

Forum:[Hack Forums](#)

Thread: [I have the Handshake but struggling with word list](#)

r.holder9090 - January 27, 2020, 7:45 am

Hey

Recently started learning how to crack WiFi with Kali Linux, fun experience so far.

I've played about with aircrack/mon/dump and after a while I got the hang of it. And then I discovered Kali had Fern WiFi cracker built in so I'm using that now.

I've easily got the Handshake for two networks but the next part I'm getting stuck on/have a few questions.

- I'm using 'WPA-BIG-LIST1' and I've had it running for hours and I've noticed a lot of the words are words with numbers on the end, but do these lists include "default" passwords? Like I don't know anyone who changes their WiFi password and just use the one printed on the router which is usually a combo of numbers and letters, are these included or am I banking on the person has changed their PW?

- is it possible to get lists specific certain routers? For example a Sky or Plusnet word list?

- do you recommend a different method or different list? Is it better to create my own?

I've also used pixie/rever but I've had no luck so far, I used a command something like 'wash - I something' which was supposed to show me only wps networks but it showed me a bunch and I had no luck.

Any helpful info or a push in the right direction would be appreciated ?

Sorry I see now there is a dedicate WiFi hack section, Mod please delete this and I'll post in the right section.

Exalted - January 27, 2020, 8:01 am

It is rather hard to crack WPA and WPA2 keys with a wordlist. Most use randomly generated ones.

I've seen multiple WPA lists within a few Google-searches, so if you want to go the wordlist path, you can test that out.

There are default logins available for router administration panels online; these shouldn't be too hard to find.

r.holder9090 - January 27, 2020, 8:21 am

(Jan 27, 2020 08:45 AM)r.holder9090

[quote='Exalted Wrote: [CITE](#)] It is rather hard to crack WPA and WPA2 keys with a wordlist. Most use randomly generated ones.

I've seen multiple WPA lists within a few Google-searches, so if you want to go the wordlist path, you can test that out.

There are default logins available for router administration panels online; these shouldn't be too hard to find.

Thanks for the reply, I'll look into the random gen ones I did look into 'crunch' the other day so I'll pick that back up.

I have no problem finding word lists but I have tried and tried to find router default logins for Sky and Plusnet with zero results. Tried Google and duckduckgo. I will keep looking though.

CyberStrike - January 27, 2020, 10:10 pm

Most of these APs have "unique" passwords for wifi, logging in after being on the network or if say they have remote login or something that you probably would find it's still default but wifi generally it's unique.

jetx - January 28, 2020, 4:01 am

try to play with new PMKID method

ComputerDoge - February 7, 2020, 5:52 pm

Rockyou Word List is a good general password to list, but as people mentioned, it's likely that its a randomly assigned password from the router manufacturer.

compalabee - February 9, 2020, 6:08 am

I've been using this since 2010

PHP Code

<?php

<https://www.onlinehashcrack.com/>

Dirk Rathken - February 12, 2020, 8:54 pm

honestly I'd look into using hashcat if you've got some graphics hardware to utilize and figure out the default key spaces to crack for that specific router this will brute force, but it'll be a bit more efficient than just straight brute force.

HeadingChilling - February 13, 2020, 10:44 pm

It is difficult to crack password using wordlist, i would rather suggest you to use the "Fake AP" method.

kibaaa - February 14, 2020, 10:21 am

Can you upload the handshake and share it? I will see what i can do.