

Forum:[Hack Forums](#)

Thread: [Is cracking WPS password with Reaver still posible](#)

Dax - July 28, 2018, 6:30 am

I've done this a long time ago with reaver. I think it was 2013. when the routers were relatively old (like from 2011. and older When they didn't patch the method for using reaver to hack WPS pin and then to obtain WPA/WPA2 password)

When I last tried, the router gets locked (timeout) because of the bruteforce multiple attempts.

Q1: Is there any way to bypass this?

Q2: Whats the best method atm?

DopplerAF - July 28, 2018, 6:47 am

Yes WPS attack still is effective unless you didn't get blocked by router for bruteforce. There is no way that I know of to bypass getting locked except adding cooldown after each try. Cooldown time can vary from router to router. Personally I think there have been no such major development in hacking wifi passwords.

I might be wrong because last time I did anything router related was back in 2015 or something. Please correct me if you find something interesting.

EDIT: I just remembered there was a method introduce to avoid getting blocked by router. In that method after every several PIN tries MAC address was changed so the router will think it as different client.

Dax - July 28, 2018, 9:04 am

(Jul 28, 2018 06:47 AM)DopplerAF Wrote: [\[CITE\]](#) Yes WPS attack still is effective unless you didn't get blocked by router for bruteforce. There is no way that I know of to bypass getting locked except adding cooldown after each try. Cooldown time can vary from router to router. Personally I think there have been no such major development in hacking wifi passwords.

I might be wrong because last time I did anything router related was back in 2015 or something. Please correct me if you find something interesting.

EDIT: I just remembered there was a method introduce to avoid getting blocked by router. In that method after every several PIN tries MAC address was changed so the router will think it as different client.

Heard about the delaying tries. But that could take for ever to crack+ every router has it's own algoritm for blocking the attack. Haven't heard that for changing mac addresses but I guess that you get the same results as the previous method.

Ps.. Installing BT atm. Gonna try all the AP :P

DopplerAF - July 28, 2018, 10:29 am

(Jul 28, 2018 09:04 AM)Mr. damca Wrote: [\[CITE\]](#) Heard about the delaying tries. But that could take for ever to crack+ every router has it's own algoritm for blocking the attack. Haven't heard that for changing mac addresses but I guess that you get the same results as the previous method.

Ps.. Installing BT atm. Gonna try all the AP :P

Well it is definitely much faster than brute forcing WPA/WPA-2.

Good luck.

kayla_90 - July 28, 2018, 8:30 pm

look up Fluxion,is pretty good

Reaper_one - July 29, 2018, 1:56 am

Yes. I find it one of the most effective methods of wifi hacking.Many times if reaver doesnt work bully has a chance to work.

ampamer - December 31, 2018, 9:19 pm

no because most routers get locked

doomlod - January 1, 2019, 9:55 pm

not anymore, new routers generate uncrackable random pins ,try your luck, try pmkid with custom worldlist

noevil223 - January 2, 2019, 8:28 pm

Good to know reaver really changed the wifi cracking game considering all new routers got wps.. 0.0

CheckMyNuts - January 9, 2019, 5:54 am

I have the same question, can someone help?

Dax - January 9, 2019, 10:06 am

(Jan 9, 2019 06:54 AM)reksai33 Wrote: [\[CITE\]](#) I have the same question, can someone help?

Reaver method is pathed. All routers that were made after 2011 are patched. You have below 1% of success. Closing this thread now.