

Airbase-ng

Usage: airbase-ng <op tions> <replay interf ace>

Syntax	Parameters	Description
-a	<i>bssid</i>	set Access Point MAC address
-i	<i>iface</i>	capture packets from this interface
-w	<i>WEP key</i>	use this WEP key to encrypt/decrypt packets
-W	<i>0/1</i>	[don't] set WEP flag in beacons 0 1 (default: auto)
-h	<i>MAC</i>	source mac for MITM mode
-f	<i>disallow</i>	disallow specified client MACs (default: allow)
-q	<i>none</i>	quiet (do not print statistics)
-v	<i>none</i>	verbose (print more messages) (long --verbose)
-M	<i>none</i>	M-I-T-M between [specified] clients and bssids
-A	<i>none</i>	Ad-Hoc Mode (allows other clients to peer) (long --ad-hoc)
-Y	<i>in/out/both</i>	external packet processing
-c	<i>channel</i>	sets the channel the AP is running on
-X	<i>none</i>	hidden ESSID (long --hidden)
-s	<i>none</i>	force shared key authentication
-S	<i>none</i>	set shared key challenge length (default: 128)
-L	<i>none</i>	Caffe-Latte attack (long --caffe-latte)
-N	<i>none</i>	Hirte attack (cfrag attack), creates arp request against wep client (long -cfrag)
-x	<i>nbpps</i>	number of packets per second (default: 100)
-y	<i>none</i>	disables responses to broadcast probes
-0	<i>none</i>	set all WPA,WEP,open tags. can't be used with -z & -Z

Airbase-ng (cont)

-z	<i>type</i>	sets WPA1 tags. 1=WEP40 2=TKIP 3=WRAP 4=CCMP 5=WEP104
-Z	<i>type</i>	same as -z, but for WPA2
-V type	<i>type</i>	fake EAPOL 1=MD5 2=SHA1 3=auto
-F	<i>prefix</i>	write all sent and received frames into pcap file
-P	<i>none</i>	respond to all probes, even when specifying ESSIDs
-I	<i>interval</i>	sets the beacon interval value in ms
-C	<i>seconds</i>	enables beaconing of probed ESSID values (requires -P)

Filter Options

Syntax	Parameters	Description
--bssids	<i><file></i>	read a list of BSSIDs out of that file (short -B)
--bssid	<i><MAC></i>	BSSID to filter/use (short -b)
--client	<i><MAC></i>	MAC of client to accept (short -d)
--clients	<i><file></i>	read a list of MACs out of that file (short -D)
--essid	<i><ESSID></i>	specify a single ESSID (short -e)
--essids	<i><file></i>	read a list of ESSIDs out of that file (short -E)

Airdecloak-ng

Usage: airdecloak-ng [options]

Syntax	Parameter	Description
-i	<i>input file</i>	Path to the capture file
-bssid	<i>BSSID</i>	BSSID of the network to filter.
-ssid	<i>ESSID</i>	ESSID of the network to filter (not yet implemented).
-filters	<i>filters</i>	Apply theses filters in this specific order. They have to be separated by a ','.
-null--	<i>none</i>	Assume that null packets can be cloaked (not yet implemented).



Airdecloak-ng (cont)

<code>-disable--base_filter</code>	<i>none</i>	Disable the base filter.
<code>-drop-frag</code>	<i>none</i>	Drop all fragmented packets. In most networks, fragmentation is not needed.

Airdrop-ng

Usage: airdrop-ng [options] <pcap file>

Syntax	Parameter	Description
<code>-i</code>	<i>card</i>	Wireless card in monitor mode to inject from
<code>-t</code>	<i>csv file</i>	Airodump txt file in CSV format NOT the pcap
<code>-p</code>	<i>psyco</i>	Disable the use of Psyco JIT
<code>-r</code>	<i>Rule File</i>	Rule File for matched deauths
<code>-u</code>	<i>update</i>	Updates OUI list
<code>-d</code>	<i>Driver</i>	Injection driver. Default is mac80211
<code>-s</code>	<i>sleep</i>	Time to sleep between sending each packet
<code>-b</code>	<i>debug</i>	Turn on Rule Debugging
<code>-l</code>	<i>key</i>	Enable Logging to a file, if file path not provided airdrop will log to default location
<code>-n</code>	<i>nap</i>	Time to sleep between loops

Airdecap-ng

Usage: airdecap-ng [options] <pcap file>

Syntax	Parameter	Description
<code>-l</code>	<i>none</i>	don't remove the 802.11 header
<code>-b</code>	<i>bssid</i>	access point MAC address filter
<code>-k</code>	<i>pmk</i>	WPA/WPA2 Pairwise Master Key in hex
<code>-e</code>	<i>essid</i>	target network ascii identifier
<code>-p</code>	<i>pass</i>	target network WPA/WPA2 passphrase
<code>-w</code>	<i>key</i>	target network WEP key in hexadecimal

Airgraph-ng

Usage: python airgraph-ng -i [airodump file e.txt] -c [APR OR CPG]

Syntax	Description
<code>-i</code>	Input File
<code>-o</code>	Output File
<code>-g</code>	Graph Type [CAPR (Client to AP Relationship) OR CPG (Client to Graph)]
<code>-a</code>	Print the about
<code>-h</code>	Print this help

Aircrack-ng

Usage: aircrack-ng [options] <capture file(s)>

Syntax	Parameter	Description
<code>-a</code>	<i>amode</i>	Force attack mode (1 = static WEP, 2 = WPA/WPA2-PSK)
<code>-b</code>	<i>bssid</i>	Long version - bssid. Select the target network based on the access point's MAC address.
<code>-e</code>	<i>essid</i>	If set, all IVs from networks with the same ESSID will be used. This option is also required for WPA/WPA2-PSK cracking if the ESSID is not broadcasted (hidden).
<code>-p</code>	<i>nbcpu</i>	On SMP systems: # of CPU to use. This option is invalid on non-SMP systems
<code>-q</code>	<i>none</i>	Enable quiet mode (no status output until the key is found, or not)
<code>-c</code>	<i>none</i>	(WEP cracking) Restrict the search space to alpha-numeric characters only (0x20 - 0x7F)
<code>-t</code>	<i>none</i>	(WEP cracking) Restrict the search space to binary coded decimal hex characters
<code>-h</code>	<i>none</i>	(WEP cracking) Restrict the search space to numeric characters (0x30-0x39) These keys are used by default in most Fritz!BOXes
<code>-d</code>	<i>start</i>	(WEP cracking) Long version -debug. Set the beginning of the WEP key (in hex), for debugging purposes.



Aircrack-ng (cont)		
-m	<i>maddr</i>	(WEP cracking) MAC address to filter WEP data packets. Alternatively, specify -m ff:ff:ff:ff:ff:ff to use all and every IVs, regardless of the network.
-M	<i>number</i>	(WEP cracking) Sets the maximum number of ivs to use.
-n	<i>nbits</i>	(WEP cracking) Specify the length of the key: 64 for 40-bit WEP, 128 for 104-bit WEP, etc. The default value is 128.
-i	<i>index</i>	(WEP cracking) Only keep the IVs that have this key index (1 to 4). The default behaviour is to ignore the key index.
-f	<i>fudge</i>	(WEP cracking) By default, this parameter is set to 2 for 104-bit WEP and to 5 for 40-bit WEP. Specify a higher value to increase the bruteforce level: cracking will take more time, but with a higher likelihood of success.
-H	<i>none</i>	Long version - -help. Output help information.
-l	<i>file name</i>	(Lowercase L, ell) logs the key to the file specified.
-K	<i>none</i>	Invokes the Korek WEP cracking method. (Default in v0.x)
-k	<i>korek</i>	(WEP cracking) There are 17 korek statistical attacks. Sometimes one attack creates a huge false positive that prevents the key from being found, even with lots of IVs. Try -k 1, -k 2, ... -k 17 to disable each attack selectively.
-p	<i>threads</i>	Allow the number of threads for cracking even if you have a non-SMP computer.
-r	<i>database</i>	Utilizes a database generated by airolib-ng as input to determine the WPA key. Outputs an error message if aircrack-ng has not been compiled with sqlite support.
-x / -x0	<i>none</i>	(WEP cracking) Disable last keybytes brutforce.

Aircrack-ng (cont)		
-x1	<i>none</i>	(WEP cracking) Enable last keybyte bruteforcing (default).
-x2	<i>none</i>	(WEP cracking) Enable last two keybytes bruteforcing.
-X	<i>none</i>	(WEP cracking) Disable bruteforce multithreading (SMP only).
-y	<i>none</i>	(WEP cracking) Experimental single bruteforce attack which should only be used when the standard attack mode fails with more than one million IVs
-u	<i>none</i>	Long form - -cpu-detect. Provide information on the number of CPUs and MMX support. Example responses to "aircrack-ng -cpu-detect" are "Nb CPU detected: 2" or "Nb CPU detected: 1 (MMX available)".
-w	<i>words</i>	(WPA cracking) Path to a wordlist or "-" without the quotes for standard in (stdin).
-z	<i>none</i>	Invokes the PTW WEP cracking method. (Default in v1.x)
-P	<i>none</i>	Long version - -ptw-debug. Invokes the PTW debug mode.
-C	<i>MACs</i>	Long version - -combine. Merge the given APs to a virtual one.
-D	<i>none</i>	Long version - -wep-decloak. Run in WEP decloak mode.
-V	<i>none</i>	Long version - -visual-inspection. Run in visual inspection mode.
-l	<i>none</i>	Long version - -oneshot. Run in oneshot mode.
-S	<i>none</i>	WPA cracking speed test.
-s	<i>none</i>	Show the key in ASCII while cracking
-E	<i>file></i>	(WPA cracking) Create EWSA Project file v3
-J	<i>file</i>	(WPA cracking) Create Hashcat Capture file



Aireplay-ng

Usage: aireplay-ng <options> <replay interface>

Filter Options

Syntax	Parameters	Description
-b	bssid	MAC address, Access Point
-d	dmac	MAC address, Destination
-s	smac	MAC address, 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
-f	fromds	frame control, From DS bit
-w	iswep	frame control, WEP bit

Replay Options

Syntax	Parameters	Description
-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
-e	essid	For fakeauth attack or injection test, it sets target AP SSID. This is optional when the SSID is not hidden.
-j	none	arp replay attack, inject FromDS pkts
-g	value	change ring buffer size (default: 8)
-k	IP	set destination IP in fragments
-l	IP	set source IP in fragments
-o	npckts	number of packets per burst (-1)
-q	sec	seconds between keep-alives (-1)
-y	prga	keystream for shared key auth
-B or -bittest	none	bit rate test (Applies only to test mode)

Aireplay-ng (cont)

-D	none	disables AP detection. Some modes will not proceed if the AP beacon is not heard. This disables this functionality.
-F or -fast	none	chooses first matching packet. For test mode, it just checks basic injection and skips all other tests.
-R	none	disables /dev/rpc usage. Some systems experience lockups or other problems with RTC. This disables the usage.

Source options

Syntax	Parameters	Description
iface	none	capture packets from this interface
-r	file	extract packets from this pcap file

Attack modes

Syntax	Parameters	Description
--deauth	count	deauthenticate 1 or all stations (-0)
--fakeauth	delay	fake authentication with AP (-1)
--interactiv	none	interactive frame selection (-2)
--arp replay	none	standard ARP-request replay (-3)
--chopchop	none	decrypt/chopchop WEP packet (-4)
--fragment	none	generates valid keystream (-5)
--test	none	injection test (-9)

