

Forum:[Hack Forums](#)

Thread: [help: recovering passphrase using wps pin](#)

zuesein - July 24, 2014, 9:39 pm

hi guys! i need help recovering the password of the router using wps pin.. here are the codes i type in the terminal...

```
reaver -i mon0 -b bssid -c channel -pin=12345678 -vv
reaver -i mon0 -b bssid -p wps
reaver -i mon0 -p12345678 -b bssid
```

i tried it many times. i used two tools . backtracks ang minidwep but same error found.. warning associate etc..

my wps pin is right..because i hack it again the target router.and wps pin is the same. only the passphrase is change..
please help.. thanks

MirrorDude - July 24, 2014, 10:07 pm

You need a space between the 'p' and the pin...

Try this...

PHP Code

```
<?php
```

```
reaver -i mon0 -b bssid -c channel -p 12345678 -vv
```

zuesein - July 25, 2014, 6:45 am

(Jul 24, 2014 10:07 PM)MirrorDude Wrote: [\[CITE\]](#) You need a space between the 'p' and the pin...

Try this...

PHP Code

```
<?php
```

```
reaver -i mon0 -b bssid -c channel -p 12345678 -vv
```

i also tried that code sir.. failed to associate etc..
or cannot recover mac something like that.

ciocan - July 25, 2014, 7:36 am

I suppose that you replace bssid with real mac from target and channel with number of the channel?
You may skip using -c option.

Also check signal level and rxq, try to spoof a client mac address.

zuesein - July 25, 2014, 6:43 pm

(Jul 25, 2014 07:36 AM)ciocan Wrote: [\[CITE\]](#) I suppose that you replace bssid with real mac from target and channel with number of the channel? You may skip using -c option.

Also check signal level and rxq, try to spoof a client mac address.

hi sir. real mac ? isnt that real mac i search in wash -i mon0?

like for example

11:22:33:44:55:66

tenda

this is very hard.. when the neighbor change the passphrase. insted of recovering the pass using wps.. i start over again to pin the router.. it take me 5hrs to hack again..

(Jul 25, 2014 06:43 PM)zuesein Wrote: [\[CITE\]](#) hi sir. real mac ? isnt that real mac i search in wash -i mon0?

like for example

11:22:33:44:55:66

tenda

this is very hard.. when the neighbor change the passphrase. insted of recovering the pass using wps.. i start over again to pin the router.. it take me 5hrs to hack again..

sir . what code should i type in the terminal? i will try it

up up and away ,:) :)

up up up up up up wake up wake up :) lol

SW4T - July 26, 2014, 8:04 pm

Code to change mac

Code ifconfig mon0 down

macchanger --mac 12:12:12:12:12:12 mon0

ifconfig mon0 up

If you are getting failed to associate you might need to get closer to the router for a stronger signal.

zuesein - July 26, 2014, 10:51 pm

(Jul 26, 2014 08:04 PM)InfSec Wrote: [\[CITE\]](#) Code to change mac

Code ifconfig mon0 down

macchanger --mac 12:12:12:12:12:12 mon0

ifconfig mon0 up

If you are getting failed to associate you might need to get closer to the router for a stronger signal.

hmmp.. i dont think the signal is the problem. because when i try to pin using reaver on minidwep.. its working pin the router. no associate etc.. just trying pin.. the problem is so long to hack again. so i want to shortcut the process because i have the wps pin ..

do you think guys the signals is the issue???? but why reaver can successful pin the router .. only this code to recover passphrase using wps pin is the problem???

Kara Davis - July 27, 2014, 12:45 am

Hi, this only happens against this particular AP? Can you post your reaver output?

zuesein - July 27, 2014, 3:22 am

(Jul 27, 2014 12:45 AM)Kara Davis Wrote: [\[CITE\]](#) Hi, this only happens against this particular AP? Can you post your reaver output?

hi sir , i tried it in two AP i already hack.. same message.. error mon0 or associate mac.. failed to .. i forgot the warning message.. sir iam using live cd.. i dont know how to copy the reaver output.. newbie :)

sir you know Minidwep-gtk? its a tool for wireless.. i used the builtin reaver and its work fine.. but its start pin from the start..so its takelong again to reveal the password..
sorry to my english bro ... godbless thanks

ciocan - July 27, 2014, 8:35 am

So you make some mistakes because you dont read to much.

When you use reaver is not necessary to change (spoof) your mac. It is need only when ap has mac address filtering.

Here are the steps:

1. start mon0

airmon-ng start wlan0

2. scan for networks (ap's)

airodump-ng mon0

3. scan just a network (your target)

airodump-ng mon0 -c (ap channel) --bssid (ap mac)

All this info you can get it from step 2.

4. run reaver

reaver -i mon0 -b (ap mac) -vv -c (channel number) -p (pin)

-c option is not necessary but will help reaver dont scan himself for channel.

-p option is used only is you know the pin

This are basics for reaver. More advance option can be use but only if you are known for what are used and when.

When you run reaver it is recommended to have another open window with step 3. So basically you need to open 2 command line windows. One with airodump and one with reaver.

Any more questions?

And post your output or screenshots to help you with more exact info.

zuesein - July 27, 2014, 4:06 pm

(Jul 27, 2014 08:35 AM)ciocan Wrote: [\[CITE\]](#) So you make some mistakes because you dont read to much.

When you use reaver is not necessary to change (spoof) your mac. It is need only when ap has mac address filtering.

Here are the steps:

1. start mon0

airmon-ng start wlan0

2. scan for networks (ap's)

airodump-ng mon0

3. scan just a network (your target)

airodump-ng mon0 -c (ap channel) --bssid (ap mac)

All this info you can get it from step 2.

4. run reaver

reaver -i mon0 -b (ap mac) -vv -c (channel number) -p (pin)

-c option is not necessary but will help reaver dont scan himself for channel.

-p option is used only is you know the pin

This are basics for reaver. More advance option can be use but only if you are known for what are used and when.

When you run reaver it is recommended to have another open window with step 3. So basically you need to open 2 command line windows. One with airodump and one with reaver.

Any more questions?

And post your output or screenshots to help you with more exact info.

sir, i type that code when iam using backtracks...and same error.. anyway sir i try your new code.. and thanks for your time to read my tread.. godbless you.. iwill post my result later sir.. thanks again

ciocan sir million thanks to you !!!.... its work perfect.. 4seconds and the password is reavel.. im so happy...

thanks hack forum .:)