Atacar WPA/WPA2 PSK

Autores: Alejandro Martín y Chema Alonso

http://elladodelmal.blogspot.com/

Recopilación: Lic. Cristian Borghello, CISSP

Fecha Publicación: 30 de agosto de 2008

Estos documentos han sido escritos y publicados por Chema Alonso en su Blog.

Indice

Atacar WPA/WPA2 PSK

http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-i-de-iv.html

Hablar de seguridad Wireless en el ámbito domestico es hablar, irremediablemente, de WPA/WPA2 PSK, dejando a un lado el viejo y vulnerado cifrado WEP. Sí, existen puntos de Acceso WiFi con servidor RADIUS incorporados, pero no es lo más común que se encuentra en el router que utiliza una familia para conectarse a Internet en su casa.

En el presente artículo vamos a ver de forma práctica cómo funcionan las amenazas en WPA/WPA-2 PSK en el ámbito domestico. Para ello se verá como se puede atacar una infraestructura de estas características y cuáles son las recomendaciones de seguridad.

WPA/WPA2

WPA [*Wifi Protected Access*] surge como una solución temporal de la Wi-Fi Alliance mientras que en IEEE se trabajaba sobre el estándar IEEE 802.11i para securizar las redes Wireless una vez que quedó de manifiesto la debilidad de WEP [*Wired Equivalent Privacy*]. Cuando IEEE sacó a la luz 802.11i, la Wi-Fi Alliance proporcionó la certificación WPA2 a todos aquellos dispositivos que cumplían con las especificaciones marcadas por el nuevo estándar. Ambas soluciones, WPA y WPA2, soportan el protocolo 802.1x para la autenticación en ámbitos empresariales y la autenticación mediante clave compartida (PSK) [*Pre-Shared Key*] para los entornos SOHO [*Small Office and Home Office*] y ámbitos domésticos.

WPA y WPA2 se diferencian poco conceptualmente y difieren principalmente en el algoritmo de cifrado que emplean. Mientras WPA basa el cifrado de las comunicaciones en el uso del algoritmo TKIP [*Temporary Key Integrity Protocol*], que está basado en RC4 al igual que WEP, WPA2 utiliza CCMP [*Counter-mode/CBC-MAC Protocol*] basado en AES [*Advanced Encrytion System*]. La segunda diferencia notable se encuentra en el algoritmo utilizado para controlar la integridad del mensaje. Mientras WPA usa una versión menos elaborada para la generación del código MIC [*Message Integrity Code*], o código *"Michael"*, WPA2 implementa una versión mejorada de MIC.

Lógicamente, a la hora de elegir cómo securizar la red domestica, mejor decantarse por WPA2-PSK debido a que la fortaleza de cifrado de AES es netamente superior a la de TKIP. Sin embargo, si no se cuenta con el hardware que soporte esta tecnología es perfectamente válido el uso de WPA-PSK pues la principal vulnerabilidad de WPA-PSK y WPA2-PSK no se encuentra en el algoritmo de cifrado sino en la fortaleza de la clave utilizada.

Arquitectura WPA/WPA2 PSK

Tanto WPA-PSK como WPA2-PSK adolecen de vulnerabilidad y es posible atacar estas tecnologías con el objetivo de poder hacer uso de la red e incluso escuchar y analizar el tráfico que por ella se propaga. En este articulo se pretenden reflejar por qué y dónde es vulnerable WPA-PSK y WPA2-PSK, cómo explotar esta vulnerabilidad y cómo proteger adecuadamente la red.

Para entender las vulnerabilidades hemos primero de analizar el proceso de asociación de un cliente a la red wireless. Independientemente del sistema de

seguridad que se elija para la red (WEP, WPA-PSK o WPA2-PSK), el proceso de asociación es siempre el mismo. Este proceso va a depender de si el punto de acceso está emitiendo tramas *"Beacon Frame"* para el anuncio de la red mediante la publicación de su ESSID [*Extended Service Set Indentifier*] o no.

Si el punto de acceso está emitiendo tramas *"Beacon frame"* el cliente se conecta a la red en dos fases, una primera Fase de Autenticación, que podrá ser abierta o con clave compartida, y una segunda Fase de Asociación.

En el supuesto caso de que el punto de acceso no esté emitiendo *"Beacon frames"* existe una Fase de Prueba inicial dónde el cliente envía el ESSID de la red wireless a la que quiere conectarse esperando que el punto de acceso responda y así iniciar las fases de Autenticación y Asociación. Todo este proceso, para una conexión WPA2-PSK puede verse en la imagen siguiente. En ella se pueden ver las tres fases descritas.

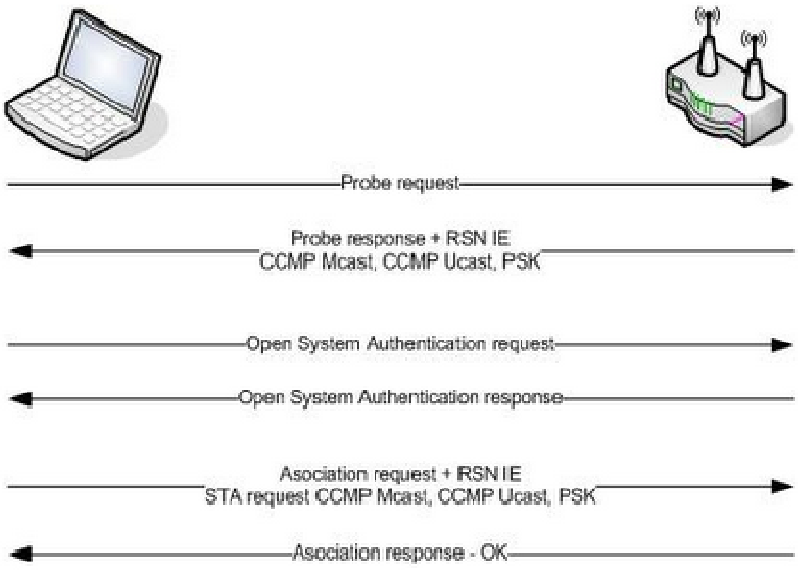

Imagen 1: Negociación WPA2-PSK en una red sin publicación de ESSID

La única diferencia con una red Abierta o WEP, es que punto de acceso y cliente acuerdan la política de seguridad a seguir, siendo ésta la primera fase del proceso de autenticación de una red WPA/WPA2.

Esta forma de funcionar es importante conocerla, pues como puede verse en al imagen, el cliente se conecta inicialmente a la red sin que haya comenzado el proceso de autenticación WPA/WPA2, tanto si es por medio de PSK como si no, por lo que el tráfico enviado todavía no está siendo cifrado. Debido a esta situación un atacante podría mandar una trama de des-asociación a un cliente de la red provocando que éste se desasocie e inicie un proceso de asociación nuevamente y un nuevo proceso de autenticación WPA/WPA2. A esto se le conoce como el ataque 0 o de des-asociación.

Este proceso de re-autenticación se realizaría únicamente si la conexión se tratase de WPA/WPA2 empresarial, es decir, la conexión está configurada utilizando 802.1x para la autenticación del puerto y EAP [*Extended Authetication Protocol*] contra un servidor RADIUS [*Remote Authentication Dial-In Service*] para autenticar la conexión. En el caso de WPA/WPA2 con PSK se pasa directamente a la fase de intercambio de claves.

En la fase de Intercambio de claves el cliente y el AP utilizan la PSK para generar un clave llamada PMK [*Pairwise Master Key*]. Esta PMK es una derivada cuando el sistema es WPA/WPA2 empresarial pero es la misma PSK en los entornos WPA/WPA2 PSK.

Con la PMK se genera una clave de cifrado para cada proceso de autenticación de un cliente llamada PTK que básicamente se genera a partir de dos números aleatorios, uno de ellos generado por el cliente y el otro por el punto de acceso que intercambian para obtener ambos la misma clave PTK. Este proceso se llama 4-way-Handshake.

Una vez que el cliente está autenticado, el protocolo TKIP utiliza 6 claves de cifrado por cada sesión, 4 de ellas son utilizadas para comunicaciones unicast y 2 para comunicaciones broadcast. Estas claves son únicas por cliente y sesión y se cambian periódicamente. Estas claves se generan a partir de derivadas de las direcciones MAC, ESSID y la PTK.

¿Cómo puede ser vulnerada la red WPA/WPA2 PSK?

Un atacante que quiera vulnerar una red WPA-PSK va a tratar de capturar ese intercambio de números aleatorios, para una vez conocidos estos, junto con el SSID y las direcciones MAC del cliente y el punto de acceso de la red obtener la frase o secreto compartido que se utilizó. Una vez que el atacante tenga la clave compartida se podrá conectar a la red.

¿Podrá el atacante acceder al tráfico generado por otro usuario?

En teoría no debería poder, pues las claves TKIP que se generan son únicas y por sesión pero sí el atacante está conectado a la red y captura todo el proceso de autenticación de otro usuario podría acceder a los números aleatorios intercambiados y al poder conocer el ESSID, la PSK y la MAC del cliente y el punto de acceso, podría generar la PTK. Con la PTK podría descubrir cuáles son las claves TKIP que se intercambian cifradas. Una vez que el atacante tiene las claves TKIP tiene acceso a todo el tráfico y por tanto SÍ puede acceder a los datos transmitidos. El proceso con WPA2-PSK es similar y el atacante buscará las claves que se intercambian en AES-CCMP.

¿Se podrá modificar la información en tránsito?

WPA y WPA2 implementan de forma distinta el MIC [Message Integrity Code] y, aunque en teoría el MIC de WPA podría ser engañado, las condiciones para poder realizar dicho cambio no se dan en la implementación práctica que se hace. Está bien explicado este aspecto y puedes leer más sobre él en el trabajo "Observations on the Message Integrity Code in IEEE802.11Wireless LANs" de Jianyong Huang, Willy Susilo y Jennifer Seberry de la School of Information Technology and Computer Science de la University of Wollongong en Australia.

No obstante, si deseas conocer a fondo la teoría de los ataques a los protocolos Wireless, el artículo de Guillaume Lehembre, publicado en la revista Hackin9 es de lo mejor que existe. Y además, está traducido al castellano: Seguridad WiFi – WEP, WPA y WPA2

Capturar el Handshake

http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-ii-de-iv.html

Cómo se ha indicado en el punto anterior, un atacante que quiera vulnerar o romper una red WPA/WPA2 debe monitorizar todas las tramas que se intercambian en la red Wireless durante el proceso de autenticación PSK para obtener los números aleatorios intercambiados. De esta forma se podrá descubrir la clave PSK que se está utilizando en la red para autenticar a los clientes.

Para monitorizar la red en un entorno Windows se puede utilizar Commview for Wifi u Omnipeek según el soporte que proporcionen a las tarjetas que vamos a utilizar, por supuesto existen más herramientas.

En este articulo se ha utilizado Commview for Wifi, junto con el chipset Intel Centrino Pro Wireless 2200BG, mientras que para las inyecciones de tráfico se ha utilizado la tarjeta Orinoco 11a/b/g ComboCard 8480-FC.

En primer lugar es necesario cargar el driver que proporciona ***Commview***, bien a través del asistente del programa o a través del administrador de dispositivos, en cualquier caso el controlador de la tarjeta debe quedar con el driver como se indica en la imagen 2.

Imagen 2: Driver de commview instalado

Una vez instalado correctamente el driver, en la barra de herramientas principal de ***Commview*** se debe activar la captura de tráfico con el botón de Play. Con la captura de tráfico activada se podrá comenzar la exploración de los canales WI-FI accesibles, como se muestra en la Imagen 3.

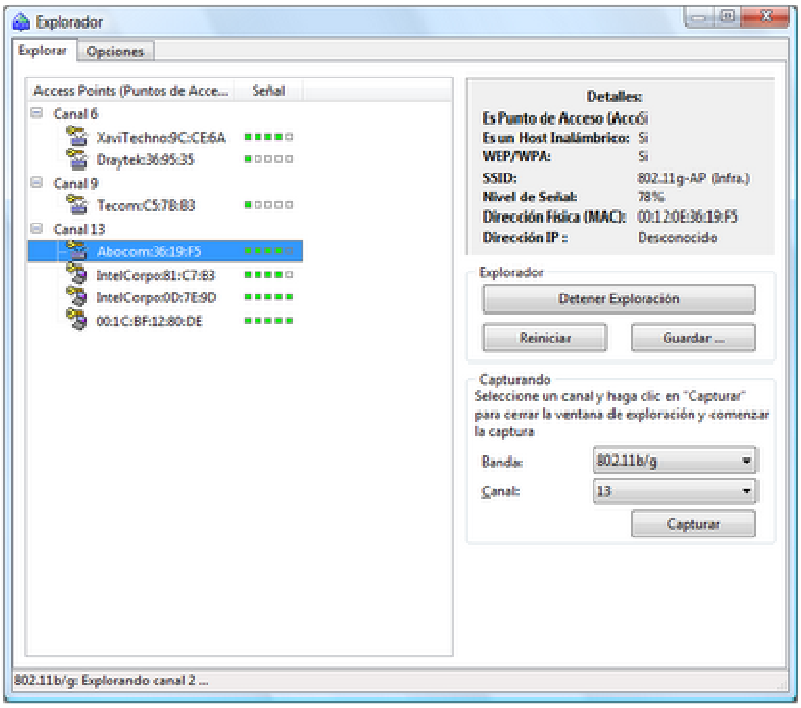

Imagen 3: Exploración de puntos de acceso

Commview mostrará todas las redes disponibles en todos los canales ofreciendo una visión global del espacio WI-FI del área. Una vez seleccionada la red objetivo, basta con activar la captura de paquetes de esa red con el botón de capturar que se encuentra en el panel de opciones de la derecha.

Commview muestra, en la pestaña Nodos, los puntos de acceso y clientes asociados que usan el canal en un determinado instante.

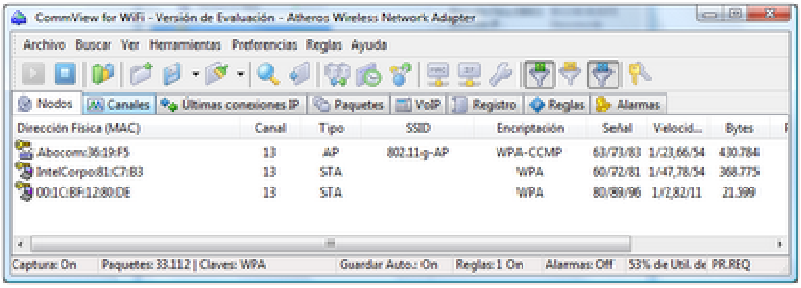

Imagen 4: Nodos usando el canal

En la imagen 4 se puede ver un punto de acceso usando WPA2-PSK con cifrado CCMP y dos clientes que se encuentran asociados a la red. En estos momentos ***Commview*** se encuentra capturando todos los paquetes que circulan por el canal. Para no saturar el equipo, dado que el objetivo en un primer momento, es capturar el intercambio de los números aleatorios en el proceso de autenticación WPA/WPA2, es suficiente con capturar únicamente los paquetes de datos. Para realizar esta selección de paquetes es posible añadir filtros en la captura, por ejemplo por direcciones MAC de los equipos.

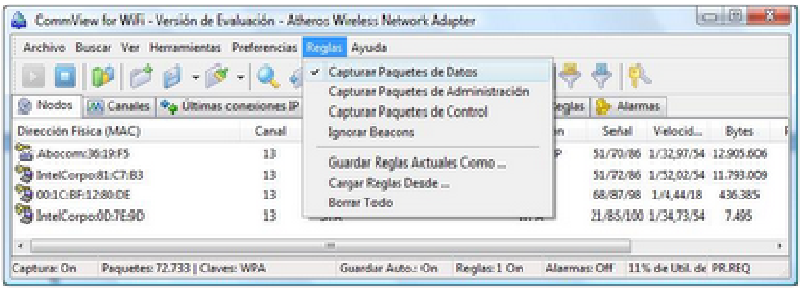

Imagen 5: Configuración de las reglas de captura

El ataque 0

Para obtener el intercambio de números aleatorios entre un equipo y el punto de acceso de forma rápida, es decir, sin esperar a que un nuevo equipo se conecte a la red, se lanza un ataque de desasociación de modo que se desconecte el equipo obligándolo a conectar de nuevo. Este proceso es automático en sistemas operaitos Windows XP pero se requiere de la intervención del usuario en Windows Vista. Para hacer esto desde Commview basta con acudir al menú herramientas y pulsar sobre ***Reasociación de Nodos***.

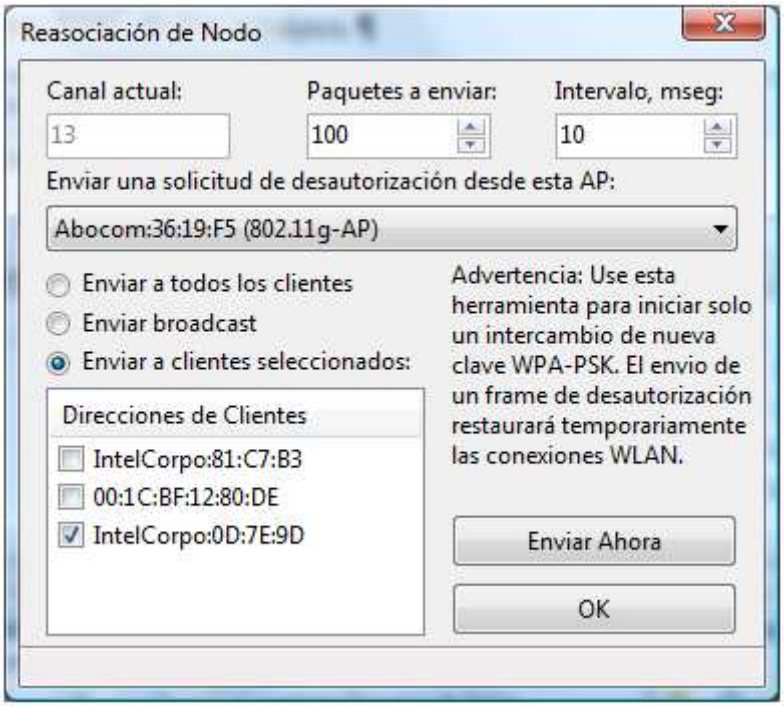

Imagen 6: Ataque para obligar a un nodo a reasociarse

Para tener acceso a estas opciones es necesario que la tarjeta wireless permita la inyección de paquetes. En caso de estar usando el chipset de ***Intel 2200BG***, no será posible realizar la inyección, con lo que la única solución es esperar a que algún cliente se autentifique con el punto de acceso.

En este cuadro de diálogo se selecciona el punto de acceso que va a ser spoofeado, es decir, la dirección que va ser simulada como origen de envío de la trama de desasociación, y el cliente que se quiere desasociar. Además, se debe indicar el número de paquetes a enviar.

Una vez lanzado el ataque, y dado que ***Commview*** ha estado capturando todos los paquetes, bastaría con almacenar los mismos en formato .cap, de modo que se tendrían todos los paquetes, incluidos aquellos donde se realiza el intercambio de números aleatorios listos para craquear la PSK que está siendo utilizada en esa red.

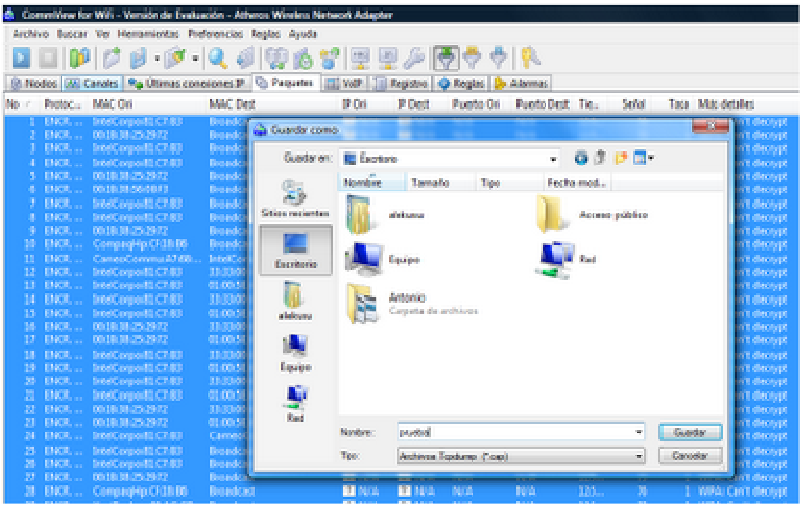

Imagen 7: Guardar los paquetes capturados

Crackeo de clave WPA/WPA2 PSK – Teoría

http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-iii-de-iv.html

En el modo WPA/WPA2 PSK la clave PMK de la cual se deriva luego la PTK se obtiene con la siguiente función:

PMK = PBKDF2(PSK, SSID, longitud SSID, 4096, 256)

Donde ***PBKDF2*** es una función de derivación de claves que forma parte de los estándares criptográficos de clave pública de los laboratorios RSA (PKCS). Se trata de una función pseudoaleatoria que se utiliza para derivar la clave (PMK) haciendo uso de la frase PSK y SSID.

Para derivar a partir de aquí la clave de cifrado por sesión (PTK) se hace uso de la PMK, los números aleatorios intercambiados, conocidos como anonce y snonce, y las direcciones MAC de cliente y punto de acceso. Dado que todo lo que se utiliza ha sido capturado salvo la PSK, basta con probar diferentes frases ya sea por fuerza bruta o mediante el uso de diccionario, para dar con la clave que se ha utilizado en el cifrado.

Para realizar este proceso de crackeo existe la posibilidad de utilizar tablas pre-calculadas [Rainbow tables] de modo que se incremente el número de pruebas que se pueden realizar por segundo para tratar de averiguar la clave. Esto es factible, sin embargo, existe una gran diferencia con el uso de este tipo de tablas en el crackeo de otras contraseñas.

El problema radica en que los hashes precalculados dependen del SSID de la red, con lo que no es posible tener precalculados todos los hashes para todos los posibles nombres de red. Existen proyectos, como el de Renderlab donde es posible obtener hasta 33 GB de hashes precalculados, partiendo de un diccionario (en inglés) y listado de SSID. Lógicamente aquí en España su utilidad es bastante más limitada.

Crackeo de clave WPA/WPA2 PSK – Práctica

Una vez que se han capturado los paquetes de una sesión de autenticación de un cliente, entonces puede ejecutarse un proceso de cracking de la clave PSK. Para realizar este proceso es posible utilizar Cain, una herramienta de auditoría de seguridad que entre otros módulos trae uno especial para craquear contraseñas. En la pestaña *Cracker* de ***Cain***, en el apartado *"802.11 Captures"* se debe importar el fichero *.cap* que contiene la captura de la autenticación de un cliente. ***Cain*** analiza el fichero de captura e indica si dentro del fichero .cap se encuentra algún Handshake válido del que se pueda extraer la clave PSK.

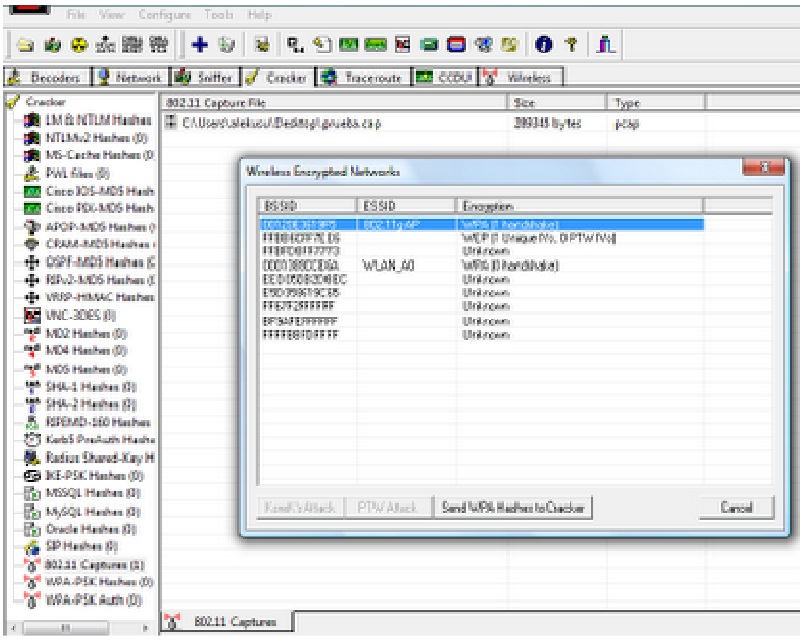

Imagen 8: Hanshake WPA2 capturado

Una vez que se tiene capturado el intercambio se envía a craquear, es posible utilizar un ataque por fuerza bruta o basarse en un diccionario para tratar de agilizar el proceso.

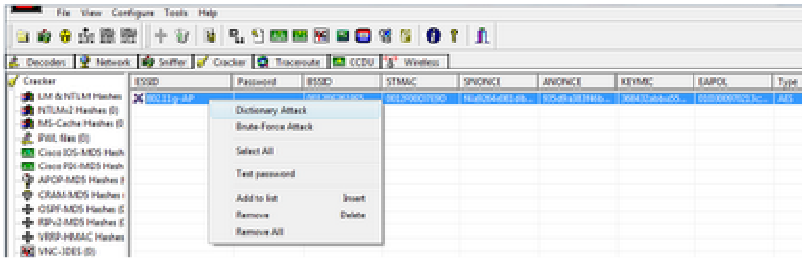

Imagen 9: Ataque sobre el hash de autenticación

El éxito del ataque ahora radica única y exclusivamente en la fortaleza de las password que haya utilizado el administrador de la red. Si ha colocado una clave de red que aparezca en un diccionario o la clave es suficientemente pequeña e insegura será factible romperla. Para tratar de romperla por fuerza bruta es necesario elegir el alfabeto a utilizar, las longitudes mínimas y máximas y empezar a probar.

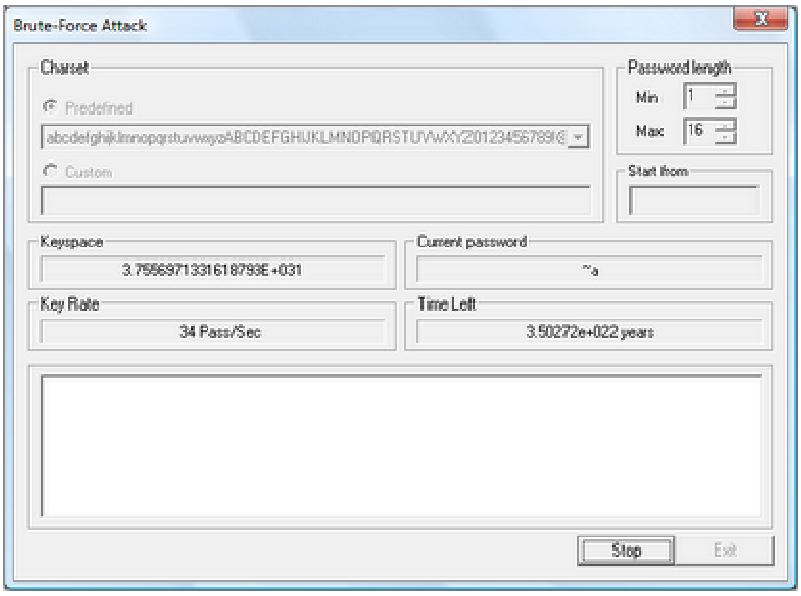

Imagen 10: Ataque por fuerza bruta sobre el hash de autenticación

Para el ataque basado en diccionario, es necesario contar con un buen diccionario, e indicar las posibles pruebas a realizar con cada una de las palabras disponibles en el diccionario.

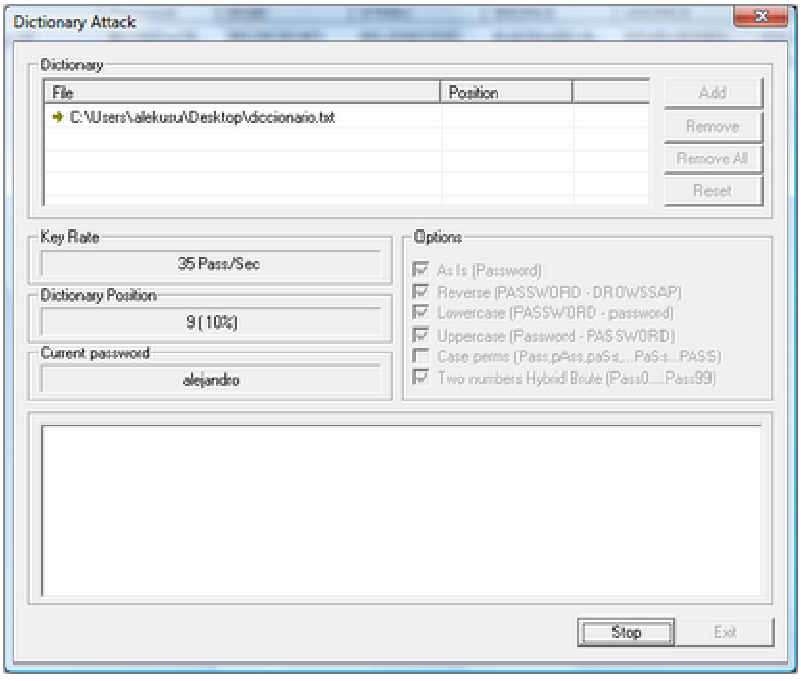

Imagen 11: Ataque por diccionario sobre el hash de autenticación

En cualquiera de los dos casos si consigue dar con la clave nos lo mostrará en la parte inferior con un mensaje como el siguiente:

Imagen 12: Resultado exitoso en el ataque sobre el hash de autenticación

La última versión de ***Cain*** tiene como limitación que no es capaz de trabajar con ciertos caracteres, con lo cual no sería posible crackear algunos hash de autenticación. Como alternativa a ***Cain*** se puede utilizar la suite aircrack, disponible tanto en Linux como en Windows, que permite trabajar con todo el abanico posible de caracteres.

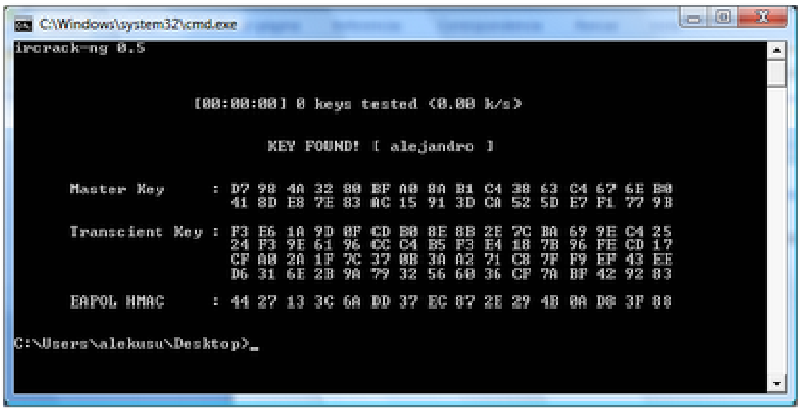

Imagen 13: Éxito en el ataque sobre el hash de autenticación con aircrak

Analizando el tráfico de otros usuarios

http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-iv-de-iv.html

Las conexiones en redes WPA/WPA2 utilizan claves por usuario y sesión derivadas de la clave PSK para el cifrado de los datos, de esta manera se supone que cada conexión tiene la privacidad necesaria para el usuario.

No obstante, si se captura el proceso de autenticación de un usuario en la red y al conocer la clave PSK que está siendo utilizada, las direcciones MAC y el SSID, basta con capturar los números Snounce y Anounce intercambiados para conocer cuál es la clave PMK y por tanto, poder acceder a las claves PTK del usuario.

Conocidas las claves PTK es posible descifrar todo el tráfico generado por un usuario. Si el usuario se encontrara conectado previamente no sería posible realizar este proceso pues no se habría podido capturar el proceso de autenticación. Por ello, es necesario realizar un ataque 0 al usuario al que se desea analizar el tráfico.

Análisis del trafico un usuario en una red WPA/WPA2-PSK

Commview permite analizar el tráfico tanto para redes WEP como para redes WPA/WPA2-PSK. Para realizar el descifrado de tráfico de la red en el menú preferencias, en la opción Claves WEP/WPA se pueden cargar las claves conocidas de las redes wireless.

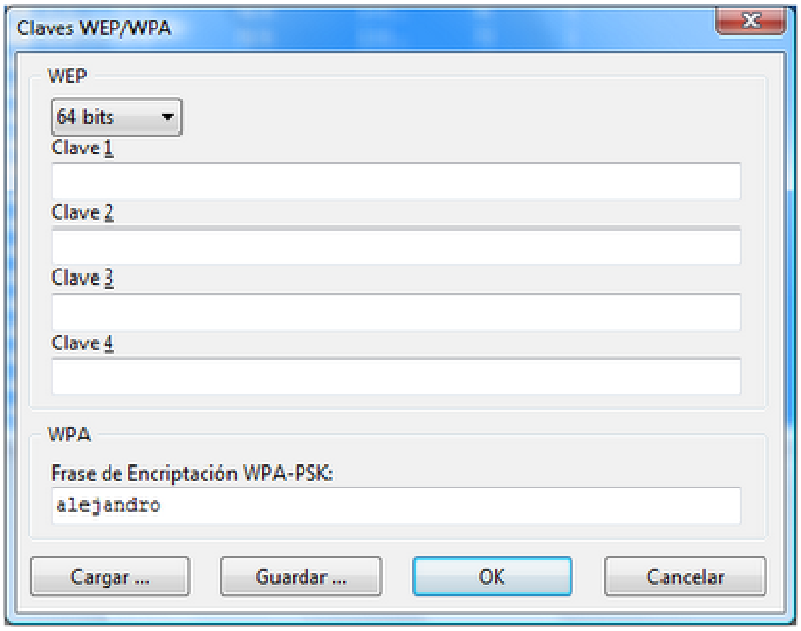

Imagen 14: Clave de cifrado WPA

A pesar de tener configurada la clave PSK de la red aún no sería posible descifrar el tráfico de red de un usuario que estuviera previamente. Para descubrir las claves que están siendo utilizadas por cada uno de los clientes es necesario lanzar un ataque 0 de des-asociación. Esto obligaría a los clientes a re-asociarse y ahora, al contar con la clave PSK de la red, ***Commview*** obtendrá la clave PMK e inmediatamente las claves de cifrado que están siendo usadas por cada cliente en concreto. Esto permitirá ver todo el tráfico de la red descifrado.

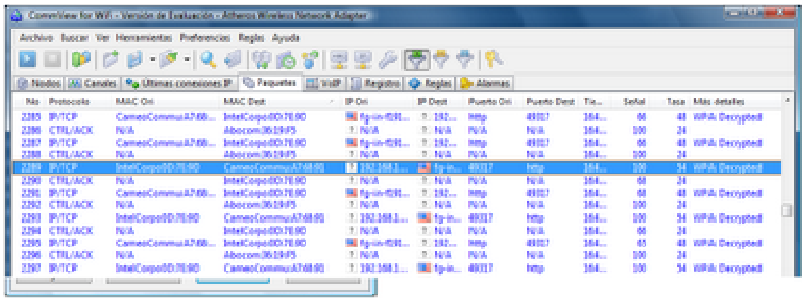

Imagen 15: Paquetes WPA2 capturados y descifrados

Recomponiendo la sesión

Al igual que con otros sniffers de red, es posible reconstruir la sesión TCP completa y ver la comunicación que se está produciendo en cada cliente. En este caso, la página Web que estaba visitando el usuario en El Lado del Mal.

magen 16: Sesión TCP/IP reconstruida

Conclusión

El uso de WPA/WPA2-PSK es una solución adecuada de seguridad en un entorno doméstico siempre y cuando se utilice una clave segura. Como se ha visto a lo largo del artículo la seguridad no depende de la cantidad de tráfico que circule por la red, sino de la posibilidad de obtener la clave de cifrado a partir de los paquetes donde se produce la autenticación del usuario. Basta con una pequeña cantidad de paquetes para poder obtener los paquetes derivados de la clave. Por lo tanto, es necesario utilizar frases o claves fuertes. Para determinar la fortaleza de una clave se puede recurrir a páginas como Passwordmeter, o a cualquiera de los generadores de claves WPA/WPA2 que proporcionan claves fuertes, como, por ejemplo el de http://www.kurtm.net/wpa-pskgen/.

Para evitar que el craqueo de la clave PSK sea trivial para un atacante hay que evitar claves que se encuentren en diccionarios, claves de poca longitud de caracteres y de poca complejidad. Así mismo, para evitar que puedan utilizar tablas pre-calculadas hay que evitar los nombres SSID simples o comunes, del tipo *“Home”*, *“Personal”*, *"Wifi"*, *“Default”*, *“Wireless”*, *“Net”*, etc…

A pesar de todo, el tener una red WPA/WPA2 PSK más o menos segura contra atacantes externos mediante el uso de claves difíciles de crackear, esta infraestructura no ofrece ninguna protección contra atacantes internos. Este artículo deja claro que cualquier usuario legítimo de la red podrá acceder a todos los datos de todos los demás usuarios como se ha visto en la última parte.

Soluciones

Para evitar que las comunicaciones pudieran ser espiadas por parejas, familiares o vecinos existen soluciones WPA/WPA2 empresariales con el uso de servidores RADIUS y sistemas de autenticación EAP basados en certificados digitales, contraseñas e incluso el uso de cifrado SSL para el intercambio EAP [*Protected EAP*]. Así podríamos implantar una infraestructura WPA/WPA2-EAP-MSCHAPv2, WPA/WPA2-EAP-MD5, WPA/WPA2-EAP-TLS (con autenticación del cliente mediante certificados digitales de usuario) y los más fortalecidos WPA/WPA2-PEAP-MSCHAPv2, también conocido como TLS-EAP-TLS por ser este el orden de las capas de los protocolos, dónde primero se autentica realiza una conexión SSL entre el servidor y el cliente con certificado de máquina del servidor o del servidor y el cliente, con lo que se autentica digitalmente la máquina cliente primero, luego se negocia con EAP la autenticación mediante el uso de certificados digitales de usuario y por último el usuario envía su certificado sobre la capa SSL inicial.

Para realizar una implantación segura aquí tienes algunos recursos:

- [PCWorld] Proteger una red wireless I
- [PCWorld] Proteger una red wireless II
- [PCWorld] Proteger una red wireless III
- Webcast Seguridad en Redes Wireless
- Securing Wireless Lans with PEAP and Passwords
- Securing Wireless Lans with Certification Services