Summary

The technique of cracking the password of a wireless WI-FI network

Hacking methods

Wireless networks combine many technologies. And where there is a lot of technology, there is a lot of security technology. And at the bottom of this technology, security holes also pop up. And every possible hole has its own method of attack.

The main ways to hack someone else's Wi-fi:

* Unsecured networks
* Manual password selection
* Password Bruteforce
* Selection of WPS code
* Phishing
* Password databases
* Bypassing filters
* Interception of the "handshake" and its decryption
* Hacking the router and pulling out an open password

Before I start, I want to ask and answer two questions.

* Is it possible to hack? – Yes, it is possible.
* Is it possible to protect yourself completely? – No, you can't. Because the technology is initially open to connecting users.

Unsecured networks

Usually nowadays all networks are encrypted and protected with a key. But there are still access points that are not protected in any way. And you can connect to them completely freely – without a password. An example of such a point is public places, metro.

Manual selection

These first two methods are written simply to show that sometimes it is not worth resorting to complex technical actions, because usually everything is in plain sight, you just have to think a little.

The average user usually sets himself a simple password – try to imagine what he could have entered and guess it. It works great to find out the Wi-Fi password from friends and a neighbor. What if you already know some password of your neighbor? People are very fond of repeating themselves, and usually enter the same thing. Works rarely, but aptly. Especially on the old WEP networks, where it was allowed to enter passwords less than 8 characters – there were often both "12345" and "QWERTY". Look at Figure 1 and try these combinations.



Figure 1 – Top 25 most common passwords

Brutforce

Brute Force is a method of automatic password brute force. After all, you enter the password freely? And what to do if you force the program to sort through all possible options on its own and try to connect with them.

There are advantages – old models without attack detection and weak password (WEP) break with a bang. There are disadvantages – new models can detect you (you have to disguise yourself) and introduce delays in the search, or even a complete ban of the attacking machine. Another disadvantage is that modern routers force users to enter complex long passwords, which will take years to sort out. So we'll have to look for other methods.

But still, it's definitely worth trying to sort out the network for easy passwords, or if it's WEP and not WPA/WPA2. There is always a possibility of a hole.

Highlights on Brutus:

* Programs can use the entire search of options – suitable for a WEP network, or for a router model that forces you to forcibly enter complex passwords, where a dictionary attack is impossible.
* There is a variant of the dictionary attack – when the file with the most frequently encountered passwords is loaded. There are a lot of these files – there are a couple dozen of them in one Kali Linux, and how many are on the network. For me, it's enough to check for basic passwords with a small list – after all, hacking through bruteforce is no longer an option, and for basic verification and saving time, the simplest list is enough.
* The program works in several threads – i.e. it can simultaneously try to iterate through many options at once. But there is a special feature here: the router itself can reject such attempts, introduce delays for authorization, or reboot altogether. I.e., you need to play with the streams carefully. In any situation, check everything on your hardware, so you will know for sure.
* Some write about proxies… But what kind of proxy is there))) We are connected over the air) We are talking about the fact that some programs successfully mask their requests for different devices, which makes it possible to work in a multi-thread.

Handshake interception

One of the most working methods is the interception of the "handshake". What is it? Also a kind of pure brutus, only with a preliminary interception of the cipher and its further attempt to decrypt. Here is a brief outline:

* You are sitting quietly online.
* The network is breaking.
* Your computer reconnects again.

What happens at the moment of reconnection: your computer sends the password to the router again, the router accepts it and, if entered successfully, establishes a connection. In practice, this is absolutely imperceptible – neither disconnecting the network, nor entering a password – everything is done automatically by your own system.

This process of sending a password can be called a "handshake". But there is a disadvantage of this method – the data is transmitted initially in encrypted form. But with a strong desire, this cipher can still be disassembled into parts (even there are services) and open the password-protected data. And it will take no more time than a direct brute force. That's the whole basis of the method.

WPS code

Some routers have the same useless button – WPS, which allows you to connect devices in a simplified mode. By default, WPS is still activated in many routers. And the connection to such a network is carried out only by entering this PIN code, which consists only of digits.

There are only 8 digits in the PIN code. I have already mentioned above about the permissibility of a complete search of WEP, but here it is even simpler – only numbers. In addition, a correlation was found that allows the methods to be selected in pairs – first 4 digits, and then 4 digits. This all speeds up the search very much, and a point with an open WPS can be broken in a few hours.

Another attack option is to use default codes. yes! Some devices from the factory come with the same PIN code installed and enabled) And the proposed programs already know these passwords, so everything can be much easier.

Phishing

Another interesting method is to display your page from the network user ... Yes, you can do this without connecting to the network. But the substitution can be noticed. The most acceptable option:

* An access point with the same name of the hacked network is created.
* A good signal and a name will force the victim to connect to it sooner or later.
* After logging in, the password is entered, which successfully comes to you.

Password databases

There are programs and services that store databases of passwords of access points of public places. This is especially true for all kinds of cafes in large cities. Do you want to break the cafe? Yes, why, usually someone has already connected to it, which means there is a chance that the password has floated into the database.

An example of such a service is an application: Wi-Fi Map or Router Scan. And it will show the map, and the available points, and it will connect itself.

Hacking the router

Sometimes you have the opportunity to connect by wire to Wi-Fi, or you know the external IP address from the Internet and can access the router (sometimes it is possible to determine it with a high degree of probability by scanning).

Then you can try to find a password to log in to his control panel. Many people leave it by default admin / admin (login / password). And already in the settings, the Wi-Fi password is stored in plain text.

Bypassing filters

Some access points won't let you in, just because you have the wrong... MAC address. It also happens. This is no longer about hacking, but sometimes the whole task of hacking comes down to changing the MAC – for example, when you previously successfully connected, but now it does not let you into any, because the administrator or parents have banned your device for the MAC. The solution is simple – change it.

In conclusion, I will give tips for protecting your network

* Put a complex password on Wi-Fi.
* Put a complex password on the router panel itself.
* In case of paranoia, enable MAC address filtering, allow only for your devices.
* Turn off WPS (sometimes called QSS).

Thanks for your attention!