

Forum: [Hack Forums](#)

Thread: [router .huawei](#)

khaled77 - August 13, 2018, 5:04 pm

[b]frist of iam try to crack wps for router .huawei hg i try with rever and other tool

no luck any one here have other way or idea

i got handshake and try to hashcat so hard to beark it year i guss

here in egypt most the router huawei

any help plzzzzzzzzzzzzzzzzzz

simobouhmidi - January 22, 2020, 7:18 am

I have the seem problem

why they don't answer you yet

CyberStrike - January 22, 2020, 11:08 pm

(Jan 22, 2020 08:18 AM)simobouhmidi Wrote: [\[CITE\]](#) I have the seem problem

why they don't answer you yet

Well here is the problem, bruteforce is not always successful in a time which is suitable. As an example let's say my password is F@rtSheetlCraPpereDMyPantal0onsZi3s probably not a password you would think of or generate too quickly also that list would be massive, bruteforce would take a while probably unless that specific word was in the list.

WPS you really want to be close to that AP (like over 70% signal strength), which sometimes is hard. Now evil twin access points (APs) they tend to be successful, but once again it may not always work, none of these techniques work 100% of the time. So perhaps we go ahead and run our own evil twin mimicking the target well we knock off devices, but alas no one was home during the time of our attack, as to log into our AP and supply the password, yet again we would fail. Had we perhaps scouted out the people associated with the target AP maybe our results would have been different. Using a combination of different tactics/techniques is really the trick and like I said it's not 100% you will always get into the wifi.

ThisBearScat - January 23, 2020, 4:24 am

not sure if its the same but most routers in my country are protected against wps attacks and also disable WPS if you try to brute force the pin.

wpa2 handshake would be better but again without a gui mining rig or powerful hacking rig it would take ages to get the password.

to speed up the proccess you need to learn the router. ask these questions.

is it one internet company (ISP) that provides the majority of those routers to their users?

if so do you know anyone that uses them?

try have a look at some of your freinds and see if the length of the standard password provided by the internet company is the same on each.

How many charecters is it?

is it a mix of letters and numbers?
is it all upper or lower case?

that way you can smallen the list of possibilitys for the password as long as it has not been changed.

example.

a router whos isp issues the routers with passwords that are 8 charecters all uppercasse
hashcat -m 16800 -a 3 /media/user/pmkid.16800.txt ?u?u?u?u?u?u?u?u --force

the more information you can give hashcat the quicker the result but with just a normal pc/laptop it would take years to crack