NAME

airuncloak-ng - Removes wep cloaked framed from a pcap file.

SYNOPSIS

airuncloak-ng <options>

DESCRIPTION

airuncloak-ng is a tool that removes wep cloaking from a pcap file. Some WIPS (actually one) can actively "prevent" cracking a WEP key by inserting chaff (fake wep frames) in the air to fool aircrack-ng. In some rare cases, cloaking fails and the key can be recovered without removing this chaff. In the cases where the key cannot be recovered, use this tool to filter out chaff.

The program works by reading the input file and selecting packets from a specific network. Each selected packet is put into a list and classified (default status is "unknown"). Filters are then applied (in the order specified by the user) on this list. They will change the status of the packets (unknown, uncloaked, potentially cloaked or cloaked). The order of the filters is really important since each filter will base its analysis amongst other things on the status of the packets and different orders will give different results.

Important requirement: The pcap file needs to have all packets (including beacons and all other "useless" packets) for the analysis (and if possible, prism/radiotap headers).

OPTIONS

-h, --help
Shows the help screen.

-i <file>
Path to the capture file.

--ssid <ESSID>
Essid of the network (not yet implemented) to filter.

--bssid <BSSID>
BSSID of the network to filter.

--null-packets
Assume that null packets can be cloaked.

--disable-base-filter
Do not apply base filter.

--drop-frag
Drop fragmented packets.

--filters <filters>
Apply different filters (separated by a comma). See below.

FILTERS

signal Try to filter based on signal (prism or radiotap headers in the pcap file).

duplicate_sn
Remove all duplicate sequence numbers for both the AP and the client (that are close to each other).

duplicate_sn_ap
Remove duplicate sequence number for the AP only (that are close to each other).

duplicate_sn_client
Remove duplicate sequence number for the client only (that are close to each other).

consecutive_sn
Filter based on the fact that IV should be consecutive (only for AP).

duplicate_iv
Filter out all duplicate IV.

signal_dup_consec_sn
Use signal (if available), duplicate and consecutive sequence number (filtering is much more precise than using all these filters one by one).

AUTHOR

This manual page was written by Thomas d'Otreppe.

SEE ALSO

airbase-ng(8)
aireplay-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)
airolib-ng(1)
besside-ng-crawler(1)
buddy-ng(1)
ivstools(1)
kstats(1)
makeivs-ng(1)
packetforge-ng(1)
wpaclean(1)
airventriloquist(8)