

Forum:[Hack Forums](#)

Thread: [WPS pin bruteforce attack with reaver/bully ISSUE](#)

LSDtoSeeHD - September 11, 2019, 6:22 am

Hello there people,

I recently tried to crack some WPA2/PSK, with WPS pin technique.

I used reaver and tried bully too.

I found some WPS pins in some Access Points that i attacked, but that happened thanks to pixie wps.

When pixie fails to find the wps pin, the only way is to bruteforce thos 11.000 combinations of numbers that WPS pin could be.

and here is my problem, when i launch the attack using either reaver or bully i got TIMEOUT warnings.

To be more specific, sometimes reaver "stuck" on trying the same pin over and over again (the 1st pin, never tried a 2nd one)

and some other times i get

```
=====
[+] Trying pin 12345670.           // this pin is the only one it tries
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
=====
```

and this continues until i force it to stop.

Clues that may help:

WPS is enabled but its a WPS 2.0 (not 1.0... the wps pins i managed to find was 1.0)

My wireless card is capable of sending injection packets

The power of Access point is about -50 (i guess is close enough)

The command i use " reaver -i wlan0mon -b (xx:xx:xx:xx:xx) - N -c (the channel) -vv

Any help or suggestion would be appreciated , thanks in advance !!!

pasnger57 - September 11, 2019, 7:19 am

give up on wps pin attack Most if not all routers now will Lock OUT the wps pin from use whit 3 failed attempts

it has not Ben a thing sens 2012

w1l5t3r - September 15, 2019, 6:32 am

(Sep 11, 2019 06:22 AM)LSDtoSeeHD Wrote: [\[CITE\]](#) Hello there people,

I recently tried to crack some WPA2/PSK, with WPS pin technique.

I used reaver and tried bully too.

I found some WPS pins in some Access Points that i attacked, but that happened thanks to pixie wps.

When pixie fails to find the wps pin, the only way is to bruteforce thos 11.000 combinations of numbers that WPS pin could be.

and here is my problem, when i launch the attack using either reaver or bully i got TIMEOUT warnings.

To be more specific, sometimes reaver "stuck" on trying the same pin over and over again (the 1st pin, never tried a 2nd one)

and some other times i get

```
=====
[+] Trying pin 12345670.           // this pin is the only one it tries
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
=====
```

and this continues until i force it to stop.

Clues that may help:

WPS is enabled but its a WPS 2.0 (not 1.0... the wps pins i managed to find was 1.0)

My wireless card is capable of sending injection packets

The power of Access point is about -50 (i guess is close enough)

The command i use " reaver -i wlan0mon -b (xx:xx:xx:xx:xx) - N -c (the channel) -vv

Any help or suggestion would be appreciated , thanks in advance !!!

Get yourself a powerful wifi adapter and kali linux

deauth the target network you want password for, kicking everyone off

set up a fake router upgrade page (should tell you make of router when doing a scan)

kick the victim router down and clone the name if the SSID

the victims log on (open wifi) and presented with a router upgrade page

once they enter passphrase it will disconnect and put them back on their own network

you now have the password to join their network