NAME

aireplay-ng - inject packets into a wireless network to generate traffic

SYNOPSIS

aireplay-ng [options] <replay interface>

DESCRIPTION

aireplay-ng is used to inject/replay frames. The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys. There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection. With the packetforge-ng tool it's possible to create arbitrary frames.

aireplay-ng supports single-NIC injection/monitor.

This feature needs driver patching.

OPTIONS

-H, --help
Shows the help screen.

Filter options:

-b <bssid>
MAC address of access point.

-d <dmac>
MAC address of destination.

-s <smac>
MAC address of source.

-m <len>
Minimum packet length.

-n <len>
Maximum packet length.

-u <type>
Frame control, type field.

-v <subt>
Frame control, subtype field.

-t <tods>
Frame control, "To" DS bit (0 or 1).

-f <fromds>
Frame control, "From" DS bit (0 or 1).

-w <iswep>
Frame control, WEP bit (0 or 1).

-D Disable AP Detection.

Replay options:

-x <nbpps>
Number of packets per second.

-p <fctrl>
Set frame control word (hex).

-a <bssid>
Set Access Point MAC address.

-c <dmac>
Set destination MAC address.

-h <smac>
Set source MAC address.

-g <nb_packets>
Change ring buffer size (default: 8 packets). The minimum is 1.

-F Choose first matching packet.

-e <essid>
Fake Authentication attack: Set target SSID (see below). For SSID containing special characters, see https://www.aircrack-ng.org/doku.php?id=faq#how_to_use_spaces_double_quote_and_single_quote_etc_in_ap_names

-o <npackets>
Fake Authentication attack: Set the number of packets for every authentication and association attempt (Default: 1). 0 means auto

-q <seconds>
Fake Authentication attack: Set the time between keep-alive packets in fake authentication mode.

-Q Fake Authentication attack: Sends reassociation requests instead of performing a complete authentication and association after each delay period.

-y <prga>
Fake Authentication attack: Specifies the keystream file for fake shared key authentication.

-T n Fake Authentication attack: Exit if fake authentication fails 'n' time(s).

-j ARP Replay attack : inject FromDS packets (see below).

-k <IP>
Fragmentation attack: Set destination IP in fragments.

-l <IP>
Fragmentation attack: Set source IP in fragments.

-B Test option: bitrate test.

Source options:

-i <iface>
Capture packets from this interface.

-r <file>
Extract packets from this pcap file.

Miscellaneous options:

-R disable /dev/rtc usage.

--ignore-negative-one if the interface's channel can't be determined ignore the mismatch, needed for unpatched cfg80211

--deauth-rc <rc>, -Z <rc> Provide a reason code when doing deauthication (between 0 and 255). By default, 7 is used: Class 3 frame received from unassociated STA. 0 is a reserved value. Reason codes explanations can be found in the IEEE802.11 standard or in https://mrncciew.com/2014/10/11/802-11-mgmt-deauth-disassociation-frames/

Attack modes:

-0 <count>, --deauth=<count>
This attack sends deauthentication packets to one or more clients which are currently associated with a particular access point. Deauthenticating clients can be done for a number of reasons: Recovering a hidden ESSID. This is an ESSID which is not being broadcast. Another term for this is "cloaked" or Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate or Generate

ARP requests (Windows clients sometimes flush their ARP cache when disconnected). Of course, this attack is totally useless if there are no associated wireless client or on fake authentications.

-1 <delay>, --fakeauth=<delay>

The fake authentication attack allows you to perform the two types of WEP authentication (Open System and Shared Key) plus associate with the access point (AP). This is only useful when you need an associated MAC address in various aireplay-ng attacks and there is currently no associated client. It should be noted that the fake authentication attack does NOT generate any ARP packets. Fake authentication cannot be used to authenticate/associate with WPA/WPA2 Access Points.

-2, --interactive

This attack allows you to choose a specific packet for replaying (injecting). The attack can obtain packets to replay from two sources. The first being a live flow of packets from your wireless card. The second being from a pcap file. Reading from a file is an often overlooked feature of aireplay-ng. This allows you read packets from other capture sessions or quite often, various attacks generate pcap files for easy reuse. A common use of reading a file containing a packet your created with packetforge-ng.

-3, --arpreplay

The classic ARP request replay attack is the most effective way to generate new initialization vectors (IVs), and works very reliably. The program listens for an ARP packet then retransmits it back to the access point. This, in turn, causes the access point to repeat the ARP packet with a new IV. The program retransmits the same ARP packet over and over. However, each ARP packet repeated by the access point has a new IVs. It is all these new IVs which allow you to determine the WEP key.

-4, --chopchop

This attack, when successful, can decrypt a WEP data packet without knowing the key. It can even work against dynamic WEP. This attack does not recover the WEP key itself, but merely reveals the plaintext. However, some access points are not vulnerable to this attack. Some may seem vulnerable at first but actually drop data packets shorter than 60 bytes. If the access point drops packets shorter than 42 bytes, aireplay-ng tries to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet.

-5, --fragment

This attack, when successful, can obtain 1500 bytes of PRGA (pseudo random generation algorithm). This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with packetforge-ng which are in turn used for various injection attacks. It requires at least one data packet to be received from the access point in order to initiate the attack.

-6, --caffe-latte

In general, for an attack to work, the attacker has to be in the range of an AP and a connected client (fake or real). Caffe Latte attacks allows one to gather enough packets to crack a WEP key without the need of an AP, it just need a client to be in range.

-7, --cfrag

This attack turns IP or ARP packets from a client into ARP request against the client. This attack works especially well against ad-hoc networks. As well it can be used against softAP clients and normal AP clients.

-8, --migmode

This attack works against Cisco Aironet access points configured in WPA Migration Mode, which enables both WPA and WEP clients to associate to an access point using the same Service Set Identifier (SSID). The program listens for a WEP-encapsulated broadcast ARP packet, bitflips it to make it into an ARP coming from the attacker's MAC address and retransmits it to the access point. This, in turn, causes the access point to repeat the ARP packet with a new IV and also to forward the ARP reply to the attacker with a new IV. The program retransmits the same ARP packet over and over. However, each ARP packet repeated by the access point has a new IV as does the ARP reply forwarded to the attacker by the access point. It is all these new IVs which allow you to determine the WEP key.

-9, --test

Tests injection and quality.

FRAGMENTATION VERSUS CHOPCHOP

Fragmentation:

Pros
- Can obtain the full packet length of 1500 bytes XOR. This means you can subsequently pretty well create any size of packet.
- May work where chopchop does not
- Is extremely fast. It yields the XOR stream extremely quickly when successful.

Cons
- Setup to execute the attack is more subject to the device drivers. For example, Atheros does not generate the correct packets unless the wireless card is set to the mac address you are spoofing.
- You need to be physically closer to the access point since if any packets are lost then the attack fails.

Chopchop

Pro
- May work where frag does not work.

Cons
- Cannot be used against every access point.
- The maximum XOR bits is limited to the length of the packet you chopchop against.
- Much slower then the fragmentation attack.

AUTHOR

This manual page was written by Adam Cecile <gandalf@le-vert.net> for the Debian system (but may be used by others).

SEE ALSO

airbase-ng(8)
airmon-ng(8)
airodump-ng(8)
airodump-ng-oui-update(8)
airserv-ng(8)
airtun-ng(8)
besside-ng(8)
easside-ng(8)
tkiptun-ng(8)
wesside-ng(8)
aircrack-ng(1)
airdecap-ng(1)
airdecloak-ng(1)
airolib-ng(1)
besside-ng-crawler(1)
buddy-ng(1)
ivstools(1)
kstats(1)

makeivs-ng(1)
packetforge-ng(1)
wpaclean(1)
airventriloquist(8)