



CODE NAME



Airodump-ng se utiliza para capturar tramas de datos o paquetes raw o crudos del protocolo 802.11 n o g etc con el fin de utilizarlos con aircrack-ng. si un receptor GPS conectado al ordenador, airodum-ng es capaz de registrar las coordenadas de los puntos de acceso encontrados. Además, airodump-ng escribe un archivo de texto que contiene los detalles de todos los puntos de acceso y Clientes vistos.

Opciones

Syntaxis

airodump-ng [opciones] <nombre de la interface>

- H** --help mostrar opciones.
- i** **--ivs** sólo guardar IVs (sólo es útil para el craqueo) si el se especifica la opción, usted tiene que dar un prefijo de archivo. (**-w** opción de escritura)
- g** **--gpsd** indican que airodump-ng debe tratar de utilizar el GPSD para obtener coordenadas.
- w** <prefix> **--write**<prefix> Es el prefijo de archivo de volcado de usar. Si esta opción no se da, sólo mostrará los datos en la pantalla. Al lado de este archivo, se creará un archivo CSV con el mismo nombre que la captura
- e** **--beacons** Se registrará todas los beacons en el archivo cap. Por defecto sólo se registra una para cada red.
- u** <secs>, **--update** <secs> Retraso <secs> segundos de retardo entre actualizaciones de la pantalla (por defecto: 1 segundo). Útil para CPU lenta
- showack**

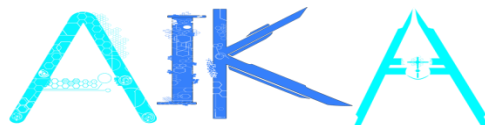
Imprime estadísticas ACK / CTS / RTS. Ayuda en la depuración y optimización general de la inyección. Es indicación de si, se inyecta demasiado rápido, llegar a la AP, si los paquetes son paquetes cifrados válidos. Permite detectar la estación de "oculto", que están demasiado lejos para capturar imágenes de alta tasa de bits, como tramas ACK se envían a 1Mbps. **-h** para estaciones ocultas **--showack**.

UNDERCODE





CODE NAME



--berlin <secs> Tiempo antes de retirar la AP / cliente cuando no se reciben más paquetes (predeterminado: 120 segundos).

-c <channel>[,<channel>[...]], tambien puede ser **--channel** <channel>[channel[,...]]

Indicar el canal (S) para escuchar. Por defecto airodump-ng escucha en todos los canales 2.ghz

-b <abq>, o tambien **--band** <abq>

Indique la banda en la que airodump-ng debe operar. que puede ser una combinación de la 'a', 'b' y Letras 'g' ('b' y 'g' utiliza 2,4 GHz y 'a' utiliza 5GHz). Incompatible con la opción **--channel**.

-s <method>, tambien puede ser **--cswith** <method>

Define la forma en airodump-ng establece los canales cuando se utiliza más de una tarjeta. valores válidos: 0 (FIFO, el valor predeterminado), 1 (Round Robin) o 2 (hop en último lugar).

-r <file> lee paquete de un archivo.

-x <msecs> simulación de exploración activa (enviar solicitud de sondeo y analizar las respuestas de la sonda).

--output-format <formats>

Definir los formatos a utilizar (separada por una coma), los valores posibles son: pcap, IVS, csv, gps, kismet, netxml. Los valores por defecto son pcap, csv, kismet, kismet-Newcore. 'pcap' es para el registro de una captura en pcap en formato pcap, "IVS" es el formato forwill (es un acceso directo para - IVS) 'csv' creará un archivo csv airodump-ng, "Kismet" creará un kismet csv archivo y 'kismte-Newcore' creará el archivo netxml kismet, 'gps' es un acceso directo para - gps. Valores Teses se pueden combinar con la excepcion de IVS y pcap.

--ignore-negative-one

Retire el mensaje que dice "canal <interface> fija: -1'.

OPCIONES DE FILTRO:

-t <OPN|WEP|WPA|WPA1|WPA2>, **--encrypt** <OPN|WEP|WPA|WPA1|WPA2>

Solo mostrara los cifrados especificados: '-t' pueden ser mas de uno ejemplo: **-t opn -t wpa2'**

-m <mask >, **--netmask** <mask> sólo mostrará las redes que coincidan con el BSSID a Conceder en combinación máscara de red. Es necesario **--BSSID** (o puede ser **-d**) a especificar.

-a sólo mostrará los clientes asociados.

INTERACTUAR CON AIRODUMP-NG.

Airodump-ng puede recibir e interpretar las pulsaciones de teclas mientras se ejecuta. La siguiente lista describe las claves asignadas actualmente y las supuestas acciones

- a** seleccione áreas activas por los ciclos a través de estas opciones de visualización: AP + STA + ACK, sólo AP: sólo STA
- d** reiniciar la clasificación por defecto (POWER)
- i** invertir algoritmo de ordenación
- m** marcar el AP seleccionado o el ciclo a través de colores diferentes si el AP seleccionado ya está marcado
- r** (de-) activa la clasificación en tiempo real - se aplica cada vez que el algoritmo de ordenación es mostrado



S cambiar Columnas de orden, que incluye actualmente; BSSID: pwr level: beacons;data packets; packet rate ; channel : max . data rate ;encryption; strongest ciphersuite; strong-est authentication; ESSID

SPACE pausar y refrescar la pantalla/mostrar resumen

TAB activar / desactiva el desplazamiento por la lista de AP

Up seleccionar el AP anterior al marcado actualmente en la lista de visualización, si es viable

DOWN seleccionar la AP después de la marcada actualmente AP

Si se selecciona un punto de acceso o marca, todas las estaciones conectadas también serán seleccionados o marcados con el mismo color que el punto de acceso correspondiente.

Ejemplos

Airodump-ng --band bg ath0

```
-----
CH 9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ BAT: 2 hours 10 mins ][ WPA handshake:
00:14:6C:7E:40:80

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             <length: 7>
00:14:6C:7A:41:81  34 100       57        14  1  9  11  WEP  WEP      bigbear
00:14:6C:7E:40:80  32 100      752        73  2  9  54  WPA  TKIP  PSK    teddy

BSSID      STATION            PWR   Rate  Lost  Frames  Probes
00:14:6C:7A:41:81  00:0F:B5:32:31:31  51   11-11    2     14  bigbear
(not associated)  00:14:A4:3F:8D:13  19   11-11    0      4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1  -1   11-2     0      5  bigbear
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2  35   36-24    0     99  teddy
-----
```

BSSID

Dirección MAC del AP. En la sección de clientes, un BSSID de "(not associated)" el cliente no esta asociado a ningun AP(acces point). En este estado no asociado, que es la búsqueda de un punto de acceso para conectarse con el.

PWR

Nivel de señal reportado por la tarjeta. La señal es mayor en cuanto este mas cerca al punto de acceso o de la estación. si el BSSID PWR es -1, entonces el driver no soporta informes de nivel de señal. Si el PWR es -1 para un número limitado de estaciones, entonces este es un paquete que venían de la AP al cliente pero las transmisiones clientes están fuera de alcance . Si todos los clientes tienen PWR como -1, entonces el controlador no es compatible con informes de nivel de señal.

RXQ

Sólo se muestra cuando en un canal fijo, recibirá la calidad se mide por el porcentaje de paquetes (calidad de tramas de datos) recibido con éxito en los últimos 10 segundos. Se mide la calidad de los datos. Esa es la idea, esto le permite leer más cosas de este valor. Digamos que tienes un 100 por ciento RXQ y los 10 (o lo que sea la tarifa) beacons por segundo estan ahora de RXQ repente cae por debajo de 90, pero todavía se capturan todas los beacons enviados. En otro caso como por ejemplo



sería que RXQ sea 10 y no obtengamos ni un solo beacon esto significaría que no existe el suficiente tráfico o que necesitamos estar mas cerca del AP .

Beacons

Número de beacons(paquetes) enviados por el AP. Cada punto de acceso envía unos diez beacons por segundo a la velocidad más baja (1M), por lo que normalmente se puede recoger la forma varía mucho.

#data

Número de paquetes capturados, incluyendo los paquetes de difusión de datos.

#/s

Numero de paquetes por cada 10 segundos.

CH

Número de canal (paquetes beacons forma adoptada). Nota: a veces los paquetes de otros canales son capturados incluso si airodump-ng esta orientado a un solo canal , debido a las interferencias de radio y/o a que mas de un AP esta en el mismo canal .

MB

Máxima velocidad soportada por AP. Si MB = 11, es 802.11b, si MB = 22 es 802.11b + las tasas más altas son 802.11g.the punto (después de 54 arriba) indica preámbulo corto es compatible. 'e' indica que la red dispone de QoS (802.11e) enable.

ENC

Algoritmo de cifrado en uso. OPN = sin encriptación "WEP" = wep o superior (no hay datos suficientes para elegir entre WEP y WPA/WPA2), WEP (sin el signo de interrogación) indica estática o dinámica WEP y WPA2 o WPA o WPA2 si TKIP o CCMP o MGT es presente.

CIPHER

El sistema de cifrado detectado. Uno de CCMP, WRAP, TKIP, WEP, WEP 40 o WEP104. No es obligatorio, pero se suele utilizar TKIP con WPA y CCMP se suele utilizar con WPA2. WEP40 se muestra cuando el índice de la clave es rallador luego 0. La norma establece que el índice puede ser 0-3 para 40 bits y debe ser 0 para 104 bits.

AUTH

El protocolo de autenticación utilizado. uno de MGT (WPA/WPA2 usando un servidor de autenticación por separado), SKA (clave compartida para WEP(shared key for WEP)), PSK (clave pre-compartida para WPA/WPA2 (pre- shared key for WPA/WPA2)), o OPN (abierto para WEP (open for WEP))



CODE NAME



ESSID

Nombre del AP "SSID", que puede estar vacía si se activa ESSID oculta. En este caso, airodump-ng intentará obtener información acerca del nombre mediante pruebas de solicitud de asociación.

STATION

La dirección MAC de cada estación o estaciones asociadas o en busca de un punto de acceso para conectar con los AP los que no están asociados actualmente con un AP tienen un BSSID de "(not associated)".

RATE

Aparece cuando existe tráfico entre el cliente y el AP siendo el primer número la velocidad de los datos del AP (BSSID) al cliente (STATION). el segundo los datos del cliente (STATION) al AP (BSSID)

LOST

Esto significa la pérdida de paquetes próximos por el cliente. Para determinar el número de paquetes perdidos hay un campo de secuencia en cada paquete enviado,

PACKETS

Número de paquetes enviados por el cliente.

Probes

Los ESSIDs sondeadas del cliente, son las redes que el cliente está tratando de conectarse o está conectado actualmente

La primera parte es los puntos de acceso detectados. Lo segundo es una lista de los clientes inalámbricos detectados, estaciones. Al basarse en la potencia de la señal, se puede determinar con precisión incluso físicamente la ubicación de una estación particular.





Bueno antes de iniciar el airodump-ng es necesario tener nuestra tarjeta de red inalámbrica en modo monitor y claro antes saber el nombre de nuestra interface tipeamos **iwconfig**

```
File Edit View Bookmarks Settings Help
root@bt:~# iwconfig>
lo    no wireless extensions.

wlan0 IEEE 802.11bg ESSID:off/any
       Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
       Retry long limit:7 RTS thr:off Fragment thr:off
       Encryption key:off
       Power Management:off

eth0  no wireless extensions.

root@bt:~#
```

Y cambiamos con airmon-ng (ver correspondiente tutorial de esta herramienta)

```
File Edit View Bookmarks Settings Help
root@bt:~# airmon-ng start wlan0
```

Una ves esto echo pasamos con el primer comando que nos permitira ver todo el trafico

```
File Edit View Bookmarks Settings Help
root@bt:~# airodump-ng mon0
```




```
File Edit View Bookmarks Settings Help
CH 3 || Elapsed: 12 s || 2013-10-02 23:06 || sorting by number of data packets
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
[redacted] -69 6 2 0 1 54 WEP WEP [redacted]
[redacted] -68 10 0 0 7 54e WEP WEP
[redacted] -58 10 0 0 6 54e WPA2 CCMP PSK
[redacted] -66 5 0 0 2 54 WEP WEP
[redacted] -72 2 0 0 11 54e WPA2 CCMP PSK

BSSID STATION PWR Rate Lost Frames Probe
[redacted] [redacted] -70 0 - 1 0 2

MAC CH PWR ACK ACK/s CTS RTS_RX RTS_TX OTHER
[redacted] 118 -70 4 0 0 0 0 0
[redacted] 158 -71 2 0 0 0 0 0
[redacted] 108 -71 1 0 0 0 0 0
```

Asi se muestra la informacion que es escuchada con nuestra tarjeta inalambrica es importante recordar que podemos interactuar con esta interface como ya se a comentado en la sintaxis de esta herramienta

```
File Edit View Bookmarks Settings Help
CH 7 || Elapsed: 20 s || 2013-10-02 23:06 || paused output
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
[redacted] -69 9 2 0 1 54 WEP WEP [redacted]
[redacted] -68 13 0 0 7 54e WEP WEP
[redacted] -58 13 0 0 6 54e WPA2 CCMP PSK
[redacted] -66 5 0 0 2 54 WEP WEP
[redacted] -71 4 0 0 11 54e WPA2 CCMP PSK

BSSID STATION PWR Rate Lost Frames Probe
[redacted] [redacted] -70 0 - 1 0 2

root@bt:~#
```

Con la tecla ctrl+c detenemos la ejecucion del programa



Una vez seleccionado el target nos valemos de los filtros para “solo” escuchar lo que se transmite en un determinado AP la sintaxis puede ser como la siguiente

Airodump-ng --bssid (mac del AP) **-c** (canal del AP) **-w** (ruta del archivo donde se escribieran los archivos en mi caso le puse el nombre de kitikiti) **mon0** (esta es el nombre de mi interface en monitor)

La mac(puede ser de AP o de un cliente) en la imagen de color turquesa y el ssid o nombre del ap de color verde

```
File Edit View Bookmarks Settings Help
root@bt:~# airodump-ng --bssid [redacted] -c 2 -w /root/pru/kitikiti mon0
```

```
File Edit View Bookmarks Settings Help
CH 2 || Elapsed: 20 s || 2013-10-02 23:07
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
[redacted] -66 50 111 0 0 2 54 WEP WEP [redacted]
BSSID STATION PWR Rate Lost Frames Probe
```

Toma en cuenta que si vemos mas de un AP en un mismo canal y tu te encuentras alajado de ellos el trafico se puede ver afectado puesto que las señales se solapan entresi y esto causa que los paquetes no sean los correctos para limpieza de tus capturas puedes usar la herramienta de airdecloak-ng para ello.



CODE NAME

AIKA

Para mas informacion visita mi blog y los sitios recomendados

Blog: <http://codenameaika.blogspot.com/>

UNDERC0DE

<http://underc0de.org>



UNDERC0DE