TECNICAS BASICAS DE EXPLOTACIÓN DE VULNERABILIDADES ACTUALES EN LOS SISTEMAS DE PROTECCIÓN DE REDES WI-FI EN SOHO

HECTOR RICARDO TRIANA ACEVEDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
ORTEGA
2015

TECNICAS BASICAS DE EXPLOTACIÓN DE VULNERABILIDADES ACTUALES EN LOS SISTEMAS DE PROTECCIÓN DE REDES WI-FI EN SOHO

HECTOR RICARDO TRIANA ACEVEDO

Proyecto de grado para optar por el título de Especialista en Seguridad Informática

Ingeniero
JOHN FREDDY QUINTERO TAMAYO
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
ORTEGA
2015

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y A Distancia, UNAD, para optar al título de Especialista en Seguridad Informática.

_____

Firma del Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Bogotá, _____

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACCESO: con respecto a la privacidad, es la habilidad de un individuo para ver, modificar y refutar lo completa y precisa que pueda ser la información personal identificable reunida sobre él o ella.

AES – ESTÁNDAR DE CIFRADO AVANZADO: también conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit.

AMENAZA: situación o evento con que puede provocar daños en un sistema.

ATAQUE DE NEGACIÓN DE SERVICIO (DOS, POR SUS SIGLAS EN INGLÉS): ataque a una red diseñada para deshabilitarla mediante congestionamientos inútiles de tráfico.

ATAQUE ACTIVO: ataque al sistema para insertar información falsa o corromper la ya existente.

ATAQUE DE FUERZA BRUTA: método para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras. Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

AUTENTICACIÓN: es el proceso de verificar que alguien o algo es quien o lo que dice ser.

AUTORIZACIÓN: con referencia a la computación, especialmente en los equipos remotos en una red, es el derecho otorgado a un individuo o proceso para utilizar el sistema y la información almacenada en éste.

CONFIDENCIALIDAD: calidad de secreto, que no puede ser relevado a terceros o personas no autorizadas.

ESTÁNDAR: norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc…

HOMBRE EN MEDIO, MAN IN THE MIDDLE: ataque mediante el cual el intruso se coloca entre las partes comunicantes e intercepta todo el tráfico que fluye entre estos.

IEEE – INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS: formada a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo.

PROBABILIDAD: probabilidad (likelihood) – Posibilidad de que un hecho se produzca. (UNE-ISO Guía 73,2010) NOTA 1 – En la terminología de la gestión del riesgo, la palabra "probabilidad" se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática (tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado).

PUNTO DE ACCESO (AP): dispositivo inalámbrico central de una WLAN que mediante un sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

SEGURIDAD: es la disciplina, técnicas y herramientas diseñadas para ayudar a proteger la confidencialidad, integridad y disponibilidad de información y sistemas.

SEGURIDAD DE LA INFORMACIÓN: confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. (UNE 71504,2008).

SISTEMA DE INFORMACIÓN: conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información.

SOHO (CONTRACCIÓN DE SMALL OFFICE — HOME OFFICE): hace referencia a entornos domésticos o de pequeña empresa con instalaciones y equipos informáticos de escasa potencia.

SSID: identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

REAVER: técnica utilizada para atacar el protocolo WPS, a través de construcciones de PIN enviados al router.

RIESGO: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización.

TKIP – PROTOCOLO DE INTEGRIDAD DE CLAVE TEMPORAL: cifra las llaves utilizando un algoritmo Hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS – TRANSPORT LAYER SECURITY: protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet.

VULNERABILIDAD: estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas, frecuencia de ocurrencia y degradación causada. (Magerit, 2006).

WI-FI. ABREVIATURA DE WIRELESS FIDELITY: es el nombre comercial con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WLAN – RED DE ÁREA LOCAL INALÁMBRICA: también conocida como red Wireless. Permite a los usuarios comunicarse con una red local o a Internet si estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o teléfono.

RESUMEN

En el presente trabajo se realiza una reseña de la forma en como son implementadas los sistemas de protección de las redes inalámbricas en pequeñas oficinas siguiendo el standard 802.11 en la actualidad, por lo cual se centra en los cifrados WEP, WPA y WPA2, además se describe el estándar WPS, que aunque no es un sistema de seguridad WLAN, representa un tema importante para la finalidad de este trabajo de grado.

El capítulo III es la parte práctica del trabajo en la cual se demuestra diferentes métodos por los cuales se vulneran los sistemas de protección inalámbricos antes mencionados, utilizando herramientas contenidas en la distribución de Wifislax, demostrando que después de varios años de haber sido puestos en funcionamiento aún siguen presentando debilidades que ponen en riesgo la seguridad de la información que en esencia deberían proteger.

Por último, se efectúa un análisis de los datos los cuales conllevan a proporcionar las conclusiones del trabajo realizado y se coligen ciertas recomendaciones que permitan minimizar los riesgos de que personas no autorizadas ingresen a la red WIFI.

PALABRAS CLAVES: Seguridad Informática. Seguridad Wireless. Seguridad WIFI. Vulnerando Redes WIFI. Usando WfiSlax. Ley WIFI Colombia.

CAPITULO I

1. INTRODUCCIÓN

Las redes inalámbricas que se rigen por estándar 802.11 actualmente son el medio de comunicación más utilizado dentro de la infraestructura LAN, debido a que utilizan ondas de radio, las cuales permiten una movilidad en un espectro más amplio, incluso a través de edificaciones, pero esa misma virtud las hace vulnerables a ataques por parte de personas que con conocimientos básicos y el software apropiado podrían ingresar de forma no autorizada a los servicios y datos que por ella circulan.

La facilidad de acceso a las redes WI-FI varía dependiendo del sistema de protección implementado en el sistema, en el presente los más utilizados son WPA, WPA2, WI-FI Protected Access, Acceso protegido WI-FI y en menor proporción WEP, Wired Equivalent Privacy, Privacidad Equivalente a cableado. Por otra parte, existe el estándar WPS, WI-FI Protected Setup, que en si no es un sistema de seguridad, sino se implementa para facilitar la configuración de la red, no obstante es una puerta de entrada para los atacantes.

Este trabajo pretende ejemplarizar diferentes métodos utilizados para la obtención de la contraseña de las redes WI-FI en la actualidad y que pueden ser utilizados por cualquier atacante para acceder ilegítimamente a la red, colocando en peligro la Integridad, la Disponibilidad y la Confiabilidad de la información del sistema vulnerado.

Igualmente, se expone, brevemente, la normatividad existente respecto a la responsabilidad penal que podría enfrentar las personas que accedan a una red sin autorización de su propietario, según la legislación colombiana.

2. PLANTEAMIENTO DEL PROBLEMA

Actualmente los Proveedores de Servicio de Internet, ISP (Internet Service Provider), suministran este servicio a los usuarios, configurando los routers con características básicas y genéricas que pueden ser deducidas por los atacantes, o bien, no deshabilitan servicios que pueden poner en riesgo la seguridad de la red.

Por otra parte los sistemas de cifrado que permiten configurar los dispositivos routers, son WEP y WPA, en sus diferentes denominaciones, los cuales han demostrado tener debilidades al momento de asegurar que la transmisión de la información donde están implementados sea obtenida y entendida por un intruso.

La presente investigación se circunscribe a demostrar con ejemplos algunos de los métodos y herramientas vigentes que pueden utilizar personas con un nivel Intermedio de conocimientos en el área de Informática y que con solo conocer el nombre de la red, ESSID (test de caja negra), que se encuentran a su alrededor, proceden a vulnerar los sistemas de protección, basados en WEP, WPA PSK, WPA2 PSK con o sin WPS obteniendo acceso a internet sin costo, inclusive y con un poco más de esfuerzo, obtendrían datos que circulan por ella (carpetas compartidas, contraseñas, etc.) y solamente usando un computador , una tarjeta inalámbrica en modo monitor, un software libre y un poco de paciencia.

Para esta labor se hace uso de la distribución de GNU-Linux, WiFiSlax, que posee las herramientas necesarias para realizar labor, tales como aircrack-ng, crunch, LINSET, entre otras , algunas con interfaces Gráficas y otras en consola pero siempre explicando el proceso que se realiza.

3. OBJETIVOS

3.1 GENERAL

- 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.

3.2 ESPECÍFICOS

- Especificar la forma como funcionan los principales métodos de protección en las redes WI-FI mediante una revisión bibliográfica.

- Ejemplarizar técnicas básicas para obtener acceso no autorizado en redes inalámbricas locales con cifrado WEP y WPA.

- Definir el funcionamiento del estándar WPS y sus debilidades frente a la configuración en el cifrado WPA2.

- Describir las vulnerabilidades existentes en las redes WI-FI mediante pruebas de rompimiento de claves en este tipo de redes, con diferentes métodos de ataque.

4. JUSTIFICACIÓN

La seguridad en la redes informáticas es un aspecto vital para minimizar los riegos de que los datos y servicios que por ella circulan no sean accedidos por individuos que no son sus reales destinatarios, pero la mayoría de los personas que hacen uso de estas redes desconocen, o bien, no otorgan la importancia que deberían al respecto, exponiéndose a que su información sea alterada, conocida, o como mínimo su servicio de internet degradado.

Este trabajo pretende concienciar al público en general de la facilidad en que las redes inalámbricas WI-FI, que no han sido correctamente configuradas, pueden ser vulneradas, permitiendo el acceso a su red privada y como primer escalón, entrada a internet, que es lo que se pretende demostrar, pero eventualmente podría permitir que sujetos inescrupulosos, violen su intimidad, exponiéndose a ser víctimas de estafa, extorsión, secuestro “bullying” entre otras conductas, y en general violación del habeas data, de una forma mucho más fácil, por cuanto cualquier otro escalamiento se hace desde adentro al estar en la misma red local.

La mayoría de las prácticas descritas y recopiladas dentro de la investigación, pueden ser realizadas por los lectores para determinar la seguridad de sus propias redes, sin que sea la intención del autor, que sean ejecutadas en contra de redes ajenas sin el permiso de sus propietarios, por cuanto este comportamiento es condenado moral y penalmente por la legislación colombiana.

Igualmente, con la ejecución de esta tesis, el investigador ampliara sus conocimientos en una de las áreas más importantes de la profesión que, por vocación, ha decido ejercer como es la Seguridad Informática en las redes Inalámbricas WI-FI.

CAPITULO II

5. FUNDAMENTACIÓN TEÓRICA

Al realizar una búsqueda de tesis anteriores que tengan una relación directa con el objeto de investigación de este trabajo, se encuentra que hay variada información al respecto, pero algunas se limitan a la parte técnica del problema, sin llegar a demostrar como explotan los fallos en los sistemas de protección.

Otras tesis halladas no abarcan, tal vez, por cuanto en el momento de su presentación no se hayan hecho públicas., las nuevas técnicas que se utilizan para vulnerar la seguridad de las redes WI-FI, o bien, porque no es el área específica de su Carrera. Las tesis que se tienen como antecedentes son las siguientes:

- Seguridad Al Acceso De Información En La Implantación De Una Red Inalámbrica, propiedad intelectual de Yelitza Pastora Álvarez Méndez, por el cual se le confiere el título de Especialista en Comunicaciones y Redes de Comunicación de Datos de la Universidad Central de Venezuela, en la ciudad Caracas, de la República Bolivariana de Venezuela en Noviembre de 2006.

- Vulnerabilidades Y Niveles De Seguridad De Redes WI-FI, propiedad intelectual de Tatiana Violeta Vallejo de León, por el cual se le confiere el título de Ingeniera en Electrónica de la Universidad de San Carlos de Guatemala, en la ciudad Guatemala, de la República de Guatemala en agosto de 2010.

- Análisis de Vulnerabilidades de Seguridades en Redes Inalámbricas dentro un entorno empresarial que utilizan cifrado AES y TKIP, WPA y WPA2 Personal del DMQ, propiedad intelectual de Andrés Guillermo Serrano Flores, por el cual se le confiere el título de Ingeniero de Sistemas de la Pontificia Universidad Católica del Ecuador, en la ciudad Quito, de la República de Ecuador en 2011.

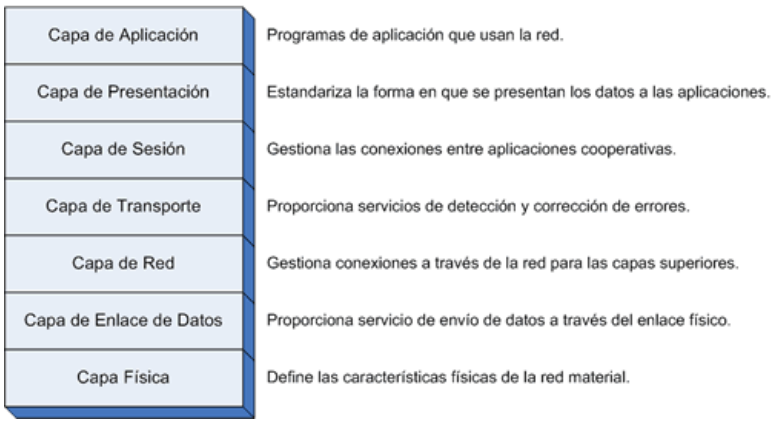
6. MARCO TEÓRICO

6.1 MODELO OSI

La Organización Internacional de Estandarización, ISO, en el año 1977, crea un comité con el objeto de que se formule un modelo para la comunicación de redes que permita que los hosts (computadores, mainframe, PDA, etc.) Fabricados por distintas Compañías y con tecnologías diferentes, pudieran interoperar entre sí, con base a este requerimiento nace la norma ISO 7498 de 1980, más conocido con el nombre de Modelo de Interconexión de Sistemas Abiertos, OSI.

Este modelo de referencia divide en siete capas la comunicación en las redes, descrita mediante la siguiente Figura:

Figura 1. Diagrama Modelo OSI



Fuente: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

Los dos primeros niveles de este Modelo Descriptivo, o sea, la capa física y la de enlace de datos, son en los cuales se enfoca el estándar IEEE 802.11 para las conexiones inalámbricas, y para el caso de las redes alámbricas el estándar IEEE 802.3 (Ethernet)[1].

[1] TANENBAUM, Andrews s. Pearson Prentice Hill: Redes de Computadoras, Cuarta Edición. México, 2003 ps. 37-48.

El Standard IEEE 802.11 contempla diferentes protocolos que regulan la actividad de una Red de Área Local Inalámbrica, WLAN. En el desarrollo del presente trabajo investigativo se reseñan los estándares individuales, que son usualmente aceptados en el ámbito internacional, en la actualidad, y más conocidos con el nombre comercial de WI-FI [2].

6.2 ESTÁNDAR 802.11

Según el diseño requerido se tienen distintas tecnologías aplicables:

Banda estrecha: se comunica en una banda definida de frecuencia lo más reducida para el paso de datos, por ende, Los hosts tienen diferentes frecuencias de canal de modo que se impiden las interferencias. Igualmente, un filtro en el destino de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

Banda ancha: utilizado en la mayoría de los casos en la comunicación inalámbrica. Fue ideado por ejército para una transferencia de datos fiable y con un grado de confidencialidad alto. Se utiliza más ancho de banda pero la señal es descubierta más rápidamente. Existen dos tipos de técnicas usadas en banda ancha:

Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): emplea una portadora de banda estrecha que alterna la frecuencia a un patrón conocido por transmisor y receptor que al sincronizarse es como tener un único canal lógico pero al no estar sincronizado el destinatario escucha un ruido de impulsos de corta duración.

Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se crea un bit redundante por cada bit transmitido, a estos bits se les denomina "chipping code". Cuanto mayor sea esta continuidad mayor es la posibilidad de rehacer los datos originales, también se requiere mayor ancho de banda.

Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado[3].

---

[2] CORLETTI ESTRADA, Alejandro. www.darFE.es: Seguridad Por Niveles. Madrid, 2011 ps. 89-104

[3] ANDREU, Fernando, PELLEJERO, Izaskun, LESTA, Amaia. Marcombo: Redes WLAN. Fundamentos y Aplicaciones de Seguridad, Barcelona 2006 ps. 20-22

En general, las redes inalámbricas se diferencian de las redes Ethernet en la Capa Física y en la Capa de Enlace de Datos, según el modelo OSI. Vale la pena anotar que la capa física se encarga de ilustrar cómo se envían los bits de una estación a otra, mientras que la capa de Enlace de Datos, describe el empaquetado y verificación de los bits de modo que no tengan errores. Las dos Técnicas utilizadas en la capa física de una Wireless para la transmisión de bits son la Radio Frecuencia y la Luz Infrarroja.

La transmisión por radiofrecuencia permite atravesar objetos y es usada para cubrir grandes áreas, pero algunas de estas frecuencias son restringidas por cuanto son utilizadas por otros sistemas, tales como radio aficionado, celulares, sistemas de radar, entre otras.

Por otro lado la transmisión por radiofrecuencia, puede presentar problemas como interferencia, debido a la dispersión y el cruce con otras comunicaciones, y por supuesta la poca seguridad debido a la falta de barreras para su propagación.

En la transmisión de luz infrarroja están limitadas por el espacio y casi generalmente las estaciones transmisoras se encuentran en un mismo piso, o se si se desea trasmitir a varios niveles deben instalarse los emisores-receptores en línea de vista, por lo general en las ventanas de los edificios.

6.2.1 Estándar 802.11b

El estándar 802.11b transferir datos, en teoría, con tasas de datos en bruto de hasta 11 Mbps, y tiene una buena gama, aunque no cuando funciona a su velocidad de datos completa.

Al transmitir datos 802.11b utiliza la técnica CSMA / CA que se definió en el estándar 802.11 base original y retuvo para 802.11b. Usando esta técnica, cuando un nodo quiere hacer una transmisión de escucha para un canal claro y luego transmite. A continuación, a la escucha de un reconocimiento y si no recibe uno que retrocede una cantidad aleatoria de tiempo, asumiendo otra transmisión causó interferencia, y luego escucha un canal claro y luego retransmite los datos.

El formato de la señal de RF utilizado para 802.11b es CCK o Código complementario Keying. Esta es una ligera variación en la tecnología CDMA (Code Division Multiple Access) que utiliza el DSSS básica (Direct Sequence Spread Spectrum) como su base.

En vista del hecho de que el uso 802.11 especificación original CDMA / DSSS, era fácil de actualizar cualquier chipset existente y otra inversión para proporcionar el nuevo estándar 802.11b. Como resultado conjuntos de chips 802.11b aparecieron de forma relativamente rápida en el mercado.

Aunque las tarjetas 802.11b están especificados para funcionar a una tasa básica de 11 Mbps, el sistema controla la calidad de la señal. Si la señal cae o se elevan los niveles de interferencia, entonces es posible que el sistema para adoptar una velocidad de datos más lento con más de corrección de error que es más resistente. Bajo estas condiciones, el sistema caerá hacia atrás a una velocidad de 5,5 Mbps, luego 2, y finalmente 1 Mbps. Este esquema se conoce como tasa de atenuación del canal (ARS).

Aunque las tasas de datos primas básicas para la transmisión de datos parecen muy bueno, en realidad las velocidades de datos reales obtenidos en una red en tiempo real son mucho más pequeños. Incluso bajo condiciones razonablemente buenas de radio, es decir, una buena señal y baja interferencia de la velocidad máxima de datos que se puede esperar cuando el sistema utiliza TCP es alrededor de 5,9 Mbps.

Esto resulta de una serie de factores, uno de ellos es el uso de CSMA / CA, donde el sistema tiene que esperar a veces claras en un canal para transmitir y otro está asociado con el uso de TCP y la sobrecarga adicional requerida. Si se utiliza UDP en lugar de TCP entonces la velocidad de datos puede aumentar a alrededor de 7,1 Mbps.

6.2.2 Estándar 802.11g

El estándar 802.11g ofrece una serie de mejoras con respecto a la norma 802.11b que fue su predecesor. Los aspectos más destacados de su rendimiento se dan en la siguiente tabla.

Como 802.11b, su predecesor, 802.11g opera en la banda ISM de 2,4 GHz. Proporciona un rendimiento máximo de datos en bruto de 54 Mbps, aunque esto se traduce en un verdadero rendimiento máximo de poco más de 24 Mbps.

Aunque el sistema es compatible con 802.11b, la presencia de un participante en una red 802.11b reduce significativamente la velocidad de una red. De hecho, fue

los problemas de compatibilidad que ocupaban gran parte del tiempo de trabajo del comité IEEE 802.11g.

A fin de proporcionar resistencia contra los efectos de trayectorias múltiples al mismo tiempo ser capaz de llevar a las altas velocidades de datos, el método de modulación principal elegido para 802.11g era la de OFDM - orthogonal multiplex por división de frecuencia, aunque otros esquemas se utilizan para mantener la compatibilidad, etc.

Además de la utilización de OFDM, DSSS - también se utiliza espectro ensanchado de secuencia directa.

Para proporcionar la máxima capacidad mientras mantiene la compatibilidad con versiones anteriores, se utilizan cuatro capas físicas diferentes - tres de los cuales se definen como exámenes físicos Puntúa Extended, ERPs Estos coexisten durante el intercambio de marco para que el emisor puede utilizar cualquiera de los cuatro, siempre que éstos sean apoyada en cada extremo del enlace.

Las cuatro opciones de capa definidos en la especificación 802.11g son:

- ***ERP-DSSS-CCK:*** Esta capa es la utilizada con 11b. Espectro ensanchado de secuencia directa se utiliza junto con CCK - código de claves complementarias. El rendimiento es el de los sistemas 802.11b anteriores.

- ***ERP-OFDM:*** Esta capa física es uno nuevo introducido por 802.11g donde se utiliza OFDM para permitir la prestación de las velocidades de datos a 2,4 GHz que se logra mediante 11a a 5,8 GHz[4].

- ***ERP-DSSS / PBCC:*** Esta capa física se introdujo para su uso con 802.11by proporcionada inicialmente las mismas velocidades de datos como la capa DSS / CCK, pero con 802.11g, las velocidades de datos se han ampliado para proporcionar 22 y 33 Mbps. Como se indica por el título, que utiliza la tecnología DSSS para la modulación combinada con la codificación PBCC para los datos.

- ***DSSS-OFDM:*** Esta capa es nuevo para 11g y utiliza una combinación de DSSS y OFDM - la cabecera del paquete se transmite utilizando DSSS, mientras que la carga útil se transmite utilizando OFDM.

[4]HUCABY, David. ciscopress.com: CCNA Wireless 640-722, Official Cert Guide, United States of America, 2014. ps. 51-55

802.11g ocupa un ancho de banda de canal de 22 MHz nominal, por lo que es posible para acomodar hasta tres señales que no se superponen dentro de la banda de 2,4 GHz. A pesar de esto, la separación entre los diferentes puntos de acceso Wi-Fi significa que la interferencia no es normalmente demasiado de un problema.

6.2.3 Estándar 802.11n

Una vez establecidos los estándares Wi-Fi, incluyendo 802.11a, 802.11by 802.11g, comenzaron los trabajos en analizar cómo las velocidades de datos crudos proporcionados por Wi-Fi, redes 802.11 podrían incrementarse aún más. El resultado fue que en enero de 2004, el IEEE anunció que había formado un nuevo comité para desarrollar la nueva de alta velocidad, IEEE 802.11 n estándar.

Los fabricantes están ahora lanzando productos basados en las primeras versiones o proyecto de las especificaciones asumiendo que los cambios sólo serán menores en su ámbito de aplicación.

La industria llegó a un acuerdo de fondo sobre las características de 802.11n a principios de 2006. Esto dio a muchos fabricantes de chips información suficiente para obtener sus desarrollos en curso. El proyecto se espera que esté finalizado en noviembre de 2008 con su publicación formal en julio de 2009.

Sin embargo, muchos con la mejora del rendimiento ofrecido por 802.11n, el estándar pronto se generalizó con muchos productos que se ofrecen a la venta y uso de dispositivos, aunque en un principio pocos puntos de acceso Wi-Fi ofrecen el estándar.

La idea detrás del estándar IEEE 802.11n era que iba a ser capaz de proporcionar un rendimiento mucho mejor y ser capaz de seguir el ritmo de las velocidades de rápido crecimiento que ofrecen las tecnologías como Ethernet.

Para lograr esto una serie de nuevas características que se han incorporado en el estándar IEEE 802.11n para que el rendimiento más alto. Las principales innovaciones se resumen a continuación:

- Los cambios en la aplicación de OFDM
- Introducción de MIMO
- De ahorro de energía MIMO

- Ancho de banda de canal más ancho
- La tecnología de antena
- El reducido apoyo para mantener la compatibilidad con las circunstancias especiales para mejorar el rendimiento de datos.

Aunque cada una de estas nuevas innovaciones añade complejidad al sistema, mucho de esto se pueden incorporar en los chipsets, lo que permite una gran cantidad de este aumento de costos para ser absorbido por las grandes producciones de los chipsets.

802.11n ofrece compatibilidad para los dispositivos en una red utilizando versiones anteriores de Wi-Fi, esto añade una sobrecarga significativa para cualquier intercambio, lo que reduce la capacidad de transferencia de datos. Para proporcionar la máxima transferencia de datos acelera cuando todos los dispositivos de la red en el estándar 802.11n, la característica de compatibilidad con versiones anteriores se pueden eliminar.

Cuando los dispositivos anteriores entran en la red, se vuelven a introducir la sobrecarga compatibilidad con versiones anteriores y características. Al igual que con 802.11g, cuando los dispositivos anteriores entran en una red, el funcionamiento de toda la red se ralentiza considerablemente. Por lo tanto opera una red en modo 802.11n sólo ofrece ventajas considerables.

En vista de las características asociadas con compatibilidad hacia atrás, hay tres modos en los que un punto de acceso 802.11n puede operar:

- Legacy (sólo 802.11 a, b, y g)
- Mezclado (ambos 802.11 a, b, g, y n)
- Greenfield (sólo 802.11 n) - el máximo rendimiento

Mediante la implementación de estos modos, 802.11n es capaz de proporcionar compatibilidad hacia atrás completa, manteniendo las velocidades de datos más altas. Estos modos tienen un impacto significativo en la capa física, PHY y la forma en que la señal está estructurado.

6.2.4 Sistemas de Protección: Estándar 802.11i (WPA2), WPA y WEP

Seguridad Wi-Fi es un tema de importancia para todos los usuarios de Wi-Fi. Se define bajo IEEE802.11i y sistemas como WEP, WPA y WPA2 son sus principales

exponentes, con las llaves o códigos que se proporcionan para los diferentes puntos de acceso wi-fi en uso.

Seguridad Wi-Fi es de significativa importancia porque muchas personas lo utilizan: en casa, en la oficina y cuando están en movimiento. A medida que la señal inalámbrica puede ser recogida por usuarios no autorizados, es imprescindible para garantizar que no puedan acceder al sistema.

Incluso los usuarios que legítimamente tienen acceso a un sistema podría el tratar de hackear otros equipos de la misma zona interactiva.

Puntos de acceso Wi-Fi anuncian su presencia enviando periódicamente una señal de baliza que contiene el SSID. Esto permite a los usuarios potenciales para identificar el punto de acceso y para tratar de conectar con él.

Una vez detectado, se puede tratar de conectarse al punto de acceso, y el procedimiento de autenticación de Wi-Fi se inicia. Para lograr el acceso, por lo general se requiere una clave.

Desde la introducción de la tecnología Wi-Fi una variedad de claves se han utilizado:

- ***WEP:*** WEP o privacidad equivalente por cable fue la primera forma de autenticación utilizado con Wi-Fi. Por desgracia, era fácil de descifrar, y otros sistemas son ahora más ampliamente utilizados.
- ***WPA:*** Wi-Fi Protected Access WPA es una mejora de software / firmware por WEP. La primera versión de este también se conoce como WPA1 o WPAv1.
- ***WPA2:*** WPA2 o WPAv2 es la actualización de WPAv1 y proporciona una mejora significativa en el nivel de seguridad.

6.2.4.1 Clave de privacidad equivalente por cable – WEP

El objetivo de esta clave era hacer redes inalámbricas como Wi-Fi tan seguro como las comunicaciones por cable. Desafortunadamente este tipo de seguridad no estuvo a la altura de su nombre, ya que pronto fue hackeado, y ahora hay muchas aplicaciones de código abierto que pueden romperse fácilmente en él en cuestión de segundos.

WEP usa la misma clave simétrica y estática en los nodos y el router , la cual debe escribirse manualmente en cada terminal, provocando variados inconvenientes, entre ellos, la contraseña es guardada en cada dispositivo, aumentando la probabilidad de que sea comprometida. Además, como la clave debe ser escrita manualmente, el cambio en cada terminal y el router es poco frecuente debido al desgaste administrativo que conlleva este proceso de seguridad.

El algoritmo utilizado para el cifrado es RC4 con claves semilla de 64 bits de longitud, de los cuales 24 bits corresponden al vector de inicialización, IV, y los restantes 40 bits se usan para la clave estática en cambio el IV es generado dinámicamente y en teoría debería ser diferente para cada trama. Esta trama IV tiene como finalidad cifrar con claves diferentes para evitar que un intruso capture suficiente tráfico cifrado con la misma clave y termine deduciendo la clave.

Para esto, router y cliente deben conocer tanto la clave secreta como el IV. La primera ya se encuentra almacenada en cada uno de los dispositivos, mientras que el Vector de Inicialización se genera en un extremo y se envía en la misma trama al otro extremo, por lo que también será conocido, por lo tanto al enviar el IV en cada flujo es sencillo de interceptar por un atacante.

El algoritmo WEP es utiliza el siguiente proceso para crear su trama:

1. Calcula la redundancia cíclica, CRC32, del mensaje para que el destinatario pueda comprobar su integridad.
2. Genera el vector de inicialización, IV, un número aleatorio entre 0 y 4094.
3. Genera una semilla, seed, concatenando la clave secreta y el IV
4. Cifra la semilla con el algoritmo RC4.
5. Se cifran el flujo obtenido realizando una operación binaria O exclusiva entre el mensaje concatenado al CRC32 y la semilla encriptada.
6. Se adjunta al mensaje encriptado el vector de inicialización para que el destinatario, conociendo la clave secreta, pueda realizar la operación inversa y obtener el mensaje original.

La seguridad del sistema WEP es un error grave. Principalmente no aborda el tema de la gestión de claves y esto es una consideración primordial a cualquier sistema de seguridad. Claves normalmente se distribuyen de forma manual o través de otra ruta insegura.

El sistema Wi-Fi WEP utiliza claves compartidas - es decir, el punto de acceso utiliza la misma clave para todos los clientes, y por lo tanto, esto significa que si se accede a la clave entonces todos los usuarios se verán comprometidos. Sólo se necesita escuchar el tráfico de autenticación para ser capaz de determinar la clave.

WEP todavía es muy utilizado y proporciona un cierto nivel de seguridad. Sin embargo, si se utiliza el cifrado de capa superior (SSL, TLS, etc.) también se debe utilizar cuando sea posible.

En el capítulo II de este trabajo se demostrara y explicara como la utilidad MinidWep, que a su vez usa la herramienta aircrack-ng captura IV y descifra fácilmente las claves WEP.

6.2.4.2 WPA Wi-Fi Protected Access

Con el fin de proporcionar una mejora viable para los defectos de WEP , se ideo la metodología de acceso WPA, Wifi Protect Access, El esquema fue desarrollado bajo el auspicio de la Alianza Wi-Fi y utiliza una parte del estándar de seguridad IEEE 802.11i.

WPA-PSK no busca eliminar el proceso de cifrado WEP, sino fortalecerlo, por lo tanto sigue el mismo sistema de autenticación y comunicación, con las diferencias que no utiliza claves estáticas sino dinámicas a través del Protocolo de Integridad de Clave Temporal, TKIP; sus claves son de 128 bits y el IV de 48 bits.

Además, WPA-PSK no utiliza CRC, con el cual podría alterarse la información y actualizar la CRC del mensaje sin conocer la clave WEP, sino que implementa un código de integridad del mensaje, MIC y además posee un contador de tramas que evita ataques de repetición, pero sigue utilizando el protocolo RC4 como su antecesor.

6.2.4.3 WPA2 / WPAv2

El esquema WPA2 ahora ha reemplazado WPA. Implementa los elementos obligatorios de IEEE 802.11i. En particular, introduce CCMP, Counter-mode/CBC-MAC Protocol, un nuevo modo de cifrado basado en AES, Advanced Encrytion Sistema, con una fuerte seguridad[5], además WPA2 implementa una versión mejorada de MIC para comprobar la integridad de los mensajes.

[5] ANDREU, Fernando, PELLEJERO, Izaskun, LESTA, Amaia. Marcombo: Redes WLAN. Fundamentos y Aplicaciones de Seguridad, Barcelona 2006. ps. 59-63

Certificación para WPA2 se inició en septiembre de 2004 y ahora es obligatorio para todos los nuevos dispositivos que llevan la marca Wi-Fi. Igualmente, en el capítulo II, se realiza una demostración de cómo se puede capturar un Handshake, tanto en WPA como en WPA2, en el proceso de autenticación y realizar el descifrado con un ataque de diccionario, utilizando las herramientas Aircrack-ng y Crunch, o bien por medio del "engaño" con la herramienta Linset.

6.3 WPS

WPS, *Wi-Fi Protected Setup*, es un estándar promovido por la Wi-Fi Alliance en el año 2007 y no es un sistema de protección, en sí, sino que tiene como fin el de lograr una conexión rápida y fácil entre el router y el host dentro de una WLAN.

WPS evita la configuración excesiva por parte de los usuario en entornos domésticos o pequeñas oficinas, para lo cual, WPS establece los pasos por los cuales los dispositivos de la red obtienen las credenciales necesarias para iniciar el proceso de autenticación, como el SSID y el PSK.

El diseño de comunicación de WPS consta de tres componentes:

- Registrar: tiene la atribución de proporcionar el acceso y credenciales a la red.
- Enrollee: el dispositivo que requiere el acceso a la red inalámbrica y no tiene ninguna configuración.
- Authenticator: generalmente este rol lo asume el mismo Punto de Acceso.

El estándar WPS puede ser configurado dentro de una red por alguno de los siguientes cuatro métodos:

- **PIN**: la entidad Enrollee o usuario debe introducir un Número de Identificación, PIN, en la venta web. Este código por lo general lo tienen escrito los router en una etiqueta y como se menciona el Enrollee debe tener interfaz, bien sea una pantalla o teclado, para ingresar e PIN.

Este mecanismo es el más utilizado en las redes domésticas, El dispositivo debe transmitir un código numérico al router y a cambio este último le envía los datos para acceder a la red este código PIN se compone de 8 dígitos para que el router permita acceder a la red inalámbrica. Generalmente, este código PIN viene escrito en la parte inferior del router, pero existen maneras alternativas de averiguarlo.

Con un código de 8 dígitos las combinaciones posibles son de 10^8, pero su diseño lo divide en dos partes, la primera parte son sus iniciales 4 dígitos, lo que significa que el número de combinaciones se reduce a 10^4, mientras que la segunda parte del PIN está compuesto por los siguientes 3 dígitos, o sea, 10^3.

El último dígito corresponde a la suma de comprobación, checksum, de los 7 dígitos anteriores y que se explicará su obtención en el capítulo II de este trabajo, aunque puede variar según la casa fabricante del dispositivo.

Por tanto solo se necesitan 11.000 combinaciones para obtener el PIN, podría tardar pocos segundos, pero actualmente los router tienen sistemas que protegen contra esta clase de ataques de fuerza bruta, reduciendo el número de intentos por PIN que se pueden enviar a ese dispositivo, por lo cual en este trabajo se aborda el uso del PIN genérico y la utilización de dos algoritmos que funcionan en la mayoría de los routers vigentes.

- **PBC**: se realiza el intercambio de credenciales a partir que presionar un botón tanto en el Punto de Acceso como en el dispositivo Enrollee. El Punto de acceso cuenta con un temporizador para dar tiempo para lograr la conexión, pero en el corto lapso de tiempo que otorga el temporizador otro hosts puede obtener el acceso a la red.

- **NFC**: intercambio de credenciales a través de comunicación NFC. La tecnología NFC, basada en RFID permite la comunicación sin hilos entre dispositivos próximos (0 - 20 cm). Entonces, el dispositivo *Enrollee* se tiene que situar al lado del *Registrar* para desencadenar la autenticación. De esta manera, cualquier usuario que tenga acceso físico al *Registrar*, puede obtener credenciales válidas.

- **USB**: con este método, las credenciales se transfieren mediante un dispositivo de memoria flash (e.g. *pendrive*) desde el *Registrar* al *Enrollee*.

Los métodos PBC, NFC y USB fueron ideados para comunicar dispositivos que no cuenta con interfaz de entrada , pero los dos últimos mecanismos nombrados no están certificados y solamente el método PIN es obligatorio en las estaciones para obtener la certificación por parte de la WiFi-Alliance y el métodos PBC es imperativo en los Puntos de Acceso.

Por último y también en el capítulo II, se utilizara la herramienta WpsPin, basada en Reaver para obtener la contraseña, método PIN, sin importar que sistemas de protección de los antes reseñados posea la wlan.

6.4 WIFISLAX

WiFiSlax es una distribución GNU/Linux basada en la primera distribución que aún se encuentra vigente, Slackware. Se puede utilizar sin ser instalada a través de un Disco Compacto un dispositivo USB, siendo perfilada para la auditoría de seguridad y en general para la seguridad informática[6].

Esta distribución posee una variada lista de herramientas de auditoria para probar la seguridad de las redes inalámbricas, inclusive alámbricas, como escáner de puertos, herramientas para creación y diseño de exploits, sniffers. Además tiene utilidades enfocadas hacia el análisis forense.

Actualmente se encuentra en su versión 4.10 que integra varios controladores de red no oficiales en su kernel de Linux, proporcionado de esta forma soporte inmediato para un gran número de tarjetas de red cableada e inalámbrica y que incorpora scripts para su actualización evitando que deba actualizarse completamente cuando salga una nueva versión.

[6]WIKIPEDIA. WifiSlax [en línea]. <https://es.wikipedia.org/wiki/WiFiSlax> [citado en 27 febrero de 2015]

6.5 MARCO LEGAL

Las normas citadas a continuación son a las que se podrían ver enfrentadas las personas que utilicen los métodos recolectados dentro del presente trabajo, por el solo hecho de tratar o ingresar en redes ajenas sin autorización, según lo legislado por el Congreso de la República de Colombia:

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- 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.

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

- Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses[7].

[7] EL CONGRESO DE COLOMBIA. Ley 1273 DE 2009 [en línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html> [citado en 03 marzo de 2015]

Ley 1341 de 2009.Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- Titulo VI REGIMEN DE PROTECCIÓN AL USUARIO; artículo 53. Régimen Jurídico; artículo 53. “Recibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la Constitución Política y la ley[8].

[7] EL CONGRESO DE COLOMBIA. Ley 1349 DE 2009 [en línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html> [citado en 03 marzo de 2015]

CAPITULO III

7. METODOLOGIA DE TRABAJO

La finalidad esencial de esta monografía es determinar si aún persisten las vulnerabilidades más comunes en los sistemas de protección en la actualidad en las redes con tecnología WIFI, para lo cual, se realizan pruebas de penetración, teniendo en cuenta los siguientes componentes:

7.1 EQUIPAMIENTO

Para obtener la información necesaria que permita alcanzar los objetivos planteados se utilizan los elementos descritos en el Cuadro 1.

Cuadro 1. Elementos Usados

HARDWARE	***CARACTERISTICAS***
Computador Portátil 	❖ Marca: ACER ❖ Modelo: TravelMate 4520 ❖ Procesador: AMD, Turion64X2 ❖ RAM: 4 Gigas,DDR-2 ❖ Disco Duro: 160 Gigas ❖ WLAN: Broadcom 802.11b/g
Tarjeta de Red Inalámbrica 	❖ Marca: TP-LINK ❖ Modelo: TL-WN722N ❖ Interfaz : USB 2.0 ❖ Velocidad: máximo 150 Mbps ❖ Antena: 4dBi ❖ Frecuencia: 2.400-2.4835GHz ❖ Standard: IEEE 802.11b/g/n
Dispositivo Flash	❖ Marca: Kingston ❖ Modelo: DTSE9 ❖ Interfaz: USB 2.0 ❖ Capacidad: 16 Gigas

	
SOFTWARE	***CARACTERISTICAS***
WifiSlax 	❖ Sistema Operativo: GNU-Linux ❖ Versión: 4.10 ❖ Instalada dentro de Dispositivo Flash

Fuente: El Autor

7.2 COBERTURA

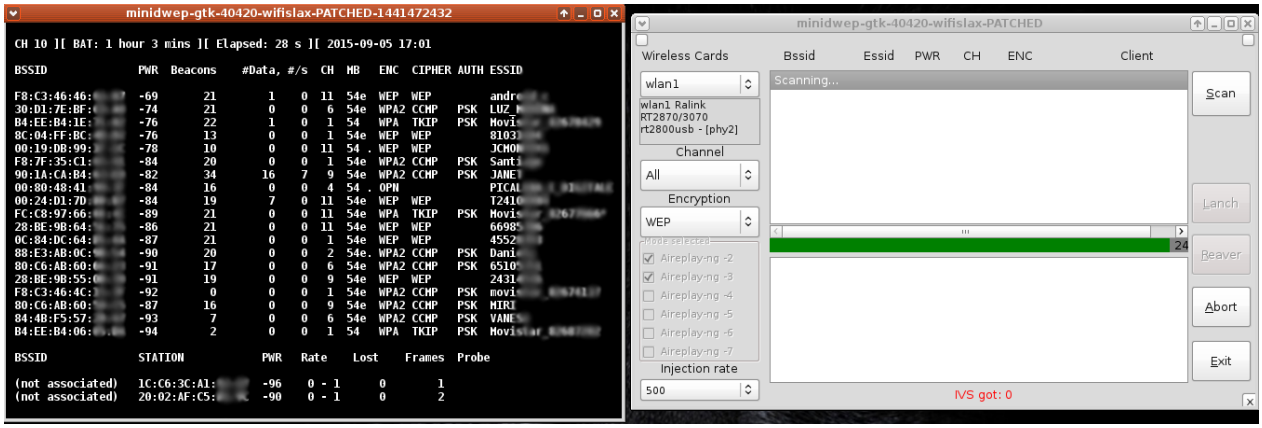
Se toma como muestra una zona residencial del municipio de Saldaña, Tolima y otra zona residencial del municipio de Ortega, donde en algunos de los casos funcionan pequeñas empresas, obteniendo el permiso por parte de los propietarios de las redes para la realización de los test por cuanto les interesa conocer la seguridad de su infraestructura inalámbrica.

7.3 VULNERANDO LOS SISTEMAS DE PROTECCIÓN

Aunque parezca imposible existen en la actualidad redes que utiliza WEP y aunque fue presentado en el año 1999 y dos años después se detectaron vulnerabilidades en su concepción, los proveedores de internet no han actualizado los routers de sus usuarios aun sistema de protección un poco más seguro como WPA o WPA2.

Para obtener la contraseña WEP solo basta con capturar paquetes IV, que dependiendo la robustez de la contraseña implementada puede variar en algunos miles, pero siempre se logra obtener. Para este caso se utilizará la utilidad MinidWep, contenida en la distribución Wifislax, como se observa en la Figura 2.

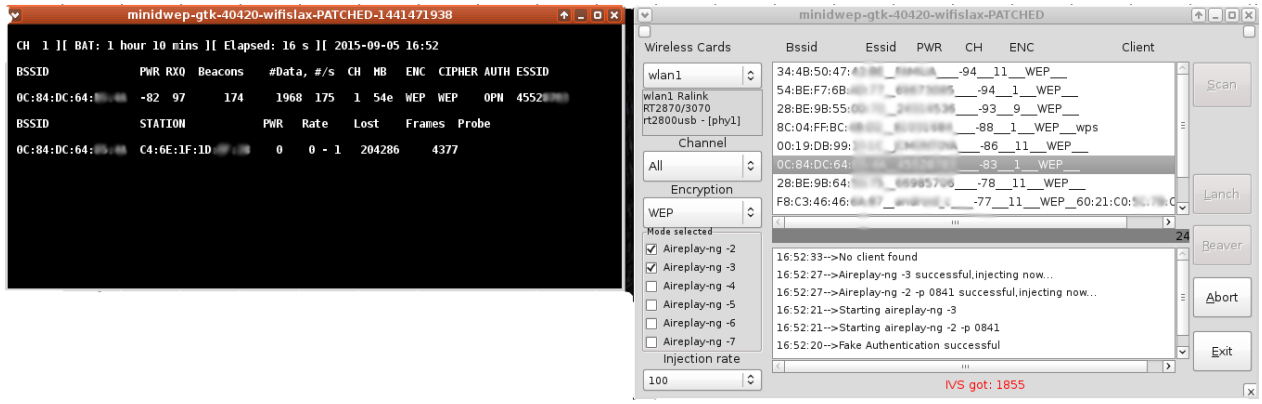
Figura 2. Escaneando con MinidWep



Fuente: El Autor

Esta herramienta a su vez usa como la mayoría de las herramientas de esta distribución a aircrack-ng, al oprimir el botón “Scan” se activa el comando airodump-ng mon0, siendo mon0 la interfaz en modo monitor, como se observa en la Figura 3, y con la cual empieza a buscar las redes alcance de la tarjeta por 30 segundos.

Figura 3. Seleccionando Router con MinidWep



Fuente: El Autor

Una vez muestra las redes encontradas se procede a seleccionar la red a auditar, en este caso, la red con el router que posee la MAC OC:84:DC:64:XX:XX, y se oprime la tecla “Lanch”.

De esta forma activa los comandos airodump-ng, pero ahora con los parámetros –bssid para seleccionar la dirección física de la tarjeta del router, o sea, OC:84:DC:64:XX:XX, -c para el canal donde se emite los paquetes de la red, 1 y –w para que guarde los IV temporalmente para posteriormente analizarlos con cualquier nombre. Como se observa en la Figura 5, ha logrado capturar 1855 IV, los cuales va almacenando en un archivo con extensión .cap.

Asimismo, utiliza los comandos aireplay-ng -1, para la falsa autenticación y asociación, igualmente utiliza el comando aireplay-ng -3, para provocar que el router envíe IV , con base a un paquete ARP que ha capturado previamente la herramienta y lo envía reiterativamente al punto de acceso para generar gran volumen de trama IV.

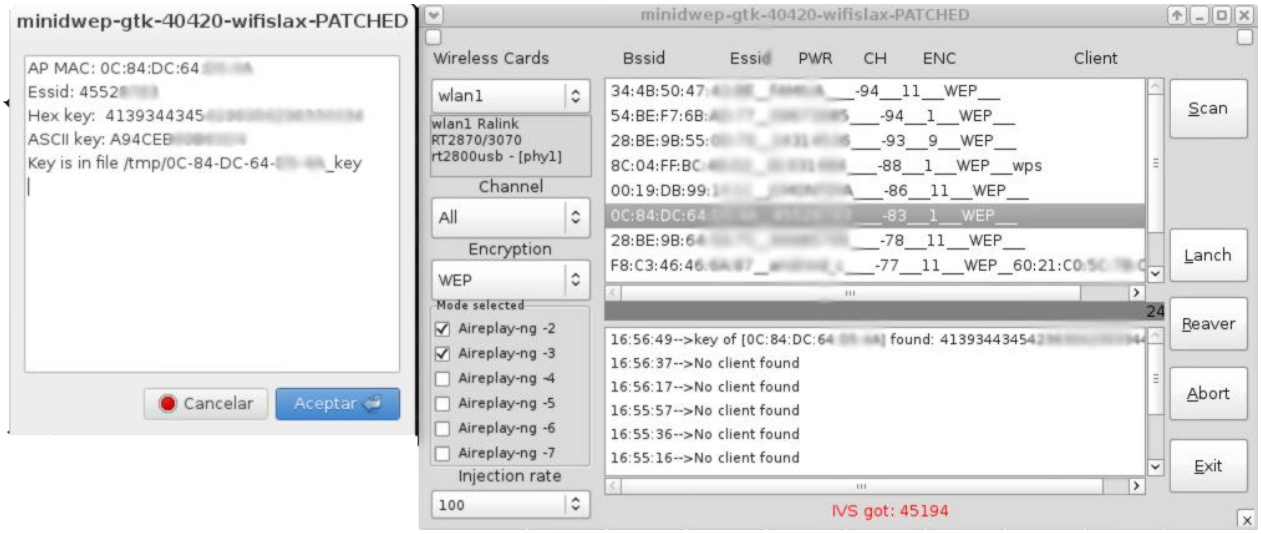
Por último, cada 5000 IV capturados lanza el comando Aircrack-ng para analizar si ya tiene los IV suficientes para descubrir la contraseña.

Los comandos quedarían así:

Airodump-ng --bssid OC:84:DC:64:XX:XX –c 1 –w *cualquier nombre* mon0 Aireplay-ng -1 0 -e nombre de la red -a MAC del Router -h MAC de cliente a asociar mon0 Aireplay-ng -3 -b MAC del Router -h MAC de cualquier cliente mon0 Aircrack-ng ruta/*nombre de archivo*.cap.

En la Figura 4 se observa la ventana lanzada por Minidwep con los datos que obtiene, entre ellos la contraseña y la ventana principal de esta herramienta:

Figura 4. Descubriendo la Contraseña con MinidWep



Fuente: El Autor

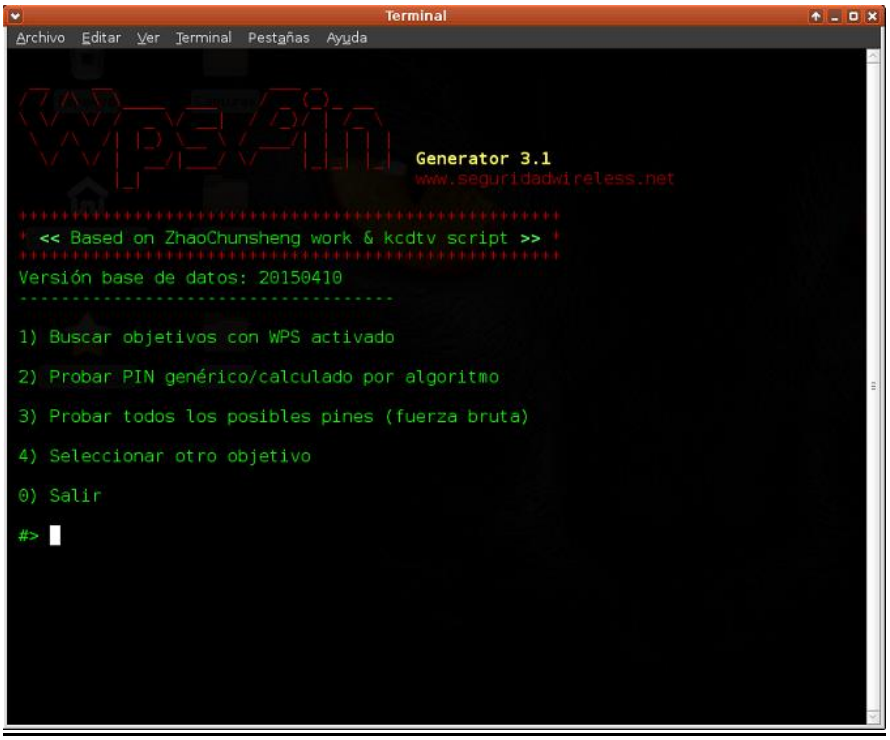
Al cabo de 45.000 IV la herramienta ha sido capaz de descubrir la contraseña la cual muestra en una ventana emergente y la guarda en un archivo del computador.

Ahora, se procede a demostrar cómo se pueden vulnerar las contraseñas protegidas con WPA o WPA2, con diferentes métodos. Primero, se procede a realizar un barrido del espectro con la tarjeta inalámbrica USB que permite un mayor alcance, con el fin de detectar las redes cercanas para lo cual se inicia la aplicación WifiSlax.

En primera instancia se ejecutará la herramienta Wps Pin, por cuanto permitirá en poco tiempo obtener la contraseña por defecto que tienen configurados los routers a través del standard WPS , y aunque en principio el sistema de seguridad WPA-PSK es el más seguro en la actualidad , tiene una gran vulnerabilidad debido a que para la certificación de la WIFI ALLIANCE obliga la implementación de este Standard.

Como se observa en la Figura 5, la interfaz está en español y fácil de entender, se selecciona la opción uno, posteriormente solicitará tiempo y canal para la realización del escaneo, pero se dejará por defecto, oprimiendo dos veces enter.

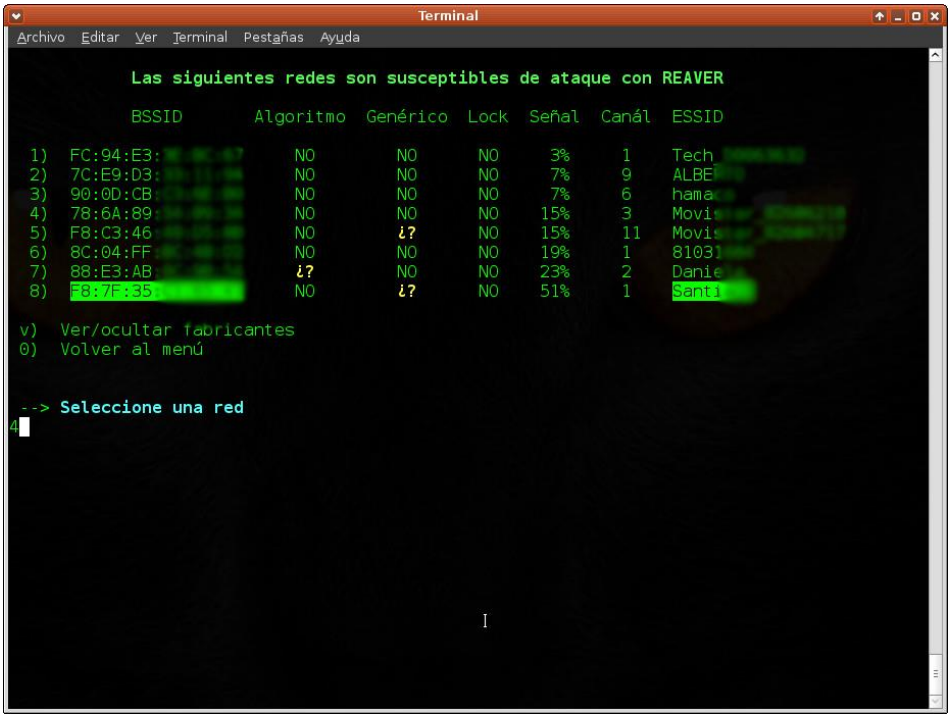
Figura 5. Ventana Principal WpsPin



Fuente: El Autor

Como se observa en la Figura 6, la pantalla donde aparecen las redes encontradas y que tienen habilitado el protocolo WPS para este caso, se escoge cualquier punto de acceso, en este ejemplo el 4, anotando que la combinación de BSSID-ESSID resaltada, se debe a que ya se encontró la clave utilizando este mismo método y se encuentra almacenada en el repositorio de contraseñas.

Figura 6. Lista redes encontradas WpsPin



Fuente: El Autor

En la Figura 7 se observa las generalidades del router auditado, como es su ESSID (nombre de la red); BSSID (dirección física) y el canal escogido para el envío de datos. Además ilustra el pin genérico (en este caso no está en su base de datos), para este modelo de router y los algoritmos (ComputerPIN y EasyboxWPS) que utilizará al momento de escoger la opción dos del menú.

Figura 7. Ventana Objetivo WpsPin

Fuente: El Autor

Se obtiene la contraseña que utiliza el protocolo WPA-PSK en pocos segundos con el uso del algoritmo computerPIN y es almacenada automáticamente en la carpeta de claves de la Utilidad.

El proceso que utiliza WpsPin en este caso para conocer la clave wpa-psk, es a través del algoritmo ComputerPin de ZaoChunsheng, el cual aprovecha la debilidad de los fabricantes de los dispositivos en la generación del PIN de sus dispositivos.

Básicamente lo que hace este algoritmo es tomar los tres últimos octetos de la dirección física o MAC del router, en este caso xx:xx:xx:54:89:34 que corresponde, en teoría, a la identificación individual de la interfaz inalámbrica y convertirlos de hexadecimal a decimal:

$548934=5*16^5 + 4*16^4 + 8*16^3 + 9*16^2 + 3*16^1 + 4*16^0=5540148$

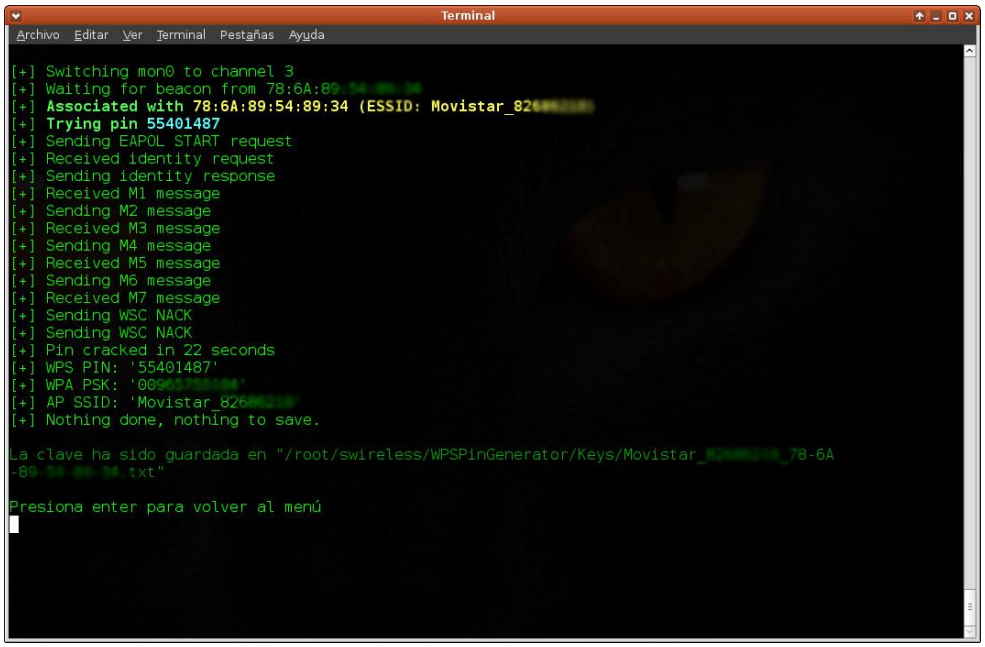
De esta forma se obtienen los siete primeros dígitos del PIN el octavo corresponde a la suma de verificación de estos mismos dígitos, de esta forma:
Se multiplica el primer número por 3 y el siguiente por 1 y así sucesivamente:

$5*3 + 5*1 + 4*3 + 0*1 + 1*3 + 4*1 + 8*3 = 63$

Se toma la unidad de la suma en este caso el 3 y siempre se le resta este valor al 10, o sea, 10 – 3= 7, obteniendo el PIN de ocho dígitos, 55401487, que es probado por la herramienta enviándolo al router, el cual devolverá la clave.

En la Figura se 8 se observa la ventana de la aplicación mientras realiza el análisis del PIN.

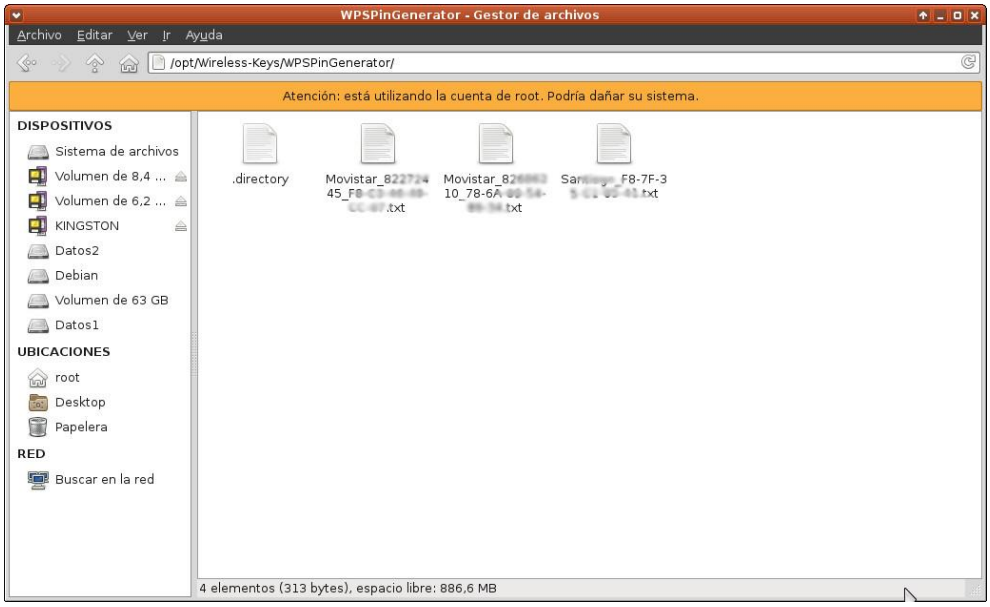
Figura 8. Obteniendo Contraseña WpsPin



Fuente: El Autor

Se observa en la Figura 9 la carpeta de claves de la herramienta WPSPinGenerator.

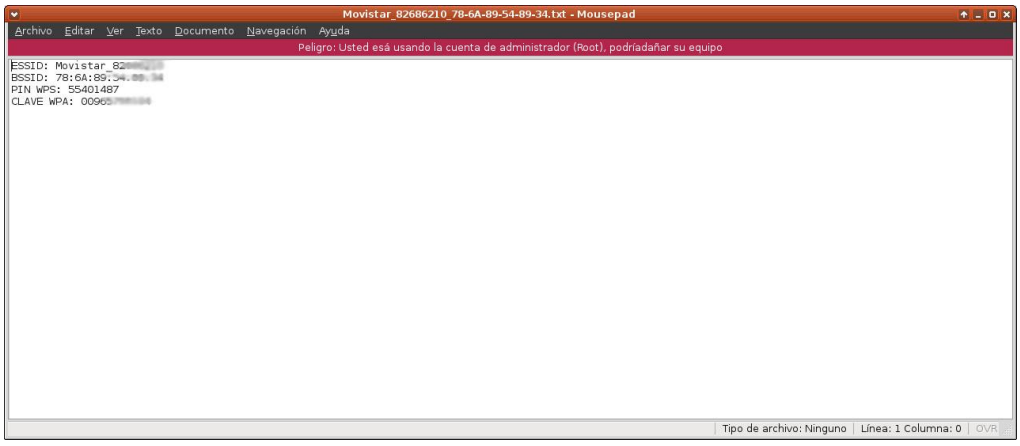
Figura 9. Directorio de Contraseñas WpsPin



Fuente: El Autor

Se observa en la Figura 10 la información contenida dentro de cada uno de los archivos creados durante el proceso de rompimiento de la clave:

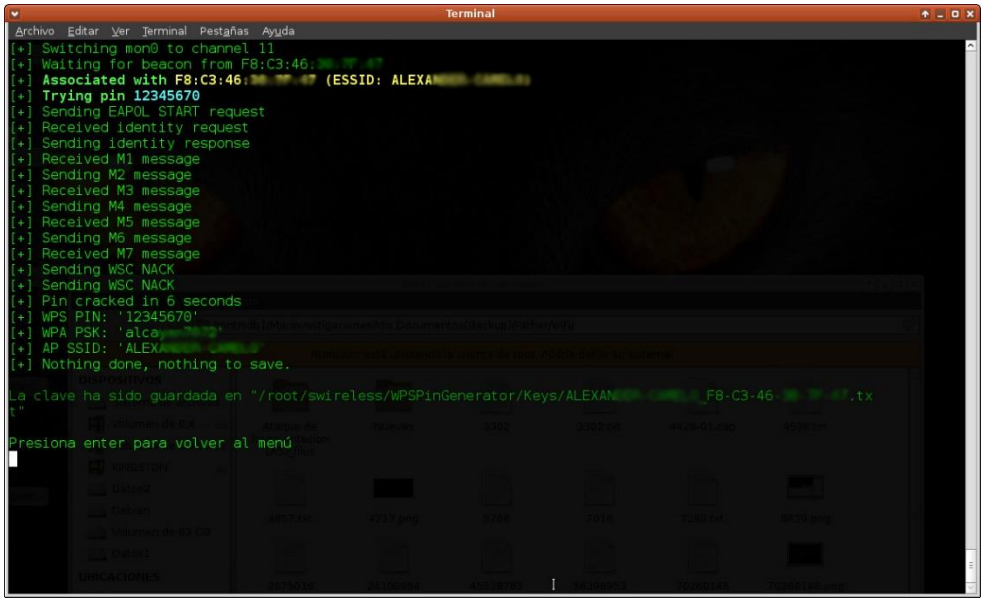
Figura 10. Archivo WpsPin de contraseña



Fuente: El Autor

La Figura 11 también muestra la contraseña obtenida mediante la misma herramienta pero esta vez con la utilización del pin genérico que utilizo la empresa en la programación del router:

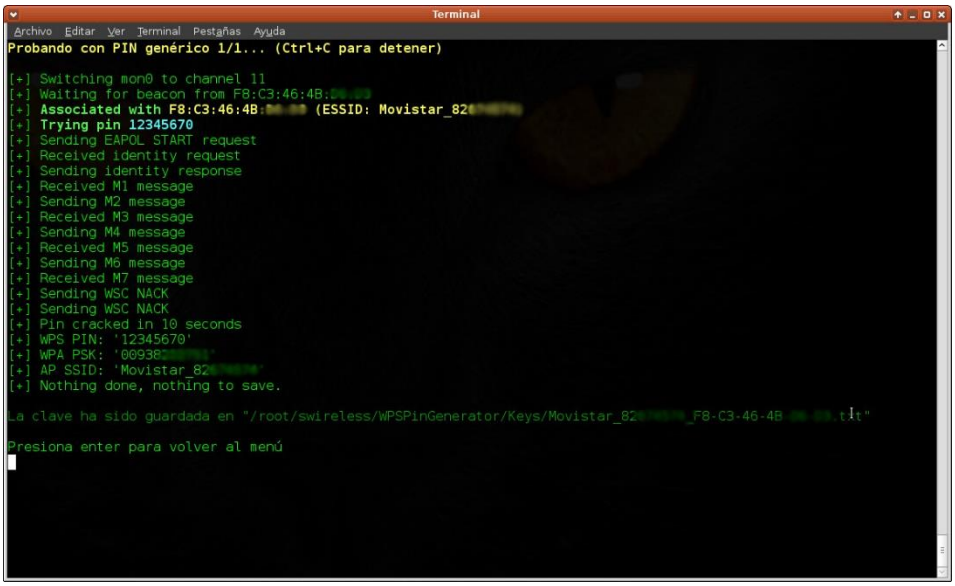
Figura 11. Obteniendo Contraseña WpsPin



Fuente: El Autor

Una red más obtenida también por el pin genérico 12345670, como se observa en la Figura 12 es la misma empresa fabricante, teniendo en cuenta que los tres primeros octetos de la dirección MAC (BSSID) son los mismos.

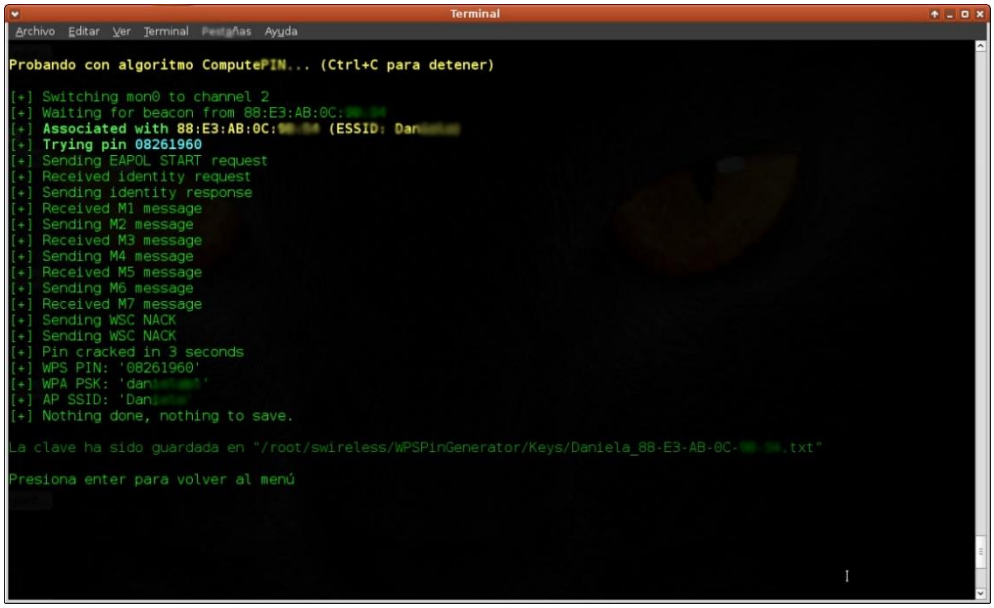
Figura 12. Obteniendo Contraseña WpsPin



Fuente: El Autor

Utilizando el algoritmo ComputerPIN de WPSPinGenerator se siguen obteniendo buenos resultados, como se ilustra en la Figura 13.

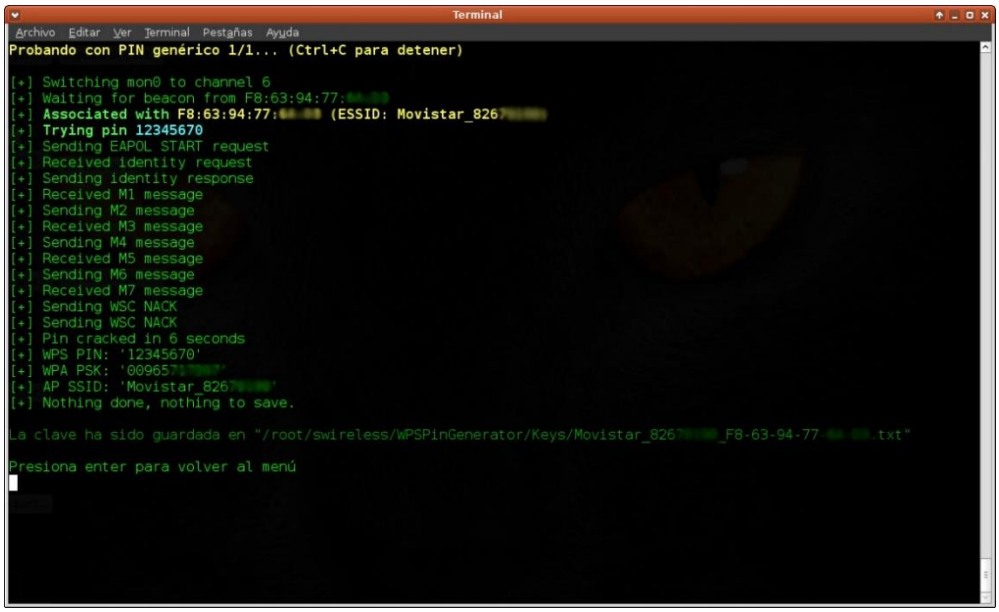
Figura 13. Obteniendo contraseña



Fuente: El Autor

Aunque el ataque usando el pin genérico da la herramienta WPSPinGenerator ha tenido mayor efectividad, en la obtención de contraseñas, como se observa en la Figura 14.

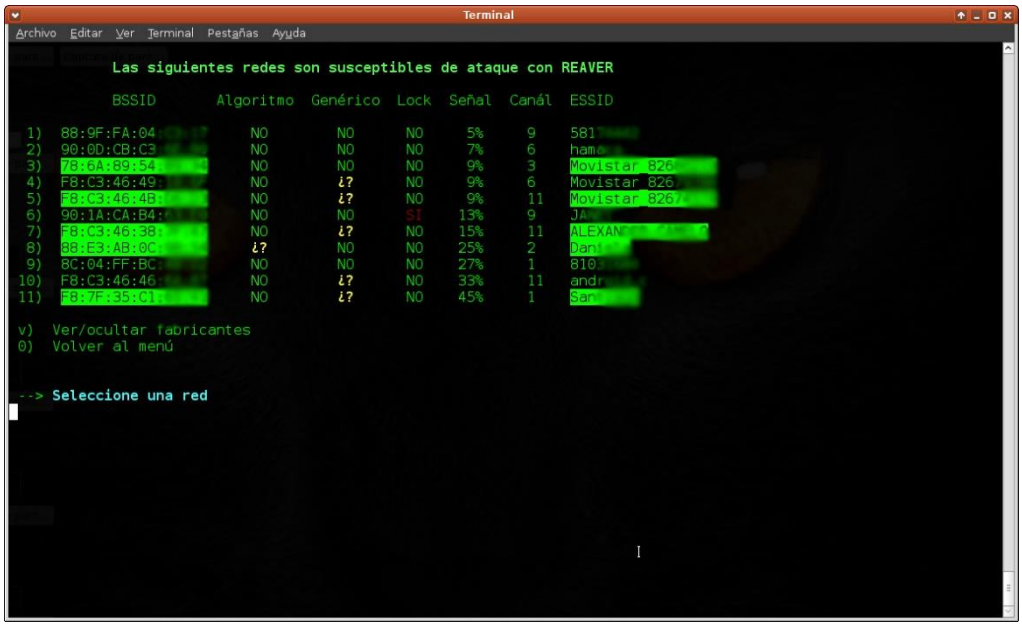
Figura 14. Obteniendo Contraseña



Fuente: El Autor

Al cabo de unas horas de escaneo y utilización de la herramienta WPS PinGenerator se han obtenido cinco contraseñas, aprovechando la debilidad del estándar WPS, aunque posea un protocolo seguro e indiferentemente sea WPA o WP2, como se observa en la Figura 15.

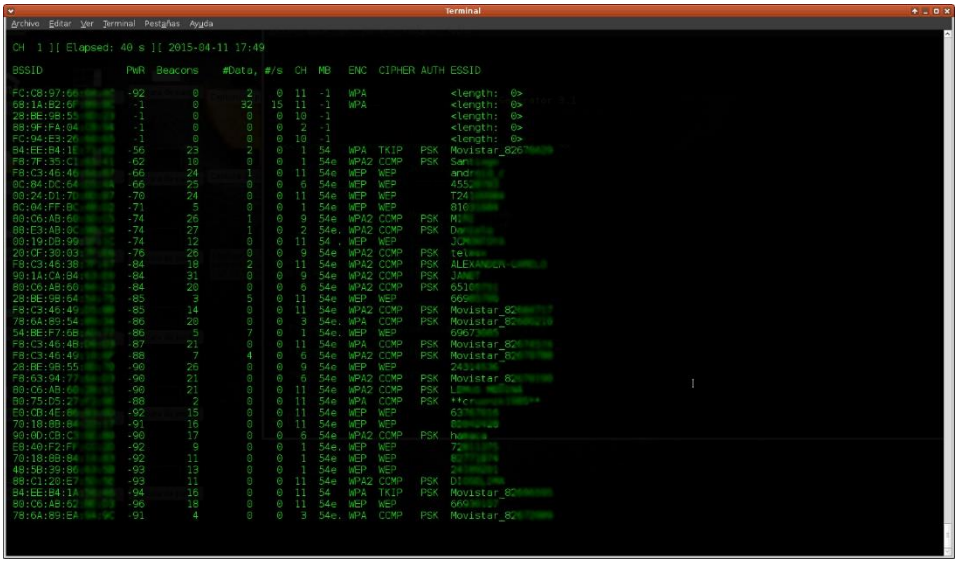
Figura 15. Listado de redes vulneradas con WpsPin



Fuente: El Autor

En la Figura 16 se observan las redes que están al alcance de la tarjeta inalámbrica utilizada donde se distinguen las redes de las cuales se obtuvo sus claves y el cifrado que poseen.

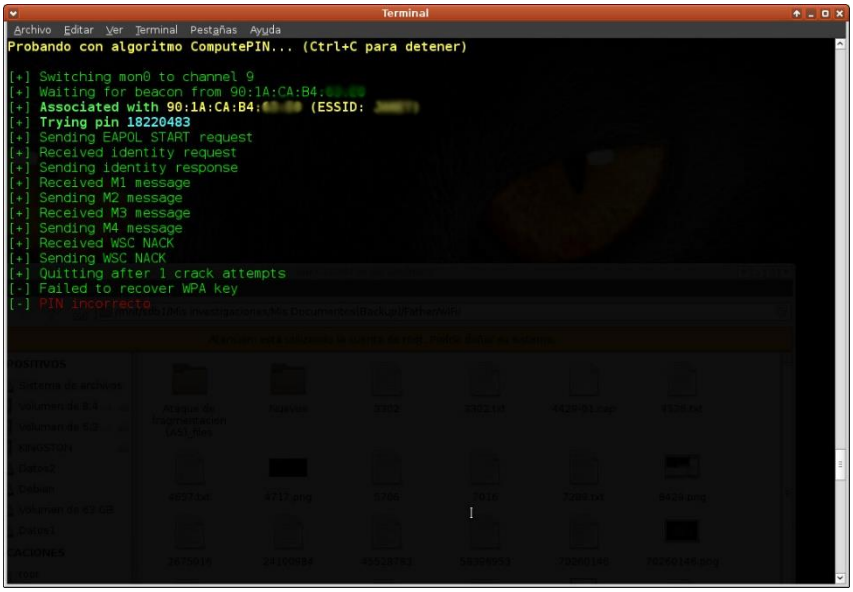
Figura 16. Tipo de Sistema de Protección de las redes vulneradas



Fuente: El Autor

No siempre se puede obtener con la utilización de esta herramienta la contraseña deseada, como se observa en la Figura 17, al menos con la utilización del pin genérico y los algoritmos, se podría usar el ataque de fuerza bruta, que es la opción tres de esta utilidad, que en condiciones ideales podría durar 9 horas, pero algunos routers utilizan medidas de protección que entorpecen este objetivo.

Figura 17. Fallo de WpsPin, método de algoritmos



Fuente: El Autor

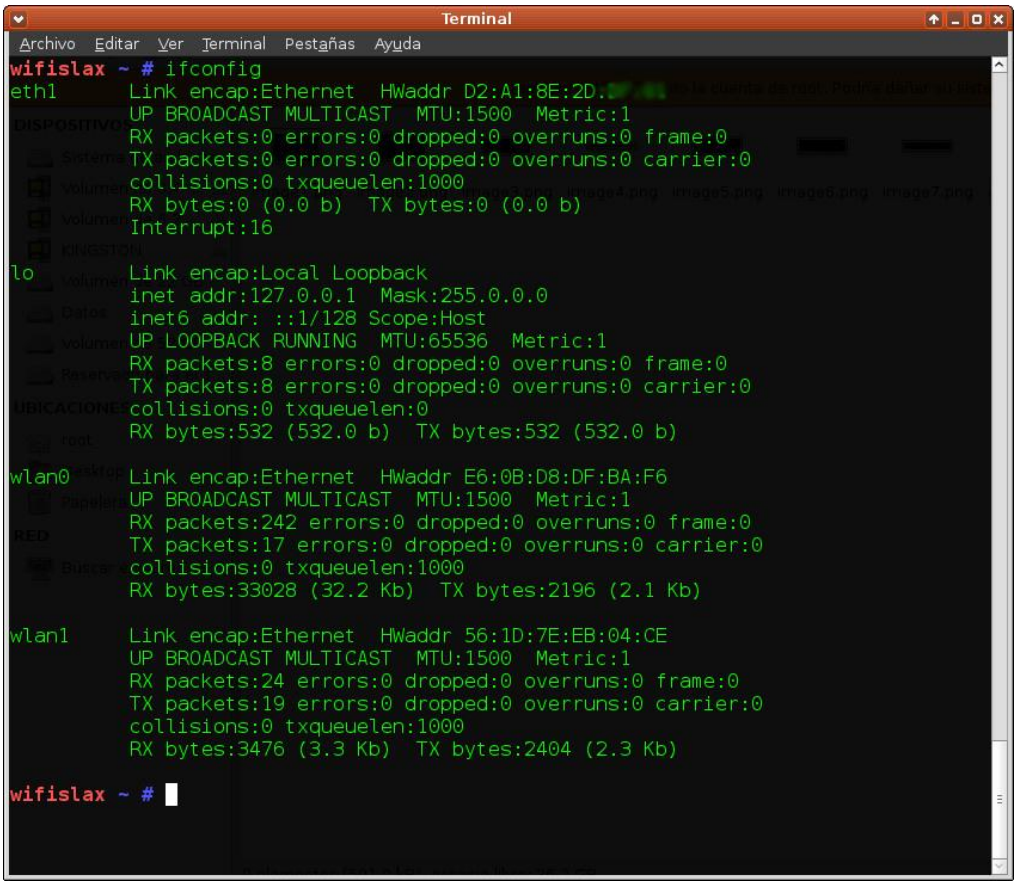
También se puede utilizar otra utilidad de esta versión de GNU-Linux para obtener la contraseña en poco tiempo basado en las capturas anteriores y es que por simple observación de los essid o nombres de las redes auditadas se puede deducir que las contraseñas usadas por defecto por la empresa movistar son el número de identificación del propietario con el precedida de los dígitos 009.

Teniendo en cuenta lo anterior, se utiliza herramienta crunch para proceder a hacer un diccionarios personalizado y pasarlo directamente a otra utilidad incluida en WifiSlax como es aircrack-ng, aunque se podría evitar todo esto con la utilización de la Ingeniería Social y realizar una llamada al número de telefonía fija que aparece después de la palabra Movistar y el guion bajo y “solicitar amablemente” el número de identificación del propietario.

CRUNCH Y AIRCRACK-NG

Se abre el Shell de la distribución de la distribución WifiSlax, y se ejecuta el comando “ifconfig”, el cual muestra por pantalla las interfaces inalámbricas que detecta, en este caso, la interfaz “wlan0” y “wlan1” que posee el driver de la empresa Broadcom b43, tarjeta Interna, y la Atheros AR9271, tarjeta USB. Las interfaces eth1, pertenece para conectar redes LAN y lo es la interfaz lógica, como se observa en la Figura 18.

Figura 18. Comando conocer interfaces de red y dirección física propia

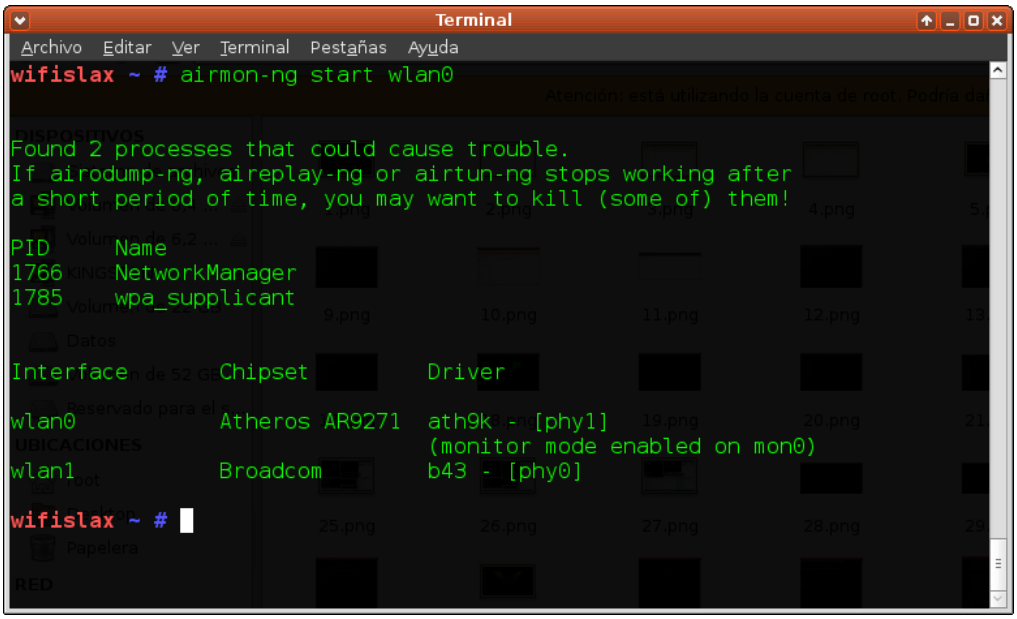


Fuente: El Autor

Se procede a colocar la interfaz “wlan0” en modo monitor para que procese todos los paquetes que captura, con el comando “airmon-ng start wlan0”, la cual crea una nueva instancia de esta interfaz con el nombre “mon0”, como se observa en la Figura 19.

En este punto vale la pena aclarar que no todos los controladores de las tarjetas inalámbricas permiten colocarse en modo monitor pero esta distribución, WifiSlax, en su versión número 10, posee la mayoría de los utilizado actualmente como son Prism54,Madwifi-ng,HostAP,Ralink rt2570 , 2500, rt73 y rt61, Zydas ZD1211rw, Intel pro wireless ipw2100 / ipw2200 / Intel pro wireless ipw3945 ,Realtek rtl8180 y rtl8187, Broadcom, Texas Instruments (acx).

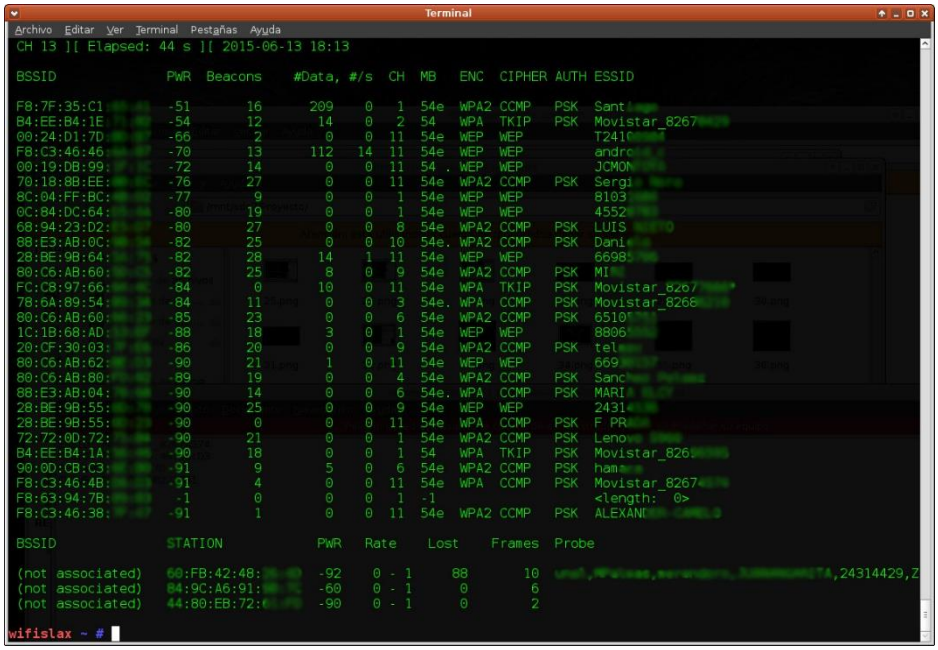
Figura 19. Colocando la interfaz en modo monitor



Fuente: El Autor

Se ejecuta el comando “airodump-ng” con el fin de que muestre por pantalla los Punto de Acceso y nodos inalámbricos que detecta, publicando la red de nombre, ESSID, “movistar_8268XXXX” y dirección física o MAC, BSSID, “F8:C3:46:49:XX:XX”, con algoritmo de cifrado WPA y protocolo de autenticación PSK. También se observa que la señal es mala, PWR “-88”, está por encima de los -75, como se observa en la Figura 20, que es un valor aceptable para lograr la desautenticación, por lo cual debe haber un acercamiento al objetivo, también para verificar si hay clientes conectados a este Punto de Acceso, requisitos necesarios para lograr la meta trazada.

Figura 20. Redes al alcance para auditar



Fuente: El Autor

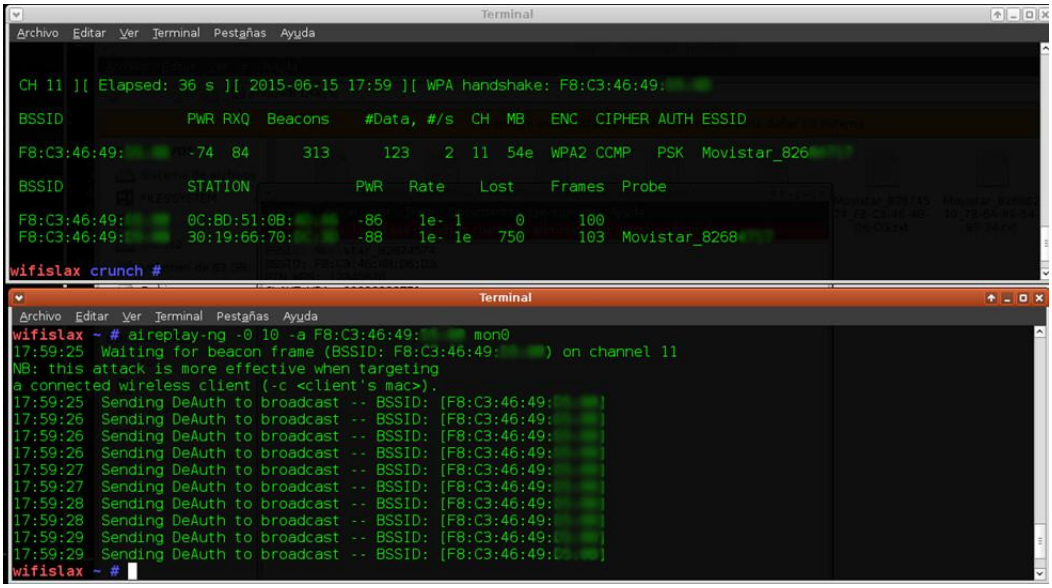
Ejecutando el comando “airodump-ng mon0 –w ProSegInf –c 11 –bssid F8:C3:46:49:XX:XX se le indica a la herramienta aircrack que guarde los datos, opción –w, con cualquier nombre de los paquetes capturados por el canal 11, opción –c, del Punto de Acceso escogido, opción – bssid, a través de la interfaz promiscua, mon0.

Se procede a abrir otro Shell donde utilizando el comando “aireplay-ng -0 10 -F8:C3:46:49:XX:XX –c 00:21:00:D6:XX:XX mon0”, con el fin de lograr la desautenticación de una de las estaciones conectadas a la red “movistar_8268XXXX”, como se ilustra en la Figura 21 parte inferior.

Donde la opción -0, le informa aircrack que es un ataque de desautenticación enviando 10 paquetes; en la opción –a se coloca la MAC del Punto de Acceso; en la opción –c se coloca la MAC de una de las estaciones conectadas.

Se observa en la Figura 21, parte superior derecha, que se ha logrado capturar el momento en que el Punto de Acceso y el Nodo atacado se vuelven asociar y autenticar, capturando el Handshake buscado.

Figura 21. Capturando Handshake para Crunch



Fuente: El Autor

En este punto se logra la primera parte importante del objetivo propuesto, que debe realizarse “On Line”, ya para la parte siguiente se necesita el archivo donde se encuentra el Handshake, en este caso “ProSegInfo-01.cap” y un buen diccionario.

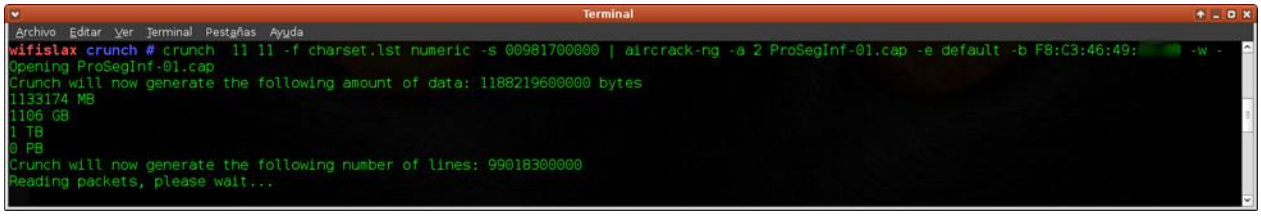
Pero como se menciona anteriormente, se basa en una red de la empresa movistar y conociendo su configuración por defecto para esta Región, según conocimientos anteriores, se presume que la contraseña WPA2 puede ser un digito con prefijo 009 y la cedula de quien adquirió el producto.

Como se realiza una prueba de concepto se iniciara el conteo desde un número cercano al del propietario de la red, para este caso 00981700000, pero para identificaciones de esta región lo normal es del 00938000000 o 00965000000, o bien 0091111000000 o 0091110000000, anotando que los valores a buscar serían 6 de diez números posibles, o sea, 10^6=1.000.000 y aircrack-ng en este

computador trabaja en promedio a 1.500 claves por segundo, 1.000.000/1500=666 segundos teóricos en obtener la clave.

Motivo por el cual se procede a crear un diccionario con la herramienta Crunch 3.3, pasándole los resultados directamente a Aircrack para lograr conocer la contraseña propósito de la actividad, como se observa en la Figura 22.

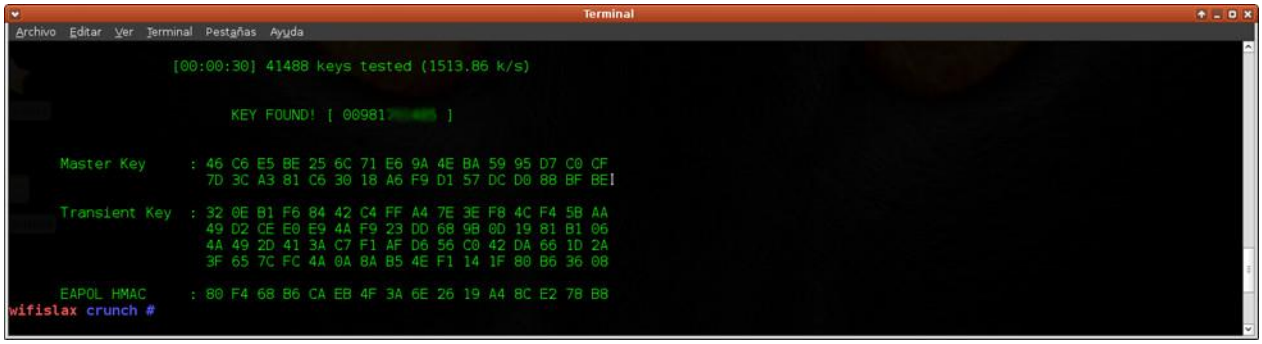
Figura 22. Ejecutando la herramienta Crunch



Fuente: El Autor

Debido a que la contraseña estaba cerca al número desde donde se inició la búsqueda no demoro sino 30 segundos en devolver el resultado y conseguir el objetivo final de este ejercicio, como se observa en la Figura 23.

Figura 23. Contraseña encontrada con Crunch



Fuente: El Autor

Si por los métodos explicados no se logra romper el sistema de protección se debe recurrir a una herramienta un poco más intrusiva pero igualmente efectiva, como es LINSET, contenida dentro de esta misma distribución de GNU-Linux.

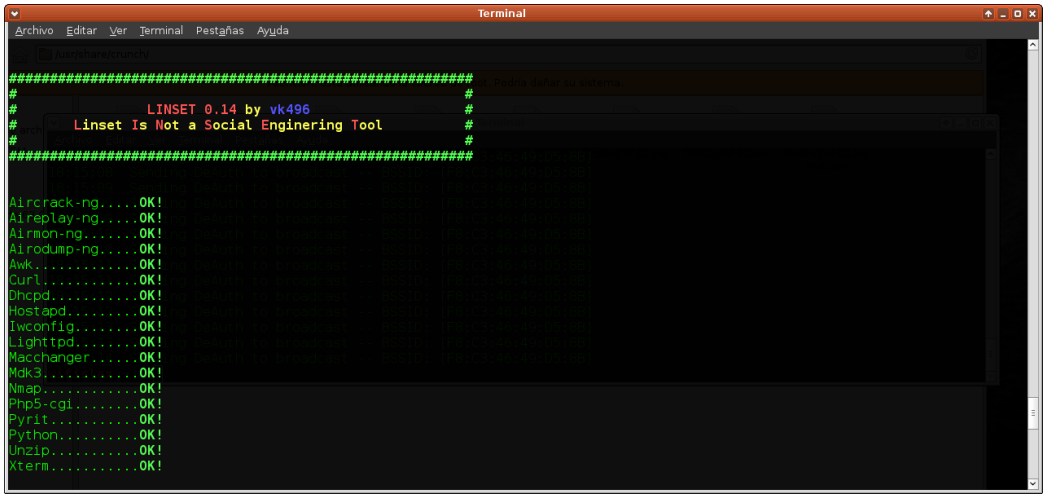
LINSET utiliza básicamente un ataque de Denegación de Servicio y Phishing, y aunque su acrónimo recursivo, LINSET, signifique que no es una herramienta de Ingeniería Social, su uso deja abierta la discusión sobre este aspecto. En la Figura 24 se observa el menú para su ingreso.

Figura 24. Menú WifiSlax

Fuente: El Autor

Se ejecuta la herramienta Linset desde el menú emergente y se abre la ventana que se describe en la Figura 25.

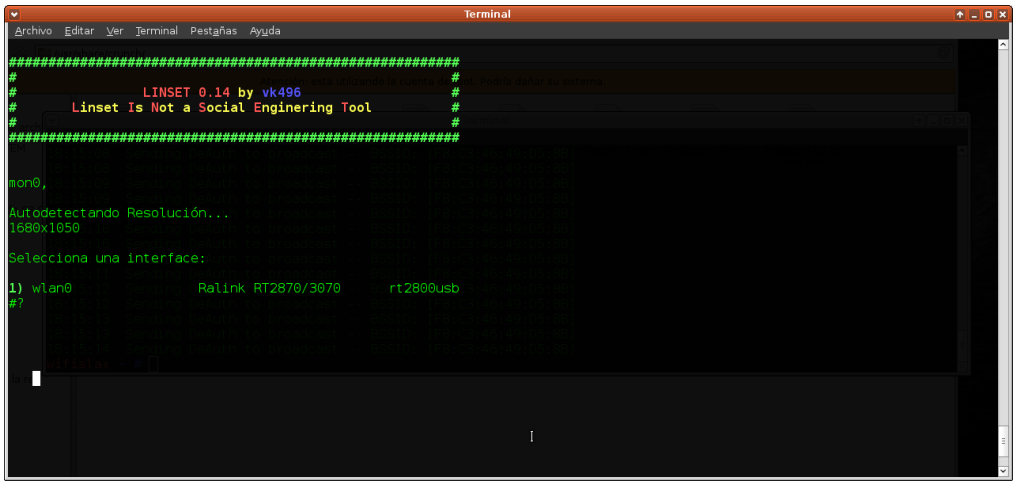
Figura 25. Ventana Principal Herramienta Linset



Fuente: El Autor

Se escoge la interfaz con la cual se procederá a realizar la auditoría, en este caso solamente hay una interfaz, wlan0, como se observa en la Figura 26, por lo cual se escoge la opción 1.

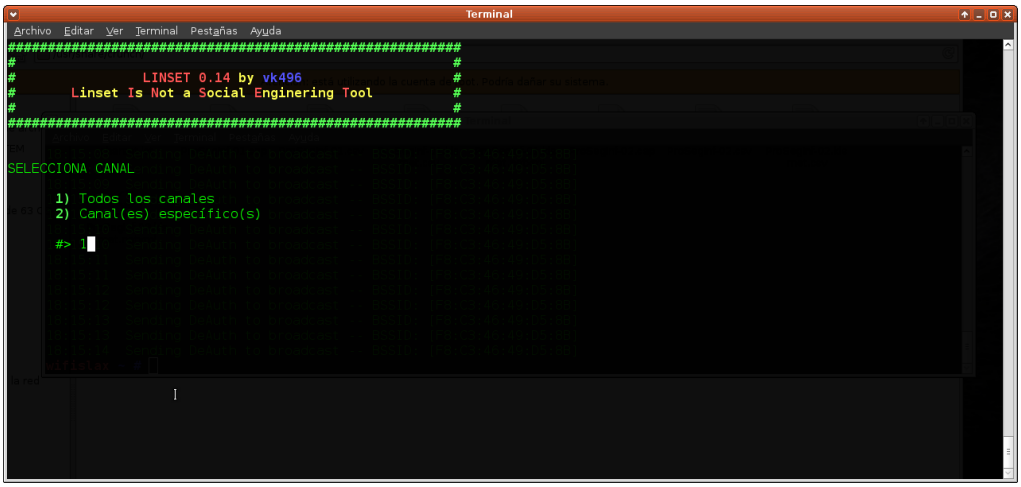
Figura 26. Escogiendo Interfaz Linset



Fuente: El Autor

Posteriormente se selecciona el canal donde se realizara la búsqueda de las redes inalámbricas al alcance de la tarjeta, como se describe en la Figura 27, para este caso seleccionamos un escaneo general, con la opción 1.

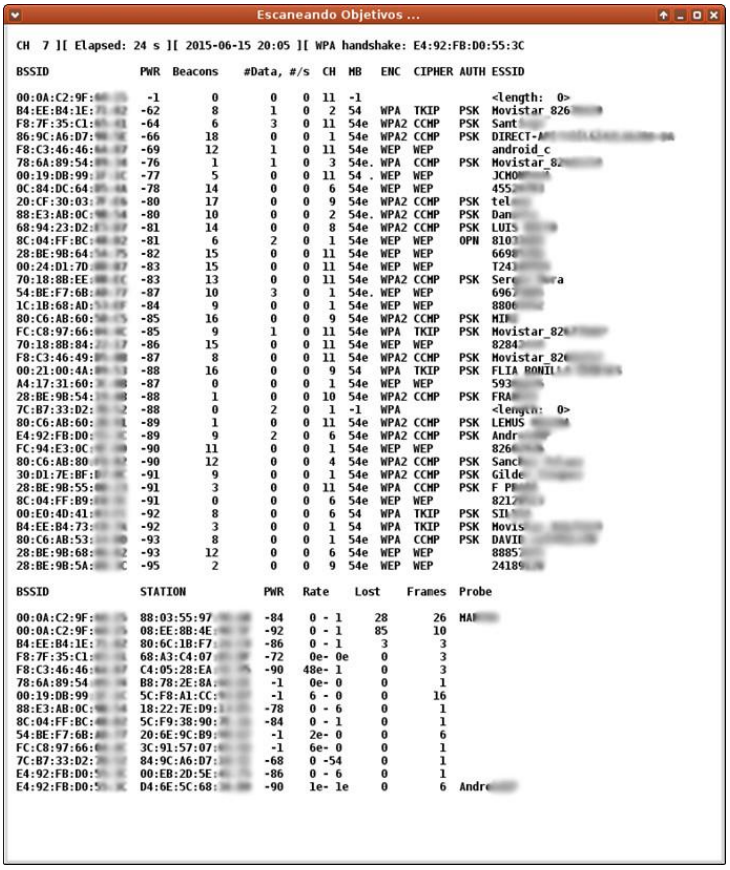
Figura 27. Seleccionando canal a auditar



Fuente: El Autor

Se observa en la Figura 28 que esta herramienta se apoya para este proceso en aircrack-ng, en este paso especifico con airodump-ng, previo comando airmon-ng para colocar la tarjeta en modo monitor, como ya se especificó anteriormente con la utilidad Crunch.

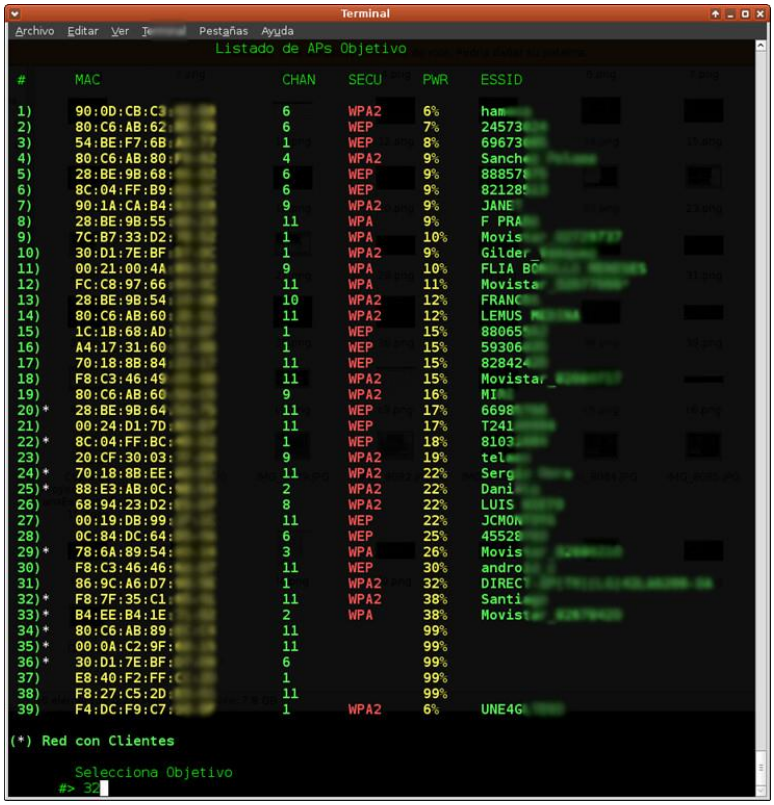
Figura 28. Listado redes encontradas por Linset



Fuente: El Autor

En una nueva ventana reseña los Puntos de Acceso disponibles y marca los que tienen usuarios conectados, como se observa en la Figura 29. Es de anotar que para que este ataque cumpla su fin necesita, básicamente, cercanía al PA y al menos usuario conectado.

Figura 29. Listado redes en Linset

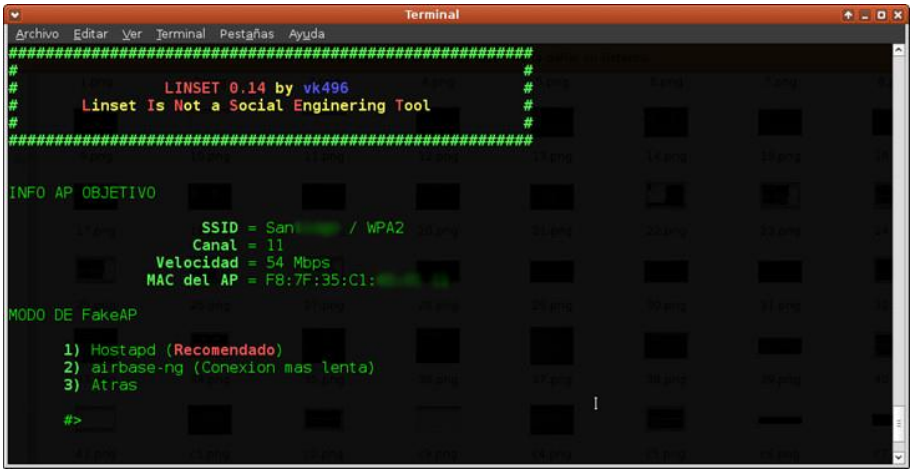


Fuente: El Autor

Una vez seleccionada la red a auditar, la herramienta solicita que Script de montaje utilizara para montar el falso Punto de Acceso, bien sea Hostapd, el cual recomienda o airbase-ng, como se observa en la Figura 30, que aunque es parte de aircrack-ng se puede presentar errores y lentitud en la conexión.

Básicamente lo que se hace en este punto es preparar el fake o rogué AP, para que los usuarios se conecten a éste y no al router.

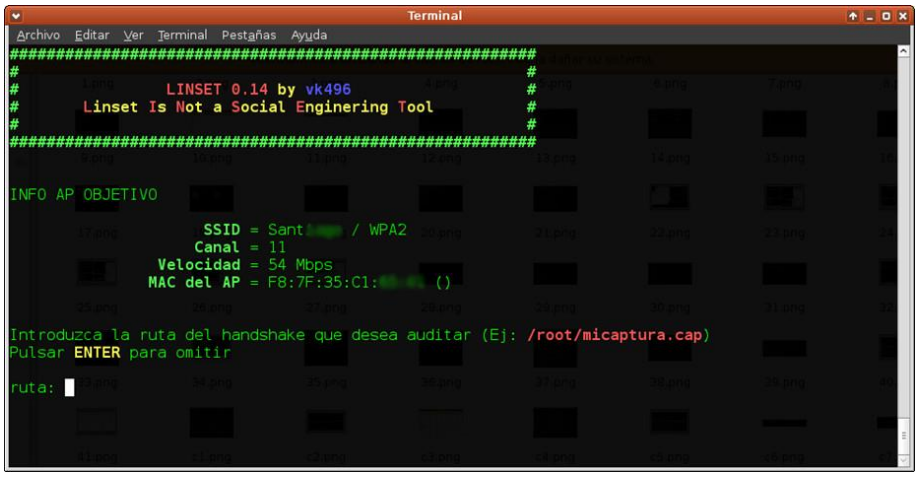
Figura 30. Fijando Objetivo con Linset



Fuente: El Autor

Seguidamente, solicita que de tener un handshake capturado de la red objetivo con anterioridad, se indique su ubicación, o sino procederá a capturarlo, como se describe en la Figura 31.

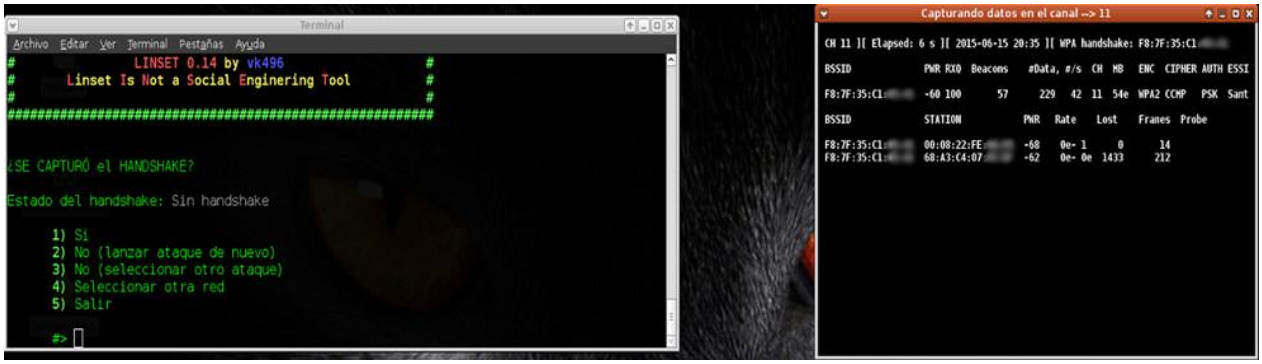
Figura 31. Buscando Handshake Linset



Fuente: El Autor

Linset procede a capturar el handshake haciendo uso de la herramienta airmon-ng, como se observa en la Figura 32, el cual servirá para comprobar si coincide con la contraseña que será escrita desde el host víctima.

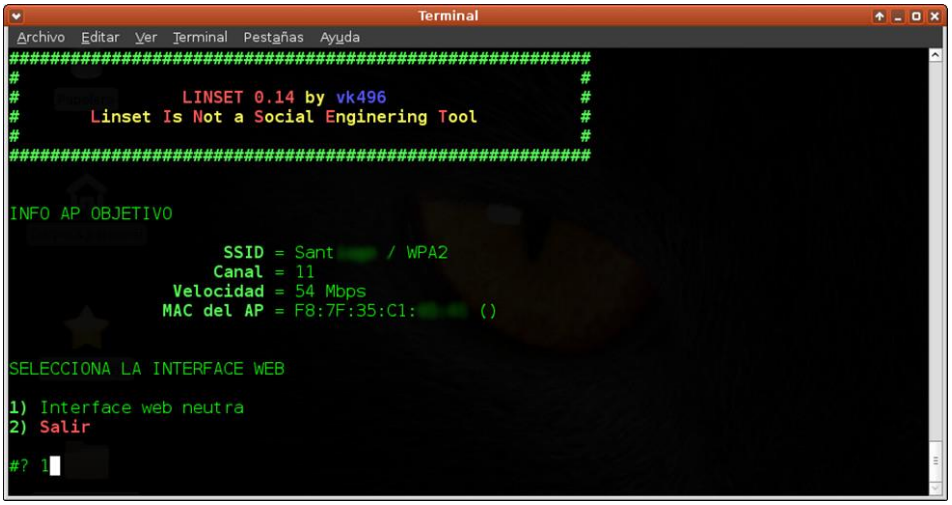
Figura 32. Capturando Handshake con LInset



Fuente: El Autor

Una vez capturado el Handshake, solicita que tipo de interfaz será presentada al usuario para que introduzca la contraseña a obtener, como se observa en la Figura 33, escogiendo La opción 1.

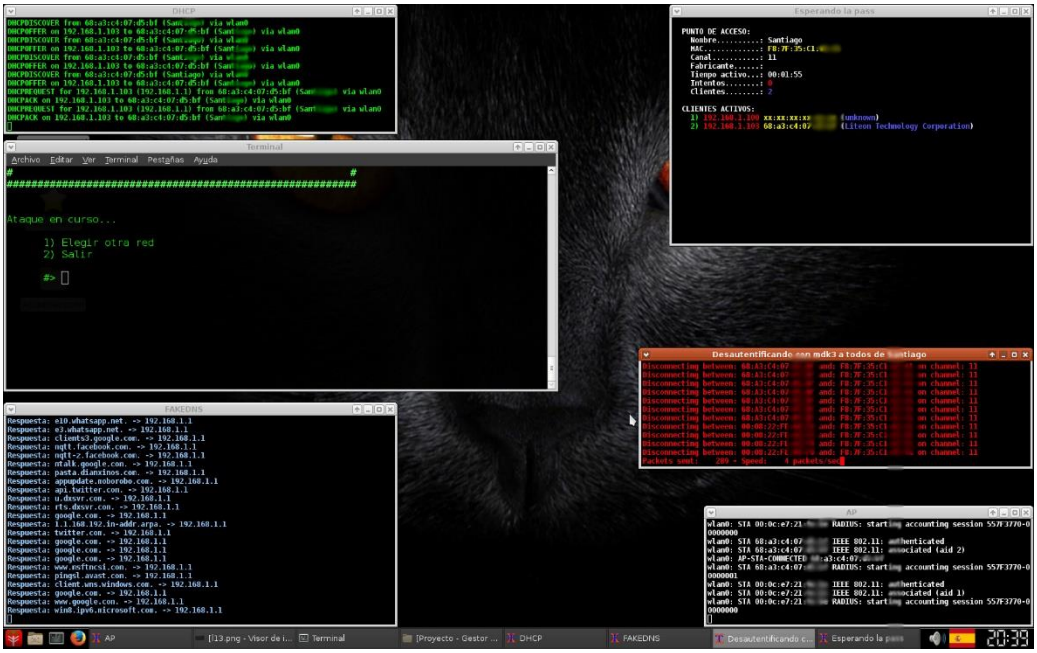
Figura 33. Escogiendo Interfaz a mostrar Linset



Fuente: El Autor

Con la información suministrada LINSET se cuenta con lo necesario para lanzar el ataque, mientras se ejecuta va indicando la situación de los servidores DHCP y DNS por ella inicializado, al igual el proceso de desautenticación que realiza de la mano de mdk3 y el estado del Punto de Acceso falso montado, como se observa en la Figura 34.

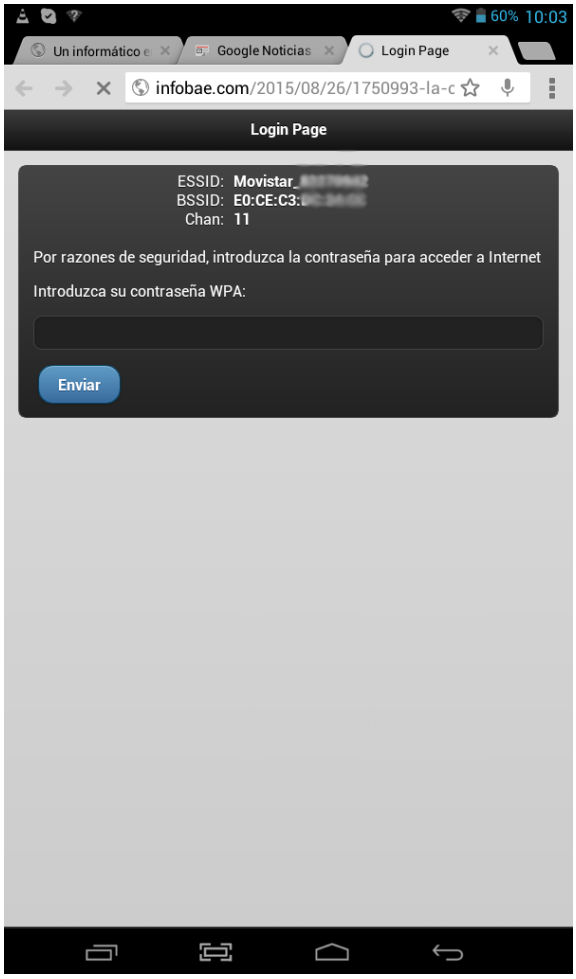
Figura 34. Atacando con Linset



Fuente: El Autor

Se describe en la Figura 35 la ventana que despliega la herramienta en el dispositivo victima para la introducción de la contraseña, en este caso una Tablet, con sistema operativo Android.

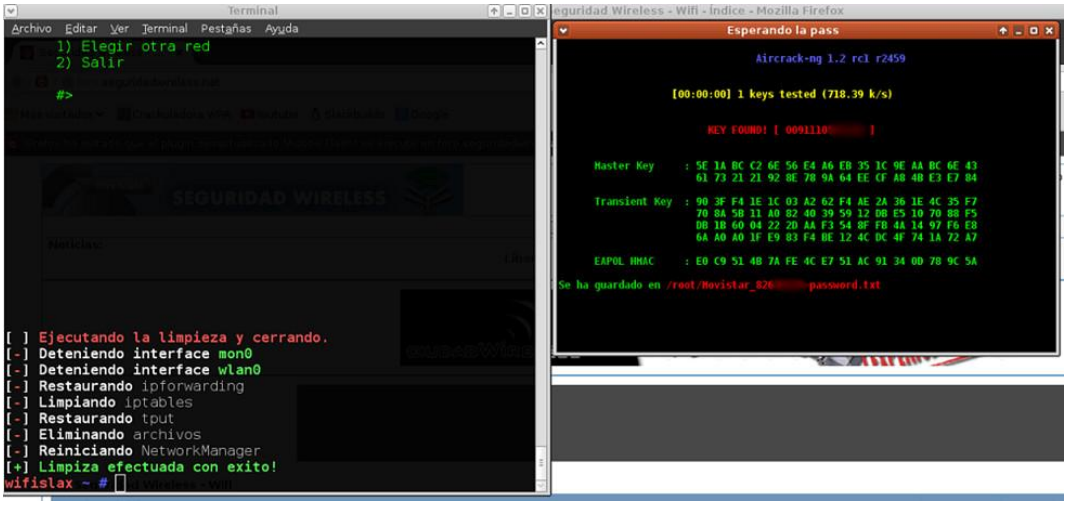
Figura 35. Ventana Emergente Linset en Host Víctima



Fuente: El Autor

El usuario ingresa una contraseña la cual se compara con el 4 way handshake capturado previamente, utilizando aircrack-ng y de ser positivo iguales arroja la contraseña WIFI del dispositivo, como se observa en la Figura 36, ventana izquierda. Posteriormente se procede a salir de la herramienta con la opción 2 como se describe en la Figura 36, ventana derecha.

Figura 36. Obteniendo la Contraseña con Linset

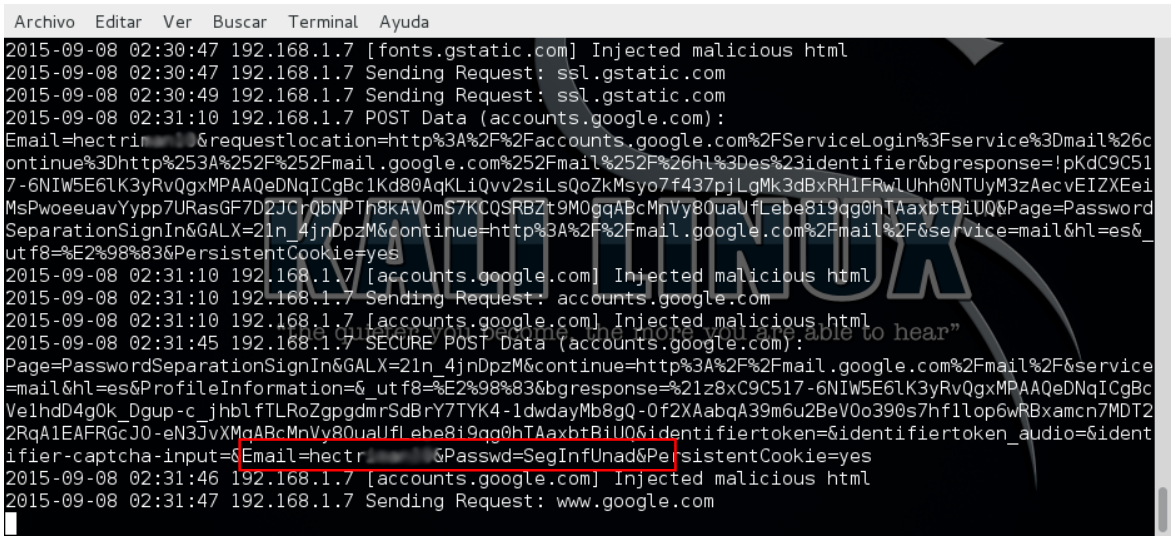


Fuente: El Autor

Por último y aunque no hace parte del presente trabajo, vale la pena agregar que, ya una vez se logra el acceso a la red, por cualquiera de los métodos expuestos anteriormente, el intruso podrá realizar una serie de ataques para tratar de conocer la información contenida en los dispositivos de la red, o bien, los datos que circulan por ella. Siguiendo con los ejemplos, podría usar herramientas de software libre como MITF, Main In The Middle Framework, combinado con BeEF, Browser Exploitation Framework, obteniendo contraseñas de sitios Web.

Se observa en la Figura 37 la herramienta MITF en ejecución, donde se resalta el momento en que captura el usuario y la contraseña ingresada en tiempo real en otro dispositivo de la red a modo de práctica.

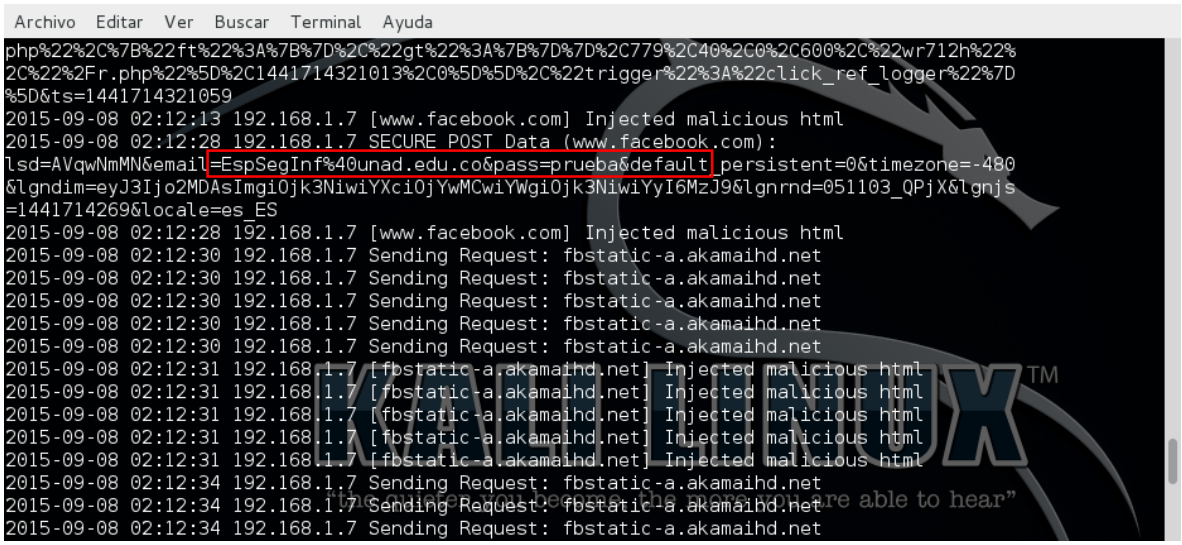
Figura 37. MITMF Capturando datos de usuario Gmail



Fuente: El Autor

Siguiendo con la prueba de concepto, el dispositivo auditado ingresa en los campos de la página de Facebook un usuario y contraseña, y nuevamente MITMF captura la información buscada, como se observa en la Figura 38.

Figura 38. Obteniendo datos de usuario con MITMF en Facebook



Fuente: El Autor

8. ANALISIS DE DATOS Y CONCLUSIONES

Durante el desarrollo del presente trabajo, específicamente en el capítulo I, se ha realizado la descripción de los sistemas de protección actuales en las redes WIFI, como son WEP, WPA y WPA2, y aunque fueron implementados desde los años 1.999,2003 y 2004, respectivamente, aún se utilizan en todas las redes inalámbricas existentes, lo cual sigue representando un riesgos para la seguridad de la información de las personas que transmiten sus datos por este medio.

Aunque WPA y WPA2, en su diseño son seguros, al momento que el proveedor de servicios de internet proporciona una clave con un patrón conocido, se vuelven vulnerables con un ataque de diccionario como se demuestra con la herramienta Crunch, o bien, por el desconocimiento de los usuarios que ingresan sus contraseñas WIFI en ventanas emergentes como ocurre con la utilidad Linset, sin la precaución de observar que en la lista de redes disponibles hay otro ESSID con seguridad abierta.

Igualmente se explica el funcionamiento del estándar WPS y aun que no es un mecanismo de seguridad de protección de redes inalámbricas, sino que fue ideado con el fin de proveer una sencilla conexión entre router y cliente, representa un hueco en la seguridad para los sistemas de protección WPA y WPA2, que en un principio son seguros, pero debido a que para ser certificados los dispositivos WPA deben tener este mecanismo, WPS, implementado al menos con el método PIN.

Se ha demostrado con el desarrollo de este trabajo, que es factible aún, vulnerar los sistemas de protección actuales de las redes 802.11, que es el objetivo principal trazado, inclusive WPA2 para obtener acceso a internet no autorizado, pero no es solamente esto, porque debe tenerse en cuenta que cualquier actividad ilícita que realicen estos intrusos dentro de la red es responsabilidad, en primera instancia, del propietario del servicio.

Además, se ha conseguido ser parte de la red local inalámbrica WLAN, lo que facilita llevar ataques a los clientes conectados a la red anfitriona, inclusive al mismo router, para conocer información personal, que dependiendo de la configuración y características de las aplicaciones instaladas en cada equipo, pueden ser a llegar efectivas, como se demuestra, brevemente, al final del capítulo III.

Por último, con el desarrollo de este trabajo se ha logrado profundizar en los fundamentos principales y las tecnologías utilizadas en las redes inalámbricas actuales, así como los diferentes métodos utilizados por personas no autorizadas para ingresar a las WIFI siendo el primer paso para lanzar ataque más sofisticado dentro de las redes LAN que podrían trasgredir la confidencialidad e integridad de los datos en tránsito y de la información contenida en cada uno de los host de la red, por tanto, es importante ahondar y hacer tomar conciencia sobre todo a las pequeñas empresas que deben endurecer su seguridad para evitar pérdidas de información, o bien hacer un esfuerzo en inversión y dejar de utilizar el sistemas de protección con clave pre compartida a uno más robusto con servidor de autenticación.

9. RECOMENDACIONES

Se recomienda que en lo posible se utilice la red cableada para el equipo de mesa y desde allí se realicen las transacciones financieras o cuando se vaya a trasmitir cualquier dato confidencial.

Lo anterior por cuanto en un principio se podría decir que el protocolo https cuando se navega por internet es seguro, pero los intrusos podrían utilizar un ataque de Hombre en Medio y enviar una página falsa idéntica a la original (Phishing) de cualquier servidor web, o bien con DNS Spoofing, obteniendo la información del usuario y la contraseña o utilizar otras técnicas basada en escaneo de puertos.

Otras recomendaciones comunes para hacer más difícil la labor de un intruso (hardening) son las siguientes:

1. Cambiar inmediatamente su sistema de protección de WEP a WPA2, de no ser posible a WPA.

2. Cambiar periódicamente la contraseña WIFI.

3. Utilizar contraseñas WIFI robustas, que incluyan, letras mayúsculas, minúsculas, números y caracteres especiales, con una longitud mayor a 7 caracteres.

4. Ocultar el SSID.

5. Desactivar, si es posible, el protocolo WPS.

6. Filtrar por dirección física e IP, con direccionamiento estático en lo posible.

7. Evitar introducir contraseñas WIFI en ventanas emergentes.

Es de anotar que una solución, tipo Enterprise, sería lo más recomendable para asegurar la red, para lo cual se podría implementar Free Radius, que necesitaría básicamente como hardware adicional un equipo que funcione como servidor y el

conocimiento para la configuración de las aplicaciones necesarias dentro del mismo, por cuanto la mayoría de los routers son compatibles con esta tecnología.

Básicamente la solución Free Radius consiste en que el router se enlaza a un host que tiene instalado el software freeradius, previamente configurado y realiza la labor de servidor RADIUS, Remote Authentication Dial-In User Server, que es un protocolo AAA (Authentication, Authorization and Accounting) y que conoce el usuario y contraseña de cada cliente.

Con Radius cuando un usuario desea ingresar a la red debe digitar el usuario y la contraseña, única para ese dispositivo, la cual es enviada al router, el cual anteriormente debió ser configurado para utilizar RADIUS y quien envía estos datos al servidor, si son inválidos no autoriza la conexión, pero de ser legítimos, le informa al router para que proceda a permitir la conexión de este usuario.

Aunque éste protocolo RADIUS es el más recomendado, como se sabe, en seguridad, no existen medidas 100% seguras y como en el caso de WPA y WPA2, las vulnerabilidades no están relacionadas directamente con los protocolos sino por la naturaleza de las mismas redes inalámbricas.

Por lo comentado anteriormente, con ataques más elaborados, se podría suplantar la red legítima con otra y engañar a los clientes para que revelen su contraseña y usuario, utilizando un fake ap similar como se utiliza la herramienta Linset.

BIBLIOGRAFIA

AIRCRACK-NG. Mapa Conceptual Wep Cracking [en línea]. <http://www.aircrack-ng.org/doku.php?id=es:flowchart> [citado en 20 de febrero de 2015]

AIRCRACK-NG. Descripción [en línea]. <http://www.aircrack-ng.org/doku.php?id=es:aircrack-ng> [citado en 22 de febrero de 2015]

AIRCRACK-NG.Aireplay-ng [en línea]. <http://www.aircrack-ng.org/doku.php?id=es:aireplay-ng> [citado en 22 de febrero de 2015]

AIRCRACK-NG.Airodump-ng [en línea]. <http://www.aircrack-ng.org/doku.php?id=es:airodump-ng> [citado en 28 de febrero de 2015]

AIRCRACK-NG. Guía Para Novatos de Aircrack-ng en Linux [en línea]. <http://www.aircrack-ng.org/doku.php?id=es:newbie_guide#conocimientos_basicos_ieee_80211> [citado en 22 de febrero de 2015]

AIRCRACK-NG. Tutorial: Como crackear WPA/WPA2 [en línea]. <www.aircrack-ng.org/doku.php?id=es:cracking_wpa> [citado en 22 de febrero de 2015]

ALVAREZ MENDEZ, Yelitza Pastora, Seguridad Al Acceso De Información En La Implantación De Una Red Inalámbrica, Caracas, 2006. 98p. Trabajo de Grado (Especialista en Comunicaciones) Universidad Central de Venezuela. Facultad de Ingeniería. Consultado En: <http://saber.ucv.ve/xmlui/bitstream/123456789/2420/1/Tesis%20yelitza%20Alvarez.pdf>

SABOGAL ROZO, Esther Angélica. Proyecto de Seguridad Informática I. Bogotá: Universidad Nacional Abierta y A Distancia, 2013. 54p.

SERRANO FLORES, Andrés Guillermo. Análisis de Vulnerabilidades de Seguridades en Redes Inalámbricas dentro un Entorno Empresarial que Utilizan Cifrado AES y TKIP, WPA y WPA2 Personal del DMQ, Quito, 2011. 132p. Trabajo de Grado (Ingeniero de Sistemas). Ponticia Universidad Católica del Ecuador. Facultad de Ingeniería. Consultado En:

<http://repositorio.puce.edu.ec/bitstream/22000/4642/1/TESIS%20-%20PUCE%204479.pdf>

VALLEJO DE LEON, Tatiana Violeta, Vulnerabilidades Y Niveles De Seguridad De Redes WI-FI. Guatemala, 2010, 116p. Trabajo de grado (Ingeniera de Sistemas). Universidad de San Carlos. Facultad de Ingeniería. Consultado En:<http://biblioteca.usac.edu.gt/tesis/08/08_0266_EO.pdf>

WIFISLAX. Guía Básica [en línea]. <http://www.wifislax.com/guia-basica/> [citado en 28 de febrero de 2015]