de la red. Este secuestro no dura mucho, pero se puede hacer a varios usuarios.
- *Suplantación de dirección MAC:* Estos ocurren cuando la red cuenta con baja seguridad permitiendo el filtrado de direcciones MAC.

Denegación de servicio (DoS): Su objetivo es volver inútil la red y sacar los usuarios autorizados, son difíciles de identificar ya que duran poco y solo se pueden identificar en tiempo real y se detectan de acuerdo al comportamiento del punto de acceso. Existen diferentes formas de denegación de servicio:

- *Saturar el ambiente:* es básicamente inyectar ruido por medio de microondas

[49] JULIO RUIZ, Op. cit. p.56.

- *Torrente de autenticaciones:* se realizan muchas peticiones de autenticación falsa, de forma repetitiva y simultánea, de manera que la red se mantiene ocupada
- *Modificación de paquetes WPA:* permite sin querer los ataques de denegación de servicio, se alteran los paquetes, logrando desconectar automáticamente los usuarios
- *Signaling DOS:* finaliza la sesión de móviles activos en la red, comprende él envió de pequeñas cantidades de datos, es un ataque a bajo nivel pero que genera congestión.

Retransmisión: También conocido como Hombre en el medio MITM, el atacante se ubica en medio de una comunicación, analiza el tráfico de la red y simula ser el ID o dirección MAC, al emular ser un punto de acceso, bloquea la información del usuario la transmite y modifica para engañar al receptor.

Estos ataques tienen la finalidad que una tercera persona adquiera la posibilidad de leer, insertar y modificar los paquetes de datos entre dos entes, sin que ninguna de las partes se dé cuenta. [50]

Para ejecutar dicho ataque se realiza desde un dispositivo *Android* mediante *dSploit* se ejecuta dicha aplicación y se espera que el programa analice la red. Una vez identificados todos los equipos de la red, se elige a la próxima víctima. Es de recordar que se puede realizar el ataque a toda la máscara de subred, a la puerta de enlace del *Router* o a un equipo determinado.

Inicialmente se debe seleccionar el destinatario a realizar el ataque, en este caso se realizara un ataque a toda la máscara de subred y una vez se

[50] PROFESORES, ARP SPOOFING - MITM, ATAQUE Y MITIGACION. [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en: http://profesores.elo.utfsm.cl/~agv/elo323/2s14/projects/reports/MoraMorales/mitm_kali.html

selecciona el ataque MITM, aparecen diferentes tipos de ataques basados en MITM, entre los que se encuentran:

- Simple *Sniffer*: se muestra el tráfico de la red, lo que utiliza cada equipo en la red.
- *Password Sniffer*: se filtra el tráfico de la red para identificar contraseñas de servicios FTP, IMAP, MSN, etc.
- *Session Hijacker*: filtra y guarda las *cookies* de inicio de sesión y así poder suplantar la identidad de las personas.
- *Kill Connections*: permite bloquear la conexión de los equipos a la red.
- *Redirect*: Hacer que el trafico http se dirija a otra *web*
- *Replace Images*: reemplaza las imágenes de una *web* por las que se desee
- *Replace* Videos: reemplaza los de videos de *youtube* por lo que se desee
- *Script Injection*: se inserta un *javascript* en todas las páginas *web* que se visiten
- *Custom Filter*: realiza el filtro a todo el texto de una *web* y lo cambia por otro[51]

4.2 Evaluar la seguridad mediante pruebas sobre las redes inalámbricas.

En primer lugar conocer las herramientas o aplicaciones para realizar diferentes pruebas de validación en la seguridad de las redes inalámbricas:

[51] PROFESORES, Op. cit. p.58.

4.2.1 Pruebas de penetración: consiste en un conjunto de metodologías y técnicas, que se realizan para la evaluación integral de los sistemas informáticos, para este caso para las redes inalámbricas y todos los dispositivos conectados a ella. [52]Consiste en realizar intentos de acceso desde diferentes puntos de entrada. Los objetivos principales son:

- Evaluar una red inalámbrica
- Demostrar los riesgos a los que se encuentra expuesta
- Conocer la situación real de red
- Realizar mantenimiento de seguridad

Existen diferentes tipos de penetración de pruebas:

- *Externo:* su objetivo es acceder remotamente desde fuera del *firewall* y penetrar a la zona desmilitarizada para acceder a la red interna, se pueden realizar pruebas de:

  Captura de tráfico

  Pruebas de fuerza de usuarios y contraseñas

  Detección de conexiones externas y rangos de direcciones

  Detección de protocolos utilizados

  Escáner de puertos TCP, UDP, ICMP

- *Interno:* su objetivo es demostrar el nivel de seguridad interno, se pueden realizar una serie de pruebas:

  Autenticación de usuarios

  Análisis de protocolos internos y sus vulnerabilidades

  Validación de permisos y recursos compartidos

[52] SILVA, Felix "Penetration Testing". [En Línea] 2016 [Citado: 16 mayo de 2016] Disponible en Internet: https://docs.google.com/presentation/d/1e3-VDVAdiV4tb-lNQ-v7hv581rhZHHg8i8cJ5gETQCk/htmlpresent?hl=es

Pruebas a los servidores (FTP, WWW, DNS, SMTP, etc.)

Validación del nivel de detección de intrusiones

Análisis de seguridad en estaciones de trabajo

Seguridad de la red

Las pruebas se realizan en las cuatro grandes etapas:[53]

- ✓ **Fase de Planeación:** Es importante determinar controles para la seguridad de acuerdo a las vulnerabilidades encontradas, y determinar un plan de revisión con el análisis de riesgo para evitar la materialización del ataque. En esta fase se define el alcance del servicio, que comprende las siguientes actividades:
  - ➢ Definir y validar el plan de trabajo , interlocutores, fechas, claves
  - ➢ Definir los roles y responsabilidades
  - ➢ Conducir la reunión con el personal de seguridad y la clave

  Depende del levantamiento de la información se establecerá las herramientas necesarias para la aplicación de las pruebas de vulnerabilidades.

  Se realiza un reconocimiento inicial de las variables que pueden ser objeto de explotación

  - ❖ **Acceso a la Red**: El objetivo asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información.

[53] SILVA, Op. cit. p.60.

- ❖ **Puertos de Red**: Identificación de la aplicación va dirigida a un puerto, Cada proceso que se comunica con otro se identifica a sí mismo a la familia de protocolos TCP/IP por uno o más puertos.
- ❖ **Configuración del Sistema:** Todo los sistemas operativos vienen por configuraciones que muchas veces tienen vulnerabilidades, estas configuraciones pueden ser cambiadas para no dejar un riesgo (Una vulnerabilidad que puede ser aprovechada).

✓ **Fase de Descubrimiento:** Es importante determinar controles para la seguridad de acuerdo a las vulnerabilidades encontradas, y determinar un plan de revisión con el análisis de riesgo para evitar la materialización del ataque. En esta fase se define el alcance del servicio, que comprende las siguientes actividades:

- Rangos de direcciones IP dentro de la red

- Direcciones IP de servidores terceros [54]

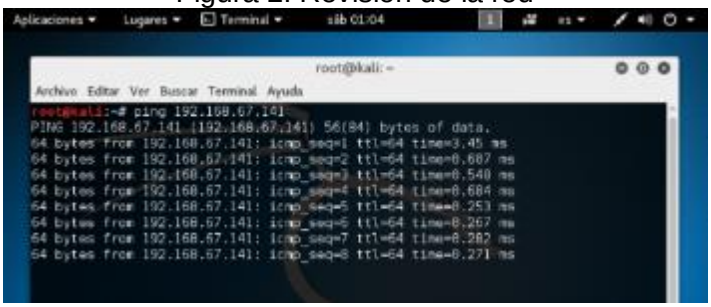
Las pruebas ejecutadas durante la fase de descubrimiento y monitoreo de red para la aplicación de pruebas de vulnerabilidades, utilizando la herramienta de *Nmap*, ya que permite hacer un mapa de la red, encontrando los dispositivos conectados en la red escaneada y detecta los servicios de puertos abiertos que están en cada uno de ellos, mostrando la información detallada de los terminales a atacar:

Pruebas Internas y Externas

[54] SILVA, Op. cit. p.60.

a. Revisión de la red /pruebas de conectividad

Figura 2. Revisión de la red

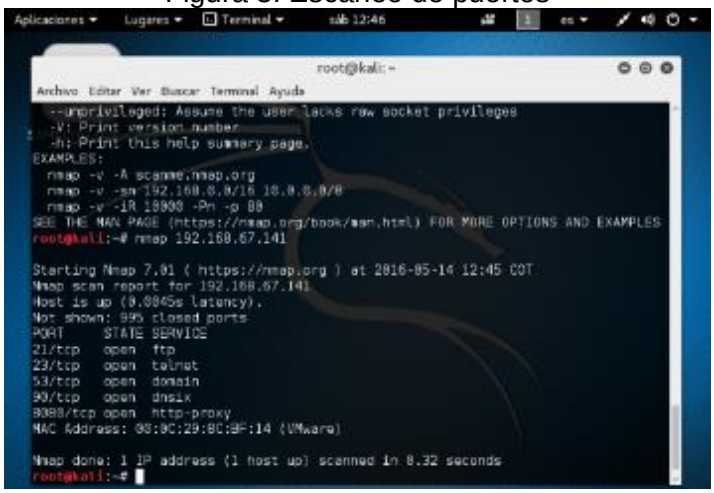


Fuente: El autor

b. Escaneo de puertos y Servicios de cada uno de los objetivos

Con esta actividad se identifica los puertos visibles, esto proporciona una información inicial acerca de potenciales puntos de acceso

Figura 3. Escaneo de puertos

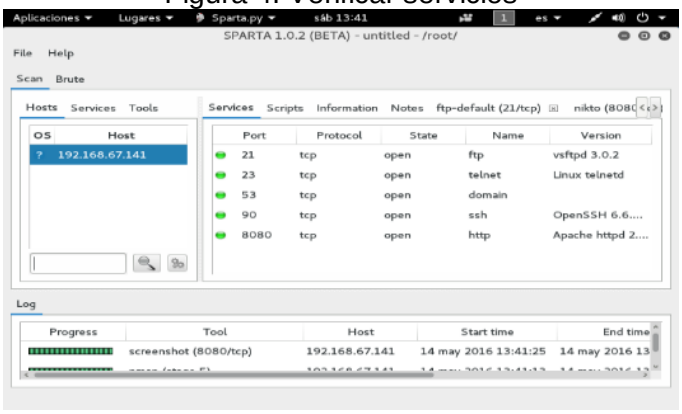


Fuente: El autor

c. Identificación de los servicios y Enumeración

Una vez se realice el escaneo se debe verificar el servicio existente en cada puerto

Figura 4. Verificar servicios

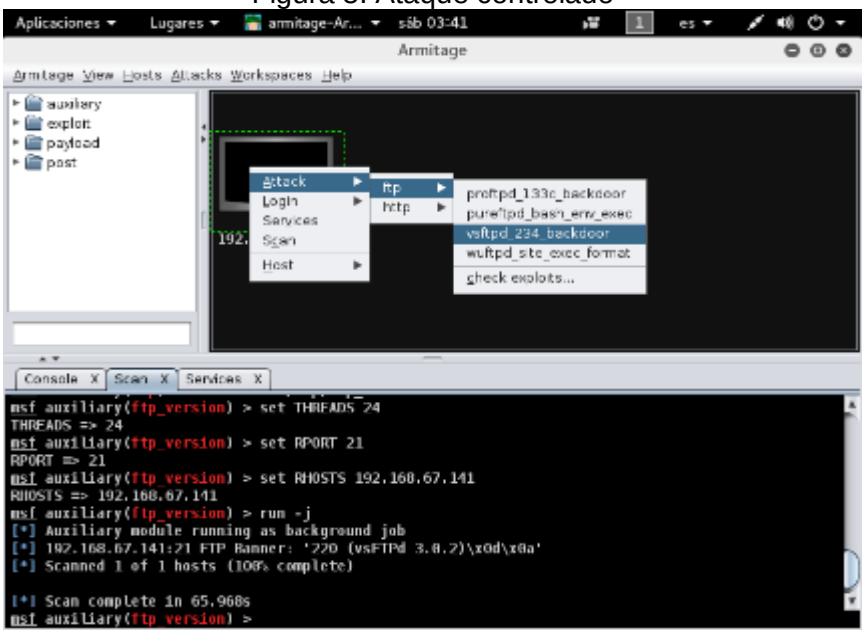


Fuente: El autor

- ✓ **Ataque:** En esta fase después de recopilar la información, con las vulnerabilidades asociadas a cada sistema y cada una de estas variables se aplican las pruebas de explotación en un ambiente controlado, se ejecuta con lineamientos establecidos.

  Para este ataque se utiliza la herramienta *Artimage* que viene incorporada en el *Kali Linux*:

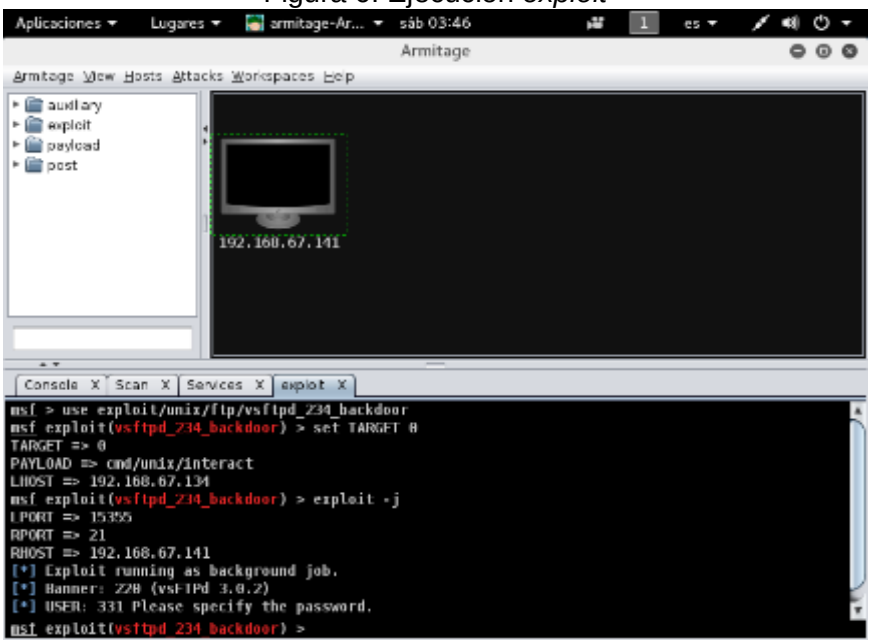
Figura 5. Ataque controlado



Fuente: El autor

Se ejecuta el *exploit* en donde comprobaremos como atacó el puerto 21 en donde el servicio ftp que se encuentra abierto

Figura 6. Ejecución *exploit*



Fuente: El autor

- ✓ **Fase de Reporte**

  Se contemplan los resultados y la validación final:

  - Validación de hallazgos, riesgos y recomendaciones
  - Elaboración de informe con resultados de la evaluación e identificar las oportunidades de mejora
  - Emisión de informe final validado

  Con el uso de *Nmap* en el equipo se detectaron vulnerabilidades de riesgo medio y bajo se relacionaron con la actualización de librerías y huecos de seguridad en la configuración del servidor ftp, esto permitió conocer los puntos débiles del equipo y las aplicaciones y hacer las correcciones necesarias para proteger el sistema.

  Mediante el correcto uso de la herramientas mencionada se logró conocer los puntos vulnerables de la red [55]

[55] SILVA, Op. cit. p.60.

4.2.2 ***Metasploit***: es una herramienta de penetración libre utilizada para detectar vulnerabilidades y permite hacer pruebas de penetración contra sistemas remotos. Tiene también un *framework* para realizar sus propias herramientas y está tanto para *Linux* como para *Windows*. Existen muchos tutoriales por la red donde explican cómo utilizarlo. [56]

La finalidad de esta herramienta es poner a prueba los controles de seguridad, al lograr violarlas se crean planes de acción antes de que atacantes maliciosos las descubran.

Cada una de las pruebas realizadas varía en diferentes técnicas y métodos.

4.2.3 NMAP: Es el mejor programa para seguridad en redes, para la exploración de redes y sondeo de puertos y seguridad, se puede usar para encontrar equipos y servicios en la red, se utiliza para escanear puertos, descubrir servicios pasivos en una red y da detalles de equipos de una red como: sistema operativo, tiempo que lleva conectado, *software* utilizado para ejecutar un servicio, la presencia de *firewall* y la identificación de la tarjeta de red.[57]

Funciones:

- Pruebas de seguridad

- Pruebas de penetración

- *Hacking*

- Buscar aplicaciones no autorizadas ejecutándose en un servidor

[56] SOTO, Jason “Qué es Metasploit?” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: https://www.jsitech.com/linux/que-es-metasploit/

[57] REDIRIS “Sistemas de detección de intrusos” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: https://www.rediris.es/cert/doc/unixsec/node26.html

- Buscar objetivos potenciales

- Inventario de computadores en red

- Auditorias de seguridad informática

- No es detectado por los Sistemas de detección de intrusos

- No interfiere con las operaciones de las redes y las computadoras analizadas

Resultados:

- Identifica servidores y host

- Identifica puertos abiertos de una computadora

- Determina servicios ejecutándose

- Determina sistema operativo

- Determina versión

- Obtiene características de *hardware* de red[58]

4.2.4 Otras herramientas

***Wireshark*:** *sniffer* de paquetes, se utiliza para analizar el tráfico de red. Es parecido a *tcpdump* (luego hablamos de él) pero con una GUI y más opciones de ordenación y filtro. Coloca la tarjeta en modo promiscuo para poder analizar todo el tráfico de la red. También está para *Windows*. [59]

***Netcat*:** herramienta que permite abrir puertos TCP/UDP en un equipo remoto (después se queda a la escucha), asociar una *shell* a ese puerto y forzar

[58] REDIRIS Op. cit. p.66.
[59] SEGU.INFO Seguridad de la Información “Detección de Intrusos en Tiempo Real” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.segu-info.com.ar/proteccion/deteccion.htm

conexiones UDP/TCP (útil para rastreo de puertos o transferencias *bit* a *bit* entre dos equipos).

***Kismet*:** sistema de detección de redes, *sniffer* de paquetes y de intrusión para redes inalámbricas 802.11.

Dentro del desarrollo de este objetivo se proponen escenarios de prueba para ejecutar con las diferentes herramientas de acuerdo a su utilidad y necesidad.

Entre los escenarios de pruebas se pueden seguir los siguientes (Ver Cuadro 1):

Cuadro1. Set de pruebas propuestas

SET DE PRUEBAS PROPUESTAS	
Nombre de prueba	**Descripción prueba**
IDENTIFICACIÓN DE REDES OCULTAS	Verificar si en el perímetro se encuentran SSID ocultos, para establecer si se trata de redes no autorizadas.
FALSO PUNTO DE ACCESO INALÁMBRICO	Punto de Acceso Falso para engañar clientes y lograr que se conecten a un SSID falso.
ROMPIMIENTO DE CONTRASEÑA	Interceptación de tráfico e inyección maliciosa del mismo para atrapar vectores de inicialización que permitan adivinar o predecir la contraseña de acceso
DENEGACIÓN DE SERVICIO – PRUEBA DE CONCEPTO	Inundación de peticiones que busca suspender un servicio, Prueba de Concepto para validar si la infraestructura es vulnerable.
FALSO PUNTO DE ACCESO INALÁMBRICO + HOMBRE EN EL MEDIO – PRUEBA DE CONCEPTO	Punto de Acceso Falso al que se conectan clientes engañados y se intercepta el tráfico – Prueba de Concepto.
PHISHING	Falsificación de Portal de Autenticación de Acceso, para robar las credenciales de inicio de sesión.
COBERTURA DE SEÑAL	Pruebas de Alcance Físico de la señal con antenas de diferentes potencias.
VULNERABILIDADES	Comprobación de Vulnerabilidades en las direcciones IP Objetivo.
GEOLOCALIZACIÓN	Utilizando un GPS de conexión USB, es

SET DE PRUEBAS PROPUESTAS	
	posible ubicar en un mapa, las redes al alcance del objetivo.
CODIGO MALICIOSO E INGENIERIA SOCIAL	Utilizando un código malicioso y técnicas de Ingeniería Social, es posible engañar a clientes potenciales para que se conecten a una red inalámbrica trampa.

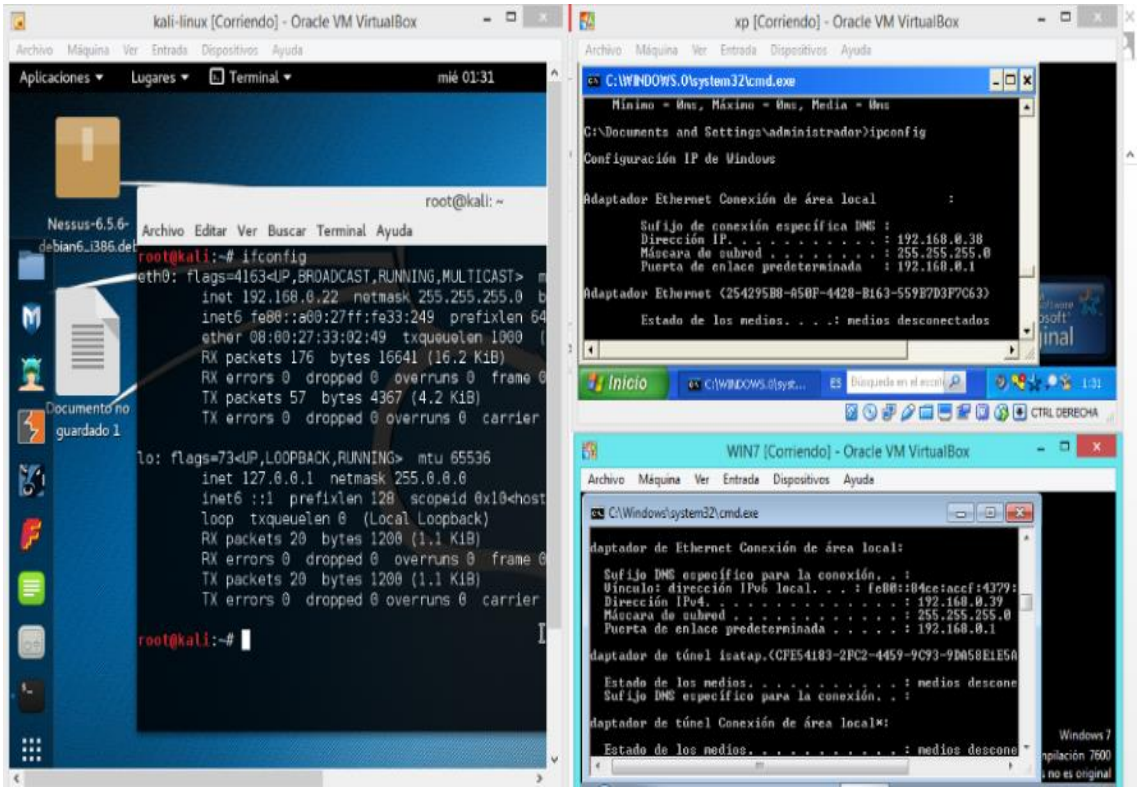
Fuente: Federico Gacharná (julio, 2014) TOP 10 DE PRUEBAS DE PENETRACIÓN Y HACKING A REDES INALÁMBRICAS (http://www.conassol.org/wp-content/uploads/2015/02/TOP-10-DE-PRUEBAS-DE-PENETRACI%C3%93N-Y-HACKING-A-REDES-INAL%C3%81MBRICAS.pdf)

De acuerdo a los escenarios de pruebas encontrados, se realizan las siguientes pruebas y validaciones:

Para el desarrollo de la prueba es necesario 2 máquinas virtuales: XP y *Windows* 7, además de la maquina atacante: *Kali Linux*. Por consiguiente, se procede a validar que exista comunicación entre cada una de ellas.

Primero se verifican las IP de cada una de las maquinas:

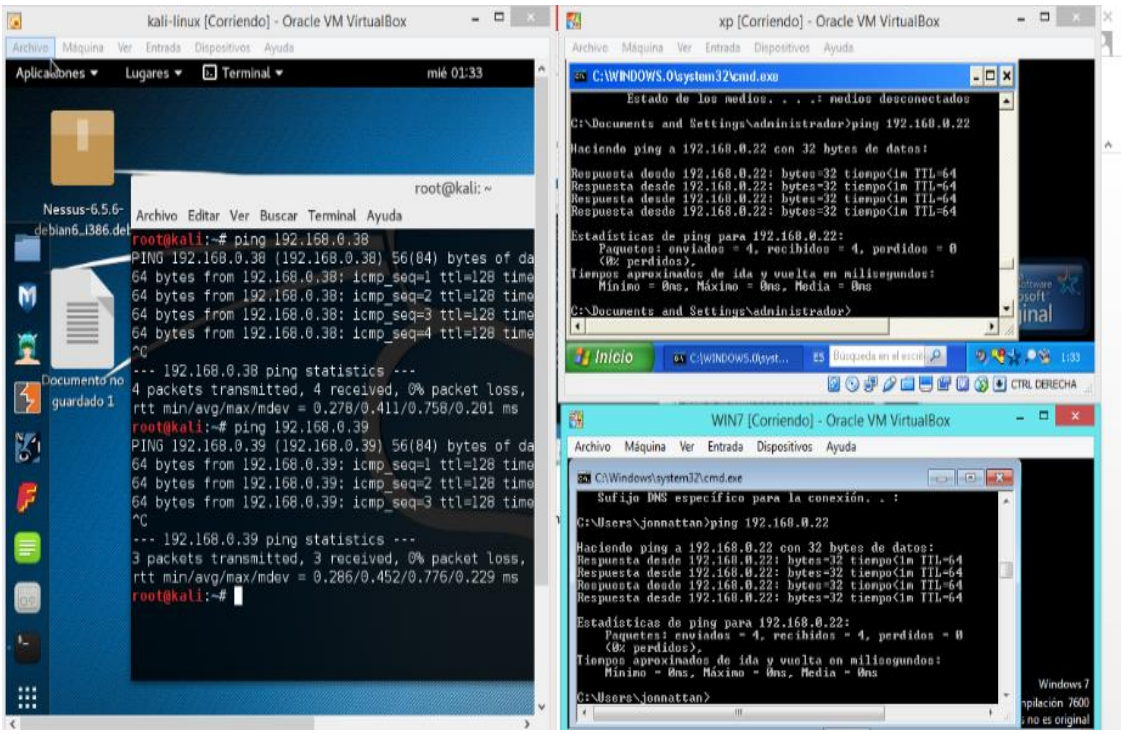
Figura 7. Validación direcciones IP



Fuente: El autor

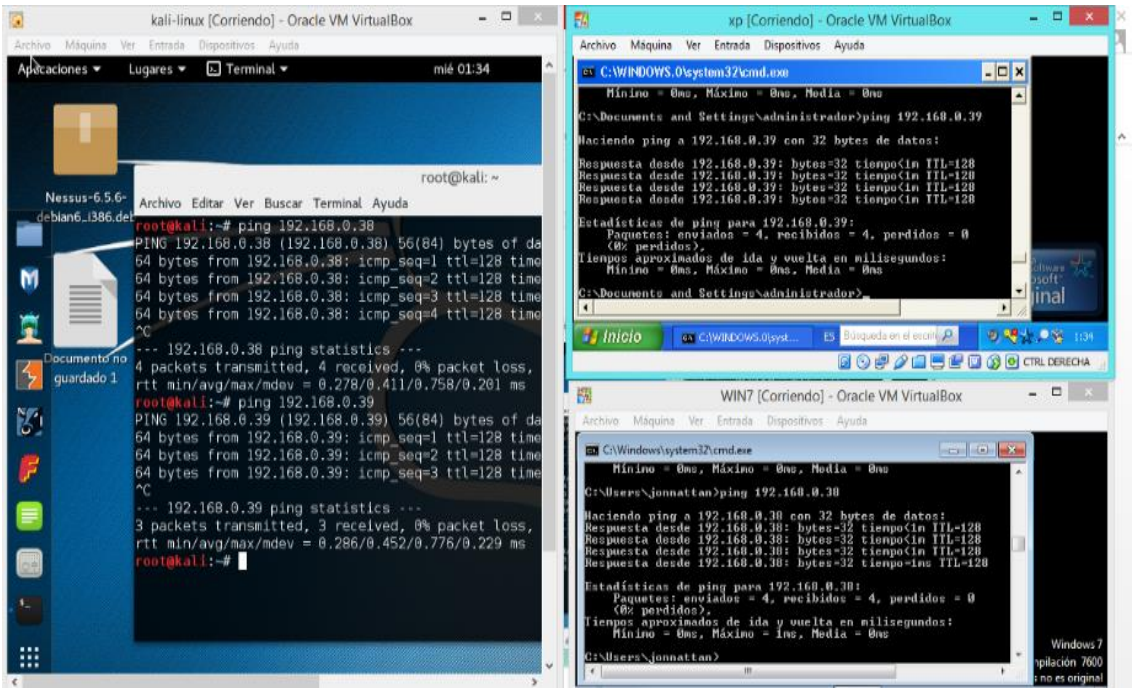
Luego se realiza un ping entre las mismas:

Figura 8. Ejecutar *PING*



Fuente: El autor

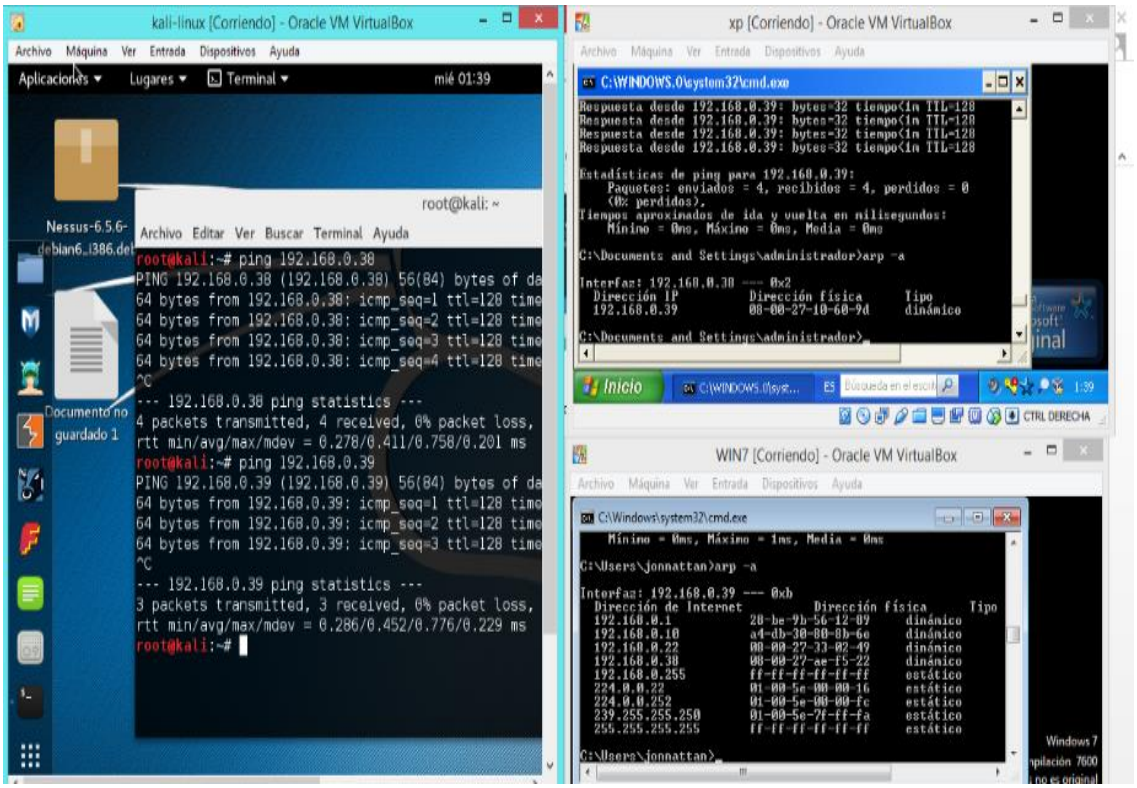
Figura 9. Validación conexión de *hosts*



Fuente: El autor

Ahora se digita el comando *arp –a* tanto XP como en *Windows* 7 para validar la IP y su respectiva MC *Addres*.

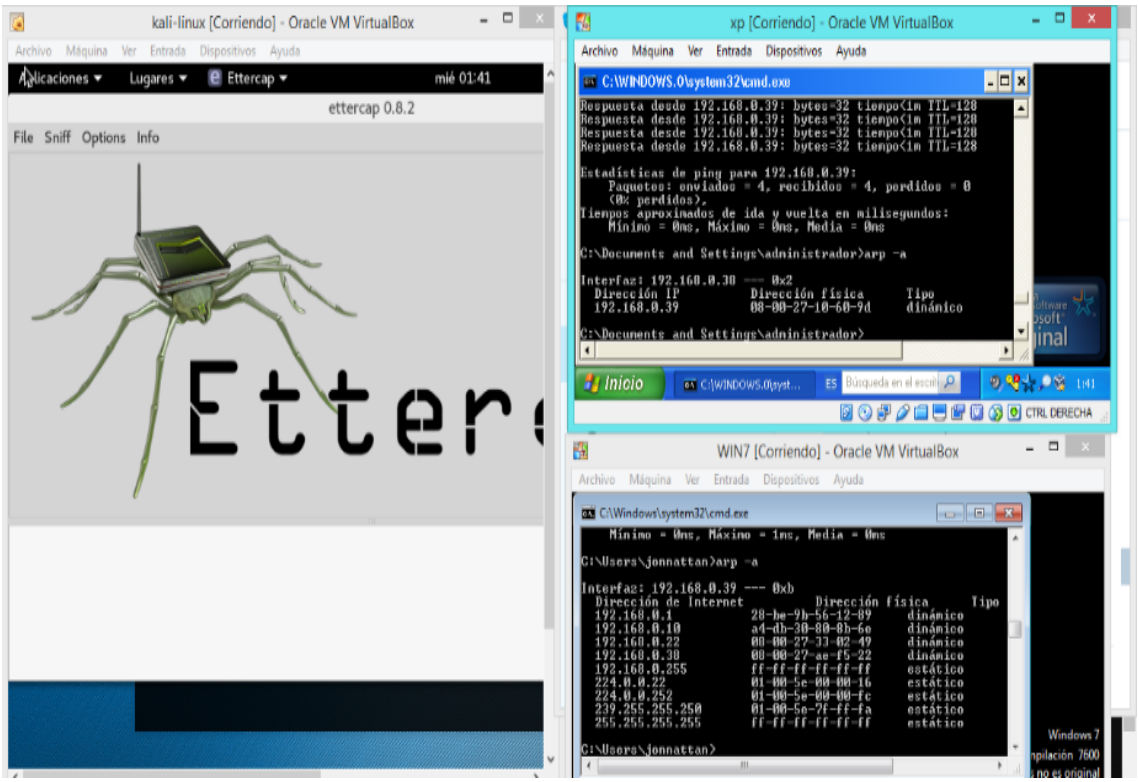
Figura 10. Ejecuta comando *arp -a*



Fuente: El autor

En consecuencia y con el propósito de llevar a cabo el ataque, desde *Kali Linux* y la herramienta *Ettercap*:

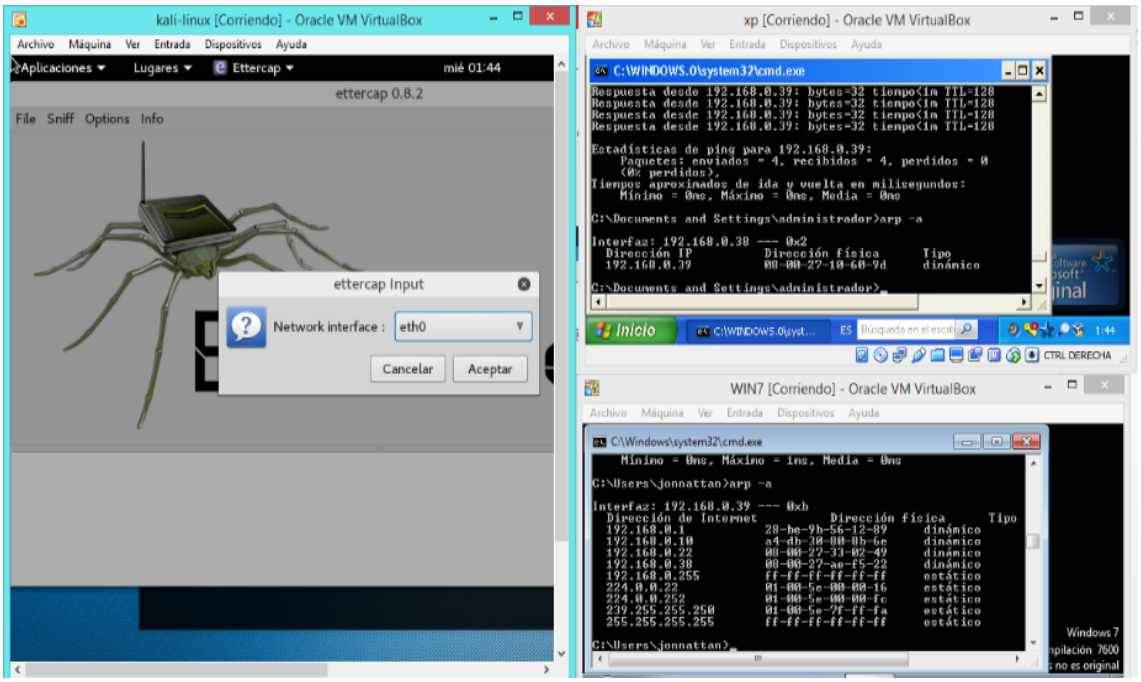
Figura 11. Herramienta *Ettercarp*



Fuente: El autor

Se selecciona en el menú *Sniff, Unified sniffing, eth0* y aceptar:

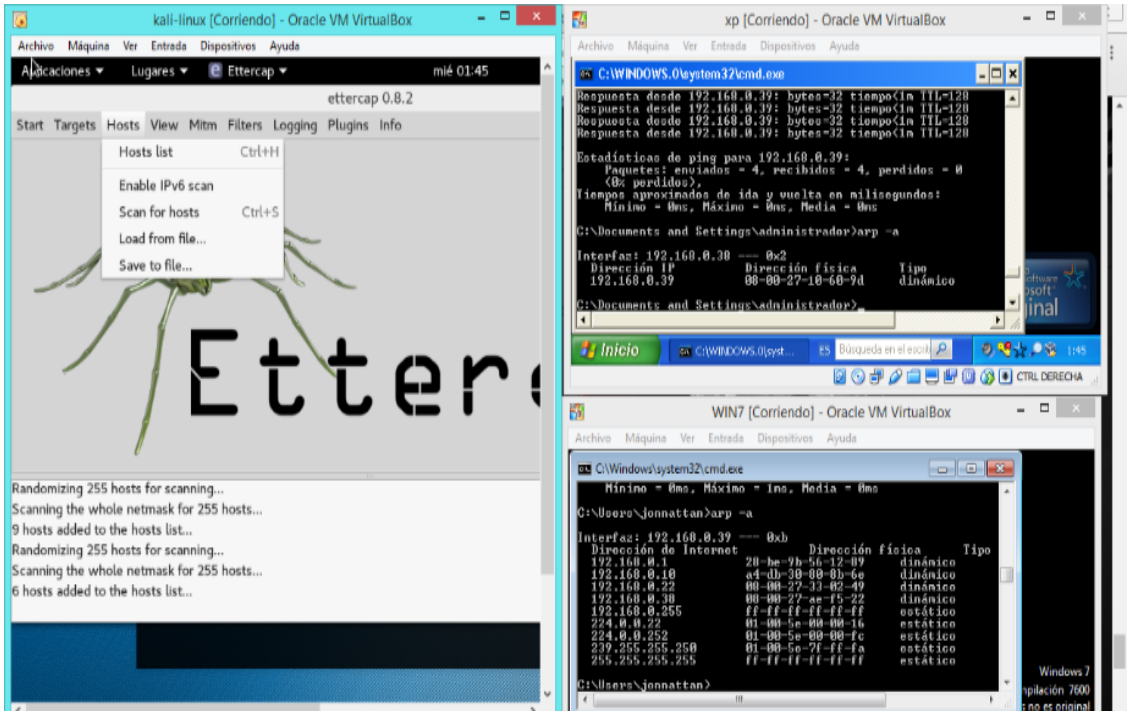
Figura 12. Validación Interfaces



Fuente: El autor

Luego se selecciona *Hosts* en el menú y seguidamente *scan for hosts* para verificar las maquinas conectadas a la red.

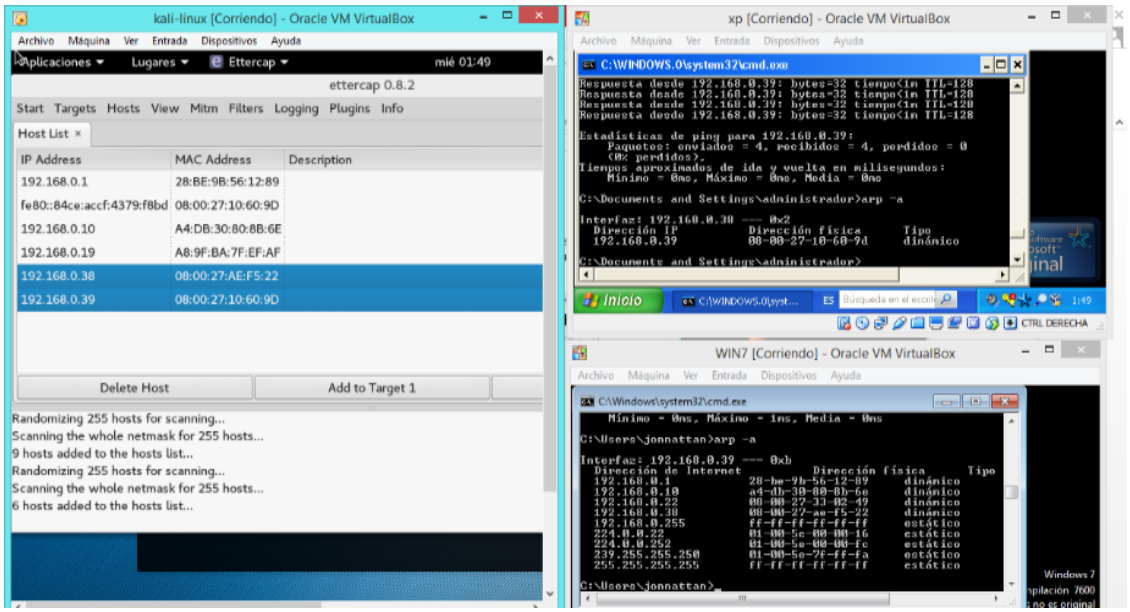
Figura 13. Escaneo de máquinas conectadas



Fuente: El autor

Al terminar este proceso, de nuevo en el menú *Host, Hosts List* y se evidencia que las maquinas 192.168.0.38 *Windows* 7 y 192.168.0.39 XP se encuentran en la red con sus respectivas MAC.

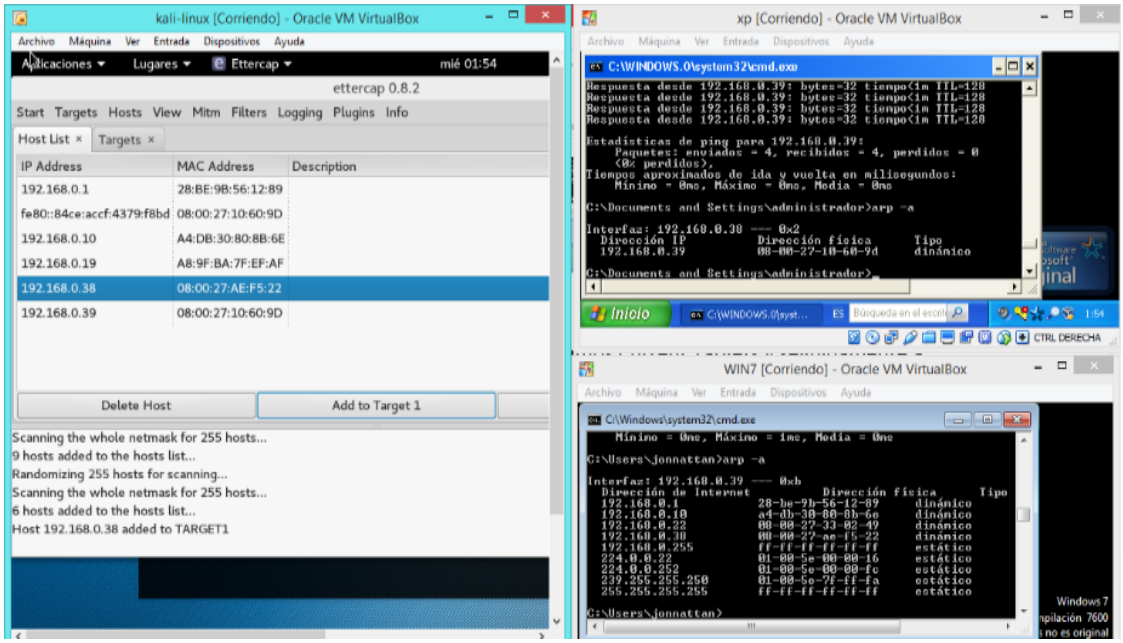
Figura 14. Verifica conexión



Fuente: El autor

Ahora se selecciona *Targets* en el menú, y *Current Targets* y seguidamente a la IP 192.168.0.38 *Windows* 7 dando clic en *Add to Target 1*

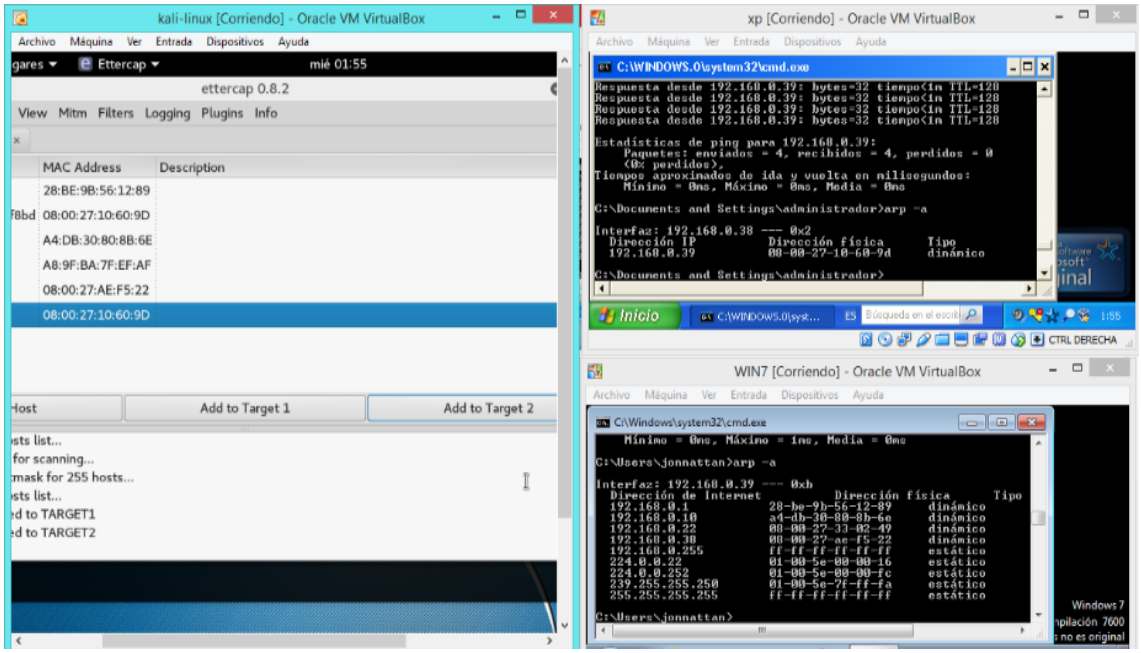
Figura 15. Selecciona *Targets*



Fuente: El autor

Se realiza para la IP 192.168.0.39 XP la misma actividad, pero damos clic en *Add to Target 2.*

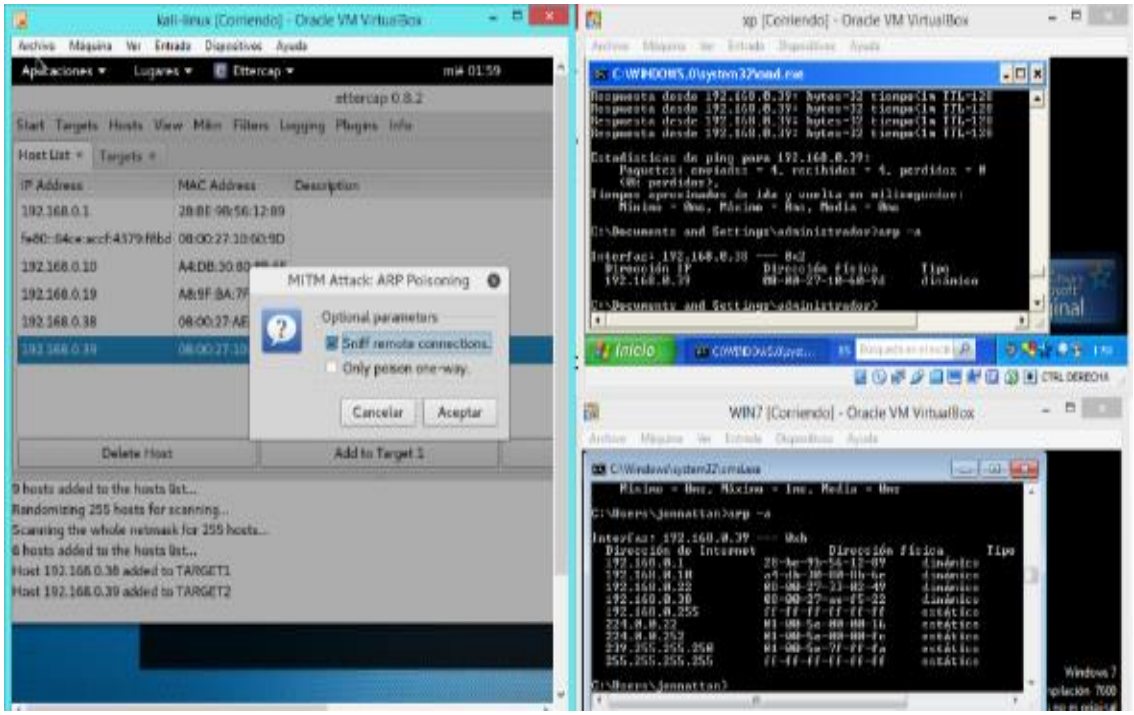
Figura 16. Seleccionar *Targets* segundo equipo



Fuente: El autor

Continuando con el desarrollo de la práctica, se selecciona en el menú *Mint* y ARP *Porsoning*. Dando clic en *Sniff remote connections* y en aceptar

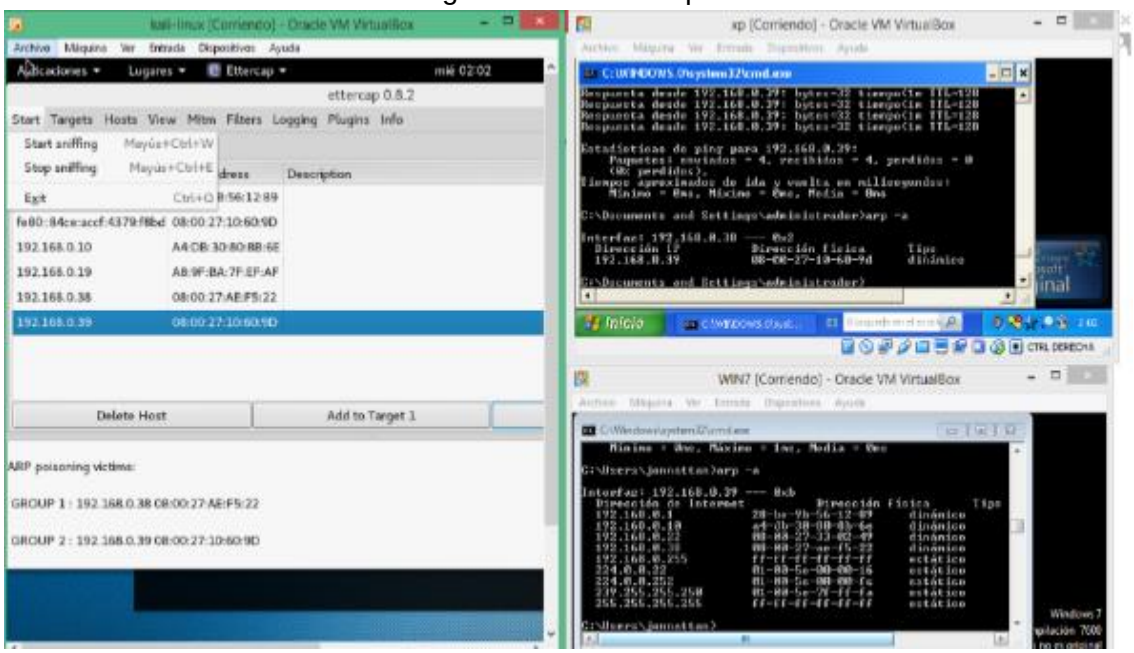
Figura 17. ARP *Porsoning*



Fuente: El autor

Seguidamente, se procede a iniciar el ataque en el menú*: start, start sniffing*

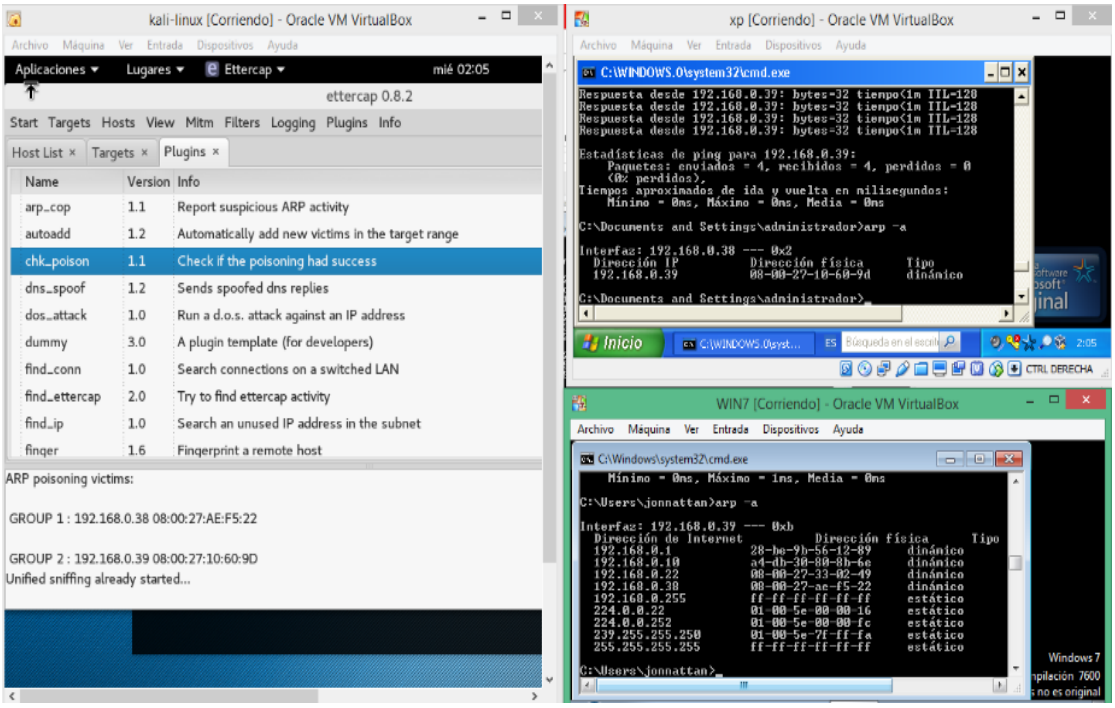
Figura 18. Inicio ataque



Fuente: El autor

Para validar que el ataque se ha realizado de manera correcta, se da clic en *Plugins* en el menú, luego *Manage Plugins* y por ultimo doble clic en *chk_poison*.

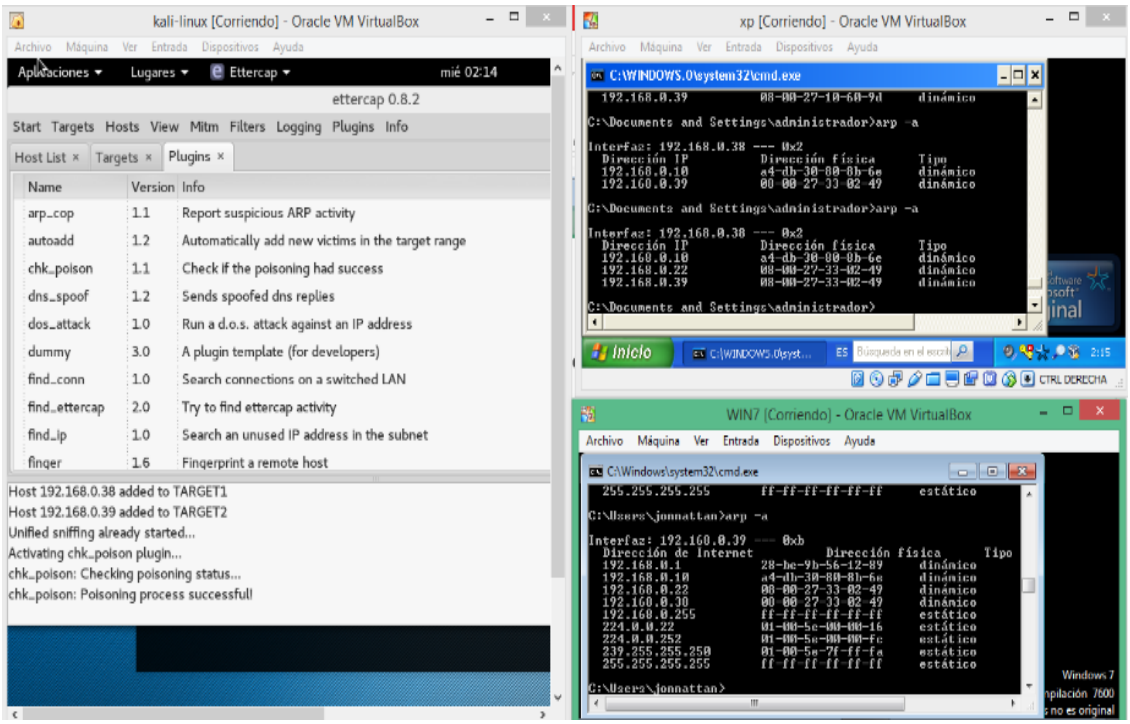
Figura 19. Validación *Spoofing*



Fuente: El autor

Luego desde las maquinas 192.168.0.38 Windows 7 y 192.168.0.39 XP, se ejecuta el comando *arp –a* y se evidencia que se encuentra la dirección de *Kali Linux* con la dirección 192.168.0.22 con la misma *Mac Addres*

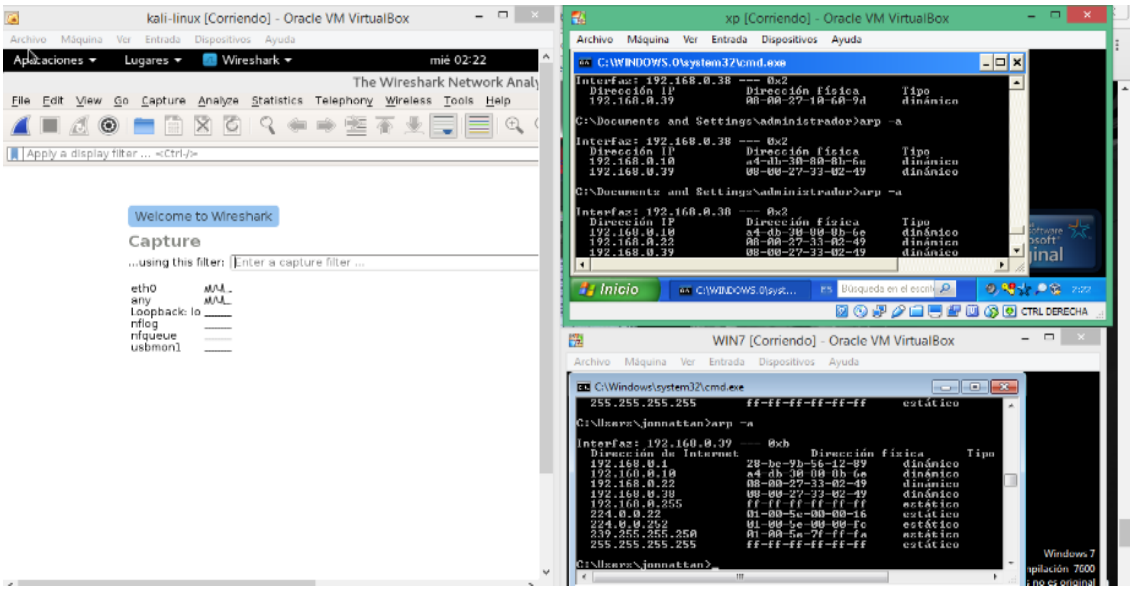
Figura 20. Confirmación de dirección Mac



Fuente: El autor

Para finalizar desde la herramienta *wireshark*, que permite visualizar los paquetes que están siendo enviados a las maquinas infectadas. Para acceder digitamos en nuestra terminal *wireshark y enter*.

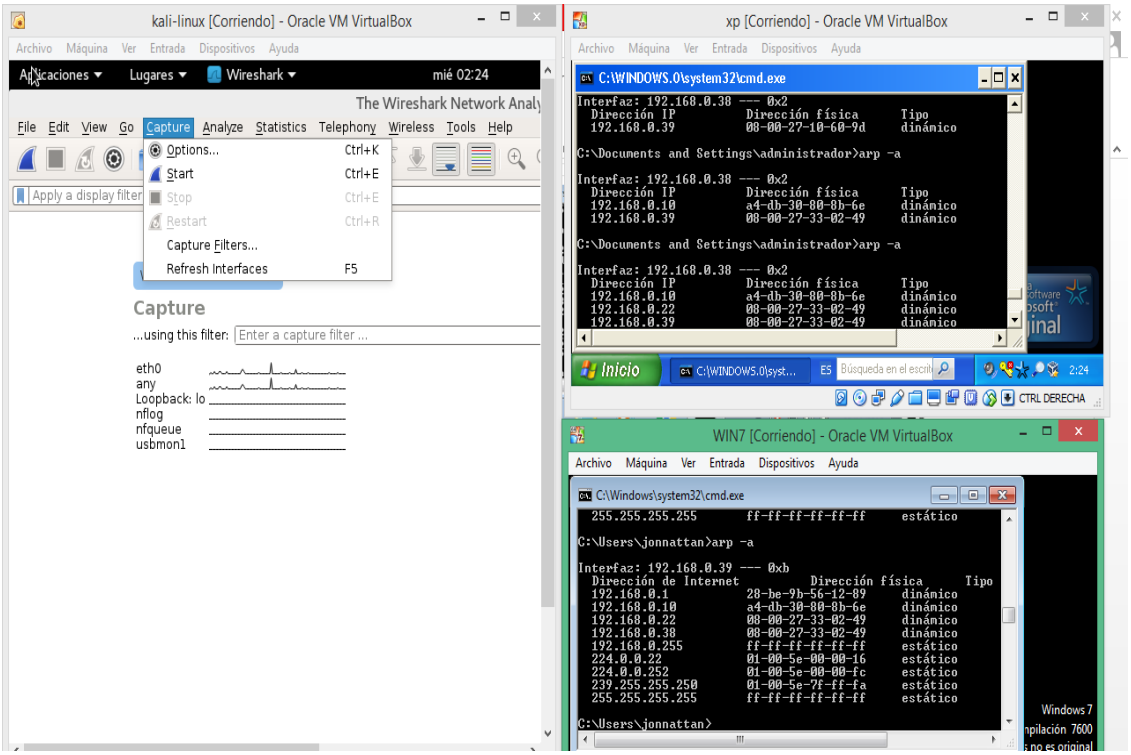
Figura 21. Validación ataque desde *Wireshark*



Fuente: El autor

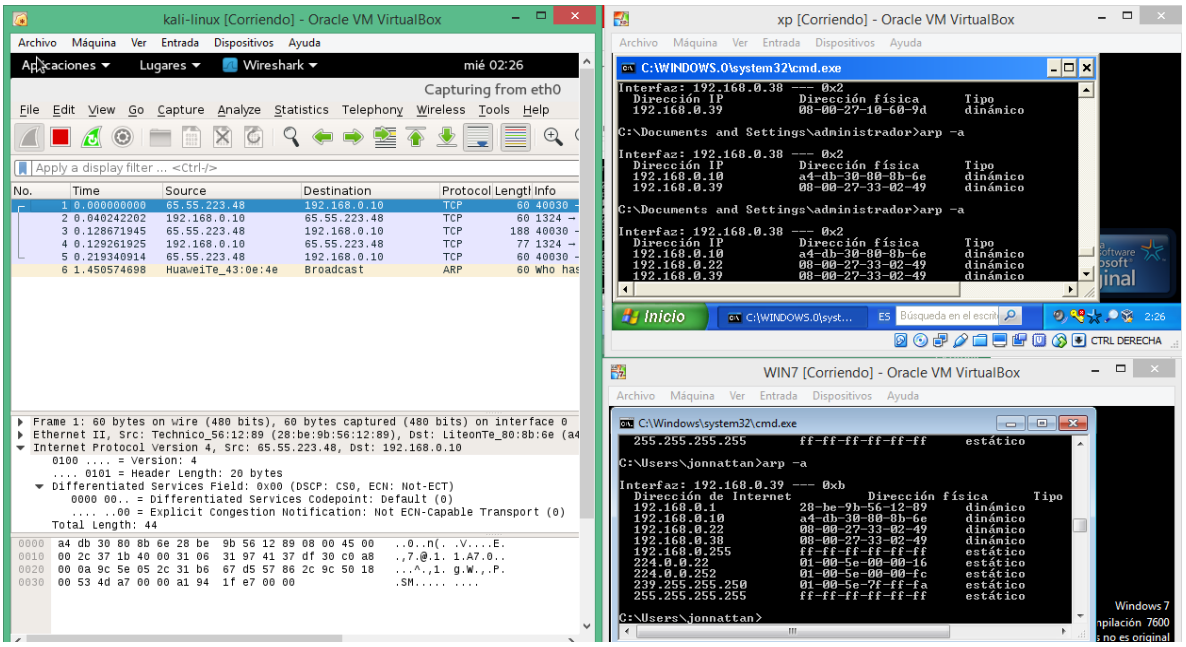
En esta herramienta se selecciona en el menú *capture*, luego *start* y seguidamente *eth0* que se encuentra en pantalla, donde se pueden visualizar los paquetes que circulan en la red.

Figura 22. Circulación de paquetes en la red



Fuente: El autor

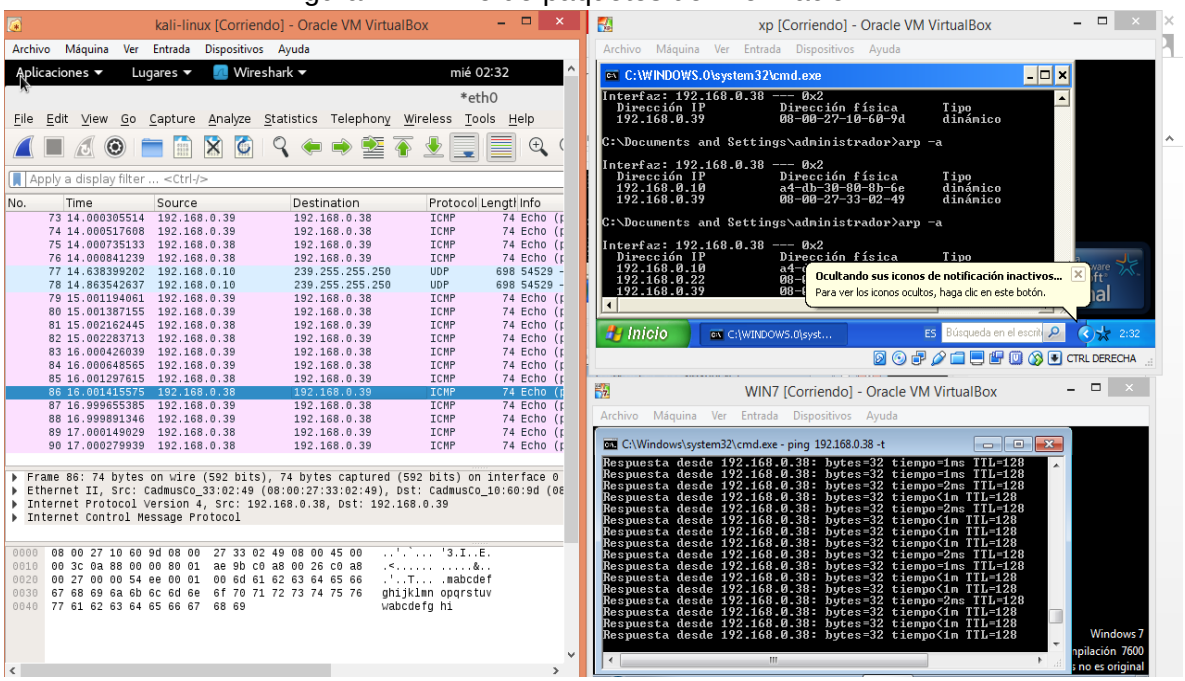
Figura 23. Ataque por *Spoofing*



Fuente: El autor

Finalmente, se realiza un *ping* entre las maquinas 192.168.0. *Windows* 7 y 192.168.0.39 XP y se logran visualizar los paquetes que se envían entre sí, por tanto, estos se pueden interceptar y almacenar para el propósito que se tenga.

Figura 24. Envió de paquetes de información

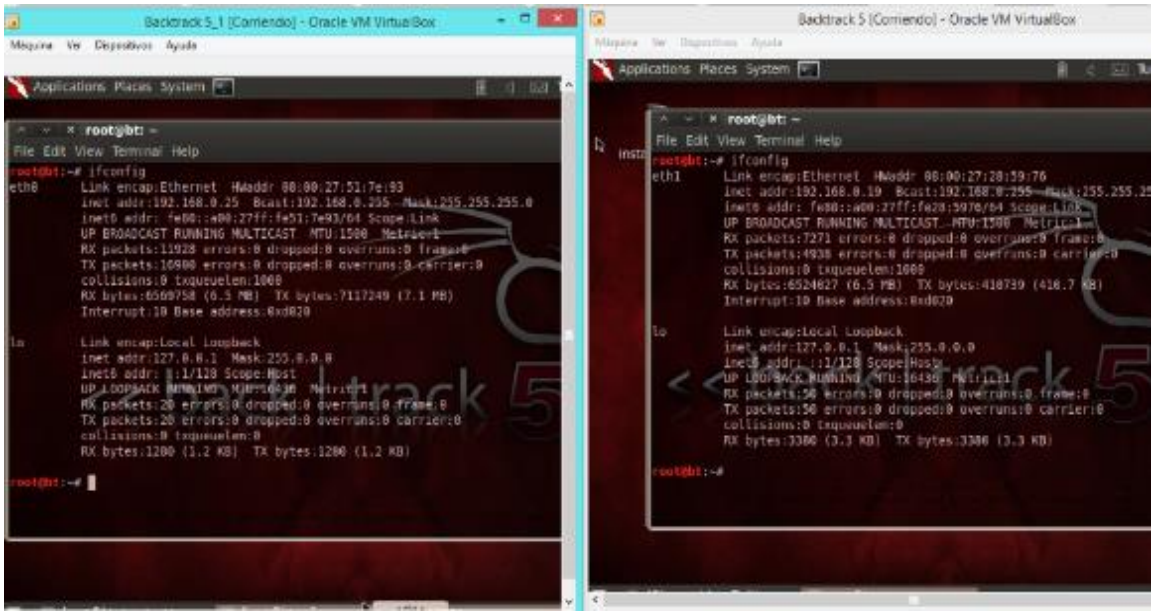


Fuente: El autor

Otra prueba es el punto de acceso falso:

Inicialmente se tienen dos máquinas virtuales, uno será el *host* atacante y el otro la víctima, se realiza la configuración de red y se verifican las direcciones IP de cada una:

Figura 25. Direcciones IP de la máquina atacante y de la víctima.



Fuente: El autor

Ejecutar herramienta que se utiliza como *exploit* y poder realizar el ataque:

Figura 26. Evidencia del uso del "*Credential Harvester Attack Method*"

Fuente: El autor

Esta aplicación de prueba, me despliega las diferentes pruebas que se pueden ejecutar aprovechando el agujero de seguridad, en este caso se selecciona la opción 1:

Figura 27. *Social –Engineering Attacks*

Fuente: El autor

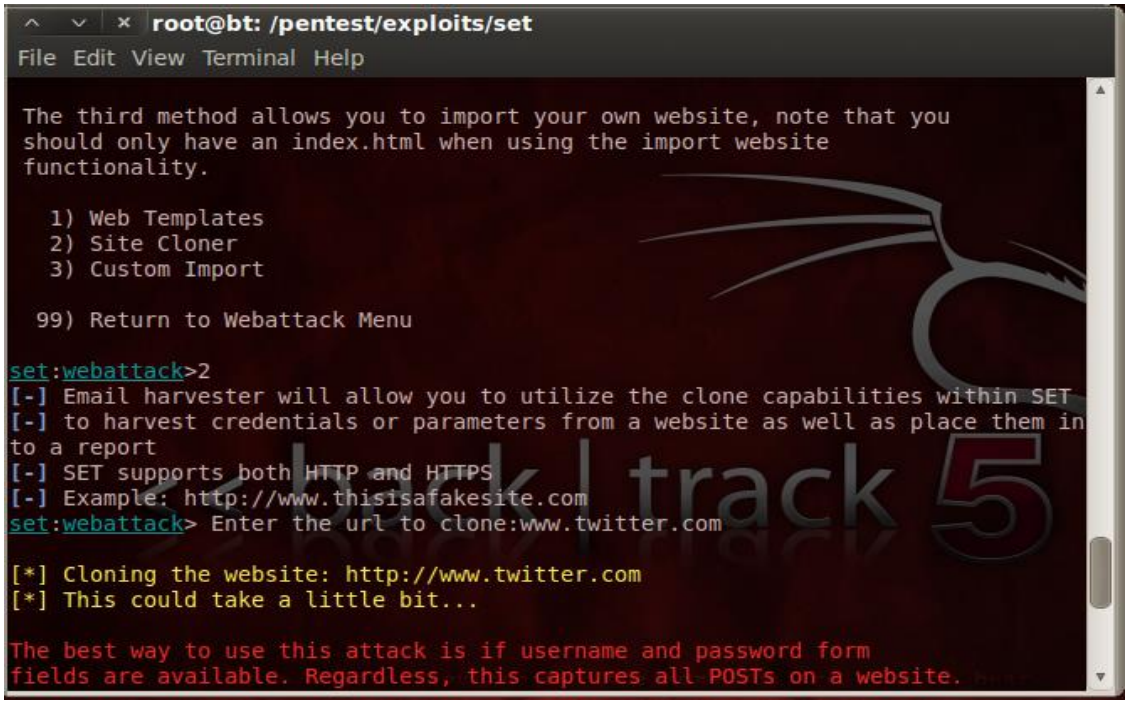
La opción 2, permite realizar un ataque a un punto falso en un *website*:

Figura 28. *Website Attack Vectors*

Fuente: El autor

Se realiza la clonación del punto de acceso y del sitio *web* para realizar el ataque:

Figura 29. Opción *Site Cloner* y sitio web a clonar



Fuente: El autor

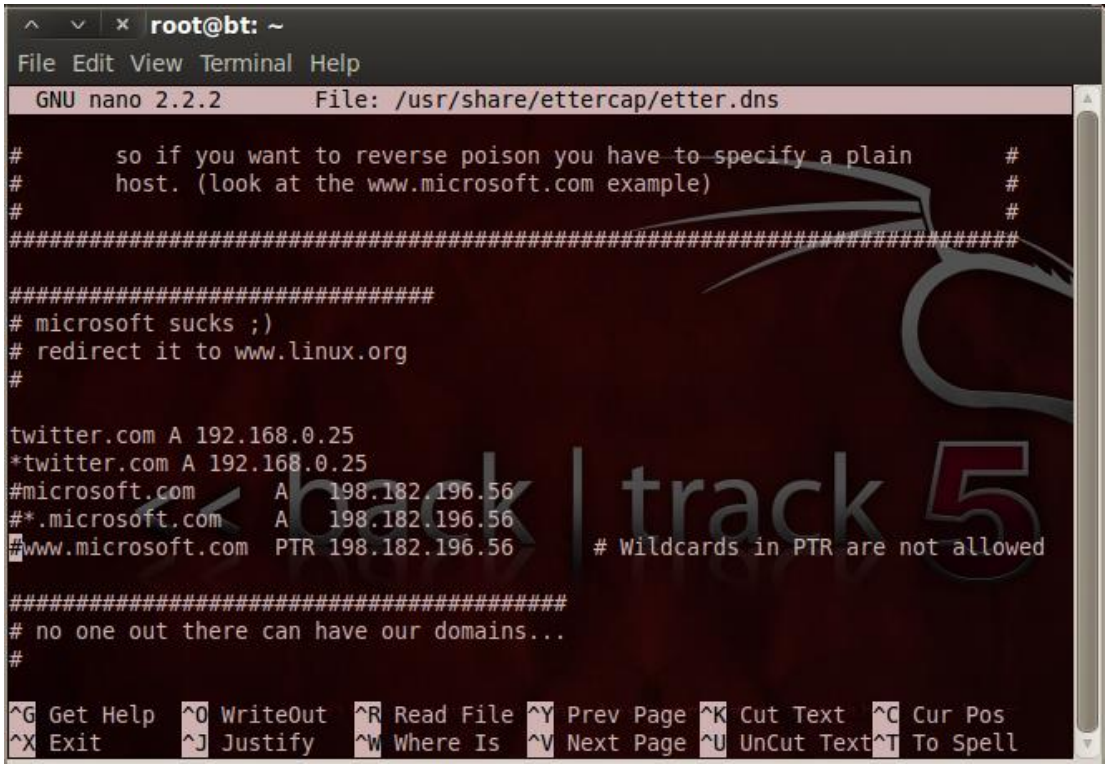
Igualmente se confirma el archivo donde se almacenara la información que el atacante desea obtener:

Figura 30. Archivo de almacenamiento

Fuente: El autor

Inicia la clonación de sitio *web*, donde el equipo está a la espera de la captura de las credenciales de usuario de la red:

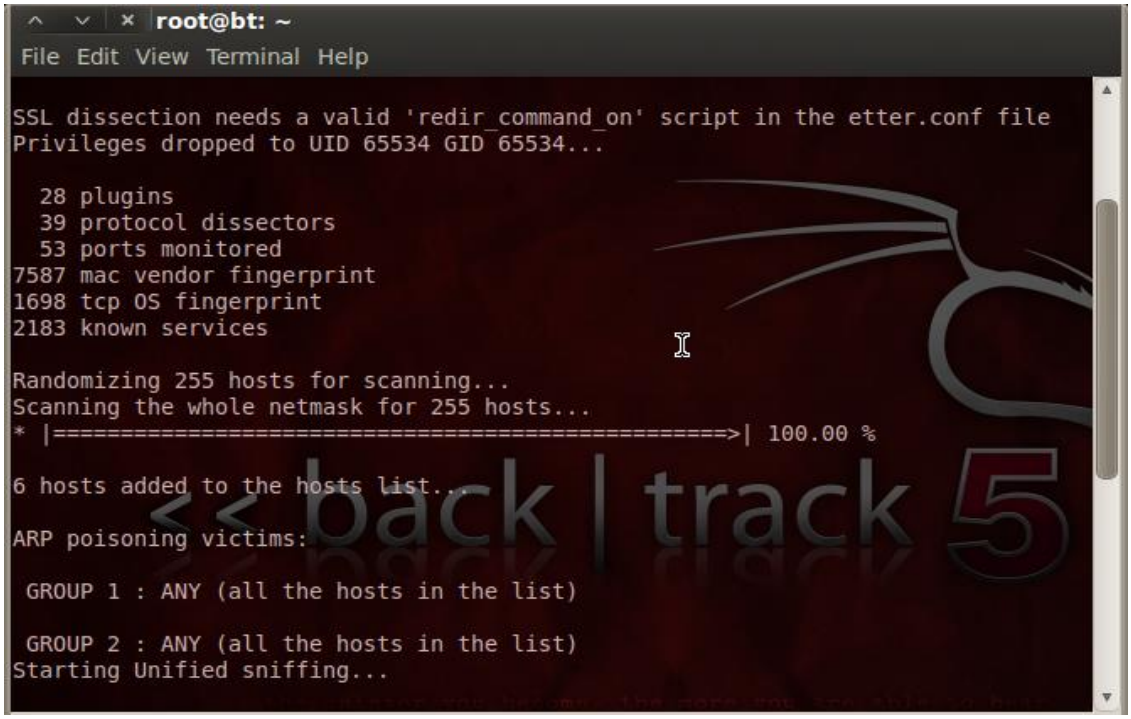
Figura 31. Clonación sitio *web*.



Fuente: El autor

Modificación del archivo *etter.dns*, por medio del comando *ettercap -T -q -i eth0 -P dns_spoof -M arp // //:*

Figura 32. Modificación del archivo *etter.dns*



Fuente: El autor

Inicia el proceso de *ettercap*:

Figura 33. Proceso de *ettercap*.

Fuente: El autor

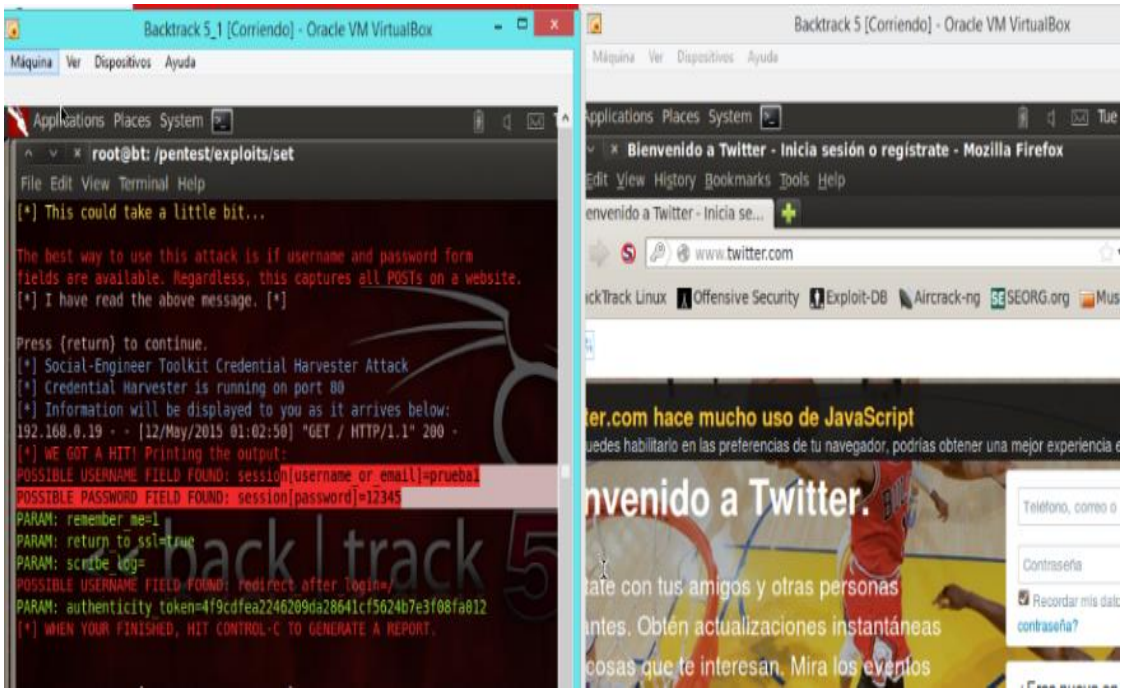
Se crea el reporte de captura del sitio *web* clonado:

Figura 34. Página *web* clonada

Fuente: El autor

Se encuentra en los archivos generados en el proceso el usuario y clave del usuario que accede al sitio web clonado:

Figura 35. Usuario y clave del usuario en la página web clonada



Fuente: El autor

4.3 Especificar medidas de seguridad de acuerdo a su función y grado de protección para establecer redes seguras.

Teniendo en cuenta las necesidades del usuario, se definen las siguientes medidas como estrategias de seguridad:

4.3.1 IDS Sistema de Detección de Intrusiones: trabaja cuidadosamente vigilando el tráfico en la red, de esta forma detectar movimientos anormales o sospechosos que puedan ser causa de riesgos de intrusión. Existen dos tipos de IDS:

- N-IDS: garantiza la seguridad dentro de la red. Confirmando los paquetes de información en línea para descubrir acciones maliciosas. Sus mecanismos consiste en poner adaptadores de red de modo invisible.
- H-IDS: garantiza la seguridad en el *host*. Se encuentra en un *host* en particular, es compatible con los diferentes sistemas operativos y actúa como un servicio estándar, analiza la información almacenada en los registros y captura paquetes de red que entran y salen del *host* y verifica las señales de intrusión. Como indica LARRIEU. [60]

Características de un IDS

Sus principales características son:

- Funciona continuamente sin la administración humana, es confiable ya que se ejecuta dentro del equipo como *background*, permitiendo extraer y examinar el registro de lo detectado.

[60] LARRIEU Cyrille “Sistema de detección de intrusiones (IDS)” [En línea]. 2003 [Citado: 16 mayo de 2016] Disponible en Internet: http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

- Tolerante a fallos, sobreponerse al momento de presentar caídas del sistema.
- El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- Flexible, no sobrecarga el sistema.
- Adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- Difícil de "engañar".[61]

Funciones de un IDS

Los sistemas de detección de intrusos tienen como función:

- Detectar ataques en línea o diferentes momentos de tiempo.
- Automatización de la búsqueda de nuevos patrones de ataque.
- Monitorización y análisis de las actividades de los usuarios.
- Auditoria de configuraciones y vulnerabilidades de determinados sistemas.
- Análisis de comportamiento anormal en la red
- Automatizar tareas: actualización de reglas, obtención y análisis de *logs*, configuración de cortafuegos y otros. [62]

[61] LARRIEU Cyrille Op. cit. p.86.
[62] Ibid,. p.86.

4.3.2 SNORT: Se recomienda utilizar SNORT, recordando que es un IDS gratuito, capaz de actuar como un *Sniffer*, de detección de intrusos en redes de tráfico moderado, es fácil de configurar y adaptable, sus requerimientos son mínimos y se puede descargar directamente desde la página oficial *http://www.snort.org/*. Funciona sobre plataformas *Windows* y *Unix/Linux*, *Solaris o BSD*.

Teniendo en cuenta que *Symantec* ofrece un *software* o dispositivo que detecta y notifica a un usuario o empresa el acceso no autorizado a una red o equipo informático, realizando el análisis de paquetes en la red orientados al nodo de red, ayuda a identificar ataques al supervisar el tráfico. Así indican Maestros de la web. [63]

Por otro lado, se establecen más a fondo cada una de estas medidas:

- ✓ **Asegurar puntos de acceso**

  Establecer un *password* de ingreso a la administración del Punto de Acceso, el cual se recomienda cambiar de forma periódica para mayor seguridad. También tener en cuenta que se debe evitar crear contraseñas como fechas de nacimientos, nombre de tu pareja, etc. Intentar intercalar letras con números y caracteres especiales.

- ✓ **Aumentar la seguridad de los datos transmitidos**

  Utilizar encriptación WEP/WPA, evitar utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado.

[63] MAESTROS DEL WEB, Sistemas de Detección de intrusos y Snort. [En línea]. 2003 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.maestrosdelweb.com/snort/

Después de configurar el AP configurar los accesorios o dispositivos Wi-Fi.

Algunos Puntos de Acceso más recientes soportan también encriptación WPA (*Wi-Fi Protected Access*), encriptación dinámica y más segura que WEP. Si se activa WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de la red como el sistema operativo deben soportarlo.

Se recomienda utilizar encriptación WPA. Cambiar las claves regularmente. Por ejemplo, semanalmente o cada 2 o 3 semanas.[64]

- ✓ **Ocultar la red Wi-Fi**

Cambia el SSID por defecto. Si no llamamos la atención del observador hay menos posibilidades de que éste intente entrar en nuestra red.

Desactivar el *broadcasting* SSID. El *broadcasting* SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo se tendrá que introducir manualmente el SSID en la configuración de cada nuevo equipo que quiera conectarse.

- ✓ **Evitar que se conecten**

Activar en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente funcionen. Al activar el filtrado MAC sólo los

[64] MAESTROS DEL WEB, Op. cit. p.88.

dispositivos con las direcciones MAC especificadas se conecten a la red Wi-Fi.

Se pueden conocer las direcciones MAC de los equipos que se conectan a la red, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

Además, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

Establecer el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

Al desactivar DHCP en el *router* ADSL y en el AP. En la configuración de los dispositivos/accesorios Wi-Fi se podrá introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario. [65]

4.4 Elaborar un manual o guía de la implementación del modelo de gestión de la seguridad en las redes inalámbricas aplicado a las pequeñas empresas del sector privado de la ciudad de Bogotá.

Este documento brinda una guía de seguridad de una red que contenga componentes inalámbricos, basados en el estándar 802.11. También se ofrecen recomendaciones para una comunicación segura entre dispositivos que

[65] SEGU.INFO Seguridad de la Información “Detección de Intrusos en Tiempo Real” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: http://www.segu-info.com.ar/proteccion/deteccion.htm

utilizan este tipo de tecnología, proporcionando buenas prácticas de implementación de redes inalámbricas.

La guía se orienta a la tecnología inalámbrica WLAN, teniendo en cuenta que las redes inalámbricas ofrecen a organizaciones y usuarios muchos beneficios como lo son portabilidad y flexibilidad. Las tecnologías inalámbricas cubren un amplio rango de capacidades orientadas a diferentes usos y necesidades. Dispositivos *Wireless Local Área Network* (WLAN) permiten que los usuarios se puedan mover de un lugar a otro en sus oficinas sin necesidad de cables y sin pérdida de conectividad de red.

Igualmente se presentan riesgos que son inherentes a cualquier tecnología, estos riesgos son similares a los de las redes cableadas, provocando la perdida de confidencialidad e integridad y amenazas asociadas a las comunicaciones inalámbricas: Usuarios no autorizados pueden tener acceso a sistemas e información corporativa, consumir ancho de banda, degradar el desempeño de la red, enviar ataques que evitan que usuarios autorizados ingresen a la red o simplemente usar la plataforma de IT como base de ataque a otras redes.

Entre las amenazas y vulnerabilidades específicas a redes inalámbricas y dispositivos de mano (*Handheld Devices*) se pueden incluir las siguientes:

- ✓ Riesgo de robo de tráfico y riesgo de un ataque de tipo intermediario. (Confidencialidad)
- ✓ Riesgo de alteración de tráfico en la red inalámbrica. (Integración)
- ✓ Riesgo de interferencia, congestionamiento (Denegación de Servicio - DoS) (Disponibilidad)

- ✓ Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio. (Disponibilidad)
- ✓ Riesgo de no disponibilidad de ancho de banda por *software* malicioso. (Disponibilidad)
- ✓ Todas las vulnerabilidades que existen en redes convencionales aplican en tecnologías *Wireless*.
- ✓ Acceso no autorizado a la red inalámbrica, traspasando la protección del *firewall*. (Autenticación)
- ✓ Información confidencial y/o sensible no es encriptado y si es transmitida entre dos dispositivos *Wireless* puede ser interceptada y modificada por personas ajenas a la organización.
- ✓ Intrusos o *malware* tipo *scripts*, pueden usar la identidad de usuarios legítimos. (Suplantación de identidad)
- ✓ Intercepción y monitoreo de tráfico.
- ✓ Ataques internos pueden ser posibles vía transmisiones *ad hoc*.
- ✓ Ataques tipo cliente – cliente o cliente –red.
- ✓ Errores de configuración.

Se recomienda tener en cuenta las siguientes normas de seguridad en el uso de redes inalámbricas:

- ✓ Se debe tener un control total y un conocimiento general de la topología de la red inalámbrica.
- ✓ Marcar y tener un inventario actualizado de dispositivos de la red *Wireless*.

- ✓ Crear *Backups* (copias de seguridad) con una periodicidad establecida.
- ✓ Realizar periódicamente pruebas de seguridad en la red *Wireless* con herramientas de *Ethical Hacking*.
- ✓ Aplicar parches y actualizaciones de seguridad, según recomendación del fabricante.
- ✓ Actualizar la guía según el estándar de la industria para redes *Wireless* que mejoren el nivel de seguridad, así como también reportes de vulnerabilidades y amenazas.
- ✓ Es necesario implementar en estos dispositivos los protocolos de encriptamiento.

Igualmente se recomienda aplicar políticas de seguridad para el uso de redes inalámbricas:

- El acceso a las redes inalámbricas debe estar autorizado por el área de seguridad de la información
- Se debe tener un programa de capacitación para los usuarios finales, con el objetivo de establecer buenas prácticas, concientizándolos del uso de las redes inalámbricas con respecto a dispositivos celulares, impresoras, portátiles, entre otros.
- Ejecutar pruebas de vulnerabilidades para identificar las grietas de seguridad en la red
- Instalar *firmware open source* en los dispositivos para mayor seguridad
- Implementar controles de acceso físico restringido a las áreas de conectividad inalámbrica

- Determinar lugares donde ubicar *Acces Point* para minimizar ataques, esto determinando coberturas y rangos de trabajo monitoreado. Para evitar el acceso de personas ajenas a una organización, provee mayor control
- Limitar el cubrimiento de la señal
- Apagar los equipos inalámbricos en horarios que no se utilicen para evitar intentos de intrusión
- Instalación de equipos activos de red, definiendo dominios de colisión para evitar y restringir el monitoreo de trafico compartido en el medio
- Los datos e información deben ser encriptados para el aseguramiento de los mismos en el proceso de comunicación
- Se debe mantener monitoreada la red en tiempo real, para identificar incidentes de seguridad
- Se tiene en cuenta el uso de direcciones IP estáticas, que permiten rastrear actividades maliciosas y evitar el acceso no autorizado.
- Implantación de IDS o IPS basados en red de segmentos vulnerables, agentes que notifiquen sobre intrusos en la red, detectar y responder actividades maliciosas
- Establecer un plan de seguimiento de amenazas, vulnerabilidades y correctivos

Adicional se deben tener en cuenta las siguientes recomendaciones de seguridad y configuración de *Access Point* y concentrador Cisco

- Todos los AP suelen tener una contraseña para acceder a la administración y configuración del dispositivo por defecto, se debe cambiar la clave de acceso, ya que una persona ajena podría conocer los datos por defecto y así tener acceso a la configuración de la red inalámbrica.
- Establecer un tiempo de sesión razonable para mitigar el riesgo de sesiones autenticadas.
- Realizar cambios SIDD, por defecto son utilizados por los fabricantes de equipos y son muy conocidos por *hackers*
- Deshabilitar *broadcast*, ya que intrusos pueden detectar fácilmente y explotar APS que ejecutan *Broadcasting* de su SSID; Se debe deshabilitar esta característica de la red en el *router* o AP, de forma que no se difunda el nombre de la red, si alguien quiere conectarse a la red debe conocer el nombre de la red.
- Validar el SSID, verificando que no refleje información sobre la entidad. El SSID puede permitir que un atacante identifique qué tipo de dispositivo está en uso y a quién pertenece
- Validación de canales de comunicación de los dispositivos cercanos para evitar interferencias
- Crear el SSID *wpawireless*, con filtrado de MAC y seguridad de clave WPA local, para brindar acceso a la red corporativa y navegación hacia la internet.

- Crear el SSID *webguest*, con filtrado MAC y autenticación vía *web* local, para brindar acceso red vía inalámbrica, ofreciendo el servicio de navegación hacia internet.
- Se asignará una dirección de red, para la red inalámbrica, esta red estará ubicada en una interface diferente de *firewall* y por cada máquina conectada a la red Wi-fi, se establecerán políticas de acceso mediante el *firewall*, en el controlador se establece la VLAN para segmentar la red.
- El concentrador se configura con una dirección de red, el acceso a la red, solo se establece para el administrador del concentrador, ya con esta acción se cambia la IP interna de los *router* que traen por defecto y se mitiga el acceso de usuarios no autorizados.
- Habilitar protocolos de seguridad de autenticación criptográfica WPA2 con encriptación AES en los equipos para optimizar la seguridad por defecto.
- Emplear tamaño de llaves de encripción con 128 o 256 bits (nivel de protección más alto) para prevenir ataques de fuerza bruta. Este tamaño de llaves es soportado por los protocolos WAP y WAP2.
- Cambiar periódicamente las llaves compartidas (*sharedkeys*) para evitar accesos no autorizados y captura de información sensible.
- Los usuarios se crean de manera local en el concentrador y se les asigna una clave de acceso de mínimo 8 caracteres alfanuméricos. Para el SSID *wpawireless*, se crean claves sin límite de tiempo, estas claves se requieren cambiar cada 6 meses.

- Aplicar políticas de filtrado de redes cableadas e inalámbricas, asegurándose de controlar el acceso de recursos y tecnologías de filtrado de paquetes (*firewall*). Por lo general, los AP deben ir enfrente de los *firewalls* y estar en la DMZ. Todas las comunicaciones entre las redes inalámbricas y las redes cableadas han de pasar por el *firewall*. Si el *router* lo permite se pueden definir qué puertos y servicios pueden estar disponibles para el acceso a la red.
- Crear una lista de direcciones MAC que se encuentran autorizadas para tener acceso a la red.
- Asegurarse de contar con mecanismos de autenticación para garantizar que sólo los usuarios autorizados puedan acceder a la interfaz de administración.

Por ultimo recomendaciones de seguridad para los clientes inalámbricos:

- El antivirus evita que código malicioso o virus ingresen a la LAN corporativa. Se debe instalar una solución en cada uno de los dispositivos móviles, debe estar en ejecución y actualizarlo regularmente.
- Los *firewalls* personales son una barrera de defensa básica en dispositivos móviles, el *firewall* debe estar instalado y activo en la conexión inalámbrica.
- La implementación de autenticación de dos factores: *Smartcards*, biometría y PKI, minimizan el riesgo a cambio de utilizar un simple

nombre de usuario y contraseña para acceder a los recursos de una compañía.

5. CONCLUSIONES

- Durante el desarrollo del proyecto se demuestra una vez más lo vulnerables que se encuentran las redes en la transmisión de información, por medio de herramientas que permiten realizar todo tipo de ataque al internet, red, *email*, etc.
- Lo ideal es conocer la amenaza y poner en práctica los métodos de prevención, que pueden proteger la red de estos ataques. Teniendo en cuenta que la seguridad es un compromiso de todos de eficiencia, disponibilidad, integridad, y confidencialidad, atención y cuidado por todos los encargados de la seguridad informática en las empresas.
- Teniendo en cuenta esta guía de seguridad para redes inalámbricas, se pretende concientizar de la necesidad de poner en práctica estrategias de control y seguridad para blindar y utilizar redes seguras en la comunicación inalámbrica, todo teniendo en cuenta las necesidades y especificaciones de la red.
- Este informe es de gran utilidad tanto a nivel estratégico como operativo, teniendo en cuenta cada uno de las recomendaciones dadas, se incrementa la percepción de seguridad y cerrar la brecha a los atacantes, la mejor línea de defensa es hacer pruebas de penetración en la misma red de trabajo, con el fin de detectar y mitigar los riesgos y amenazas asociados a las redes inalámbricas. Ya que así como crecen los protocolos y medidas de seguridad, así mismo crecen y avanzan las herramientas y los métodos de ataque, por esto es muy importante

mantenerse actualizado y al día en cuanto a las diferentes formas de ataque y las medidas de seguridad para contrarrestarlos.

6. RECOMENDACIONES

Partiendo de cada una de las estrategias se establece una metodología para la seguridad de redes inalámbricas WLAN, cubriendo los siguientes aspectos:

- Normas, regulaciones y estándares para la seguridad en redes inalámbricas WLAN: Teniendo en cuenta el estándar IEEE 802.11 que define las características de una red inalámbrica.
- Tipos de conexión en redes inalámbricas: teniendo en cuenta los tipos de conexión de acuerdo a su tamaño, aplicado a las redes WLAN (*Wireless Local Area Network*), que permiten la conexión entre dispositivos en un área local geográfica, permitiendo compartir archivos, servicios, impresoras, entre otros recursos; utiliza señales de radio tiene un alcance de 30 a 300 metros, con señales capaces de atravesar paredes, ofrecen movilidad, flexibilidad, velocidad, escalabilidad, costos reducidos de instalación. Se tendrá en cuenta este tipo de red inalámbrica.
- Tipos de Tecnología de redes inalámbricas: La tecnología a utilizar será FHSS (Espectro ensanchado por salto de frecuencia), ya que soporta todo tipo de infraestructura teniendo en cuenta las estaciones de trabajo y se aplica a formas industriales: este consiste en transmitir una parte de los datos en una determinada frecuencia durante un intervalo de tiempo y estos datos se transmiten saltando de una frecuencia a otra en un orden determinado. Entre sus principales ventajas son: resistentes a las interferencias, son difícilmente interceptadas y pueden compartir bandas de frecuencia con diferentes transmisores.

- Protocolos de seguridad para las redes inalámbricas: se determina utilizar WPA: *Wi-Fi Protected Access*, este protocolo emplea un cifrado dinámico, es decir que la clave va cambiando constantemente haciendo que el acceso a la red inalámbrica sea más difícil. Es considerado como uno de los protocolos de más alto nivel de seguridad y el más recomendado. Las claves se insertan como dígitos alfanuméricos, sin restricciones de longitud, donde se recomienda utilizar caracteres especiales, números, mayúsculas, minúsculas y palabras difíciles de asociar.

  WPA2: es la segunda generación de WPA, su diferencia radica en que esta utiliza un estándar de cifrado avanzado AES, que aporta altos niveles de seguridad para cumplir los estándares máximos.
- Definir los tipos de componentes de *hardware* y *software* para redes inalámbricas:

  Componentes de *hardware*:

  - *Access Point*
  - Antena
  - *Bridges*
  - Adaptadores de cliente
  - Cables y accesorios
- Definir escenarios de pruebas para el soporte, actualización y mantenimiento de la seguridad en redes inalámbricas

Teniendo en cuenta el diseño formulado se puede establecer el método o configuración de seguridad:

a) Modificar las credenciales de acceso: cambiar la clave de acceso a la configuración del *router*, ya que una persona ajena podría conocer los datos por defecto y así tener acceso a la configuración de la red. Es recomendable implementar para mayor seguridad una contraseña alfanumérica.

b) Asignar una contraseña de acceso a la red

c) Configurar el tipo de cifrado de la red: Es recomendable utilizar y configurar la red para que utilice cifrado WPA2 con encriptación AES, recomendado para cifrar los *Wireless* de los *routers* usando una clave pública estática o dinámica. De esta forma, los datos que circulen por la red no serán legibles por parte de terceros que estén monitoreando los mismos.

Con estas tres sencillas configuraciones, el usuario ya habrá modificado radicalmente la seguridad de la red inalámbrica, haciendo mucho menos probable que una persona no autorizada acceda a la red y pueda utilizar la misma con fines maliciosos.

Para una configuración de seguridad más avanzada:

a) Configurar el *firewall*: Si el *router* lo permite, es posible definir qué servicios y puertos pueden estar disponibles para el acceso externo a la red.

b) Acceso al *router* por HTTPS: También es posible habilitar la configuración del *router* a través del protocolo HTTP seguro, para evitar que un atacante capture la contraseña de acceso a la configuración.

c) Ocultar el SSID de la red: consiste en ocultar el SSID (*Service Set Identifier*) que es el nombre que identifica a la red inalámbrica. El usuario puede cambiar y establecer un SSID diferente.

REFERENCIAS BIBLIOGRÁFICAS

BAUTISTA, Hipólito “Vulnerabilidades de una red Wi-fi” [En línea]. 2013 [Citado: 16 mayo de 2016] Disponible en Internet: (http://rootear.com/seguridad/vulnerabilidades-una-red-wi-fi)

BLAIR MANDEVILLE Stephen “Network Wireless Security” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: (https://www.exploit-db.com/docs/24895.pdf)

CALLES, Juan Antonio “Wi-Fis: Tipos de ataque y recomendaciones de seguridad” [En línea]. 2013 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html).

CCM “Introducción a Wi-Fi (802.11 o WiFi)” [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: (http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi)

CIOPERU “5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: (http://cioperu.pe/articulo/18229/5-ataques-comunes-a-las-redes-wifi-y-como-defenderse-de-ellos/).

CISCO “Tecnología inalámbrica” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html).

DE LUZ, Sergio “Conoce la última vulnerabilidad en redes Wi-Fi 802.11n sin contraseña (abiertas)” [En línea]. 2015 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.redeszone.net/2015/07/05/conoce-la-ultima-vulnerabilidad-en-redes-wi-fi-802-11n-sin-contrasena-abiertas/)

DE LUZ, Sergio “Ataques a las redes: Listado de diferentes ataques a las redes de ordenadores” [En línea]. 2010 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/).

ESCUDERO Alberto “Unidad 02: Estándares en Tecnologías Inalámbricas” [En línea]. 2007 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf)

ESET “Guía de seguridad en redes inalámbricas” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_wifi.pdf).

GACHARNÁ Federico “TOP 10 DE PRUEBAS DE PENETRACIÓN Y HACKING A REDES INALÁMBRICAS” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.conassol.org/wp-content/uploads/2015/02/TOP-10-DE-PRUEBAS-DE-PENETRACI%C3%93N-Y-HACKING-A-REDES-INAL%C3%81MBRICAS.pdf).

GALÁN Manuel “Guía Metodológica” [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: (http://manuelgalan.blogspot.com.co/p/guia-metodologica-para-investigacion.html).

GARCÍA ARANO Carlos “IMPACTO DE LA SEGURIDAD EN REDES INALÁMBRICAS DE SENSORES IEEE 802.15.4” [En línea]. 2010 [Citado: 16 mayo de 2016] Disponible en Internet: (http://eprints.ucm.es/11312/1/Memoria_Fin_de_Master_-_Carlos_Garc%C3%ADa_Arano.pdf)

GIMÉNEZ AMADO, Roberto “Análisis de la seguridad en redes 802.11” [En línea]. 2008 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.securityartwork.es/wp-content/uploads/2008/10/seguridad-en-redes-80211.pdf)

GUTIERREZ, Juan David “Vulnerabilidades en 802.11” [En línea]. 2006 [Citado: 16 mayo de 2016] Disponible en Internet: (https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwirydX23tXLAhXJ9R4KHTnEDP8QFghOMAc&url=http%3A%2F%2Fpegasus.javeriana.edu.co%2F~edigital%2FDocs%2F802.11%2FVulnerabilidades%2FVulnerabilidades%2520v0.5.doc&usg=AFQjCNEK_Ve7jOEdey7b05D2_YrZSajyVw).

HERNANDEZ HERNANDEZ, Evaristo “Vulnerabilidad en redes” [En línea]. 2016 [Citado: 16 mayo de 2016]. Disponible en Internet: (http://es.lin01.wikia.com/wiki/Vulnerabilidad_en_redes).

IBERSYSTEMS “Redes WiMAX” [En línea]. 2016 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.redeswimax.info/).

INFORMÁTICA HOY “Vulnerabilidades de las redes” [En línea]. 2012 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php)

Jonnathan “Wireless Network” [En línea]. 2009 [Citado 16 mayo de 2016] Disponible en Internet: (http://wagneredesinalambricas.blogspot.com.co/2009/10/marco-teorico.html).

JULIO RUIZ, José “Seguridad en redes Wi-Fi inalámbricas” [En línea]. 2004 [Citado: 16 mayo de 2016] Disponible en Internet:

(http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml).

KARTHIK R “10 herramientas de seguridad Wi-Fi para su arsenal” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: (http://searchdatacenter.techtarget.com/es/foto-articulo/2240220535/10-herramientas-de-seguridad-Wi-Fi-para-su-arsenal/10/10-Xirrus-Wi-Fi-Inspector).

LARRIEU Cyrille “Sistema de detección de intrusiones (IDS)” [En línea]. 2003 [Citado: 16 mayo de 2016] Disponible en Internet: (http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids)

LÓPEZ Juan Miguel, DOMÍNGUEZ Roció, BENÍTEZ Rubén “Seguridad en redes Inalámbricas” [En línea]. 2010 [Citado: 16 mayo de 2016] Disponible en Internet: (http://informatica.gonzalonazareno.org/plataforma/file.php/7/G21.pdf)

MARTIN, Alejandro “Redes Inalámbricas” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: (http://inalambricas2009.blogspot.com.co/2009/10/marco-teorico.html).

MONTES DÍAZ, María José “Wi-Fis: Tipos de ataque y recomendaciones de seguridad” [En línea]. 2015 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html).

POLANCO, Juan José “WiMAX que es y para qué sirve?” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: (https://hackinglinux.wordpress.com/2009/04/09/wimax-que-es-y-para-que-sirve/).

REDIRIS “Sistemas de detección de intrusos” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: (https://www.rediris.es/cert/doc/unixsec/node26.html)

SEGU.INFO Seguridad de la Información “Detección de Intrusos en Tiempo Real” [En línea]. 2009 [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.segu-info.com.ar/proteccion/deteccion.htm)

SILVA, Felix “Penetration Testing”. [En Línea] 2016 [Citado: 16 mayo de 2016] Disponible en Internet: (https://docs.google.com/presentation/d/1e3-VDVAdiV4tb-lNQ-v7hv581rhZHHg8i8cJ5gETQCk/htmlpresent?hl=es)

SITES “Características cualitativa y cuantitativa” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: (https://sites.google.com/site/51300008metodologia/caracteristicas-cualitativa-cuantitativa)

SLIDESHARE “Proyecto de red wifi formulación 1” [En línea]. 2013 [Citado: 16 mayo de 2016] Disponible en Internet: (http://es.slideshare.net/Cruch/proyecto-de-red-wifi-formulacion-1)

SOTO, Jason “Qué es Metasploit?” [En línea]. 2014 [Citado: 16 mayo de 2016] Disponible en Internet: (https://www.jsitech.com/linux/que-es-metasploit/)

TARLOGIC “Auditoría wireless – Auditoría de seguridad WiFi OWISAM” [En línea]. 2015 [Citado: 16 mayo de 2016] Disponible en Internet: (https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/).

VERA PORTILLA Gonzalo, WICHE LATORRE Cristian, ZEPEDA POZO Pedro “Proyecto Seguridad en redes Wifi” [En línea]. [Citado: 16 mayo de 2016] Disponible en Internet: (http://www.profesores.elo.utfsm.cl/~agv/elo322/1s15/projects/reports/Seguridad_Redes_Wifi.pdf)

ANEXOS

Anexo 1: RESUMEN PROYECTO - ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA UNAD

Titulo	**Diseño de un modelo de gestión de seguridad en redes de comunicación inalámbricas aplicado a pequeñas empresas del sector privado de la ciudad Bogotá.**
Integrantes	**Jennifer Johana Cifuentes Rodríguez**
Palabras Claves	Red, inalámbrica, vulnerabilidades, amenazas, perdidas, riesgos, medidas, protocolos, métodos, estrategias, soluciones, información, metodologías, configuración, comunicación, suplantación, seguridad, Wi-Fi.
Descripción	Se realizó un proyecto de investigación con el objetivo recopilar las diferentes vulnerabilidades, amenazas y riesgos a los que se encuentra expuesta las redes inalámbricas y por ende la información que viaja por ellas y exponer unas pautas para proporcionar seguridad a las redes y mantener la confidencialidad, disponibilidad e integridad de la información.
Fuentes Bibliográficas	- DE LUZ Sergio, Conoce la última vulnerabilidad en redes Wi-Fi 802.11n sin contraseña (abiertas), disponibilidad desde Internet en: <http://www.redeszone.net/2015/07/05/conoce-la-ultima-vulnerabilidad-en-redes-wi-fi-802-11n-sin-contrasena-abierta/>[Citado 2015] - CALLES Juan Antonio, Wi-Fis: Tipos de ataque y recomendaciones de seguridad, disponibilidad desde Internet en: <http://www.flu-project.com/2013/10/wi-fis-tipos-de-ataque-y_1098.html> [Citado 2013] - DE LUZ Sergio, Ataques a las redes: Listado de diferentes ataques a las redes de ordenadores, disponibilidad desde Internet en: <http://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/>[Citado 2010 - GACHARNÁ Federico, TOP 10 DE PRUEBAS DE PENETRACIÓN Y HACKING A REDES

	INALÁMBRICAS, disponibilidad desde Internet en: <http://www.conassol.org/wp-content/uploads/2015/02/TOP-10-DE-PRUEBAS-DE-PENETRACI%C3%93N-Y-HACKING-A-REDES-INAL%C3%81MBRICAS.pdf> [Citado 2014] - CAMPOS. Diego Fernando, Metodología para la implementación de seguridad en redes inalámbricas version_2.0, disponibilidad desde Internet en: <http://miseriwlan.blogspot.com.co/2006/08/metodologia-para-la-implementacion-de.html>[Citado 2006]
Contenido	**Resumen** La seguridad en redes surge como consecuencia de la necesidad de utilizar medios y procedimientos para reducir riesgos debidos a las posibles amenazas y vulnerabilidades sobre la red inalámbrica. Para las empresas es vital importancia dar un buen manejo y seguridad a la información, razón por la cual, es importante hacer uso de una metodología adecuada. Actualmente la utilización e implementación de redes inalámbricas en las empresas de la ciudad de Bogotá es más frecuente, por tanto, es necesario a través de este proyecto de investigación identificar las amenazas y procedimientos que permitan controlar los riesgos a los que está expuesta la información como principal activo de las empresas mediante un modelo de gestión de seguridad adecuado. Toda organización que maneje sistemas de información está expuesta a amenazas y ataques que ponen en riesgo su permanencia, más aún cuando hablamos de conexiones inalámbricas en donde son accedidas por diferentes personas desde diferentes medios como celulares, portátiles, servidores, *tablets*, impresoras etc. Las empresas que utilizan redes inalámbricas se encuentran más expuestas a ataques que puedan generar la pérdida o robo de información, entre las que encontramos: *Access Point Spoofing*, *MAC*

	Spoofing, ARP Poisoning, Denial of service, WLAN escaners, Wardriving, entre otras como intercepción, intrusión e interferencia de datos; razón por la cual, el propósito de este proyecto es realizar una investigación a fondo sobre las vulnerabilidades de las diferentes redes de información inalámbricas, con esto encontrar que medidas de seguridad se pueden implantar para eliminar o reducir cualquier riesgo, que metodologías se pueden utilizar de acuerdo a cada uno de los protocolos utilizados en las redes de informática para garantizar la seguridad de cualquier empresa u organización, basados en normas o estándares internacionales que aporten a la misma. Lo anterior, enfocado al mejoramiento del negocio y a la seguridad de la información. **Formulación del problema** ¿Cómo el diseño de un modelo de gestión de seguridad en redes ayudará a disminuir los riesgos potenciales en las redes inalámbricas de las pequeñas empresas del sector privado de la ciudad Bogotá? **Objetivo general** Diseñar un modelo de gestión de seguridad en redes de comunicación inalámbricas para disminuir los riesgos potenciales en las pequeñas empresas del sector privado de la ciudad Bogotá. **Objetivos específicos** • Identificar las diferentes vulnerabilidades, amenazas y riesgos a que se ven expuestos los usuarios al conectarse a las redes inalámbricas de las pequeñas empresas del sector privado de Bogotá. • Evaluar la seguridad mediante pruebas sobre las redes inalámbricas. • Especificar medidas de seguridad de acuerdo a su función y grado de protección para establecer redes seguras. • Elaborar un manual o guía de la

	implementación del modelo de gestión de la seguridad en las redes inalámbricas aplicado a las pequeñas empresas del sector privado de la ciudad de Bogotá.
Metodología	Se establece que el tipo de metodología que se maneja en este proyecto es investigativa con enfoque cuantitativo, ya que se expone la manera como se va a realizar el estudio, los pasos para realizarlo y su método. Donde es posible hablar de una metodología aplicada a todos los campos, que recoge las pautas presentes en cualquier proceder con el aumento del conocimiento y solución de problemas.
Conclusiones	▪ Durante el desarrollo del proyecto se demuestra una vez más lo vulnerables que se encuentran las redes en la transmisión de información, por medio de herramientas que permiten realizar todo tipo de ataque al internet, red, *email*, etc. ▪ Lo ideal es conocer la amenaza y poner en práctica los métodos de prevención, que pueden proteger la red de estos ataques. Teniendo en cuenta que la seguridad es un compromiso de todos de eficiencia, disponibilidad, integridad, y confidencialidad, atención y cuidado por todos los encargados de la seguridad informática en las empresas. ▪ Teniendo en cuenta esta guía de seguridad para redes inalámbricas, se pretende concientizar de la necesidad de poner en práctica estrategias de control y seguridad para blindar y utilizar redes seguras en la comunicación inalámbrica, todo teniendo en cuenta las necesidades y especificaciones de la red. ▪ Este informe es de gran utilidad tanto a nivel estratégico como operativo, teniendo en cuenta cada uno de las recomendaciones dadas, se incrementa la percepción de seguridad y cerrar la brecha a los atacantes, la mejor línea de defensa es hacer pruebas de penetración en la misma red de trabajo, con el fin de detectar y mitigar los riesgos y

	amenazas asociados a las redes inalámbricas. Ya que así como crecen los protocolos y medidas de seguridad, así mismo crecen y avanzan las herramientas y los métodos de ataque, por esto es muy importante mantenerse actualizado y al día en cuanto a las diferentes formas de ataque y las medidas de seguridad para contrarrestarlos.
Recomendaciones	Partiendo de cada una de las estrategias se establece una metodología para la seguridad de redes inalámbricas WLAN, cubriendo los siguientes aspectos: - Normas, regulaciones y estándares para la seguridad en redes inalámbricas WLAN. - Tipos de conexión en redes inalámbricas - Tipos de Tecnología de redes inalámbricas - Protocolos de seguridad para las redes inalámbricas - Definir los tipos de componentes de *hardware* y *software* para redes inalámbricas. - Definir escenarios de pruebas para el soporte, actualización y mantenimiento de la seguridad en redes inalámbricas Teniendo en cuenta el diseño formulado se puede establecer el método o configuración de seguridad: a) Modificar las credenciales de acceso: cambiar la clave de acceso a la configuración del *router*. b) Asignar una contraseña de acceso a la red c) Configurar el tipo de cifrado de la red