NAME

easside-ng - an auto-magic tool which allows you to communicate via an WEP-encrypted AP without knowing the key

SYNOPSIS

easside-ng <options>

DESCRIPTION

easside-ng is an auto-magic tool which allows you to communicate via an WEP-encrypted access point (AP) without knowing the WEP key. It first identifies a network, then proceeds to associate with it, obtain PRGA (pseudo random generation algorithm) xor data, determine the network IP scheme and then setup a TAP interface so that you can communicate with the AP without requiring the WEP key. All this is done without your intervention.

OPTIONS

-h   Shows the help screen.

-v <victim mac>
Victim BSSID (Optional).

-m <src mac>
Source MAC address to be used (Optional).

-i <ip>   Source IP address to be used on the wireless LAN. Defaults to the decoded network plus '.123' (Optional).

-r <router ip>
IP address of the AP router. This could be the WAN IP of the AP or an actual router IP depending on the topology. Defaults to the decoded network plus '.1' (Optional).

-s <buddy ip>
IP address of Buddy-ng server (Mandatory)

-f <iface>
Wireless interface to use (Mandatory)

-c <channel>
Lock interface to this channel (Optional).

-n   Determine Internet IP only.

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)
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)