Aircrack-ng

Airodump-ng

Description

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs [http://en.wikipedia.org/wiki/Initialization_vector] (Initialization Vector) for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

Additionally, airodump-ng writes out several files containing the details of all access points and clients seen.

Usage

Before running airodump-ng, you may start the airmon-ng script to list the detected wireless interfaces. It is possible, but not recommended, to run Kismet [http://www.kismetwireless.net] and airodump-ng at the same time.

```
usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
    --ivs                 : Save only captured IVs
    --gpsd                : Use GPSd
    --write      <prefix> : Dump file prefix
    -w                    : same as --write
    --beacons             : Record all beacons in dump file
    --update       <secs> : Display update delay in seconds
    --showack             : Prints ack/cts/rts statistics
    -h                    : Hides known stations for --showack
    -f            <msecs> : Time in ms between hopping channels
    --berlin       <secs> : Time before removing the AP/client
                            from the screen when no more packets
                            are received (Default: 120 seconds)
    -r             <file> : Read packets from that file
    -T                    : While reading packets from a file,
                            simulate the arrival rate of them
                            as if they were "live".
    -x            <msecs> : Active Scanning Simulation
    --manufacturer        : Display manufacturer from IEEE OUI list
    --uptime              : Display AP Uptime from Beacon Timestamp
    --wps                 : Display WPS information (if any)
    --output-format
                <formats> : Output format. Possible values:
                            pcap, ivs, csv, gps, kismet, netxml, logcsv
    --ignore-negative-one : Removes the message that says
                            fixed channel <interface>: -1
    --write-interval
                <seconds> : Output file(s) write interval in seconds
    --background <enable> : Override background detection.
    -n              <int> : Minimum AP packets recv'd before
                            for displaying it

Filter options:
    --encrypt   <suite>   : Filter APs by cipher suite
    --netmask <netmask>   : Filter APs by mask
    --bssid     <bssid>   : Filter APs by BSSID
    --essid     <essid>   : Filter APs by ESSID
    --essid-regex <regex> : Filter APs by ESSID using a regular
                            expression
    -a                    : Filter unassociated clients

By default, airodump-ng hop on 2.4GHz channels.
You can make it capture on other/specific channel(s) by using:
    --ht20                : Set channel to HT20 (802.11n)
    --ht40-               : Set channel to HT40- (802.11n)
    --ht40+               : Set channel to HT40+ (802.11n)
    --channel <channels>  : Capture on specific channels
    --band <abg>          : Band on which airodump-ng should hop
    -C    <frequencies>   : Uses these frequencies in MHz to hop
    --cswitch  <method>   : Set channel switching method
                  0       : FIFO (default)
                  1       : Round Robin
                  2       : Hop on last
    -s                    : same as --cswitch

    --help                : Displays this usage screen
```

You can convert .cap / .dump file to .ivs format or merge them.

Usage Tips

What's the meaning of the fields displayed by airodump-ng ?

airodump-ng will display a list of detected access points, and also a list of connected clients (“stations”). Here's an example screenshot:

```
 CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ 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              NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11e  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  Packets  Notes  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24    2       14
 (not associated)   00:14:A4:3F:8D:13   19    0-0     0        4           mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36    0        5
 00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54    0       99           teddy
```

The first line shows the current channel, elapsed running time, current date and optionally if a WPA/WPA2 handshake was detected. In the example above, “WPA handshake: 00:14:6C:7E:40:80” indicates that a WPA/WPA2 handshake was successfully captured for the BSSID.

In the example above the client rate of “36-24” means:

- The first number is the last data rate from the AP (BSSID) to the Client (STATION). In this case 36 megabits per second.
- The second number is the last data rate from Client (STATION) to the AP (BSSID). In this case 24 megabits per second.
- These rates may potentially change on each packet transmission. It is simply the last speed seen.
- These rates are only displayed when locked to a single channel, the AP/client transmission speeds are displayed as part of the clients listed at the bottom.
- NOTE: APs need more then one packet to appear on the screen. APs with a single packet are not displayed.

Field	**Description**
BSSID	MAC address of the access point. In the Client section, a BSSID of “(not associated)” means that the client is not associated with any AP. In this unassociated state, it is searching for an AP to connect with.
PWR	Signal level reported by the card. Its signification depends on the driver, but as the signal gets higher you get closer to the AP or the station. If the BSSID PWR is -1, then the driver doesn't support signal level reporting. If the PWR is -1 for a limited number of stations then this is for a packet which came from the AP to the client but the client transmissions are out of range for your card. Meaning you are hearing only 1/2 of the communication. If all clients have PWR as -1 then the driver doesn't support signal level reporting.
RXQ	Receive Quality as measured by the percentage of packets (management and data frames) successfully received over the last 10 seconds. See note below for a more detailed explanation.
Beacons	Number of announcements packets sent by the AP. Each access point sends about ten beacons per second at the lowest rate (1M), so they can usually be picked up from very far.
# Data	Number of captured data packets (if WEP, unique IV count), including data broadcast packets.
#/s	Number of data packets per second measure over the last 10 seconds.
CH	Channel number (taken from beacon packets). Note: sometimes packets from other channels are captured even if airodump-ng is not hopping, because of radio interference or overlapping channels.
MB	Maximum speed supported by the AP. If MB = 11, it's 802.11b, if MB = 22 it's 802.11b+ and up to 54 are 802.11g. Anything higher is 802.11n or 802.11ac. The dot (after 54 above) indicates short preamble is supported. Displays “e” following the MB speed value if the network has QoS enabled.
ENC	Encryption algorithm in use. OPN = no encryption,“WEP?” = WEP or higher (not enough data to choose between WEP and WPA/WPA2), WEP (without the question mark) indicates static or dynamic WEP, and WPA, WPA2 or WPA3 if TKIP or CCMP is present (WPA3 with TKIP allows WPA or WPA2 association, pure WPA3 only allows CCMP). OWE is for Opportunistic Wireless Encryption, aka Enhanced Open.
CIPHER	The cipher detected. One of CCMP, WRAP, TKIP, WEP, WEP40, or WEP104. Not mandatory, but TKIP is typically used with WPA and CCMP is typically used with WPA2. WEP40 is displayed when the key index is greater then 0. The standard states that the index can be 0-3 for 40bit and should be 0 for 104 bit.
AUTH	The authentication protocol used. One of MGT (WPA/WPA2 using a separate authentication server), SKA (shared key for WEP), PSK (pre-shared key for WPA/WPA2), or OPN (open for WEP).
ESSID	Shows the wireless network name. The so-called “SSID”, which can be empty if SSID hiding is activated. In this case, airodump-ng will try to recover the SSID from probe responses and association requests. See this section for more information concerning hidden ESSIDs.
STATION	MAC address of each associated station or stations searching for an AP to connect with. Clients not currently associated with an AP have a BSSID of “(not associated)”.
Rate	Station's receive rate, followed by transmit rate. Displays “e” following each rate if the network has QoS enabled.
Lost	The number of data packets lost over the last 10 seconds based on the sequence number. See note below for a more detailed explanation.
Packets	The number of data packets sent by the client.
Notes	Additional information about the client, such as captured EAPOL or PMKID.
Probes	The ESSIDs probed by the client. These are the networks the client is trying to connect to if it is not currently connected.

NOTES:

RXQ expanded:
Its measured over all management and data frames. The received frames contain a sequence number which is added by the sending access point. RXQ = 100 means that all packets were received from the access point in numerical sequence and none were missing. That's the clue, this allows you to read more things out of this value. Lets say you got 100 percent RXQ and all 10 (or whatever the rate) beacons per second coming in. Now all of a sudden the RXQ drops below 90,

but you still capture all sent beacons. Thus you know that the AP is sending frames to a client but you can't hear the client nor the AP sending to the client (need to get closer). Another thing would be, that you got a 11MB card to monitor and capture frames (say a prism2.5) and you have a very good position to the AP. The AP is set to 54MBit and then again the RXQ drops, so you know that there is at least one 54MBit client connected to the AP.

N.B.: RXQ column will only be shown if you are locked on a single channel, not channel hopping.

Lost expanded:
It means lost packets coming from the client. To determine the number of packets lost, there is a sequence field on every non-control frame, so you can subtract the second last sequence number from the last sequence number and you know how many packets you have lost.

Possible reasons for lost packets:

1. You cannot send (in case you are sending) and listen at the same time, so every time you send something you can't hear the packets being transmitted in that interval.
2. You are maybe losing packets due too high transmit power (you may be too close to the AP).
3. There is too much noise on the current channel (other APs, microwave oven, bluetooth…)

To minimize the number of lost packets, vary your physical position, type of antenna used, channel, data rate and/or injection rate.

Run aircrack-ng while capturing data

To speed up the cracking process, run aircrack-ng while you are running airodump-ng. You can capture and crack at the same time. Aircrack-ng will periodically reread the captured data so it is always working with all the available IVs.

Limiting Data Capture to a Single AP

To limit the data capture to a single AP you are interested in, include the "- -bssid" option and specify the AP MAC address. For example: "airodump-ng -c 8 - -bssid 00:14:6C:7A:41:20 -w capture ath0".

How to Minimize Disk Space for Captures

To minimize disk space used by the capture, include the "- -ivs" option. For example: "airodump-ng -c 8 - -bssid 00:14:6C:7A:41:20 -w capture - -ivs ath0". This only stores the initialization vectors and not the full packet. This cannot be used if you are trying to capture the WPA/WPA2 handshake or if you want to use PTW attack on WEP.

How to Select All APs Starting With Similar BSSIDs

Lets say, for example, you wish to capture packets for all Cisco-Linksys APs where the BSSID starts with "00:1C:10".

You specify that starting bytes you wish to match with the "-d" / "–bssid" option and pad with zeroes to a full MAC. Then use "-m" / "–netmask" option to specify which part of the BSSID you wish to match via "F"s and pad with zeroes to a full MAC.

So since you want to match "00:1C:10", you use "FF:FF:FF".

```
airodump-ng -d 00:1C:10:00:00:00 -m FF:FF:FF:00:00:00 wlan0
```

How to Select Specific Channels or a Single Channel

The "–channel" (-c) option allows a single or specific channels to be selected.

Example of a single channel:

```
airodump-ng -c 11 wlan0
```

For cards which needs to be reset when on a single channel:

```
airodump-ng -c 11,11 wlan0
```

Example of selected channels:

```
airodump-ng -c 1,6,11 wlan0
```

Text Files Containing Access Points and Clients

Each time airodump-ng is run with the option to write IVs or full packets, a few text files are also generated and written to disk. They have the same name and a suffix of ".csv" (CSV file), ".kismet.csv" (Kismet CSV file) and ".kismet.netxml" (Kismet newcore netxml file).

The CSV file contains the details of all access points and clients seen. See kismet documentation for more details about the kismet CSV and netxml.

Here is an example:

```
BSSID, First time seen, Last time seen, channel, Speed, Privacy, Cipher, Authentication, Power, # beacons, # IV , LAN IP, ID-length, ESSID, Key
00:1C:10:26:22:41, 2007-10-07 12:48:58, 2007-10-07 12:49:44,  6,  48, WEP , WEP,   , 171,      301,        0, 0.  0.  0.  0,   5, zwang,
00:1A:70:51:B5:71, 2007-10-07 12:48:58, 2007-10-07 12:49:44,  6,  48, WEP , WEP,   , 175,      257,        1, 0.  0.  0.  0,   9, brucey123,
00:09:5B:7C:AA:CA, 2007-10-07 12:48:58, 2007-10-07 12:49:44, 11,  54, OPN ,    ,   , 189,      212,        0,   0.  0.  0.  0,   7, NETGEAR,

Station MAC, First time seen, Last time seen, Power, # packets, BSSID, Probed ESSIDs
00:1B:77:7F:67:94, 2007-10-07 12:49:43, 2007-10-07 12:49:43, 178,        3, (not associated) ,
```

Usage Troubleshooting

I am getting no APs or clients shown

If you have a laptop with a builtin wireless card, ensure it is “turned on / enabled” in the bios

Does your card works in managed mode? If not, the problem is not with airodump-ng. You need to get this working first.

See if this madwifi-ng web page [http://madwifi-project.org/wiki/UserDocs/MiniPCI] has information that may be helpful.

Although it is not very “scientific”, sometimes simply unloading then reloading the driver will get it working. This is done with the rmmod and modprobe commands.

Also see the next troubleshooting tip.

I am getting little or no data

- Make sure you used the “-c” or “- -channel” option to specify a single channel. Otherwise, by default, airodump-ng will hop between channels.
- You might need to be physically closer to the AP to get a quality signal.
- Make sure you have started your card in monitor mode with airmon-ng (Linux only).

Note for madwifi-ng

Make sure there are no other VAPs running. There can be issues when creating a new VAP in monitor mode and there was an existing VAP in managed mode.

You should first stop ath0 then start wifi0:

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

or

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

Airodump-ng keeps switching between WEP and WPA

This is happening because your driver doesn't discard corrupted packets (that have an invalid CRC). If it's a ipw2100 (Centrino b), it just can't be helped; go buy a better card. If it's a Prism2, try upgrading the firmware.

Airodump-ng stops capturing data after a short period of time

The most common cause is that a connection manager is running on your system and takes the card out of monitor mode. Be sure to stop all connection managers prior to using the aircrack-ng suite. In general, disabling “Wireless” in your network manager should be enough but sometimes you have to stop them completely. It can be done with airmon-ng:

```
airmon-ng check kill
```

Recent linux distributions use *upstart*; it automatically restarts the network manager. In order to stop it, see the following entry.

As well, make sure that wpa_supplicant [http://hostap.epitest.fi/wpa_supplicant/] is not running. Another potential cause is the PC going to sleep due to power saving options. Check your power saving options.

The madwifi-ng driver for the atheros chipset contains a bug in releases up to r2830 which causes airodump-ng in channel hopping mode to stop capturing data after a few minutes. The fix is to use r2834 or above of the madwifi-ng drivers.

See also this entry for recent

Hidden SSIDs "<length: ?>"

You will sometimes see “<length: ?>” as the SSID on the airodump-ng display. This means the SSID is hidden. The “?” is normally the length of the SSID. For example, if the SSID was “test123” then it would show up as “<length: 7>” where 7 is the number of characters. When the length is 0 or 1, it means the AP does not reveal the actual length and the real length could be any value.

To obtain the hidden SSID there are a few options:

- Wait for a wireless client to associate with the AP. When this happens, airodump-ng will capture and display the SSID.
- Deauthenticate an existing wireless client to force it to associate again. The point above will apply.
- Use a tool like mdk3 [http://homepages.tu-darmstadt.de/~p_larbig/wlan] to bruteforce the SSID.
- You can use Wireshark combined with one or more of these filters to review data capture files. The SSID is included within these packets for the AP.

```
 wlan.fc.type_subtype == 0 (association request)
 wlan.fc.type_subtype == 4 (probe request)
 wlan.fc.type_subtype == 5 (probe response)
```

Airodump-ng freezes when I change injecting rate

There are two workarounds:

- Change the rate before using airodump-ng
- Restart airodump-ng

"fixed channel" error message

If the top of your airodump screen looks something like:

```
 CH  6 ][ Elapsed: 28 s ][ 2008-09-21 10:39 ][ fixed channel ath0: 1
```

Then this means you started started airodump-ng with a fixed channel parameter (-c / –channel) but some other process is changing the channel. “CH 6” on the left is the channel that was specified when airodump-ng was started. “fixed channel ath0: 1” on the right indicates that ath0 was used when airodump-ng was started but the interface is currently on channel 1 (instead of channel 6). You might also see this channel number changing indicating that channel scanning is taking place.

It is critical that the root cause of the problem be eliminated and then airodump-ng restarted again. Here are some possible reasons and how to correct them:

- There is one or more interfaces in “managed mode” and these are are scanning for an AP to connect to. Do not use any command, process or program to connect to APs at the same time as you use the aircrack-ng suite.
- Other processes are changing the channel. A common problem are network managers. You can also use “airmon-ng check” on current versions of the aircrack-ng suite to identify problem processes. Then use “kill” or “killall” to destroy the problem processes. For example, use “killall NetworkManager && killall NetworkManagerDispatcher” to eliminate network managers.
- If you are using the madwifi-ng driver and have more then the ath0 interface created, the driver may be automatically scanning on the other interfaces. To resolve this, stop all interfaces except ath0.
- You have wpa_supplicant running at the same time. Stop wpa_supplicant.
- You run airmon-ng to set the channel while airodump-ng is running. Do not do this.
- You run another instance of airodump-ng in scanning mode or set to another channel. Stop airodump-ng and do not do this.

It can also means that you cannot use this channel (and airodump-ng failed to set the channel). Eg: using channel 13 with a card that only supports channels from 1 to 11.

Where did my output files go?

You ran airodump-ng and now cannot find the output files.

First, make sure you ran airodump-ng with the option to create output files. You must include -w or –write plus the file name prefix. If you fail to do this then no output files are created.

By default, the output files are placed in the directory where you start airodump-ng. Before starting airodump-ng, use “pwd” to display the current directory. Make a note of this directory so your return to it a later time. To return to this directory, simply type “cd <full directory name including the full path>”.

To output the files to a specific directly, add the full path to the file prefix name. For example, lets say you want to output all your files to “/aircrack-ng/captures”. First, create /aircrack-ng/captures if it does not already exist. Then include “-w /aircrack-ng/captures/<file prefix>” on your airodump-ng command line.

To access your files later when running aircrack-ng, either change to the directory where the files are located or prefix the file name with the full path.

Windows specific

The adapter is not detected

1. Make sure the special driver is installed. Read Driver installing page for a guide on installing such driver.
2. If the special driver is installed but it still isn't detected, try another version of the driver (older or newer).

The application has failed to start because MSVCR70.dll was not found

Obtain the file from http://www.dll-files.com/dllindex/dll-files.shtml?msvcr70 [http://www.dll-files.com/dllindex/dll-files.shtml?msvcr70] or it is also located in the bin directory of the zip file of the Windows version of aircrack-ng suite. Typically, it should be located in **C:\<windows root directory>\system32**.

The application freezes under Microsoft Windows

Ensure you are using the correct drivers for your particular wireless card. Plus the correct Wildpackets driver. Failure to do so may result in your PC freezing when running airodump-ng.

The powersaver option on the card can also cause the application to freeze or crash. Try disabling this option via the “Properties” section of your card. Another kludge is to keep moving your mouse every few minutes to eliminate the powersaver option from kicking in.

How to get airodump-ng to work under Windows Vista?

The following fix has reportedly worked for some people: What you have to do is right click on airodump-ng.exe, select properties, compatibility, and check run in compatibility mode for Windows XP. Also, check the box at the bottom that says to run as administrator.

peek.sys file is zero bytes!

Peek.sys being zero bytes is normal. You can proceed to use airodump-ng.

This file is created by airodump-ng to prevent the driver dialog box from being shown each time the program is run.

error: "Failed to download Peek files"

You may have a DNS problem or there is an Internet connectivity problem. Manually download the following files and place them in the same directory as the airodump-ng.exe file.

- Peek.dll and Peek5.sys [http://www.tuto-fr.com/tutoriaux/crack-wep/fichiers/wlan/winxp/Peek.zip]

Various errors referencing peek.dll

If you receive one or more of these errors:

- Dialog Box Error: “The application or DLL C:\????\bin\Peek.dll is not a valid Windows image. Please check this against your installation diskette.”
- GUI Screen Error: “LoadLibrary (Peek.dll) failed, make sure this file is present in the current directory. Press Ctrl-c to exit.”

This means the peek.dll and/or peek5.sys file are missing from the directory which contains the airodump-ng.exe file or are corrupted. See the previous troubleshooting entry for instructions on how to download the files.

No data is captured under Windows

- Using the Windows network connections manager, ensure the wireless device is enabled.
- Ensure that your Windows wireless configuration manager is enabled and the configuration manager that comes with your card is disabled.
- Do not run any wireless configuration manager while trying to use the aircrack-ng suite.
- Do not run any wireless program such as monitor mode checkers while trying to use the aircracck-ng suite.
- Check the “Driver Provider” name for the driver being used for your wireless device via properties to ensure it says Wildpackets. Also confirm the driver version is what you expect.
- Using a command prompt, change to the directory where airodump-ng.exe is located. Confirm that peek.dll and peek.sys exist in this directory.
- Using the command prompt and while still in the directory containing airodump-ng, try starting airodump-ng. It should not ask you about downloading Wildpackets or peek files. If it does, you do not have everything installed correctly. Redo the installation instructions.

Review all your steps

If airodump-ng is not functioning, it cannot detect your card or you get the blue screen of death, review the instructions for installing the software and drivers. If you cannot identify the problem, redo everything from scratch. Also check the this tutorial for ideas.

Airodump-ng Bluescreen

Airodump-ng or any “user space” program cannot produce a bluescreen, it is the driver which is the root cause. In most cases, these bluescreen failures cannot be resolved since these drivers are closed source.

Interaction

Since revision r1648, airodump-ng can receive and interpret key strokes while running. The following list describes the currently assigned keys and supposed actions.

- [a]: Select active areas by cycling through these display options: AP+STA; AP+STA+ACK; AP only; STA only
- [d]: Reset sorting to defaults (Power)
- [i]: Invert sorting algorithm
- [m]: Mark the selected AP or cycle through different colors if the selected AP is already marked
- [r]: (De-)Activate realtime sorting - applies sorting algorithm everytime the display will be redrawn
- [s]: Change column to sort by, which currently includes: First seen; BSSID; PWR level; Beacons; Data packets; Packet rate; Channel; Max. data rate; Encryption; Strongest Ciphersuite; Strongest Authentication; ESSID
- [SPACE]: Pause display redrawing/ Resume redrawing
- [TAB]: Enable/Disable scrolling through AP list
- [UP]: Select the AP prior to the currently marked AP in the displayed list if available
- [DOWN]: Select the AP after the currently marked AP if available

If an AP is selected or marked, all the connected stations will also be selected or marked with the same color as the corresponding Access Point.

airodump-ng.txt · Last modified: 2020/01/26 01:07 by mister_x