DE COMPUCERVERO PARA TODOS LOS BAKUNOS DE BA-K

MANUAL DEL AIR-CRACK-NG

Aireplay-ng

Descripción

Aireplay-ng se usa para inyectar paquetes.

Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves WEP y WPA-PSK. Hay varios ataques diferentes que se pueden utilizar para hacer deautenticaciones con el objetivo de capturar un handshake WPA, para realizar una falsa autenticación, un reenvio interactivo de un paquete, o una reinyección automática de un ARP-request. Con el programa packetforge-ng es posible crear paquetes ARP request de forma arbitraria.

La mayoría de los drivers tienen que estar parcheados para ser capaces de inyectar, no te olvides de leer Installing drivers.

Uso de los ataques

Actualmente se pueden realizar cinco ataques diferentes:

- Ataque 0: Deautenticación
- Ataque 1: Falsa autenticación
- Ataque 2: Selección interactiva del paquete a enviar
- Ataque 3: Reinyección de una petición ARP (ARP-request)
- Ataque 4: Ataque chopchop
- Ataque 5: Ataque de Fragmentación

Uso

Esta sección proporciona un repaso general de todos los ataques. No todas las opciones se aplican a todos los ataques. Mira los detalles de cada ataque para ver todos los parámetros que se pueden usar.

Usa:

```
aireplay-ng <opciones> <interface>
```

Para todos los ataques, excepto el de deautenticación y el de falsa autenticación, puedes usar los siguientes filtros para limitar los paquetes que se usarán. El filtro más común es usar la opción -b para seleccionar un punto de acceso determinado.

Opciones de filtro:

- -b bssid : Dirección MAC del punto de acceso
- -d dmac : Dirección MAC de destino
- -s smac : Dirección MAC origen (source)
- -m len : Longitud mínima del paquete
- -n len : Longitud máxima del paquete
- -u type : frame control, type field
- -v subt : frame control, subtype field
- -t tods : frame control, To DS bit
- -f fromds : frame control, From DS bit
- -w iswep : frame control, WEP bit

Cuando reenviemos (inyectemos) paquetes, podremos utilizar las siguientes opciones. Recuerda que no todas las opciones se usan en cada ataque. La documentación específica de cada ataque tiene ejemplos con las opciones que se pueden usar.

Opciones de inyeción:

- -x nbpps : número de paquetes por segundo
- -p fctrl : fijar palabra frame control (hexadecimal)
- -a bssid : fijar dirección MAC del AP
- -c dmac : fijar dirección MAC de destino
- -h smac : fijar dirección MAC origen
- -e essid : ataque de falsa autenticación: nombre del AP
- -j : ataque arp-replay: inyectar paquetes FromDS
- -g valor : cambiar tamaño de buffer (default: 8)
- -k IP : fijar IP de destino en fragmentos
- -l IP : fijar IP de origen en fragmentos
- -o npckts : número de paquetes por burst (-1)
- -q sec : segundos entre paquetes sigo aquí o keep-alives (-1)
- -y prga : keystream para autenticación compartida (shared key)

Los ataques pueden obtener los paquetes para reenviarlos de dos orígenes distintos. El primero es un paquete capturado en el mismo momento por la tarjeta wireless. El segundo es de un archivo cap. El formato estandard cap o Pcap (Packet CAPture , está relacionado con la libreria libpcap y http://www.tcpdump.org), ess reconozido por la mayoría de los programas comerciales y open-source de captura de tráfico wireless. La capacidad de leer los archivos cap es una característica de aireplay-ng. Esto permite leer paquetes de otra sesión anterior o que se puedan generar archivos pcap para reenviarlos fácilmente.

Opciones de origen:

- -i iface : capturar paquetes con esa interface
- -r archivo : utilizar paquetes de ese archivo cap

Esta es la forma de especificar el modo de ataque que utilizará el programa. Dependiendo del modo, no todas las opciones descritas se pueden aplicar.

Modos de ataque (Los números también se pueden seguir usando como en versiones anteriores):

- - -deauth [número]: deautenticar 1 o todos los clientes (-0)
- - -fakeauth [nº repetición]: falsa autenticación con el AP (-1)
- - -interactive : selección interactiva del paquete a enviar (-2)
- - -arpreplay : estandard reinyección ARP-request (-3)
- - -chopchop : desencriptar paquete WEP/chopchop (-4)

- - -fragment : generar keystream válido (-5)

Ataque de Fragmentación vs. Chopchop

Aquí exponemos las diferencias entre los ataques de fragmentación y chopchop

Fragmentación

Ventajas

- Normalmente se obtiene un paquete entero de una longitud de 1500 bytes xor. Esto significa que podemos crear otro paquete de cualquier tamaño. Incluso en los casos que obtenemos un paquete de menos de 1500 bytes, será suficiente para crear ARP requests .
- Puede funcionar en situaciones en las que chopchop no lo hace.
- Es extremadamente rápido. Se obtiene el xor muy rápido cuando funciona.

Inconvenientes

- Se necesita más información para ejecutarlo, (por ejemplo, información acerca de la dirección IP). Aunque con frecuencia se puede adivinar. Y todavía mejor es que aireplay-ng asume que las IPs de origen y destino son 255.255.255.255 si no se especifica nada. De esta forma funcionará bien en la mayoría de los APs. Por lo tanto esto no es un inconveniente muy grande.
- Este ataque lo podremos ejecutar dependiendo de si los drivers de nuestra tarjeta lo soportan. Por ejemplo, hoy en dia, Atheros no genera el paquete correcto a menos que cambiemos la dirección MAC de nuestra tarjeta wireless a la misma mac que queremos utilizar.
- Se necesita estar físicamente cerca del punto de acceso porque si se pierde algún paquete fallará el ataque.
- El ataque fallará en los puntos de acceso que no manejan los paquetes fragmentados de forma adecuada.

Chopchop

Ventajas

- Puede funcionar en algunos casos en los que no lo hace el ataque de fragmentación.
- No se necesita conocer información acerca de ninguna IP.

Inconvenientes

- No se puede usar contra todos los puntos de acceso.
- El tamaño máximo del xor en bits está limitado por la longitud del paquete contra el que hagas el chopchop. Aunque en teoría se pueden obtener 1500 bytes del xor stream, en la práctica, raramente verás paquetes de 1500 bytes.
- Mucho más lento que el ataque de fragmentación

Problemas de uso

Esto se aplica a todos los modos de aireplay-ng.

Con madwifi-ng, asegúrate de que no hay otras VAPs

Cerciorate de que no has creado varias VAPs. Porque puede haber problemas cuando se crea una nueva VAP en modo monitor y ya hay una VAP en modo managed.

Tienes que parar primero ath0 y reiniciar wifi0:

```
airmon-ng stop ath0
airmon-ng start wifi0
```

o

```
wlanconfig ath0 destroy
wlanconfig ath create wlandev wifi0 wlanmode monitor
```

General

También asegúrate de que:

- El driver de la tarjeta wireless está bien instalado y parcheado.
- La tarjeta wireless está en modo monitor.
- La tarjeta se encuentra en el mismo canal que el punto de acceso.
- Estás físicamente cerca del punto de acceso.
- Asegúrate de que estás usando una dirección MAC real. Mira esta discusión en inglés setting MAC address).
- Algunos puntos de acceso están programados para aceptar solamente conexiones de una dirección MAC específica. En este caso necesitas obtener una dirección MAC de un cliente legítimo utilizando airodump-ng y usar esa MAC. No hagas una falsa autenticación con una dirección MAC de un cliente activo en el AP. El filtrado MAC en un AP no influye para poder realizar ataques de deautenticación.
- El BSSID y ESSID (opciones -a / -e) son correctos.
- Si tu tarjeta es Prism2, asegúrate que tienes el firmware actualizado.
- Cerciorate de que tienes la última versión estable del programa. algunas opciones no están disponibles en versiones anteriores.
- No te olvides de mirar el Trac System para ver si tu problema es un bug conocido.

Descripción

Este ataque envia paquetes de desasociación a uno o más clientes que están actualmente asociados a un punto de acceso. Las razones por las que es útil desasociar clientes pueden ser:

- Recuperar o desvelar un ESSID oculto. Este es un ESSID que no es divulgado o anunciado por el AP.
- Capturar handshakes WPA/WPA2 forzando a los clientes a volverse a autenticar
- Generar peticiones ARP (en Windows, algunas veces, los clientes borran su ARP cache cuando son desconectados)

Por supuesto, este ataque es totalmente inútil si no existen clientes wireless asociados.

Uso

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0
```

Donde:

- -0 significa deautenticación
- 1 es el número de deautenticaciones a enviar (puedes enviar todas las que quieras); 0 significa enviarlas continumente
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -c 00:0F:B5:34:30:30 es la dirección MAC del cliente a deautenticar; si se omite serán deautenticados todos los clientes
- ath0 es el nombre de la interface

Ejemplos de uso

Deautenticación típica

Primero, es necesario averiguar si hay algún cliente actualmente conectado. Necesitaremos su dirección MAC para el siguiente comando:

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0

Donde:

- -0 significa deautenticación
- 1 es el número de deautenticaciones a enviar (puedes enviar todas las que quieras)
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -c 00:0F:B5:34:30:30 es la dirección MAC del cliente que queremos deautenticar
- ath0 es el nombre de la interface

La salida será algo similar a esto:

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

Captura del Handshake WPA/WPA2 con Atheros

```
airmon-ng start ath0
airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w out ath0  (y abrimos otra consola)
aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
(esperamos algunos segundos)
aircrack-ng -w /path/to/dictionary out.cap
```

A continuación explicamos estos comandos:

airodump-ng -c 6 bssid 00:14:6C:7E:40:80 -w out ath0
Donde:

- -c 6 es el número del canal
- bssid 00:14:6C:7E:40:80 limita los paquetes capturados únicamente a este punto de acceso
- -w out es el nombre del archivo donde se guardarán las capturas
- ath0 es el nombre de la interface

aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
Donde:

- -0 significa ataque de deautenticación
- 5 es el número de paquetes de deautenticación a enviar

- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -c 00:0F:B5:AB:CB:9D es la dirección MAC del cliente que queremos deautenticar
- ath0 es el nombre de la interface

A continuación puedes ver la salida del comando aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0

```
 12:55:56  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:56  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:57  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:58  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
 12:55:58  Sending DeAuth to station   -- STMAC: [00:0F:B5:AB:CB:9D]
```

Generar peticiones ARP con una tarjeta Prism2

```
airmon-ng start wlan0
airodump-ng -c 6 -w out --bssid 00:13:10:30:24:9C wlan0  (abrimos otra consola)
aireplay-ng -0 10 -a 00:13:10:30:24:9C wlan0
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:09:5B:EB:C5:2B wlan0
```

Despues de enviar los 10 paquetes de deautenticación, comenzamos a escuchar para pescar algún ARP requests con el ataque 3. La opción -h es obligatoria y tiene que ser la dirección MAC de un cliente asociado.

Si estás usando el driver wlan-ng/, deberías ejecutar el script airmon-ng (a menos que sepas lo que estás haciendo) o sino la tarjeta no funcionará de forma correcta para poder inyectar.

Pistas de uso

Es más efectivo atacar a un cliente determinado usando la opción -c.

Los paquetes de deautenticación son enviados directamente desde el PC a los clientes. Por lo que se debe comprobar que estamos físicamente cerca de los clientes para que les lleguen los paquetes que enviamos desde nuestra tarjeta wireless. (En airodump-ng mirar el PWR de los clientes y no el del AP)

Autenticación falsa

Descripción

El ataque de falsa autenticación permite realizar los dos tipos de autenticación WEP (abierta u Open System y compartida o Shared Key) y asociarse con el punto de acceso (AP). Esto es muy útil cuando necesitamos una dirección MAC asociada para usarla con alguno de los ataques de aireplay-ng y no hay ningún cliente asociado. Se debe tener en cuenta que el ataque de falsa autenticación NO genera ningún paquete ARP.

Uso

aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0

Donde:

- -1 significa falsa autenticación
- 0 tiempo de reasociación en segundos
- -e teddy es el nombre de la red wireless
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:09:5B:EC:EE:F2 es la dirección MAC de nuestra tarjeta
- ath0 es el nombre de la interface wireless

U otra variación útil para algunos puntos de acceso:

```
aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2
ath0
```

Donde:

- 6000 - Reautentifica cada 6000 segundos. El largo periodo también provoca que se envien paquetes de sigo aquí o keep alive .
- -o 1 - Enviar solo un tipo de paquetes de cada vez. Por defecto está fijado en múltiples y esto puede confundir a algunos APs.
- -q 10 - Envia paquetes de sigo aquí cada 10 segundos.

Ejemplos de uso

La falta de asociación con el punto de acceso es la razón más habitual por la cual falla la inyección.

Para asociarse con un punto de acceso, usa la falsa autenticación:

aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0

Donde:

- -1 significa falsa autenticación
- 0 tiempo de reasociación en segundos
- -e teddy es el nombre de la red wireless
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:09:5B:EC:EE:F2 es la dirección MAC de nuestra tarjeta
- ath0 es el nombre de la interface wireless

Si tienes éxito verás algo como esto:

```
18:18:20  Sending Authentication Request
18:18:20  Authentication successful
18:18:20  Sending Association Request
18:18:20  Association successful :-)
```

U otra variación útil para algunos puntos de acceso:

```
aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2
ath0
```

Donde:

- 6000 - Reautentifica cada 6000 segundos. El largo periodo también provoca que se envien paquetes de sigo aquí o keep alive .
- -o 1 - Enviar solo un tipo de paquetes de cada vez. Por defecto está fijado en múltiples y esto confunde a algunos APs.
- -q 10 - Enviar paquetes de sigo aquí cada 10 segundos.

Si tienes éxito verás algo como esto:

```
18:22:32  Sending Authentication Request
18:22:32  Authentication successful
18:22:32  Sending Association Request
18:22:32  Association successful :-)
18:22:42  Sending keep-alive packet
18:22:52  Sending keep-alive packet
# etc...
```

Pistas de uso

Fijar la dirección MAC

Una buena idea es cambiar la dirección MAC de tu tarjeta wirelees por la misma que usas en el parámetro -h en el caso de que sean diferentes. Usando la misma, te aseguras que los ACK s se envian por tu tarjeta. Esto hace que el ataque funcione mejor.

Instrucciones detalladas de como cambiar la dirección MAC de la tarjeta las puedes encontrar en el FAQ: How do I change my card's MAC address ?.

Aviso: Una dirección MAC es algo similar a: 00:09:5B:EC:EE:F2. La primera mitad (00:09:5B) de la dirección MAC se refiere al fabricante. La segunda mitad (EC:EE:F2) es única para cada aparato. Algunos puntos de acceso ignorarán direcciones MAC inválidas. Por lo tanto asegúrate de usar una dirección de un fabricante wireless válido cuando decidas cambiar la MAC. En otro caso los paquetes serán ignorados.

Inyectar en Modo Managed

Con los drivers parcheados madwifi-old CVS 2005-08-14, es posible inyectar paquetes en modo managed (la clave WEP no importa, si el AP acepta la autenticación abierta u Open-System). Entonces, en vez de usar el ataque 1, podemos asociarnos e inyectar / monitorizar a través de la interface athXraw:

```
ifconfig ath0 down hw ether 00:11:22:33:44:55
iwconfig ath0 mode Managed essid 'el ssid' key AAAAAAAAAA
ifconfig ath0 up

sysctl -w dev.ath0.rawdev=1
ifconfig ath0raw up
airodump-ng ath0raw out 6
```

Ahora podemos ejecutar el ataque 3 o 4 (aireplay-ng automáticamente reemplazará ath0 por ath0raw):

```
aireplay-ng -3 -h 00:11:22:33:44:55 -b 00:13:10:30:24:9C ath0

aireplay-ng -4 -h 00:10:20:30:40:50 -f 1 ath0
```

Problemas de uso

Identificando autenticaciones fallidas

A continuación se puede ver un ejemplo de una autenticación fallida:

```
8:28:02  Sending Authentication Request
18:28:02  Authentication successful
18:28:02  Sending Association Request
18:28:02  Association successful :-)
18:28:02  Got a deauthentication packet!
18:28:05  Sending Authentication Request
18:28:05  Authentication successful
18:28:05  Sending Association Request
18:28:10  Sending Authentication Request
18:28:10  Authentication successful
18:28:10  Sending Association Request
```

Presta atención a la frase Got a deauthentication packet y los continuos reintentos. No realices otros ataques hasta que consigas efectuar la falsa autenticación de forma correcta.

Otra forma de identificar que la falsa autenticación falla es ejecutar tcpdump y mirar los paquetes. Inicia otra consola o shell mientras estás inyectando y&

Escribe: tcpdump -n -e -s0 -vvv -i ath0

Aquí puedes ver un mensaje de error de tcpdump como el que estás buscando:

```
11:04:34.360700 314us BSSID:00:14:6c:7e:40:80 DA:00:0f:b5:46:11:19 SA:00:14:6c:7e:
40:80 DeAuthentication: Class 3 frame received from nonassociated station
```

Date cuenta de que el punto de acceso (00:14:6c:7e:40:80) le está diciendo al cliente origen (00:0f:b5:46:11:19) que no está asociado. Lo que significa, que el AP no aceptará los paquetes inyectados.

Si quieres seleccionar solo los paquetes de DeAutenticación con tcpdump, puedes usar: tcpdump -n -e -s0 -vvv -i ath0 | grep DeAuth . Necesitas utilizar la palabra DeAuth para encontrar exactamente los paquetes que buscas.

Mira las siguientes secciones para posibles soluciones.

Reasociación

Algunas veces nos desasociamos del AP de forma periódica. Algunos puntos de acceso requieren que nos reasociaciemos cada 30 segundos, o sino considera que el falso cliente se ha desconectado. En este caso, es necesario fijar el periodo de re-asociación:

```
aireplay-ng -1 30 -e 'el ssid' -a 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
```

Otros problemas y soluciones

Si la falsa autenticación nunca tiene éxito (aireplay-ng se queda enviando intentos de autenticación) puede que esté activo el filtrado MAC. En este caso el punto de acceso solo aceptará conexiones de una/s dirección/es MAC concretas. La única solución es averiguar una dirección MAC válida utilizando la observación con airodump-ng. No hagas una autenticación falsa para una dirección MAC

si ese cliente se encuentra activo en el AP.

También asegúrate de que:

- Estás físicamente cerca del punto de acceso.
- Asegúrate que usas una dirección MAC de un fabricante real
- El driver de la tarjeta wireless está correctamente instalado y parcheado.
- La tarjeta está configurada en el mismo canal que el AP.
- El BSSID y el ESSID (opciones -a / -e) son correctos.
- Si es una Prism2, cerciórate de que has actualizado el firmware.

Descripción

Este ataque nos permite escoger el paquete a reenviar (inyectar). Este ataque puede obtener paquetes para inyectar de 2 formas. La primera es capturando paquetes con la tarjeta wireless. La segunda es utilizando un archivo cap. El formato estandard cap o Pcap (Packet CAPture, está asociado con la librería libpcap http://www.tcpdump.org), es reconocido por la mayoría de los programas de captura y análisis de tráfico. Esto permite leer paquetes capturados en sesiones anteriores, o que han sido obtenidos con otros ataques. Un uso común puede ser leer un archivo creado con packetforge.

Uso

aireplay-ng -2 <opciones de filtro> <opciones de reenvio> -r <nombre de archivo> <interface>

Donde:

- -2 significa ataque de reenvio interactivo
- <opciones de filtro> se describen aquí
- <opciones de reenvio> se describen aquí
- -r <nombre de archivo> se usa para especificar un archivo cap del que leer los paquetes para inyectarlos (es opcional)
- <interface> es la interface wireless, por ejemplo ath0

Ejemplos de uso

Podrías usarlo, por ejemplo, para radiodifundir (broadcast) los paquetes del AP y generar nuevos vectores de inicialización (IVs):

```
 aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:14:6C:7E:40:80 -h
00:0F:B5:88:AC:82  ath0
```

Donde:

- -2 significa ataque de inyección interactivo
- -p 0841 fija el Frame Control en el paquete para que parezca que está siendo enviado desde un cliente wireless.
- -c FF:FF:FF:FF:FF:FF fija como dirección MAC de destino cualquiera (broadcast). Esto es

necesario para que el AP responda con otro paquete y así generar un nuevo IV.

- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso (BSSID). Este es un filtro para seleccionar un único AP.
- -h 00:0F:B5:88:AC:82 es la dirección MAC de los paquetes que se están transmitiendo, que debe coincidir con la MAC de tu tarjeta wireless.
- ath0 es el nombre de la interface wireless.

Los IVs generados por segundo variarán dependiendo del tamaño del paquete que seleccionemos. Cuanto más pequeño sea el tamaño del paquete, mayor será la velocidad por segundo. Cuando lanzemos el programa, veremos algo como esto:

```
Read 99 packets...

     Size: 139, FromDS: 1, ToDS: 0 (WEP)

          BSSID  =  00:14:6C:7E:40:80
      Dest. MAC  =  01:00:5E:00:00:FB
     Source MAC  =  00:40:F4:77:E5:C9

     0x0000:  0842 0000 0100 5e00 00fb 0014 6c7e 4080  .B....^.....l~@.
     0x0010:  0040 f477 e5c9 5065 917f 0000 e053 b683  .@.w..Pe.ɑ...S..
     0x0020:  fff3 795e 19a3 3313 b62c c9f3 c373 ef3e  ..y^..3.,...s.>
     0x0030:  87a0 751a 7d20 9e6c 59af 4d53 16d8 773c  ..u.} .lY.MS..w<
     0x0040:  af05 1021 8069 bbc8 06ea 59f3 3912 09a9  ...!.i....Y.9...
     0x0050:  c36d 1db5 a51e c627 11d1 d18c 2473 fae9  .m.....'....$s..
     0x0060:  84c0 7afa 8b84 ebbb e4d2 4763 44ae 69ea  ..z.......GcD.i.
     0x0070:  b65b df63 8893 279b 6ecf 1af8 c889 57f3  .[.c..'.n.....W.
     0x0080:  fea7 d663 21a6 3329 28c8 8f              ...c!.3)(..

Use this packet ?
```

Respondiendo y los paquetes serán inyectados:

```
Saving chosen packet in replay_src-0303-103920.cap
You should also start airodump-ng to capture replies.

Sent 4772 packets...
```

Utilizando el filtro para indicar el tamaño del paquete, podemos usar manualmente el ataque 2 para reenviar peticiones ARP con encriptación WEP. Las peticiones ARP o ARP requests tienen un tamaño típico de 68 (si son de un cliente wireless) o 86 (si son de un cliente cableado) bytes:

aireplay-ng -2 -p 0841 -m 68 -n 86 -b 00:14:6C:7E:40:80 -c FF:FF:FF:FF:FF:FF -h 00:0F:B5:88:AC:82 ath0

Donde:

- -2 significa ataque de inyección interactivo
- -p 0841 fija el Frame Control para que parezca que el paquete se está enviando desde un cliente wireless.
- -m 68 es la longitud mínima del paquete
- -n 86 es la longitud máxima del paquete
- -c FF:FF:FF:FF:FF:FF fija la dirección MAC de destino como cualquiera (broadcast). Esto se requiere para que el AP conteste al paquete y así generar el nuevo IV.
- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso (BSSID). Este es un filtro para seleccionar un AP.

- -h 00:0F:B5:88:AC:82 es la dirección MAC de los paquetes que se están transmitiendo, que debe coincidir con la MAC de tu tarjeta wireless.
- ath0 es el nombre de la interface wireless.

Una vez que inicias el comando verás algo como:

```
Read 145 packets...

      Size: 86, FromDS: 1, ToDS: 0 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  FF:FF:FF:FF:FF:FF
      Source MAC  =  00:40:F4:77:E5:C9

      0x0000:  0842 0000 ffff ffff ffff 0014 6c7e 4080  .B..........l~@.
      0x0010:  0040 f477 e5c9 9075 a09c 0000 d697 eb34  .@.w...u.......4
      0x0020:  e880 9a37 8bda d0e7 fdb4 252d d235 313c  ...7......%-.51<
      0x0030:  16ab 784c 5a45 b147 fba2 fe90 ae26 4c9d  ..xLZE.G.....&L.
      0x0040:  7d77 8b2f 1c70 1d6b 58f7 b3ac 9e7f 7e43  }w./.p.kX....~C
      0x0050:  78ed eeb3 6cc4                           x...l.

Use this packet ? y
```

Contesta y si el paquete es de 68 o 86 bytes, en otro caso escribe n . Ahora empezará a inyectar paquetes:

```
Saving chosen packet in replay_src-0303-124624.cap
You should also start airodump-ng to capture replies.
```

Como decíamos antes, aireplay-ng se puede usar para reenviar paquetes guardados en un archivo cap. Date cuenta que puedes leer en el ejemplo: Saving chosen packet in replay_src-0303-124624.cap . También se puede usar cualquier otro archivo cap creado no solo con aireplay-ng, sino también con airodump-ng, kismet, etc.

A continuación puedes ver un ejemplo usando el archivo cap anterior:

aireplay-ng -2 -p 0841 -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 -r replay_src-0303-124624.cap ath0

Donde:

- -2 significa ataque de inyección interactivo
- -p 0841 fija el Frame Control para que parezca que el paquete se está enviando desde un cliente wireless.
- -c FF:FF:FF:FF:FF:FF NOTE: Este parámetro no lo incluimos porque un paquete ARP ya tiene como destino cualquier dirección MAC (broadcast).
- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso (BSSID). Este es un filtro para seleccionar un AP.
- -h 00:0F:B5:88:AC:82 es la dirección MAC de los paquetes que se están transmitiendo, que debe coincidir con la MAC de tu tarjeta wireless.
- ath0 es el nombre de la interface wireless.

El programa responde:

```
      Size: 86, FromDS: 1, ToDS: 0 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  FF:FF:FF:FF:FF:FF
```

```
      Source MAC  =  00:40:F4:77:E5:C9

      0x0000:  0842 0000 ffff ffff ffff 0014 6c7e 4080  .B..........l~@.
      0x0010:  0040 f477 e5c9 9075 a09c 0000 d697 eb34  .@.w...u.......4
      0x0020:  e880 9a37 8bda d0e7 fdb4 252d d235 313c  ...7......%-.51<
      0x0030:  16ab 784c 5a45 b147 fba2 fe90 ae26 4c9d  ..xLZE.G.....&L.
      0x0040:  7d77 8b2f 1c70 1d6b 58f7 b3ac 9e7f 7e43  }w./.p.kX....~C
      0x0050:  78ed eeb3 6cc4                           x...l.

Use this packet ? y
```

Respondemos y para seleccionar ese paquete. Y seguidamente comenzará a inyectar los paquetes:

```
Saving chosen packet in replay_src-0303-124624.cap
You should also start airodump-ng to capture replies.
```

Pistas de uso

Hay algunas aplicaciones interesantes del primer ejemplo anterior. Se puede usar para atacar redes sin clientes wireless conectados. Inicia el ataque de aireplay-ng. Ahora siéntate y espera por algún paquete que vaya destinado a cualquier cliente (broadcast). No importa de que tipo sea. Responde y y se empezarán a generar IVs. El mayor problema puede ser la velocidad, ten en cuenta que los paquetes grandes producen menos IVs por segundo. La mayor ventaja es poder utilizarlo una vez que hemos obtenido el xor (con chopchop o el ataque de fragmentación), construyendo un paquete y enviándolo con este ataque.

Esto también funcionará en APs con clientes. Es mucho más rápido ya que no es necesario esperar por un ARP, cualquier paquete nos servirá.

Problemas de uso

El problema más común es que no estés asociado con el AP. Incluso si usas una dirección MAC de un cliente ya asociado con el AP o si usas la falsa autenticación.

Revisa el tutorial Estoy inyectando pero los ivs no aumentan.

También mira las ideas y problemas generales de aireplay-ng: Problemas de uso de aireplay-ng

Ataque de reenvio de "ARP Request"

Descripción

El clásico ataque de reenvio de petición ARP o ARP request es el modo más efectivo para generar nuevos IVs (vectores de inicialización), y funciona de forma muy eficaz. El programa escucha hasta encontrar un paquete ARP y cuando lo encuentra lo retransmite hacia el punto de acceso. Esto provoca que el punto de acceso tenga que repetir el paquete ARP con un IV nuevo. El programa retransmite el mismo paquete ARP una y otra vez. Pero, cada paquete ARP repetido por el AP tiene un IV nuevo. Todos estos nuevos IVs nos permitirán averiguar la clave WEP.

ARP es un protocolo de resolución de direcciones: Es un protocolo TCP/IP usado para convertir una

dirección IP en un dirección física, como por ejemplo una dirección Ethernet. Un cliente que desea obtener una dirección envia a todo el que le escuche (broadcasts) una petición ARP (ARP request) dentro de la red TCP/IP. El cliente de la red que tenga esa dirección que se pide contestará diciendo cual es su dirección física.

Uso

Uso básico:

```
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
```

Donde:

- -3 significa reenvio estandard de petición arp (arp request)
- -b 00:13:10:30:24:9C es la dirección MAC del punto de acceso
- -h 00:11:22:33:44:55 es la dirección MAC origen (de un cliente asociado o de una falsa autenticación)
- ath0 es el nombre de la interface wireless

Reenviar una petición arp previa. Este es un caso especial del ataque de reenvio interactivo de paquetes. Lo presentamos aquí porque es unn complemento al ataque de reenvio de ARP request .

```
aireplay-ng -2 -r replay_arp-0219-115508.cap ath0
```

Donde:

- -2 significa selección interactiva del paquete
- -r replay_arp-0219-115508.cap es el nombre del archivo con el ARP
- ath0 es el nombre de la interface wireless

Ejemplos de uso

Para todos estos ejemplos, es necesario primero poner la tarjeta en modo monitor con airmon-ng. No se pueden inyectar paquetes si no estamos en modo monitor.

Para este ataque, necesitas o bien la dirección MAC de un cliente asociado, o una MAC falsa asociada con el ataque 1. La forma más fácil y más rápida es utilizar la dirección MAC de un cliente asociado. Esta se puede obtener con airodump-ng. La razón para usar una dirección MAC asociada es que el punto de acceso solo aceptará y contestará a los paquetes en los cuales la MAC que se los envia esté asociada .

Puede que tengas que esperar un par de minutos, o incluso más, hasta que aparezca una petición ARP; este ataque fallará si no hay tráfico.

Introduce este comando:

```
aireplay-ng -3 -b 00:14:6c:7e:40:80 -h 00:0F:B5:88:AC:82 ath0
```

El sistema responderá:

```
Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies.
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Inicialmente la última linea será similar a:

```
Read 39 packets (got 0 ARP requests), sent 0 packets...
```

Más tarde, cuando el ataque progrese, no aparecerán ceros y veremos la cuenta actual como en el ejemplo de arriba. Puedes ejecutar airodump-ng para capturar los IVs cundo se empiecen a generar. Verás aumentar la columna de data rápidamente para ese punto de acceso.

El segundo ejemplo lo haremos reutilizando la petición ARP del ejemplo anterior usando la opción -r. Date cuenta que te dicen Saving ARP requests in replay_arp-0219-123051.cap , es decir se están gravando las peticiones ARP en el archivo replay_arp-0219-123051.cap. Por lo tanto no es necesario esperar por un nuevo ARP, podemos simplemente reusar uno viejo con el parámetro -r :

```
aireplay-ng -2  -r replay_arp-0219-123051.cap ath0
```

El sistema responderá:

```
      Size: 86, FromDS: 0, ToDS: 1 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  FF:FF:FF:FF:FF:FF
      Source MAC  =  00:0F:B5:88:AC:82

      0x0000:  0841 0000 0014 6c7e 4080 000f b588 ac82  .A....l~@.......
      0x0010:  ffff ffff ffff 7092 e627 0000 7238 937c  ......p..'..r8.|
      0x0020:  8011 36c6 2b2c a79b 08f8 0c7e f436 14f7  ..6.+,.....~.6..
      0x0030:  8078 a08e 207c 17c6 43e3 fe8f 1a46 4981  .x.. |..C....FI.
      0x0040:  947c 1930 742a c85f 2699 dabe 1368 df39  .|.0t*._&....h.9
      0x0050:  ca97 0d9e 4731                           ....G1

Use this packet ? y
```

Escribe y y comenzará la inyección:

```
Saving chosen packet in replay_src-0219-123117.cap
You should also start airodump-ng to capture replies.

Sent 3181 packets...
```

Ahora, si aun no lo has hecho, inicia airodump-ng para capturar los IVs que se están generando. El número de paquetes de datos debería de empezar a aumentar rápidamente.

Pistas de uso

Como estás probando en tu casa a generar un paquete ARP para comenzar la inyección, puedes hacer un ping en tu red a una IP que ni siquiera tiene que existir en la misma.

KoreK chopchop

Este ataque, cuando es exitoso, puede desencriptar un paquete de datos WEP sin necesidad de conocer la clave. Incluso puede funcionar con WEP dinámica. *Este ataque no recupera la clave WEP en sí misma, sino que revela únicamente el texto plano.* De cualquier modo, algunos puntos de acceso no son en absoluto vulnerables. Algunos pueden en principio parecer vulnerables pero en realidad tiran los paquetes menores de 60 bytes. Si el punto de acceso tira paquetes menores de 42 bytes, aireplay intenta

adivinar el resto de los datos, tan pronto como el encabezado (headers) sea predecible. Si un paquete IP es capturado, automáticamente comprueba el checksum del encabezado para ver si es correcto, y despues trata de adivinar las partes que le faltan. Este ataque requiere como mínimo un paquete de datos WEP.

1. Primero, desencriptamos un paquete

```
aireplay-ng -4 ath0
```

Esto puede que no funcione, ya que en muchos casos los puntos de acceso no aceptan los paquetes de datos porque no saben que MAC se los está enviando. En este caso tenemos que usar la dirección MAC de un cliente conectado que si va a tener permiso para enviar paquetes de datos dentro de la red:

```
aireplay-ng -4 -h 00:09:5B:EB:C5:2B ath0
```

2. Vamos a echar un vistazo a la dirección IP

```
tcpdump -s 0 -n -e -r replay_dec-0627-022301.cap
reading from file replay_dec-0627-022301.cap, link-type [...]
IP 192.168.1.2 > 192.168.1.255: icmp 64: echo request seq 1
```

3. Ahora, forjemos una petición (ARP request) La IP de origen no importa (192.168.1.100) pero la Ip de destino (192.168.1.2) debe responder a las peticiones ARP (ARP requests). La dirección MAC de origen tiene que ser la de un cliente asociado, en caso de que exista filtrado MAC.

```
packetforge-ng replay_dec-0627-022301.xor 1 00:13:10:30:24:9C 00:09:5B:EB:C5:2B
192.168.1.100 192.168.1.2 arp.cap
```

4. Y reenviamos nuestra petición ARP forjada

```
aireplay-ng -2 -r arp.cap ath0
```

Ataque de fragmentación

Descripción

Con este ataque, cuando tiene éxito, podemos obtener 1500 bits de un PRGA (pseudo random generation algorithm). Este ataque no recupera la clave WEP por si mismo, simplemente sirve para conseguir el PRGA. Despues podemos usar el PRGA para generar paquetes con packetforge-ng. Se requiere al menos un paquete de datos recibido del punto de acceso para poder iniciar el ataque.

Básicamente, el programa obtiene una pequeña cantidad de información sobre la clave de un paquete e intenta enviar un ARP y/o paquetes LLC al punto de acceso (AP). Si el paquete es recibido y contestado por el AP de forma satisfactoria, entoces se podrá obtener un poco más de información sobre la clave de ese nuevo paquete enviado por el AP. Este ciclo se repite varias veces hasta que obtenemos los 1500 bits del PRGA o algunas veces se obtienen menos de 1500 bits.

La información original de Andrea Bittau la puedes encontrar en technique_papers que proporciona mucha más información técnica y más detallada. Aquí puedes ver diapositivas de este ataque.

Uso

aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Donde:

- -5 significa ataque de fragmentación
- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:0F:B5:AB:CB:9D es la dirección MAC origen de los paquetes que serán inyectados
- ath0 es el nombre de la interface

Opcionalmente, se pueden aplicar los siguientes filtros:

- -b bssid : dirección MAC del punto de acceso
- -d dmac : dirección MACde destino
- -s smac : dirección MAC origen
- -m len : longitud mínima del paquete
- -n len : longitud máxima del paquete
- -u type : frame control, tipo de campo
- -v subt : frame control, subtipo de campo
- -t tods : frame control, A DS bit
- -f fromds : frame control, Desde DS bit
- -w iswep : frame control, WEP bit

Opcionalmente, se pueden utilizar las siguientes opciones:

- -k IP : fijar IP de destino - por defecto 255.255.255.255
- -l IP : fijar IP de origen - por defecto 255.255.255.255

Ejemplos de uso

Notas:

- La dirección MAC origen usada en el ataque debe ser la asociada con el punto de acceso. Para ello, se puede realizar una falsa autenticación o usar una dirección MAC de un cliente wireless ya conectado.
- Para los drivers madwifi-ng (chipset Atheros), es necesario cambiar la dirección MAC de la tarjeta por la dirección MAC que se usará para la inyección, sino el ataque no funcionará.

Esencialmente se inicia el ataque con el siguiente comando y seleccionamos el paquete con el que queremos probar:

```
aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0

Waiting for a data packet...
Read 96 packets...

      Size: 120, FromDS: 1, ToDS: 0 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  00:0F:B5:AB:CB:9D
      Source MAC  =  00:D0:CF:03:34:8C

      0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B.........l~@.
      0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
      0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
```

```
      0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
      0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
      0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
      0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q.D...w.....<R.
      0x0070:  0505 933f af2f 740e                      ...?./t.

Use this packet ? y
```

El programa responde esto (o similar):

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

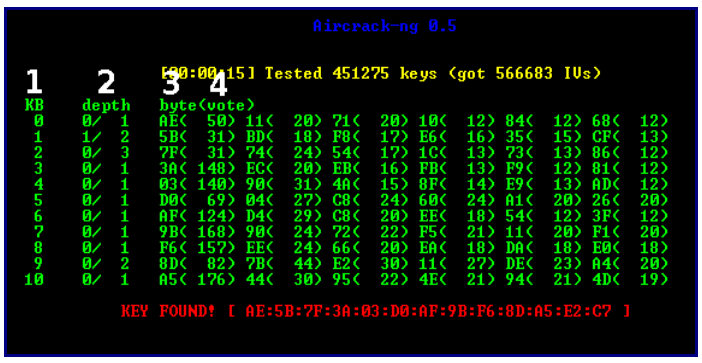
Has obtenido satisfactoriamente el PRGA que está guardado en el archivo nombrado por el programa (fragment-0124-161129.xor). Ahora puedes usar packetforge-ng para generar uno o más paquetes y usarlos con alguno de los ataques de inyección.

Aircrack-ng

Descripción

Aircrack-ng es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con airodump-ng. Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario.

Captura de pantalla



LEYENDA
1 = Keybyte, es decir el número de cada uno de los bytes o caracteres de la clave.
2 = Profundidad de la actual búsqueda de la clave
3 = Byte o caracter que se está probando
4 = Votos o número de probabilidades de que sea correcto ese byte

¿Cómo funciona?

En esta página: Techniques Papers encontrarás muchos links a otras webs que tienen algunos manuales que describen estas técnicas de forma más detallada y como funcionan las matemáticas que hay detrás de ellas.

Múltiples técnicas se combinan para crackear la clave WEP:

- Ataques FMS (Fluhrer, Mantin, Shamir) - son técnicas estadísticas
- Ataques Korek - tambien técnicas estadísticas
- Fuerza bruta

Cuando se usan técnicas estadísticas para crackear claves WEP, cada byte de la clave es tratado de forma individual. Usando matemáticas estadísticas, la posibilidad de que encuentres un byte determinado de la clave crece algo más de un 15% cuando se captura el vector de inicialización (IV) correcto para ese byte de la clave. Esencialmente, ciertos IVs revelan algún byte de la clave WEP. Esto es básicamente en que consisten las técnicas estadísticas.

Usando una serie de pruebas estadísticas llamadas FMS y ataques Korek, se van acumulando posibilidades o votos (votes) para cada byte de la clave WEP. Cada ataque tiene un número diferente de votos asociado con él, por lo que la probabilidad de cada ataque varia matemáticamente. Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto. Para cada byte de la clave, la pantalla nos muestra el caracter más probable y el número de votos que ha acumulado. Sobra decir, que la clave que tenga el mayor número de votos es la que más probabilidades tiene de ser la correcta, pero no está garantizado. Aircrack-ng probará continuamente de la más probable a la menos probable para encontrar la clave.

Usando un ejemplo entenderemos esto de forma más clara. En la anterior captura de pantalla, puedes ver, que para el primer caracter o byte 0, 0xAE ha obtenido unos cuantos votos, 50 exactamente. Entonces, matemáticamente, es más probable que la clave comience por AE que por 11 (el segundo valor en la misma linea) que es el siguiente con más posibilidades. Esta es la razón por la cual cuantos más paquetes tengas, más fácil será para aircrack-ng determinar la clave WEP.

La aproximación estadística puede por si sola darnos la clave WEP de la red. Pero la idea es que tambien podemos complementarlo con la fuerza bruta para realizar el trabajo. Aircrack-ng usa la fuerza bruta para determinar cuantas claves se han de probar para intentar encontrar la clave WEP.

Aquí es donde entra en juego el fudge factor . Basicamente el fudge factor le dice a aircrack-ng hasta donde probar claves. Es como si quisiesemos encontrar un balón diciéndole a alguien que el balón se puede encontrar entre 0 y 10 metros alrededor. Pero si le decimos que el balón se encuentra entre 0 y 100 metros alrededor. En este escenario de 100 metros le llevará mucho más tiempo realizar la búsqueda pero tendrá más posibilidades de encontrarlo.

Por ejemplo, si le decimos a aircrack-ng que use un fudge factor de 2, dividirá los votos del byte más probable, y probará todas las posibilidades con un número de votos de al menos la mitad de los que tiene el caracter más posible. Cuanto mayor sea el fudge factor, más posibilidades probará aircrack-ng aplicando fuerza bruta. Recuerda, que cuanto mayor sea el fudge factor, el número de claves a probar

crecerá tremendamente y mayor será el tiempo que se esté ejecutando aircrack-ng. En cambio, cuantos más paquetes de datos tengas, minimizarás la necesidad de aplicar fuerza bruta a muchas claves, lo que hace que no trabaje tanto tiempo la CPU y se reduce mucho el tiempo necesario para encontrar la clave.

Al final, es todo muy simple matemáticas y fuerza bruta!

Las técnicas mencionadas hasta ahora no funcionan para claves WPA/WPA2 pre-shared. La única forma de crackear estas claves pre-compartidas (pre-shared) es a través de un ataque de diccionario. Esta capacidad está tambien incluida en aircrack-ng.

Con claves pre-compartidas, el cliente y el punto de acceso establecen las claves que se van a usar en sus comunicaciones al comienzo cuando el cliente se asocia por primera vez con el punto de acceso. Hay cuatro paquetes handshake entre el cliente y el punto de accesoairodump-ng puede capturar estos cuatro paquetes handshake. Y usando un diccionario con una lista de palabras, aircrack-ng duplica los cuatro paquetes handshake para mirar si hay alguna palabra en el diccionario que coincida con el resultado de los cuatro paquetes handshake. Si lo consigues, habrás identificado de forma satisfactoria la clave pre-compartida.

Hay que resaltar que este programa hace un uso muy intensivo del procesador del ordenador, y que en la práctica claves WPA pre-compartidas muy largas o inusuales no podrán ser encontradas . Un buen diccionario te dará mejores resultados. Otra posibilidad es usar un pograma como john the ripper para generar contraseñas que podrán ser utilizadas por aircrack-ng.

Explicación de la profundidad (depth) y del Fudge Factor

La mejor explicación es un ejemplo. Nos fijaremos en un byte en concreto. Todos los bytes son tratados de la misma manera.

Tu tienes los votos (votes) como en la captura de pantalla anterior. Para el primer byte ves lo siguiente: AE(50) 11(20) 71(20) 10(12) 84(12)

Los AE, 11, 71, 10 y 84 son los valores posibles de la clave para el primer caracter (byte 0). Los números que están entre paréntesis son los votos que cada posible valor ha acumulado hasta ahora.

Ahora si decides usar un fudge factor de 3. Aircrack-ng realizará la siguiente operación a partir del byte que tiene más probabilidades o votos: AE(50):

50 / 3 = 16.666666

Aircrack-ng probará (fuerza bruta) todas las claves posibles que tengan un número de votos superior a 16.6666, resultando que

AE, 11, 71

serán utilizados, por lo que tenemos un número total de 3 valores a probar para ese byte o caracter (depth):

0 / 3 AE(50) 11(20) 71(20) 10(12) 84(12)

Cuando aircrack-ng está probando claves con AE, muestra 0 / 3, cuando acabe de probar todas las claves con ese byte, pasará al siguiente con más votos (11 en este ejemplo) y mostrará:

1 / 3 11(20) 71(20) 10(12) 84(12)

Uso

```
aircrack-ng [opciones] <archivo(s) de captura>
```

Puedes especificar múltiples archivos de captura (incluso mezclando formatos .cap y .ivs). También se puede ejecutar airodump-ng y aircrack-ng al mismo tiempo: aircrack-ng se actualizará de forma automática cuando estén disponibles nuevos IVs.

Aquí está la explicación para todas y cada una de las opciones disponibles:

Option	Param.	Description
-a	amode	Fuerza el tipo de ataque (1 = WEP estática, 2 = WPA/WPA2-PSK).
-e	essid	Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID. Está opción es necesaria para crackear claves WPA/WPA2-PSK si el ESSID está oculto.
-b	bssid	Selecciona el AP objetivo basándose en la dirección MAC.
-p	nbcpu	En sistemas SMP, especifica con esta opción el número de CPUs usadas.
-q	*none*	Activa el modo silencioso (no muestra ninguna salida hasta que encuentra o no la clave).
-c	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres alfanuméricos (0×20 - 0x7F).
-t	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres hexadecimales codificados en binario.
-h	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres numéricos (0×30-0×39). Estas claves numéricas son utilizadas por defecto por muchos APs y muchas compañias de ADSL.
-d	start	(WEP cracking) Especifica el comienzo de la clave WEP (en hexadecimal).
-m	maddr	(WEP cracking) Dirección MAC para la que filtrar los paquetes de datos WEP. Alternativamente, se puede especificar -m ff:ff:ff:ff:ff:ff para usar todos y cada uno de los IVs, sin preocuparnos de la red.
-n	nbits	(WEP cracking) Especifica la longitud de la clave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. La opción por defecto es 128.
-i	index	(WEP cracking) Guarda solo los IVs que tienen este índice de clave (1 to 4). La opción predeterminada es ignorar el índice de clave.
-f	fudge	(WEP cracking) Por defecto, esta opción está fijada en 2 para WEP de 104-bit y en 5 para WEP de 40-bit. Especifica un valor más alto para para elevar el nivel de fuerza bruta: la obtención de la clave llevará más tiempo, pero la probabilidad de éxito será mayor.
-k	korek	(WEP cracking) Hay 17 ataques korek de tipo estadístico. Algunas veces un ataque crea un falso positivo que evita que encontremos la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, & -k 17 para ir desactivando cada uno de los ataques.
-x/-x0	*none*	(WEP cracking) No aplicar fuerza bruta sobre los dos últimos bytes de la clave (keybytes).
-x1	*none*	(WEP cracking) Aplicar fuerza bruta sobre el último byte de la clave (opción por

		defecto).
-x2	*none*	(WEP cracking) Aplicar fuerza bruta sobre los dos últimos bytes.
-X	*none*	(WEP cracking) No aplicar fuerza bruta con multiprocesadores (solo sistemas SMP).
-y	*none*	(WEP cracking) Éste es un ataque de fuerza bruta experimental, que solo debe ser usado cuando el ataque estandard falle con más de un millón de IVs
-w	words	(WPA cracking) Ruta al diccionario.

Ejemplos de uso

El caso más simple es crackear una clave WEP. Si quieres probar esto por ti mismo, aquí tienes un archivo de prueba. La clave de este archivo de prueba coincide con la de la pantalla anterior de este tutorial, pero no coincide con la del siguiente ejemplo.

aircrack-ng 128bit.ivs
Donde:

- 128bit.ivs es el nombre del archivo que contiene los ivs.

El programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

Si hay múltiplies redes en el archivo, entonces tendrás la opción de seleccionar la que quieras. Por defecto, aircrack-ng supone que la encriptación es de 128 bit.

El proceso de crackeo comienza, y una vez obtenida la clave, verás algo como esto:

```
                                      Aircrack-ng 0.7 r130


                          [00:00:10] Tested 77 keys (got 684002 IVs)

 KB    depth   byte(vote)
  0    0/  1   AE( 199) 29(  27) 2D(  13) 7C(  12) FE(  12) FF(   6) 39(   5) 2C(
3) 00(   0) 08(   0)
  1    0/  3   66(  41) F1(  33) 4C(  23) 00(  19) 9F(  19) C7(  18) 64(   9) 7A(
9) 7B(   9) F6(   9)
  2    0/  2   5C(  89) 52(  60) E3(  22) 10(  20) F3(  18) 8B(  15) 8E(  15)
14(  13) D2(  11) 47(  10)
  3    0/  1   FD( 375) 81(  40) 1D(  26) 99(  26) D2(  23) 33(  20) 2C(  19)
05(  17) 0B(  17) 35(  17)
  4    0/  2   24( 130) 87( 110) 7B(  32) 4F(  25) D7(  20) F4(  18) 17(  15)
8A(  15) CE(  15) E1(  15)
  5    0/  1   E3( 222) 4F(  46) 40(  45) 7F(  28) DB(  27) E0(  27) 5B(  25)
71(  25) 8A(  25) 65(  23)
  6    0/  1   92( 208) 63(  58) 54(  51) 64(  35) 51(  26) 53(  25) 75(  20)
0E(  18) 7D(  18) D9(  18)
  7    0/  1   A9( 220) B8(  51) 4B(  41) 1B(  39) 3B(  23) 9B(  23) FA(  23)
63(  22) 2D(  19) 1A(  17)
  8    0/  1   14(1106) C1( 118) 04(  41) 13(  30) 43(  28) 99(  25) 79(  20)
```

```
B1(  17) 86(  15) 97(  15)
  9    0/  1   39( 540) 08(  95) E4(  87) E2(  79) E5(  59) 0A(  44) CC(  35)
02(  32) C7(  31) 6C(  30)
 10    0/  1   D4( 372) 9E(  68) A0(  64) 9F(  55) DB(  51) 38(  40) 9D(  40)
52(  39) A1(  38) 54(  36)
 11    0/  1   27( 334) BC(  58) F1(  44) BE(  42) 79(  39) 3B(  37) E1(  34)
E2(  34) 31(  33) BF(  33)

           KEY FOUND! [ AE:66:5C:FD:24:E3:92:A9:14:39:D4:27:4B ]
```

Esta clave puede ser usada para conectarse a la red.

Ahora para crackear claves WPA/WPA2:

aircrack-ng -w password.lst *.cap
Donde:

- -w password.lst es el nombre del diccionario con la lista de palabras. Recuerda que tienes que especificar la ruta completa si el archivo no se encuentra en el directorio actual.
- *.cap es el nombre de los archivos que contienen los ivs. Date cuenta que en este caso usamos el comodín * para incluir múltiples archivos.

El programa responde:

```
 Opening wpa2.eapol.cap
 Opening wpa.cap
 Read 18 packets.

 #  BSSID              ESSID                     Encryption

 1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
 2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

 Index number of target network ?
```

Date cuenta que en este caso como hay dos redes necesitamos seleccionar la que queremos atacar. Escogeremos la número 2. El programa entonces responde:

```
                              Aircrack-ng 0.7 r130


                    [00:00:03] 230 keys tested (73.41 k/s)


                           KEY FOUND! [ biscotte ]


    Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                     39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

    Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                     73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                     AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                     D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

    EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Ahora que sabemos la palabra, podremos conectarnos a la red.

Técnicas de uso

Aproximación general para crackear claves WEP

La forma más simple es escribir aircrack-ng archivo.cap . Tenemos que decir que hay algunas técnicas para aumentar las posibilidades de encontrar la clave WEP rápidamente. Pero no existe la magia. A continuación se describen algunos métodos para obtener la clave más rápido.

La mejor de todas las técnicas es capturar tantos paquetes como sea posible; cuantos más mejor. Esto es lo más sencillo y lo más importante. El número de vectores de inicialización (IVs) que se necesitan para obtener una clave WEP varia dependiendo de la longitud de la clave y del punto de acceso de que se trate. Habitualmente se necesitan 250,000 o más IVs para claves de 64 bit y 1.5 millones o más para claves de 128 bit. Y por supuesto que muchos más para claves más largas. Pero si tenemos suerte, hay veces que la clave WEP se puede obtener con 50,000 IVs o menos. Aunque esto no ocurre con frecuencia. Y al revés, habrá veces en las que se necesitarán varios millones de IVs para crackear la clave WEP. El número de IVs necesarios es muy dificil de predecir porque la mayoría de los puntos de acceso actuales funcionan muy bien y no generan IVs débiles que revelen parte de la clave WEP.

Generálmente, no intentes crackear la clave WEP hasta que tengas 200,000 o más IVs. Si lo ejecutas con pocos IVs, aircrack probará muchas claves durante mucho tiempo y no aplicará las técnicas estadísticas de forma adecuada. Puedes empezar probando con claves de 64 bit aircrack-ng -n 64 archivo.cap . Si se está usando una clave WEP de 64 bit, normalmente será crackeada en menos de 5 minutos (y con frecuencia en menos de 60 segundos) con pocos IVs. Es sorprendente que haya tantos APs que usan claves de 64 bit. Si no encuentras la clave de 64 bit en 5 minutos, reinicia aircrack con el modo genérico: aircrack-ng archivo.cap . Y cada vez que tengas 100,000 IVs más, reintenta aircrack-ng -n 64 archivo.cap y déjalo 5 minutos.

Cuando llegues a 600,000 IVs, cambia y empieza a probar claves de 128 bit. Sería extraño (pero no imposible) que fuese una clave de 64 bit y no se diese crackeado con 600,000 IVs. Por lo tanto ahora prueba aircrack-ng archivo.cap .

Cuando llegues a 2 millones de IVs, prueba a cambiar el fudge factor a -f 4 . Y déjalo entre 30 minutos y una hora. Reintenta aumentando el fudge factor sumando 4 de cada vez. Otra buena ocasión para aumentar el fudge factor es cuando aircrack-ng se para porque ha probado todas las claves.

Y mientras tanto, no te olvides de seguir capturando paquetes de datos. Recuerda la regla de oro, cuantos más IVs mucho mejor .

También lee la siguiente sección sobre como determinar las mejores opciones a usar. Esto te puede ayudar tambien a acelerar el proceso de obtención de la clave WEP. Por ejemplo, si la clave es numérica, podremos crackear la clave WEP con muchísimos menos IVs si usamos la opción -t . Entonces, si averiguas algo acerca de la naturaleza de la clave WEP, es sencillo probar algunas variaciones para tener éxito.

Como determinar las mejores opciones a usar

Mientras aircrack-ng se está ejecutando, frecuentemente solo puedes ver el comienzo de la clave en la primera columna. Aunque no conoces la clave WEP, esta información puede darte pistas sobre cual es la clave. si un caracter o byte de la clave tiene un número muy grande de votos, hay un 99.5% de posibilidades de que sea correcto. Vamos a ver que se puede hacer con estas pistas.

Si los bytes son por ejemplo: 75:47:99:22:50 entonces es obvio que la clave está formada solo por

números, como los 5 primeros bytes. Por lo tanto obtendremos la clave mucho antes y con menos IVs usando la opción -t para probar únicamente este tipo de claves. Mira Wikipedia Binary Coded Decimal para ver una descripción de los caracteres que busca la opción -t.

Si los bytes son 37:30:31:33:36 estos son todos valores numéricos si los convertimos a Ascii (70136). En este caso, es una buena idea usar la opción -h. El link del FAQ Converting hex characters to ascii te da información para relacionar los caracters hexadecimales con los Ascii. De todas formas sabremos muy fácilmente que se trata de caracteres numéricos porque veremos que empiezan todos los bytes por 3.

Y si los primeros bytes son algo como esto 74:6F:70:73:65, deberias de introducir esos valores en tu editor hexadecimal favorito o en alguno de los links proporcionados anteriormente, y verás, que puede ser el comienzo de alguna palabra, por lo que parece que está usando una clave ASCII; en esta situación activa la opción -c para probar únicamente con claves ASCII.

Otras pistas

Para procesar varios archivos al mimso tiempo, se puede usar un cmodín como el * o especificar cada archivo uno por uno.

Ejemplos:

- aircrack-ng -w password.lst wpa.cap wpa2.eapol.cap
- aircrack-ng *.ivs
- aircrack-ng archi*.ivs

Determinar una clave WPA/WPA2 depende absolutamente de que la palabra se encuentre en el diccionario que usemos. Por lo que es muy importante usar un buen diccionario. Puedes buscar en Internet algún diccionario. Hay varios disponibles.

Como has visto, si hay varias redes en tus archivos necesitarás elegir la que quieres crackear. En lugar de hacerlo manualmente, puedes especificar la red que quieras en la linea de comandos indicando su essid o su bssid. Esto se hace con las opciones -e o -b.

Otra alternativa es usar John the Ripper para crear un diccionario específico. Si sabes que la palabra clave es el nombre de una calle además de 3 digitos. Puedes crear una regla en JTR y ejecutar un comando como este:

```
 john --stdout --wordlist=specialrules.lst --rules | aircrack-ng -e test -a 2 -w
- /root/capture/wpa.cap
```

Problemas de uso

Mensaje de error "Please specify a dictionary (option -w)"

Esto significa que no tienes ese archivo de diccionario o que no se encuentra en el directorio actual. Si el diccionario se encuentra en otra carpeta, debes escribir la ruta completa al diccionario.

Votos negativos

Hay ocasiones en que los bytes tienen votos negativos. Y si tienes un montón de votos negativos significa que algo va mal. Lo más probable es que estés intentando crackear una clave dinámica o que

han cambiado la clave WEP mientras estabas capturando paquetes de datos. Recuerda que WPA/WPA2 solo puede ser crackeada con un diccionario. Si han cambiado la clave WEP, tendrás que empezar a capturar paquetes de nuevo desde el principio.

Airdecap-ng

Descripción

Con airdecap-ng puedes desencriptar archivos capturados que tengan encriptación WEP/WPA/WPA2. Tambien puede ser usado para ver la cabecera de una captura wireless sin encriptación.

Uso

```
airdecap-ng [opciones] <archivo cap>
```

Opción	Param.	Descripción
-l		no elimina la cabecera de 802.11
-b	bssid	dirección MAC del punto de acceso
-k	pmk	WPA/WPA2 Pairwise Master Key en hexadecimal
-e	essid	Nombre de la red
-p	pass	Clave WPA/WPA2
-w	key	Clave WEP en hexadecimal

Ejemplos de uso

El siguiente comando elimina las cabeceras wireless de una captura de una red sin encriptación:

```
airdecap-ng -b 00:09:5B:10:BC:5A red-abierta.cap
```

El siguiente comando desencripta un archivo con encriptación WEP usando la clave hexadecimal:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
```

El siguiente comando desencripta un archivo con encriptación WPA/WPA2 usando la palabra o passphrase :

```
airdecap-ng -e 'the ssid' -p passphrase  tkip.cap
```

Recomendaciones de uso

Para ESSIDs que contengan espacios, escribe el ESSID entre comillas: 'este contiene espacios'.

Airmon-ng

Descripción

Este script puede usarse para activar el modo monitor de las tarjetas wireless. Tambien puede usarse para parar las interfaces y salir del modo monitor. Si escribimos el comando airmon-ng sin parámetros veremos el estado de nuestras tarjetas.

Uso

usa: airmon-ng <start|stop> <interface> [canal]

Donde:

- <start|stop> indica si deseas iniciar o parar el modo monitor.(obligatorio)
- <interface> el nombre de la interface. (obligatorio)
- [channel] opcionalmente se puede especificar un número de canal.

Ejemplos de uso

Usos típicos

Para iniciar wlan0 en modo monitor: airmon-ng start wlan0

Para iniciar wlan0 en modo monitor en el canal 8: airmon-ng start wlan0 8

Para parar wlan0: airmon-ng stop wlan0

Para ver el estado: airmon-ng

Modo monitor de driver Madwifi-ng

Describimos como poner la interface en modo monitor. Despues de encender tu ordenador, escribe en una consola el comando iwconfig para ver el estado actual de tus tarjetas wireless. Verás algo similar a la siguiente salida:

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11b  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:0 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Si quieres usar la interface ath0 (que ya está siendo usada en modo managed):

airmon-ng stop ath0

Y el sistema responderá:

```
 Interface       Chipset         Driver

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

Ahora, si escribes iwconfig :

```
 lo        no wireless extensions.

 eth0      no wireless extensions.

 wifi0     no wireless extensions.
```

Puedes ver que ya no existe ath0.

Para iniciar ath0 en modo monitor: airmon-ng start wifi0

Y el sistema responderá:

```
 Interface       Chipset         Driver

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

Y si ahora escribimos iwconfig

```
 lo        no wireless extensions.

 eth0      no wireless extensions.

 wifi0     no wireless extensions.

 ath0      IEEE 802.11g  ESSID:""  Nickname:""
           Mode:Monitor  Frequency:2.457 GHz  Access Point: Not-Associated
           Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=0/3
           Retry:off   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality=0/94  Signal level=-98 dBm  Noise level=-98 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Observamos que ath0 está en modo monitor.

Si ath1/ath2 etc. están funcionando en modo managed, tienes que pararlas primero con la opción stop, por ejemplo:

```
 airmon-ng stop ath1
```

Y despues recuerda que puedes indicar el número del canal añadiéndolo al final del comando: airmon-ng start wifi0 9

Recomendaciones de uso

Para confirmar que la tarjeta está en modo monitor, escribe iwconfig . Así verás el nombre de la interface y si está activado el modo monitor .

Para el driver madwifi-ng, la información del punto de acceso que muestra iwconfig es la dirección MAC de la tarjeta wireless.

Si quieres capturar paquetes de un punto de acceso concreto, el canal actual de la tarjeta debe ser el mismo que el del AP. En este caso, es una buena idea incluir el número de canal cuando ejecutes el comando airmon-ng.

Airodump-ng

Descripción

Airodump-ng se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IVs con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP. Si tienes un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.

Uso

Antes de ejecutar airodump-ng, tienes que mirar con el script airmon-ng la lista de tus interfaces wireless detectadas. Es posible, pero no recomendable, ejecutar Kismet y airodump-ng al mismo tiempo.

```
uso: airodump-ng <opciones> <interface>[,<interface>,...]

Opciones:
    --ivs               : Graba ¨nicamente los IVs capturados
    --gpsd              : Usa GPSd
    --w <nombre archivo>: Nombre del archivo donde guardar las capturas
    -write     : Lo mismo que --w
    --beacons           : Guardar todas las balizas o beacons en el archivo
    --netmask <m·scara de red> : Filtrar APs por m·scara
    --bssid     <bssid> : Filtrar APs por BSSID

Por defecto, airodump-ng va saltando alrededor de los canales 2.4Ghz.
Puedes capturar en un canal especÌfico usando:
    --channel <canal>: Capturar en un canal especÌfico
    --band <abg>        : Banda en la que actuar· airodump-ng
    --cswitch  <mÈtodo> : Saltar de canal con este mÈtodo:
                  0     : FIFO (opciÛn por defecto)
                  1     : Round Robin
                  2     : Saltar al ¨ltimo
    -s                  : Lo mismo que --cswitch
```

Puedes convertir archivos .cap / .dump a formato .ivs o juntarlos.

Pistas de uso

¿Cual es el significado de los datos mostrados por airodump-ng?

airodump-ng nos mostrará una lista de los puntos de acceso detectados, y también una lista de los clientes conectados (stations). Como ejemplo puedes ver la siguiente captura de pantalla:

```
 CH  9 ][ Elapsed: 4 s ][ 2007-02-25 16:47

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

 00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN
NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP
bigbear

 BSSID              STATION            PWR  Lost  Packets  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51     2       14
 (not associated)   00:14:A4:3F:8D:13   19     0        4  mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1     0        5
```

Field	Descripción
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal. Su significado depende del driver que usemos, pero cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el driver no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes (stations) es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de tu tarjeta. Lo que significa que solo escuchas la mitad de la comunicación. Si todos los clientes tienen PWR -1 significa que el driver no tiene la cpacidad de detectar el nivel de señal.
RXQ	Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recividos correctamente en los últimos 10 segundos. Mira la nota para una explicación más detallada.
Beacons	Número de paquetes anucio o beacons enviadas por el AP. Cada punto de acceso envia alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
# Data	Número de paquetes de datos capturados (si tiene clave WEP, equivale tambien al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
#/s	Número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
CH	Número de canal (obtenido de los paquetes anuncio o beacons). Nota: Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
MB	Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22es 802.11b+ y velocidades mayores son 802.11g. El punto (despues del 54) indica que esa red soporta un preámbulo corto o short preamble .
ENC	Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta), WEP? = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o

	WPA/WPA2), WEP (sin el interrogante) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.
CIPHER	Detector cipher. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
AUTH	El protocolo de autenticación usado. Puede ser MGT, PSK (clave precompartida), o OPN (abierta).
ESSID	Tambien llamado SSID , que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes probe responses y association requests (son paquetes enviados desde un cliente al AP).
STATION	Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).
Lost	El número de paquetes perdidos en los últimos 10 segundos.
Packets	El número de paquetes de datos enviados por el cliente.
Probes	Los ESSIDs a los cuales ha intentado conectarse el cliente.

NOTAS:

RXQ: Se calcula a partir de los paquetes de datos y management. Supongamos que tienes 100% de RXQ y recibes 10 (o cualquier otra cantidad) beacons por segundo. Ahora de repente el RXQ baja a 90, pero todavía capturas las mismas beacons. Esto significa que el AP está enviando paquetes a un cliente pero no puedes escuchar o capturar los paquetes que salen del cliente hacia el AP (necesitas acercarte más al cliente). Otra situación puede ser, que tengas una tarjeta de 11MB (por ejemplo una prism2.5) y estes cerca del AP. Pero el AP está configurado en modo únicamente de 54MBit y tambien el RXQ disminuye, en este caso sabrás que hay conectado al menos un cliente a 54MBit.

Problemas de uso

airodump-ng cambia entre WEP y WPA

Esto ocurre porque tu driver no descarta los paquetes corruptos (que tienen un CRC inválido). Si es una ipw2100 (Centrino b), no tiene solución; por lo que deberías comprar una tarjeta mejor. Si es una Prism2, prueba a actualizar el firmware. En la sección de tutorials tienes un manual en castellano de como actualizar el firmware Prism.

airodump-ng no muestra ningún dato

Con el driver madwifi-ng asegúrate de que no hay otras VAPs activas. Hay problemas cuando se crea una nueva VAP en modo monitor y ya había otra VAP en modo managed.

Tienes que parar primero ath0 y despues iniciar wifi0:

```
airmon-ng stop ath0
airmon-ng start wifi0
```

o

```
wlanconfig ath0 destroy
wlanconfig ath create wlandev wifi0 wlanmode monitor
```

acketforge-ng

Descripción

El propósito de packetforge-ng es crear paquetes encriptados para poder inyectarlos con posterioridad. Podemos crear varios tipos de paquetes como arp requests , UDP, ICMP o paquetes hechos a la medida. El uso más común es crear paquetes ARP requests para ser inyectados.

Para crear un paquete encriptado, es necesario tener un archivo PRGA (pseudo random genration algorithm). Este archivo lo usaremos para encriptar el paquete que vamos a crear. Este archivo se obtiene con aireplay-ng chopchop o con el ataque de fragmentación.

Uso

Uso: packetforge-ng <modo> <opciones>

Opciones:

- -p <frame ctrl> : Fijar palabra frame control (en hexadecimal)
- -a <bssid> : seleccionar el punto de acceso por su dirección MAC
- -c <dmac> : seleccionar por la dirección MAC de destino
- -h <smac> : seleccionar por la dirección MAC de origen
- -j : seleccionar el bit FromDS
- -o : borrar el bit ToDS
- -e : deshabilitar la encriptación WEP
- -k <ip[:puerto]> : Fijar IP de destino [Puerto]
- -l <ip[:puerto]> : Fijar IP de origen [Puerto]
- -t ttl : Fijar hora
- -w <archivo> : Guardar el paquete es este archivo cap

Opciones de origen:

- -r <archivo> : leer paquete de este archivo
- -y <archivo> : leer PRGA de este archivo

Modos:

- arp : Crear paquete ARP (-0)
- udp : Crear paquete UDP (-1)
- icmp : Crear paquete ICMP (-2)
- custom : Crear paquete a la medida (-9)

Ejemplos de uso

Aquí ponemos un ejemplo de como generar un paquete arp request .

Primero hay que obtener un archivo xor (PRGA) con el ataque chopchop o con el ataque de fragmentación.

Despues usa un comando como el siguiente:

```
packetforge-ng -0 -a 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D -k 192.168.1.100 -l
192.168.1.1 -y fragment-0124-161129.xor -w arp-request
```

Donde:

- -0 indica que quieres generar un paquete arp request
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:0F:B5:AB:CB:9D es la dirección MAC que quieres usar
- -k 192.168.1.100 es la IP de destino. Por ejemplo en un paquete arp es la frase Who has this IP que quiere decir en castellano Quien tiene esta IP
- -l 192.168.1.1 es la IP de origen. Por ejemplo en un paquete arp aparecerá la frase Tell this IP , que significa Digo o tengo esta IP
- -y fragment-0124-161129.xor
- -w arp-packet

Asumiendo que estás experimentando con tu propio punto de acceso, el paquete arp request generado con anterioridad puede desencriptarse con la clave que ya conoces. Por lo que para mirar el paquete que hemos creado podemos desencriptarlo:

Escribe airdecap-ng -w <clave> arp-request

El resultado es algo como esto:

```
Total number of packets read            1
Total number of WEP data packets        1
Total number of WPA data packets        0
Number of plaintext data packets        0
Number of decrypted WEP  packets        1
Number of decrypted WPA  packets        0
```

Para ver el paquete que acabamos de desencriptar , escribimos tcpdump -n -vvv -e -s0 -r arp-request-dec

El resultado será similar a:

```
reading from file arp-request-dec, link-type EN10MB (Ethernet)
18:09:27.743303 00:0f:b5:ab:cb:9d > Broadcast, ethertype ARP (0x0806), length 42:
arp who-has 192.168.1.100 tell 192.168.1.1
```

Que es lo que esperábamos ver. Ahora podemos inyectar este paquete arp request con el siguiente comando: aireplay-ng -2 -r arp-request ath0 .

El programa nos contestará:

```
      Size: 68, FromDS: 0, ToDS: 1 (WEP)

           BSSID  =  00:14:6C:7E:40:80
       Dest. MAC  =  FF:FF:FF:FF:FF:FF
      Source MAC  =  00:0F:B5:AB:CB:9D

      0x0000:  0841 0201 0014 6c7e 4080 000f b5ab cb9d  .A....l~@.......
      0x0010:  ffff ffff ffff 8001 6c48 0000 0999 881a  ........lH......
      0x0020:  49fc 21ff 781a dc42 2f96 8fcc 9430 144d  I.!.x..B/....0.M
      0x0030:  3ab2 cff5 d4d1 6743 8056 24ec 9192 c1e1  :.....gC.V$.....
      0x0040:  d64f b709                                .O..

Use this packet ? y
```

```
Saving chosen packet in replay_src-0124-163529.cap
You should also start airodump-ng to capture replies.
End of file.
```

Introduciendo la y , inyectaremos el paquete que hemos creado con packetforge-ng.

Trucos de uso

A la mayor parte de los puntos de acceso no les importa las IPs que se usan en los paquetes arp request . En estos casos podemos usar 255.255.255.255 tanto para la IP de origen como para la IP de destino.

Problemas de uso

Un error muy común que comete mucha gente es incluir las opciones -j y/o -o creando paquetes inválidos. Estas opciones ajustan las variables FromDS y ToDS en el paquete que se ha generado. A menos que estes haciendo algo especial y realmente sepas lo que estás haciendo; no uses estas opciones. En general, no son necesarias.

Airtun-ng

Descripción

Airtun-ng sirve para crear interfaces virtuales denominadas tunnel interface . Tiene básicamente dos funciones:

- Permite monitorizar todo el tráfico encriptado con propósitos wIDS (wireless Intrusion Detection System).
- Inyectar de forma arbitraria tráfico en una red.

Para perfeccionar la captura de paquetes wIDS, debes conocer la clave de encriptación y el bssid de la red a monitorizar. Airtun-ng desencripta todo el tráfico de la red y lo pasa al sistema tradicional IDS usado por ejemplo por snort.

La inyección de tráfico puede hacerse bidireccional si conocemos la clave de encriptación completa. y solo podrá ser unidireccional si tenemos un PRGA obtenido a través de chopchop o un ataque de fragmentación. La principal ventaja de airtun-ng respecto a las otras utilidades de la suite aircrack-ng es que no puedes usar cualquier otra herramienta para crear, inyectar o esnifar paquetes.

Airtun-ng solo funciona en sistemas operativos linux.

Uso

uso: airtun-ng <opciones> <interface>

- -x nbpps : número máximo de paquetes por segundo (opcional)
- -a bssid : Fijar dirección MAC del punto de acceso (obligatorio)

- -i iface : capturar paquetes desde esta interface (opcional)
- -y archivo: leer PRGA de este archivo (opcional / tiene que usarse al menos una de las dos opciones: -y o -w)
- -w wepkey : usar esta clave WEP para encriptar los paquetes (opcional / tiene que usarse al menos una de las dos opciones: -y o -w)
- -t tods : Enviar paquetes al AP (1) o al cliente (0) (opcional / por defecto es 0)

Escenarios

wIDS

El primer escenario es wIDS. Pon tu tarjeta wireless en modo monitor y escribe el comando:

```
airtun-ng -a 00:14:6C:7E:40:80 -w 1234567890 ath0
```

Donde:

- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso a monitorear
- -w 1234567890 es la clave de encriptación
- ath0 es la interface que tenemos en modo monitor

El sistema nos contestará:

```
created tap interface at0
WEP encryption specified. Sending and receiving frames through ath0.
FromDS bit set in all frames.
```

Date cuenta que se ha creado la interface **at0**. Abre otra consola o shell y puedes levantar esta interface para poder usarla:

```
ifconfig at0 up
```

Esta interface (at0) recivirá una copia de cada paquete wireless que circule por la red. Los paquetes serán desencriptados con la clave que has proporcionado. En este punto, puedes usar algún programa para esnifar y analizar el tráfico. Por ejemplo, tcpdump o snort.

Inyección WEP

El siguiente escenario es cuando quieres inyectar paquetes en una red. Sigue los mismos pasos que en el primer escenario excepto definir una dirección IP válida para la red cuando levantes la interface at0:

```
ifconfig at0 192.168.1.83 netmask 255.255.255.0 up
```

Puedes comprobarlo con el comando ifconfig at0 analizando la salida.

```
at0       Link encap:Ethernet  HWaddr 36:CF:17:56:75:27
       inet addr:192.168.1.83  Bcast:192.168.1.255  Mask:255.255.255.0
       inet6 addr: fe80::34cf:17ff:fe56:7527/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:192 errors:0 dropped:0 overruns:0 frame:0
       TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:500
       RX bytes:25113 (24.5 KiB)  TX bytes:516 (516.0 b)
```

En este punto puedes usar cualquier programa para enviar tráfico a través de la interface at0 a cualquier cliente wireless. Por favor date cuenta de que por defecto FromDS está seleccionado. Lo que significa que los paquetes están marcados para ir a los clientes wireless. Si quieres que la comunicación sea con el AP o con clientes cableados, especifica la opción -t 1 cuando inicies airtun-ng.

NOTA IMPORTANTE: Las reglas normales para la inyección se aplican aquí tambien. Por ejemplo, estar asociado con el AP, que la MAC de la tarjeta sea la misma que utilizamos como origen de la inyección, etc.

Un uso interesante de este escenario es que permite usar una red con encriptación WEP utilizando un driver que soporte la inyección, pero no esa encriptación WEP; y hay que tener en cuenta que no todos los drivers soportan claves wep de 256bit o de 512bit o WPA.

Inyección PRGA

El siguiente escenario es aquel caso en el que queremos inyectar paquetes a la red pero no tenemos la clave WEP completa. Solo tenemos el PRGA obtenido a través de un ataque chopchop o de fragmentation. En este caso solo podremos inyectar paquetes salientes o outbound. No hay forma de desencriptar los paquetes entrantes (inbound) ya que no conocemos la clave WEP.

Pon la tarjeta wireless en modo monitor y escribe:

```
airtun-ng -a 00:14:6C:7E:40:80 -y fragment-0124-153850.xor ath0
```

Fijate en que el archivo PRGA se ha especificado utilizando la opción -y .

El sistema responde (fijate en el estado no reception):

```
created tap interface at0
WEP encryption by PRGA specified. No reception, only sending frames through ath0.
FromDS bit set in all frames.
```

A partir de aquí puedes definir una dirección IP válida para la red y levantar la interface at0:

```
ifconfig at0 192.168.1.83 netmask 255.255.255.0 up
```

Puedes comprobar esto escribiendo ifconfig at0 . Ahora puedes usar algún programa para enviar tráfico a través de la interface at0 a los clientes wireless.

Conectándose a dos puntos de acceso

El siguiente escenario es conectarse a dos redes wireless al mismo tiempo. Esto se hace simplemente iniciando airtun-ng dos veces, especificando la dirección MAC o bssid de cada una. Si los dos APs están en el mismo canal, esto debe funcionar a la perfeccción. Si no comparten el mismo canal, puedes escuchar con airodump-ng en ambos canales (no de forma simultanea, pero solo saltando entre esos dos canales). Suponiendo que los dos APs a los que nos queremos conectar están en los canales 1 y 11, escribiriamos airodump-ng -c 1,11 ath0 .

Conseguiremos dos tunnel interfaces (at0 y at1), cada una para un AP. Si no usan el mismo rango de IPs, las podremos usar al mismo tiempo. En teoria, se puede hacer esto incluso para más que dos APs, pero la calidad del enlace será peor ya que habrá que alternar entre 3 o más canales.

Copiar paquetes desde la interface opcional

El siguiente escenario consiste en copiar paquetes desde la interface opcional. El parámetro -i <interface wireless> es igual al parámetro -i de aireplay-ng. Se usa para especificar un origen distinto desde el que leer los paquetes, otra tarjeta diferente a la que usaremos para inyectar (ath0 en nuestro ejemplo). Un uso típico es escuchar con una tarjeta con muy buena sensibilidad en una interface; e inyectar con otra tarjeta con gran potencia de transmisión, que tienen mucha menos sensibilidad.

Pistas de uso

Esta utilidad es muy poderosa y utiliza conceptos avanzados. Por favor asegurate de que tienes conocimientos y experiencia suficiente con las otras utilidades de la suite aircrack-ng antes de usar airtun-ng.

Problemas de uso

S.O. Windows - No puedo encontrar el programa airtun-ng . Respuesta: airtun-ng solo funciona en linux.

Otras utilidades

WZCook

Recupera claves WEP en PCs con sistema operativo Windows XP, que se encuentran configuradas a través del servicio Wireless Zero Configuration utility . Este software es experimental, por lo que puede funcionar o no, dependiendo de la versión del Service Pack que tenga el Windows XP.

WZCOOK puede tambien recuperar la clave PMK (Pairwise Master Key), un valor de 256-bit que es el resultado de combinar la frase o passphrase 8192 veces junto con el ESSID y el tamaño del ESSID. La passphrase no puede recuperarse en si misma aunque, conocer la clave PMK es suficiente para conectarse a la red WPA con wpa_supplicant (mira el archivo README). El archivo de configuración wpa_supplicant.conf debe ser algo parecido a:

```
network={
   ssid="el_essid"
   pmk=5c9597f3c8245907ea71a89d[...]9d39d08e
```

Si no usas el servicio WZC, pero si usas la utilidad de USR, prueba a usar este valor del registro here:

```
HKey_Current_User/Software/ACXPROFILE/profilename/dot11WEPDefaultKey1
```

ivstools

Esta utilidad une varios archivos *.ivs*. Puedes unirlos (merge) o convertirlos (convert).

Merge

Uso merge archivos.*ivs*. Ejemplo:

```
ivstools --merge dump1.ivs dump2.ivs dump3.ivs out.ivs
```

Unirá los archivos dump1.ivs, dump2.ivs y dump3.ivs y creará un nuevo archivo out.ivs. Se pueden unir más de dos archivos, el archivo nuevo que vamos a crear debe ser el último argumento.

Nota: aircrack-ng es capaz de abrir varios archivos al mismo tiempo (cap y/o ivs)

Convert

Uso convert archivo.*cap* a *.ivs*. Ejemplo:

```
ivstools --convert out.cap out.ivs
```

Grabará los IVs contenidos en el archivo out.cap a out.ivs

Nota: Kismet crea archivos cap (la extensión es *.dump*), y tambien pueden ser convertidos

WARNING: pcap2ivs de algunas versiones de la suite aircrack, y aircrack-ng tiene un bug que crea capturas corruptas. No uses pcap2ivs. Si tienes un archivo con IVs corrupto por haber usado pcap2ivs, prueba a usar FixIvs para recuperarlo.