UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Esquemas de seguridad en redes inalámbricas

Trabajo Monográfico

para obtener el grado de

Ingeniero en Redes

PRESENTA

Andrea Pérez Gómez

Supervisores de Monografía

Dr. Jaime Silverio Ortegón Aguilar

M.T.I Vladimir Veniamin Cabañas Victoria

Ing. Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Septiembre de 2009.

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo monográfico elaborado bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo Monográfico

Supervisor:

Dr. Jaime Silverio Ortegón Aguilar

Supervisor:

MTI. Vladimir Veniamin Cabañas Victoria

Supervisor:

Ing. Rubén Enrique González Elixavide

Chetumal, Quintana Roo, México, Septiembre de 2009.

Agradecimientos

A MIS PADRES:
Por su infinito amor y por no dejarme sola en ningún momento.

A MIS HERMANOS
Por gran apoyo y por demostrarme que los sueños se hacen realidad y que siempre contaré con ellos en todo momento.

A MIS ASESORES:
Al Dr. Jaime Ortegón, por ser un valioso ejemplo de motivación para mí, por su constancia y dedicación para que este trabajo llegue a buen término.
Al M.T.I Vladimir Cabañas por ser más que un maestro, ser un amigo que siempre me aconsejó, felicitó y regañó a lo largo de mi carrera.
Al Ing. Rubén González por ser un gran ejemplo dentro y fuera del aula, que siempre transmitió una gran confianza y muchos conocimientos al ser un excelente maestro.

Dedicatoria

A mis padres, Eddie y Bertha que siempre creyeron en mí.
A mis hermanos Cecilia y David que nunca me dejaron caer.

"Lo que hoy es utópico mañana es real. Mundos Posibles. La utopía es lo que ha conducido a que seamos posibles."
Jerome Bruner.

Resumen

La comunicación inalámbrica es el tipo de comunicación en la que no se utiliza un medio guiado. Lo anterior permitió a las redes inalámbricas ganar mucho terreno, ya que presentan ventajas como su rápida instalación sin la necesidad de usar cableado. También permiten la movilidad y tienen menos costos de mantenimiento que una red convencional; en consecuencia permite una mayor comodidad en hogares, oficinas y espacios públicos, entre otros.

Una de las principales preocupaciones de las redes inalámbricas se centra en la seguridad, al utilizar el espacio como medio de propagación. Para proteger la información, se han desarrollado protocolos que incorporan mecanismos de autenticación y cifrado de los paquetes que se transmiten. El cifrado WEP (Wired Equivalent Privacy) fue el primero que se desarrolló para proveer seguridad a las redes inalámbricas, sin embargo pronto se descubrieron debilidades en la implementación; por lo que más tarde comenzó a usarse el cifrado WPA (Wi-Fi Protected Access). WPA, por algún tiempo, fue computacionalmente difícil de descifrar, pero en la actualidad ya se realizan ataques exitosos que comprometen su implementación.

Este trabajo está enfocado a mostrar la forma en que se pueden descifrar dichas redes, así como también emitir recomendaciones para hacerlas más confiables.

Contenido

Antecedentes

Las primeras experiencias con redes inalámbricas datan de 1979, cuando científicos de IBM en Suiza despliegan la primera red de importancia con tecnología infrarroja. Pero hasta 1985 se comienzan los desarrollos comerciales de redes con esta filosofía. En ese momento, el órgano regulador del espectro radioeléctrico americano, la Comisión Federal de las Comunicaciones (FCC, por sus siglas en inglés), asignó un conjunto de estrechas bandas de frecuencia para libre uso alrededor de los 2.4 y los 5 GHz (1).

Las ventajas de las redes inalámbricas en los rangos de frecuencias antes mencionados son claras: no requieren licencias y pueden ser implantadas en cualquier ubicación, tanto para uso público, como privado. Por otra parte presentan una serie de importantes inconvenientes: interferencias impredecibles con redes próximas, con frecuencias iguales o parcialmente iguales; espectro empleado por otras aplicaciones (redes Bluetooth, teléfonos inalámbricos, emisores de vídeo, hornos de microondas, etc.); una potencia de emisión muy limitada que restringe mucho la cobertura; y una banda de uso muy estrecha que permite delimitar muy pocos canales no interferentes.

En febrero de 1980 se formó en el IEEE (*The Institute of Electrical and Electronics Engineers*) un comité de redes locales con la intención de estandarizar un sistema de 1 o 2 Mbps, que básicamente era Ethernet, al cual asignaron el número 802. Decidieron estandarizar el nivel físico, el de enlace y superiores. Dividieron el nivel de enlace en dos subniveles: el de enlace lógico, encargado de la lógica de re-envíos, control de flujo y comprobación de errores, y el subnivel de acceso al medio, encargado de arbitrar los conflictos de acceso simultaneo a la red por parte de las estaciones (2).

El estándar 802.11 se refiere a una familia de especificaciones desarrolladas por la IEEE para la tecnología de red de área local Inalámbrica (WLAN, por sus siglas en inglés). El 802.11 especifica una interfaz sobre el aire entre el cliente y

una estación base o entre dos clientes inalámbricos. La IEEE aceptó la especificación en 1997.

Entre los principales estándares para redes inalámbricas se encuentran: IEEE 802.11, IEEE 802.11a, IEEE 802.11b, y IEEE 802.11g.

El estándar original de este protocolo es el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2.4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy."

La siguiente modificación apareció en 1999, y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabaja en la frecuencia de 2.4 GHz. También se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente, se incorporó un estándar a esa velocidad y compatible con el b, este recibió el nombre de 802.11g. Este opera en la banda de frecuencias de 2.4 GHz y asegura una velocidad de 24 Mbps y un máximo de 54 Mbps.

En la actualidad la mayoría de productos son de la especificación b y g, sin embargo se están desarrollando productos que soportan la 802.11n, que puede alcanzar hasta 300 Mbps. Esto significa una verdadera revolución en el mundo de las redes inalámbricas, aumentando la velocidad de las redes inalámbricas de una forma increíble, acercándolas al mundo de las redes cableadas.

La Wi-Fi Alliance realiza pruebas rigurosas para certificar dispositivos que usen la red inalámbrica y dar confianza tanto a los consumidores como a los fabricantes. Sus pruebas son tan importantes y a la vez necesarias para ver el logo certificado en nuestro móvil o laptop y saber que legalmente nuestro

dispositivo soporta Wi-Fi en cualquier red inalámbrica. Wi-Fi es la certificación de la industria para asegurar que se cumple con algún estándar de la familia 802.11 y se es compatible con todos los dispositivos certificados.

Es importante tener una buena seguridad en una red inalámbrica debido a que este tipo de red es muy susceptible a los ataques y la información que se envía a través de ella es muy valiosa, se abundará más sobre la seguridad en el marco teórico.

Objetivo

Analizar la confiabilidad de los métodos de cifrado de datos en redes inalámbricas de la familia 802.11 A/B/G.

Objetivos Particulares

1. Describir los diferentes métodos de cifrado existentes para redes inalámbricas
2. Implementar los métodos de cifrado.
3. Probar la confiabilidad de los métodos de cifrado existentes, mediante el uso de herramientas de distribución gratuita para descifrar los datos.
4. Indicar el método de cifrado más confiable, disponible en la actualidad.

Justificación

La seguridad en la transmisión de datos es sumamente importante, más aún cuando se trata de una red inalámbrica, ya que al no contar con seguridad “física” se puede revisar qué se está enviando y hacia dónde se dirige. Es por esto que, el cifrado de los datos tiene que llevarse a cabo para garantizar que la información enviada llegue de manera privada a su destino. En este trabajo se analizarán los tipos de cifrado existentes para las redes inalámbricas para poder determinar cuáles son los más confiables y resistentes a amenazas.

Marco teórico

Una red inalámbrica es sencillamente un grupo de dispositivos que se comunican sin necesidad de cables. A pesar que las redes inalámbricas iniciaron orientadas al uso exclusivo de las empresas también han incursionando en los hogares.

Una de las ventajas al momento de instalar una red inalámbrica es que es mucho más rápido y flexible que instalar una red cableada; sin contar con la movilidad que se tendría sin miedo a perder la comunicación. Esta comunicación permite al igual que una red cableada, compartir varios recursos tales como: archivos, directorios, impresoras e incluso la posibilidad de acceder a otras redes.

Las señales inalámbricas viajan a través de las paredes, pisos y otros obstáculos físicos, de modo que se puede disfrutar de la abundante información de Internet y de la vida al aire libre al mismo tiempo, mientras un enrutador inalámbrico proporciona la señal. (3)

El riesgo de seguridad en las redes inalámbricas resulta evidente al estar formado por equipos que emiten los datos al entorno, cualquier receptor que esté dentro del área de cobertura del emisor puede interceptar dichos datos (4). Si cuenta con las herramientas apropiadas, podrá extraer información sensible como contraseñas de cuentas de correo electrónico, conversaciones privadas y otros datos no cifrados que inevitablemente salen de la computadora, al conectarse a diferentes servidores de autorización en Internet.

Seguridad en IEEE 802.11

El IEEE 802.11 utiliza tres mecanismos para proteger las redes WLAN (5):

- SSID (Identificador de Servicio): Es un código simple que identifica la WLAN y se le conoce como el nombre de red. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado dado que se puede obtener de los paquetes de la red inalámbrica en los que viaja en texto claro. Comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía.

Existen dos tipos de SSID dependiendo de si la red inalámbrica funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

- ESSID (Extensión del conjunto de servicios de identificación): Es empleado para las redes inalámbricas en modo infraestructura donde participan uno o más APs como lo muestra la Figura 1.

Figura 1 ESSID modo infraestructura

- BSSID (Identificación del conjunto de servicios básicos): Este identificador, es la dirección MAC del punto de acceso (AP). Empleado para redes inalámbricas en modo Ad-hoc, donde una

computadora puede estar conectada a uno o varios dispositivos, y pueden estar conectados entre sí sin ningún punto de acceso como se observa en la Figura 2.

Figura 2 BSSID Modo Ad-Hoc

• Filtrado con dirección MAC (Control de Acceso al Medio): Restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico o se clona la dirección MAC.

• Datos de cifrado WEP (Privacidad Equivalente a Cable): Es un esquema de cifrado que protege el flujo de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación de Wi-Fi Alliance exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves surge cuando se distribuyen ampliamente, entonces la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación; este método ofrece una alternativa más segura, porque menos

estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.

Además de los medios de seguridad ofrecidos por el 802.11, existen otras posibilidades como los que se describen a continuación:

Estándar 802.1X.
Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

WPA (Wi-Fi Protected Access)
Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras– Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación.

Desarrollo

El ambiente en que se desarrollará la implementación de los métodos de cifrado es en un ambiente controlado usando como equipo de inyección y captura de paquetes una computadora portátil HP Pavilion dv2125LA; la cual cuenta con un Intel Core Duo T2050 (1.60GHz), así como de una tarjeta de red Intel PRO/Wireless 3945 802.11 a/b/g. El sistema operativo es BackTrack 3 (6), debido a que es la distribución GNU/Linux más popular y actualizada que está diseñada para trabajar con redes inalámbricas, y cuenta con una amplia gama de herramientas para el escaneo de redes y pruebas de seguridad.

En una WLAN, los clientes inalámbricos y los puntos de acceso envían y reciben información a través de una vía aérea. De no implementarse seguridad, es posible que una persona no autorizada intercepte la información. El cifrado es una manera usual de asegurar y de proteger la información. El encriptado aplica a la información un conjunto de instrucciones, llamado algoritmo, estas instrucciones combinan el texto plano o limpio de la información con una secuencia de números hexadecimales, llamada clave de encriptado (7).

La información es solamente legible para los dispositivos WLAN que tienen la clave correcta de cifrado. Cuanto más larga es la clave, más seguro es el cifrado.

WEP

En una red WLAN en la que se emplea WEP, el usuario y el punto de acceso (AP) deben establecer una relación antes de poder intercambiar datos. Esta relación puede encontrarse en tres estados diferentes donde intervienen la autenticación y la asociación (8); la primera se da cuando un usuario es reconocido en el AP para poder conectarse a la red y el segundo para poder intercambiar datos con otros.

1. Sin autenticación y desasociado

   El usuario está desconectado de la red y no puede enviar peticiones para validarse ante el AP.

2. Con autenticación y desasociado.

   El usuario entra al proceso de autenticación, pero no se encuentra asociado con el AP.

3. Con autenticación y asociado.

   El usuario ya se encuentra conectado a la red.

En la Figura 3 se muestra la manera en la cual se establece la relación entre en el usuario y el punto de acceso, si la autenticación y asociación es o no exitosa el punto de acceso determinará el tipo de notificación que se enviará.

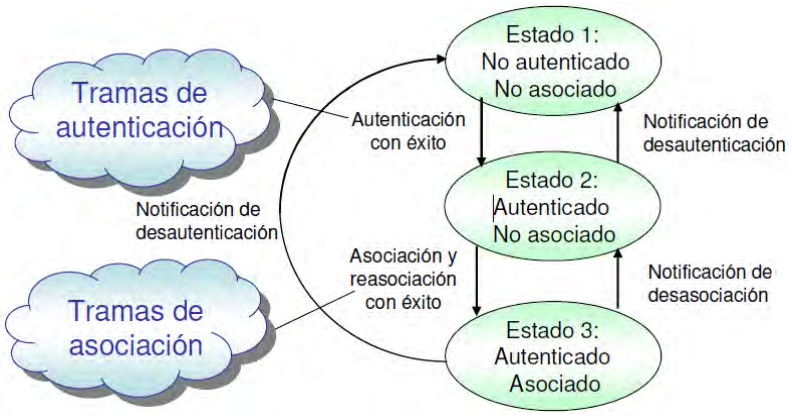

Figura 3 Estados Clientes WEP

Debido a que las transmisiones inalámbricas pueden ser captadas por terceros, WEP hace que estas transmisiones no tengan sentido para otro que no sea el destinatario, ya que los mensajes son enviados de manera cifrada.

El cifrado WEP utiliza una clave secreta compartida y el algoritmo de cifrado RC4. El punto de acceso (AP) y todas las estaciones que se conectan a él deben utilizar la misma clave compartida. Para cada paquete de datos enviado en una dirección, el transmisor combina el contenido del paquete con una suma de comprobación del mismo. Después, WEP solicita que el transmisor cree un vector de inicialización (IV) específico del paquete, que se combina con la clave y se utiliza para cifrarlo. El receptor genera su propia clave correspondiente del paquete y la utiliza para descifrarlo.

Proceso de cifrado WEP:

1. El texto plano recibe una suma de comprobación llamada CRC-32 para garantizar la integridad del texto transmitido, el resultado es el vector de verificación de integridad (ICV). CRC-32 se usa por ser simple y muy poderoso detectando errores en canales de alto ruido.

2. Se forma una cadena de 64 bits, utilizando 24 bits del llamado vector de iniciación y 40 bits correspondientes a la clave de autentificación de la red. El vector de iniciación es un vector binario generado unilateralmente por el punto de acceso.
3. Utilizando un método llamado RC4 se genera una cadena binaria a partir de la cadena de 64 bits.
4. La cadena del RC4 y el texto plano son pasados por un proceso de XOR, dando por resultado el texto cifrado. Es importante saber que para recuperar el mensaje en el otro extremo se debe saber el valor de la cadena RC4, que como ya se expuso, es el vector de iniciación junto a la clave.

Finalmente se envía un paquete que tiene por encabezado lo establecido en la norma 802.11, luego lleva el vector de iniciación, luego el mensaje cifrado y finalmente el valor de la suma de chequeo CRC-32. A continuación, en la Figura 4 se detalla el proceso de cifrado WEP, el cual comienza con el envió de los datos en texto plano usando el CRC para verificar dicho envió, posteriormente se le comenzaran a añadir bits mediante el método RC4 para poderlo cifrar.

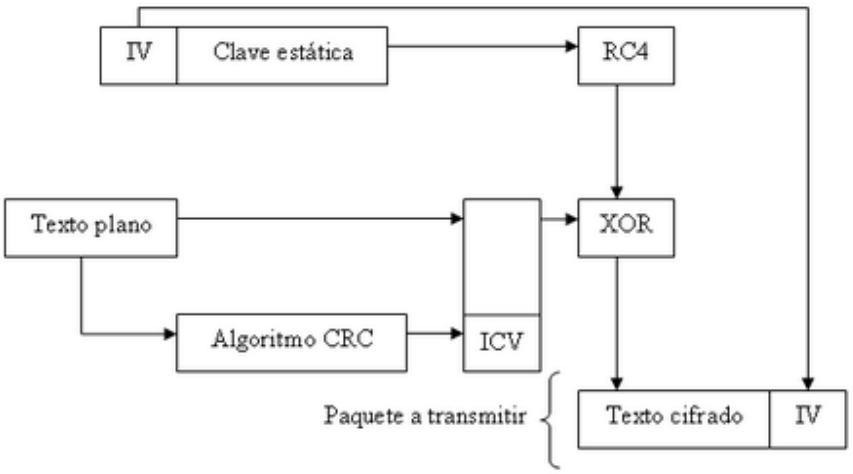

Figura 4 Proceso de cifrado WEP

Ataques a WEP

Algunos ataques a WEP son (9):

- Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico: Un intruso puede reunir dos textos cifrados con la misma secuencia de llaves y con base en esto se puede recuperar el texto original.

- Ataques activos basados en la introducción de paquetes. Cuando un intruso conoce un paquete y su texto cifrado, puede modificarlo y reenviarlo.

- Ataques de diccionario: Para descubrir una clave de cifrado se utilizan una serie de palabras probables, generalmente tomadas de un glosario de palabras y nombres, en lugar de todas las combinaciones posibles. Si la clave utilizada está en el diccionario se consigue reducir el tiempo para encontrarla.

El grupo de investigación ISAAC (Internet Security, Applications, Authentication and Cryptography) hizo un estudio minucioso acerca de los problemas y debilidades de WEP llegando a las siguientes conclusiones generales (10):

- El uso de claves estáticas origina que todos y cada uno de los usuarios utilice la misma clave; además de que no se cambia con regularidad, esto da como resultado que dicha clave se vuelva pública y cualquiera pueda acceder a ella,
- Por otra parte el hecho de que el IV (vector de inicialización) se transmita sin cifrar, y de que se pueda repetir cada cierto tiempo; además de que el algoritmo que genera este vector presenta ciertos

caracteres de predictibilidad, hace que sea un sistema perfecto para romper por la fuerza bruta,

- Una longitud de claves de 64 o 128 bits se ha vuelto insuficiente para garantizar una completa seguridad.

Descifrar WEP

El nivel de seguridad que provee WEP se centra en la transmisión que se lleva a cabo entre las estaciones móviles y el Access Point. El mecanismo de encriptación WEP se basa en el uso de una clave confidencial conocida como "*Passphrase*", la cual se comparte entre las estaciones y el Access Point (11).
WEP se implementa debido a que las comunicaciones inalámbricas tienen un punto de vulnerabilidad en la transmisión de datos.

Este fue el primer cifrado que se usó y es relativamente sencilla la obtención de las claves mediante aplicaciones de software, técnicas de ataque a diccionario o por fuerza bruta. El proceso de verificación de los niveles de confiablidad en una red inalámbrica se puede resumir en cinco pasos que se deben de seguir para la ruptura de la clave WEP, las cuales son (12):

- Recolección de información.
- Análisis de datos.
- Obtención del SSID (nombre de la red).
- Generación de tráfico (*packet injection*).
- Rotura del cifrado y obtención del resultado.

Para descifrar una clave WEP, se necesita de paquetes IV (vector de inicialización), y lanzar ataques de fuerza bruta. Para obtener paquetes es necesario capturarlos, para esto es preciso contar con una tarjeta de red inalámbrica, en MODO MONITOR. Esto permitirá la captura de paquetes de

información, mientras el punto de acceso (AP) se comunica con alguna máquina de la red.

Cuando un usuario se encuentra asociado al AP, es relativamente fácil capturar paquetes; pero cuando no hay usuarios asociados, el AP no envía paquetes, y por lo tanto no existen paquetes para capturar. Por esta razón se recurre a la inyección de tráfico para forzar al AP a que responda pedidos de asociación de forma constante, y de esa manera, obtener tráfico en la red.

El descifrado de WEP puede ser demostrado con facilidad utilizando herramientas como *Aircrack* (creado por el investigador francés en temas de seguridad, Christophe Devine). *Aircrack* cuenta con tres utilidades principales, utilizadas en las tres etapas del ataque para recuperar la clave:

- *Airodump-ng*: Herramienta de monitoreo (sniffing) utilizada para descubrir las redes que tienen activado WEP,
- *Aireplay-ng*: Herramienta de inyección para incrementar el tráfico,
- *Aircrack-ng*: Descifrador de claves WEP que utiliza los IV únicos recogidos.

A continuación se desarrollará el proceso de obtención de claves WEP en una red inalámbrica utilizando la distribución de Linux llamada *BackTrack 3* y la suite *Aircrack-ng*.

Para poder empezar hay que tomar en cuenta que no todas las tarjetas inalámbricas sirven, porque no todas soportan monitoreo e inyección a la vez, algunas solo soportan monitoreo. Las tarjetas más usuales que soportan ambos modos son las Atheros e Intel. Es de gran importancia contar con un chipset de tarjetas inalámbricas que soporte tanto la inyección de tráfico como la obtención de paquetes, en este caso se usará la tarjeta Intel PRO/Wireless 3945 A/B/G la

cual viene integrada en la computadora portátil. La tarjeta Intel 3945 usa el driver del kernel denominado iwl3945 para el modo monitor; para el modo de inyección debe usar el módulo *ipwraw*. A continuación se mostrarán los pasos necesarios para reemplazar el módulo *iwl3945* por el *ipwraw*.

Lo primero a realizar es iniciar el BackTrack 3 desde el live CD, a continuación abrir una Shell (terminal de comandos) (13),

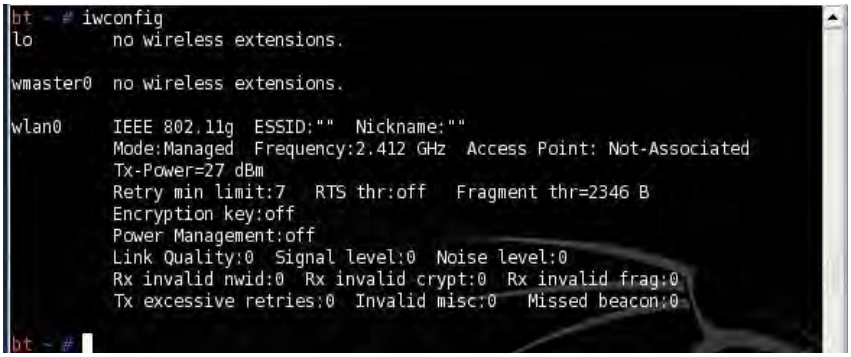

Figura 5 Configuración de red inicial

Como se observa en la Figura 5 al usar el comando *iwconfig* existe una interfaz llamada wlan0, esta interfaz soporta ipw3945, pero que no se encuentra en posición de inyectar y monitorear paquetes. Para esto es necesario deshabilitar el módulo del kernel con el driver de la tarjeta con el siguiente comando:

rmmod iwl3945

Con el siguiente comando se habilita la tarjeta para que pueda inyectar tráfico a la red:

modprobe ipwraw

El comando modprobe permite cargar el driver ipwraw con soporte de inyección de paquetes para tarjetas que utilizan el módulo iwl3945, nuevamente se teclea el comando iwconfig para verificar que el módulo se ha cargado y se creó una interfaz llamada WIFI0 que indica que el modo monitor ha sido habilitado, como se puede apreciar en la Figura 6.

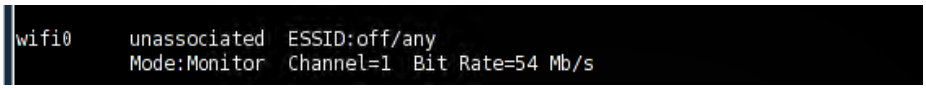

Figura 6 Tarjeta en modo monitor y para inyección de tráfico

El paso siguiente, será descubrir redes cercanas y sus clientes, escaneando los canales que utilizan las redes Wi-Fi, para eso se utiliza el comando *airodump-ng wifi0*

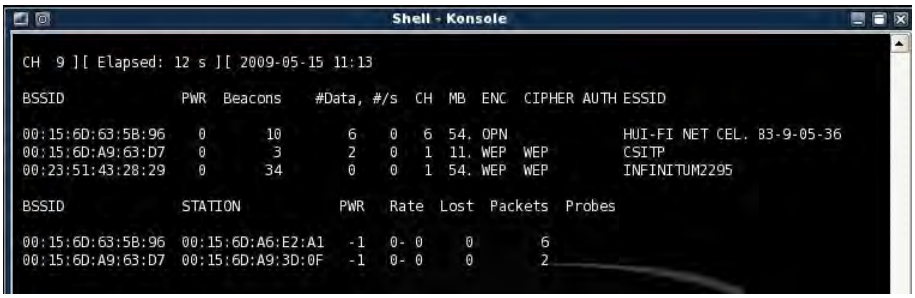

Figura 7 Escaneo de redes

El resultado que aparece en la Figura 7 se interpreta de la siguiente forma: un punto de acceso con BSSID 00:23:51:43:28:29 en el canal 1 con ESSID INFINITUM2295 está usando encriptación WEP. Una vez localizada la red a descifrar (en este caso aquella con BSSID 00:23:51:43:28:29), se debe capturar en el canal correcto para evitar la pérdida de paquetes, para ello se usa *airodump-ng* con el siguiente comando:

airodump-ng -c 1 --bssid 00:23:51:43:28:29 -w infoWEP wifi0

La descripción del contenido del comando es el siguiente:

- **-c** Canal de la red inalámbrica, en este caso es 1.
- **--bssid** dirección MAC del punto de acceso del que se obtendrá la contraseña.
- **-w** archivo donde se guardarán los paquetes en este caso es infoWEP. utilizado en un paso posterior para poder descifrar la contraseña.
- **Wifi0** interfaz inalámbrica.

Una vez hecho lo anterior, se prosigue a realizar una falsa autenticación, esto servirá para que el AP (Access Point) no rechace los paquetes que serán inyectados. Para ello se utiliza el comando aireplay-ng en una nueva Shell y se ejecuta el siguiente comando:

 # aireplay-ng -1 0 –e INFINITUM2295 -a 00:23:51:43:28:29 -h 00:11:22:33:44:55 wifi0

Los elementos de la sentencia anterior significan:

- **-1** lo usa *aireplay* para hacer la falsa autentificación, el **0** indica que se autentica una sola vez.
- **-e** Nombre del Access Point (ESSID).
- **-a** Dirección MAC del Access Point (BSSID).
- **-h** MAC que será asociada con el Access Point, en este caso se usa una MAC ficticia para no dar la información real de la tarjeta inalámbrica.

En la Figura 8 se puede observar que se hace la petición de la autenticación y que ésta fue exitosa, por lo que se envía la asociación.

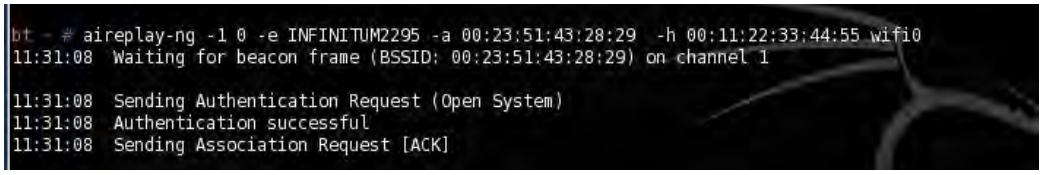

Figura 8 Falsa autenticación

Una vez efectuada la asociación, se capturan las peticiones ARP con el comando *aireplay-ng*, es necesario hacer reinyecciones en la red, con esto se generan paquetes que sirven para poder descifrar la contraseña. En una Shell se ejecuta el siguiente comando:

aireplay-ng -3 -b 00:23:51:43:28:29 -h 00:11:22:33:44:55 wifi0

Los elementos del comando significan:

- **-3** Captura y reenvió de las peticiones ARP
- **-a** Dirección MAC del Access Point (BSSID)
- **-h** Dirección MAC previamente asociada

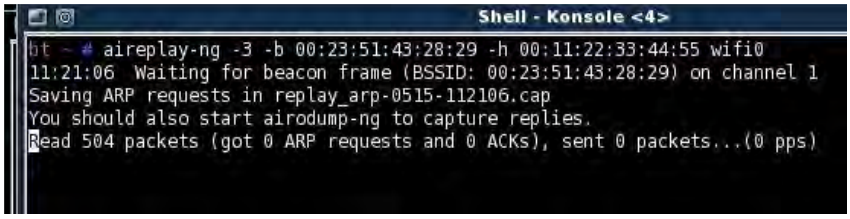

Figura 9 Inyección de paquetes

En la Figura 9 se puede apreciar que aireplay comenzará con la captura de paquetes ARP, es cuestión de a lo mucho 10 minutos para tener a próximamente 160000 mil paquetes necesario para descifrar la clave WEP.

El resultado de la captura de paquetes se puede apreciar en la Figura 10.

Figura 10 Captura de paquetes

Una vez conseguido el número de peticiones ARP necesarios se finaliza la captura con CTRL + C. seguidamente se descifra la clave WEP de la red usando *aircrack*.

Aircrack puede recuperar una clave WEP una vez que se hayan capturado suficientes paquetes cifrados. Usando una serie de ataques, basados en estadísticas, y fuerza bruta combinados, es relativamente fácil obtener la contraseña.

En un nuevo Shell, se debe ejecutar el siguiente comando:

aircrack-ng InfoWEP.cap

- **InfoWEP.cap** Archivo de captura de airodump-ng

Aircrack muestra redes proporcionando información como tipo de cifrado y número de IV capturados para cada una. La Figura 11 muestra los resultados del comando que realiza el ataque comprobando que ahora la red se encuentra comprometida.

Figura 11 Clave encontrada

Fallas en la descifrado WEP

En el momento de escanear redes con *airodump-ng* habrá problemas si la señal es muy pobre, por lo tanto habrá que optar por redes donde la señal sea buena o de lo contrario será difícil poder obtener la contraseña. Como se aprecia en la Figura 12 la señal de la red es muy pobre lo que da como resultado que se envié las peticiones de autenticación y estas no puedan ser aceptadas.

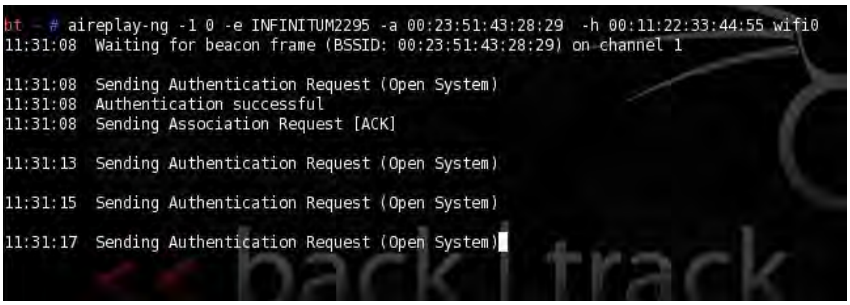

Figura 12 Autenticación Fallida

Es importante mencionar que algunos ESSID están nombrados con 2 palabras separadas por un espacio en blanco por ejemplo: Alicia Key, en este caso *aireplay* puede no encontrarla por lo que cuando se escribe es necesario que se encuentre entre comillas “Alicia Key” o incluyendo un carácter de escape \, con la cual se indica que el siguiente carácter es en blanco “Alicia\ Key”

WPA

El estándar WPA (*Wi-FI Protected Access*) tiene su origen en los problemas detectados en el anterior sistema de seguridad creado para las redes inalámbricas. La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i (WPA2), el cual estaba por llegar.

WPA fue desarrollado por la Wi-Fi Alliance para mejorar el nivel de codificación existente en WEP, la cual era menos segura por contar con un nivel de cifrado menos avanzado. Aportaba también un elemento del que WEP carecía: autenticación de usuario.

Las principales características de WPA son las siguientes:

- Autenticación y Cifrado usando TKIP (*Temporal Key Integrity Protocol*).
- Integridad con MIC (*Message Integrity Check*).
- Puede incorporar un servidor de autenticación (*RADIUS*) para el manejo de las claves.
- En el encabezado se envía el hash del IV (Vector de inicialización) y no en texto claro.

WPA utiliza TKIP que tiene la misma estructura de algoritmo que WEP para llevar a cabo el cifrado de los datos. TKIP cifra cada paquete de datos con una única clave de cifrado y las claves son mucho más fuertes. Propone 3 mejoras importantes:

- **Combinación de clave por paquete:** La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (*Pre-shared Key*). Genera dinámicamente una clave entre 280 trillones por cada paquete.
- **IV (Vector de inicialización) de 48 bits:** Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad. Los 48 bits los cuales permiten más combinaciones de claves.

- **MIC (*Message Integrity Check*):** Se crea para evitar los ataques "*man in the middle*". Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y generará una alerta, que indicará una posible falsificación del mismo.

TKIP inicia mediante una clave de 128 bits compartida entre los usuarios y los puntos de acceso (AP), esta clave se combina con la dirección MAC del usuario y se añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos. Utiliza cifrado entre la estación cliente y el Punto de Acceso con clave simétrica.

Para el cifrado emplea 4 claves distintas entre Punto de Acceso (AP) y cada Cliente *Wireless* para tráfico *Unicast* y 2 claves para tráfico *broadcast* o *multicast* y se cambian cada 10.000 paquetes o cada 10 Kb de transferencia.

La Figura 13 ilustra el formato de los datos de protocolo MAC 802.11 cifrada con algoritmo TKIP (14).

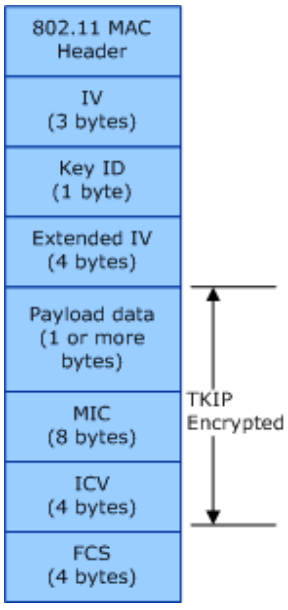

Figura 13 Formato de datos cifrado TKIP

A continuación se presenta el contenido de un paquete cifrado TKIP

- Vectores de inicialización (IV): Contiene 3 bytes para el contador de secuencia de TKIP (TSC) y es usado para protección.
- Clave de identificación (ID): Está constituido por 8 bytes en donde los que van de 0 a 4 son usados de reserva y llevan cero, el bit 5 está configurado para indicar la presencia del campo IV extendido y los bits 6 a 7 se usan para almacenar el índice de la clave, dentro de la tabla de claves por defecto.
- IV Extendido: Contiene los bits 5 a 2 del TSC
- Carga útil de datos: Aquí se encuentran los datos de los paquetes de la unidad de datos de servicio MAC (MSDU).
- MIC: Se calcula usando el algoritmo de Michael en toda la carga de datos de los paquetes MDSU. Añade 8 bytes al final de ultimo MPDU del MDSU
- Valor de verificación de integridad (ICV): Es la suma de comprobación que se calcula con los datos sin cifrar.
- Secuencia del marco de verificación (FCS): El IEEE de 32 bits Código de redundancia cíclica (CRC) calculado en todos los ámbitos de la MPDU.

Integridad con MIC (Message Integrity Check)

MIC es un hash que se calcula sobre una base por paquete, lo cual indica que uno solo podría abarcar varios marcos y manejar la fragmentación (15). El hash es un valor numérico de longitud fija que identifica datos de forma unívoca.

El protocolo fue creado para ayudar a luchar contra ataques de modificación de mensajes que fueron frecuentes en el protocolo WEP.

MIC se basa en un valor semilla (seed value) o clave secreta, en una MAC de origen y destino; y una carga útil (payload). Si alguno de estos valores es cambiado la MIC se vería seriamente afectada.

WPA2

La Wi-Fi Alliance lanzó en septiembre de 2004 WPA2, que es la implementación de la especificación completa del estándar IEEE 802.11i. Elimina muchas de las debilidades de sus predecesores tanto en lo que autenticación de usuarios como a robustez mediante el método de cifrado *Advanced Encryption Standard* (AES).

El sistema AES, diseñado por Vincent Rijmen y Joan Daemen, funciona para varios tamaños en los bloques de información. Sin embargo, el AES está especificado para un bloque de 128 bits de tamaño y llaves de: 128, 192 y 256 bits de tamaño. Fue desarrollado originalmente para WPA pero ante la impaciencia de los fabricantes se empezó a emplear WPA con TKIP.

IEEE 802.11i y WPA2 son implícitamente idénticos. Ambos usan AES como método de cifrado en lugar de RC4/TKIP usado en WPA y añaden, opcionalmente, pre-autenticación a WPA.

AES es el estándar de cifrado basado en bloques que a partir del año 2000 utiliza el algoritmo Rijndael. Se usa para asegurar la red inalámbrica de transmisión de datos con WPA2. Es un algoritmo de cifrado por bloques con longitud de bloque y longitud de clave variables.

Descifrar WPA/WPA2

El protocolo de seguridad WPA (*Wi-Fi Protected Access*) se puede dividir a grandes rasgos en dos modalidades (16):

- WPA empresarial: Diseñado para trabajar con un servidor de autentificación de los usuarios en la red, que en la mayoría de los casos es un servidor RADIUS, suele ser el usado por proveedores de servicios de Internet (ISP).
- WPA personal: Conocido también como WPA-PSK (*Pre Shared Key*), se basa en una autentificación por contraseña del cliente *Wireless* al punto de acceso, se encuentra en la mayoría de las redes caseras y pequeñas oficinas.

Una de las vulnerabilidades está en el ataque contra la clave PSK de WPA/WPA2. La PSK proporciona una alternativa a la generación de 802.1X usando un servidor de autentificación, pero queda en evidencia que es mejor solución emplear un servidor RADIUS.

Para descifrar habrá que intentar obtener la clave de red, para esto basta con un sólo paquete que contenga la autentificación del cliente al punto de acceso (*handshake*). Esto se logra con la captura y el descifrado mediante un ataque de fuerza bruta con un diccionario; el éxito del ataque está ligado a la robustez de la contraseña que puede tener de 8 a 63 caracteres ASCII.

Para realizar la siguiente prueba se utilizará de nueva cuenta la suite *aircrack-ng*, *BackTrack* 3 y la computadora portátil HP *Pavilion* dv2125LA. .

En la captura de paquetes se necesita la tarjeta de red inalámbrica en modo monitor y prepararla para que pueda inyectar trafico a la red, así como también

cambiar la dirección MAC de la tarjeta esto es con el fin de evitar que sea descubierto, siguiendo los mismos pasos que en la clave WEP.

Ahora se escanean las redes que se encuentran al alcance y para ello se emplea el *airodump-ng*, en la Shell escribe el siguiente comando:

airodump-ng wifi0

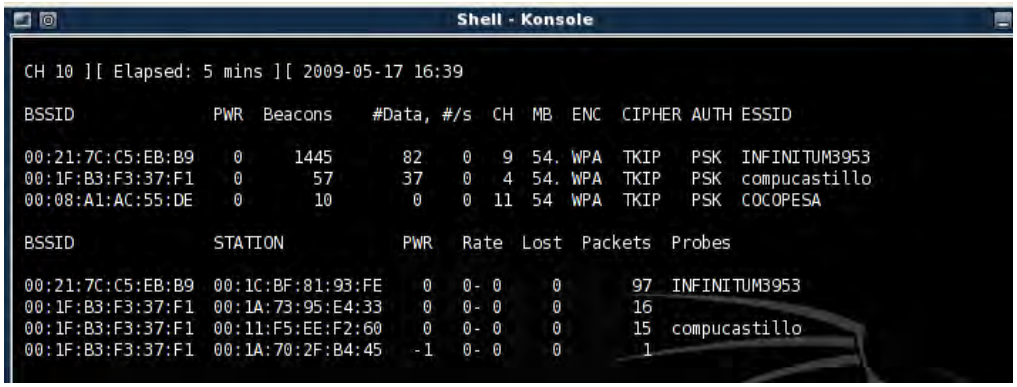

Figura 14 Escaneo de redes

La Figura 14 muestra 3 redes próximas pero se intentará conectar a la red “INFINITUM3953”. Es importante mencionar que para que se efectúe la captura de paquete de *Handshake* es necesario que al menos un cliente se encuentre asociado al AP. Se empieza con la captura de los datos usando el *airodump-ng*:

 # airodump-ng -c 9 --bssid 00:21:7C:C5:EB:B9 -w infoWPA wifi0

Donde los componentes significan lo siguiente:

- **-c** Canal del AP (Access Point).
- **--bssid** MAC del AP (Access Point).
- **-w** guardará los datos obtenidos en el archivo "infoWPA".
- **Wifi0** interfaz adaptador inalámbrico.

En la Figura 15 se puede apreciar que la captura de los datos de Handshake se centra en el AP que eligió.

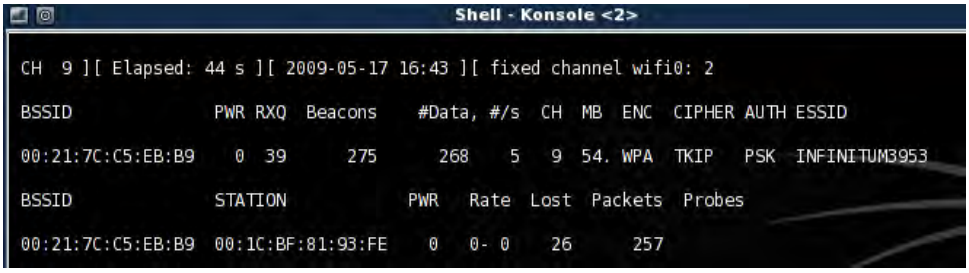

Figura 15 Captura de Handshake

Mientras se encuentra capturando los paquetes, se procede a la des-autenticación del cliente, esto es para forzarlo a volverse a autenticar y generar peticiones ARP. Esto se hace usando el siguiente comando

 # aireplay-ng -0 15 -a 00:21:7C:C5:EB:B9 -c 00:1C:BF:81:93:F3 wifi0

- **-0** significa des-autenticación
- **15** el número de des-autenticaciones a enviar
- **-a** dirección MAC del AP
- **-c** dirección MAC del cliente a des-autenticar

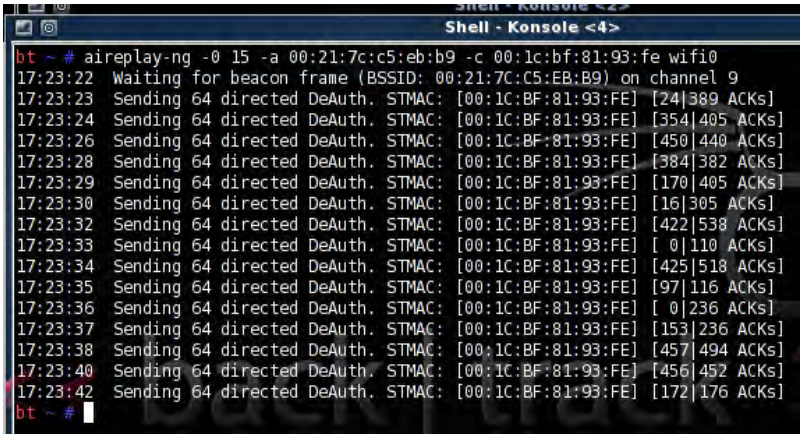

Figura 16 Des-autenticación de clientes

Una vez hecha la des-autenticación, representado en la Figura 16, y haber obtenido los paquetes de datos, se está listo para descifrar la contraseña como se aprecia en la Figura 17. Esto es mediante el uso de diccionarios los cuales contienen una amplia lista de posibles contraseñas:

aircrack-ng -w password.lst InfoWPA.cap

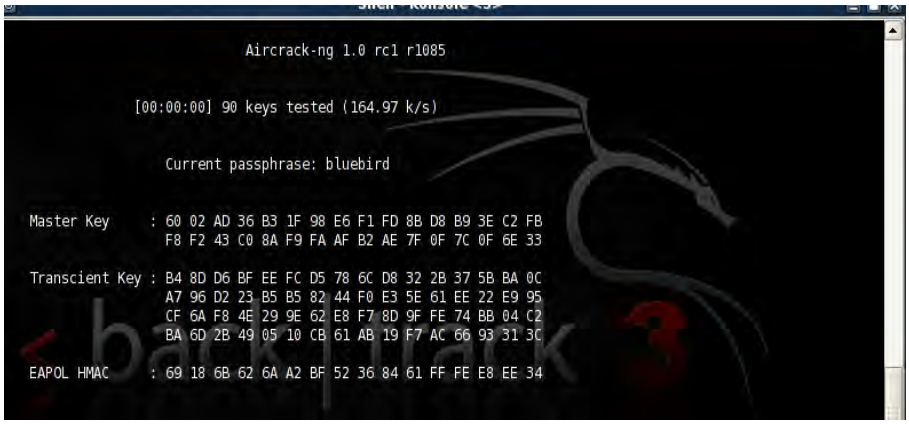

Figura 17. Desencripción de clave WPA

El cifrado WPA que usa autenticación RADIUS es imposible de descifrar usando la fuerza bruta, por lo que es necesario algún otro tipo de ataque como

lo son el ataque Rogue. Dicho ataque consiste en suplantar la identidad de un AP legitimo por uno con acceso no autorizado, y el ataque LEAP que consiste en ataques de diccionario (esto es para dispositivos CISCO), debido a que la clave se genera para cada sesión lo que hace que ésta sea difícil de descubrir.

Conclusiones

El análisis realizado permite determinar algunos de los puntos vulnerables dependiendo del tipo de cifrado en la seguridad de una red inalámbrica.
El cifrado WEP presenta una debilidad importante que radica en el vector de inicialización (IV), esto ocasiona que se pueda descubrir la contraseña de una red en pocos minutos, generalmente los dispositivos de red vienen configurados por defecto con este tipo de cifrado y pocas veces los usuarios cambian estas contraseñas.
WPA y WPA2 mejoran el cifrado debido a que usan claves temporales (TKIP), lo cual permite que no se pueda enviar ataques de recuperación de claves como en WEP.
Aunque en WPA la debilidad se encuentra en el sistema que implementa llamado WPA-PSK (WPA con una clave previamente compartida) es necesario el uso de la fuerza bruta mediante ataques de diccionarios los cuales pueden contener las posibles claves de AP. Estos diccionarios deben ser lo más completo posibles, para que la búsqueda sea exitosa; esto puede llevarse de un par de horas hasta varias semanas.

En respuesta a ello es necesario usar contraseñas robustas, es decir, con características como contar con un mínimo de 8 caracteres, combinar letras y números, mayúsculas y minúsculas además de caracteres especiales. Lo anterior permite tener una red más confiable. Además se puede reforzar realizando filtrado de MAC para determinar cuáles computadoras podrán conectarse a la red.

Para las Pequeña Oficina/Oficina en casa (SOHO por sus siglas en inglés), es necesario cambiar las contraseñas a WPA o WPA2; debido a que aun siendo pequeñas empresas, por defecto las compañías que proveen el servicio de Internet configuran sus equipos con una contraseña WEP. Además por lo visto en el presente trabajo, se ha demostrado que es poco seguro y que personas con habilidades básicas en el manejo de herramientas de análisis inalámbrico puedan comprometer sus redes.

Es recomendable que al usar aplicaciones específicas como *BackTrack* 3 para poder escanear las redes se tome en cuenta aspectos de compatibilidad, del hardware de las tarjetas inalámbricas, contar con diccionarios adecuados y software especializado en el análisis de vulnerabilidades de redes inalámbricas.

Para futuras investigaciones habrá que analizar los parámetros de configuración de las contraseñas de red, porque estas irán cambiando conforme a las necesidades que los usuarios vayan requiriendo en cuanto a la seguridad de los datos que transmitan.

Los ataques a las redes inalámbricas son cada vez más frecuentes, esto se debe a que la seguridad que tienen no son tan sólidas como las redes cableadas, sin embargo habrá que estar un paso adelante para poder prever un ataque o al menos mitigar su impacto.

Bibliografía

1. **ACTA .** Wi-Fi: conectividad en todo lugar y en todo momento. [En línea] [Citado el: 3 de Diciembre de 2008.] http://www.acta.es/articulos_mf/35031.pdf.

2. IEEE Standards Association. [En línea] [Citado el: 22 de Septiembre de 2008.] http://standards.ieee.org/getieee802/802.11.html.

3. **Agnitum.** Recomendaciones básicas de seguridad para redes inalámbricas. [En línea] 2008. [Citado el: 1 de Diciembre de 2008.] http://www.outpost-es.com/pressroom_security_insight/2007-06.html.

4. **Carballar, José Antonio.** *WI-FI: Cómo construir una red inalámbrica.* México : Alfaomega, 2005.

5. **Jaime, Cuéllar Ruiz.** Enter@te en linea. [En línea] 2008. [Citado el: 17 de Septiembre de 2008.] http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm.

6. **remote-exploit.** BackTrack. [En línea] [Citado el: 2 de Septiembre de 2008.] http://www.remote-exploit.org/backtrack.html.

7. Información general sobre redes inalámbricas. [En línea] [Citado el: 25 de Enero de 2009.] http://support.dell.com/support/edocs/network/p57205/sp/intro/wireless.htm.

8. **Andreu, Fernando, Pellejero, Izaskun y Lesta, Amaia.** *Fundamentos Y Aplicaciones De Seguridad En Redes Wlan.* España : Marcombo S.A., 2006. 8426714056.

9. **Tech Support y Computer Security.** SmartComputing. [En línea] [Citado el: 7 de Febrero de 2009.] http://www.smartcomputing.com/editorial/dictionary/detail.asp?&searchtype=0&DicID=19634&RefType=Encyclopedia.

10. **Pellejero, Izaskun, Andreu, Fernando y Lesta, Amaia.** *Fundamentos y aplicaciones de seguridad en redes WLAN.* s.l. : Marcombo, 2006. 8426714056.

11. **Chavarría Rodríguez, Róger y Murillo Hernández, Emilio.** Redes Inalámbricas de Área Local (WLAN) de Alta Velocidad. [En línea] 2004. [Citado el: 21 de Febrero de 2009.] http://www.eie.ucr.ac.cr/uploads/file/proybach/pb0406t.pdf.

12. **GALPon.** Vulnerabilidades del protocolo WEP. [En línea] [Citado el: 21 de Febrero de 2009.] http://www.galpon.org/wiki/images/4/4b/GALPonada_Taller_de_seguridad_WIFI.pdf.

13. Aircrack-ng . [En línea] [Citado el: 3 de Febrero de 2009.] http://aircrack-ng.org/doku.php.

14. **Microsoft Corporation.** TKIP. [En línea] [Citado el: 31 de 2009 de Enero.] http://msdn.microsoft.com/en-us/library/aa503357.aspx.

15. **Haas, Herbert.** Perihel. *WLAN Security.* [En línea] [Citado el: 25 de 2008 de Diciembre .] http://www.perihel.at/2/wlan/07WL-Security-C-TKIP-MIC-v2.1.pdf.

16. **DELL.** Descripción de la seguridad. [En línea] [Citado el: 5 de Febrero de 2009.] http://supportapj.dell.com/support/edocs/network/R196255/sp/overview.htm.

Glosario

802.11: Estándar para comunicaciones inalámbricas aceptado en 1997 por el IEEE, que actualmente rige la conexiones Wi-Fi y determina sus características

Access Point (AP): Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

ARP: Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

BSSID: Dirección única que identifica al un punto de acceso o router en la red inalámbrica.

CRC-32: Código de Redundancia Cíclica utilizado para verificar la integridad de los datos de transmisión,

Dirección MAC: Es un identificador único asociado con una parte del equipo de red o, más concretamente, su interfaz con la red.

ESSID: Es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos, es el nombre de la red.

HANDSHAKE: Es el protocolo de comienzo de comunicación entre dos máquinas o sistemas.

IEEE: Institución americana responsable de la creación de una gran cantidad de estándares en electrónica e informática (Institute of Electrical and Electronics Engineers).

Mbps: Medida de la velocidad de bits, es decir, la velocidad a la que pasan los bits en un punto determinado.

RC4: Algoritmo de cifrado que provee confidencialidad al WEP.

SSID: Identificador de red inalámbrica.

WLAN: Es una red de área local inalámbrica que utiliza ondas de radio como portador, donde las conexiones de red para los usuarios finales son inalámbricas.