

Forum:[Hack Forums](#)

Thread: [HOW TO HACK WPA2 WIFI](#)

lights out - September 29, 2023, 10:50 am

Wi-Fi hacking examples and walkthrough

The edited transcript of the Wi-Fi password hack walkthrough video is provided below, separated into each step Mike covers in the video.

WPA and WPA2 security

(0:00- 0:24) WPA and WPA2 are very good encryptions. If you're using WPA, you're using RC4, but you're using TKIP with that. If you're using WPA2 while you're using AES with CCMP, then you are not going to be able to crack these passwords, except for one little problem.

Problem with WPA and WPA2

(0:25- 1:35) The problem is that the initial connection between a wireless WPA or WPA2 client to an access point has what we call a four-way handshake. Not that many years ago, there was a small weakness discovered in this four-way handshake that allows us to do something very interesting.

Now, I need to be careful here. When you're cracking WEP, you can mathematically derive the password just by looking at packets. You can't do that with WPA and WPA2.

What should you learn next?

What should you learn next?

From SOC Analyst to Secure Coder to Security Manager — our team of experts has 12 free training plans to help you hit your goals. Get your free copy now.

With WPA and WPA2, think more instead that you've got this guy who's really good at turning the numbers on a bicycle lock and then pulling on it. So you can go up to this guy and say, "Hey, try 0000," and he could do that real quick and pull on it.

If you wanted to, you could tell this guy, start with all zeros and then just keep going and go to 9999. Now, if there were only 10,000 different permutations that would work great. But with WPA or WPA2, take that same bike lock analogy and turn it from four digits to like 128 digits. So it would take that guy, even if he was fast, a very, very long time to go through all these.

Humans use weak passwords

(1:36- 2:15) Luckily for us, we know that human beings don't use good, randomized, long passwords. We know that most human beings are going to use a phrase and then a number. Or their pet's name and then the date they were born, or the number of kids they have and their wife's name and the date that they got married. Little, simple, things like that.

And if we know that, we can tell the guy who's spinning on that bicycle lock, "No, no, no. Don't start at the zeros, just try all of these first." So we've got to give this WPA, WPA2 cracker what we call a dictionary file.

What is a dictionary file?

(2:16- 3:07) Now, a dictionary file is nothing more than a big text file full of tens of millions of different types of permutations of well-known words, numbers and all kinds of different things. Now you think, "Whoa, tens of millions." Well, compared to 128th power stuff, at 10 million even my laptop, give it a day, could knock all that stuff out. So it makes a big difference.

Here's what we're going to be doing with WPA and WPA2. We've got a whole bunch of packets. What we're going to grab is those four-way handshakes when people start to connect. Using that, we can derive the passwords by using a dictionary file. Basically saying, "Try all these, and if people use it, then we're going to have them." So let's go ahead and let me show you how the setup works this time.

Setting up the Wi-Fi hacking demo

(3:08- 4:26) So I've got my same wireless access point. Now, he's still set to WEP at this moment. So we're going to change him to a regular, old WPA-PSK, and get him up and running.

We'll put a really weak password on here, then we're going to go back over to the Kali box and in this case, what we're going to do is we're still going to monitor the traffic, but we're just going to wait for somebody to authenticate, and we got them. We'll run the cracker, and with luck, since it's a weak password, we're going to be able to get it pretty easily.

So let's take a look at the setup. All right, so let's go over here, and first of all, instead of calling it a NOTSECUREWEP, let's call it NOTSECUREWPA.

The next thing I'm going to do is go over to Wireless Security, and we're going to take off WEP, and let's go to WPA Personal. This type of attack will work with a WPA or WPA2 personal shared key. So I've already got a password here, and I want to keep it.

The password is "timmytimmy," so it's a pretty simple password. It's just a very common word, used twice. So let me go ahead and apply all this, we'll save it, and we're pretty much ready to go.

Role Ebook - GIF Test (GIF)

Using airodump to grab WPA connection data

(4:27- 6:29) So this guy is now WPA personal, he has a very simple password of "timmytimmy," and now what we're going to do is go over here, we're going to grab a bunch of data. But in particular, we're not just grabbing data, we're looking for handshakes, and that's where airodump does a great job. Let me show you.

Now, what I've got here is I've got airodump still running on my screen. If you take a look right here at the top, you're going to see there's NOTSECUREWPA. You can even see that it's WPA and it's running TKIP. No great surprise there, and there's the MAC address for it.

So what we're going to do now is let's start airodump, and we're going to watch for handshakes.

I'm going to put all the stuff that it finds into a file called wpafile, and this guy's on channel 6, and the bssid is 20:AA:4B:42:43:E8 and we're going to tell them to listen on wlan0mon.

```
root@kali:~# airodump-ng -w wpafile -c 6 --bssid 20:AA:4B:42:43:E8 wlan0mon
```

So what we're going to do now is keep watching this and see if somebody comes in.

There it is. Wow! That was really quick. Let's go ahead and take a look at that file and go ahead and see if we can pull the password out. We can go ahead and turn this off.

Cracking passwords with aircrack

(6:30- 7:31) Let me make sure I've got a dictionary file in there.

```
root@kali:~# ls
```

There it is. Way up at the top, you see the word dictionary? That's a dictionary file that I've created. So to actually go about the cracking, we go ahead and run Aircrack. "a2" means I'm doing a WPA attack on this guy.

```
root@kali:~# airodump-ng -a2
```

I got to tell it where my dictionary file is. It's right here in the same folder, so I type in "dictionary." Then I tell it which file I want to crack. In this case, it's going to be wpafile-01.cap.

```
root@kali:~# airodump-ng -a2 -w dictionary wpafile-01.cap
```

Ta-da! There it is, right there.

Weak keys are vulnerable to attack

(7:32-8:17) Pretty easy stuff. Now, you're looking at this probably saying, "Wait a minute, Mike. You put the right password into your dictionary file." Yeah, I did. But I did that just to speed up this demonstration. Trust me, there are huge dictionary files, and they got "timmytimmy" in there just as

easily.

If you have a weak WPA or WPA2-PSK, odds are good that people will be able to crack it almost as quickly as I've done right here.

The right answer is simple. Use long, complex private shared keys when you're dealing with WPA and WPA2. A lot of people recommend that you don't use any human words and make sure you use at least 20 characters, which can sometimes be long to remember, but boy, does it make it secure.

little - October 6, 2023, 4:44 pm

I think these are of no use at all, unable to even crack a basic home Wi-Fi router. Many routers on the market today have default passwords that are 12 characters long, consisting of 26 English letters (both uppercase and lowercase), 10 numbers, and 10 special symbols. Even if you can capture the handshake packets, cracking it, I believe, is something for the next century.

DramaKing - October 7, 2023, 8:51 am

(Oct 6, 2023 04:44 PM)little Wrote: [\[CITE\]](#) I think these are of no use at all, unable to even crack a basic home Wi-Fi router. Many routers on the market today have default passwords that are 12 characters long, consisting of 26 English letters (both uppercase and lowercase), 10 numbers, and 10 special symbols. Even if you can capture the handshake packets, cracking it, I believe, is something for the next century.

I've seen TP-Link routers with 8-digit passwords even recently. Lot of Spectrum and Netgear routers around me, too.

Rogers Communications - October 7, 2023, 10:21 am

I still have a 80% crack rate around me..... NOT CRACKHEAD but WPA2 Crack rate.. What im finding is its gettin harder to get a handshake!!! I deauth etc and cannot get a handshake.. most times I just monitor til someone logs in

pasnger57 - October 8, 2023, 2:20 am

(Oct 7, 2023 10:21 AM)Wpginterceptor Wrote: [\[CITE\]](#) I still have a 80% crack rate around me..... NOT CRACKHEAD but WPA2 Crack rate.. What im finding is its gettin harder to get a handshake!!! I deauth etc and cannot get a handshake.. most times I just monitor til someone logs in EXACTLY!!!!!!!

The Quieter you are the More you can Hear

arav - October 26, 2023, 3:56 am

(Oct 7, 2023 10:21 AM)Wpginterceptor Wrote: [\[CITE\]](#) I still have a 80% crack rate around me..... NOT CRACKHEAD but WPA2 Crack rate.. What im finding is its gettin harder to get a handshake!!! I deauth etc and cannot get a handshake.. most times I just monitor til someone logs in how do you do ? I want to learn haha

If you have time to teach me something can I write to you privately?

Rogers Communications - October 26, 2023, 2:46 pm

(Oct 26, 2023 03:56 AM)arav Wrote: [\[CITE\]](#) how do you do ? I want to learn haha

If you have time to teach me something can I write to you privately?

no, read and read and watch youtube videos and learn. dont bother me to spoon feed you

VenomsRatzs19954 - *October 28, 2023, 4:43 pm*

interesting brou. testingg

Username10 - *November 17, 2023, 11:53 am*

it takes too long, need faster option