UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

WIRELESS HACKING, PROTEGIDO CON IDS, FIREWALLS Y HONEYPOTS

Estudiante

Miguel Francisco León Jaramillo

Tutor

Ing. Diego Fajardo

Cuenca Ecuador

2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Diego Fajardo., certifico que el señor Miguel Francisco León Jaramillo con C.C, No. 010285470-0 realizó la presente tesis con el título **"Wireless hacking, protegiendo con idss firewalls y honeypots"**, y que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Diego Fajardo

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, Miguel Francisco León Jaramillo, con C.C. Nº. 0102854700, estudiante de la carrera de Sistemas Informáticos, declaro conocer y aceptar las disposiciones del Programa de Pregrado, que en lo pertinente dice: *"Es patrimonio de la Universidad Tecnológica Israel, todos los resultados provenientes de trabajos investigativos, científicos o técnicos o tecnológicos, o productos tangibles y de tesis o trabajos de grado que se realicen a través o con el apoyo de cualquier tipo de la Universidad de Tecnológica Israel, esto significa la cesión de los derechos de propiedad intelectual a la Universidad Tecnológica Israel".*

_____

Miguel Francisco León J.

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

El documento de tesis con título **"Wireless hacking, protegiendo con idss firewalls y honeypots"** ha sido desarrollado por Miguel Francisco León Jaramillo con C.C, No. 010285470-0 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Miguel Francisco León Jaramillo

DEDICATORIA

La presente Tesis de Grado la dedico a mi esposa Fanny a mi hijo Eduardo y a mis Padres: quienes que con su amor, paciencia, comprensión y apoyo me han dado fuerzas para poder cumplir con otra etapa de la vida. Que este esfuerzo sirva de ejemplo para mi hijo para que cada meta que se lo proponga en la vida la cumpla a cabalidad sin rendirse por ningún motivo ni deje las cosas a medias.

AGRADECIMIENTO

Les agradezco a mis profesores que brindándome su amistad, paciencia, apoyo y lo más importante sus conocimientos. Además agradezco de forma muy especial a mi tutor el ingeniero Diego Fajardo, persona que ha brindado su amistad sincera y un gran apoyo para poder me guiar el en desarrollo de esta tesis.

RESUMEN

La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). **Wi-Fi** (que significa "Fidelidad inalámbrica", a veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la certificación

La capa física (a veces abreviada capa "PHY") ofrece tres tipos de codificación de información.

- La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red. En realidad, el estándar 802.11 tiene tres capas físicas que establecen modos de transmisión alternativos

SUMARY

The IEEE 802.11 specification (ISO / IEC 8802-11) is an international standard that defines the characteristics of a wireless local area network (WLAN). Wi-Fi (which stands for "Wireless Fidelity", sometimes incorrectly abbreviated Wi-Fi) is the name of the certification by the Wi-Fi Alliance, formerly WECA (Wireless Ethernet Compatibility Alliance), a group that ensures compatibility between devices that use the 802.11 standard. On the misuse of the terms (and for marketing reasons) the name of the standard is often confused with the name of the certification.

The physical layer (sometimes abbreviated layer "PHY") offers three types of encoding information.

• The data link layer consists of two sub layers: Logical Link Control (LLC) and media access control (MAC).

The physical layer defines the modulation of radio waves and signaling characteristics for the transmission of data while the data link layer defines the interface between the team bus and the physical layer, including an access method similar to used in the Ethernet standard and rules for communication between network stations. In fact, the 802.11 standard has three physical layers that establish alternative modes of transmission

Tabla de contenido

LISTA DE CUADROS Y GRÁFICOS

CAPITULO I

1.1 ANTECEDENTES

Redes y Comunicación Inalámbrica

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

Tiempo después, se introdujeron equipos de respuesta automática que hicieron posible el uso de redes telefónicas públicas conmutadas para realizar las conexiones entre las terminales y la computadora.

A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito, como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía. Se analizaron las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo del grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

Se puede ubicar la primera Red de área local, la red WLAN (Wireless Local Area Network) en una industria suiza, donde se obtuvieron los primeros resultados satisfactorios de comunicación inalámbrica dentro de una red local. A partir de allí, se han impulsado notablemente las investigaciones, y se han desarrollo ampliamente dispositivos que han hecho posible el auge que disfrutan hoy en día las redes inalámbricas.

Por otra parte cabe mencionar que, el físico alemán Heinrich Rudolph Hertz en 1887, anunció que existían las ondas electromagnéticas y que éstas podrían ser usadas para enviar y recibir información a muy grandes distancias.

La base teórica de las ondas electromagnéticas fue desarrollada en 1864 por el físico escocés James Clerk Maxwell. Las ondas electromagnéticas fueron usadas por primera vez en la telegrafía inalámbrica. Este relevante acontecimiento sería el predecesor de la propagación electromagnética o transmisión de radio.

Estudiando y desarrollando estas nociones, el italiano Guglielmo Marconi inventó la radio en 1901. La radio fue el primer medio masivo de comunicación inalámbrica, y a poco más de 100 años de su invención, las comunicaciones móviles han demostrado ser una alternativa a las redes cableadas, al ofrecer beneficios como la movilidad y la localización[1].

Gracias a la comunicación inalámbrica podemos estar comunicados en cualquier lugar y en cualquier momento.

1.2 FORMULACIÓN DEL PROBLEMA

En la actualidad, un gran número de empresas poseen conexiones de red con cableado, lo que ocasiona dificultades en el desarrollo del trabajo, en zonas de difícil acceso. Por estas razones, hoy en día se implementa la utilización de tecnología WI-FI. Cuando se activan las medidas de seguridad en los aparatos WI-FI, se utiliza un protocolo de encriptación débil, como WEP (Protocolo de equivalencia con red cableada).

[1] Nieves, A. Redes y Comunicación Inalámbrica. Recuperado el 08 de septiembre del 2011, de http://www.ilustrados.com/tema/8666/Redes-Comunicacion-Inalambrica.html

Al examinar las debilidades de WEP se observa que es sencillo crackear el protocolo. Lamentable la inadecuación de WEP resalta la necesidad de una nueva arquitectura de seguridad en el estándar 802.11, por lo que se analizará la puesta en práctica de WPA y WPA2 junto a sus primeras vulnerabilidades menores y su integración en los sistemas operativos

1.3 SISTEMATIZACIÓN

1.3.1 DIAGNÓSTICO

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes, sin proteger la información que por ellas circulan.

La protección que se utiliza de manera general en las redes wireless es WEP, la misma que posee dos niveles de cifrados, de 64 y 128. Estos niveles son fácilmente vulnerables a ser descifrados por terceros.

DIAGRAMA CAUSA - EFECTOS

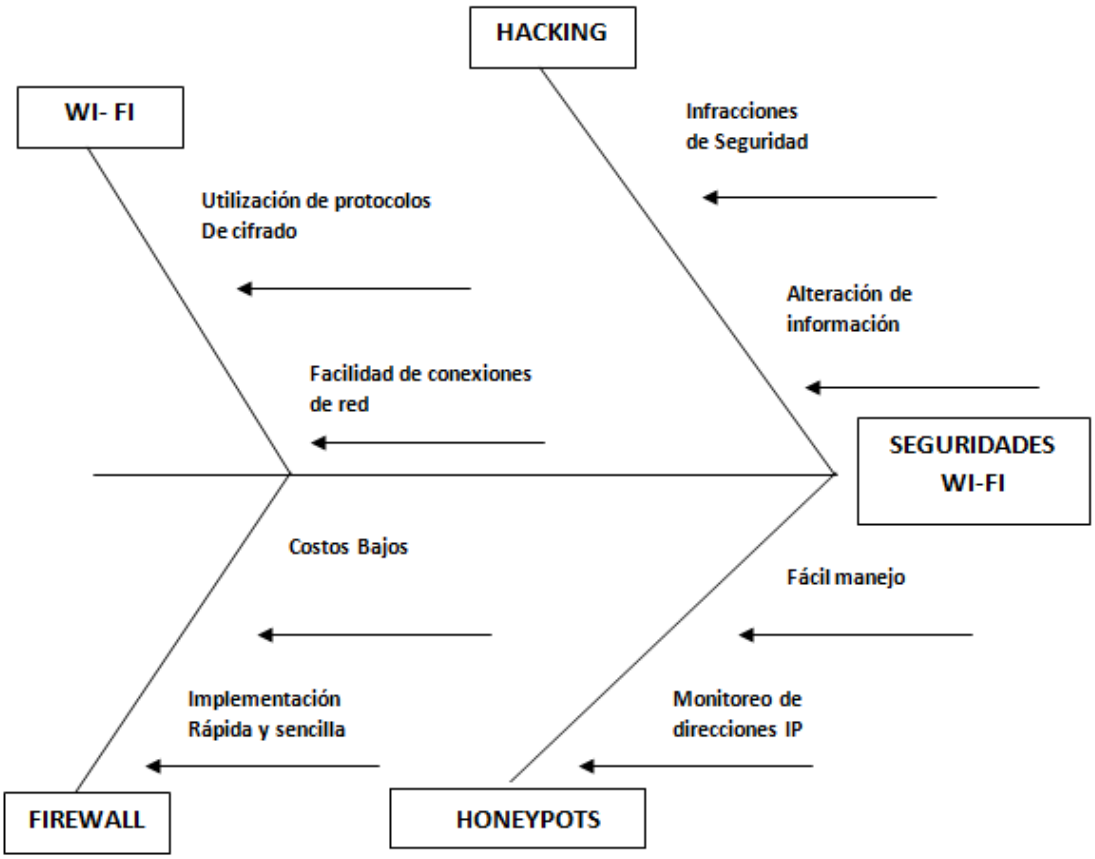

Fig. 01 Diagrama Causa - Efecto

1.3.2 PRONÓSTICO

Al no cambiar la tecnología WEP a la tecnología WAP, las empresas van a seguir asumiendo ataques en sus redes y perjudicándolas.

Las redes inalámbricas inundan cada vez más todo el entorno, sin tener en cuenta ni valorar la inseguridad del medio. Éste suele ser el vector de ataque utilizado para vulnerar e interceptar datos de redes internas, tanto de PYMES como de grandes empresas.

1.3.3 CONTROL PRONÓSTICO

Las redes inalámbricas o Wi-Fi ofrecen mayor comodidad que las redes cableadas, debido a que cualquier usuario que tenga acceso a la red puede conectarse desde distintos puntos dentro de un amplio rango de espacio. Además una vez configuradas, permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.

Pero al implementar redes Wi-Fi se debe considerar utilizar protocolos de cifrado de datos como el WPA o el WPA2, que se encargan de codificar la información transmitida para proteger su confidencialidad. Estos cifrados son propios de los dispositivos inalámbricos y su manipulación es sencilla de aplicar

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Analizar los cifrados (WEP, WAP y WAP2) y softwares (IDS y Honeypots) de seguridad de autenticación de las redes Wi-Fi y determinar la vulnerabilidad de ataque de las redes Wi-Fi que cuentan con cifrado WEP.

.

1.4.2 OBJETIVOS ESPECÍFICOS

- Determinar las falencias que presenta el protocolo WEP de seguridad de las redes inalámbricas o Wi-Fi, a través de la aplicación del programa Backtrack, a una red doméstica.
- Valorar las fortalezas que presentan los cifrados de seguridad WAP y WAP2.
- Analizar los software IDS y Honeypots, como opciones de protección a ataques externos a redes inalámbricas

1.5 JUSTIFICACIÓN

Hoy en día para el conjunto de organizaciones es una necesidad básica contar con una red que permita disponer de acceso a Internet. Actualmente un gran número de organizaciones (pymes, empresas, oficinas, hogares, etc.) para suplir esta necesidad, han optado por instalar redes inalámbricas, debido a las ventajas que este tipo de redes proporcionan. Las principales ventajas que se pueden destacar son el bajo costo de infraestructura y cableado, pero sobretodo la comodidad de acceso y uso (movilidad, desplazamiento, flexibilidad). Sin embargo, las redes inalámbricas, más conocidas como Wi-Fi, también presentan varios problemas, los más importantes mantienen relación directa con el tema de “Seguridad”.

El presente trabajo tiene como fin presentar los cifrados (WEP, WAP y WAP2) y softwares (IDS y Honeypots) de seguridad de autenticación de las redes Wi-Fi, analizarlos y evidenciar la vulnerabilidad que posee la tecnología WEP, que es el cifrado de autenticación más utilizado actualmente en las redes inalámbricas.

Con el análisis del presente trabajo, se pretende demostrar la necesidad de cambio de la tecnología WEP a la tecnología WAP, con el objeto que las organizaciones que utilizan las redes inalámbricas o Wi-Fi, incrementen su nivel de seguridad, al implementar mecanismos que protejan a la red inalámbrica del acceso de usuarios no autorizados, permitiendo que los usuarios autorizados accedan de forma cómoda y segura. Alcanzando así, el hecho de evitar ser víctimas de ataques y perjuicios.

1.5.1 TEÓRICA

Las redes Wi-Fi son importantes, porque buscan proponer una solución al problema existente sobre redes no portátiles y, respaldar las cualidades que tienen las redes inalámbricas en la cobertura, como son:

Movilidad. La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un computador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red, sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio.

No es necesario estar atado a un cable para: navegar en Internet, imprimir un documento, acceder a los recursos compartidos desde cualquier lugar, o hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficiente mente largo.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que se puede desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edifico.

Flexibilidad. Las redes inalámbricas no solo permiten estar conectados mientras se desplaza de un sitio a otro con una computadora portátil, sino que también permite conectar una computadora en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones se colocan peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas.

Resultan también apropiadas para aquellos lugares en los que se necesitan accesos esporádicos. Es una alternativa mucho más viable que las redes cableadas.

Ahorro de costos. Diseñar o instalar una red cableada puede llegar a alcanzar un alto costo, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales, donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costos al permitir compartir recursos: acceso a Internet, impresoras, etc.

Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial.

Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esta tarea, requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede tomar a la ligera o descuidar, debido a que las transmisiones viajan por un medio no seguro. Por este motivo es necesario contar con mecanismos que aseguren la confidencialidad de los datos, así como su integridad y autenticidad.

La autenticación es el proceso de verificar y asegurar la identidad de las partes involucradas en una transacción. Si este servicio no se llevara a cabo cabe la posibilidad de que una entidad desconocida asuma una identidad falsa, comprometiendo de esta manera la privacidad y la integridad de la información. En el contexto de las redes LAN, la

autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas[2].

1.6 ALCANCES Y LIMITACIONES

1.6.1 ALCANCES

La presente tesina tiene como alcance realizar el análisis de la vulnerabilidad del cifrado de seguridad WEP, efectuando una aplicación práctica del software Backtrack a una red inalámbrica doméstica privada, y presentar un manual de la aplicación del mencionado software.

Por otra parte, se efectuará una valoración de las fortalezas que presentan los cifrados de seguridad WAP y WAP2, y las ventajas de los softwares IDS y Honeypots, como opciones de protección a ataques externos a redes inalámbricas, a través de un análisis bibliográfico

1.6.2 LIMITACIONES

La presente tesina se limita a realizar exclusivamente un análisis bibliográfico sobre los cifrados WAP y WAP2, y los programas IDS y Honeypots, sin efectuar una aplicación demostrativa/práctica de los mismos.

1.7 ESTUDIOS DE FACTIBILIDAD

1.7.1 FACTIBILIDAD TÉCNICA

Las redes inalámbricas no requieren cables para establecer la conexión, sino que usan ondas de radio como los teléfonos inalámbricos. La ventaja

[2] Filip, A., y Vásquez, E. (2000). Seguridades en redes WiFi Eduroam. Sevilla: Universidad de Sevilla.

de la red inalámbrica radica en la movilidad y libertad que brinda en comparación con las restricciones propias de los cableados y las conexiones fijas. Las ventajas de una red inalámbrica incluyen:

- Movilidad y libertad para trabajar y entretenerse en cualquier lugar.
- Sin restricciones de cables o conexiones fijas.
- Instalación rápida y fácil “no es necesario realizar perforaciones”.
- No es necesario comprar cable
- Ahorro del tiempo y el esfuerzo que demanda la instalación del cableado.
- Facilidad de expansión

Las redes inalámbricas permiten utilizar las computadoras en cualquier lugar del hogar o la oficina. Permiten consultar el correo electrónico o navegar por internet, e imprimir en una impresora que se encuentre en otra habitación. No hay necesidad de realizar perforaciones en la pared para colocar cables Ethernet, porque puede conectarse desde cualquier lugar sin usar cables.

Fuera del hogar, las redes inalámbricas están disponibles en sitios de acceso público como cafeterías, empresas, habitaciones de hotel y aeropuertos, lo que resulta ideal para las personas que viajan con frecuencia.

1.7.2 FACTIBILIDAD OPERATIVA

La instalación y configuración del equipo en una red inalámbrica es mucho más rápida y sencilla que instalar un nuevo punto de red para una red cableada.

Con la amplia variedad de redes inalámbricas y las posibles configuraciones, se puede instalar redes inalámbricas fácilmente con cualquier presupuesto, y después ir ampliándola cuando el presupuesto lo permita, o la empresa lo requiera.

Razones para instalar redes inalámbricas:

- Ofrecer a los clientes la posibilidad de conectase a la red si le resulta necesario.
- Posibilidad de trabajar cuando, como y donde se necesite.
- Reducción del costo total e inicial. Las redes inalámbricas se pueden instalar poco a poco, según las necesidades o el presupuesto.
- Las redes inalámbricas son una opción adecuada para las PYMES con un presupuesto ajustado.
- Cualquier usuario autorizado en una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios e inclusive sobre áreas metropolitanas a velocidades de 11Mbit/s, o superiores.
- La mayoría de los fabricantes de ordenadores y equipos como PDAs, TPVs y otros dispositivos ya han adaptado sus productos a las tecnologías inalámbricas, por lo que se abarata las instalaciones de las redes Wi-Fi.

CAPITULO II

MARCO DE REFERENCIA

2.1. MARCO TEÓRICO

2.1.1 WI-FI

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuera compatible entre los distintos aparatos (si bien técnicamente no es difícil transmitir información de manera inalámbrica, es necesario ponerse de acuerdo entre fabricantes para que el protocolo de comunicación sea universal, de tal manera de poder interpretar esta información de manera coherente en diferentes equipos).

En busca de esa compatibilidad fue que en 1999 las empresas 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se reunieron para crear la Wireless Ethernet Compability Aliance (WECA), actualmente llamada Wi-Fi Alliance.

2.1.2 COMUNICACIÓN INALÁMBRICA

La comunicación inalámbrica o sin cables es aquella en la que extremos de la comunicación (emisor/receptor) no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio. En este sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, entre los cuales encontramos: antenas, computadoras portátiles, PDA, teléfonos móviles, etc.

WIRELESS (inalámbrico o sin cables) es un término usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas (en vez

de cables) llevan la señal sobre parte o toda la trayectoria de la comunicación. Algunos dispositivos de monitorización, tales como alarmas, emplean ondas acústicas a frecuencias superiores a la gama de audiencia humana; éstos también se clasifican a veces como wireless.

Los primeros transmisores sin cables vieron la luz a principios del siglo XX usando la radiotelegrafía (código Morse). Más adelante, como la modulación permitió transmitir voces y música a través de la radio, el medio se llamó radio. Con la aparición de la televisión, el fax, la comunicación de datos, y el uso más eficaz de una porción más grande del espectro, se ha resucitado el término wireless.

2.2. MARCO ESPACIAL

La presente tesina a realizar es enfocada para cualquier tipo de empresa que lo desee aplicar. Generando una concientización de seguridades wireless, la cual se encargan en proteger los procesos y la información, al no mantener una buena seguridad en las instituciones será difícil neutralizar los ataques.

2.3. MARCO TEMPORAL

Al implementar configuraciones inalámbricas el tiempo será de dos meses ya que en este tiempo debemos tener en cuenta las tres diferentes tipos de protección de las redes wireless

CAPITULO III

METODOLOGÍA

Para desarrollar una configuración de redes inalámbricas es factible llevare a cabo una investigación Descriptiva la cual consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades por lo cual nos permite conocer el análisis e interpretación de la información del medio actual.

3.1. ETAPAS DE LA INVESTIGACIÓN DESCRIPTIVA

- Examinar las características del problema escogido.
- Elegir temas y las fuentes apropiadas.
- Seleccionar o elaborar técnicas para la recolección de datos.
- Establecer, a fin de clasificar los datos, categorías precisas, que se adecuen al propósito del estudio y permitan poner de manifiesto las semejanzas, diferencias y relaciones significativas.

3.1.1. UNIDAD DE ANÁLISIS

Esta investigación tendrá como unidad de análisis las normas para análisis al wireless hacking de acuerdo al software de desencriptación

3.1.2. MÉTODOS

El método que se aplicará en el desarrollo de la presente tesina es el método deductivo, ya que se partirá de los conceptos sobre los diferentes cifrados de seguridad aplicados sobre las redes inalámbricas, para extraer como conclusiones las falencias que presenta el cifrado usado comúnmente, frente a las virtudes de otros códigos de protección. Y

finalmente examinar a través de una demostración práctica las vulnerabilidades específicas del cifrado WEP.

3.1.3. TÉCNICAS

La técnica de investigación a utilizar en la presente tesina, es la técnica bibliográfica, ya que la información base se obtendrá de fuentes bibliográficas como libros, papers, revistas, etc.

CAPITULO IV

DESARROLLO

4.1. WI-FI

4.1.1. ¿QUÉ ES WI-FI?

Wi-Fi (Wireless Fidelity) es un conjunto de estándares de la IEEE 802.11 (especialmente la 802.11b) que son redes inalámbricas basadas en las especificaciones, creadas para redes locales inalámbricas, las cuales se utilizan para acceso a internet y redes privadas.

El término Wi-Fi fue dado por la Wi-Fi Alliance, los que ha testeado y aprobado el nombre de "Wi-Fi Certified". Los equipos que llevan este nombre son los únicos que garantiza su interoperabilidad.

4.1.2. ESTÁNDARES QUE CERTIFICA WI-FI

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11. En la tabla a continuación se describen los estándares que certifican Wi-FI:

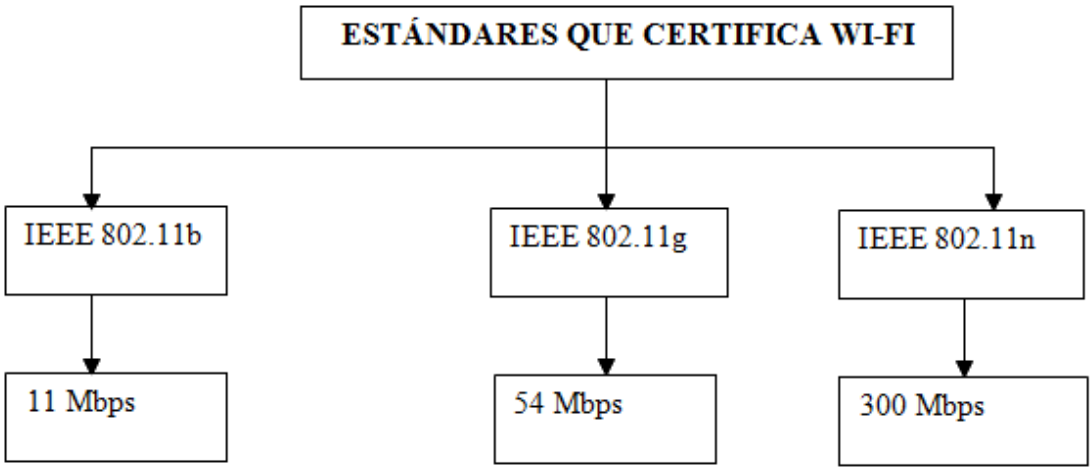

Tabla 01 Estándares WI-Fi

En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WI-FI5, que opera en la banda de 5 GHz y que goza de una operatividad con unos canales relativamente limpios.

La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

4.1.3. VENTAJAS DE LAS REDES WI-FI

La principal ventaja que supone una red Wireless frente a una de cables, es la movilidad.

En la actualidad, muchos usuarios y empleados de empresas requieren para sus tareas acceder en forma remota a sus archivos, trabajos y recursos. La red Wireless permite hacerlo sin realizar ninguna tarea compleja de conexión o configuración, y evita que cada usuario viaje hasta su empresa o su casa para poder acceder a los recursos de su red de datos.

En síntesis, las redes inalámbricas a diferencia de sus antecesoras son:

- Más simples de instalar.
- Escalables muy fácilmente
- Menos complejas en su administración.

El hecho de que no posean cables, nos permite adaptarlas a casi cualquier estructura, y prescindir de la instalación de pisos técnicos y la instalación de cables molestos que crucen oficinas, habitaciones, etc.

A través de esta tecnología, puede disponerse de conexión a Internet casi en cualquier lugar donde se cuente con tal servicio y, de esta forma, también a todas las ventajas que ofrece la Red de redes respecto de lo que es comunicación e información.

4.1.4. DESVENTAJAS DE LAS REDES WI-FI

En este punto se describe algunas de las desventajas más notorias que acarrea la instalación de una red Wireless.

La primera de ellas es la velocidad. Hasta el momento las redes Wi-Fi no superan la velocidad de 54 Mbps, mientras que las redes cableadas ya llegaron hace unos cuantos años a los 100 Mbps.

Otra desventaja es la seguridad. Muchas redes Wireless sufren accesos no debidos, debido a la inexperiencia de quienes las instalaron y no configuraron correctamente los parámetros de seguridad. Lo que puede ocasionar que las redes sean invadidas por usuarios externos, quienes pueden acceder a las redes hasta con dispositivos de menor jerarquía, como por ejemplo Palms, PDA o pequeños dispositivos portátiles. Por la razón descrita, es imprescindible cumplir en la configuración de este tipo de redes con una serie de requisitos mínimos e indispensables concernientes a la seguridad.

Otro punto débil presente en las redes Wireless consiste en su propensión a interferencias. Debido al rango de señal en el cual trabajan (en su mayoría en los 2,4 GHz) suelen ser interferidas por artefactos de uso

común en cualquier casa u oficina, como teléfonos inalámbricos, que utilizan ese mismo rango de comunicación.

4.1.5. ¿CÓMO FUNCIONA LO INALÁMBRICO?

Para transportar la información de un punto a otro de la red sin necesidad de un medio físico, se utilizan ondas de radio. Al hablar de ondas de radio, nos referimos normalmente a ondas portadoras de radio sobre las que se transporta la información (trasladando la energía a un receptor remoto).

La transmisión de datos entre dos computadoras se realiza por medio de un proceso conocido como modulación de la portadora. El aparato transmisor agrega datos a una onda de radio (onda portadora). Esta onda, al llegar al receptor, es analizada por éste, el cual separa los datos útiles de los inútiles.

Una frecuencia de radio es la parte del espectro electromagnético donde se generan ondas electromagnéticas mediante la aplicación de corriente alterna a una antena. Si las ondas son transmitidas a distintas frecuencias de radio, varias ondas portadoras pueden existir en igual tiempo y espacio sin interferir entre sí, siempre que posean una frecuencia distinta. Para extraer los datos, el receptor debe situarse en una determinada frecuencia (frecuencia portadora) e ignorar el resto.

4.2. WEP *(*Wired Equivalent Privacy *o* Privacidad Equivalente a Cableado*)*

4.2.1. ¿QUÉ ES WEP?

Tabla 02 El WEP

Una encriptación **WEP** (*Wired Equivalent Privacy* o *Privacidad Equivalente a Cableado*) es un tipo de cifrado, implementado en el protocolo de conexión Wifi 802.11, que se encarga de cifrar la información que vamos a transmitir entre dos puntos de forma que solo la sea posible tener acceso a ellos e interpretarlos a aquellos puntos que tengan la misma clave.

En general, un router Wifi o un Access Point solo va a permitir el acceso a aquellos terminales que tengan la misma clave de encriptación WEP.

Esta clave puede ser de tres tipos:

- **Clave WEP de 64 bits.-**, 5 Caracteres o 10 dígitos hexadecimales ("0 a 9" "A a F", precedidos por la cadena "0x").
- **Clave WEP de 128 bits.-**, 13 Caracteres o 26 dígitos hexadecimales ("0 a 9" "A a F", precedidos por la cadena "0x").

- **Clave WEP de 256 bits.-**, 29 Caracteres o 58 dígitos hexadecimales ("0 a 9" "A a F", precedidos por la cadena "0x").

La que más se suele usar es la de 128 bits, que ofrece un bien nivel de protección sin ser excesivamente larga y complicada.

La encriptación WEP de 256 bits no es soportada por muchos dispositivos.

Una clave de encriptación **WEP** se puede descifrar (existen programas para ello), pero para esto es necesario un tráfico ininterrumpido de datos durante un tiempo determinado (bastantes datos y bastante tiempo).

Evidentemente, cuanto mayor sea el nivel de encriptación y más complicada sea la clave más difícil va a ser de descifrar.

No se tarda lo mismo (a igualdad volumen de datos y tiempo) en descifrar la clave de una encriptación WEP de 64 bits que una de 128 bits, no existiendo además entre ambos una relación aritmética, es decir, que no se tarda el doble en descifrar una clave de encriptación WEP de 128 bits que una de 64 bits.

A pesar de que es posible descifrar estas claves de encriptación, no debemos pensar que sea fácil ni rápido. Una buena clave de encriptación WEP de 128 bits (por no decir una de 256 bits) puede llegar a ser prácticamente indescifrable si nos hemos asegurado de que sea lo suficientemente complicada.

La mayoría de los programas para descifrar claves están basados en una serie de secuencias más o menos lógicas con las que empieza a atacar a nuestro sistema hasta entrar en él. Evidentemente, una clave del tipo

1234567890 tarda segundos en ser localizada, pero a nadie se le ocurre (o se le debería ocurrir) poner esta clave.

Se deben evitar claves que contengan secuencias relacionadas con información personal (fechas, nombres, lugares), así como frases típicas, ya que es lo primero que intentan este tipo de programas. Esto no solo es válido para una clave WEP, sino para cualquier tipo de clave que se utilice. También se debe evitar claves fáciles, como secuencias consecutivas de teclas o números.

4.2.2. ESTÁNDAR

Las personas que desarrollaron el estándar 802.11b pretendían que hiciera precisamente lo que dice su nombre: ofrecer la privacidad semejante a la que había en una red con cableado. Para complicar una red de cable, un atacante generalmente tiene que entrar en una cuarto e instalar un programa de rastreo que observe el tráfico que viaja por el cable. WEP se diseñó para actuar como una puerta cerrada, para impedir que los intrusos comprometieran en el propio tráfico de la red inalámbrica; la idea era que otras medidas complementaran esta línea de defensa inicial. WEP básicamente cifra todos los datos que fluyen por la red inalámbrica, impidiendo que los atacantes rastreen el tráfico de la red.

Desgraciadamente, incluso esta protección bastante mínima se vio mermado por varias decisiones de criptografía y porque algunas opciones se integraron pero nunca fueron habilitadas. Además, aunque el cifrado WEP sigue ofreciendo cierta protección, la mayoría de la gente no lo activa porque es una molestia utilizarlo.

4.2.3. CIFRADO

Los tipos cifrado disponibles son configurados en 64-bits, pero poco después ya se podía cifrar con 128 bits y hasta 256-bits

4.3. LOS IDS (SISTEMAS DE DETECCIÓN DE INTRUSIONES)

El término **IDS** (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo **N-IDS** (*Sistema de detección de intrusiones de red*), que garantiza la seguridad dentro de la red.
- El grupo **H-IDS** (*Sistema de detección de intrusiones en el host*), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

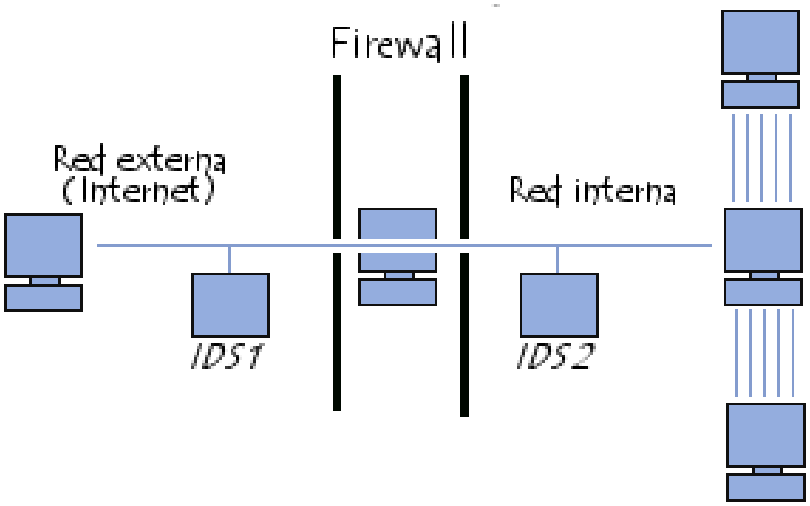

Tabla 03 IDS

El H-IDS se encuentra en un host particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.

El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

4.3.1. TÉCNICAS DE DETECCIÓN

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un N-IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N-IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones:

- **Verificación de la lista de protocolos**: Algunas formas de intrusión, como "Ping de la muerte" y "escaneo silencioso TCP" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.

- **Verificación de los protocolos de la capa de aplicación**: Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N-IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.

  Esta técnica es rápida (el N-IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, N-IDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).

4.3.2. RECONOCIMIENTO DE ATAQUES "COMPARACIÓN DE PATRONES"

Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N-IDS y todavía es de uso frecuente.

Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica. Por ejemplo, al buscar la cadena de caracteres "cgi-bin/phf", se muestra un intento de sacar provecho de un defecto del script

CGI "phf". Este método también se utiliza como complemento de los filtros en direcciones IP, en destinatarios utilizados por conexiones y puertos de origen y/o destino. Este método de reconocimiento también se puede refinar si se combina con una sucesión o combinación de indicadores TCP.

Esta táctica está difundida por los grupos N-IDS "Network Grep", que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al utilizar un analizador de "expresiones regulares". Éste intentará hacer coincidir las secuencias en la base de firmas byte por byte con el contenido del paquete capturado.

La ventaja principal de esta técnica radica en la facilidad de actualización y también en la gran cantidad de firmas que se encuentran en la base N-IDS. Sin embargo, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes “CE63D1D2 16E713CF”, cuando se colocan al inicio de una transferencia de datos UDP, indican un tráfico Back Orifice con una contraseña predeterminada. Aunque el 80% de las intrusiones utilicen la contraseña predeterminada, el 20% utilizarán contraseñas personalizadas y no serán necesariamente reconocidas por el N-IDS. Por ejemplo, si la contraseña se cambia a "evadir", la serie de bytes se convertirá en "8E42A52C 0666BC4A", lo que automáticamente la protegerá de que el N-IDS la capture. Además, la técnica inevitablemente conducirá a un gran número de falsas alarmas y falsos positivos.

Existen otros métodos para detectar e informar sobre intrusiones, como el método Pattern Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

4.3.3. ¿QUÉ HACEN LOS IDS?

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**: Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).

- **Envío de una trampa SNMP a un hipervisor externo**: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.

- **Envío de un correo electrónico a uno o más usuarios**: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.

- **Registro del ataque**: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.

- **Almacenamiento de paquetes sospechosos**: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

- **Apertura de una aplicación**: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).

- **Envío de un "ResetKill"**: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).

- **Notificación visual de una alerta**: Se muestra una alerta en una o más de las consolas de administración.

4.4. LA PROTECCIÓN CON HONEYPOTS

4.4.1. USOS DE LOS HONEYPOTS

Los honeypots son muy flexibles por lo que el campo de acción es bastante grande, dependiendo de la configuración se pueden llegar a tener tres tipos de usos:

- **Detectar ataques:** la detección suele ser una tarea difícil, se colecta demasiada información que después es difícil de analizar y se vuelve tediosa, a la vez es difícil de distinguir cual es la actividad normal del día a día del trabajo y la que se puede atribuir a algún atacante. Con los honeypots se pueden reducir las falsas alarmas al capturar poca cantidad de información de las actividades de los atacantes, en general se usan honeypots de baja interacción para las tareas de detección.

- **Prevenir ataques:** los honeypots pueden ayudar a prevenir ataques de muchas maneras, un ataque común es el automatizado, que son gusanos que revisan redes en busca de vulnerabilidades y si encuentran un sistema vulnerable, éste es atacado y tomado, en general esto sucede replicándose en la red haciendo copias de sí mismo tanto como pueda. Un honeypot puede reducir la velocidad de este proceso e incluso llegarlo a detener, este tipo de honeypot es llamado sticky honeypot (tarro de miel pegajoso) y es el encargado de

interactuar con el atacante haciéndolo más lento, para ello se usan una variedad de trucos sobre el protocolo TCP, como un tamaño de ventana de longitud cero u otros.

- **Responder ataques:** en grandes sistemas, una vez detectado un ataque, éste puede ser respondido, pero no siempre es la mejor medida a tomar, no sabemos quienes atacan a nuestros equipos y que propósitos tienen, por lo que a veces, es mejor esperar a obtener mayor información o como sucede a menudo, los sistemas no pueden detenerse para analizar daños y realizar un examen exhaustivo de que ha sucedido, esto pasa con servidores web o de correo electrónico, en donde toda la organización depende de esos servicios y el tiempo fuera de servicio de los mismos es crítico.

  Otro problema es que si el sistema es puesto fuera de servicio, se tendrá muchísima información a analizar (ingreso de usuarios, correos enviados y leídos, archivos escritos, accesos a base de datos) que son el resultado de la operación normal de cualquier sistema, pero donde se hace muy difícil separar esa actividad de las de un atacante. Los honeypots pueden ayudar a resolver estos problemas en forma fácil y rápida ya que es sencillo poner el sistema fuera de línea para un análisis detallado sin necesidad de tocar nada en los sistemas de producción. Esto es posible porque en los honeypots la única información que se almacena es la sospechosa, de ahí surge que la cantidad de información a analizar es mucho menor y casi de seguro que de un atacante. Con esta información de las herramientas y procedimientos usados por los atacantes se aumentan las posibilidades de que un contraataque tenga éxito. Para este tipo de uso los honeypots de alta interacción son los usados.

4.4.2. TIPOS DE HONEYPOTS

Se puede dividir a los honeypots en dos tipos:

- **Para investigación:** se usan para recolectar información sobre los movimientos de los intrusos, o sea se registra cada movimiento del atacante para usar esta información y crear perfiles de los mismos.

- **Para producción:** se usan para proteger a los verdaderos servidores y desviar la atención de los atacantes. De esta manera se disminuye la superficie de ataque de los intrusos.

Otra división que suelen tener los honeypots es en base al grado de interacción con el usuario, aquí nuevamente se presentan dos tipos:

- **Alta interacción:** se usan sistemas complejos que recrean un sistema completo con sistema operativo y aplicaciones reales, en este caso no hay emulación, quien entre encontrará un gran sistema para interactuar, de esta manera se pueden estudiar mejor las actividades de quienes ingresan al mismo. Estos sistemas requieren más trabajo de implementación y solamente son usados por grandes organizaciones que disponen de los recursos necesarios para hacerlo.

- **Baja interacción**: en este tipo la interacción con el usuario es mucho menor y se limita por lo general a emular servicios. Son rápidos y fáciles de implementar por lo que, en general, son los más utilizados.

4.4.3. VENTAJAS

- Los honeypots no requieren gran hardware, ya que solamente registran datos cuando son accedidos y se pueden configurar para sólo registrar ciertos tipos de eventos, de esta manera los

responsables de la seguridad no se ven sobrepasados con registros de miles de líneas que muchas veces son difíciles de analizar.

- Se pueden reducir las falsas alertas, es decir, muchas veces ciertos eventos que suceden a menudo suelen ignorarse de la misma manera que cuando suenan las alarmas de los autos en un estacionamiento, la mayoría de la gente cansada de las alarmas empieza a ignorarlas creando una falsa alarma o falso positivo. Todo acceso a un honeypot por definición es no autorizado, por lo tanto no hay que obviarlo.
- Detección de falsos negativos, es decir, se pueden detectar nuevos y desconocidos ataques, ya que todo acceso, como se dijo antes, es una anomalía y debe ser analizada.
- Trabajan con nuevas tecnologías como SSH, IPSec, SSL e Ipv6.
- Nivel de flexibilidad, se pueden adaptar casi a cualquier situación y recrear cualquier ambiente y de esta manera ofrecer base de datos o situaciones para atraer atacantes.

4.4.4. DESVENTAJAS

- Solamente se puede ver lo que pasa con los honeypots, ya que las actividades a las que se está registrando son sobre este sistema y nada se puede hacer sobre sistemas vecinos.
- Como toda nueva tecnología usada, se agregan riesgos inherentes a ellas y pueden llegar a ser usados para nuevos y diferentes ataques.

4.4.5 CUADRO COMPARATIVO DE LA APLICACIÓN BACKTRACK

	BACKTRACK	**WIFISLAX**
VENTAJAS	Sistema operativo de fácil manipulación Es una aplicación para auditoria de seguridad informática	Desencripta de forma fácil Es un aplicacion que trabaja bajo plataforma linux
DESVENTAJAS	Es un software libre y puede ser usada con malos fines	Es un programa que muy confiable su manipulación

4.5. MANUAL DE WEP CRACKING

Con este manual demostraremos como se puede desincriptar una clave WEP de una red privada.

Como primer paso colocamos en el disco de Backtrack y booteamos desde la lector. Se verá algo así:

Figura 1 Instalación Backtrack

Una vez seleccionado, cargará los archivos necesarios y escribiremos en la consola el comando:

startx

Después de esto escrito, presionamos enter y nos llevará al escritorio en donde encontraremos las herramientas para trabajar.

Hacemos click derecho en la bandera, Configure, luego buscamos Spain en el menú izquierdo, doble click en ella, y ya la podremos seleccionar para utilizarla.

Figura 2 Backtrack

Cambiando nuestra MAC

Lo primero que se hará es cambiar nuestra MAC, para que sea más fácil de recordar. Accedemos a la consola y escribimos:

airmon-ng

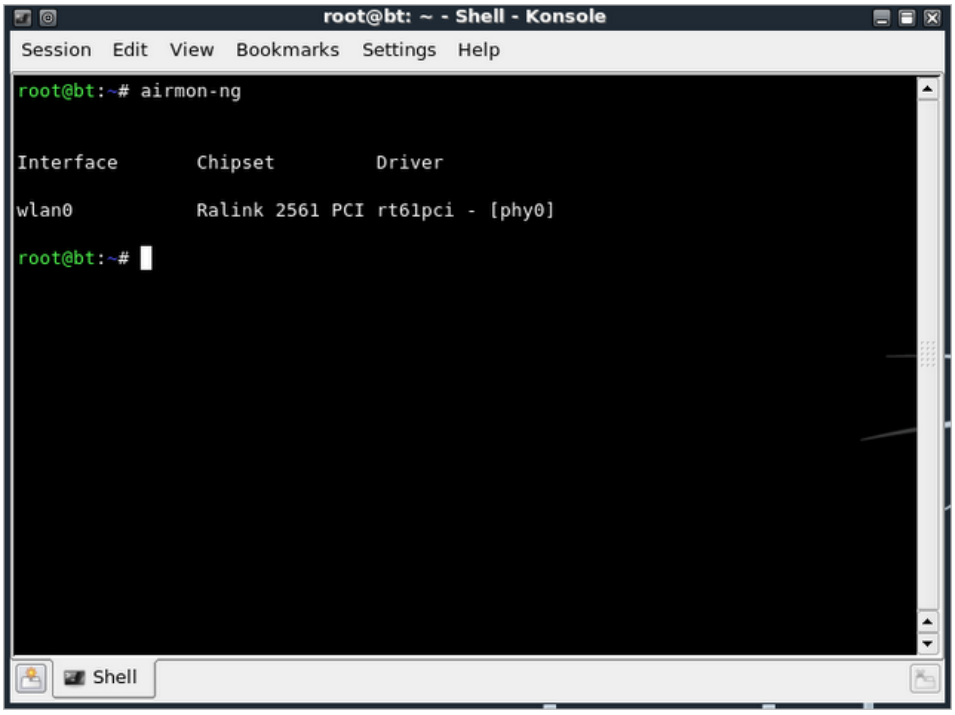

Figura 3 Localizar el nombre del puerto

Presionamos enter como vemos en la imagen, la interfaz se llama: wlan0

Lo que haremos ahora será detener el servicio. Para ello escribimos:

airmon-ng stop wlan0

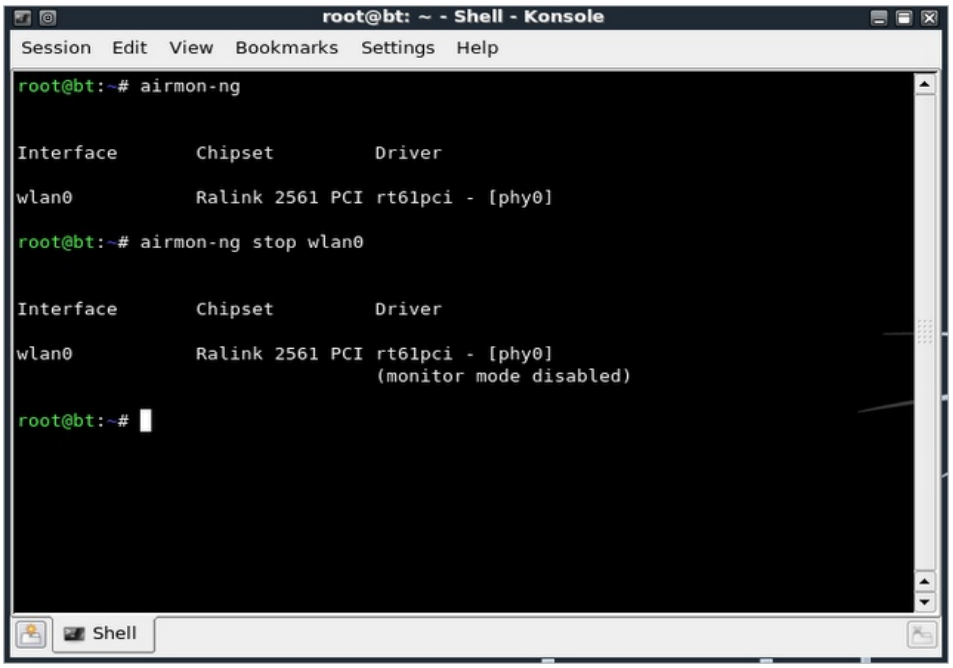

Figura 4 Detener en servicio

Una vez hecho esto escribimos lo siguiente:

ifconfig wlan0 down

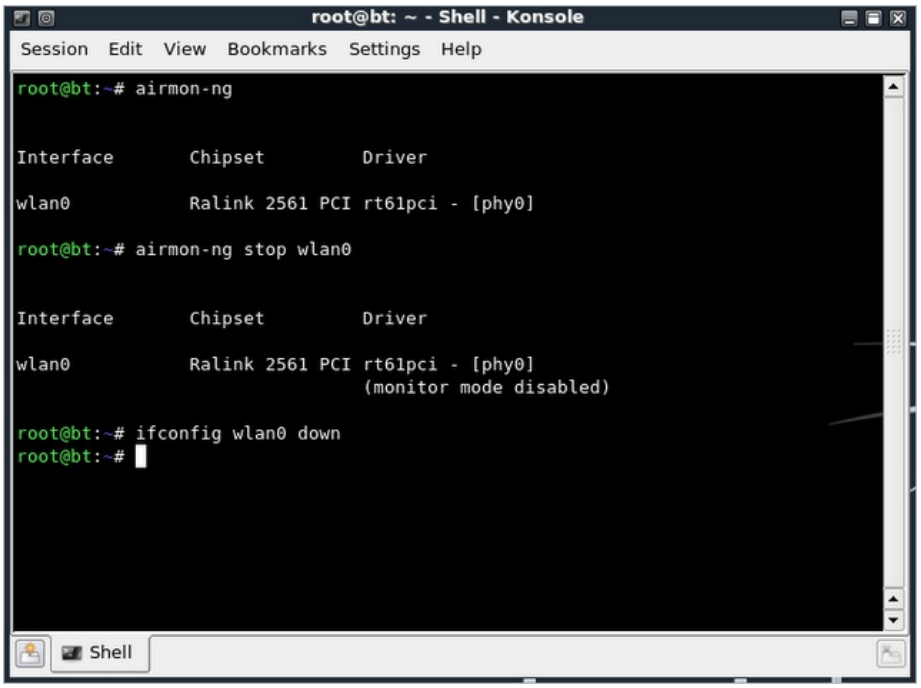

Figura 5 Configuración wlan0

Ahora iremos a cambiar nuestra MAC. Para ello escribimos:

macchanger –mac

00:11:22:33:44:55 wlan0

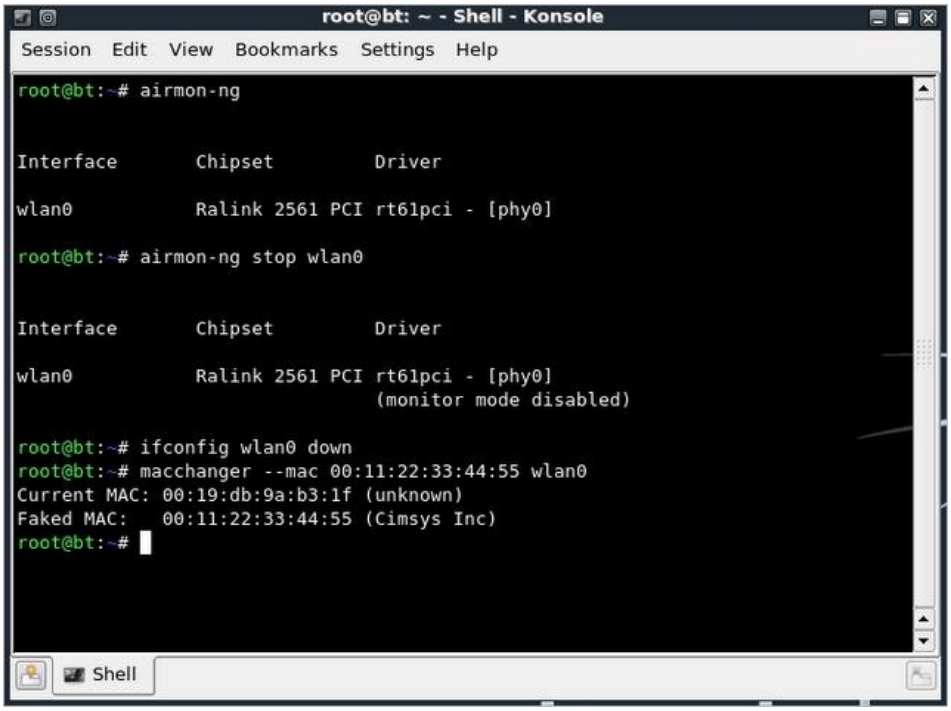

Figura 6 Cambio de MAC

Si nos aparece algo como en la imagen, quiere decir que hemos hecho todos los pasos correctamente.

Finalmente podremos nuevamente activamos el servicio de la tarjeta colocándola en modo monitor escribimos:

airmon-ng start wlan0

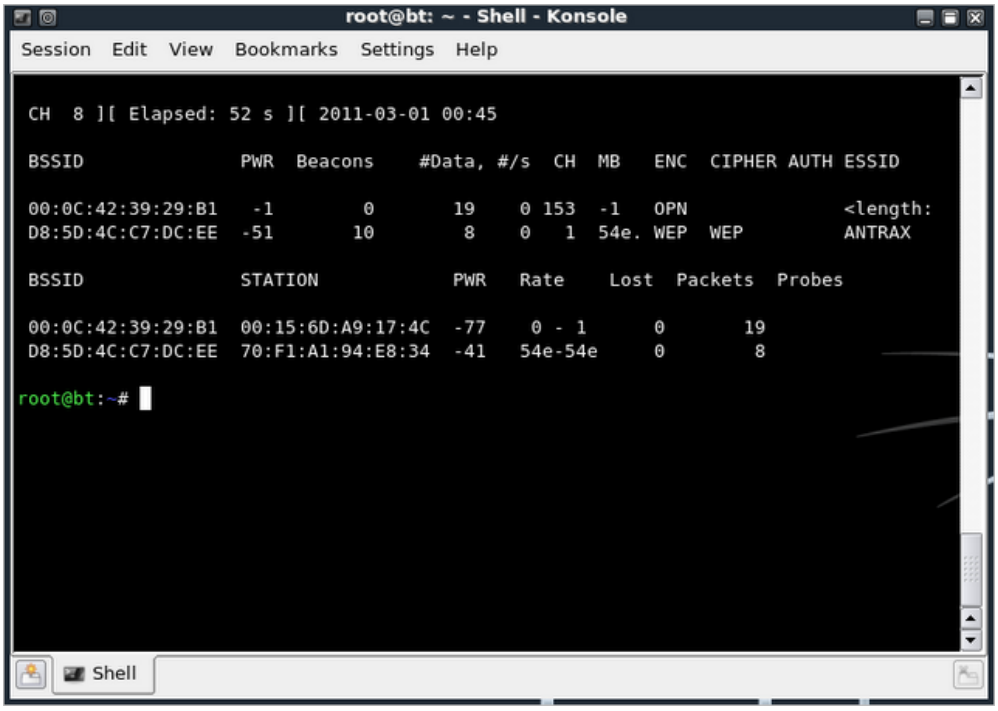

Figura 7 Modo monitor

Buscado redes

Para comenzar escribiremos la siguiente línea:

airodump-ng wlan0

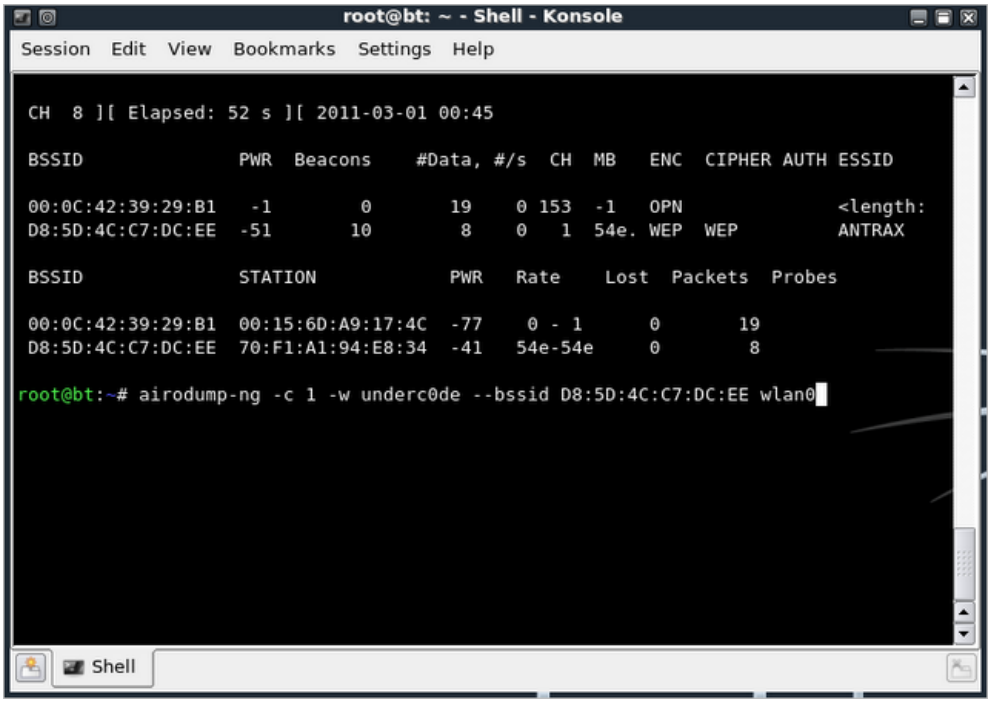

Figura 8 Buscado red

Para este el router debe de estar con un cifrado WEP

Como se puede ver, apareció la red mía, tiene encriptación WEP. Lo que se hará ahora será parar el scanneo presionando CTRL + C

Capturando DATOS

Escribimos la siguiente línea:

airodump-ng –c 1 –w underc0de –bssid D8:5D:4C:C7:DC:EE wlan0

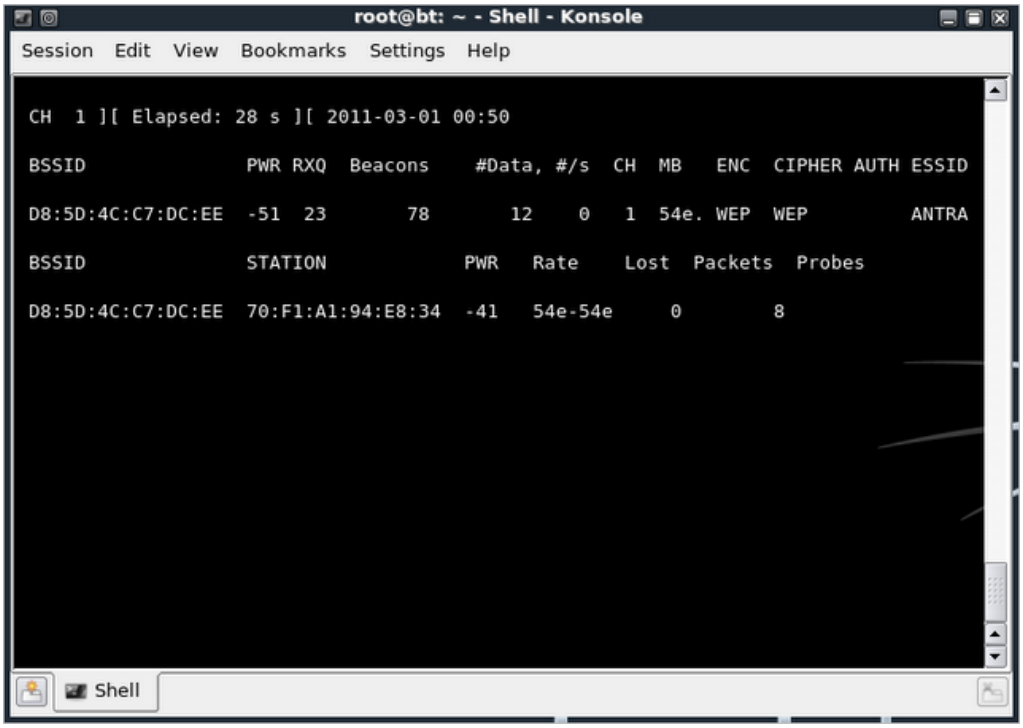

Figura 9 Capturación de Datos

Donde dice underc0de, debemos modificarlo por un nombre que nosotros queremos. Por ultimo en donde está la MAC, deben colocar la MAC que están atacando.

Una vez ejecutada esta línea, iniciara a capturar los DATA, que son datos necesarios para luego descifrar la Password.

Asociándonos a la red

Lo que haremos ahora será asociarnos. Para ello abrimos otra consola, “SIN CERRAR LA ANTERIOR”, ya que seguirá capturando los DATOS que necesitaremos más adelante.

En la nueva consola escribimos:

Aireplay-ng -1 0 –a D8:5D:4C:C7:DC:EE –h 00:11:22:33:44:55 –e ANTRAX wlan0

En esta línea modificaremos nuevamente. En este caso la MAC por lo que estamos atacando y en donde dice mi nombre por el ESSID que estamos atacando que en mi caso se llama ANTRAX

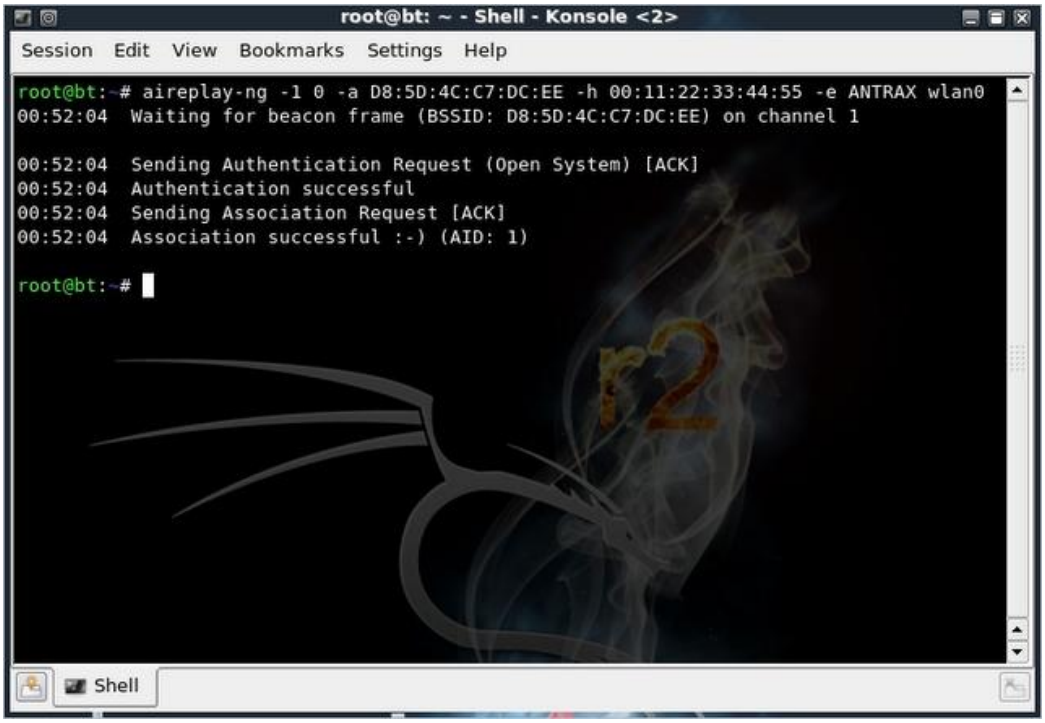

Figura 10 Modificación de Datos

Si llegamos hasta acá, y nos aparece de la imagen, quiere decir que hasta el momento hemos hecho las cosas a la perfección En caso contrario aparecerá algún tipo de error (unsuccessful), las causas pueden ser las siguientes:

- La red a la que quieres atacar está muy lejos.
- Tu tarjeta de red no puede hacer inyección de paquetes
- El router tiene seguridad para evitar este tipo de ataques

Inyectando tráfico

Escribimos ahora en la misma consola el siguiente comando:

aireplay-ng -3 –b B8:5D:4C:C7:DC:EE –h 00:11:22:33:44:55 wlan0 Al igual que antes, modificamos la MAC que estamos atacando. Una vez hecho esto, comenzara a inyectar tráfico y los datos comenzaran a subir velozmente.

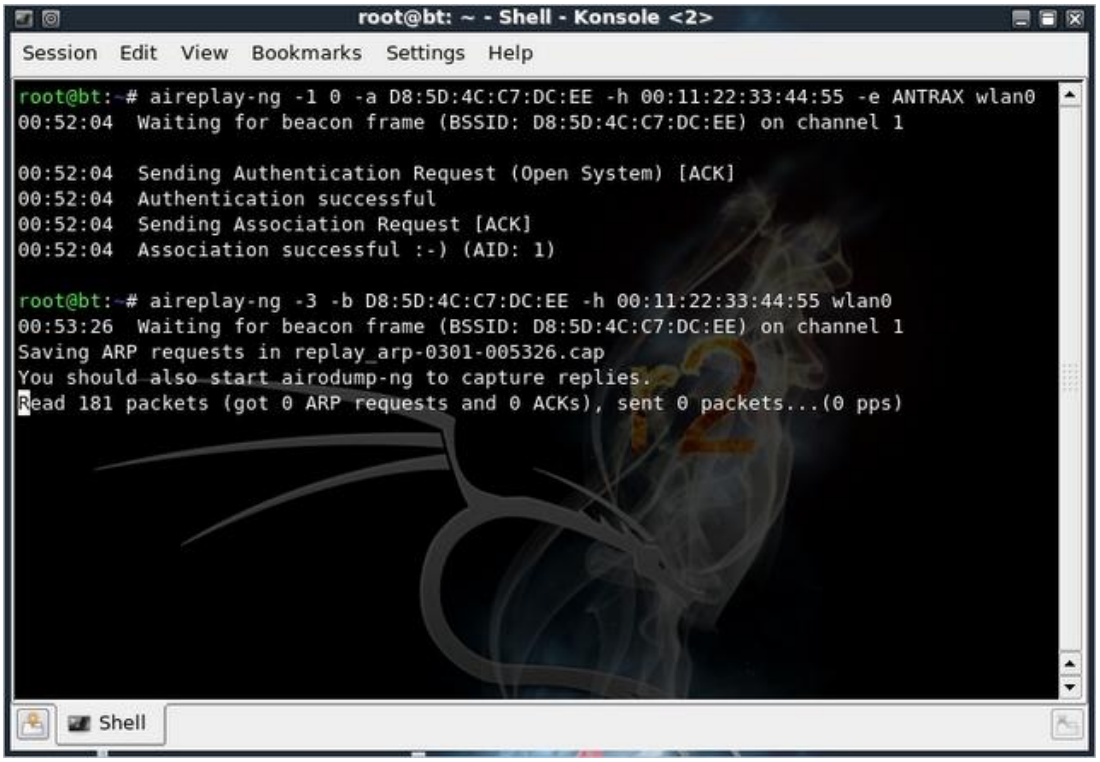

Figura 11 Inyección de datos

Si llegamos hasta acá y tenemos todo bien, estamos a solo un paso. Recuerde que es necesario capturar muchos datos, mientras más tengamos mejor. La cantidad de datos que debamos capturar dependerá de que tan complicada sea la Password.

Desencriptando la Password

Hemos llegado al final. En una tercera consola, escribiremos lo siguiente:

aircrack-ng underc0de-01.cap

Como siempre modificamos por el nombre que pusimos previamente en el paso 4.

Al ejecutar el comando, la password se comenzara a desencriptar.

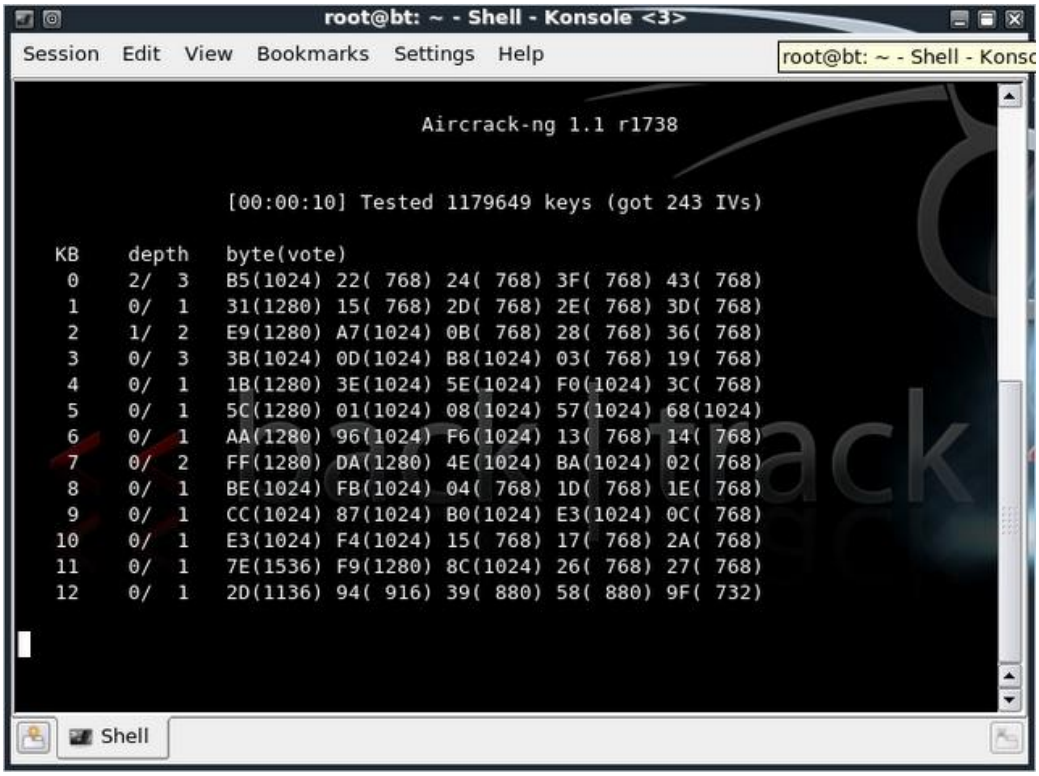

Figura 12 Desencriptación de clave

Esperamos unos minutos a que se desencripte, y si todo está correcto, nos mostrara la password, de lo contrario deberemos seguir capturando más datos hasta obtener la password

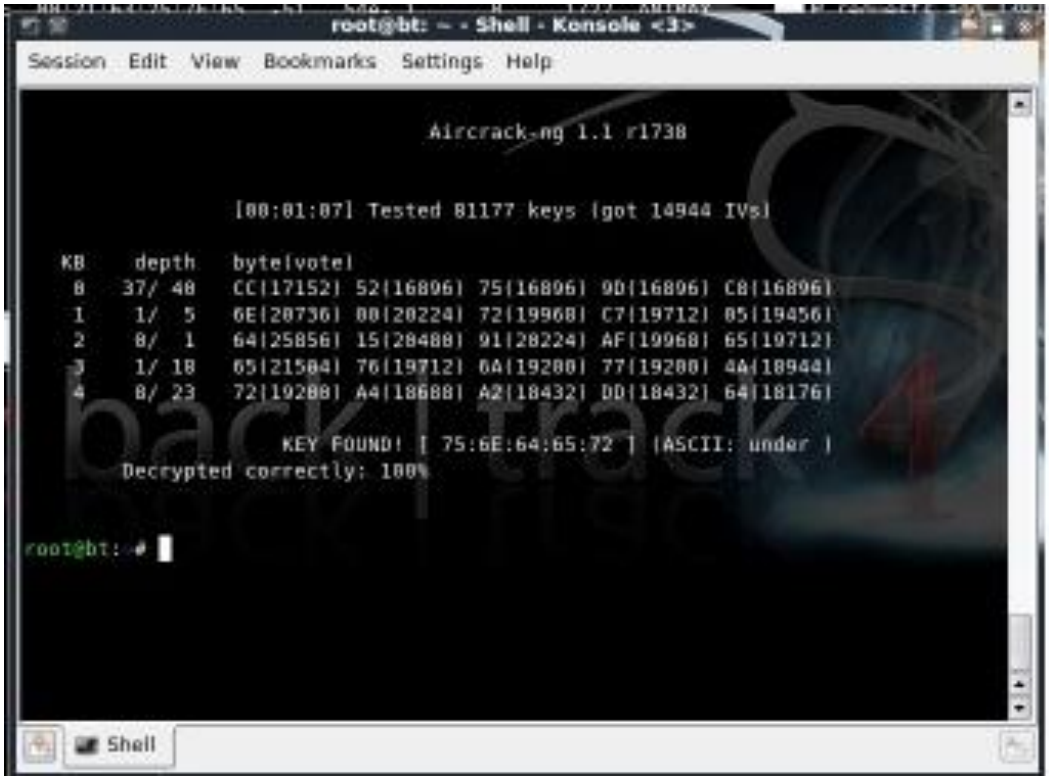

Figura 13 Clave de la Red

Como pueden ver, en mi caso la password es: **under**

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

a. El cifrado WEP, cifrado de uso generalizado en la red wireless, resulta ser un cifrado excesivamente básico, fácilmente vulnerable a través de cualquier tipo de ataque.
b. La encriptación WEP es insegura, al aumentar el tamaño de las claves de cifrado sólo aumenta el tiempo necesario para romperlo
c. El programa Backtrack es el software más utilizado para hackear las redes inalámbricas debido a que es de fácil acceso y uso resulta sencillo.
d. La mayor parte de las redes inalámbricas o Wi-Fi comparte una misma clave entre todas las estaciones y puntos de acceso de la red, lo cual ocasiona a corto plazo que la clave compartida sea desencriptada, convirtiéndose en una presa fácil de ataques.
e. Existen mecanismos complementarios para incrementar la seguridad de las redes inalámbricas basadas en WAP y WAP2, que resultan de difícil encriptación.
f. IDS y Honeypots son software que brindan mayor protección a las redes inalámbricas.

5.2. RECOMENDACIONES

a. Aplicar el cifrado WPA2 para poner atenuar los riesgos en las redes wireless.
b. Proteger la red con los IDS que son la mejor forma para poder proteger su red.
c. Tener muy en cuenta que cifrado WEP es el menos confiable para una red inalámbrica.
d. Revisar siempre que personas están conectadas a la red wireless.

BIBLIOGRAFÍA.

- CEH Official Certified Ethical Hacker Review Guide Fecha de publicación: 27 de febrero 2007

- Filip, A., y Vásquez, E. (2000). Seguridades en redes WiFi Eduroam. Sevilla: Universidad de Sevilla.

- Barajas, Saulo. Protocolos de seguridad en redes inalámbricas. Recuperado el 12 de septiembre del 2011, de http://www.saulo.net

- De Nuevo: las Redes Wireless No Son Seguras. Recuperado el 07 de septiembre de 2011, de http://www.virusprot.com

- (2011). Comunicación inalámbrica. Recuperado el 10 de septiembre de 2011, de http://es.wikipedia.org

- (2008). Wireless Hacking. Recuperado el 08 de septiembre de 2011, de http://filesseguridad7455.cteducacion.org

- Nieves, A. Redes y Comunicación Inalámbrica. Recuperado el 08 de septiembre. del 2011, de http://www.ilustrados.com/tema/8666/Redes-Comunicacion-Inalambrica.html

- ¿Qué es wireless? - ¿Qué significa wireless? - Definición del término wireless. Recuperado el 08 de septiembre de 2011, de http://www.masadelante.com

- Qué es WiFi?. Recuperado el 12 de septiembre de 2011, de http://www.misrespuestas.com

- (2005). Honeypots (Servidores Trampa). Recuperado el 10 de septiembre de 2011, de http://www.xombra.com