NAME

tkiptun-ng - inject a few frames into a WPA TKIP network with QoS

SYNOPSIS

tkiptun-ng [options] <replay interface>

DESCRIPTION

tkiptun-ng is a tool created by Martin Beck aka hirte, a member of aircrack-ng team. This tool is able to inject a few frames into a WPA TKIP network with QoS. He worked with Erik Tews (who created PTW attack) for a conference in PacSec 2008: "Gone in 900 Seconds, Some Crypto Issues with WPA".

OPERATION

-H, --help
Shows the help screen.

Filter options:

-d <dmac>
MAC address of destination.

-s <smac>
MAC address of source.

-m <len>
Minimum packet length.

-n <len>
Maximum packet length.

-t <tods>
Frame control, "To" DS bit.

-f <fromds>
Frame control, "From" DS bit.

-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.

-e <essid>
Set target SSID.

-M <sec>
MIC error timeout in seconds. Default: 60 seconds

Debug options:

-K <prga>
Keystream for continuation.

-y <file>
Keystream file for continuation.

-j Inject FromFS packets.

-P <PMK>
Pairwise Master key (PMK) for verification or vulnerability testing.

-p <PSK>
Preshared key (PSK) to calculate PMK with essid.

Source options:

-i <iface>
Capture packets from this interface.

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

AUTHOR

This manual page was written by Thomas d'Otreppe. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU General Public License, Version 2 or any later version published by the Free Software Foundation On Debian systems, the complete text of the GNU General Public License can be found in /usr/share/common-licenses/GPL.

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)
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)