FALLAS DE SEGURIDAD EN SISTEMAS DE COMUNICACIÓN INALÁMBRICAS

SANTIAGO DUQUE MARTINEZ
YUDIMAN ROJAS MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL
2019

FALLAS DE SEGURIDAD EN SISTEMAS DE COMUNICACIÓN INALÁMBRICAS

SANTIAGO DUQUE MARTINEZ
YUDIMAN ROJAS MARTINEZ

Proyecto de grado monografía, para optar por el título de Especialista En Seguridad Informática

Ingeniero / Especialista
Yina Alexandra González Sanabria
Asesor de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL
2019

Nota de aceptación

Firma del Presidente del jurado

Firma del Jurado

Firma del Jurado

Yopal 02/04/19

Dedicamos este proyecto principalmente a Dios, a la UNAD, Tutores y directores de proyectos, también dedicado a todas aquellas personas que participaron directa e indirectamente en la realización de este proyecto, a nuestros padres que los queremos mucho y los cuales nos apoyaron moral y económicamente.

AGRADECIMIENTOS

Gracias a Dios por permitirnos estar realizando este gran estudio de especialización, Agradecemos a la UNAD y todos aquellos que en ella trabajan, Directivos, comité de investigación, tutores, directores de proyectos.

Fueron muchas las entidades, empresas, instituciones, personas, a todos ellos muchas gracias por la confianza puesta en este proyecto el cual fue el resultado de mucha investigación al respecto.

Agradecer especialmente a nuestros padres quienes son ejemplo de vida y quienes nos alientan a seguir estudiando para ser mejores y poder ser de gran utilidad en este mundo moderno.

Nuestros agradecimientos a amigos y conocidos, quienes colaboraron bridando la posibilidad de poder realizar los pentest en sus redes Wi-Fi.

CONTENIDO

PÁG.

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El proyecto permitió evidenciar y dar a conocer fallas de seguridad en sistemas de comunicación inalámbricas en el municipio de Aguazul, haciendo uso de los diferentes métodos que existen para realizar pentesting a redes inalámbricas (Wi-Fi).

Se encontraron graves fallas de seguridad, la gran mayoría de redes Wi-Fi en el municipio de Aguazul son susceptibles a ataques sencillos, el problema más común encontrado es el sistema de generación de contraseñas que implementan las empresas prestadoras del servicio de internet, ese problema hace que las contraseñas sean fácilmente deducibles y por ende vulnerables a ataques de fuerza bruta.

INTRODUCCIÓN

La seguridad de la información y de las redes inalámbricas son importantes para garantizar los pilares de la seguridad informática: confidencialidad, integridad y disponibilidad.

El presente documento evidencia y da a conocer las Fallas de seguridad en sistemas de comunicación inalámbricas en el municipio de Aguazul, se realizó una serie de auditorías a las redes con el fin de cumplir a cabalidad con los objetivos del proyecto.

En el presente se encuentran las conclusiones al detalle del proceso realizado incluyendo, métodos de auditorías, tipos de vulnerabilidades y la documentación paso a paso del proceso de pentesting realizado a las diferentes redes en el municipio, Se tomó como muestra una o más redes de cada operador del total de los distintos operadores de internet del municipio de Aguazul-Casanare, se realizaron las respectivas pruebas de todas las maneras posibles para lograr evidenciar los problemas que tienen esas redes.

Las empresas proveedoras de internet en el municipio de Aguazul no configuran adecuadamente los routers y asignan contraseñas las cuales son fácilmente predecibles o default, esto hace que dichas redes estén susceptibles a distintos ataques que pueden ver comprometida la seguridad del sistema, La seguridad en las redes inalámbricas son un factor a tener en cuenta para cualquier persona u organización y saber las técnicas de auditoria de redes se hace indispensable para saber cómo defenderse ante dichos ataques, actualmente en el municipio de Aguazul se han visto muchos problemas con respecto a la seguridad de las redes ya que hay muchas personas que ya saben del tema y logran acceder a las redes inalámbricas haciendo uso de herramientas avanzadas de auditoria de redes, es un problema muy grave que se tiene que evidenciar ya que esto no puede pasar por alto.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES

Actualmente en el mundo no se tiene en un lugar de interés la seguridad informática. En la rama de la seguridad informática existe entidades las cuales por medio de certificaciones e implementaciones controles pueden llevar a cabo mejoras de seguridad que llegan a garantizar una buena seguridad en cuanto a todo lo referente seguridad de la información y toda la infraestructura tecnológica informática y de sistemas.

En la actualidad las empresas prestadoras del servicio de internet domiciliario y para empresas, no cobran o implementan controles de protección en cuanto a la seguridad de las redes LAN y WLAN.

Existen ahora protocolos de cifrado “supuestamente seguros” pero en algunos lugares de Colombia se siguen instalando protocolos que ya son obsoletos por su nivel de vulnerabilidad como los ya conocidos WEP de 64bits y 128bits.

En muchos municipios de Colombia los operadores de internet no se interesan por instalar redes inalámbricas seguras ya sea por falta de hardware o conocimientos, La mayoría de personas creen que las redes son seguras, Hay un gran desconociendo en cuanto a la seguridad de las redes esto hace que muchas personas que conocen la forma de vulnerar las redes se encargan de realizar delitos informáticos como robo de información con fines lucrativos

Actualmente existen varios tipos de protocolos unos más seguros que otros, pero ninguno con un nivel de seguridad del 100%

A continuación, se muestra una tabla en donde se pueden observar los diferentes protocolos que existen y sus respectivas vulnerabilidades.

Tabla 1 Protocolos WLANs IEEE 802.11 (Wi-Fi) y sus vulnerabilidades

Protocolos WLANs IEEE 802.11 (Wi-Fi) y sus vulnerabilidades	
WEP Estándar 802.11b algoritmo RC4 Longitud de claves 64 (40) o 128 (104) bits	• La linealidad del CRC – ICV lineares (integrity Check Value) • El chequeo de la integridad independiente de la llave • Los IV (Initialization Vector) eran demasiado cortos, reutilización de IV's, Débiles IV´s • La transmisión de IV´s en plaintext • Vulnerabilidad Shared key Authentication • No impide la falsificación de paquetes
WPA Estándar 802.11g algoritmo RC4TKIP Longitud de claves 128 a 256 bits	• Susceptible a des-autenticación de clientes • Susceptible a ataques de denegación de servicios • Se pueden desasociar usuarios • Mediante la captura del handshake debido a una asociación permite ataques de diccionario o fuerza bruta. • Se puede capturar información (sniffing)
WPA2 Estándar 802.11i Algoritmo AES Longitud de claves 128 a 256 bits	• Susceptible a des-autenticación de clientes • Susceptible a ataques de denegación de servicios • Se pueden desasociar usuarios • Mediante la captura del handshake debido a una asociación permite ataques de diccionario o fuerza bruta. • Se puede capturar información (sniffing) • Vulnerable a reinstalación de claves (Krack) • Susceptible a contaminación radial, (Ruido RF)

Fuente. El autor

1.1.1. Protocolos obsoletos vulnerables: WEP.

- WEP de 64bits: fue el primer estándar de encriptación (WEP) tiene demasiados problemas de seguridad, es muy vulnerable y no es nada recomendable.
- WEP de 128bits: se basa en el sistema WEP anterior pero con un cifrado de mayor tamaño, de igual manera es inseguro y para nada recomendable.

1.1.2. Protocolos con riesgo medio: WPA, WPA1, WPA2.

- WPA o WPA1, fue una buena transición y se arreglaron muchos fallos con respecto a WEP, pero ahora no es seguro.
- WPA-PSK (AES): usa el protocolo inalámbrico WPA con un cifrado mejorado AES.
- WPA2-PSK (TKIP): usa un cifrado TKIP con el estándar WPA2.

1.1.3. Protocolo recomendado: WPA2-PSK(AES)

- WPA2-PSK (AES): es la opción más segura. Utiliza WPA2 que es el último estándar de encriptación, y también usando el cifrado mejorado de encriptación AES [4]

1.1.4. Crecimiento de las fallas de seguridad de las redes Wi-Fi

Al pasar el tiempo se modernizan los métodos de Hacking y cada vez son más complejos, las corporaciones encargadas de realizar los protocolos 802.11 hacen su mayor esfuerzo por cada vez brindar un nivel de seguridad más avanzada pero siempre quedan fallas las cuales se pueden explotar para lograr conseguir acceso a las redes, por lo tanto se requiere que se mejoren los protocolos de tal manera que no se permita realizar ataques de denegación de servicios y mucho menos ataques de des-autenticación que permitan capturar paquetes que se puedan desencriptar por medio de ataques de diccionario (Fuerza bruta)

Las fallas han aumentado desde la desastrosa implementación del protocolo WEP el cual tubo innumerables fallas y que ahora no es para nada recomendado, con la salida del WPA2 se logró reducir las fallas y brindar un poco más de seguridad, pero esto no es suficiente ya que siempre hay alguien intentando y probando nuevos y mejorados métodos para lograr vulnerar aun los protocolos más seguros.

En la actualidad existen varios métodos por los cuales vulnerar el último protocolo de red los cuales son muy efectivos, las noticias sobre estas fallas no se publican o no se dan a conocer ya que son muy mínimas las denuncias sobre algún caso de delito informático derivado del acceso no autorizado a una red inalámbrica protegida.

En la cultura colombiana no se tiene por costumbre la seguridad, es un hecho que la gran mayoría de redes inalámbricas son inseguras, pero nadie hace algo al respecto.

---

[4] Isidro Ros. Muycomputer. Wi-Fi y protocolos de cifrado. 13 de noviembre, 2016. Disponible en: https://www.muycomputer.com/2016/11/13/wifi-cifrado-todo-saber/

1.2. DESCRIPCIÓN

En el municipio de Aguazul hay prestadores de internet como son Claro, Movistar, Tigo, Directv, Telefónica, Internet Inalámbrico, Azteca entre otros y debido a que las empresas prestadoras de internet Hogar Wi-Fi configuran mal los puntos de acceso y colocan contraseñas débiles o con patrones conocidos es muy fácil obtener acceso a esas redes.

El problema reside en la falta de seguridad debido a la mala configuración en los routers esto hace que queden fallas de seguridad con las cuales los atacantes puede tener acceso a la información importante y confidencial de los usuarios de dichas redes quienes confían ingenuamente en la protección de dicho sistema, la gravedad de esto es alta y solucionar estos problemas es de carácter urgente.

1.3. FORMULACIÓN DEL PROBLEMA

¿Qué pasaría si alguien sin autorización ingresa a su red y se roba o elimina su información confidencial?
Como ejemplos se tienen los testimonios de las personas afectadas por estos hechos, ellos manifiestan que por motivos que aún desconocen, personas sin autorización ni permisos pudieron tener acceso a la red sin darles la contraseña y esas personas están haciendo uso del servicio realizando descargas haciendo que la navegación se vea afectada por la lentitud. Esto pasa en los casos menos graves, pero que pasaría si de esta misma manera accedieran a la red de una empresa en donde tienen archivos en compartidos de red.

Las redes que tienen estos tipos de fallas son susceptibles a distintas técnicas de intrusión como son: - explotación de la vulnerabilidad wps (generador de pines) – fuerza bruta con diccionarios modificados – fuerza bruta con diccionarios numéricos de 1 a 100 millones – ingeniería social – Keyloggers – phishing – Sniffing - denegación de Servicio. [1]

---

[1] Identificación de ataques y técnicas de intrusión. Una técnica de intrusión es un conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap3.html

1.4. JUSTIFICACIÓN

La necesidad de una maximización de la seguridad es tema a fortalecer para garantizar un mayor grado de confidencialidad de la información.
Este proyecto tiene como fin evidenciar y dar a conocer fallas de seguridad de las redes wi-fi domiciliarias, ya que en el momento se han venido repitiendo constantemente errores de seguridad en el momento de configurar el router y en la asignación de las contraseñas, esto se hará con herramientas de auditoria especiales para la detección de los errores.

La razón por la cual se pretende realizar la monografía es para que las personas se enteren que están vulnerables a intrusiones no deseadas y que la información puede estar en peligro al no tener las debidas medidas de seguridad que garanticen una integridad de los datos.

Para corregir estos errores propuestos anteriormente se describirá en modo de conclusión en la monografía las formas en las que se pueden solucionar estos problemas de manera que quedará a consideración del usuario realizar los cambios necesarios. Un ejemplo de solución sería la deshabilitación de la funcionalidad wps la cual es un medio por el cual se generan vulnerabilidades.

Este proyecto aportará conocimientos avanzados en el campo de la seguridad informática a tal grado que si se implementan las correcciones a estos errores tendría un impacto social importante ya que el tener la información segura en estos tiempos es muy importante para las personas y organizaciones.
El proyecto tiene una duración estimada de 4 meses en las cuales se realizarán las respectivas actividades para dar cumplimiento a los objetivos propuestos.

El Proyecto analizará el total de las redes inalámbricas del municipio de Aguazul Casanare tomando como muestra una o más redes de cada operador del total de los distintos operadores de internet y se le harán las respectivas pruebas de todas las maneras posibles para lograr evidenciar los problemas que tienen esas redes.
Aguazul es un municipio grande y tiene muchos operadores como Claro, Movistar, Tigo, Directv, Telefónica, Internet Inalámbrico, Azteca entre otros; luego de esto, se dará un veredicto de cuáles fueron las redes más seguras y en seguida se genera un listado de las redes las cuales se encontraron fallas o errores.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Realizar un estudio en el municipio de Aguazul - Casanare que permita evidenciar y dar a conocer las Fallas de seguridad en sistemas de comunicación inalámbricas.

2.2. OBJETIVOS ESPECÍFICOS

1. Dar a conocer las distintas maneras de explotar dichos errores de seguridad.

2. Realizar pruebas de intrusión en el municipio de Aguazul con herramientas de auditoria para evidenciar errores de seguridad en las redes Wi-Fi.

3. Documentar cada una de las acciones con el fin de tener pruebas concisas de dichos hallazgos.

4. Documentar las soluciones a los fallos de seguridad encontrados en las redes inalámbricas.

3 MARCO REFERENCIAL

3.1 ESTADO DEL ARTE

3.1.1 Historial ataques y vulnerabilidades de redes Wi-Fi.

Vulnerabilidades de seguridad Wi-Fi, un grupo de investigadores han encontrado en el mes de octubre del 2017 diversas vulnerabilidades que hacen que todas las redes inalámbricas Wi-Fi sean inseguras, se trata de KRACK, este tipo de ataque se le conoce como ataque de reinstalación de clave y puede afectar a todos los estándares Wi_Fi y también sus distintos protocolos de cifrado, esta noticia fue de gran relevancia a nivel mundial ya que estuvo en peligro la gran mayoría de dispositivos, pero gracias a que se mantuvo en secreto durante un tiempo esto le dio tiempo a las empresas encargadas de solucionar dichos fallos de crear un parche de actualización que ayudo a mitigar dicha vulnerabilidad.

Existe una gran vulnerabilidad la cual es la de poder visualizar todo el historial de las redes Wi-Fi a las que nos hemos conectado tanto por Smartphone como por computadora, esto se puede lograr rooteando los móviles, con los privilegios de súper usuario se pueden acceder a dicho historial por medio de una simple app, en cuanto a Windows hasta Windows 7 se podía visualizar dichas contraseñas de redes a partir de la salida de Windows 8 se quitó dicha posibilidad, pero por medio de una simple herramienta como lo es ´dumpper´ se puede acceder al historial de contraseñas ya sea en cualquier versión de Windows, esto representa una vulnerabilidad grave ya que cualquiera que se robe o haga uso de algún dispositivo sin autorización podrá ver las claves de todas las redes a las que se ha conectado con anterioridad.

Acceso a la configuración del punto de acceso (Router), gracias a las contraseñas por defecto, la gran mayoría de routers tiene un login primario para la configuración de dicho dispositivo y en muchas de las ocasiones no se cambia y ello permite que se pueda acceder a toda la configuración y la contraseña de red inalámbrica, normalmente el usuario y la contraseña es “admin”, si una persona lograra ingresar de manera no autorizada a dicha red podrá modificar el nombre de la red, la contraseña o dejar sin uso dicho dispositivo.

Vulnerabilidad del protocolo WEP, el protocolo WEP con el cifrado RC4, este sistema de seguridad usaba el formato hexadecimal, la vulnerabilidad de este protocoló se popularizo, hubo muchos problemas a nivel mundial y se perdieron miles de millones de dólares, este sistema fue fácilmente crackeado y se realizaron bastantes herramientas muy eficientes como lo fue la suit de aircrack-ng.

Unos de los más graves casos de crackeo fue protagonizado por el hacker Albert González quien fue capturado y condenado a 20 años de prisión por robar 100 millones de cuentas de usuario y esto supuso pérdidas apreciadas por más de 1000 millones de dólares.

3.1.2 Nacional

GEOVANNY ALONSO RAMÍREZ HERRERA estudiante de la Universidad Nacional Abierta Y A Distancia "Unad" para el año 2017, GEOVANNY para optar por el título de especialista en seguridad informática realizó un proyecto que denominó "DETERMINAR LOS PRINCIPALES ATAQUES A LOS QUE SE EXPONEN LOS USUARIOS QUE UTILIZAN LA RED WI-FI "IDEA INTERNET EN EL PARQUE" DEL MUNICIPIO DE URRAO" se enfocó en Investigar tres tipos de ataques a los que están expuestas las redes WI-FI. Analizo y recomendó buenas prácticas de seguridad para que sean tenidas en cuenta por los usuarios de la red WI-FI "IDEA internet en el parque", de la Plaza Rafael Uribe Uribe del municipio de Urrao antes de conectarse a la red. Este proyecto está disponible en línea en el siguiente link: http://hdl.handle.net/10596/17596

HECTOR RICARDO TRIANA ACEVEDO, Estudiante de la universidad nacional abierta y a distancia "UNAD" para el año 2015, HECTOR para optar por el título de especialista en seguridad informática realizó un proyecto que denominó "TECNICAS BASICAS DE EXPLOTACIÓN DE VULNERABILIDADES ACTUALES EN LOS SISTEMAS DE PROTECCIÓN DE REDES WI-FI EN SOHO" en dicho proyecto se hace énfasis en los métodos de pentesting que están disponibles para la auditoria de seguridad que implementó en la empresa objetivo, en su justificación recalcó que el estándar WPS es una funcionalidad de las redes la cual es aprovechada para acceder a la red sin autorización alguna. Su objetivo general era "Determinar las vulnerabilidades más comunes en los sistemas de protección de redes WI-FI que implementan los operadores locales de redes usando técnicas de hacking" [2]

[2] HECTOR RICARDO TRIANA ACEVEDO, 2015. técnicas básicas de explotación de vulnerabilidades actuales en los sistemas de protección de redes wi-fi en soho http://repository.unad.edu.co:8080/bitstream/10596/3839/3/80374178.pdf

En Colombia se ha hecho poca investigación en cuanto a la seguridad de las redes wi-fi, las metrologías de pentesting y las vulnerabilidades expuestas en este proyecto son poco conocidas y no hay mucha información al respecto en internet.

3.1.3 Internacional

JOSÉ MANUEL LUACES NOVOA, Estudiante de la universidad Oberta de Cataluña para el año 2013, José Manuel para optar por el título de Ingeniero en telecomunicaciones, realizó un proyecto que denominó "Seguridad en redes inalámbricas de área local (WLAN)" en dicho proyecto se enfatiza en dar a conocer la seguridad que existe en las redes WLAN y los ataques que hay para las redes WLAN "Dado que las comunicaciones inalámbricas viajan libremente por el aire, una persona equipada con una antena que opere en el rango de frecuencias adecuado y dentro del área de cobertura de la red puede captarlas." Los objetivos a alcanzar en este proyecto son los siguientes: Definir de forma clara las WLAN, Valorar las ventajas y los inconvenientes del uso de estas redes, Analizar las propuestas de seguridad actuales que hay para este tipo de redes, Identificar los diferentes tipos de ataques que podemos encontrar actualmente, Comprobar mediante auditoria los métodos de seguridad WLAN más utilizados actualmente, Crear una WLAN segura mediante servidor de autenticación y autorización Radius.[3]

ALEJANDRO GONZÁLEZ MARTÍNEZ Estudiante de la universidad Oberta de Cataluña para el año 2016 realizo un proyecto para optar por el grado de tecnologías de telecomunicaciones, nombro al proyecto "Estudio de los riesgos relacionados con las redes Wi-Fi" el objetivo principal del proyecto es la de realizar un estudio completo de la seguridad en las redes inalámbricas implementadas con Wi-Fi. Se pondrán de manifiesto los problemas, más comunes, presenta en el campo de la seguridad. también se darán una serie de soluciones y recomendaciones que obstaculicen lo máximo posible esos intentos de acceso no autorizados, Este proyecto está disponible en línea en el siguiente link:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52924/9/aglezTFG0616memoria.pdf#page=12&zoom=100,0,725

[3] José Manuel Luaces Novoa. Trabajo de Final de Carrera. Seguridad en redes inalámbricas de área local (WLAN) http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

3.2 MARCO CONCEPTUAL

En este marco se encuentran unas definiciones que se verán en el proyecto; la mayoría de herramientas informáticas nombradas a continuación están incluidas en la distribución de linux (wifislax64 1.1) es en su totalidad software libre.

- HASH: Un hash es una conversión o traducción que se realiza con diferentes algoritmos, es una función muy utilizada para encriptar información o para garantizar la integridad de la información, Por ejemplo, la conversión a hash de la palabra (hola) con el algoritmo MD5 es (4d186321c1a7f0f354b297e8914ab240)

- HANDSHAKE: Handshake es el establecimiento de conexión de sistemas de comunicación, su traducción es apretón de manos, se podría decir que es un paquete de información que envía un dispositivo para enlazarse con un terminal.

En dicho paquete de conexión o enlace se encuentran los parámetros e información necesarios para establecer el intercambio de información, entre esa información están las contraseñas Wi-Fi y se encuentran de forma codificada por medio de la traducción a hash.

- PENTESTING: Es la acción de realizar diversas pruebas de penetración a sistemas protegidos con el fin de descubrir fallas o vulnerabilidades de seguridad y de esta manera prevenir ataques de piratas informáticos u otros peligros.

- CRACKEAR: Acción de romper la seguridad de un sistema informático para obtener algún beneficio derivado de ello, las maneras más usadas para esta práctica es la ejecución de ataques de fuerza bruta. Descifrar contraseñas por métodos informáticos algorítmicos es denominado Crackeo,

- TARJETAS DE GRÁFICOS: Son unidades de procesamiento de gráficos encargadas de procesar contenido multimedia en general, también se usan para realizar tareas de crackeo con mayor rapidez, las tarjetas gráficas debido a que son creadas para procesar gran cantidad de ejecución de algoritmos matemáticos complejos son recomendables para realizar comprobaciones de hash$_S$ prueba/error (Fuerza bruta).

- AIRCRAK-NG: Es una herramienta especializada en crackear claves 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede realizar comprobaciones de hash/hash

que permite decodificar información de paquetes encriptados, aircrack-ng es usualmente usado para tareas de crackeo ya que esta herramienta permite convertir una serie de variables a hash y realizar una comprobación con otro hash.

- AIRSSL: Herramienta para crear un punto de acceso falso (AP fake) los beneficios de crear un AP son con el fin de capturar información y todo lo que ello con lleva. ejemplo, hacer que un dispositivo se conecte a él pensando que es el Punto de acceso legítimo.

- AIROSCRIPT: Es un script que se encuentra en la suite aircrack-ng, con el que se puede realizar todos los ataques en dicha suite automáticamente sin introducir comandos.

- GOYSCRIPT-WEP: Software similar a la suite de Aircrack-ng para la explotar vulnerabilidades en el cifrado protocolo WEP.

- BRUTUSHACK: BrutusHack es una herramienta, para ejecutar diccionarios con parámetros pre-configurados con un handshake, anteriormente capturado.

- GOYSCRIPT WPA: Script de la suit de Goyfilms para atacar al protocolo por pines WPS a fuerza bruta si es necesario.

- REAVER: Es un script para ataques por fuerza bruta a la funcionalidad WPS: envía uno por uno todas las variantes posibles de pines a un punto de acceso objetivo, cuando se encuentra el pin valido se puede autenticar y conseguir la clave WPA.

- STRINGENERATOR: Es un Generador de diccionarios, para crackear handshake de redes WPA. Es una herramienta muy completa con la que se puede crear diccionarios con las variables personalizadas como consideremos eficaces, para algún caso en específico.

- WPSPINGENERATOR: Herramienta creada por SeguirdadWireless.net, con el cual se pueden visualizar objetivos con WPS activado y además comprueba su dirección MA C con una base de datos para verificar si el router utiliza un pin con patrón conocido o por default. Si se encuentra el pin en la base de datos se obtiene la clave WPA en segundos [4]

---

[4]Sanson - HERRAMIENTAS DE AUDITORIA WIRELESS - 15-04-2016 – Disponible en: http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/

3.3 MARCO LEGAL

3.3.1 INFORME: Amenazas de cibercrimen en Colombia 2016-2017 centro de cibernético policial.

Según el informe de amenazas de cibercrimen del centro cibernético policial de Colombia en los años 2014, 2016, 2016 y 2017 se realizaron 13.774 denuncias por delitos informáticos. [5]

- 12074 Hurtos por medios informáticos.
- 2389 Accesos abusivos a un sistema informático.
- 2195 Violaciones de datos personales.
- 625 Transferencias no consentida de activos.
- 259 Suplantaciones de sitios web para capturar datos personales.
- 100 Daños Informáticos.
- 69 Interceptaciones de datos informáticos.
- 44 Usos de software malicioso.
- 24 Obstaculizaciones ilegítimas de Sistemas informáticos o redes de telecomunicaciones.

3.3.2 Accesos abusivos a un sistema informático. Es de los delitos más cometidos, consiste en que el delincuente accede sin autorización o por fuera de lo acordado a todo o en parte de un sistema informático que está protegido con medidas de seguridad o se mantiene dentro del mismo haciendo uso de los datos o de red. [6]

3.3.3 Implicaciones legales por acceder a un sistema informático sin autorización. En general los delitos informáticos en Colombia están tipificados en la Ley 1273 del 5 de enero de 2009

---

[5]CIBERCRIMEN EN COLOMBIA 2016-2017 CENTRO DE CIBERNÉTICO POLICIAL. Ministerio de defensa nacional policía nacional de Colombia. Documento pdf disponible para la descarga en: https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

[6]Ramón J. Pérez - Los 10 delitos informáticos más frecuentes - 20 octubre, 2015. Disponible en: https://pro.giztab.com/2015/10/20/los-10-delitos-informaticos-mas-frecuentes/

“Artículo 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 1.000 salarios mínimos legales mensuales vigentes.” [7]

3.3.4 Caso ocurrido en Colombia por delitos de Acceso abusivo a un sistema informático. En una operación efectuada por la Fiscalía General de la Nación y la Policía Nacional, fueron capturadas 16 individuos, 13 de ellos adscritos a la Policía Metropolitana de Barranquilla, por otros delitos.

Después de una exhaustiva investigación, se estableció que los policías estarían cometiendo delitos de acceso no autorizado a sistemas informáticos protegidos con el fin de consultar informaciones personales a través de una herramienta que permite tener la información sobre la vigencia de seguros obligatorios y de la revisión técnico-mecánica de los automóviles exigiendo dádivas a cambio de no aplicar la norma. [8]

[7]Ley 1273 del 5 de enero de 2009 Artículo 269A: Acceso abusivo a un sistema informático.
[8] CARACOL RADIO, Barranquilla 23/11/2016 Capturan a 13 policías por presunto Acceso Abusivo a Sistemas Informáticos. Disponible en http://caracol.com.co/emisora/2016/11/23/barranquilla/1479900086_849154.html

3.4 MARCO TEÓRICO

3.4.1 Protocolos 802.11. Los protocolos 802.11 son la base de Wi-Fi. Las tecnologías específicas utilizadas por los dispositivos Wi-Fi contienen 802.11a, b, g, y n. 802.11n fue ratificado por IEEE en septiembre 2009, es un estándar nuevo, 802.11g es compatible con 802.11b, 802.11n es compatible con 802.11ª

Cuando se opera a 5 GHz, y con b/g en una banda de 2.4 GHz. 802.11n puede usar dos canales contiguos de 20 MHz, quedarían 40MHz lo que no está contemplado en los estándares preliminares, con lo anterior se puede alcanzar rendimientos reales superiores a 100 Mbps. Este estándar permite inclusive optimar esta cifra usando múltiples salidas de datos y ya existen dispositivos que utilizan esta modalidad.

802.11a,b, y g son en el momento parte del estándar IEEE 802.11-2007 que entiende todas las enmiendas certificadas hasta ese año, incluido el 802.11e que permite QoS (calidad de Servicio).[6]pag.5

3.4.2 Canales de los radios 802.11

Tabla 2. Canales IEEE 802.11 b/g Wi-Fi

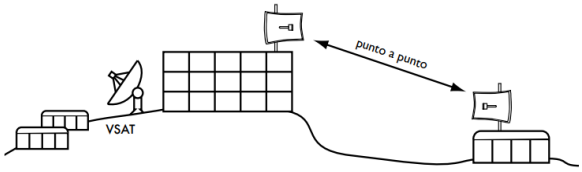
Banda	Frecuencia	Canal
2.4GHz	2412.0 MHz	1
2.4GHz	2417.0 MHz	2
2.4GHz	2422.0 MHz	3
2.4GHz	2427.0 MHz	4
2.4GHz	2432.0 MHz	5
2.4GHz	2437.0 MHz	6
2.4GHz	2442.0 MHz	7
2.4GHz	2447.0 MHz	8
2.4GHz	2452.0 MHz	9
2.4GHz	2457.0 MHz	10
2.4GHz	2462.0 MHz	11
2.4GHz	2467.0 MHz	12
2.4GHz	2472.0 MHz	13
2.4GHz	2484.0 MHz	14

Fuente: http://www.scielo.org.co/img/revistas/cein/v23n2/v23n2a01t1.jpg

3.4.3 Topología de las redes inalámbricas. Todas las redes inalámbricas complejas están constituidas por las combinaciones de uno más de las siguientes tipologías de conexiones [9]pag.12

3.4.3.1 Punto a Punto. El enlace más simple es una conexión punto a punto. Estas conexiones pueden usarse para ampliar una red a gran distancia.

Figura 1. Tipología de red WLAN Punto a Punto

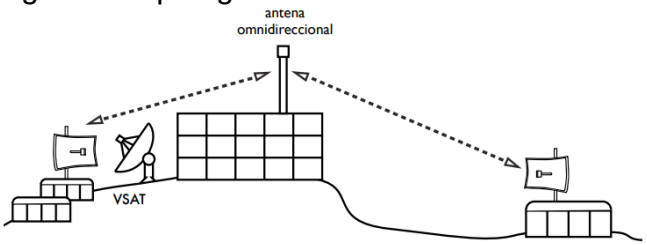


FUENTE: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf pag.13

Las conexiones punto a punto ofrecen el mayor ancho posible entre todas las configuraciones indicadas porque hay poca contienda por usar un canal.[6]pag.13

3.4.3.2 Punto a Multipunto. Es cuando un nodo debe comunicarse con el punto central se tendría una red punto a multipunto.

Figura 2. Tipología de red WLAN Punto a Multipunto



FUENTE: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf pag.14

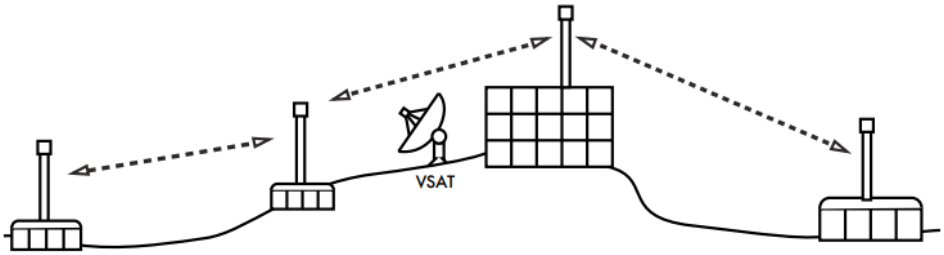
La conexión punto a multipunto una topología muy común. Considerándose en un caso un AP con demasiados clientes, A menudo la red punto a punto puede transformarse a redes punto a multipunto es posible conectarse inalámbricamente. El esquema de redes punto a multipunto es muy distinto de las redes punto a punto. No se puede sencillamente reemplazar una antena parabólica por una omnidireccional y esperar que eso sea todo. [9]pag.14

---

[9] ICTP. Introducción a las redes Wi-Fi. Materiales de entrenamiento para instructores de redes inalámbricas. Disponible en: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf

3.4.3.3 Multipunto a Multipunto. Cuando todos los nodos de una red pueden comunicarse con cualquier otro tendríamos una red multipunto a multipunto, también es conocida como redes en malla (mesh) o ad-hoc.

Figura 3. Tipología de red WLAN Multipunto a Multipunto



FUENTE:[http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf pag.14](http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf)

Las conexiones Multipunto a Multipunto son un poco más complejas, pero también más flexibles que las conexiones punto a multipunto. No hay una autoridad central en una red en malla. La tipología de malla automáticamente incluye nuevos nodos a medida que se añaden a la red, sin la necesidad de cambiar configuraciones de ningún nodo existente. Las conexiones en malla suelen ser difíciles de afinar a comparación de las redes punto a punto y punto a multipunto. Lo complicado es la escogencia del canal a ser utilizado en la red. Por lo que cada nodo comunica con todos los demás, sólo es posible usar un canal en una malla dada. Esto oprime de gran manera el caudal máximo permitido. [9]pag.14

3.4.4 Modos de funcionamiento y operación en Wi-Fi. Los dispositivos emisores y receptores de ondas wi-fi dependiendo sus especificaciones pueden operar bajo los siguientes modos

- Master (AP -access point-)

El modo master (también llamado modo AP o de infraestructura) se utiliza para instalar una red con un punto de acceso que enlaza a los diferentes clientes. El punto de acceso AP crea una red con un SSID y un canal que ofrece los servicios de la red. Los terminales Wi-Fi en modo master logran comunicarse sólo con los terminales asociados a ellos que están en modo managed. [6]pag.17

- Managed (también llamado cliente o estación)

El modo cliente. Los terminales inalámbricos en modo managed se unen a una red generada por el master y automáticamente cambia el canal para conectarse al del master. Los clientes que utilizan un determinado punto de acceso están asociados

con él. El radio en modo managed no puede enlazarse directamente entre sí y sólo se puede conectar con el master al cual está asociado. [6]pag.18

- Ad-hoc (usado en redes en malla)

El modo Ad-hoc modo se usa para generar redes en malla donde:

▸ No hay terminales en modo master (AP)

▸ Se realiza la conexión directamente a todos los nodos, Los terminales deben estar dentro de su rango de señal para poder comunicarse y deben escoger un nombre de red y canal igual. [6]pag.19

- Modo Monitor (no se usa normalmente en comunicaciones)

El modo Monitor se utiliza para oír pasivamente el tráfico en un canal dado. Es útil para:

▸ Analizar los inconvenientes en un enlace inalámbrico.
▸ Ver el uso del espectro en una zona.
▸ Ejecutar tareas de mantenimiento y de seguridad.

El modo monitor se utiliza en herramientas de auditoria (tales como Kismet) para oír pasivamente el tráfico que se transmite en un canal seleccionado. Esto ayuda a que el análisis de los inconvenientes la red y en la visualización del uso local del espectro. El modo monitor no se utiliza normalmente para comunicaciones. [6]pag.20

[6] ICTP. Introducción a las redes Wi-Fi. Materiales de entrenamiento para instructores de redes inalámbricas. Disponible en: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf

4 LABORATORIO DE ATAQUE CON PENTESTING

FASE I

En esta fase se dará a conocer las distintas maneras de explotar o aprovechar los errores de seguridad de las redes inalámbricas Wi-Fi, se tienen en cuenta todos los métodos posibles y se realiza una explicación detallada.

4.1 MÉTODOS DE PENTESTING DISPONIBLES PARA WPA/WPA2 PSK

4.1.1 Método 1: Explotación de la vulnerabilidad WPS. ¿Primero qué es WPS?

WPS es Wi-Fi Protect Setup, esta es una utilidad de los routers que permite realizar conexiones más seguras y fáciles para dispositivos.

El WPS sirve para conectar con un router sin necesidad de ingresar contraseña alguna, para ello se debe activar el escáner WPS del dispositivo oprimir el botón WPS del router y de esta manera ya tendrá acceso a la red.

Este método consiste en aprovechar la vulnerabilidad WPS, en muchos casos esta funcionalidad esta activada permitiendo una conexión fácil y rápida para cualquier atacante, debido a que hay muchas redes que tienen el pin por defecto.

Para atacar una red con vulnerabilidad WPS necesitamos ejecutar una herramienta de Wifislax la cual nos permitirá realizar un escáner de las redes las cuales tienen activada la Función WPS luego determina cual es el pin para dicho router y lo envía, lo confirma y de vuelta envía la contraseña de la red.

La mayoría de redes Wi-fi de movistar son susceptibles a esta vulnerabilidad ya que los módems vienen configurados con un pin default muy conocido el cual es 12345670.

4.1.2 Método 2: Ingeniería Social.

La ingeniería social es una técnica de hacking la cual se aprovecha de la ingenuidad y confianza de las personas.

Este tipo de ataque se puede realizar de muchas formas, una de las más comunes es por medio de una llamada haciéndose pasar por el operador de internet y pidiendo datos los cuales ayudarán a dar con la contraseña de la red.

Otra manera es por medio de la confianza hacer que la víctima preste un dispositivo como Smartphone, Tablet, Laptop, PC, luego fácilmente por medio de programas extraer todas las contraseñas de red que hay guardadas.

Este método de hacking es uno de los más efectivos ya que ataca directamente al eslabón más débil el cual es los usuarios, Todos los Sistemas de comunicación inalámbricas son susceptibles a este ataque.

4.1.3 Método 3: Captura de Handshake y búsqueda en diccionario (Fuerza Bruta). Esta técnica consiste en capturar un Handshake el cual es un paquete de datos que se obtiene por medio de la desautenticación y reconexión de un usuario legítimo de la red.

Luego se realiza un Diccionario el cual es una lista de números, letras, caracteres; comúnmente se generan en formatos (.txt).

Luego que se tienen los dos requerimientos el Handshake y el diccionario se procede a utilizar software como aircrack-ng o hashcatGUI.

Dependiendo de la computadora se pueden obtener tiempos de Crackeo más rápidos, la mejor manera de Crakear contraseñas con este método es utilizar un pc Gamer que disponga de una muy buena tarjeta de gráficos de NVIDIA.

Si no se dispone de tarjeta de gráficos NVIDIA se debe usar la herramienta aircrack-ng la cual utiliza el procesador para ejecutar el Crackeo, usar el procesador no es muy conveniente ya que este no está demasiado optimizado para este tipo de tareas ya que necesita de un poder de solución de algoritmos matemáticos de alta complejidad.

El tiempo que le lleva al procesador (Intel(R) Core(TM) i7-7500U Kaby Lake a 3.5Ghz.) en Crackear una clave de 8 dígitos es de 12 Horas, esto con una medida de 2400 comprobaciones por segundo.

Si se dispone de una tarjeta gráfica NVIDIA se puede usar la herramienta HashcatGUI la cual utiliza el poder computacional de la tarjeta de gráficos, usar la tarjeta gráfica es mucho más conveniente ya que dichas tarjetas están más

optimizadas para tareas que necesitan solución de algoritmos matemáticos de alta complejidad, por estas razones es que también utilizan estas tarjetas para minería de bitcoins. Existen versiones especiales de tarjetas gráficas de NVIDIA que disponen de procesamiento paralelo CUDA la cual proporciona un incremento considerable en los tiempos de Crackeo.

El tiempo que le lleva a la tarjeta gráfica (NVIDIA: GeForce 920MX 2GB) en Crackear una clave de 8 dígitos es de tan solo 1Hora y 15 Minutos. Esto con una medida de 19650 comprobaciones por segundo.

Estos tiempos se pueden mejorar si se dispone de diccionarios personalizados con lo cual reduciría el tiempo, esto se puede realizar por ejemplo con las redes Wi-Fi de movistar la cual tiene contraseñas de 10, 11, 12, 13, variables numéricas las cuales comienzan por los números 009 y seguido del número de cedula del propietario de la red. Teniendo ciertos números fijos podemos generar un diccionario el cual contenga el 009 y seguido todas las demás posibles combinaciones.

Para sacar por ejemplo una contraseña de Movistar como esta 00963748264 solo se tardaría 45 minutos con la tarjeta gráfica NVIDIA: GeForce 920MX 2GB

Pero ahora con los avances tecnológicos se puede disponer de tanta potencia que la única limitante será el dinero, se puede construir una maquina la cual disponga de tanta capacidad como para crackear contraseñas de 12 dígitos en tan solo 4 segundos.

Si se tienen 35 millones de pesos, es posible comprar un súper computador con las siguientes características.

Tabla 3 Características súper computador.

Placa base	Tyan
Procesador	Xeon E5 X2
RAM	64gb
SSD	1TB
Tarjeta Gráfica	EVGA NVIDIA GeForce GTX 1080 Founders Edition X8
S.O	Ubuntu 14.04.3 Server
Software para Crackear	Hashcat y Hashview

Fuente. El autor

Con esta inusual maquina se puede obtener una potencia de 341GH/s lo que equivale a que analiza 300.000.000.000 de contraseñas por segundo, esto es demasiada potencia y los tiempos de crackeo duran menos de 1 segundo, Según los datos estos serían algunas duraciones de crackeo con esta máquina.

- Tiempo de duración de descifrado con variables numéricas

8 variables en: 0.001 segundos, 9 variables en: 0,01 segundos, 10 variables en: 0,1 segundos, 11 variables en: 1 segundo, 12 variables en 4 segundos, 13 variables 1 minuto, 14 variables en: 6 minutos, 15 variables en: 56 minutos.

Esto demuestra que crackear contraseñas es relativamente fácil y muy rápido si se dispone de las herramientas necesarias, y esto sin hablar que los gobiernos mundiales tienen maquinas supremamente más potentes que la antes expuesta con las cuales pueden sacar cualquier contraseña sin importar el número de caracteres y variables, fácilmente podrían Crackear contraseñas que tengan 96 caracteres y 32 variables en menos de un segundo.

Llevamos mucho tiempo confiando en el sistema de contraseñas tradicional la cual no es un mito que ya no son seguras para nada, esto nos llevará a implementar medidas de seguridad que complementen o sustituyan las contraseñas como método para asegurar una red.

4.1.4 Método 4: Phishing (Linset Evil Attack). Como bien lo dice este software, no es ingeniería social, este ataque es uno de los métodos más intrusivos, se trata de bloquear y suplantar la red de la víctima.

Por medio de una funcionalidad de las tarjetas de red se puede tener un control total de las redes esta función es el modo monitor.

Gracias al modo monitor de las tarjetas de red es posible ver el tráfico de las redes, saber que clientes hay en cada red, expulsar a todos los usuarios de la red o sólo a los que se seleccione, capturar paquetes de conexión, crear redes falsas, clonación de redes, denegación de servicios, dañar el router por sobrecarga de tráfico o por exceso de intentos de conexión y todo esto sin estar dentro de la red.

Este método consiste en ejecutar los siguientes pasos:

- Primero, se debe escanear todas las redes para buscar una red con clientes.
- Luego, se elige una red y se realiza una desautenticación total, o sea, se desconectan los clientes.
- Después, se capturan los datos de conexión de los dispositivos que se volvieron a reconectar.
- Con dicha captura se realiza la desautenticación masiva y se clona la red original.
- Con la red original deshabilitada los usuarios tendrán que conectarse a la red clonada, cuando ingresen les pedirá que por motivos de seguridad digiten la contraseña para que puedan tener acceso a la red de nuevo.
- Cuando los usuarios introducen la contraseña esta llega al pc del atacante.

4.1.5 Método 5: Modo tramitador. Este método consiste en usar de manera no autorizada la plataforma de tramitador de telefónica que es dueña movistar.

A mediados del 2016 y 2017 la compañía telefónica tenía una página web en las que los asesores y tramitadores, empleados de la compañía pudieran realizar modificaciones y ver la configuración de todas las redes movistar de Colombia, de esta manera se podían visualizar las contraseñas sin importar que estuvieran por default o modificadas, esta práctica ilegal funcionó por un poco más de 2 años, movistar realizó acciones al respecto para mitigar dicha vulnerabilidad.

A comienzos del 2016 se conoció las primeras intrusiones a las páginas de telefónica, esto constituyo una grave falla de seguridad en las políticas internas de la multinacional.

El método consistía en ingresar con un login a las páginas de tramitador de telecom con alguno de los siguientes links:
http://trs.telecom.com.co/login.php

https://tramitador.telecom.net.co/soltecweb/login.html

https://tramitador.telecom.net.co/bandejaweb/login.html

Luego se tenía que ingresar usuario y contraseña

Usuario: Gloria.vela Clave: Colombia2017

Luego salía un panel en el que se podía administrar y ver la configuración e información de cualquier red movistar solo con ingresar el SSID.

Actualmente Telefónica cambio este sistema de tramitador, las páginas han sido bloqueadas para evitar estas prácticas ilícitas. Este método representó una de las fallas más graves que ha tenido telefónica después de la manera tan insegura de generar las contraseñas Wi-Fi.

FASE II

En esta fase se establece la práctica a seguir en cuanto a las pruebas de auditoria, también se exponen la forma en la que se recolecto la información y las herramientas necesarias para la correcta realización de los objetivos planteados.

4.2 PENTESTING A REDES WI-FI

Para esta fase del proyecto se toman como muestra una red de cada operador de internet del municipio de Aguazul Casanare, el objetivo es realizar una serie de pruebas de intrusión para determinar el nivel de seguridad y para evidenciar si hay problemas de seguridad que pongan en riesgo dicha red o la información contenida en ella.

Para estas pruebas de pentesting se hace uso de un sistema operativo distribución Linux el cual es la herramienta especializada en seguridad inalámbrica (Wifislax64bits).
Hay 5 proveedores de internet en el municipio de Aguazul cada proveedor tiene diferentes maneras de configurar las redes inalámbricas Wi-Fi.

4.3 RECOPILACIÓN DE INFORMACIÓN SOBRE LOS OPERADORES DE INTERNET

A lo largo de la ingeniería de sistemas y la especialización se comenzó con la recolección de información entre amigos y conocidos los cuales disponen de internet fijo e inalámbrico, muchos de ellos son de operadores distintos lo cual beneficia la compilación de información, dichas personas suministraron información como nombre de las redes y las contraseñas de acceso, de esta forma se logró identificar los diferentes patrones que hay para cada operador.

4.4 SELECCIÓN DE PARTICIPANTES PARA LAS PRUEBAS DE PENTESTING WI-FI

Aguazul es un municipio de Colombia ubicado en el departamento de Casanare, Cuenta con cerca de 40mil habitantes, se han elegido entre amigos y conocidos una persona por cada operador de internet, se les realizo la debida explicación pertinente antes de realizar cada prueba y cada dueño dio su autorización expresa.

Las pruebas se realizaron de forma controlada sin llegar a afectar los dispositivos ni su configuración, No se realizaron auditorías a empresas, únicamente a usuarios de internet fijo residencial.

4.5 OPERADORES SELECCIONADOS Y UBICACIONES POR BARRIOS

- MOVISTAR
- UNE INALÁMBRICO
- DIRECT TV INTERNET
- AZTECA COMUNICACIONES
- INTERNET INALÁMBRICO TV CABLE YOPAL SAS

Todos los operadores a excepción de AZTECA COMUNICACIONES tienen cobertura en todo el municipio por lo cual los operadores están dispersos de forma homogénea en todo el municipio,
En los barrios altos del norte predominan las redes de movistar y Directv Internet y para los barrios del sur están más presentes las redes de Azteca y Une.

4.6 HERRAMIENTAS NECESARIAS PARA ALCANZAR LOS OBJETIVOS PLANTEADOS

Tabla 4. Herramientas y sus características

HERRAMIENTA	CARACTERÍSTICAS
Computador portátil 	Marca: ASUS ASUSTeK COMPUTER INC. SO: Microsoft Windows 10 Pro 64-bit Procesador: Intel(R) Core(TM) i7-7500U Kaby Lake up to 3.5Ghz. Memoria RAM: DDR4 8,00 GB ADATA Premier 2400 MHz Modelo: X441UVK NVIDIA: GeForce 920MX 2GB Pantalla: 14” Intel HD Graphics 620 (1920x1080@60Hz) Disco Duro: 1TB Hitachi HGST HTS541010A9E680 (SATA) Red: Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC

Tarjeta De Red Inalámbrica USB de alta potencia Rompe Muros 5dBi 	Marca: TP-LINK Modelo: TL-WN7200ND Interfaz: MiniUSB/USB Conectividad: WPS Antena: antena desmontable omnidireccional (RP-SMA) Ganancia de Antena: 5dBi Frecuencia: 2.400-2.4835GHz Wireless Standards: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
USB 	Kingston 8GB DataTraveler USB 3.0 Pen Drive - DT111
S.O. (Wifislax) 	Wifislax64bits: final versión 1.1 Imagen: Iso Base: slackware64-14.2 Live Wifislax Wifislax es un live CD. Es una distribución sistema operativo Linux, se puede iniciar sin necesidad de instalación directamente desde un dvd, memorias USB o en disco duro. Wifislax es un linux live cd creado por www.seguridadwireless.net y está totalmente pensado para realizar pruebas de seguridad a las redes wireless.
	Rufus: es una herramienta útil que ayuda a formatear y crear USBs de arranque, como «pendrives», tarjetas de memoria, etcétera.

Fuente. El autor

FASE III

En esta fase se realizan pruebas de intrusión a las redes Wi-Fi en el municipio de Aguazul haciendo uso de los métodos de pentesting expuestos en la fase I, se hace uso de equipos de cómputo y periféricos expuestos en la fase II, con el fin de evidenciar errores de seguridad en las redes Wi-Fi, se documentan cada una de las acciones como prueba de dichos hallazgos.

4.7 PENTESTING A REDES WI-FI MOVISTAR

La compañía multinacional de tecnología y comunicaciones Telefónica, dueña de la marca Movistar, ha tenido en los últimos años un crecimiento en sus ventas y clientes gracias a la mejora de sus servicios.

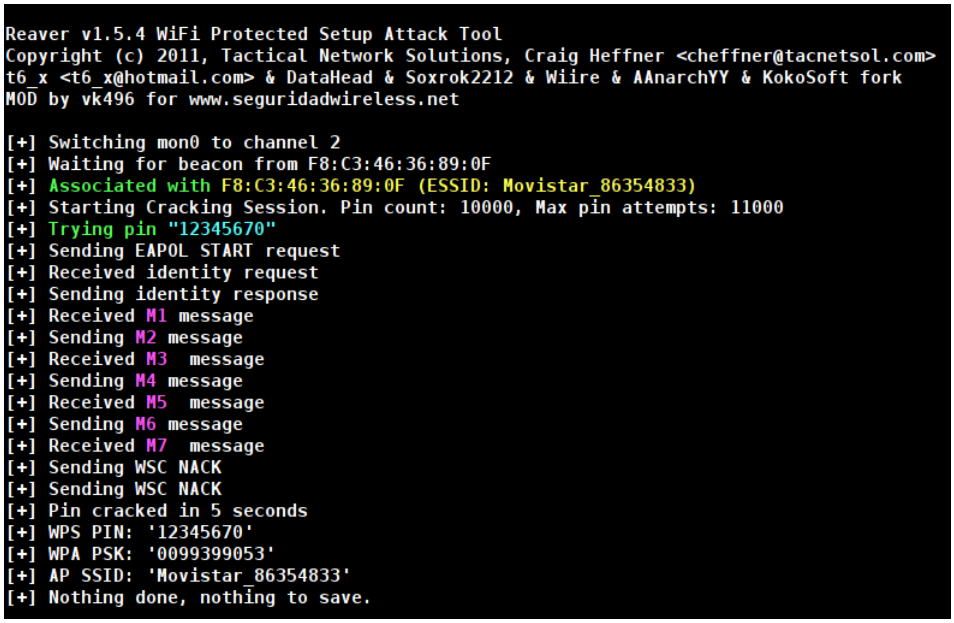
La empresa movistar se ha ganado una gran aceptación en Colombia por la gran cobertura con la que cuenta para prestar los servicios de comunicaciones móviles, redes de datos móviles 4g e internet local cableado banda ancha.

En cuanto al sistema de encriptación, generación de contraseñas de las redes Wi-Fi es la empresa con la peor seguridad, acceder a estas redes es tan fácil que hasta se puede con ejecutar una simple aplicación en el Smartphone.

La seguridad de estas redes de internet Wi-Fi es tan pésima que con todos los métodos se puede obtener la clave de Wi-Fi.

Para probar esta afirmación se ha realizado la siguiente auditoria en donde se evidencia que dicha red fue hackeada por medio de la vulnerabilidad wps,

Figura 4. Obteniendo contraseñas Movistar con bug wps



Fuente: El Autor

Como se ve en la imagen, la contraseña salió por el método de explotación de vulnerabilidad WPS en tan solo 5 segundos, algunas veces sólo dura 2 segundos dependiendo de la distancia del AP, el pin utilizado en este ataque fue automático calculado por el software y el cual envió el pin 12345670 que es el más inseguro ya que es el que comúnmente se utiliza como default, movistar tiene esta grave vulnerabilidad desde hace mucho tiempo.

Todos los routers configurados hasta finales de 2016 tienen esta vulnerabilidad, a principios de 2017 movistar decidió cambiar el sistema de generación de contraseñas, pero este cambio agravo el error en vez de arreglarlo. Hasta el momento de hoy, un total del 80% de las redes Wi-fi de movistar son susceptibles a ataques de fuerza bruta con diccionarios personalizados.

Aquí algunas otras capturas de pantalla demostrando esta vulnerabilidad con diferentes pines.

Figura 5. Obteniendo contraseñas Movistar con bug wps

Fuente: El Autor

Como se puede observar estas redes movistar las cuales tienen el ssid Movista_xxxxxxx son altamente susceptibles y fácilmente hackeables ahora movistar ha corregido esta vulnerabilidad, pero siguen fallando con la generación de contraseñas.

4.7.1 Nuevo sistema de generación de contraseñas de Movistar. En la actualidad movistar establece 12 números en las contraseñas haciendo que obtener estas contraseñas por fuerza bruta sea dificil para personas que no tengan una computadora tan potente.

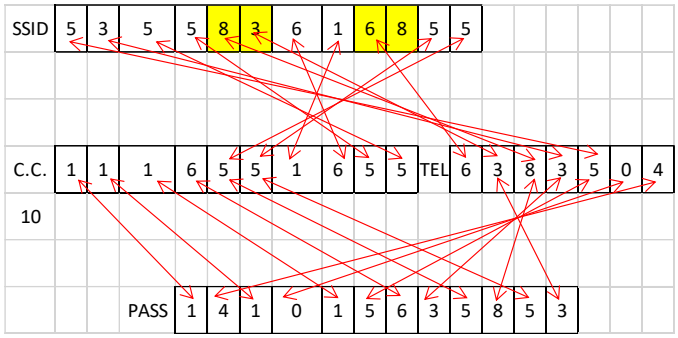
Para descifrar una contraseña de 12 variables numéricas con la tarjeta de gráficos NVIDIA GeForce 920MX de 2GB duraría 20 meses, de 12 variables numéricas con el computador de 35 millones anteriormente mencionado duraría tan solo 4 segundos.

Hace dos años Movistar ha venido cambiando el sistema de generación de contraseñas y los SSID ahora es de la siguiente manera:

Los SSID son 12 números ejemplo: 535583616855, Las contraseñas también son 12 ejemplo: 141015635853, El dueño de la red es el señor Ingeniero Yudiman Rojas El número de cédula del propietario de la red es 1116551655 y el teléfono fijo es 6383680.

Aparentemente se ve seguro, pero no, realizando un pequeño análisis a estos números se puede evidenciar que dichos números coinciden, o sea, que la mayoría de los números usados en el SSID y la contraseña proceden de la cédula y el número de teléfono fijo.

Figura 6. Nuevo sistema de generación de contraseñas de Movistar



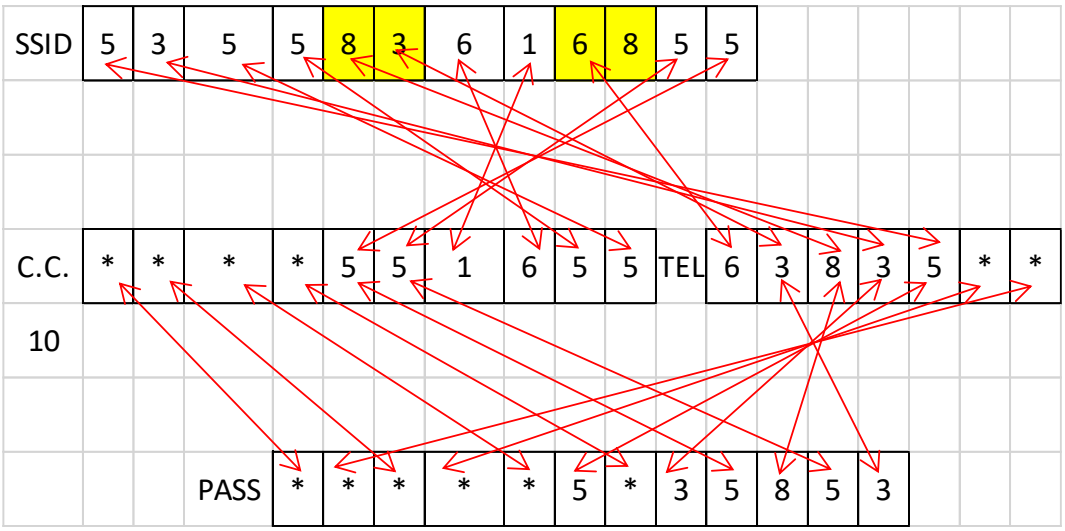
Fuente: El Autor

Como se puede observar en la imagen, movistar está generando las contraseñas tomando los números de cédula y los del teléfono, intercalados.

Ahora con estos cambios movistar sigue siendo susceptible a ataques de ingeniería social y fuerza bruta con diccionarios personalizados.

En este caso para generar un diccionario personalizado tan solo se necesita el SSID de la red, por ejemplo:

Figura 7. Descifrado parcial de la contraseña



Fuente: El Autor

Como se puede observar en la imagen con tan solo el ssid salen 5 números sufijos ósea que están fijos en la derecha con esta ventaja solo faltarían 7 números.
Ahora simplemente hay que hacer un diccionario que comience en 100000035853 y termine en 199999935853 lo cual es muy simple.

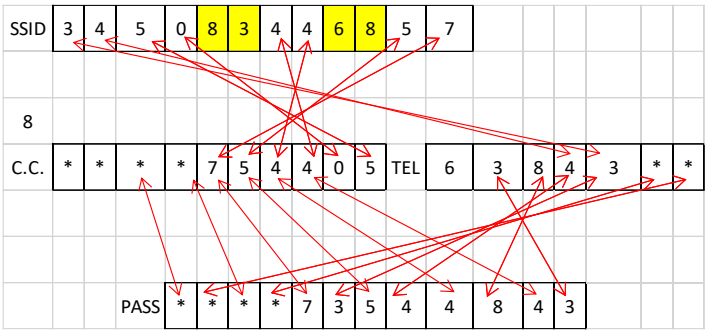
Como ya se generaron 5 números, faltarían por saber 7 números para ello se ejecuta el diccionario y con la tarjeta de gráficos NVIDIA GeForce 920MX 2GB duraría tan solo 10 minutos. Movistar sigue siendo la empresa más insegura de todas a menos que desactiven el wps y que mejoren el sistema de generación de contraseñas.

4.7.2 Paso a paso auditoria a red Wi-fi Movistar. El método a usar para la auditoria a la red inalámbrica de la empresa movistar es por fuerza bruta usando diccionario personalizado.

4.7.2.1 Identificación de la red. Lo primero es identificar el SSID de la red (Nombre de red Inalámbrica) En este caso será la red Wi-Fi de Movistar con el siguiente SSID (345083446857)

4.7.2.2 Generación de parte de la contraseña. Para generar el diccionario adecuado en el que este la contraseña para esta red se debe hacer uso del sistema de generación de contraseñas de movistar

Figura 8. Generación de parte de la contraseña

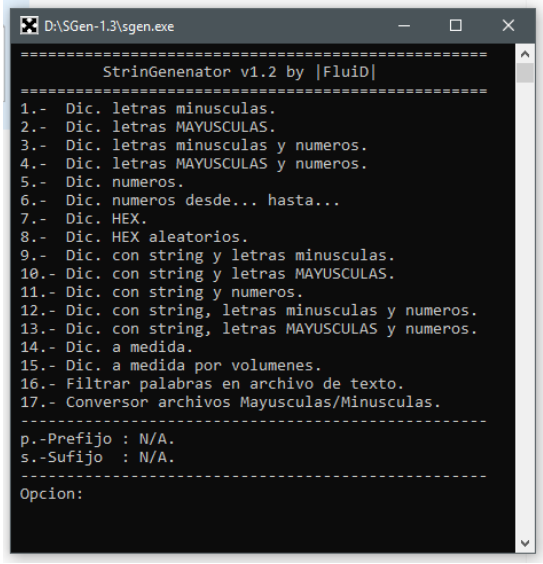


Fuente: El Autor

Con el nuevo sistema de generación de contraseñas de movistar, solo con saber el SSID se puede saber parte de la contraseña como se muestra en la gráfica anterior, como se puede evidenciar parte de la contraseña es (****73544843)

4.7.2.3 Generación del Diccionario personalizado. Generación del Diccionario personalizado haciendo uso da la herramienta de generación de diccionarios personalizados llamado StringGenerator v1.2 de FluiD

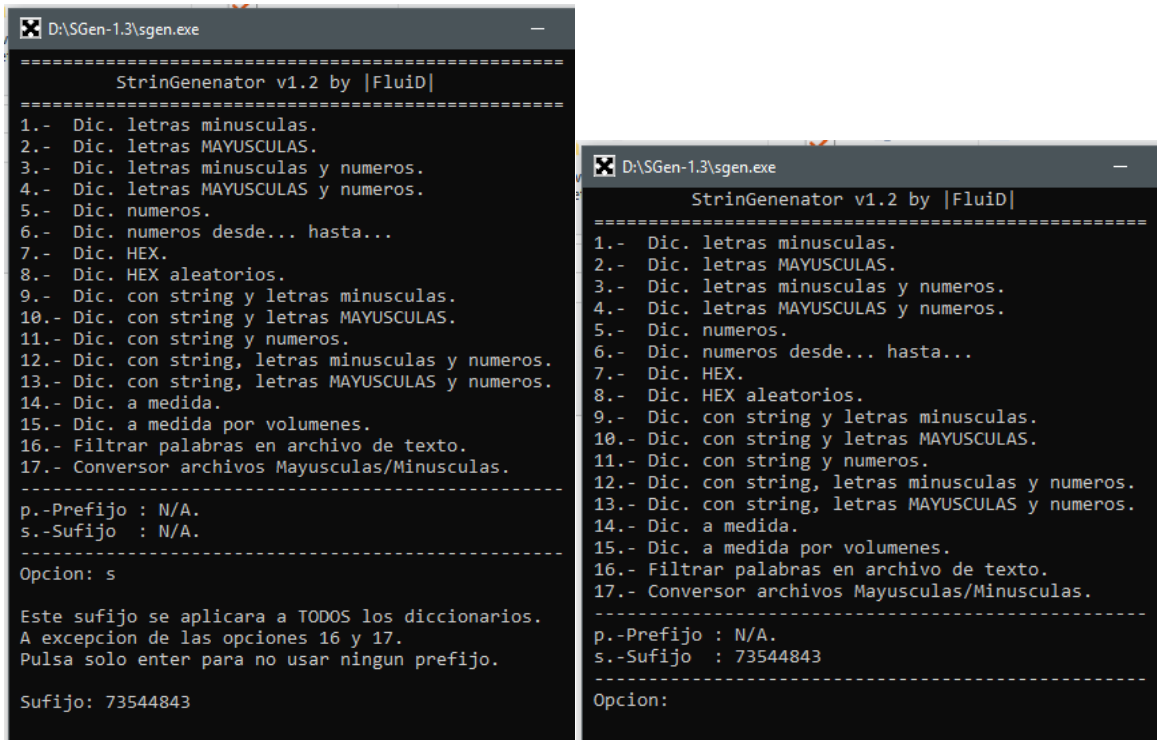
Figura 9. Generación del Diccionario personalizado



Fuente: El Autor

Luego que ejecutamos la herramienta, sé genera el diccionario de la siguiente manera; colocar el sufijo con el fragmento de contraseña, para ello se oprime (s) y se introduce (73544843) y enter.

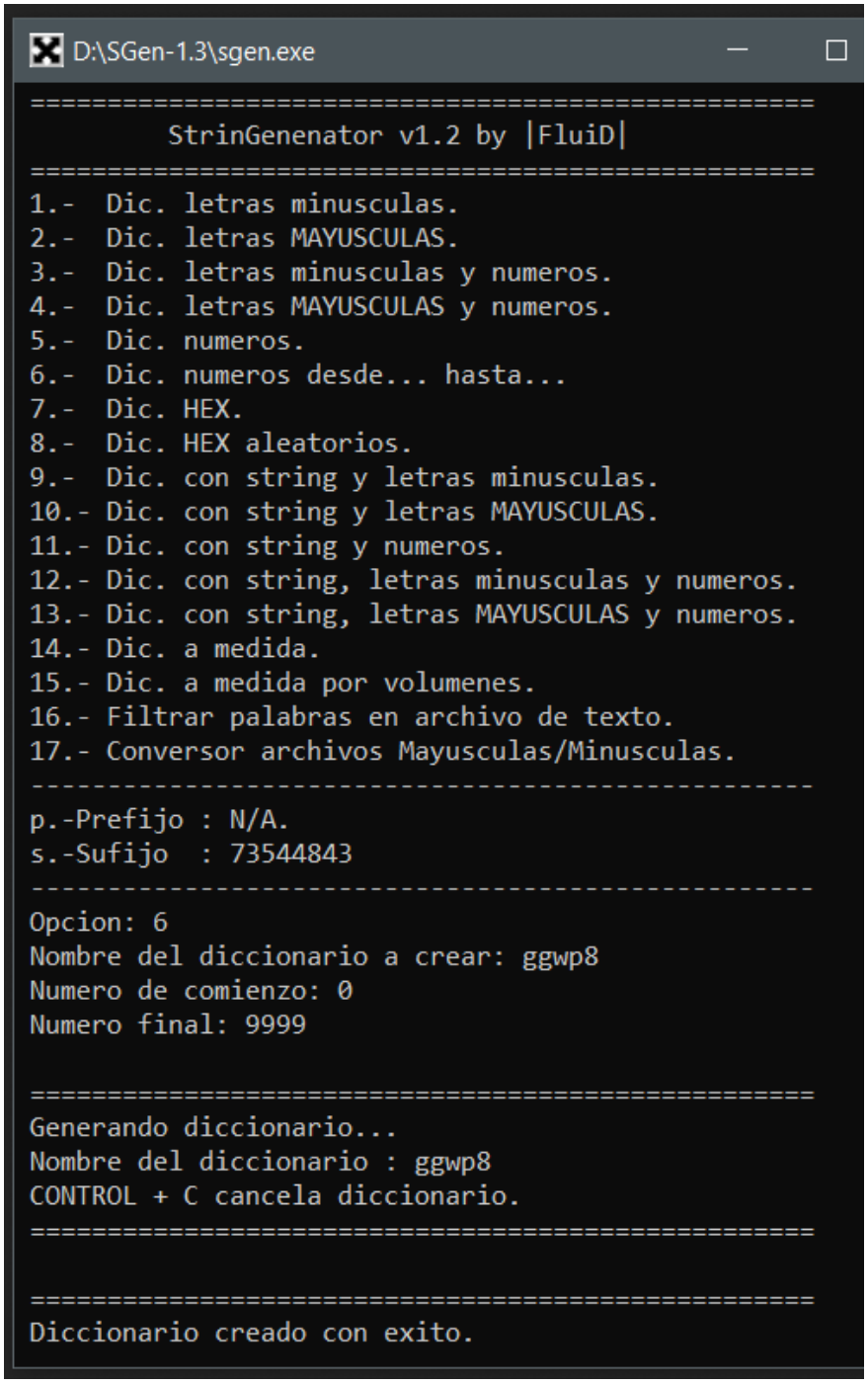
Figura 10. Generación de diccionario



Fuente: El autor

Luego seleccionar la opción Dic. Números desde… hasta…(Opción 6) luego colocarle nombre al diccionario en este caso se llamará (ggwp8), en seguida se escribe el número de inicio (0) y luego el número de final (9999) y enter.

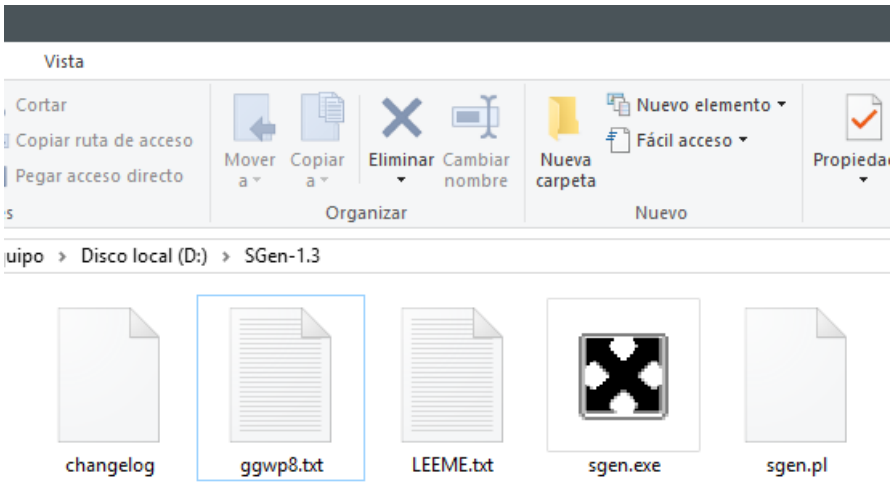
Figura 11. Generación de diccionario



Fuente: El autor

El diccionario queda generado en la carpeta del StringGenerator v1.2

Figura 12. Generación de diccionario



Fuente: El autor

4.7.2.4 Captura de Handshake. Ahora se tiene que capturar el Handshake para ello se usa la herramienta Handshake disponible en el sistema operativo Wifislax, de la siguiente manera:

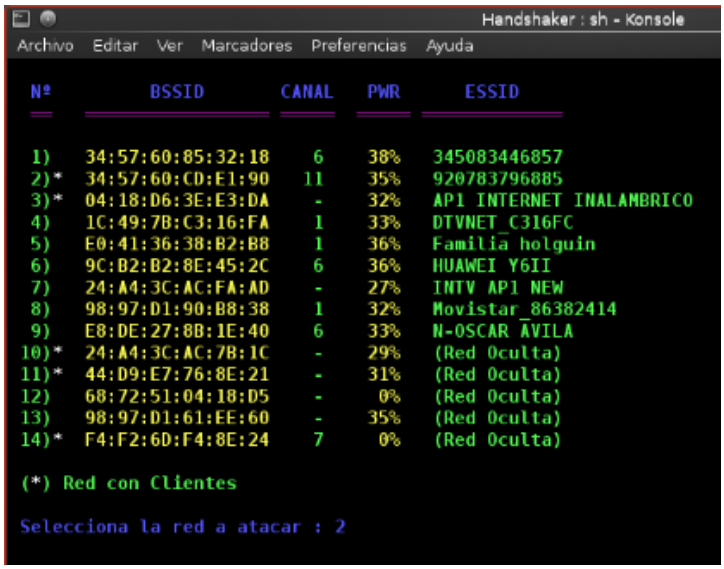
Se ejecuta la herramienta Handshaker y se selecciona la tarjeta de red a utilizar, en este caso (1)

Figura 13. Selección de tarjeta de red

Fuente: El autor

Luego se selecciona la red a la que se quiere obtener el Handshake

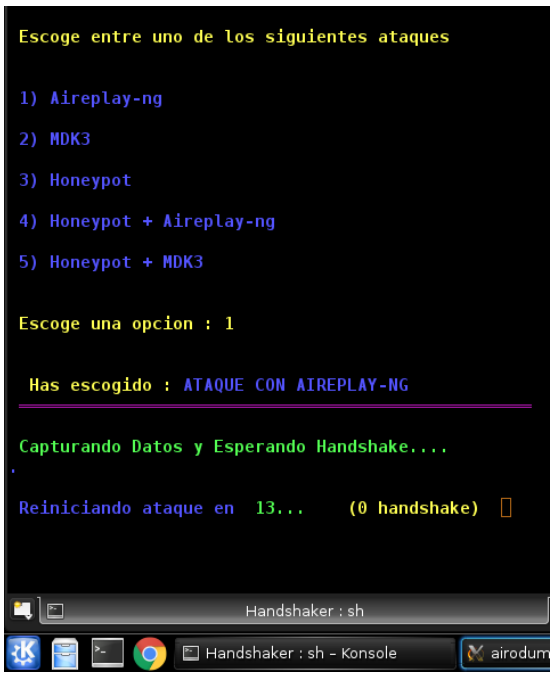
Figura 14. Selección de red



Fuente: El autor

Una vez seleccionada la red se escoge el tipo de ataque a usar, en este caso es recomendable la primera opción 1) Aireplay-ng, enseguida se iniciará el ataque.

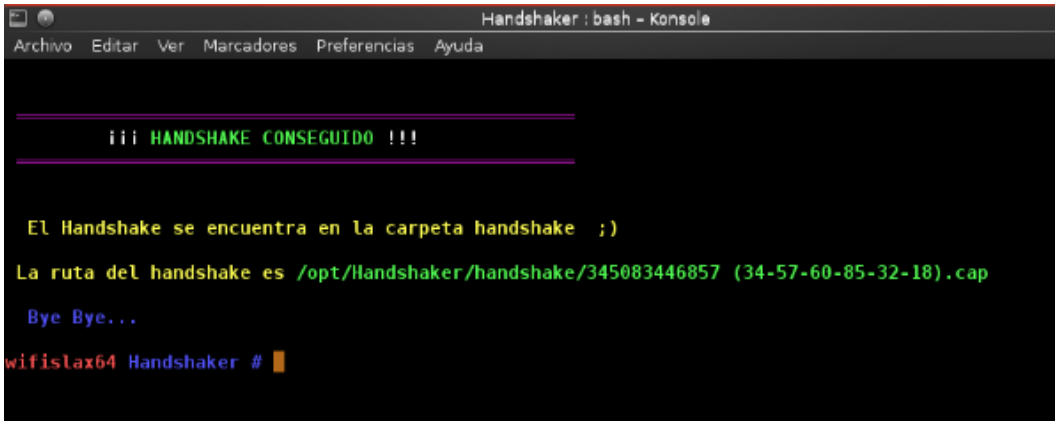
Figura 15. Selección de ataque



Fuente: El autor

Una vez iniciado el ataque se desautenticarán usuarios legítimos y al momento de la reconexión se captura el Handshake como lo muestra la siguiente figura:

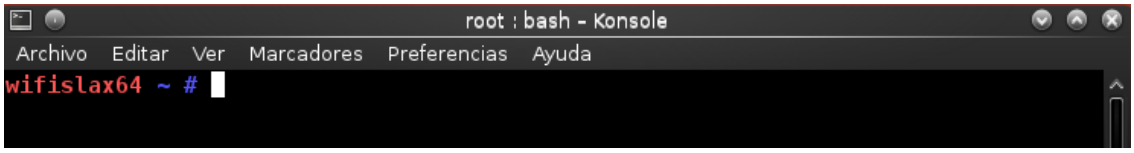
Figura 16. Handshake Capturado



Fuente: El autor

4.7.2.5 Ataque con la Herramienta Aircrack-ng (Fuerza bruta). Para usar Aircrack en Wifislax se debe ejecutar la consola

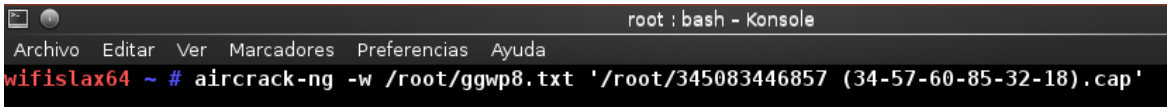
Figura 17. Consola de Wifislax



Fuente: El autor

Una vez iniciada la consola se debe ingresar el siguiente comando (aircrack-ng –w diccionario.txt Handshake.cap) para seleccionar el diccionario y el Handshake, en este caso sería (aircrack-ng –w '/root/ggwp8.txt /root/345083446857 (34-57-60-85-32-18).cap) como se muestra en la siguiente figura.

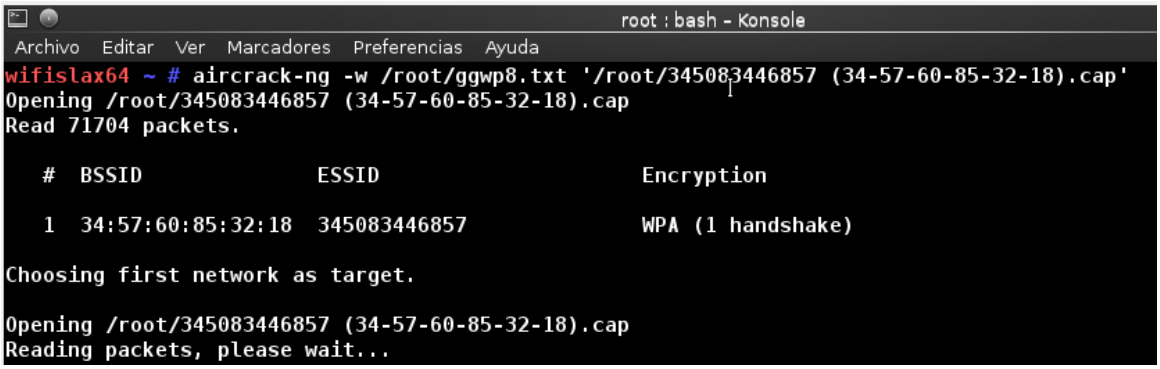
Figura 18. Comando de Aircrack-ng



Fuente: El autor

Una vez se da enter inicia el ataque de fuerza bruta.

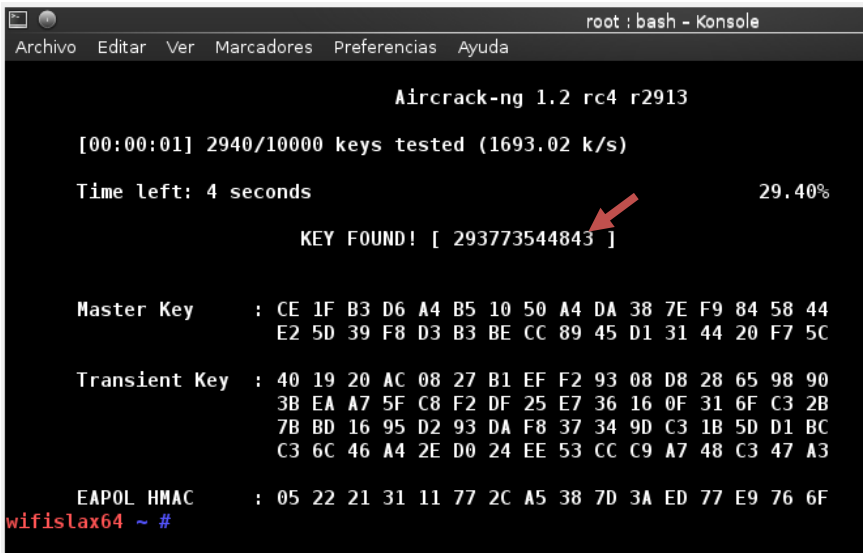
Figura 19. Ataque de fuerza bruta



Fuente: El autor

Como el diccionario solo tenía 9999 posibles contraseñas la herramienta Aircrack-ng logró dar con la contraseña en 4 segundos como lo muestra la siguiente figura:

Figura 20. Ataque de fuerza bruta, contraseña encontrada



Fuente: El autor

4.8 PENTESTING A REDES WI-FI DTVNET (Internet inalámbrico de DIRECTV)

4.8.1 Sistema de seguridad de las redes DTVNET. Las redes DTVNET cuentan con un sistema de generación de contraseñas de seguridad medianamente robusta, el sistema de seguridad que implementa DTVNET en la mayoría de casos es el uso de 8 letras minúsculas totalmente aleatorias Ejemplo:(wrktvwvb) esta seguridad es

relativamente buena ya que para descifrar este tipo de contraseñas con medios convencionales se tardaría demasiado tiempo.

Para descifrar una contraseña así haciendo uso de un PC i7 y una tarjeta gráfica NVIDIA: GeForce 920MX tardaría 5 meses, Para lograr descifrar esa contraseña haciendo uso de la fuerza bruta tocaría disponer de 50 PCs para que se lograra descifrar la contraseña en una hora, esto hace que los ataques por fuerza bruta no sean una opción recomendable en este caso.
En tal caso el ataque más efectivo seria por medio de phishing o ingeniería social.

4.8.2 Paso a paso auditoria a red Wi-fi DTVNET

4.8.2.1 Identificación de la red

Figura 21. Identificación de la red

Fuente: El autor

Las redes Wi-Fi de Directv generalmente tienen como SSID las iniciales DTVNET y seguido de la terminación de la numeración MAC, en seguida se realizará la auditoria a la red con SSID (DTVNET_D57062)

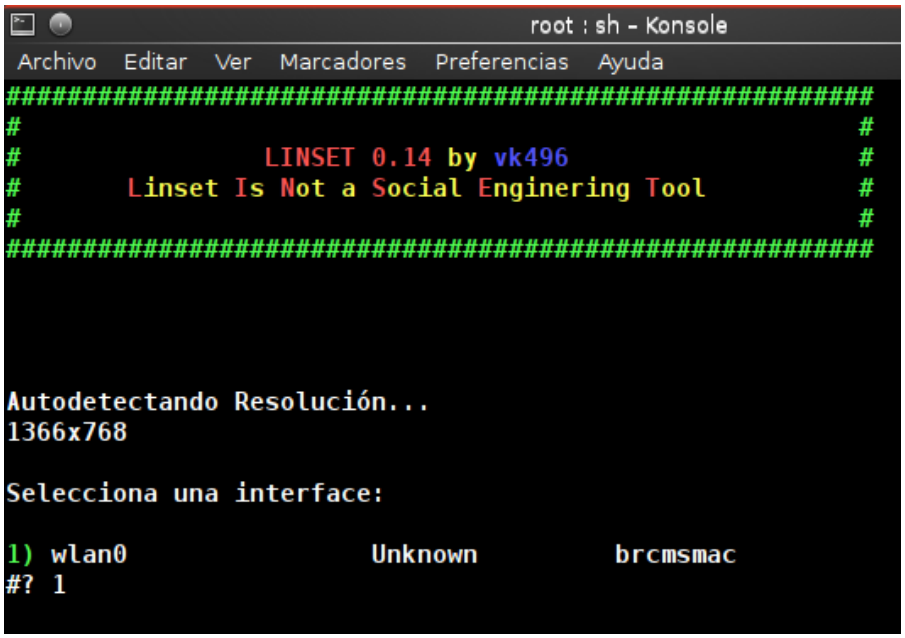
4.8.2.2 Ejecución de la herramienta Linset (Evil twin attack). La herramienta Linset se encuentra disponible en el sistema operativo Wifislax.

Figura 22. Ubicación de la herramienta Linset en Wifislax

Fuente: El autor

Una vez se ejecuta esta herramienta, se debe seleccionar la tarjeta de red que vamos a usar, en este caso la wlan0 (opción 1).

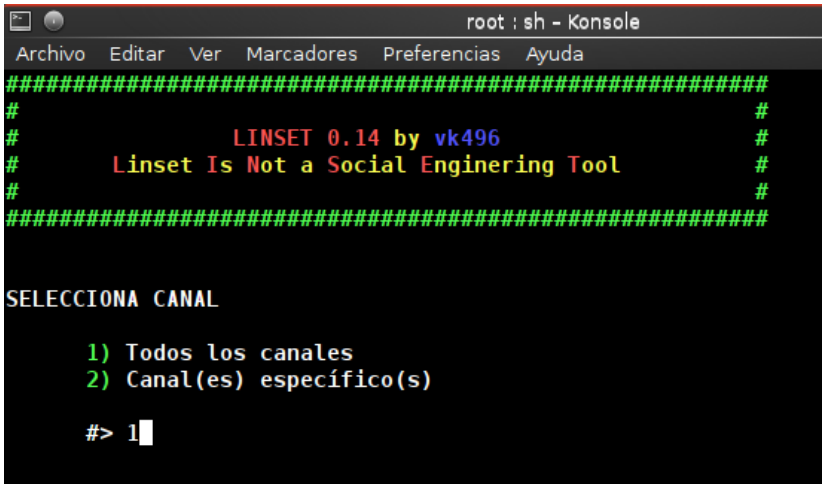
Figura 23. Selección de Interface



Fuente: El autor

Se debe seleccionar los canales, en este caso se seleccionan todos los canales (opción 1).

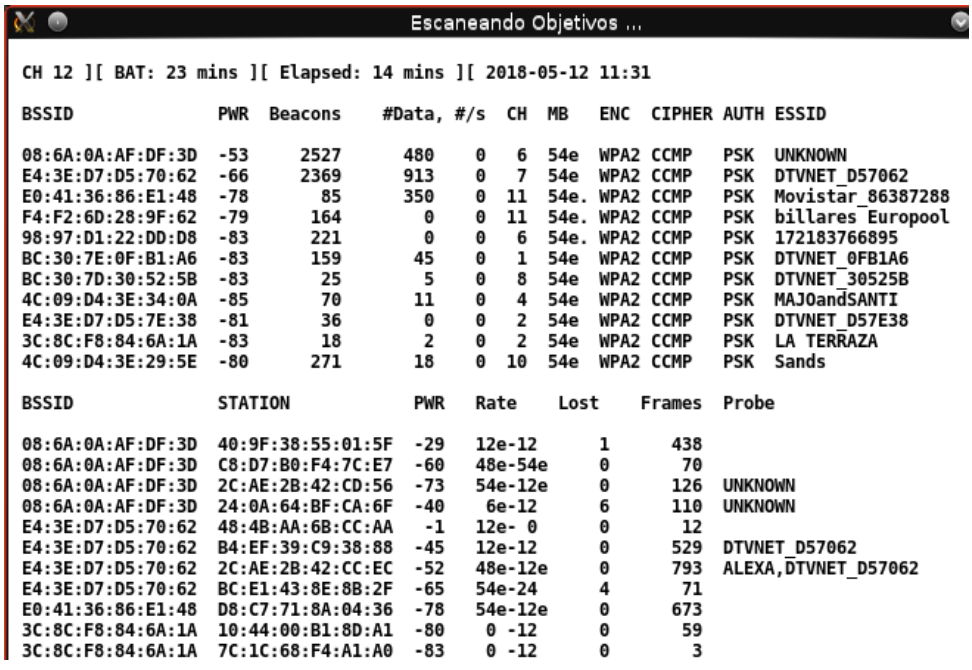
Figura 24. Selección Opción 1.



Fuente: El autor

En este paso se activa un escáner en el que se puede observar el total de las redes que se tengan según su cobertura, se tiene que dejar escanear por unos 5 minutos mientras encuentra clientes, luego de eso se puede cerrar esta ventana.

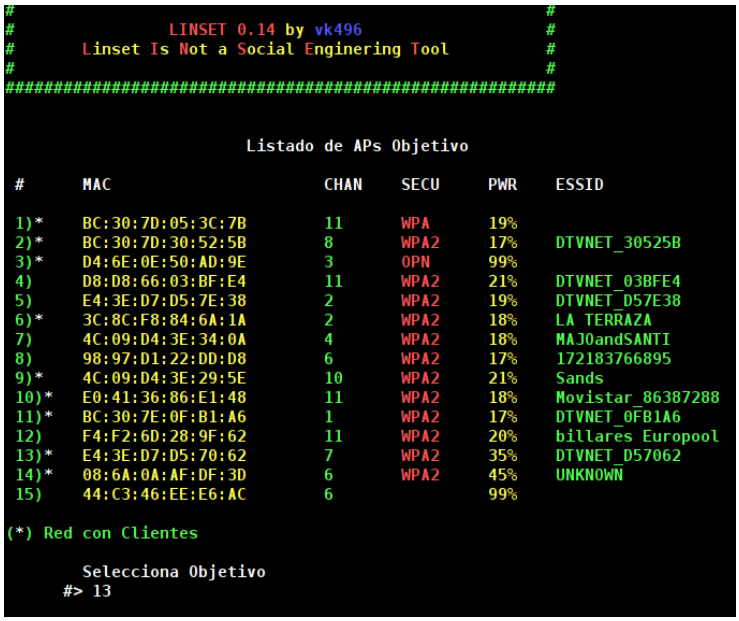
Figura 25. Escaneo de redes



Fuente: El autor

Una vez se cierra la ventana de escaneo se podrá visualizar un listado de redes, lo siguiente es seleccionar la red a la que queremos auditar en este caso es la numero 13, se escribe 13 y enter.

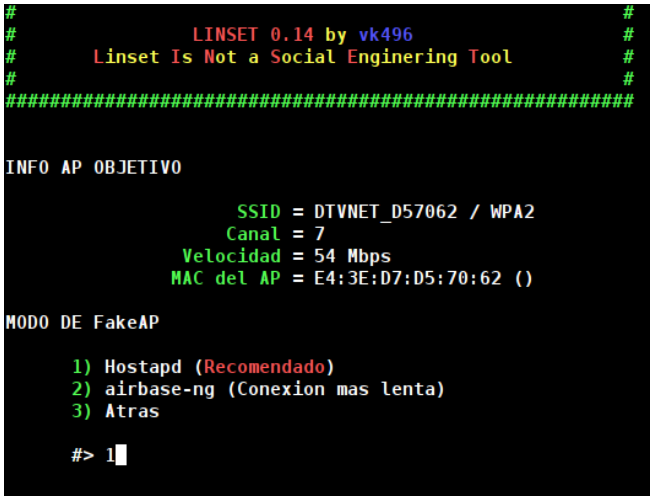
Figura 26. Resultado del escaneo



Fuente: El autor

Una vez se selecciona la red se da ahora a escoger el modo FakeAP en este caso es recomendable la opción 1.

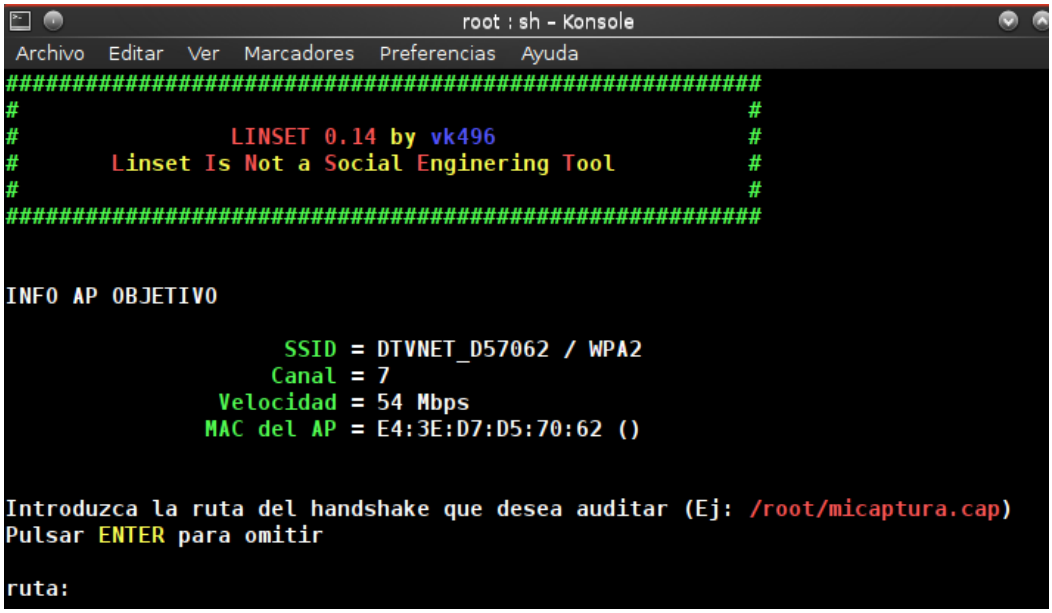
Figura 27. Selección del modo FakeAP



Fuente: El autor

En este paso, si se tiene la ruta de la una captura del handshake se debe introducir ahí, de lo contrario dar enter para omitir y capturar el handshake.

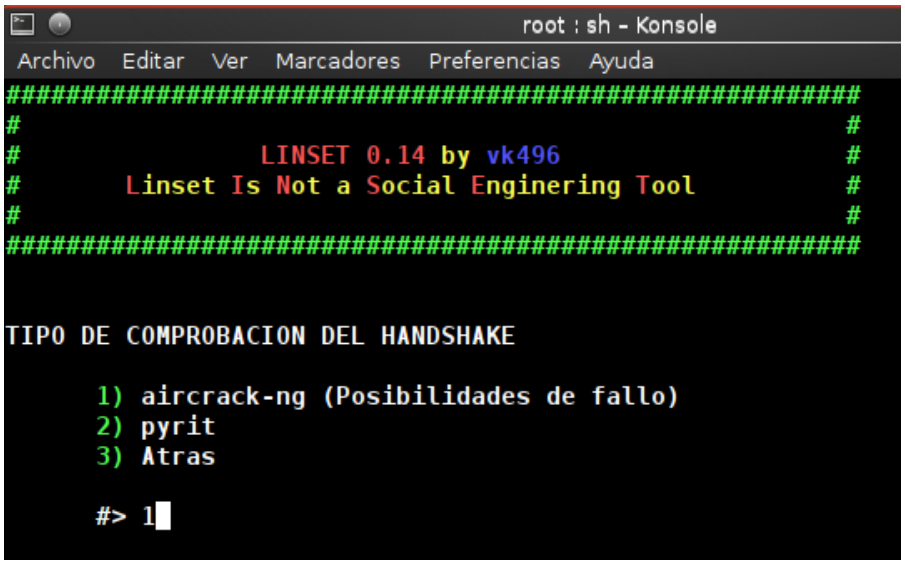
Figura 28. Captura o selección del Handshake



Fuente: El autor

Luego, se tiene que seleccionar el tipo de comprobación de handshake en este caso es recomendable Aircrack-ng se selecciona (opción 1).

Figura 29. Selección de comprobación



Fuente: El autor

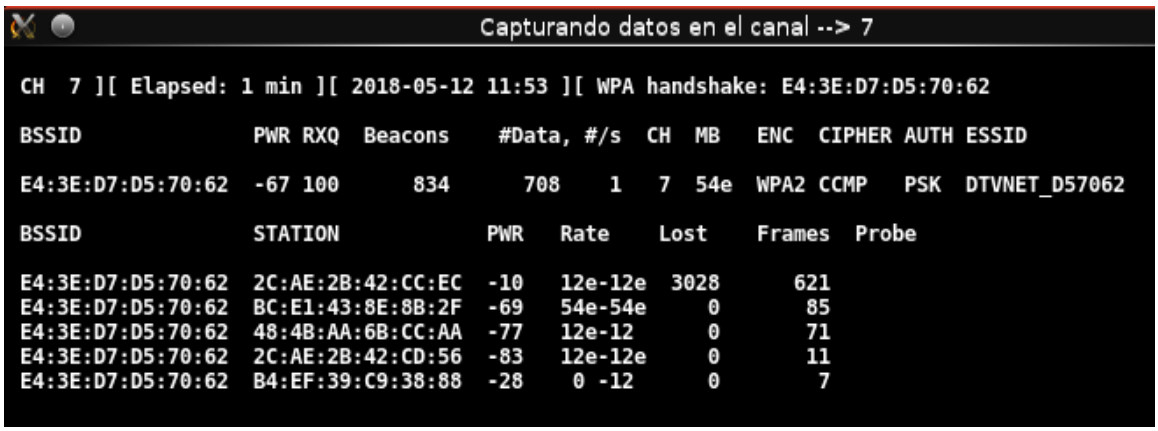
Enseguida se debe capturar el handshake para ello se le da a la opción 1, para que se realice una desautenticación masiva al punto de acceso objetivo.

Figura 30. Modo de captura

Fuente: El autor

Es ahora cuando se van a desautenticar los usuarios para poder capturar el handshake.

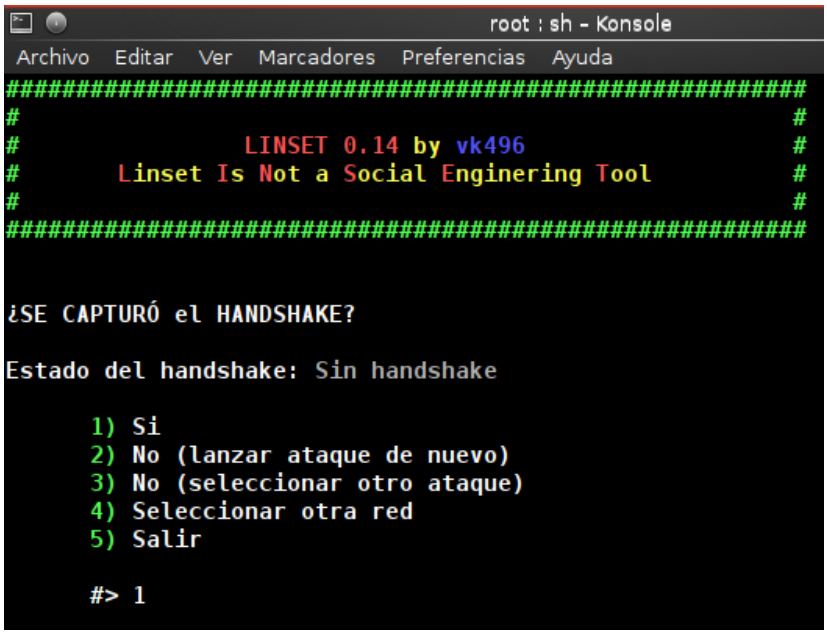
Figura 31. Captura del Handshake



Fuente: El autor

Cuando ya se tiene capturado el handshake se puede cerrar esta ventana y dar continuación al estado del handshake para ello se debe dar (opción 1).

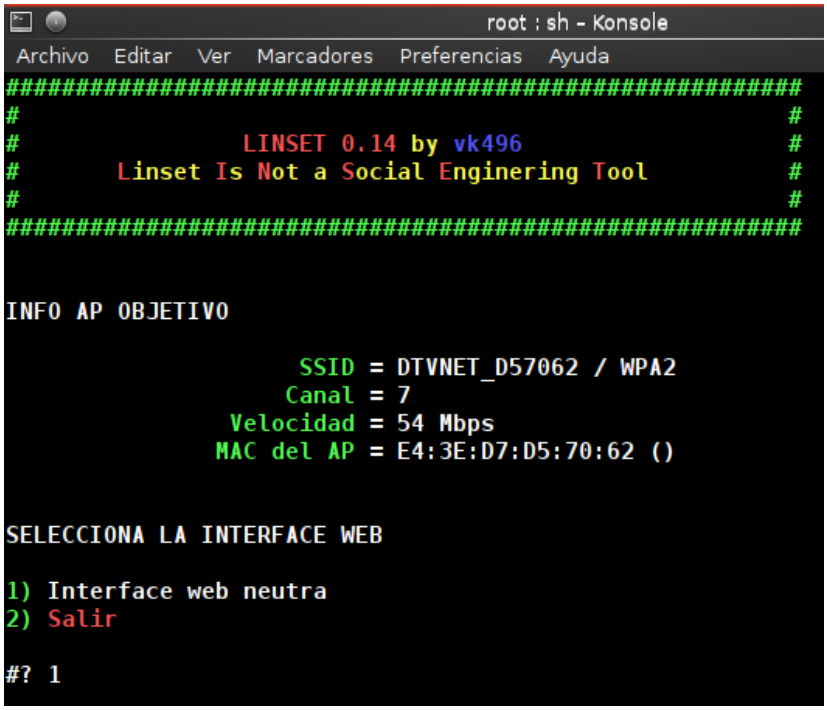
Figura 32. Captura del Handshake efectuada



Fuente: El autor

Ahora se selecciona el tipo de interfaz en este caso se selecciona interface web neutra.

Figura 33. Selección de interface Web



Fuente: El autor

Lo que sigue es seleccionar el idioma para la página falsa dentro de la red falsa.

Figura 34. Selección de idioma

Fuente: El autor

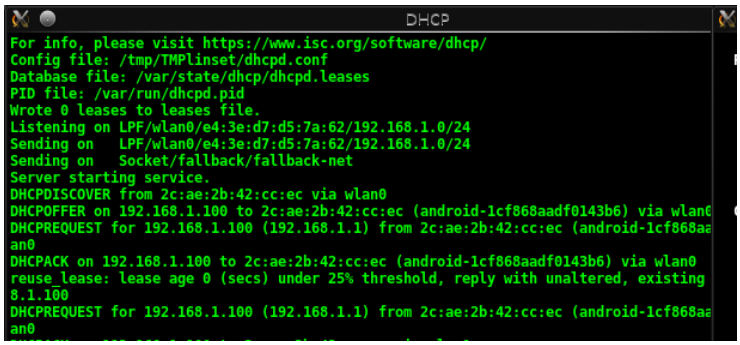
Si la captura se realizó de manera exitosa, comenzará a crear la red falsa, para ello la herramienta estará desautenticando con mdk3 a todos los usuarios de la red, esto permitirá que el usuario al estar desconectado va a tener que conectarse a la red clonada.

Figura 35. Desautenticando Usuarios legítimos

Fuente: El autor

Un servicio DHCP realiza el redireccionamiento de tráfico a la página de login falsa.

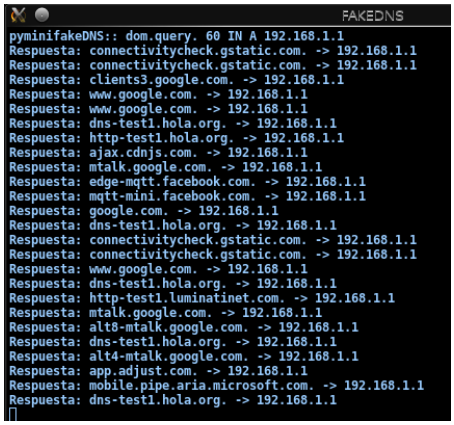
Figura 36. Desautenticando Usuarios legítimos



Fuente: El autor

Vista de respuesta de la redirección.

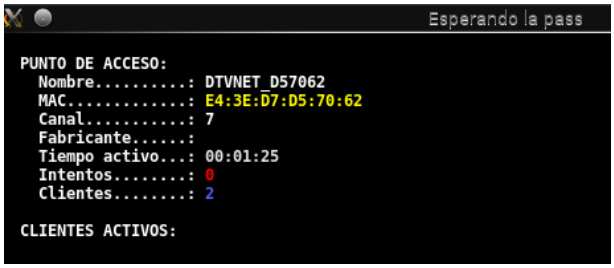
Figura 37. view of the redirection



Fuente: El autor

Panel de seguimiento y control, esperando que un usuario se conecte a la red falsa e introduzca la contraseña de red WPA

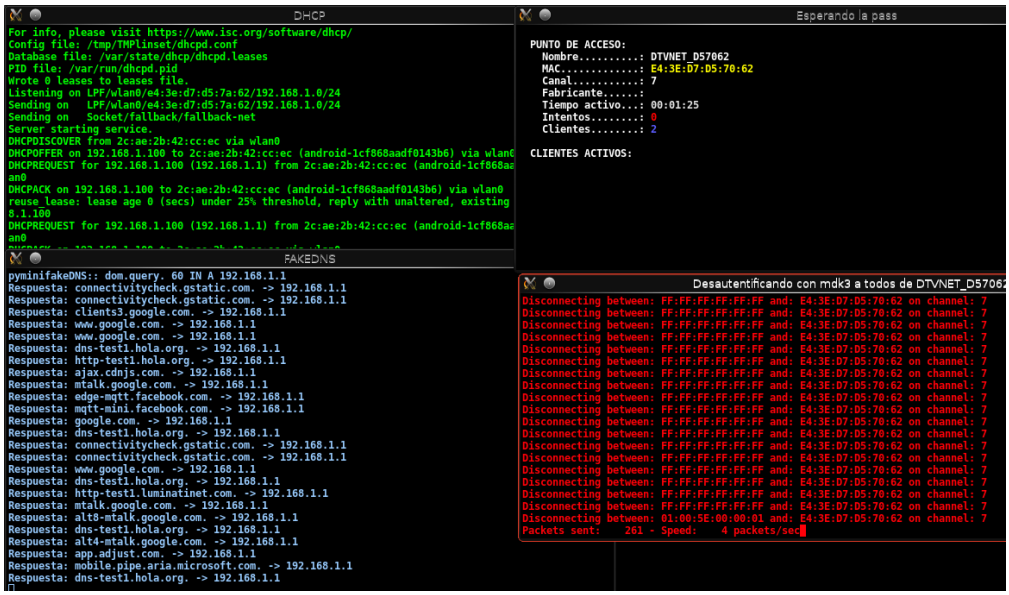
Figura 38. A la espera de la contraseña



Fuente: El autor

Ahora se tiene que esperar que los usuarios de dicha red se conecten a la red falsa e introduzcan la contraseña en la página falsa.

Figura 39. Vista general del ataque



Fuente: El autor

Esta página se les abrirá si se conectan a la red falsa, si introducen la contraseña en este apartado, automáticamente ya se tiene la contraseña.

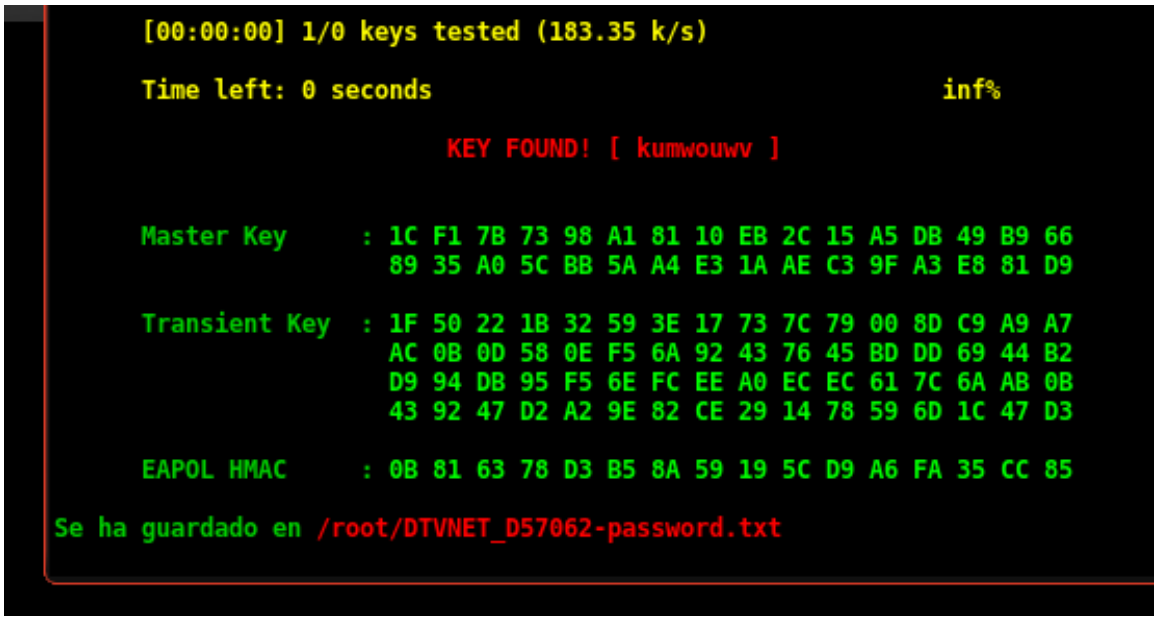
Figura 40. Página falsa

Fuente: El autor

4.8.2.3 Contraseña DTVNET capturada

Si algún usuario ingresa la contraseña al login falso, esta contraseña será convertida a hash y contrastada con la captura del Handshake, si estos coinciden se mostrará la contraseña.

Figura 41. Contraseña crackeada



Fuente: El autor

El archivo generado por la herramienta Linset contiene los detalles del ataque:

LINSET 0.14 by vk496

SSID: DTVNET_D57062

BSSID: E4:3E:D7:D5:70:62 ()

Channel: 7

Security: WPA2

Time: 00:07:04

Password: kumwouwv

FASE IV

En esta fase se encuentran una serie de soluciones que ayudarán a que las redes inalámbricas Wi-Fi sean lo más seguras posible.

4.6. SOLUCIONES A LOS PROBLEMAS DE SEGURIDAD DE LAS REDES INALÁMBRICAS.

4.6.1. Cambiar contraseñas impuestas.

- Muchas de las empresas asignan las contraseñas a su modo, y muchas de las veces tienen patrones específicos los cuales, son una gran debilidad porque pueden ser susceptibles a ataques de fuerza bruta, se recomienda que si se tiene una red con una contraseña por default del proveedor sea cambiada de manera inmediata.

4.6.2. Implementación de contraseñas fuertes.

- Este es de los menores controles disponibles para la seguridad de las redes, se recomienda lo siguiente:

  La longitud de las contraseñas debe ser mayor a 12 caracteres, entre más longitud tenga será mucho más difícil intentar un ataque de fuerza bruta.

  La generación de contraseñas debe hacer uso de todo tipo de caracteres, entre ellos usar alfabeto en mayúscula y minúscula, números, e incluso caracteres especiales (Ejemplo = s7Ds5U+Hd@-t).

  No colocar las mismas contraseñas para otros dispositivos, cuentas o redes sociales.

  Se recomienda cambiar las contraseñas dependiendo de la importancia de la información, el cambio puede ser cada mes.

  La contraseña no debe tener nombres de los usuarios o cualquier otra información que sea fácil de averiguar.

Evitar almacenar contraseñas en lugares no seguros.

No enviar las contraseñas por internet o por mensajes de cualquier tipo.

Borrar las contraseñas de los dispositivos cuando los necesitemos vender o prestar, hay muchos métodos para sacar las contraseñas de los dispositivos.

4.6.3. Configuración del cifrado de red (WPA2-PSK (AES)

- WPA2-PSK (AES): se podría afirmar que este protocolo de cifrado es el de mejor seguridad, este es el último estándar de cifrado Wi-Fi. Aun así, este protocolo aun es susceptible a ataques de fuerza bruta, por eso se recomienda que las contraseñas sean fuertes.

4.6.4. Doble autenticación

- Se puede realizar una implementación de doble autentificación para tener acceso a información en una red, La doble autentificación consiste en que aparte de conectarse a la red además se necesita pasar por un login el cual permitirá el acceso a la red sin limitaciones.

4.6.5. Ocultación de SSID

- Se puede configurar esta funcionalidad para que las redes no difundan el ssid, este control consiste en crear la red oculta, esto posibilita no mostrar el ssid, esto conlleva a que el que se quiera conectar a esa red tiene que digitar el ssid oculto más la contraseña.

4.6.6. Filtrado de direcciones Mac

- Este control consiste en solo autorizar el acceso a la red e información de la red a las direcciones Mac registradas.

4.6.7. Desactivación de la funcionalidad WPS

- La funcionalidad WPS fue creada inicialmente para que algunos dispositivos periféricos se pudieran conectar al router con tan solo oprimir el botón WPS, esta funcionalidad es aprovechada para enviar el pin identificador WPS y lograr emparejar los pines y de esa manera acceder a la red.

4.6.8. Selección del mejor canal.

- Este control consiste en dejar que el router escoja automáticamente el canal para que éste por medio de un scanner de red identifique cual es el mejor canal, el cual no tenga demasiadas interferencias.

4.6.9. Reducción del rango.

- En algunos router existe la posibilidad de regular la distancia que puede alcanzar la señal wi-fi, esto sería bueno ya que se puede hacer que la señal no salga de la casa o empresa.

4.6.10. Siempre tener activo un cortafuego (Firewall).

4.6.11. No dejar la red inalámbrica encendida cuando no se esté usando.

5. RESULTADOS

5.6. ENTREGA DE HALLAZGOS

Los resultados de las auditorías realizadas a los diferentes operadores de internet Wi-Fi en Aguazul Casanare fueron contundentes en cuanto al descubrimiento y la revelación de las fallas que tienen con respecto a la seguridad que brindan.

5.6.1. Resultados del pentest a redes Movistar. La empresa de servicios de comunicaciones Movistar se gana el premio a las redes más inseguras ya que casi con cualquier método se puede obtener las contraseñas de red.
Estas redes tienen muchos errores, el principal de ellos es el sistema de generación de contraseñas la cual es fácilmente deducible con herramientas criptográficas por lo que es susceptible a ataque de fuerza bruta haciendo uso de diccionarios personalizados

Otro de los grandes problemas de las redes Wi-Fi de Movistar es la mala configuración de los routers los cuales, algunos de ellos los dejan activado y por default el sistema Wps el cual es una funcionalidad, por la cual se puede llegar a obtener acceso a una red muy fácilmente.

El operador Movistar tiene una gran presencia en el municipio, casi todas las redes de internet Wi-fi le pertenecen, es lamentable que una empresa tan reconocida y con un muy buen servicio en cuanto a la velocidad y la estabilidad tenga estos errores tan inmensos en cuanto a la seguridad de sus redes.

Como resultado del pentest se tiene la obtención del acceso a la red por medio del crackeo de la contraseña por el método de Fuerza bruta.
5.6.2. Resultados del pentest a redes DTVNET. La Empresa Directv prestadores del servicio de internet DTVNET tiene una buena seguridad en cuanto a la configuración y generación de claves de seguridad para los sistemas de redes Wi-fi.
El sistema de generación de contraseñas de DTVNET por lo general es una cadena de números o más comúnmente 8 letras aleatorias, esto hace que hackear este tipo de contraseñas demore mucho tiempo y se requiere de mucho poder computacional para lograrlo, claro está que podría ser susceptibles a ataques de fuerza bruta si se tienen las herramientas necesarias para este nivel de seguridad.

La configuración de estos routers protege contra posibles ataques por el método wps, aun así el sistema wps esté activado.
Dejando como resultado que el único o más posible método para lograr dar con la contraseña de estas redes es por medio de phishing o ingeniería social. Como resultado del pentest se tiene la obtención de acceso a la red por medio del método Phishing usando la herramienta Linset disponible en Wifislax.

5.7. EMPRESAS PRESTADORAS DEL SERVICIO DE INTERNET FIJO RESIDENCIAL EN EL MUNICIPIO DE AGUAZUL

Estos datos son únicamente del municipio de Aguazul Casanare, no se tiene confirmación si en los demás departamentos se cuente con los mismos problemas de seguridad.

Las contraseñas que se muestran a continuación son las que cada empresa impone a las redes, pero el usuario tiene la total libertad de cambiar el nombre de red y la contraseña.

- MOVISTAR

Movistar es la empresa con mayor presencia en el municipio, su buena disponibilidad y velocidad a bajo costo han hecho que sea la más recomendada, Movistar es líder y tiene cobertura en todo el municipio.

- Deficiencias de seguridad de Movistar

  Movistar tiene un problema grave en cuanto a la generación de SSID y contraseña ya que por default establecen 12 números en el SSID y en la contraseña ejemplo;

Tabla 5. SSID y contraseñas de Movistar

SSID	PASSWORD
630683326888	209886832833
535583616855	141015635853
829783356811	150408321813

Fuente: El autor

Al tener únicamente números es susceptible a ataque de fuerza bruta

- UNE INALÁMBRICO

UNE distribuye módems MI-FI con buena velocidad de conexión, son portables y susceptibles a pérdidas de señal debido a inclemencias climáticas

- Deficiencias de seguridad de Une Inalámbrico

  Une tiene un grave problema con la generación de SSID y contraseña ya que por default todas las contraseñas inician con 4glte0c y seguido de letras y números intercalados ejemplo;

Tabla 6. SSID y contraseñas de Une

SSID	PASSWORD
UNE4GLTE323F	4glte0c323f
UNE4GLTE1041	4glte0c1041
UNE4GLTE0989	4glte0c0989
UNE4GLTE325f	4glte0c325f

Fuente: El autor

Al tener unas variables fijas como prefijos es posible generar un diccionario WPA, estas redes son susceptibles a ataques de fuerza bruta

- DIRECT TV INTERNET

A comienzos del año 2017 la empresa DIRECTV comenzó la distribución de internet inalámbrico en el municipio y obtuvo buena acogida gracias a que el modem es trasportable y tiene conectividad en cualquier lugar

- Deficiencias de seguridad de Direct Tv Internet;

  La empresa tiene una falla leve en el sistema de generación del SSID y la contraseña, las contraseñas son 8 letras minúsculas aleatorias ejemplo;

Tabla 7. SSID y contraseñas de DIRECTV Tv Internet

SSID	PASSWORD
DTVNET_D57062	kumwouwv
DTVNET_781A3C	brarbkxk
DTVNET_1A740E	mssrtmhm
DTVNET_C30ED7	cltbmzoy

Fuente: El autor

Las contraseñas que cuentan con letras dificultan la realización de ataques de fuerza bruta ya que es necesario un poder computacional muy alto para lograr descifrar

- AZTECA COMUNICACIONES

Es una empresa que tiene el apoyo del gobierno nacional y está en cerca de 753 municipios y está orientado en la expansión de la conexión de fibra óptica por todo el país, en Aguazul hay gran cantidad de usuarios de esta empresa, la mensualidad del este servicio es el más económico, pero a su vez es el internet más inestable.

- Deficiencias de seguridad de Azteca Comunicaciones

  Azteca comunicaciones tiene una grave falla de seguridad con respecto a la generación de contraseñas ya que todas comienzan por la palabra “total” y seguido de los últimos 4 números de la cedula del usuario ejemplo;

Tabla 8. SSID y contraseñas de Azteca Comunicaciones

SSID	PASSWORD
N-KAROL	total1615
N-N-FAMILIA RIAY	total2124
N-FAMILIA MOSQUERA	total1397
N-FAMILIA BELTRAN	total4839

Fuente: El autor

Este tipo de configuración es la más insegura ya que lo único que cambia de la contraseña son los últimos 4 números, un ataque de fuerza bruta podría descifrar una contraseña así entre 1 a 5 segundos

- INTERNET INALÁMBRICO TV CABLE YOPAL SAS

La empresa tiene cobertura en todo el departamento de Casanare además de tener precios asequibles dependiendo de la velocidad que se quiera tener, en el municipio de aguazul cuenta con muchos clientes.

- Deficiencias de seguridad de Internet Inalámbrico Tv Cable Yopal SAS

  La empresa casanareña cuenta con la mayor seguridad ya que en el momento de la instalación del servicio se le da la oportunidad al usuario de colocar el SSID y la Contraseña que desee, ejemplo;

  Tabla 9. SSID y contraseñas de Internet Inalámbrico Tv Cable Yopal SAS

SSID	PASSWORD
RAMON	483RAMON
Katheriine	tuymitodo04
BELENO HERNANDEZ	19680225VH
290317AS011114HB	44$rE201

  Fuente: El autor

Con este tipo de combinaciones sin ningún patrón en específico es casi imposible ejecutar un ataque de fuerza bruta ya que no se cuenta con ningún tipo de referente para crear diccionarios WPA.

6 DIVULGACIÓN

La divulgación de este proyecto y sus resultados se realizó a todas aquellas personas que fueron parte del trabajo investigativo, aquellas personas que prestaron sus redes Wi-Fi para efectuar las auditorias necesarias, se les presentó un breve resumen de lo que se evidenció en cada una de las etapas, además, se les dio a conocer las medidas de protección necesarias para impedir o mitigar posibles ataques.

Los autores de este estudio monográfico no se hacen responsables del mal uso que se le dé a la información sensible expuesta.

Las auditorías realizadas a las redes inalámbricas se hicieron con la debida autorización de los dueños de las redes, todas las pruebas y auditorias se realizaron con fines educativos, ninguna red auditada resultó afectada y se les advirtió a los respectivos dueños la falla encontrada.

El enfoque principal que se dio a los objetivos fue lograr conseguir con ayuda de herramientas avanzadas de auditoria las contraseñas de redes Wi-fi de los distintos operadores de internet del municipio, existen otras vulnerabilidades que se pueden explotar cuando ya se está dentro de la red, pero ese es un tema aparte.

Figura 42. Fotos de la divulgación a los dueños de las redes Wi-Fi auditadas.

Fuente: El autor

7 CONCLUSIONES

En el proceso de identificar los tipos de ataques se lograron identificar 5 tipos, unos más complicados que otros, pero con un grado de efectividad alto. Los métodos encontrados fueron probados con éxito.

Los equipos necesarios para realizar las auditorias estuvieron disponibles y se usaron para el desarrollo del proyecto dando resultados efectivos, los resultados fueron diversos y de ellos podemos resaltar que en general las redes inalámbricas Wi-Fi del municipio de Aguazul tienen innumerables problemas de seguridad. Se realizaron bastantes pruebas con los métodos expuestos en la Fase 1, las redes inalámbricas por cuestiones de su arquitectura en los protocolos de cifrado WPA2 generalmente son susceptibles a ataques de fuerza bruta, dicho protocolo ya quedo anticuado y es el supuestamente más seguro. Se está a la espera de la llegada y la implementación del nuevo sistema de cifrado WPA3 el cual podría solucionar dichos errores de seguridad.

Se evaluó la seguridad de las redes que instala el operador movistar y se detectó que es el de peor seguridad ya que cometen errores graves y comunes entre ellos, la generación de contraseñas con patrones preestablecidos, y demasiado predecibles, esto hace que sean susceptibles a ataques de fuerza bruta, el tiempo estimado para crackear estas redes es de 1 segundo a 24 horas dependiendo del poder del GPU o CPU.

Las auditorías realizadas a estas redes de movistar fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.
Caso similar ocurre con las redes inalámbricas de la compañía Azteca la cual provee internet por medio de fibra óptica, las contraseñas son preestablecidas en si sólo utilizan 1000 contraseñas por lo cual romper la seguridad de dichas redes es demasiado fácil, en general las contraseñas de estas redes consisten en las iniciales, total, más 4 números; ejemplo: total2375, el tiempo estimado para crackear esta red es de 1 segundo.
Las auditorías realizadas a estas redes de Azteca fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.

En cambio, la seguridad de las redes de la empresa de telecomunicaciones DIRECTV con sus redes DTVNET tienen un sistema de seguridad más robusto ya que sus contraseñas combinan 8 letras y números además de mayúsculas y minúsculas ejemplo kumwouwv, n32daA78, dichas combinaciones hacen que prácticamente sea inviable intentar un ataque de fuerza bruta, ya que dicho proceso demoraría mucho tiempo y sería necesario un poder computacional elevado, a pesar de que tienen buenas contraseñas aún son susceptibles a ataques de desautenticación, por lo cual se pueden duplicar las credenciales y lograr que la víctima se conecte a una red falsa con el mismo SSID, Este tipo de ataque se conoce como ¨phishing¨ Linset (Evil twin attack).

Las auditorías realizadas a estas redes de DIRECTV fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.
El método de clonación de red Wi-fi se puede ejecutar siempre y cuando existan clientes en las redes, este método es efectivo y se puede aplicar a todas las redes, los actuales sistemas de encriptación de wi-fi ya llevan con nosotros más de 13 años, ya se hace necesario que se realice o se implemente una actualización al sistema WPA2 ya que se le han comprobado brechas de seguridad que comprometen la integridad y disponibilidad de la información compartida en las redes Wi-fi.

En el transcurso del desarrollo del proyecto, se realizó un estudio que logró dar como resultado una serie de soluciones las cuales son de gran ayuda para disponer de redes inalámbricas seguras, si se aplican estas medidas de seguridad se podría garantizar con mayor eficiencia la seguridad en general ya que abarca la protección de la red inalámbrica y la seguridad de la información que circule y se comparta por medio de la red.

8 RECOMENDACIONES

Existen muchas recomendaciones que se pueden implementar para que las redes sean seguras y lograr mitigar errores de seguridad de los protocolos de red existentes (802.11i) a continuación se darán algunas recomendaciones las cuales serán de gran ayuda.

La señal de una red wi-fi es como un campo abierto y colocar una puerta de seguridad es muy complicado, ya que es posible saltar la puerta, hacer otra, o robar la llave, esta analogía aplica en las redes inalámbricas, ya que la señal de esta se dispersa homogéneamente, hay la posibilidad que intrusos logren acceder.
En la fase IV se expone una serie de soluciones que se pueden aplicar, esas soluciones son recomendaciones que al aplicarlas se podría blindar la seguridad de la red wi-fi, las recomendaciones generales ahora que las metodologías de hacking se han modernizado es conocer los métodos que existen de vulneración de redes para no caer en falsificación de credenciales o en ataques de fuerza bruta.
La manera más sencilla de evitar ser víctima de intrusos es tener un buen router el cual tenga buenas medidas de protección preferiblemente con un firewall incluido y con la posibilidad de solo dar acceso a la MAC registrados, aparte de eso es muy importante generar una contraseña con muchos caracteres diferentes incluyendo mayúsculas, minúsculas, números y símbolos.

Es recomendable cambiar las contraseñas cada cierto tiempo y estar revisando si la velocidad del internet es la misma que el proveedor promete, esto con el fin que no se tengan problemas de lentitud de conexión a internet.
Hay herramientas las cuales sirven para para revisar si existen intrusos en la red, para los dispositivos móviles hay una aplicación llamada (Fing), el cual es un analizador de red que permite visualizar todos los dispositivos conectados a la red, para los computadores está el software (Advanced IP Scanner), son herramientas sencillas pero que ayudan a salir de la duda si estamos siendo víctimas de intrusos.

9 BIBLIOGRAFÍA

ATAQUE DOS WIRELESS] DENEGACIÓN DE SERVICIO A UNA RED WI-FI Publicado por Zioner Heidegger el 6 mar. 2012 Esto se logra inundando con paquetes de deautenticación al punto de acceso [en línea] Disponible en: https://www.blackploit.com/2012/03/ataque-dos-wireless-denegacion-de.html

AIRCRACK-NG, Descripción, 2009/09/05 23:28 por mister_x [en línea] Disponible en: https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng

AMENAZAS DE CIBERCRIMEN EN COLOMBIA 2016-2017 CENTRO DE CIBERNÉTICO POLICIAL. Ministerio de defensa nacional policía nacional de Colombia [en línea] Documento pdf disponible para la descarga en: https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

AMENAZAS DE CIBERCRIMEN EN COLOMBIA 2016-2017 CENTRO DE CIBERNÉTICO POLICIAL. Ministerio de defensa nacional policía nacional de Colombia. Documento pdf[en línea] disponible para la descarga en: https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

ASOCIACIÓN DE PROVEEDORES DE RED, INTERNET Y TELECOMUNICACIONES "Seguridad Informática en Redes Inalámbricas" Francisco Caballero: Consultor Seguridad Telemática.S21sec. Ctra . Coruña Km. 23,200. Edificio ECU. 2ªPl. 28230. Las Rozas. Madrid. [en línea] Disponible en: http://www.aslan.es/boletin/boletin32/s21sec.shtml

ASPECTOS GENERALES DE LOS DELITOS INFORMÁTICOS Y EL COMBATE A LOS MISMOS
Autor: Pedro Torres-Ruiz [en línea] Disponible en: http://ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/TorresRuiz.pdf

CARACOL RADIO, Barranquilla 23/11/2016 Capturan a 13 policías por presunto Acceso Abusivo a Sistemas Informáticos [en línea] Disponible en http://caracol.com.co/emisora/2016/11/23/barranquilla/1479900086_849154.html

Coronel Fredy Bautista, director del Centro Cibernético de la Dijín, Delitos informáticos en el país [en línea] Disponible en:

http://www.eltiempo.com/archivo/documento/CMS-14841739

Dialogo revista militar digital (ciberdefensa y ciberseguridad) Coronel (r) Jairo Andrés Cáceres García, Docente Investigador Ciberguerra y Logística Militar, Escuela Superior de Guerra de Colombia | 22 septiembre 2016 [en línea] Disponible en: https://dialogo-americas.com/es/articles/cyberdefense-and-cybersecurity-colombia

EL PELIGRO DE LA INTERCEPTACIÓN WI-FI (DIRECTOR: JUAN JOSÉ GARRIDO) © Prensa Popular. Jr. Miro Quesada 247. Piso 6. Lima 1. [en línea] Disponible en: http://blogs.peru21.pe/atajosweb/2013/04/el-peligro-de-la-interceptacion-wi-fi.html

Guía de Seguridad en Redes Inalámbricas (eset) antivirus [en línea] Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_wifi.pdf

HECTOR RICARDO TRIANA ACEVEDO, 2015. TECNICAS BASICAS DE EXPLOTACIÓN DE VULNERABILIDADES ACTUALES EN LOS SISTEMAS DE PROTECCIÓN DE REDES WI-FI EN SOHO [en línea] Disponible en: http://repository.unad.edu.co:8080/bitstream/10596/3839/3/80374178.pdf

ICTP. Introducción a las redes WiFi. Materiales de entrenamiento para instructores de redes inalámbricas [en línea] Disponible en: http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf

Identificación de ataques y técnicas de intrusión. [en línea] Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap3.html

INGENIERÍA SOCIAL ¿Qué es?. OWAND'11 Granada Ingeniería social, David Montero Abujas OWASP Andalucia Chapter Leader Grupo iSoluciones (OWASP) hoja 8. Pdf [en línea] Disponible para la descarga en: http://osl.ugr.es/descargas/OWAND11/OWAND11%20Granada%20-%20Ingenier%C3%ADa%20social.pdf

Isidro Ros. Muycomputer. WiFi y protocolos de cifrado. 13 de noviembre, 2016. [en línea]. Disponible en: https://www.muycomputer.com/2016/11/13/wifi-cifrado-todo-saber/

José Manuel Luaces Novoa. Trabajo de Final de Carrera. Seguridad en redes inalámbricas de área local (WLAN) [en línea] Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

Ley 1273 del 5 de enero de 2009 Artículo 269A: Acceso abusivo a un sistema informático.

LOS RIESGOS RELACIONADOS CON LAS REDES INALÁMBRICAS (802.11 O WI-FI) Disponible en: http://es.ccm.net/contents/792-los-riesgos-relacionados-con-las-redes-inalambricas-802-11-o-wi

Madrid Molina, J. M. (2006). Seguridad en redes inalámbricas 802.11. Sistemas Y Telemática. http://bibliotecadigital.icesi.edu.co/biblioteca_digital/handle/10906/400

Manual básico de WIFISLAX y sus herramientas de Auditoria 31-07-2013, 20:19 sanson
Moderador Global [en línea] Disponible en: http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/

NORMA TÉCNICA COLOMBIANA - NTC 1486 Documentación, Presentación de tesis, trabajos de grado y otros trabajos de investigación. [en línea] Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

NORMA TÉCNICA COLOMBIANA - NTC 5613 (INCONTEC) referencias bibliográficas, contenido y forma de escritura [en línea] Disponible en: http://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

ORGANIZACIÓN DE ESTADOS AMERICANOS. REFERENCIA: C-063/16 (OEA) [en línea] Disponible en: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

PREVENCIÓN CONTRA INTRUSIÓN EN REDES INALÁMBRICAS (TELCOM) (6 agosto, 2014) El uso masivo de las redes WI-FI obliga a todos los responsables IT. [en línea] Disponible en: http://www.telcomsa.es/prevencion-contra-intrusion-en-la-redes-inalambricas/

Ramón J. Pérez - Los 10 delitos informáticos más frecuentes - 20 octubre, 2015 [en línea] Disponible en: https://pro.giztab.com/2015/10/20/los-10-delitos-informaticos-mas-frecuentes/

RIESGOS DE LAS REDES INALÁMBRICAS, Cuaderno de notas del OBSERVATORIO Instituto Nacional de Tecnologías de la Comunicación (INTECO) [en línea] Disponible en: http://www.egov.ufsc.br/portal/sites/default/files/riesgos_de_las_redes_inalambricas.pdf

Sanson - HERRAMIENTAS DE AUDITORIA WIRELESS - 15-04-2016 [en línea] Disponible en: http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/

SEGURIDAD Cómo protegerte de la vulnerabilidad KRACK en redes Wi-Fi Por Luis Del Barco 17/10/17 - 16:45 [en línea] Disponible en: https://hipertextual.com/2017/10/protegerte-vulnerabilidad-krack-redes-wi-fi

10 ANEXOS

RAE

Título de Documento.	FALLAS DE SEGURIDAD EN SISTEMAS DE COMUNICACIÓN INALÁMBRICAS
Autor	SANTIAGO DUQUE MARTINEZ YUDIMAN ROJAS MARTINEZ
Palabras Claves	Hacking, cracking, hash, Seguridad, integridad, disponibilidad, confidencialidad, Wi-Fi, software, Auditorias, redes.

CONTENIDO:

FALLAS DE SEGURIDAD EN SISTEMAS DE COMUNICACIÓN INALÁMBRICAS

DESCRIPCIÓN DEL PROBLEMA:

En el municipio de aguazul hay prestadores de internet como son Claro, Movistar, Tigo, Directv, Telefónica, Internet Inalámbrico, Azteca entre otros y debido a que las empresas prestadoras de internet Hogar Wi-Fi configuran mal los puntos de acceso y colocan contraseñas débiles o con patrones conocidos es muy fácil obtener acceso a esas redes.

El problema reside en la falta de seguridad debido a la mala configuración en los routers esto hace que queden fallas de seguridad con las cuales los atacantes puede tener acceso a la información importante y confidencial de los usuarios de dichas redes quienes confían ingenuamente de la seguridad de dicho sistema, la gravedad de esto es alta y solucionar estos problemas es de carácter urgente.

OBJETIVO GENERAL.

Realizar un estudio en el municipio de Aguazul-Casanare que permita evidenciar y dar a conocer las Fallas de seguridad en sistemas de comunicación inalámbricas

OBJETIVOS ESPECÍFICOS.

1. Dar a conocer las distintas maneras de explotar dichos errores de seguridad.
2. Realizar pruebas de intrusión en el municipio de Aguazul con herramientas de auditoria para evidenciar errores de seguridad en las redes Wi-Fi.

3. Documentar cada una de las acciones con el fin de tener pruebas concisas de dichos hallazgos.
4. Documentar las soluciones a los fallos de seguridad encontrados en las redes inalámbricas.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

El proyecto permitió evidenciar y dar a conocer fallas de seguridad en sistemas de comunicación inalámbricas en el municipio de Aguazul, haciendo uso de los diferentes métodos que existen para realizar pentesting a redes inalámbricas (Wi-Fi).

Se encontraron graves fallas de seguridad, la gran mayoría de redes Wi-Fi en el municipio de Aguazul son susceptibles a ataques sencillos, el problema más común encontrado es el sistema de generación de contraseñas que implementan las empresas prestadoras del servicio de internet, ese problema hace que las contraseñas sean fácilmente deducibles y por ende vulnerables a ataques de fuerza bruta.

METODOLOGÍA DE DESARROLLO

La seguridad de la información y de las redes inalámbricas son importantes para garantizar los pilares de la seguridad informática: confidencialidad, integridad y disponibilidad.

El presente documento evidencia y da a conocer las Fallas de seguridad en sistemas de comunicación inalámbricas en el municipio de Aguazul, se realizó una serie de auditorías a las redes con el fin de cumplir a cabalidad con los objetivos del proyecto.

En el presente se encuentran las conclusiones al detalle del proceso realizado incluyendo, métodos de auditorías, tipos de vulnerabilidades y la documentación paso a paso del proceso de pentesting realizado a las diferentes redes en el municipio.

Se tomó como muestra una o más redes de cada operador del total de los distintos operadores de internet del municipio de Aguazul Casanare, se realizaron las respectivas pruebas de todas las maneras posibles para lograr evidenciar los problemas que tienen esas redes.

Las empresas proveedoras de internet en el municipio de Aguazul no configuran adecuadamente los routers y asignan contraseñas, las cuales son fácilmente predecibles o default esto hace que dichas redes estén susceptibles a distintos ataques que pueden ver comprometida la seguridad del sistema.

La seguridad en las redes inalámbricas son un factor a tener en cuenta para cualquier persona u organización y conocer las técnicas de auditoria de redes, se hace indispensable para saber cómo defenderse ante dichos ataques, actualmente en el municipio de Aguazul se han visto muchos problemas con respecto a la seguridad de las redes ya que hay muchas personas que ya saben del tema y logran acceder a las redes inalámbricas haciendo uso de herramientas avanzadas de auditoria de redes, es un problema muy grave que se tiene que evidenciar ya que esto no puede pasar por alto.

Conclusiones

En el proceso de identificar los tipos de ataques se lograron identificar 5 tipos, unos más complicados que otros, pero con un grado de efectividad alto. Los métodos encontrados fueron probados con éxito.

Los equipos necesarios para realizar las auditorias estuvieron disponibles y se usaron para el desarrollo del proyecto dando resultados efectivos, los resultados fueron diversos y de ellos podemos resaltar que en general las redes inalámbricas Wi-Fi del municipio de Aguazul tienen innumerables problemas de seguridad. Se realizaron bastantes pruebas con los métodos expuestos en la Fase 1, las redes inalámbricas por cuestiones de su arquitectura en los protocolos de cifrado WPA2 generalmente son susceptibles a ataques de fuerza bruta, dicho protocolo ya quedo anticuado y es el supuestamente más seguro, Se está a la espera de la llegada y la implementación del nuevo sistema de cifrado WPA3 el cual podría solucionar dichos errores de seguridad.

Se evaluó la seguridad de las redes que instala el operador movistar y se detectó que es el de peor seguridad ya que cometen errores graves y comunes entre ellos; la generación de contraseñas con patrones preestablecidos y demasiado predecibles, esto hace que sean susceptibles a ataques de fuerza bruta, el tiempo estimado para crackear estas redes es de 1 segundo a 24 horas dependiendo del poder del GPU o CPU.

Las auditorías realizadas a estas redes de movistar fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.

Caso similar ocurre con las redes inalámbricas de la compañía Azteca la cual provee internet por medio de fibra óptica, las contraseñas son preestablecidas, en sí, sólo utilizan 1000 contraseñas por lo cual romper la seguridad de dichas redes es

demasiado fácil, en general las contraseñas de estas redes consisten en las iniciales, total más 4 números, ejemplo: total2375, el tiempo estimado para crackear esta red es de 1 segundo.

Las auditorías realizadas a estas redes de Azteca fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.

En cambio, la seguridad de las redes de la empresa de telecomunicaciones DIRECTV con sus redes DTVNET tienen un sistema de seguridad más robusto ya que sus contraseñas combinan 8 letras y números además de mayúsculas y minúsculas; ejemplo kumwouwv, n32daA78, dichas combinaciones hacen que prácticamente sea inviable intentar un ataque de fuerza bruta, ya que dicho proceso demoraría mucho tiempo y sería necesario un poder computacional elevado, a pesar de que tienen buenas contraseñas aún son susceptibles a ataques de desautenticación, por lo cual se pueden duplicar las credenciales y lograr que la víctima se conecte a una red falsa con el mismo SSID este tipo de ataque se conoce como ¨phishing¨ Linset (Evil twin attack).

Las auditorías realizadas a estas redes de DIRECTV fueron efectivas y se logró comprobar que son vulnerables como se expone en la fase III.

El método de clonación de red Wifi se puede ejecutar siempre y cuando existan clientes en las redes, este método es efectivo y se puede aplicar a todas las redes, los actuales sistemas de encriptación de wifi ya llevan con nosotros más de 13 años, ya se hace necesario que se realice o se implemente una actualización al sistema WPA2 ya que se le han comprobado brechas de seguridad que comprometen la integridad y disponibilidad de la información compartida en las redes Wifi.

En el transcurso del desarrollo del proyecto se realizó un estudio que logró dar como resultado una serie de soluciones, las cuales son de gran ayuda para disponer de redes inalámbricas seguras, si se aplican estas medidas de seguridad se podría garantizar con mayor eficiencia la seguridad en general, ya que abarca la protección de la red inalámbrica y la seguridad de la información que circule y se comparta por medio de la red.

Recomendaciones.

Existen muchas recomendaciones que se pueden implementar para que las redes sean seguras y lograr mitigar errores de seguridad de los protocolos de red existentes (802.11i), a continuación se darán algunas, las cuales serán de gran ayuda.

La señal de una red wifi es como un campo abierto y colocar una puerta de seguridad es muy complicado ya que es posible saltar la puerta, hacer otra o robar

la llave, esta analogía aplica en las redes inalámbricas, ya que la señal de estas se dispersa homogéneamente, existe la posibilidad que intrusos logren acceder.

En la fase IV se expone una serie de soluciones que se pueden aplicar, estas soluciones son recomendaciones que al aplicarlas se podría blindar la seguridad de la red wifi, las recomendaciones generales ahora que las metodologías de hacking se han modernizado, se deben conocer los diferentes métodos que existen de vulneración de redes para no caer en falsificación de credenciales o en ataques de fuerza bruta.

La manera más sencilla de evitar ser víctima de intrusos es tener un buen router, el cual tenga buenas medidas de protección, preferiblemente con un firewall incluido y con la posibilidad de solo dar acceso a la MAC registrados, aparte de eso es muy importante generar una contraseña con muchos caracteres diferentes incluyendo mayúsculas, minúsculas, números y símbolos.

Es recomendable cambiar las contraseñas cada cierto tiempo y estar revisando si la velocidad del internet es la misma que el proveedor promete, esto con el fin que no se tengan problemas de lentitud de conexión a internet.

Hay herramientas las cuales sirven para para revisar si existen intrusos en la red para los dispositivos móviles hay una aplicación llamada (Fing) el cual es un analizador de red que permite visualizar todos los dispositivos conectados a la red, para los computadores está el software (Advanced IP Scanner), son herramientas sencillas pero que ayudan a salir de la duda si estamos siendo víctimas de intrusos.