

Forum:[Hack Forums](#)

Thread: [Is Reaver Just Plain Wanky?](#)

TheDovahkiin909 - December 18, 2013, 7:00 pm

This is actually my first time cracking an AP, so please be patient.

So I notice that with Reaver, you can't really just lay back and watch. Though I'm already at 8.50%, I get error messages (0x02, 0x03, and 0x04) all the time, and it will normally get stuck somewhere and I will have to start it over again. I've experimented with the settings, and added a few delays, but what gives?

Is Reaver just unreliable?

Also, the signal is between 50 and 90.

Rogers Communications - December 18, 2013, 7:06 pm

reaver does occasionally work, but yes it is... umm unstable in my opinion!

I only use it as last resort

r00tuuu123 - December 18, 2013, 8:08 pm

(Dec 18, 2013 08:06 PM)wpginterceptor Wrote: [\[CITE\]](#) reaver does occasionally work, but yes it is... umm unstable in my opinion!

I only use it as last resort. Reaver works like 90% of the time it is not unstable by any means. Some wps open routers are just harder to crack than others it may take 30:00 or 3 days just depends on the router and the signal. To use reaver as a last resort is ridiculous that should be your first option considering a dictionary or a brute force attack is gonna take way longer. Even sniffing the password is going to involve some time to gain trust..

Rogers Communications - December 18, 2013, 9:33 pm

well, ive used reaver 30 times, and out of 30, ive cracked 2! and they were a pain in the ass, had to babysit the program ;(

anyways just my opinion

ciocan - December 19, 2013, 3:30 am

(Dec 18, 2013 08:00 PM)TheDovahkiin909 Wrote: [\[CITE\]](#) Also, the signal is between 50 and 90.

If the signal fluctuates so much you are wasting your time. This is why you have so many errors and eventually when the pin and psk are cracked you will have a big surprise... The connection on that ap will not be stable, lots of disconnect and low transfer rate. All this in case the you manage to connect...

Find another one with a stable signal and good rxq (quality of signal). If rxq is below 80 then is not worth to try.

Gunz_kruunG - December 19, 2013, 7:06 am

(Dec 18, 2013 08:00 PM)TheDovahkiin909 Wrote: [\[CITE\]](#) This is actually my first time cracking an AP, so please be patient.

So I notice that with Reaver, you can't really just lay back and watch. Though I'm already at 8.50%, I get error messages (0x02, 0x03, and 0x04) all the time, and it will normally get stuck somewhere and I will have to start it over again. I've experimented with the settings, and added a few delays, but what gives?

Is Reaver just unreliable?

Also, the signal is between 50 and 90.

I think you should back up your reaver works "ctrl+c" [save it before error occurred] then locate it at /usr/local/etc/reaver/ copy it to usb pendrive then when you want to continue your reaver again just put it back there.. it would continued your session before, and it would help you a lot rather than restart the whole session again because of the error ?

That error would happen if you gave "a lot of kept changing command" in 1 time.. had happen to me ? then the router's would not associated with my "nic" although i spoof my mac address and shown that the router's not locked but after a few days i can give a tried again but on that timed i just stick with my command without keep changing it and poof i successfully retrieve the wps pin and the wpa password ? The delays are used for delaying the reaver to proceed it pins because some router's would locked itself after several pins are been attempted..?

and the other things is, how come your signal like that it really are unstable 50-90 what your real view in that? because i would never ever had been associated or visible to me to get an "ap" that above -80 and if the signal is -75 to -77 it already hard or no hope to associated with the router's .?

TheDovahkiin909 - December 19, 2013, 3:58 pm

(Dec 19, 2013 08:06 AM)Gunz_kruunG Wrote: [\[CITE\]](#) The delays are used for delaying the reaver to proceed it pins because some router's would locked itself after several pins are been attempted..?

and the other things is, how come your signal like that it really are unstable 50-90 what your real view in that? because i would never ever had been associated or visible to me to get an "ap" that above -80 and if the signal is -75 to -77 it already hard or no hope to associated with the router's .?

Yeah I know, after I set the delays I noticed that I had to restart less often.

Probably because I have no idea where it's coming from lol, but I get some APs in the list with signals of 20-.

Dragonlord - December 19, 2013, 6:57 pm

It works absolutely fine, but you just have to know which networks to use it on.

Some networks will work, some won't.

Gunz_kruunG - December 19, 2013, 10:23 pm

(Dec 19, 2013 04:58 PM)TheDovahkiin909 Wrote: [\[CITE\]](#) Yeah I know, after I set the delays I noticed that I had to restart less often.

Probably because I have no idea where it's coming from lol, but I get some APs in the list with signals of 20-.

Lol.. I think you should give a try on that AP [-20 signal] I am sure you would appreciate reaver been invented for wpa attacks[wps feature] ?

Yup Dragonlord right.. Not all routers still can be attacked by using reaver but some still will be, there still hopes ? because as we all had already noted that reaver are not been updated anymore but firmwares still updated so we can understand why reaver abilities are been faded away.. ? but I am not sure about the Reaver Pro 2 because I don't have it hope someone that owned it can share with it ?

Tyranic - December 20, 2013, 4:19 am

TheDovahkiin909,

You should try looking here :

<https://docs.google.com/spreadsheets/lv?key=0Ags-JmeLMFP2dFp2dkhJZGlxTTFkdFpEUDNSSHZEN3c>

Very handy resource.

I've found that reaver will fall down a lot unless you your signal strength is lower than -50. you could try using a panel antenna & turning you tx power up but being that far away you might just be SOL.

You want the be using the delay & timeout flags (almost all modern routers will lock up without them)

Can you post details about which router your trying to break (use wpscan.py) and the reaver command your using?

TheDovahkiin909 - December 20, 2013, 5:04 pm

(Dec 20, 2013 05:19 AM)Tyranic Wrote: [\[CITE\]](#) You want the be using the delay & timeout flags (almost all modern routers will lock up without them)

Can you post details about which router your trying to break (use wpscan.py) and the reaver command your using?

Yeah, I had to implement 35 secs for each before it would work (kinda) effectively.

I can't check right now, but it's a Netgear.

Code iwconfig

airmon-ng start wlan0

airodump-ng mon0

reaver -i mon0 -b #BSSID# -vv -d 35 -t 35Should I use -n too or no?

(Dec 19, 2013 11:23 PM)Gunz_kruunG Wrote: [\[CITE\]](#) Yup Dragonlord right.. Not all routers still can be attacked by using reaver but some still will be, there still hopes ? because as we all had already noted that reaver are not been updated anymore but firmwares still updated so we can understand why reaver abilities are been faded away.. ? but I am not sure about the Reaver Pro 2 because I don't have it hope someone that owned it can share with it ?

Well it's working, I'm at 19.50% now. Slowly but surely, and pain-in-the-ass-ly.

squadz - December 20, 2013, 5:24 pm

It's always been stable for me, the only issue is speed sometimes, but that isn't reaver as much as the the setting/hardware device of the target, and proximity.

Gunz_kruunG - December 20, 2013, 8:43 pm

(Dec 20, 2013 06:04 PM)TheDovahkiin909 Wrote: [\[CITE\]](#) Well it's working, I'm at 19.50% now. Slowly but surely, and pain-in-the-ass-ly.

I'm glad to hear that..? just stick with your command but if you want to added more command just don't forget to back it up first just for precaution lol..?

19.50% it good enough you just need to hope that the router's wps pin would not be start with number 9 at front because it really are pain-in-ass lol..? believe me after the reaver found the first 4 pin [if not mistaken] it would jump to 90% above, it not likely it a must to waited until the whole time for percentage 1-100%.. happen to me waited so long for the percentage to achieve 20% something, then suddenly it jumped to 90%, after a minutes later poof it show me the wps pin and wpa password..? Hope this could encourage you to be patient for waiting lol ?

TheDovahkiin909 - December 20, 2013, 9:15 pm

(Dec 20, 2013 09:43 PM)Gunz_kruunG Wrote: [CITE](#) I'm glad to hear that..? just stick with your command but if you want to added more command just don't forget to back it up first just for precaution lol..?

19.50% it good enough you just need to hope that the router's wps pin would not be start with number 9 at front because it really are pain-in-ass lol..? believe me after the reaver found the first 4 pin [if not mistaken] it would jump to 90% above, it not likely it a must to waited until the whole time for percentage 1-100%.. happen to me waited so long for the percentage to achieve 20% something, then suddenly it jumped to 90%, after a minutes later poof it show me the wps pin and wpa password..? Hope this could encourage you to be patient for waiting lol ?Thanks for the encouragement! But nothing could shake me in my quest to accomplish my first WPA2 crack :D