

Forum:[Hack Forums](#)

Thread: [Crack Wifi Password Fritz Box WPA2/3?](#)

dashka - September 9, 2024, 12:49 pm

Hello there,

if you see this, you are right to assume that I am not the best yet, but I am working on my skills so far so Id be glad to get some help as a beginner.

So I want to crack a Wifi Password and so far I captured a handshake and as far as I know they have WPA2 but I cant tell you for sure cause they somehow have like 4 Wifis with the same name??? But anyways at least one of them has WPA2 and thats the one I am interested in. I tried to brute force it with a few password lists of like 100gb and stuff like that but considering their technical skills Id presume that they use a random generated Fritz Box Password (with I think around 16-20 digits), so brute force does not make much sense. I might add that they are Romanians so maybe a password list in their language would be an option as well.

So now my question is: What do I do now?

I read about an evil twin or honey pot wifi but I dont know how much sense that would make or if there are easier methods

Best regards,
a newbie

PS why I do this?

1. My dad turns off the wifi at night and then Id have another one
2. They have a security camera thats probably not well secured and I wanna try get some pictures of it

DramaKing - September 9, 2024, 8:41 pm

(Sep 9, 2024 12:49 PM)dashka Wrote: [\[CITE\]](#) Hello there,

if you see this, you are right to assume that I am not the best yet, but I am working on my skills so far so Id be glad to get some help as a beginner.

So I want to crack a Wifi Password and so far I captured a handshake and as far as I know they have WPA2 but I cant tell you for sure cause they somehow have like 4 Wifis with the same name??? But anyways at least one of them has WPA2 and thats the one I am interested in. I tried to brute force it with a few password lists of like 100gb and stuff like that but considering their technical skills Id presume that they use a random generated Fritz Box Password (with I think around 16-20 digits), so brute force does not make much sense. I might add that they are Romanians so maybe a password list in their language would be an option as well.

So now my question is: What do I do now?

I read about an evil twin or honey pot wifi but I dont know how much sense that would make or if there are easier methods

Best regards,

a newbie

PS why I do this?

1. My dad turns off the wifi at night and then I'd have another one
2. They have a security camera that's probably not well secured and I wanna try get some pictures of it

What did you use that captured a WPA/WPA2 handshake, but didn't tell you the security? If the password is random and bruteforcing doesn't make much sense, then I'm afraid that you're SOL.

dashka - September 10, 2024, 9:00 am

(Sep 9, 2024 08:41 PM)DramaKing Wrote: [\[CITE\]](#) What did you use that captured a WPA/WPA2 handshake, but didn't tell you the security? If the password is random and bruteforcing doesn't make much sense, then I'm afraid that you're SOL.

Hi, sorry for the bad wording or writing what I mean and mb for the lack of informations so i checked again and it is a WPA2 Wifi and the point of my question here was to be clear this time:

1. Does it make sense to brute force a Password Wifi if I know the amount of digits
 - 1.1 Are there any available lists to use?

2. What other options do I have to crack their wifi or what other informations do I need like which router and so

DramaKing - September 11, 2024, 8:30 am

(Sep 10, 2024 09:00 AM)dashka Wrote: [\[CITE\]](#) Hi, sorry for the bad wording or writing what I mean and mb for the lack of informations so i checked again and it is a WPA2 Wifi and the point of my question here was to be clear this time:

1. Does it make sense to brute force a Password Wifi if I know the amount of digits
 - 1.1 Are there any available lists to use?

2. What other options do I have to crack their wifi or what other informations do I need like which router and so

10 digits would be about my limit.

I went back to another thread where I calculated 200-250 years to crack a default Fritzbox password.

dashka - September 12, 2024, 11:45 am

(Sep 11, 2024 08:30 AM)DramaKing Wrote: [\[CITE\]](#) 10 digits would be about my limit.

I went back to another thread where I calculated 200-250 years to crack a default Fritzbox password.

Alright thanks for the help so far, but I do have a last question.

Considering the amount of time a password list takes to run I thought about just letting a server run that but are there any other options to get into their Wifi which are faster?

DramaKing - September 12, 2024, 12:21 pm

(Sep 12, 2024 11:45 AM)dashka Wrote: [\[CITE\]](#) Alright thanks for the help so far, but I do have a last question.

Considering the amount of time a password list takes to run I thought about just letting a server run that but are there any other options to get into their Wifi which are faster?

Pixie Dust, Null PIN, WPS Bruteforce, ChopChop, Fragmentation, or Evil Twin Captive Portal

attacks or bruteforcing the owner.

Sparton - September 12, 2024, 12:33 pm

(Sep 11, 2024 08:30 AM)DramaKing Wrote: [\[CITE\]](#) 10 digits would be about my limit.

I went back to another thread where I calculated 200-250 years to crack a default Fritzbox password.

Using a RTX4090 20 digits would take about 1,255,500 years to crack.

DramaKing - September 12, 2024, 12:41 pm

(Sep 12, 2024 12:33 PM)Sparton Wrote: [\[CITE\]](#) Using a RTX4090 20 digits would take about 1,255,500 years to crack.

I only say 16, but yeah, either way it's not feasible.

Wifi Pineapple - September 12, 2024, 2:23 pm

vast.ai is a place you can rent GPUs for pretty cheap /hour. Get a lot of them strung together and feel free to crack that way. But no body would willingly run Fritz network to crack without a good chunk of money up front.

DramaKing - September 12, 2024, 4:39 pm

(Sep 12, 2024 02:23 PM)Wifi Pineapple Wrote: [\[CITE\]](#) vast.ai is a place you can rent GPUs for pretty cheap /hour. Get a lot of them strung together and feel free to crack that way. But no body would willingly run Fritz network to crack without a good chunk of money up front.

Right. It would cost ~400k if the password hasn't been changed.