Reaver Cheat Sheet Cheat Sheet

by jlunz via cheatography.com/147470/cs/32070/

Required Arguments

-i, --interface=<wlan>	Name of the monitor-mode interface to use
-b, --bssid=<mac>	BSSID of the target AP

Optional Arguments

-m, --mac=<mac>	MAC of the host system
-e, --essid=<ssid>	ESSID of the target AP
-c, --channel=<channel>	Set the 802.11 channel for the interface (implies -f)
-o, --out-file=<file>	Send output to a log file [stdout]
-s, --session=<file>	Restore a previous session file
-C, --exec=<command>	Execute the supplied command upon successful pin recovery
-D, --daemonize	Daemonize reaver
-f, --fixed	Disable channel hopping
-5, --5ghz	Use 5GHz 802.11 channels
-v, --verbose	Display non-critical warnings (-vv or -vvv for more)
-q, --quiet	Only display critical messages
-h, --help	Show help

Advanced Options

-p, --pin=<wps pin>	Use the specified pin (may be arbitrary string or 4/8 digit WPS pin)
-d, --delay=<seconds>	Set the delay between pin attempts [1]
-l, --lock-delay=<seconds>	Set the time to wait if the AP locks WPS pin attempts [60]
-g, --max-attempts=<num>	Quit after num pin attempts
-x, --fail-wait=<seconds>	Set the time to sleep after 10 unexpected failures [0]
-r, --recurring-delay=<x:y>	Sleep for y seconds every x pin attempts
-t, --timeout=<seconds>	Set the receive timeout period [10]
-T, --m57-timeout=<seconds>	Set the M5/M7 timeout period [0.40]
-A, --no-associate	Do not associate with the AP (association must be done by another application)

Advanced Options (cont)

-N, --no-nacks	Do not send NACK messages when out of order packets are received
-S, --dh-small	Use small DH keys to improve crack speed
-L, --ignore--locks	Ignore locked state reported by the target AP
-E, --eap-terminate	Terminate each WPS session with an EAP FAIL packet
-n, --nack	Target AP always sends a NACK [Auto]
-w, --win7	Mimic a Windows 7 registrar [False]
-K, -Z, --pixie-dust	Run pixiedust attack

Reaver Examples

reaver -i <interface> -b <MAC>	Usually, the only required arguments to Reaver are the interface name and the BSSID of the target AP.
reaver -i <interface> -b <MAC> -vv	It is suggested that you run Reaver in verbose mode in order to get more detailed information about the attack as it progresses.
reaver -i <interface> -b <MAC> -c <channel> -e <essid>	The channel and SSID (provided that the SSID is not cloaked) of the target AP will be automatically identified by Reaver, unless explicitly specified on the command line.
reaver -i <interface> -b <MAC> --dh-small	Since version 1.3, Reaver implements the small DH key optimization which can speed up the attack speed.
reaver -i <interface> -b <MAC> --fixed	By default, if the AP switches channels, Reaver will also change its channel accordingly. However, this feature may be disabled by fixing the interface's channel.

Reaver Examples (cont)

reaver -i <interface> -b <MAC> --mac=<spoofed MAC>	When spoofing your MAC address, you must set the desired address to spoof using the ifconfig utility, and additionally tell Reaver what the spoofed address is.
reaver -i <interface> -b <MAC> -t <sec>	The default receive timeout period is 5 seconds. This timeout period can be set manually if necessary (minimum timeout period is 1 second).
reaver -i <interface> -b <MAC> -d <sec>	The default delay period between pin attempts is 1 second. This value can be increased or decreased to any non-negative integer value. A value of zero means no delay.
reaver -i <interface> -b <MAC> --lock-delay=<sec>	Some APs will temporarily lock their WPS state, typically for five minutes or less, when "suspicious" activity is detected. By default when a locked state is detected, Reaver will check the state every 315 seconds (5 minutes and 15 seconds) and not continue brute forcing pins until the WPS state is unlocked. This check can be increased or decreased to any non-negative integer value.
reaver -i <interface> -b <MAC> -T <sec, .2-1sec>	The default timeout period for receiving the M5 and M7 WPS response messages is .1 seconds. This timeout period can be set manually if necessary (max timeout period is 1 second).

Reaver Examples (cont)

reaver -i <interface> -b <MAC> --fail-wait=<sec>	sending an EAP FAIL message to close out a WPS session is sometimes necessary. By default this feature is disabled, but can be enabled for those APs that need it. When 10 consecutive unexpected WPS errors are encountered, a warning message will be displayed. Since this may be a sign that the AP is rate limiting pin attempts or simply being overloaded, a sleep can be put in place that will occur whenever these warning messages appear.