URKUND

Urkund Analysis Result

Analysed Document: Chulli-Espinoza-TesinaFinal.docx (D43910003)
Submitted: 11/13/2018 2:04:00 AM
Submitted By: espinozaplaza94@gmail.com
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

INTRODUCCIÓN

Hoy en la actualidad las redes inalámbricas tienen un papel fundamental, debido que su funcionalidad es mantener la conectividad entre los dispositivos, e intercambio de la información en un mundo tan globalizado en el que vivimos. Este tipo de redes muestran ciertas vulnerabilidades a nivel de seguridad CITATION Dom12 \l 12298 (Rodríguez, 2012).

El auge del internet ha proporcionado la mejora de la comunicación entre los usuarios, que día a día son más los que buscan estar vinculados al mundo de la tecnología, es por eso que los usuarios buscan adquirir equipos informáticos de los diferentes proveedores de servicios de internet para lograr mantener la comunicación de manera virtual.

En la elaboración de la presente investigación se hizo uso de herramientas MITM (Man in the middle), estas siglas en español son interpretadas como ataque de intermediario u hombre en el medio, este término hace referencia a la extracción de información por medio de las conexiones de redes inalámbricas de los usuarios, es decir, el usuario proporcionará la clave porque es engañado por un mensaje de confirmación de datos que le llega, en esto se centra el uso de herramientas MITM.

La presente investigación a elaborar está compuesta por 5 Capítulos que consisten en: • Capítulo 1: Este capítulo abarca el desarrollo de la temática, la descripción del problema de la investigación, sus objetivos y justificación. • Capítulo 2: Es la elaboración del marco teórico de la investigación basados en repositorios científicos, libros para su elaboración. • Capítulo 3: Se describe la metodología a usar en este caso es una investigación de campo-cualitativa. • Capítulo 4: Es la elaboración de desarrollo del tema que es análisis de la vulnerabilidad de las redes inalámbricas con herramientas MITM. • Capítulo 5: En este se realiza las conclusiones a las que se llegaron mediante la propuesta de investigación planteada.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del Problema

Las redes inalámbricas son usadas por las mayorías de las personas hoy en la actualidad debido a su fácil manipulación y conectividad entre los diversos dispositivos. El crecimiento de las redes inalámbricas y la acogida de las conexiones Wifi; hacen más sencilla la manera de detectar una red inalámbrica.

Este tipo de redes se caracterizan debido a que no hacen uso de un cableado de forma estructurada estas se realizan por medio de conexiones que son a través de ondas electromagnéticas. Según (Carl, 2015) La diversidad de las comunicaciones inalámbricas reside en el desplazamiento en diversas áreas logrando por medio de esto mantener la conexión como si se realizara de una forma cableada, dicha conexión deber están en el perímetro que abarca la cobertura de la red.

El problema de la vulnerabilidad de las redes inalámbricas radica en que cualquier individuo tiene acceso a la visualización de la red, es decir dicha persona puede que no sea el propietario del dispositivo de red inalámbrica, pero tiene acceso a la red esta puede ser manipulada y por medio de esto se logra la extracción de la información que es trasmitida por medio de dicha red.

Las redes wifi se encuentran dentro de las redes inalámbricas y estas son consideradas como punto de acceso para que la información sea transmitida por medio de estos dispositivos en señales de ondas. Este tipo de red es más fácil de visualizar, debido a que genera ondas se encuentran en el entorno y cualquier dispositivo puede interceptarlas y esto genera que las personas busquen la manera de tener acceso a la red.

En la mayoría de las casas optan por implementar routers inalámbricos, puesto que al adquirir estos equipos informáticos que les proporcionan sus proveedores de servicios de internet, hacen que el usuario se conecte a este dispositivo y logre tener el acceso al mundo del internet permitiéndole una navegación inalámbrica. Sin tener en cuenta las medidas de seguridad y la falta de información de los usuarios sobre las configuraciones de seguridad permite que individuos que no son autorizados tenga el acceso a la red.

Con el auge de los equipos informáticos inalámbricos, también existe la demanda de herramientas que permiten vulnerar dichas redes para tener acceso a los datos de los usuarios, uno de esos datos son las claves de las redes wifi, que las obtienen con la utilización de herramientas MIITM, son aquellas que permiten conseguir la extracción de datos de los usuarios, cuando terceras personas obtienen las claves de red, la utilizan en todo momento.

1.2 Objetivo General

Determinar el grado de factibilidad de un ataque MITM de redes inalámbricas mediante Scripts.

1.3 Objetivos Específicos

• Describir las herramientas MITM para redes inalámbricas. • Identificar los puntos de accesos vulnerables a las Herramientas MITM. • Efectuar diversas pruebas de vulnerabilidad en diferentes tipos de routers con el uso de herramientas MITM.

1.4 JUSTIFICACIÓN

Desde el punto de vista teórico, la vulnerabilidad de las redes inalámbricas está presente en cualquier dispositivo tecnológico, ya que el funcionamiento de las redes inalámbricas se centra en mantener la conexión entre diferentes puntos de acceso por medio de ondas electromagnéticas, dichas ondas se encuentra en el aire, tal es el caso de las redes Wifi estas pueden ser detectadas desde cualquier dispositivo que presente conexión inalámbrica, lo cual a este tipo de redes las hace más manipulables para terceras personas.

Desde el punto de vista metodológico, la vulnerabilidad de redes inalámbricas mediante herramientas MITM, tiene un enfoque investigativo de Campo-Cualitativa, que consiste en la

utilización de una herramienta MITM, esta herramienta será utilizada por diferentes marcas de equipos informáticos y con todas las pruebas realizadas se podrá apreciar posibles beneficios para el atacante.

Desde el punto de vista social, actualmente las mayorías de los hogares y empresas hacen uso de dispositivos informáticos para mantener una conexión al mundo del internet y lograr una comunicación de forma virtual con los demás personas, son pocos los usuarios que tienen conocimientos sobres las normas de seguridad al momento de utilizar una red inalámbrica, y por culpa del desconocimiento muchas veces somos víctimas de ataques informáticos.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Antecedentes Históricos Según CITATION Dom12 \l 12298 (Rodríguez, 2012) El origen de las redes inalámbricas se centra a partir del año 1979 por unos estudios realizados por ingenieros de IBM. Además con los avances tecnológicos que se han suscitados los últimos años se buscar lograr una comunicación de manera efectiva entre los usuarios y el mundo digital.

En el año 1989 se logró establecer las primeras redes de comunicación inalámbrica, pero sus inicios fueron muy disperso debido q que eran fabricadas por diversos propietarios de fabricación y carecían de compatibilidad, pero actualmente las redes inalámbricas logran establecer la comunicación por medio de las ondas electromagnéticas que generan sin hacer uso del cableado estructurado.

Una red inalámbrica proporcional el mismo servicio que una red tradicional pero la falta del cableado hace que este tipo de res sea más flexible, la ubicación es rápida.

Según CITATION Wal14 \l 12298 (Isaacson, 2014) Alohanet fue el nombre que se le asignó a la red de área local en el años 1971 en la Universidad de Hawái, esta logó la comunicación entre 6 pc en los diversos áreas localizadas en las isla; como se muestra en la figura 1.

Figura 1.Alohanet Tomado de (Sebatian, 2011)

2.2 Redes Inalámbricas y sus normas de Seguridad según autores Según (Monsalve Pulido, Aponte Novoa, & Chaparro Becerra, 2015) en su artículo titulado “Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia”, se analizó sobre los tipos de seguridad en las redes inalámbricas de Área Local\(WLAN) delimitando el análisis en el país de Colombia específicamente en la ciudad de Tunja. En la investigación desarrollada se ha recolectado la información, la cual es analizada mediante el desarrollo de técnicas necesarias para medir que tan segura es una red inalámbrica en empresas tanto públicas como privadas y en demás instituciones. En la gran mayoría de las instituciones analizadas han dado como resultado, múltiples problemas en las configuraciones de todos los dispositivos que se encuentran utilizando en las empresas. Según los diferentes análisis de las diferentes instituciones se llegaron a varias conclusiones incluso se puede llegar a realizar recomendaciones, muy necesarias para ser aplicadas y no ser víctimas de los hackers.

Por citar un ejemplo (Mario & Mónica, 2018) en su artículo cuyo tema es “Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador”. El propósito de la investigación es el análisis de las fue realizar un diagnóstico de inseguridades en los diferentes tipos de redes inalámbricas existentes en nuestro país, esto permitirá que los profesionales tengan precaución en la seguridad de las redes inalámbricas, y así las empresas no tendrán inconvenientes en algún futuro. El desarrollo de la investigación fue en Quito, en Universidad Internacional SEK, con el uso de una metodología descriptiva y analítica, y también se usó técnicas de muestreo como encuestas, entrevistas. Según los resultados que se han observado se puede llegar a la conclusión que las empresas están interesadas en implementar técnicas de seguridad para sus redes inalámbricas.

Para (Reconocimiento-no, 2006) en su tesis cuyo tema es “Diseño de una red local inalámbrica utilizando un sistema de seguridad basado en los protocolos wpa y 802.1x para un complejo hotelero”; el autor de artículo relata la definición de redes inalámbricas de área local, él dice que son aquellas redes que se limitan en su área y que emplean una radiofrecuencia para el intercambio de información En la actualidad las redes inalámbricas tienen mayor acogida que las redes alámbricas, la mayoría de empresas no les gusta el tendido de cables de las redes alámbricas, por la razón antes mencionada es factible el uso de redes inalámbricas.

Otros estudios realizado por(Strategia et al., 2016), con la temática “Estudio De Esquemas De Seguridad En Redes Inalámbricas: Aplicación De Buenas Practicas En Pymes Y Usuarios Finales”; ellos en su tesis se pronuncian sobre la importancia de las redes inalámbricas en oficinas, hogares, entre otras instituciones. Pero ellos analizan que si usan redes inalámbricas el problema de seguridad surge, entonces si una PYMES incorpora redes inalámbricas, deben pensar en las medidas de seguridad pertinentes. Desde el punto de vista tecnológico, tanto los dispositivos como los usuarios deben adaptarse a las redes inalámbricas como a las medidas de seguridad. Como conclusión de la tesis llegan al punto de concientización por parte de los usuarios a interesarse por las normas de seguridad, porque así como ellos se interesan en conocer sobre seguridad de los dispositivos, existen otras personas que desean conocer sobre herramientas que les permitan acceder a datos importantes de la red inalámbrica.

2.3 Fundamentos Teóricos

2.3.1 Definición de una Red

Una red es aquella que tiene como función que la agrupación de varios dispositivos puede comunicarse entre ellos. Cuando nos referimos dispositivos no solo se refiere a las portátiles, es a todo aquel dispositivo que transmite datos, sin importar la distancia ni el conjunto de nodos que está compuesta la red. En término muy sencillo una red es la agrupación de dispositivos tecnológicos, relacionados entre en sí, permitiendo que los usuarios conectados a la red puedan transmitir y compartir datos

2.3.2 Redes Inalámbricas

Según (Baran, 2012) “las redes inalámbricas son redes que utilizan ondas de radio para conectar dispositivos sin la necesidad de usar cables de ningún tipo”. Los dispositivos actualmente hacen uso de estas redes su funcionamiento tiene una similitud muy parecida al cableado de red, estas su propósito en la transformación de la señales que recibe para ser trasmitida por medio del aire.

Este tipos de redes permiten que los dispositivos que se encuentre dentro del perímetro que cubra el dispositivo acceder a la red, esto es lo que hace que estas tengan más acogidas todavía en el mercado CITATION Dur08 \l 12298 (Durán, 2008).Las redes inalámbricas abarcan 4 grandes grupos que son:

• Redes inalámbricas de área personal (WPAN) • Redes inalámbricas de área local (WLAN) • Redes inalámbricas de áreas metropolitanas(WMAN) • Redes inalámbricas de área amplia (WWAN)

Figura 12.Clasificación de las redes inalámbricas Tomado de CITATION Sal161 \l 12298 (Salazar , 2016)

En la figura 1 se muestra en nivel de alcance de distancia de cada uno de las redes inalámbricas. Según (Cisco, 2012) Una red de área local LAN permite la conexión de dispositivos sin hacer uso de los cables, además los dispositivos usado con frecuencia actualmente hacen uso de las tecnología wifi para lograr establecer una conexión inalámbrica.

2.3.3 Ventajas y Desventajas de las Redes WIFI

Las redes Wifi poseen las siguientes ventajas: • Los usuarios al utilizar una red WIFI se sienten muy cómodos porque pueden hacer uso de la misma, varios dispositivos dentro de una zona limitada, en comparación con una red LAN. • Si comparamos un teléfono celular con una red WIFI, la red WIFI puede ser utilizada en cualquier país del mundo, mientras que el celular es restringido el uso en ciertos países. • En la infraestructura las redes WIFI no se gasta dinero mientras que en las redes LAN los gastos son muy altos. • Las redes WIFI utiliza la banda 2,4 GHz, es decir no necesita consentimientos de regulación. Las desventajas más importantes de la red WIFI son las siguientes: • Problemas de red colapsadas. • Si nos referimos a seguridad, son muy vulnerables, porque son las redes wifi las que son constantemente abusadas por hackers. • La intensidad de la red en ocasiones es mala porque son muchos dispositivos que se conectan a la red.

2.4 TIPOS DE SITIOS DE TRANSMISIÓN DE LAS REDES INALÁMBRICAS

Las redes inalámbricas se clasifican en la siguiente subdivisión:

2.4.1 Wireless WAN (Wide Area Network) Es aquella red de equipos informáticos muy extensa, por ejemplo, las redes que existen en universidades, edificios, entre otros organismos tanto públicos como privados. Estas redes utilizan las redes tanto telefónicas o las conocidas líneas muertas.

Figura 23.Diagrama de una red WiMax Tomado de (Zalazar Jordie, 2016)

2.4.2 Wireless LAN (Local Area Network) Son aquellas redes que conectan dispositivos en un área geográfica limitada, utilizan señales de radio y soportan una transmisión entre 11 Mbps y 54 Mbps, con distancia considerada de 30 a 300 metros.

Figura 34.Esquema de una WLAN en el hogar Tomado de (Zalazar Jordie, 2016)

2.4.3 Wireless PAN (Personal Área Network) Conecta dispositivos con una distancia considerada de metros, como es el caso de bluetooth, una de las tecnologías de gran utilidad para el usuario. Cabe recalcar que, para entender gráficamente sobre los tipos de redes inalámbricas, se observe la figura 2.

Figura 45.Red dispersa Bluetooth formada de dos picoredes. El maestro de la picored A es un esclavo en la picored B. Tomado de (Zalazar Jordie, 2016)

2.5 MITM (Man In the Middle) Cuando nos referimos a Man In the Middle (MITM), significa Hombre en el Medio, que básicamente consiste en el ataque que el ser humano realiza para la obtención de datos personales como las contraseñas, números de cuentas bancarias, entre otros datos de gran relevancia personal. Estos tipos de ataques se efectúan con la utilización de 2 equipos, uno que actúa como atacante y otro como la víctima, y dentro de los requisitos para utilizar la aplicación capaz de desencriptar necesita del sistema operativo Kali Linux. CITATION Nav08 \l 3082 (Joel, 2008)

2.6 Kali LINUX Es un sistema operativo, con una variedad de aplicaciones, el único sistema operativo muy útil para realizar ataques MITM (Hombre en el medio), eficiente en las normas de seguridad, es decir es difícil ser descubierto, debido que todo sus ingresos son mediante códigos únicos de acceso. CITATION Alv10 \l 3082 (Aldea, 2010)

Figura 6.Kali Linux Fuente tomado de (Linux, 2018)

2.7 Estándares 802.11 Este estándar se centra en el nivel inferior del modelo OSI, este estándar fue establecido por el Instituto de Ingenieros en electricidad y electrónica, estos estándares son aplicado en las redes wifi, debido a que hace referencia a la rapidez de la transferencia de la información CITATION Car06 \l 12298 (Carlos Pérez & Galván Salazar, 2006). Este estándar opera desde los 5 GZ, y con una velocidad aproximada de 54 Mbps, pero esta va a depender de los equipos informáticos que cuenten los personas, debido que para la frecuencia de wifi se establece desde 2.5 HZ, llegando a máximo alcanzo de 11 Mbps en dispositivos que mantengan una distancia de 300 metros. CITATION Oca05 \l 12298 (Ocando & Ugas, 2005). Los routers mantienen una conexión que se rigen en estándares para establecer una conexión entre estos estándares se encuentra:

Tabla 11.Estándares 802.11 Estándares 802.11 Descripción A Conexión 54 Mps y banda de 5 GHz B Conexión 11 Mps y banda de 2.4 GHz G Conexión 54 mbps y banda de 2.4 GHz N Conexión 54 mbps y banda de 2.4 y 5 GHz Ac Conexión 1300 mbps y banda de 5 GHz Fuente: Elaboración Propia

Las funciones de estos estándares es hacer que la tarjeta de red inalámbrica que cuente los equipos wifi, será la velocidad que pueda alcanzar el equipo.

CAPÍTULO 3

METODOLOGÍA

Según los objetivos proyectados y las fuentes bibliográficas que tienen relación con la temática: “Análisis de vulnerabilidad de redes inalámbricas con herramienta MITM”; y la línea de investigación, se utilizará investigación documental y de Campo-Cualitativa. Antes de realizar una breve síntesis conceptual de los tipos de investigación a utilizar, se definirá que es la investigación, (Graterol, 2011) expresa que todos los problemas tienen su causa y sus consecuencias.

3.1 Investigación documental La investigación según el autor Bernal Torres en su libro “Metodología de la investigación”. Define la investigación documental de la siguiente manera: “La investigación documental consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto a un tema de estudio”.CITATION Ber061 \p 110 \y \l 3082 (Bernal Torres, pág. 110) Para Cazares Hernández citado por CITATION Ber061 \l 3082 (Bernal Torres, 2006) afirma lo siguiente: La investigación documental está pendiente esencialmente de la información que se obtiene o se junta en documentos, todo material al que se puede definir como origen de la información , sin que trastorne su esencia sentido, esta información recolectada en base a documentos contribuyen y proporcionan argumentos en base a la realidad o conocimiento de un determinado tema CITATION Ber061 \l 3082 (Bernal Torres, 2006). Este tipo de investigación se basa en la obtención de la información por medio de documentos que se encuentran en los diferentes repositorios de base de datos, aquí podemos extraer información de revistas científicas para la redacción documental del presente trabajo de investigación.

3.2 Investigación de Campo-Cualitativa

La investigación de Campo según (Zanetti et al., 1990), es aquel diseño ordenado de la problemática cuyo objetivo es analizar las causas y consecuencias de la misma, haciendo uso de diferentes métodos para llegar a una conclusión especifica. Se aplicara una investigación de campo, porque en el desarrollo del tema se utilizara una herramienta cuyo nombre es Fluxion, es aquella que me permitirá conocer los beneficios de su uso, y también llegare a la conclusión de la utilidad de la misma y posteriormente a dar recomendaciones. CITATION Rod96 \l 12298 (Rodríguez Gómez, Gil Flores , & Garcia Jiménez, 1996) expresa que la investigación cualitativa es aquella muy capaz de observar el comportamiento del individuo. Con la utilización de diálogo, tradiciones de vida, reflexiones, textos fidedignos, retratos, retumbos que narran la tradición y las situaciones inciertas y los destacados en la vida de los individuos” En cuanto al término cualitativa, se refiere que los datos a localizar son los datos de la red, principalmente la clave de la red, entonces en ocasiones no tenemos conocimiento de la utilidad de las herramientas informáticas.

CAPITULO 4

DESARROLLO DEL TEMA

Existen una variedad de herramientas MITM (Man in the middle), cada una tiene sus propios requisitos; a continuación, se va describir 11 herramientas y se llegará a seleccionar una de las 11, como se muestra en la figura.

Figura 57.Herramientas MITM Fuente: Elaboración Propia

4.1 HERRAMIENTAS MITM Las herramientas MITM son las siguientes: Aircrack-Ng Esta herramienta que viene por defecto en Kali Linux, además es usada en el ámbito de auditorías informáticas. Con esta herramienta se realizan ataques para craquear las redes inalámbricas.

MITMAT Es una herramienta muy recocida de hombre en el medio, está desarrollado en python, es reconocida por generar accesos falsos y hacer que las victimas accedan a la red falsa facilitando sus datos intencionalmente. Wifite Esta herramienta es solo para Linux, usada para ataques inalámbrico de redes, almacenar claves, adulteración de direcciones Mac. Fern Wifi Cracker Es más usada en el ámbito informático para las auditorias de redes wifi. Pero también esta herramienta es usada para realizar ataques tipo hombre en el medio, esta herramienta está desarrollada en python. Bettercap Es utilizado para realizar diversos tipos de ataques en la red, manipula http, https y el tráfico del protocolo de trasporte en tiempo real, esta herramienta en muy flexible y dinámica. John The Ripper Esta herramienta cuyo nombre es “John The Ripper”, su desarrollador es Alexander Peslyak, con sistema Unix, tiene como prioridad descubrir aquellas contraseñas inseguras, las cuales son muy fáciles de ataque, es decir se puede acceder a ellas sin tanto trabajo. HashCat Esta herramienta tiene 2 notaciones, uno de ellos está enfocado al CPU y otro al GPU. Si se hace comparaciones el GPU es más eficiente que el CPU, porque el GPU tiene bastantes núcleos. Se puede aprovechar mejor esta herramienta si se usa palabras especializadas de búsqueda.

Wireshark Anteriormente tenía el nombre de Ethereal, pertenece al grupo de herramientas MITM de Kali Linux, esta herramienta tiene como función un control interno de la red .El análisis que realiza es más detallado porque va desde la conexión hasta el paquete destinario. Los paquetes destinarios con el uso de esta herramienta, brinda información sobre el tiempo de uso, el nombre del protocolo, y demás datos relevantes de los paquetes. THC Hydra Esta herramienta es una de las mejores por su rapidez y porque utiliza un método más efectivo de ataque, como lo es la fuerza bruta o diccionario, aquel método permite conseguir contraseñas sin importar los protocolos FTP, HTTP, y esto se lo realiza con la combinación de contraseñas y al momento de introducir nuestro correo y contraseña en páginas que lo requieren. Nmap Nmap, es aquella herramienta de MITM (Man in the middle), es de código abierto y tiene mayor acogida por parte de los usuarios que desean acceder a una red de forma oculta. Esta herramienta tiene varios beneficios de uso y estos son: muestra las actividades de uso de red, la configuración de los equipos, es decir, sistema operativo, RAM, etc. Fluxion Fluxión para ser instalada necesita el sistema operativo Linux, es capaz de que el usuario de la red por medio de engaño introduzca su contraseña con la verificación de la misma, y por medio de este ataque la contraseña de esa red será enviada a la persona que ocasiono la manipulación de fluxión.

4.2 Análisis comparativo entre Herramientas MITM

Luego que se analizó cada una de ellas se procede a realizar una tabla comparativa con todas las herramientas MITM nombradas anteriormente y sus respectivas características:

Tabla 22.Comparación entre Herramienta MITM Herramientas Características

Aircrack-Ng Craquear claves-Captura handshake; Ataque de autentificación.

MITMAT

Ataques DNS; Desarrollada en Python-Crea puntos de accesos falsos.

Wifite

Solo para Linux; Herramienta de ataque automatizada; Debe ejecutarse como root.

Fern Wifi Cracker

Descifra y recuperar claves WEP / WPA / WPS; Ataques de redes inalámbricas; Sistema automática de puntos de acceso. Bettercap

Ataques en la red; Manipula http, https y el tráfico del protocolo de trasporte.

John The Ripper

Desarrollada por Alexander Peslyak; Descubre contraseñas inseguras.

HashCat

Tiene 2 notaciones, uno de ellos está enfocado al CPU y otro al GPU.

Wireshark

Anteriormente tenía el nombre de Ethereal; Control interno de la red.

THC Hydra

Herramienta muy rápida; Utiliza la fuerza bruta o diccionario.

Nmap

Tiene código abierto; Muestra las actividades de uso de red.

Fluxion Necesita el sistema operativo Linux; Similar a la herramienta Wifite.

Fuente: Elaboración Propia

4.3 Selección de la Herramienta a utilizar: Fluxion

Para el presente trabajo de investigación elaborado con la temática “Análisis de la vulnerabilidades de las redes inalámbricas con herramientas MITM” luego del análisis de un grupo de herramienta se procedió a utilizar la herramienta Fluxión, aquella elección fue por su variedad de beneficios, a continuación se detalla el uso de la herramienta: Instalación fluxion en kali linux

Figura 8.Página web para descargar fluxión Fuente: Elaboración Propia

Para el uso de esta herramienta se necesita contar con el sistema operativo kali Linux, donde se procede ir a la dirección web de la página oficial de dicha herramienta mediante el siguiente enlace: https://github.com/wi-fi-analyzer/fluxion.git

Se abre una terminal y luego se selecciona la ubicación donde se clonara el repositorio. En mi caso elegiré guardar en el Escritorio. Luego escribimos el comando git clone y pegamos el link del repositorio. Esto quedara así: ~ # git clone https://github.com/wi-fi-analyzer/fluxion.git y lo ejecutamos. Vemos que en el Escritorio se creó la carpeta fluxion mediante el repositorio clonado, ahora debemos entrar a la carpeta y elegiremos el archivo llamado fluxion.sh con el siguiente comando: ./fluxion.sh lo ejecutamos y procederá con la instalación.

Figura 9.Comandos git clone Fuente: Elaboración Propia

Si la instalacion fue exitosa se procedera a ejecutar la herramiente Fluxion e omitiremos el siguiente paso. • Si al momento de instalar se produjo algun error haremos lo siguente: • Dentro de la carpeta fluxion, entramos al directorio install, luego ejecutamos el archivo install.sh, con esto se solucionara los errores de instalacion. ~ # cd install

Figura 10.Comandos para la instalación Fuente: Elaboración Propia

~ # ./install.sh

Después de la instalación se ejecutará la herramienta fluxion. Fluxion nos dará la opción de elegir el idioma.

Figura 611. Selección de idioma Fuente: Elaboración Propia

Figura 12.Canales o redes disponibles Fuente: Elaboración Propia

Luego se analiza todos los canales o redes disponibles que encontrara esta herramienta, además de presentarnos que redes se pueden localizar en el entorno.

Se tiene que tener una espera de un terminado tiempo en este caso serán treinta segundos para que la herramienta realice en análisis respectivo y muestra las redes que se hayan en el entorno y de esta manera proceder a acceder a ellas.

Figura 13.Visualización de las redes Figura: Elaboración Propia

Al momento de determina que red se va a proceder acceder, se procede a crear un punto de conexión falsa, el cual va a lograr que el usuario crea que está accediendo a su red original.

Figura 14.Creación del punto de acceso falso Fuente: Elaboración Propia

Luego de realizar las configuraciones correspondientes, se tiene que crear una interface para que la persona afectada en este caso la víctima, nos proporcione la clave de acceso a la red, además de seleccionar el idioma que va a visualizar la interface el individuo afectado.

Figura 15.Creación de la interfaz y selección del idioma Fuente: Elaboración Propia

Luego nos parecerá 4 ventanas donde se visualizan los usuarios que han realizado la conexión a red falsa; como se muestra en la figura 9.

Figura 716.Ventanas que muestran el acceso de las personas a la red falsa Fuente: Elaboración Propia Al momento que la víctima accede a la red falsa esta nos permite observar por medio de ventanas a que sitio este mantiene una conexión de que dispositivo lo está realizado y los paquetes están transmitiendo por medio de esta red.

Figura 817.Visualización de la red. Conexión de sitios y visualización de paquetes Fuente: Elaboración Propia Esto nos permite que la víctima sufra una desconexión de la red inalámbrica y al momento de querer acceder a dicha red le vas aparecer dos redes con el mismo nombre, está sin procederá a realizar la conexión de manera automática. Se realizó la prueba mediante un dispositivo Smartphone. Al momento de conectar a nuestra red falsa, a la víctima se le presentara una notificación que debe iniciar sesión en la red Wifi.

Figura 18.Demostración de la red falsa generando al usuario (Victima) Fuente: Elaboración Propia

Figura 19.Direccionamiento del navegador Fuente: Elaboración Propia

Al momento que la víctima inicie sesión en la red wifi, inmediatamente nos direccionara abriendo el navegador mostrando un mensaje que por seguridad debemos ingresar nuestra contraseña de red wifi.

Después de ingresar nuestra contraseña nos presentara un mensaje diciendo que nuestra conexión será restaurada en unos instantes, cuando en realidad lo que hará es desconectarse de nuestra red falsa y nos conectara a nuestra red real.

Figura 20.Mensaje de conexión restaurada Fuente: Elaboración Propia

Por terminar nuestra herramienta Fluxion procesará y verificará. Si la contraseña es correcta, Fluxion se cancelará automáticamente, detendrá todos los ataques y mostrará la contraseña.

Figura 921.Visualización de la contraseña por medio de la herramienta Fluxion Fuente: Elaboración Propia

Por medio de esta herramienta se obtuvo como resultado la contraseña de usuario, este caso la contraseña de la red inalámbrica de nuestra victima que es: **Plaza94**

Determinamos las pruebas elaboradas con la herramienta Fluxion, en distintas redes inalámbricas y proveedores de internet, con sus respectivas ubicaciones.

DESCRIPCIÓN PROVEEDOR MODELO_ROUTER PROCOLO_DE SEGURIDAD DIRECCIÓN CONTRASEÑA 1 NETLIFE_ Plaza NETLIFE D-Link 610 WPA Av. Colon y Panigon Encontrada 2 Netlife_Espinoza NETLIFE Cisco-Linksys E900 WPA / WPA2 Av. Colon y Panigon Encontrada 3 CNT ARMIJOS CNT Huawei HG532s WPA / WPA2 AVE Paquisha y Rio Pastaza Encontrada 4 GITO NETLIFE Cisco-Linksys E900 WPA / WPA2 Antonio Torres y Naranjal Encontrada 5 CNT GUSÑAY CNT Huawei HG531s WPA2 García Moreno y Patate Encontrada 6 WIFI SANTUR

NETLIFE Cisco-Linksys E900 WPA / WPA2 Federico Santur y Miguel C. Fuente Encontrada 7 In.Planet_Macancela IN.PLANET Qpcom QP-WR227N WPA / WPA2 García Moreno Encontrada 8 Red Oculta IN.PLANET Qpcom QP-WR330N WPA / WPA2 Av. Colon y Panigon Encontrada 9 ASTUDILLO WIFI CNT Huawei HG532c WPA / WPA2 Av. Amazonas y Atahualpa Encontrada 10 Netlife-Mayuri NETLIFE Cisco-Linksys E900 WPA / WPA2 Av. Amazonas y Calicuchima Encontrada 11 SUQUE IN.PLANET COM QP-WR227N WPA / WPA2 Carlo Julio Arosemena Encontrada 12 INPLANET Zurita IN.PLANET Qpcom QP-WR330N WPA / WPA2 Carlos Julio Arosemena y Guarda Encontrada 13 Gitoo__Red CLARO Galaxy S6 Edge WPA / WPA2 Antonio Torres y Naranjal Encontrada 14 CNT CASTILLO CNT Huawei HG531s WPA2 Elio Rivera Herbozo Encontrada Tabla 33.Pruebas realizadas con la Herramienta Fluxion

Fuente: Elaboración Propia

Figura 22.Ubicaciones donde se realizaron las pruebas

Fuente: Elaboración Propia

CAPÍTULO 5 CONCLUSIONES

Según 14 pruebas realizadas con la herramienta fluxion en diferentes lugares del Cantón Milagro, las redes inalámbricas son muy vulnerables, a pesar de utilizar los diferentes tipos de proveedores de Internet (NETLIFE, CNT e INPLANET), modelos distintos de router (D-Link 610, Cisco-Linksys E900, Huawei HG531s ,Huawei HG532s, Qpcom QP-WR227N, QP-WR330N), los cuales tenían diferentes protocolos de seguridad (WPA, WPA2), en todos las pruebas la víctima fue engañada, facilitando su contraseña de Red Wifi.

Como anteriormente se mencionó los puntos de acceso a las redes inalámbricas fueron en diferentes lugares, no se consideró una ciudadela específica, porque se quería conocer que tan útil es la herramienta MITM, por eso fueron analizadas las redes inalámbricas de algunos hogares.

Por medio de la herramienta MITM utilizada se pudo obtener el handshake de la red inalámbrica, es decir, el ataque informático, logrando la des-autenticación de los usuarios de la red, con el propósito de conectarlo al punto de acceso falso y esto facilitó el ataque para conseguir la contraseña de la red inalámbrica, como se observa en la Tabla 3, la herramienta fue efectiva porque se encontraron todas las contraseñas.

Muchas personas creían que según el proveedor o incluso según el tipo de protocolo de seguridad, dependía la confiabilidad de las redes inalámbricas, criterio erróneo, porque con el desarrollo de esta investigación quedó demostrado que ninguna red inalámbrica es segura, todas pueden ser víctimas de las herramientas MITM.

Se recomienda a los clientes que utilizan el servicio de internet, tenga precaución al momento de introducir su contraseña de su red de manera inesperada, sin ninguna explicación coherente, es una alternativa para que a futuro no sean víctimas de las herramientas MITM, porque logrando conseguir su contraseña, se conectaran con facilidad a su red y tendrán

problemas de intensidad de red y podrán extraer su datos; así como fluxión hay muchas otras herramientas que tienen como objetivo obtener claves de redes inalámbricas.

1

MERGEFORMAT 28

[Metadata removed]

Hit and source - focused comparison, Side by Side:

Left side: As student entered the text in the submitted document.
Right side: As the text appears in the source.
