Hristo Kolew

Personal Vulnerability Investigation Project

Table of Contents

[Introduction 1](#_Toc134386313)

[Research Questions 1](#_Toc134386314)

[Planning 2](#_Toc134386315)

[Preparation 2](#_Toc134386316)

[Attacks 3](#_Toc134386317)

[Wireless hacking 3](#_Toc134386318)

[Router exploitation 7](#_Toc134386319)

[Phishing attack 7](#_Toc134386320)

[Conclusion 7](#_Toc134386321)

# Introduction

I decided to make my personal vulnerability investigation (PVI) about a home router. The motivation for hacking a home router for educational purposes is typically to teach individuals about the vulnerabilities and risks associated with these devices. Also, it may involve setting up a simulated attack on a router to demonstrate how an attacker might exploit vulnerabilities in the device's firmware or configuration. This type of exercise can help individuals understand the techniques and tools that hackers use, as well as the potential consequences of a successful attack.

# Research Questions

Main question:

What are the options and alternatives to hack a home router?

Sub question:

1. What software tools do I need?
2. What devices do I need for the attack?
3. What kind of attacks are possible for router?

|  |  |  |
| --- | --- | --- |
| Research Questions | Strategies | Methods |
| What software tools do I need? | Library, Field | Literature study, Community research, Problem analysis |
| What devices do I need for the attack? | Library, Field | Literature study, Community research, Problem analysis |
| What kind of attacks are possible for router? | Library, Field, Lab | Literature study, Community research, Problem analysis, Security test |

# Planning

|  |  |
| --- | --- |
| Sprint1- Researching | 13.03.2023-31.03.2023 |
| Sprint2- Technical exercise | 3.04.2023-21.04.2023 |

I decided to approach with the following scenario: find the nearest router and try to access it without having the correct password. This includes doing Death Aireplay attacks, which disconnect all users from the WI-FI network and forcing them to re-join again. These crucial attacks allow me to capture the handshake. Afterwards, the only thing that left is to crack the password and I am able to join the network.

I knew hacking a router, which I do not own or have permission to crack will be absolutely illegal. I did not have any problems with that because the router was mine and I was able to do with it whatever I want.

# Preparation

For hacking device, I choose an old router. After getting it, I had to set it up in order to see the wireless connection.

Information about the router:

1. BELKIN N Wireless Router
2. Model no: F5D8233-4v3



Another important thing was to setup my own Virtual machine with Kali Linux on my personal computer. Also, I needed WI-FI adapter to see all the networks in my range. I borrowed it from the ISSD and add it to my Virtual Machine to see if I had t install specific drivers for it.

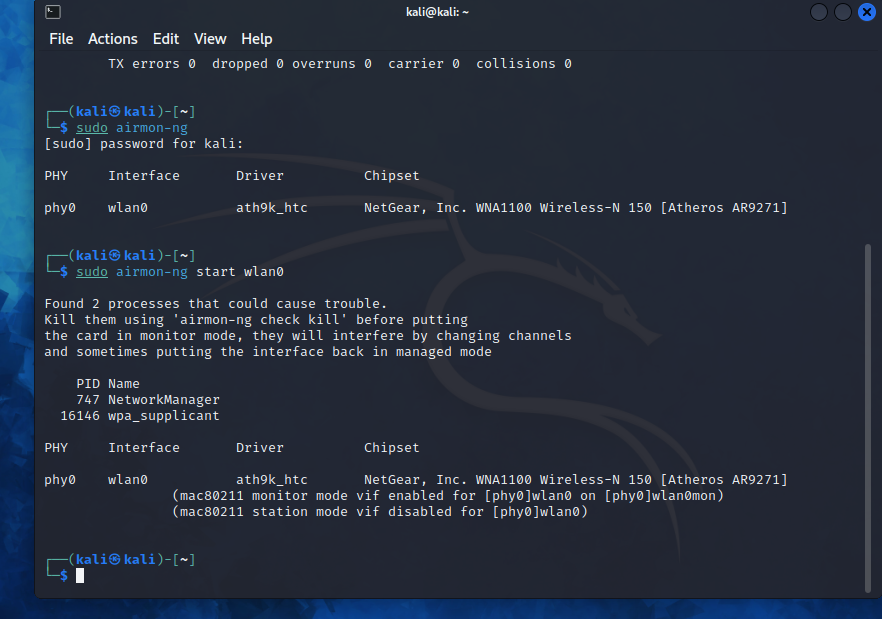


# Attacks

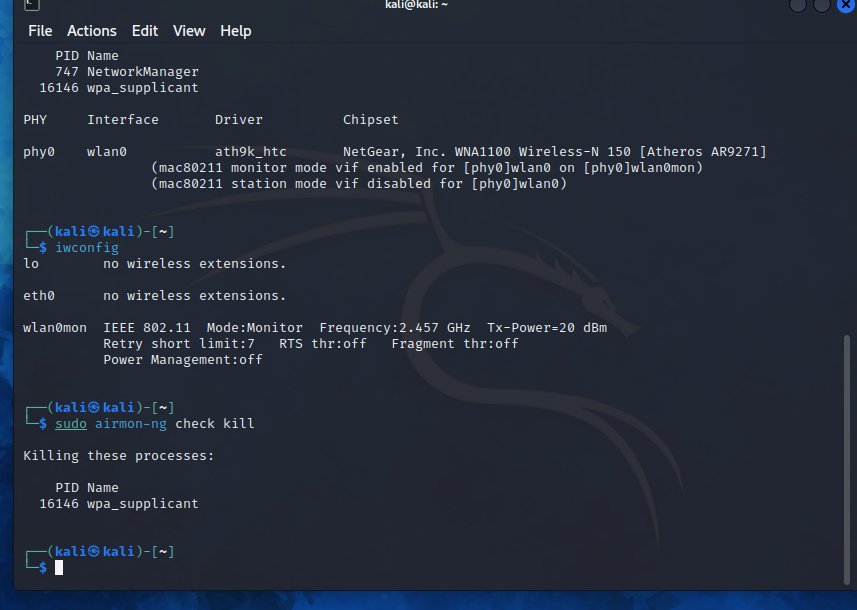
## Wireless hacking

After preparing everything, it was time for the technical part.

The first thing to do is to put your WIFI card to monitor mode. It is important to run airmon-ng as an administrator.

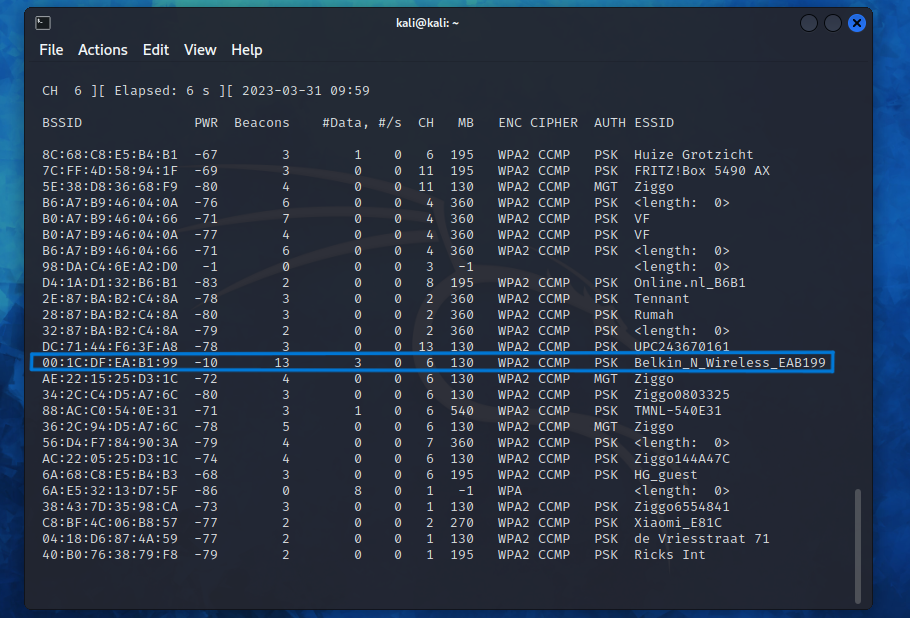


To be sure that the monitor mode is enabled I run the “iwconfig” command:

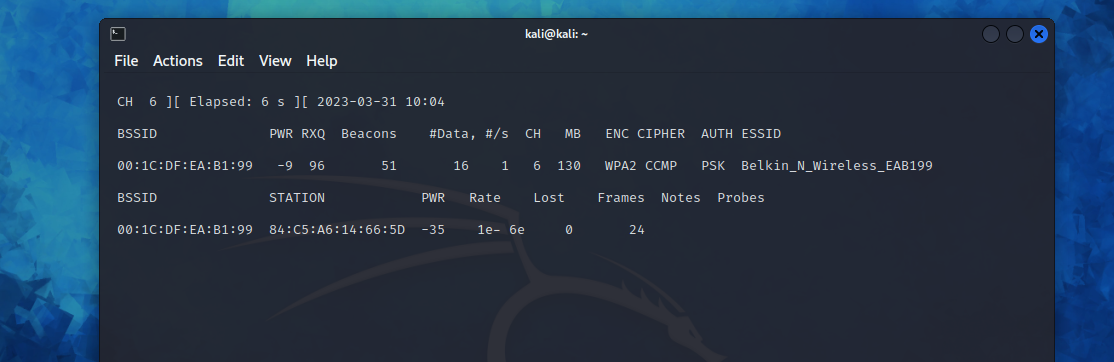


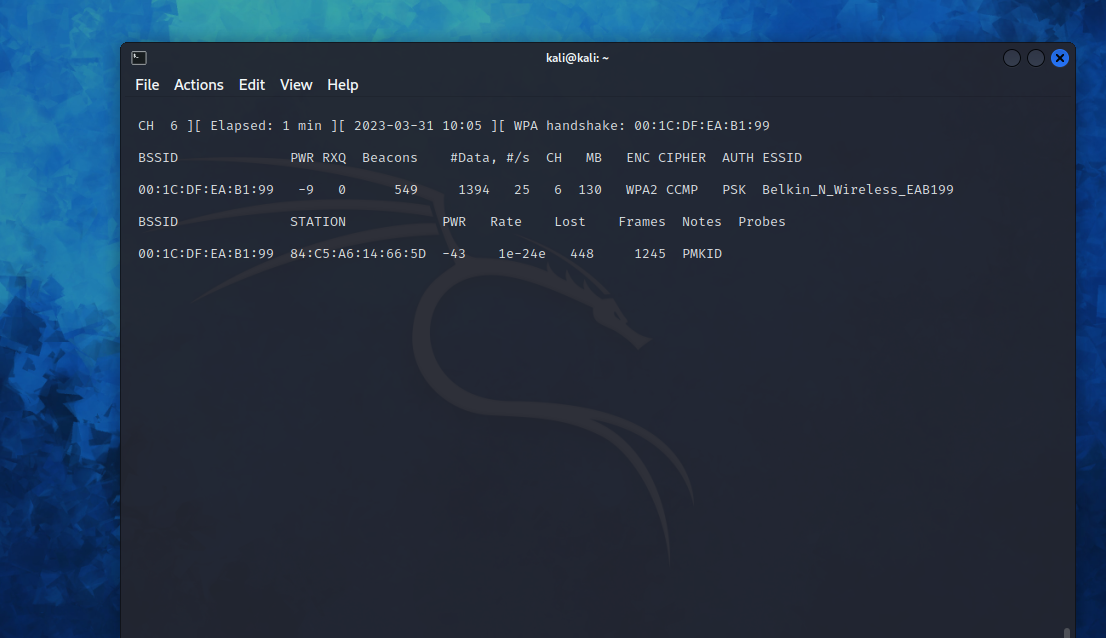
As you can see the WIFI card is on monitor mode and the name is modified from “wlan0” to “wlan0mon”. Before looking into the available WIFI connection I had to kill the processes that could interfere by changing the channels or putting the interface to managed mode. I do that with the command “airmon-ng check kill”

Then I used the command “airodump-ng [Network interface]” (in my case the interface will be “wlan0mon”). The airodump-ng command will display a list of detected access points near me, and also a list of connected clients (“stations”).



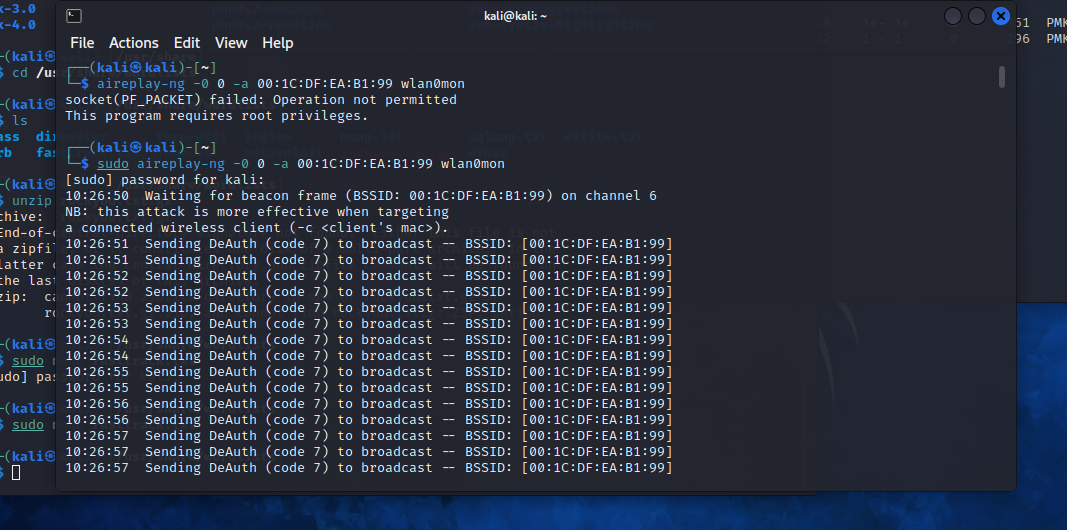
The selected target is “Belkin\_N\_Wireless\_EAB199” and the important here is to remember the MAC address and the channel because I need them for the next command. Now I had to execute “airodump-ng -c [Channel of the network] –bssid [MAC address] -w [Directory where the file is going to be saved] [Network interface]”. In my case the command looks like this: “airodump-ng -c 6 –bssid 00:1C:DF:EA:B1:99 -w /home/ wlan0mon”.



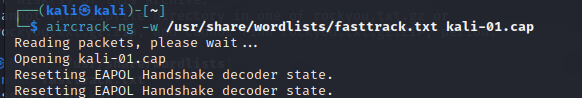


The first picture shows no wireless client is connected. The second one shows when there is wireless client connected. On the top right corner there is “WPA handshake: 00:1C:DF:EA:B1:99”, this means that the airodump-ng has successfully captured the four-way handshake.

The next step is too deauthenticate the wireless client. The wireless client will then hopefully reauthenticate with the AP. The reauthentication is what generates the 4-way authentication handshake that I had to collect in order to break the WPA2 password. I used the command “airplay-ng -0 [Number of deauths to send] -a [MAC address] [Network interface]”.



After the deauthentication I had the file, which only needed to be cracked to see the password. The final step is to use aircrack-ng with a specific word file with a lot possible password.

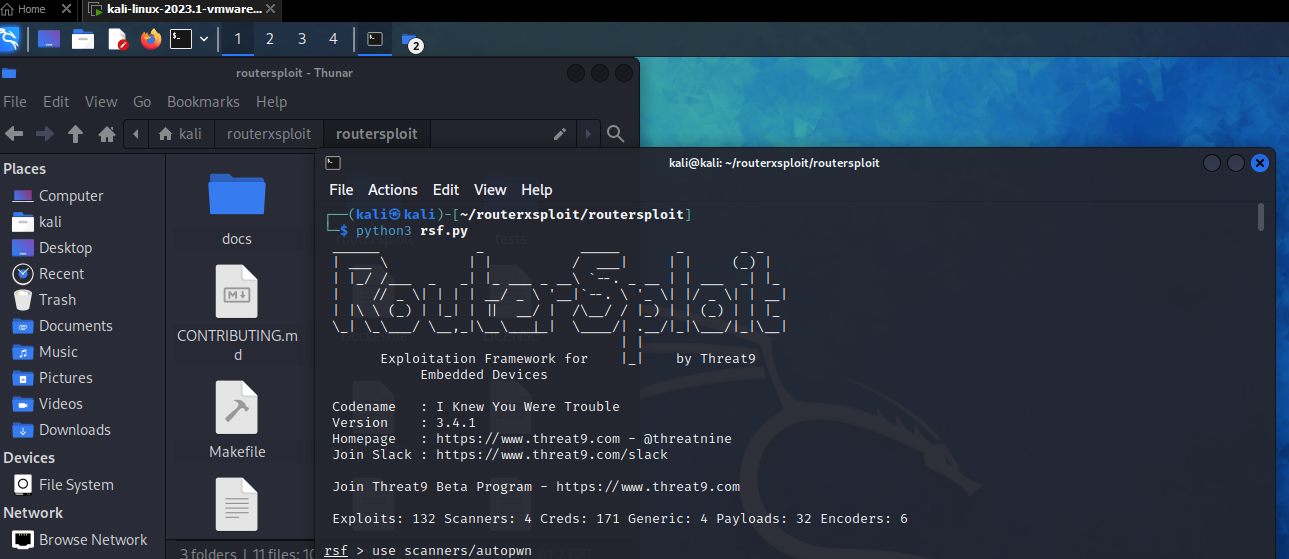


After a little bit of waiting, I got the password:



## Router exploitation

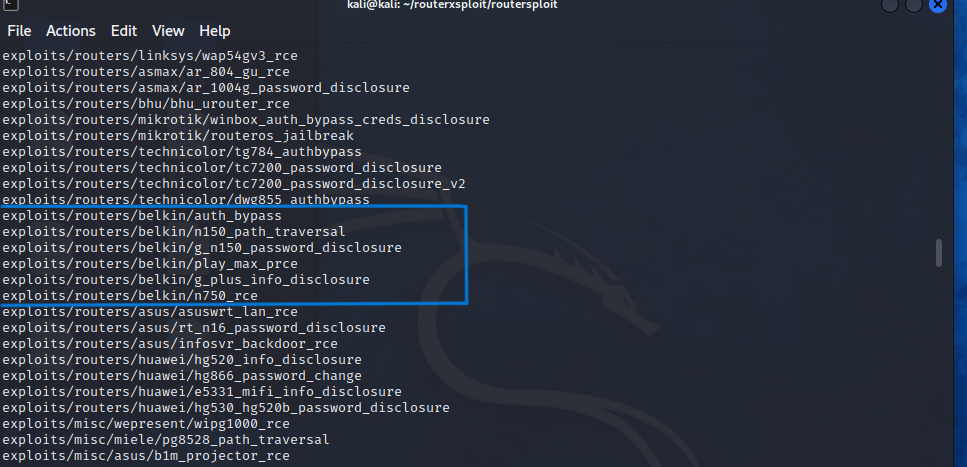
For this attack I had to install “RouterSploit” tool and run it in order to check if it is ready for work.



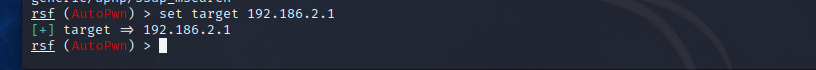
I wanted to see all possible exploits, which I could find for the router. I run a specific command, which allowed me to see all the possibilities.



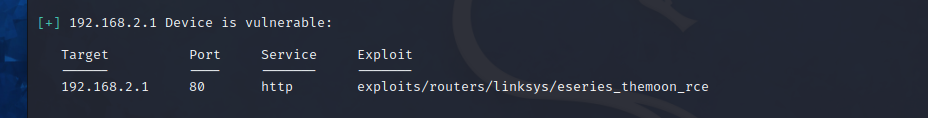
I managed to see that there are some exploits for my Router.



Then I needed to set the target IP, which in my case was 192.168.2.1, and just type the command ‘run’ to start the tool for scanning for possible exploits.

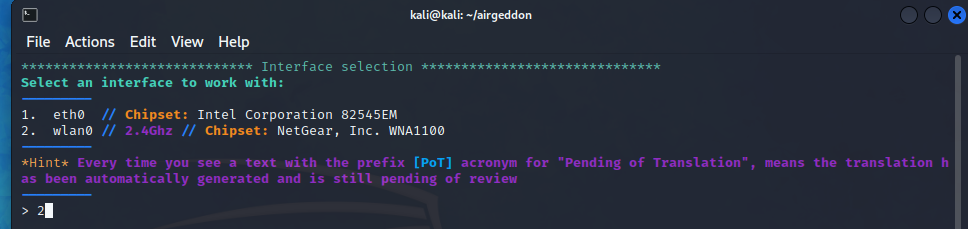


After several minutes waiting I got the result, and it is showing there is one vulnerability. I made a little research and it turns out that is a vulnerability for Linksys routers, which is strange because mine is not on that brand. The exploit is “The Moon worm”, which connects to ports 80 and 8080. The worm sends the HNAP request in order to identify the router's model and firmware version. If it determines that a device is vulnerable, it sends another request to a particular CGI script (this script has an authentication bypass vulnerability) that allows the execution of local commands on the device.

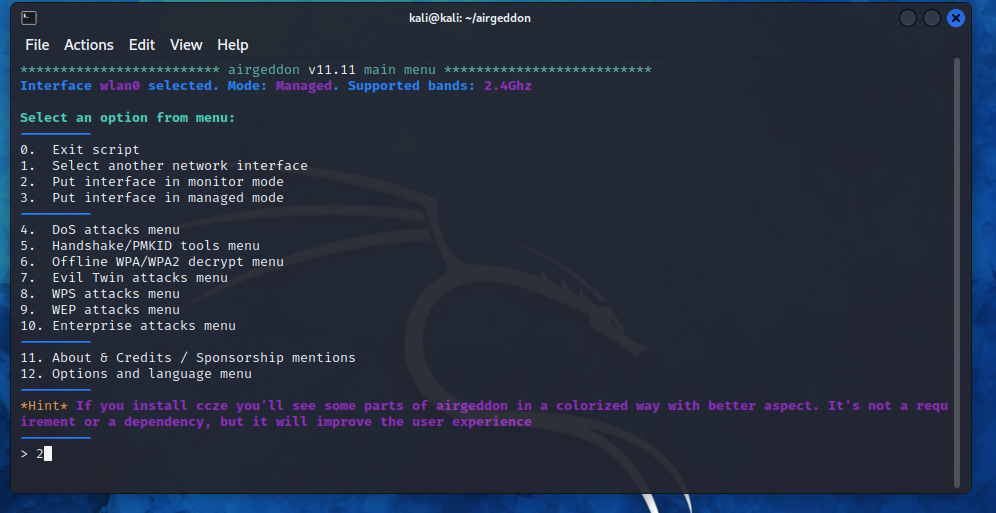


## Phishing attack

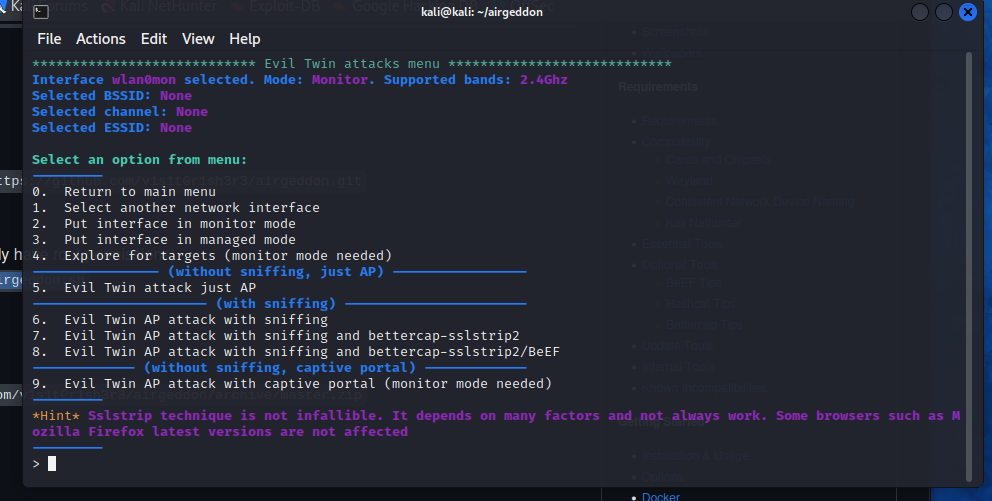
For this attack I needed the tool “Airegoddon”, which I downloaded and install from Git. After everything was set up, I start the tool and I was ready for the attack. Important thing is to use the WIFI adapter.



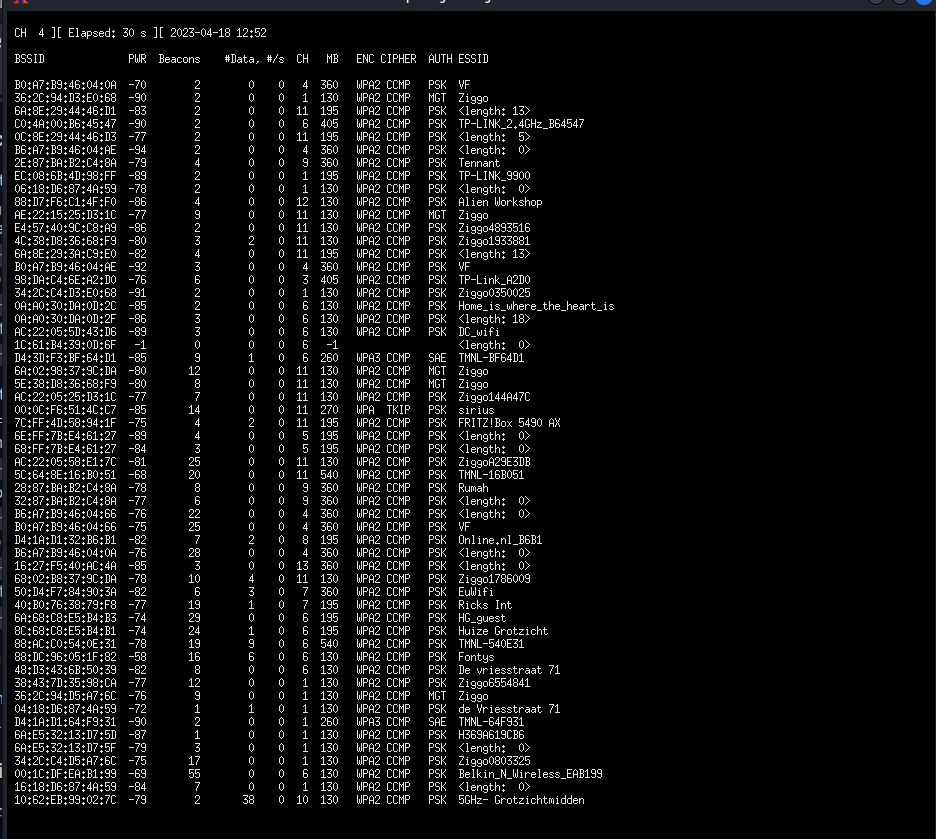
The first thing to do is to enter in monitor mode because it will allow me to see wireless connections around me.



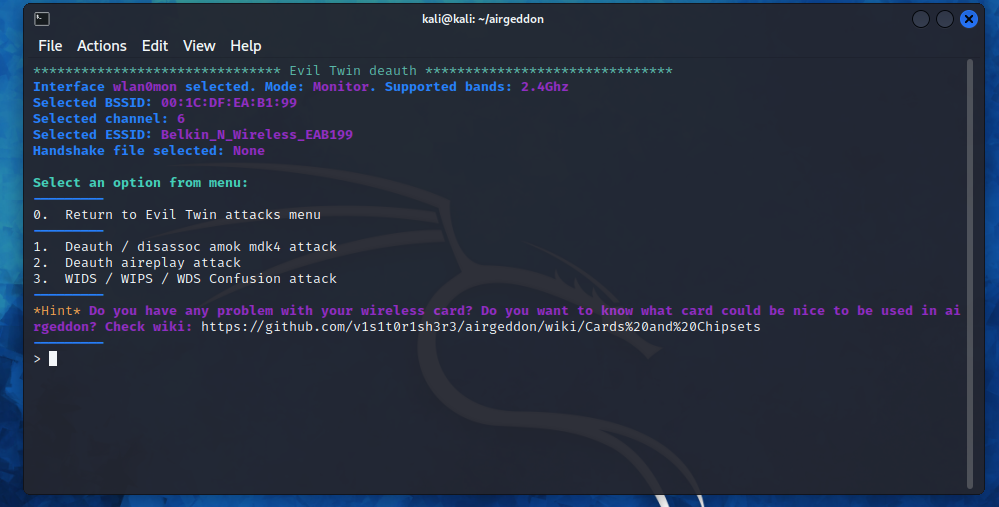
There are a lot of options of attacks that you can perform with this tool, but I continued with selecting Evil Twin attacks menu, which had also a lot of options to choose from.



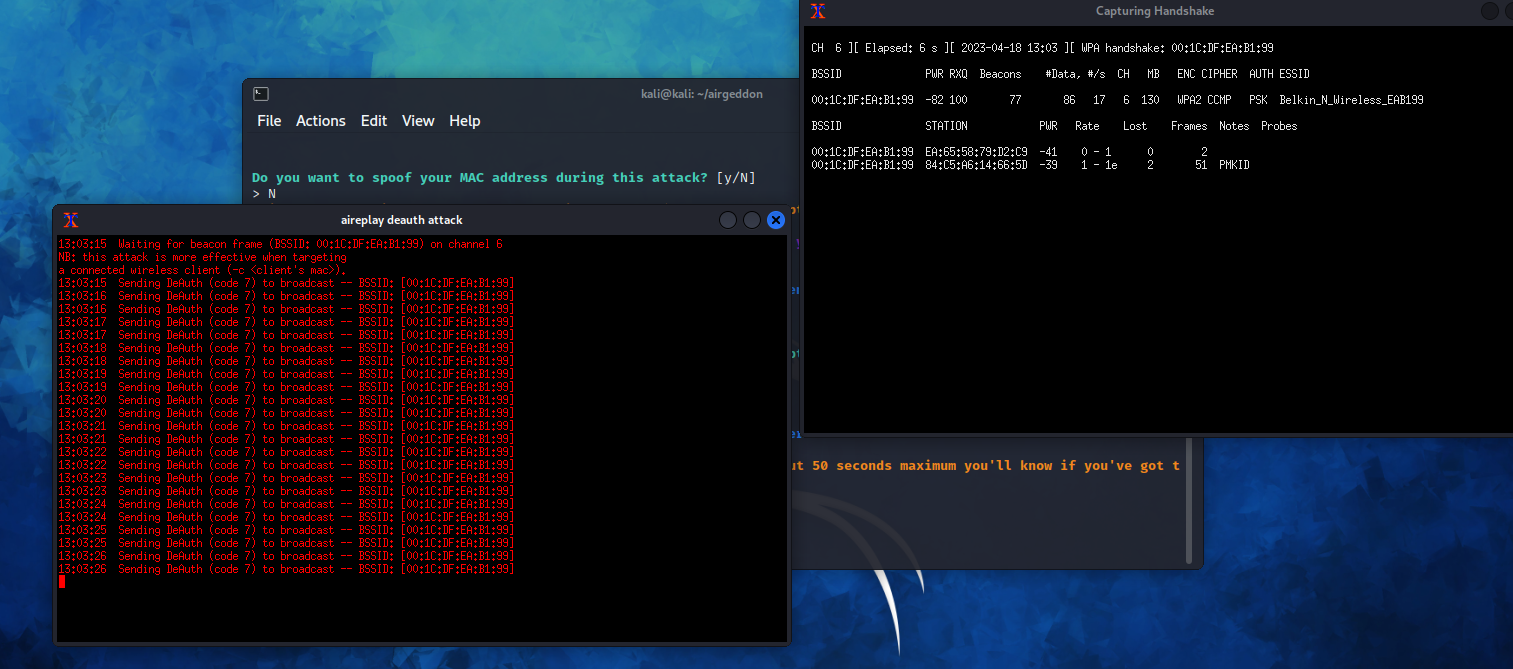
The next step I needed to choose was the Evil Twin AP attack with captive portal. From there I needed to explore the targets, I selected it and It showed a list with all detected networks. I saw my target’s name “Belkin\_N\_Wireless\_EB199”, and I selected it.



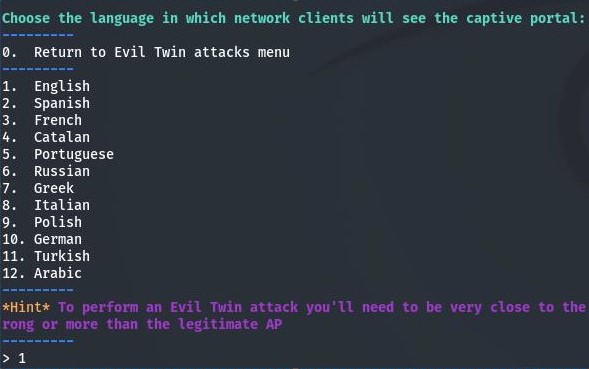
When the target is selected, I had to perform Deauth aireplay attack, which I also perform in my first attack.



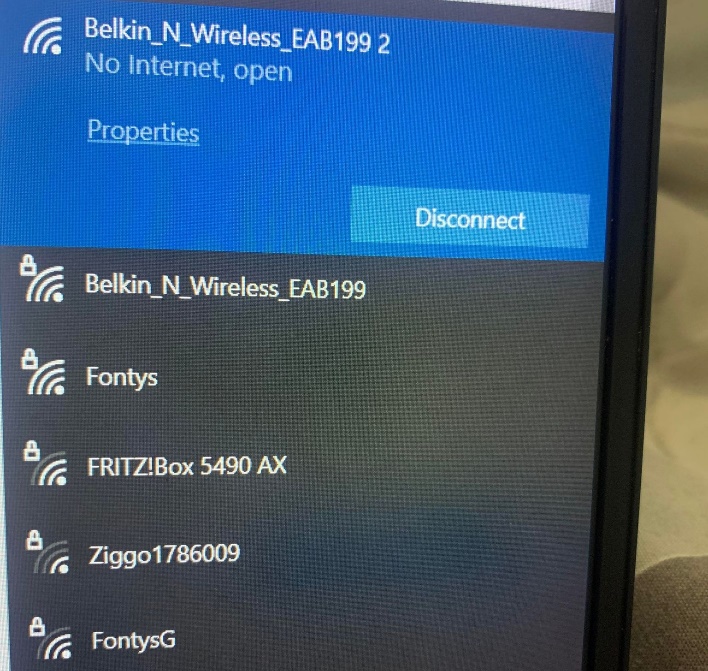
After launching the attack i waited a little bit to capture the handshake. This is very important step.

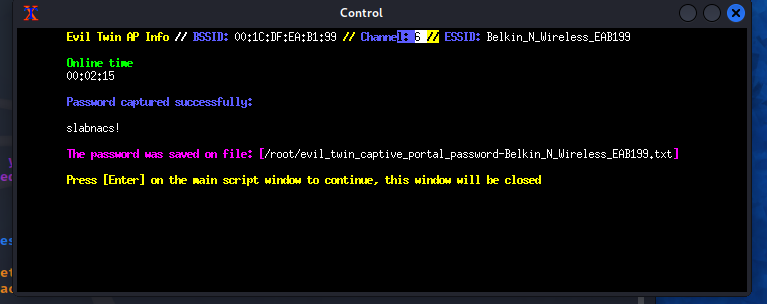


When the handshake was captured, the final step was here- I had to set up the phishing page (it is provided by the tool).



After setting up the page, I had 6 consoles, which were gathering information about who joins the network and to capture the password. On my other laptop I saw exact replica of the WIFI, which I was attacking. It did not allow to join in the real one, so I join the fake one. I was redirected to the browser where it asked for the WIFI password. This was monitored by the hacking tool and when the WIFI password is typed, it will pop up a window with the password.





# Conclusion

l could say that l definitely managed to find vulnerabilities, which was connected with the router. l could say that WPA/WPA2 are vulnerable to wireless attacks. WPA has a less secure encryption method and requires a shorter password, making it the weaker option. WPA2 is an updated version of WPA that uses AES encryption and long passwords to create a secured network. WPA2 has personal and enterprise options, making it ideal for home users and businesses. However, it needs a significant amount of processing power so if someone have an old device, it may be slow or not work at all. Talking more about WPA2 is vulnerable, when for example someone uses weak passwords for the WIFI. The fact that l managed to hacked without it having the password is thing that l considered and certainly l used old router, which probably is outdated for this time. Also, every router has his exploits in my case l was able to find available for Belkin, but l was impressed that my router was not vulnerable to them. The only exploit that was found for my router was “The moon warm”, which is very common exploit for Linksys models, not for the Belkin ones. Another attack, which l managed to do was creating WIFI, but fake one. It looks exactly the same as the real one and l was also forcing them to join the fake network. In that way, immediately after joining it they were redirected to a browser asking them for the password, which looked like hotspot networks. The attack was not stopping until the users putting the correct password.

Overall, it was enjoyable writing about this topic. l believe that my project was on a good level with different types of attacks. l managed to create plan to follow and also did some good researching in order to be able to hold the correct path. l was very interested in doing this kind of project, where l had my responsibility to choose the device, then research for it and do different attacks. l believe with l was developed my research skills even more.