© Journal of the Technical University - Sofia
Plovdiv branch, Bulgaria
"Fundamental Sciences and Applications"
Vol. 26, 2020

Wireless Network Password Cracking with Evil Twin Attack

Senol Sen and Tarık Yerlikaya

Trakya University Balkan Campus Information Technologies Department
Edirne/Turkey

senolsen@trakya.edu.tr, tarikyer@trakya.edu.tr

Abstract. With the increasing popularity of wireless network technology, security is becoming more and more important. The convenience provided by the increasing importance of portable systems, increased the popularity of wireless networks. Wireless networks are more vulnerable to security weaknesses in structure than wired networks because the data is circulating in the air. It is very easy for an attacker who listens to the air to obtain the data in the air with today's technological facilities. We can define Evil Twin Attack, which is one of the effective attack methods and based on social engineering attack, to broadcast a fake access point by broadcasting the same SSID as the victim's SSID name and obtaining the Wi-Fi password by connecting the victim to this broadcast. While a more technical user can detect this attack, it is a surprisingly effective attack against those who are not trained in searching suspicious network activity. In our study, this attack method is explained and the main protection methods that can be taken are mentioned.

1. Introduction

It has become one of the important issues in ensuring the security of corporate structures by using wireless networks effectively. An attacker who can leak into wireless networks can easily be aware of any activities carried out within the network without the need for physical access.

A bad twin attack is a type of Wi-Fi attack that works, taking advantage of the fact that most computers and phones will only see the "name" or SSID of a wireless network. This is actually very difficult to distinguish between networks that have the same name and have the same type of encryption. In fact, many networks have many network access points that use the same name to extend access without confusing users. For example, if you want to simply see how this attack works, you can create a Wi-Fi hotspot on your phone and name it the same as your home network and realize how difficult it is to understand the difference between the two networks.

2. Technologically Assisted Social Engineering

This is great for fooling a user if we have a network with the same name, same password, and same encryption, but if we don't know the password yet, we will first need to get the password from the victim. Since we don't have the password, we won't be able to create a network that will allow the victim to automatically connect, but we can try a social engineering attack to force the user out of the real network and give us the password. In a secret portal-style evil twin attack, we will perform the wireless attack using the Airgeddon tool to force the user to connect to an open network with the same name they trust. A captive portal is a page that you see when you connect to an open network in a coffee shop, an airport or a hotel and asks you to enter a password. This page with terms and

Online ISSN 2603-459X

conditions is actually a phishing page that users use to connect and looks like the interface of the router [1].

The Wi-Fi network, which is primarily reliable in the attack, is filled with authentication packages, making it impossible to connect to the internet normally. Then, when the victim encounters an internet connection that refuses to connect and does not allow any internet access, it will discover and direct to an open Wi-Fi network with the same name as the network it cannot connect to.

Once connected to the network, the victim is redirected to a phishing page stating that the router has been updated and requires a password to continue. If the user knows this password, he will enter the network password here, but if our victim is disturbed by this event and writes the wrong password, we can say the correct password incorrectly. To do this, we will first pull a handshake from the network so that we can check every password the user has given us and say this when he enters the correct one.

In short, the attack steps will be as follows:

1. Scan Network
2. Select Target
3. Handshake data is being collected.
4. A fake ap (fake access point) with the same name is created on the same channel on the same SSID.
5. DHCP server is installed on the access point.
6. A dns server is being set up to direct all requests to the host.
7. A mechanism is created to compare the passwords entered in the web interface with the handshake data.
8. Deauth packages are sent to the clients on the network and they are thrown from the network.
9. The victim is expected to be trapped and appears on your screen as soon as you enter the password correctly and the access point with the fake SSID is closed [2].

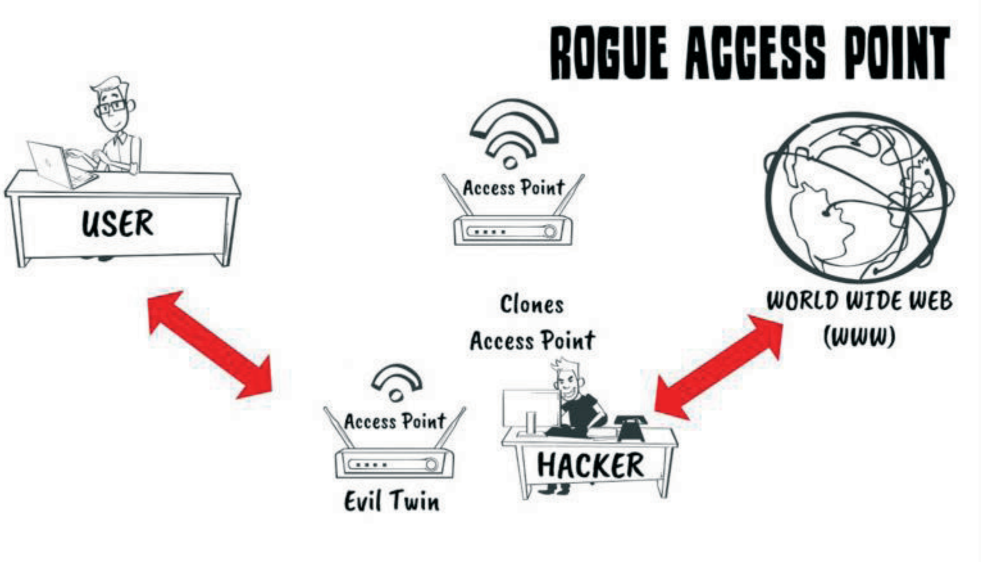
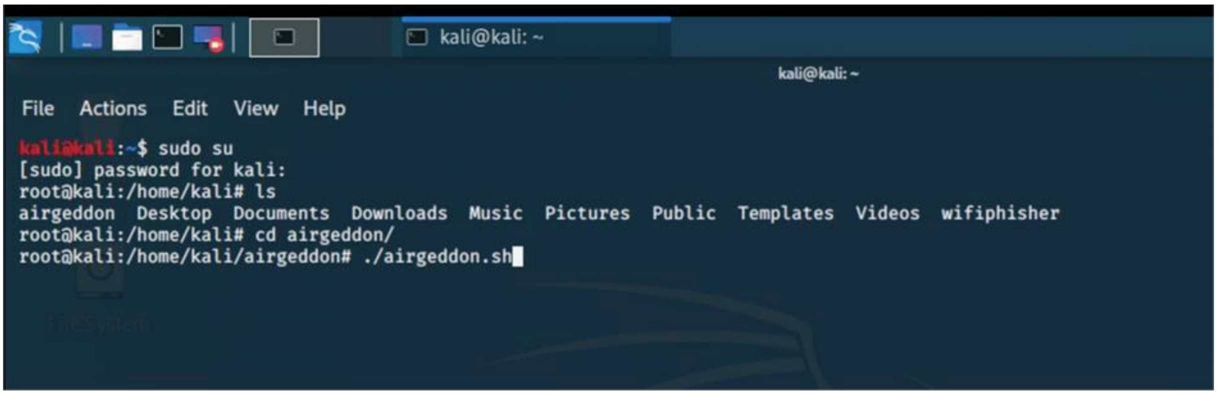


Figure 1. Wifi Evil Twin Attack

3. Example attack

We will use the Airgeddon tool on Kali Linux to prepare our nasty twin access point attack. We will install the related tool from the git hub using the following commands and install all the packages required for the tool to work in our system. We run the following commands respectively and install our attack tool.

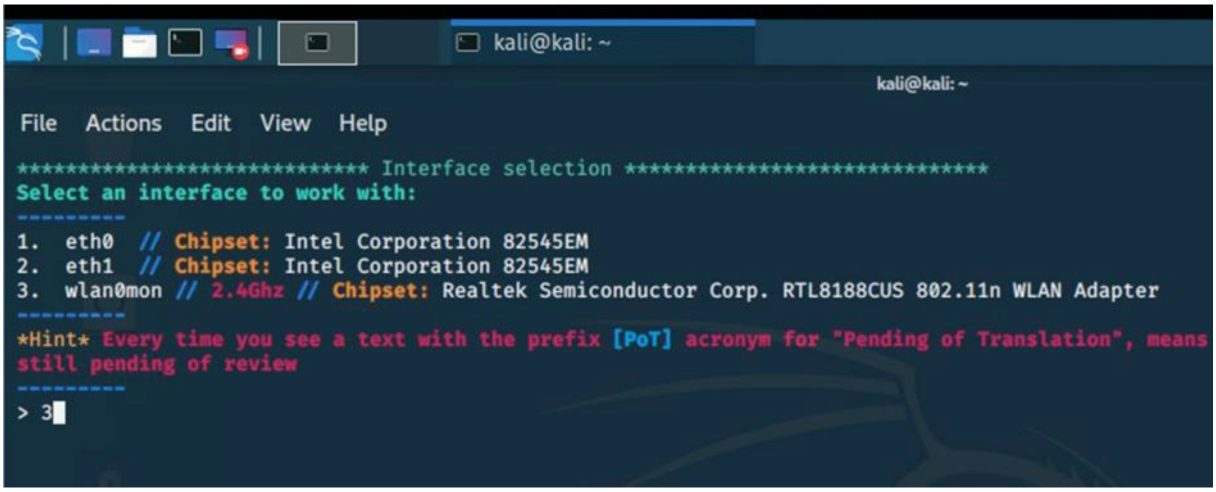
- git clone github.com/v1s1t0r1sh3r3/airgeddon.git
- cd airgeddon
- sudo bash ./airgeddon.sh



```
kali@kali:~$ sudo su
[sudo] password for kali:
root@kali:/home/kali# ls
airgeddon  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  wifiphisher
root@kali:/home/kali# cd airgeddon/
root@kali:/home/kali/airgeddon# ./airgeddon.sh
```

Figure 2. Installing the Airgeddon tool in Kali Linux

Then all packages are made sure that they are fully installed and the script is run. Then, we select our Wireless network adapter from the screen we see. In our example, our wireless adapter is seen and selected in option 3.



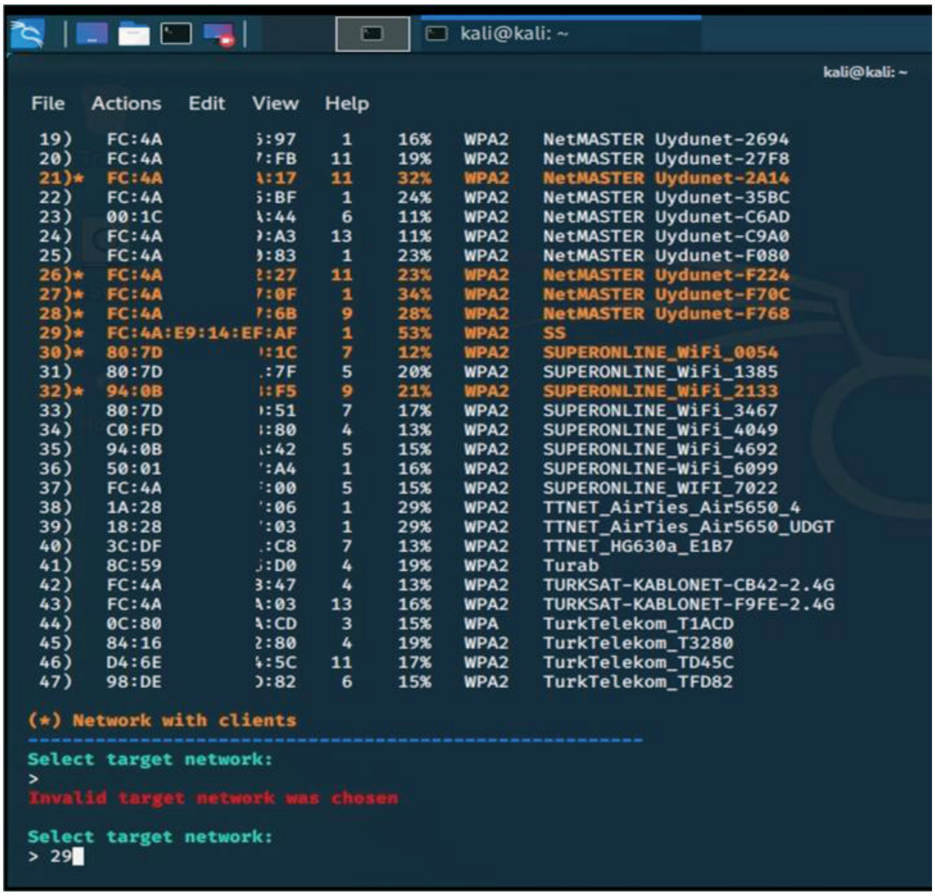
```
***************************** Interface selection ******************************
Select an interface to work with:
---------
1.  eth0  // Chipset: Intel Corporation 82545EM
2.  eth1  // Chipset: Intel Corporation 82545EM
3.  wlan0mon // 2.4Ghz // Chipset: Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means
still pending of review
---------
> 3
```

Figure 3. Wireless adapter selection screen

From the next menu, we select option 2 to switch our Wireless card to monitor mode.

Then we select the 7th option for the "Evil Twin attacks" menu from the same screen and we select the "Evil Twin AP attack with captive portal" option 9, from the bottom menu of this attack module.

The scan will start and after about 60 seconds, a list of destinations will appear in a small window in the upper right. The networks used will have an asterisk next to it and you will be asked to enter the target number of the network you want to attack.



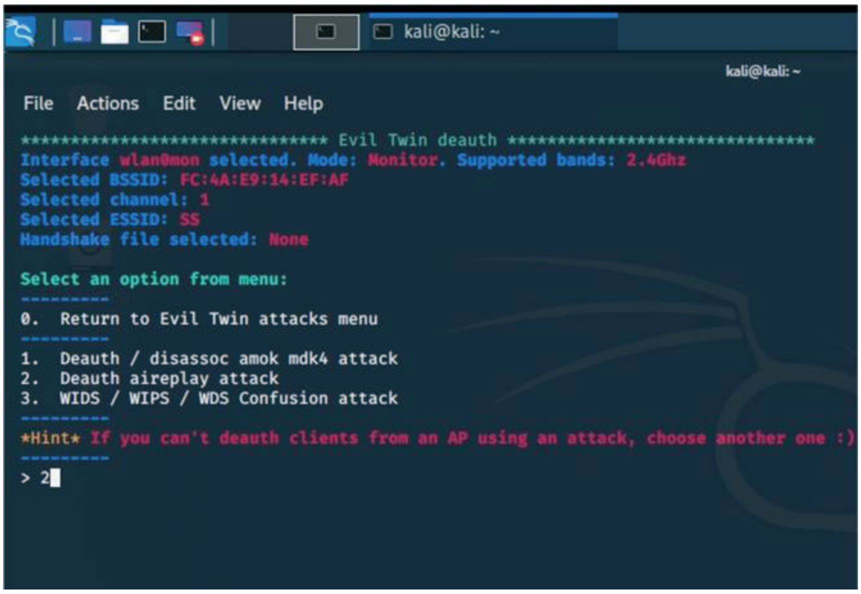
```
 19)   FC:4A        5:97    1    16%   WPA2   NetMASTER Uydunet-2694
 20)   FC:4A        7:FB   11    19%   WPA2   NetMASTER Uydunet-27F8
 21)*  FC:4A        A:17   11    32%   WPA2   NetMASTER Uydunet-2A14
 22)   FC:4A        5:BF    1    24%   WPA2   NetMASTER Uydunet-35BC
 23)   00:1C        A:44    6    11%   WPA2   NetMASTER Uydunet-C6AD
 24)   FC:4A        9:A3   13    11%   WPA2   NetMASTER Uydunet-C9A0
 25)   FC:4A        9:83    1    23%   WPA2   NetMASTER Uydunet-F080
 26)*  FC:4A        2:27   11    23%   WPA2   NetMASTER Uydunet-F224
 27)*  FC:4A        7:0F    1    34%   WPA2   NetMASTER Uydunet-F70C
 28)*  FC:4A        7:6B    9    28%   WPA2   NetMASTER Uydunet-F768
 29)*  FC:4A:E9:14:EF:AF    1    53%   WPA2   SS
 30)*  80:7D        1:1C    7    12%   WPA2   SUPERONLINE_WiFi_0054
 31)   80:7D        .:7F    5    20%   WPA2   SUPERONLINE_WiFi_1385
 32)*  94:0B        1:F5    9    21%   WPA2   SUPERONLINE_WiFi_2133
 33)   80:7D        1:51    7    17%   WPA2   SUPERONLINE_WiFi_3467
 34)   C0:FD        1:80    4    13%   WPA2   SUPERONLINE_WiFi_4049
 35)   94:0B        1:42    5    15%   WPA2   SUPERONLINE_WiFi_4692
 36)   50:01        ':A4    1    16%   WPA2   SUPERONLINE-WiFi_6099
 37)   FC:4A        ::00    5    15%   WPA2   SUPERONLINE_WIFI_7022
 38)   1A:28        ':06    1    29%   WPA2   TTNET_AirTies_Air5650_4
 39)   18:28        ':03    1    29%   WPA2   TTNET_AirTies_Air5650_UDGT
 40)   3C:DF        .:C8    7    13%   WPA2   TTNET_HG630a_E1B7
 41)   8C:59        5:D0    4    19%   WPA2   Turab
 42)   FC:4A        3:47    4    13%   WPA2   TURKSAT-KABLONET-CB42-2.4G
 43)   FC:4A        A:03   13    16%   WPA2   TURKSAT-KABLONET-F9FE-2.4G
 44)   0C:80        A:CD    3    15%   WPA    TurkTelekom_T1ACD
 45)   84:16        2:80    4    19%   WPA2   TurkTelekom_T3280
 46)   D4:6E        4:5C   11    17%   WPA2   TurkTelekom_TD45C
 47)   98:DE        0:82    6    15%   WPA2   TurkTelekom_TFD82

(*) Network with clients
------------------------------------------------------------
Select target network:
>
Invalid target network was chosen

Select target network:
> 29
```

Figure 3. Selecting the SSID to attack

Since we will test our own network, SS network, we continue by choosing our target number 29. Now we will choose the type of authentication attack we want to use to expel the user from his trusted network. We select the second option as "Deauth aireplay attack" and start the process.



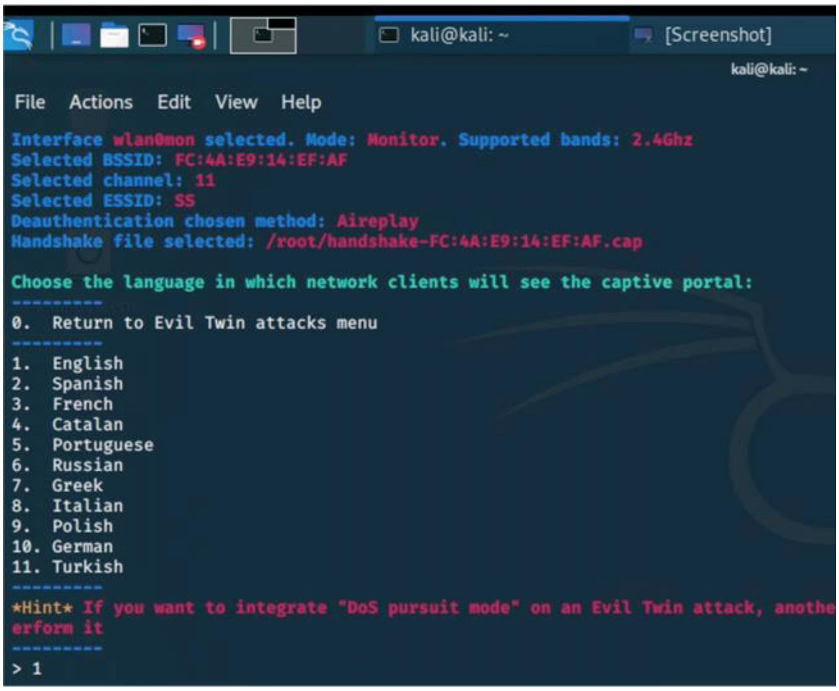
```
******************************** Evil Twin deauth ********************************
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: FC:4A:E9:14:EF:AF
Selected channel: 1
Selected ESSID: SS
Handshake file selected: None

Select an option from menu:
---------
0.  Return to Evil Twin attacks menu
---------
1.  Deauth / disassoc amok mdk4 attack
2.  Deauth aireplay attack
3.  WIDS / WIPS / WDS Confusion attack
---------
*Hint* If you can't deauth clients from an AP using an attack, choose another one :)
---------
> 2
```

Figure 4. Choice of attack type

In the next step, we will need a handshake package to enable us to check the password that the user enters through the fake password portal, which we will use to get the password. For this purpose, we need to get a handshake package. Then the file of the handshake package we captured is saved. Then, we choose the place where we will write the stolen password and configure the phishing page to go to the last step.

In the last step before starting the attack, we will set the language of the phishing page. The page provided by Airgeddon is well suited for testing this style of attack. In this example, we will select 1 for English. Once you have made your choice, all of the under attack windows will open and start at the same time to perform various functions of the attack.



```
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: FC:4A:E9:14:EF:AF
Selected channel: 11
Selected ESSID: SS
Deauthentication chosen method: Aireplay
Handshake file selected: /root/handshake-FC:4A:E9:14:EF:AF.cap

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
---------
*Hint* If you want to integrate "DoS pursuit mode" on an Evil Twin attack, anothe
erform it
---------
> 1
```

Figure 5. Setting up the phishing page

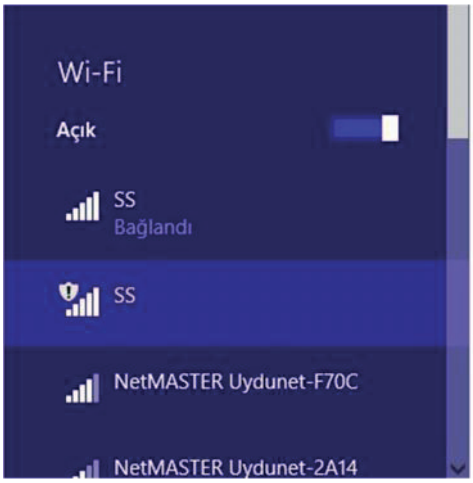
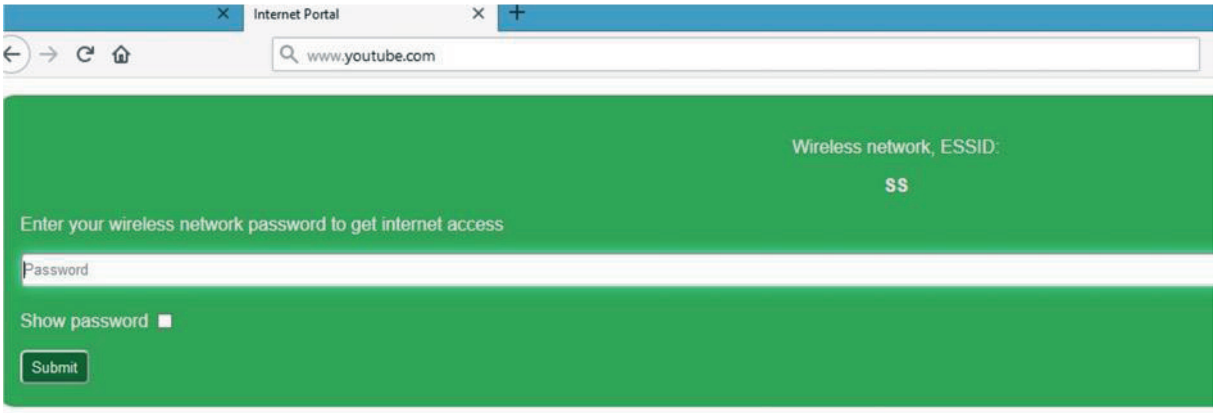


Figure 6. Broadcast of the fake twin access point

While the attack continues, the victim must be expelled from the existing WiFi network and forced to connect to the false twin access point. When the victim tries to connect to the fake SSID, which is a twin, it will be thrown from its current connection, and will come across a screen to ask for a password like below.



Wireless network, ESSID:

SS

Enter your wireless network password to get internet access

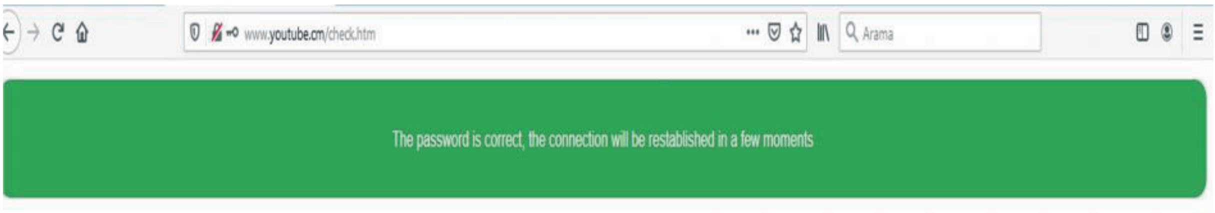
Password

Show password □

Submit

Figure 7. Password login screen of fake SSID network

When the victim is connected to our fake network, a password entry screen will appear as in the picture above. Thanks to the handshake packages we have collected, the process of asking for the password will continue until the victim enters the correct password, and all internet requests will fail until the correct password is entered.

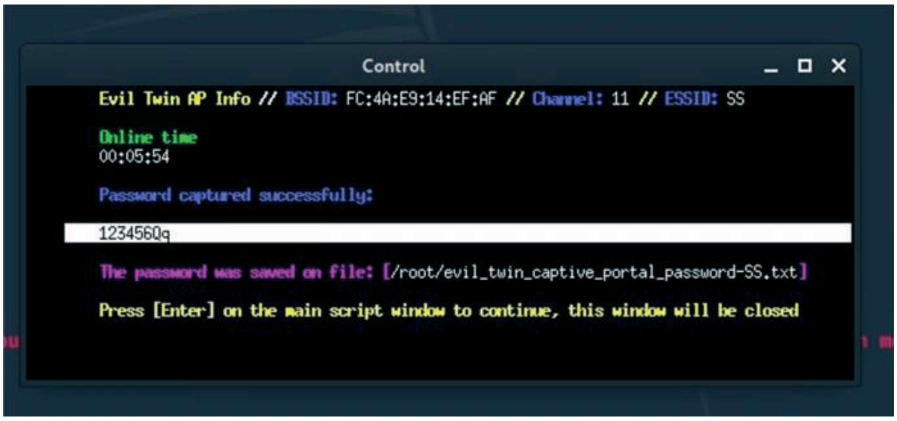


The password is correct, the connection will be restablished in a few moments

Figure 8. Correct password screen

When our victim finally enters the correct password, all the windows will be closed except for the window showing the password. The fake network will disappear and the victim will be free to reconnect to the trusted wireless network.

The found password is displayed on the screen below and saved in the script of the related path.



```
Evil Twin AP Info // BSSID: FC:4A:E9:14:EF:AF // Channel: 11 // ESSID: SS

Online time
00:05:54

Password captured successfully:

1234560q

The password was saved on file: [/root/evil_twin_captive_portal_password-SS.txt]

Press [Enter] on the main script window to continue, this window will be closed
```

Figure 9. Captured password screen

4. Results

With the increasing popularity of wireless network technology, security is becoming more and more important. The convenience provided by the increasing importance of portable systems, increased the popularity of wireless networks. Wireless networks are more vulnerable to security weaknesses in structure than wired networks because the data is circulating in the air. It is very easy for an attacker who listens to the air to obtain the data in the air with today's technological facilities. We can define Evil Twin Attack, which is one of the effective attack methods and based on social engineering attack, to broadcast a fake access point by broadcasting the same SSID as the victim's SSID name and obtaining the Wi-Fi password by connecting the victim to this broadcast. While a more technical user can detect this attack, it is a surprisingly effective attack against those who are not trained in searching suspicious network activity.

For Wi-Fi users, an evil twin AP is nearly impossible to detect because the SSID appears legitimate and the attackers typically provide Internet service. In most cases, the best way to stay safe on unfamiliar Wi-Fi networks is to always use a VPN to encapsulate the Wi-Fi session in another layer of security [3].

One of the defenses you can make against this attack is to limit Mac addresses. You can set the limit of the devices you want to connect through the modem interface by registering the ip addresses on the mac and local so that other devices cannot connect even if the password is correct. As another solution, it is recommended to lower your Wifi range.

Businesses offering Wi-Fi to their employees and customers can use wireless intrusion prevention systems (WIPS) to detect the presence of an evil twin AP and prevent any managed corporate clients from connecting to them [3].

References

[1] Wifi Password Hijacking Evil Twin Attack *https://medium.com/@aattk/wifi-%C5%9Fifresi-ele-ge%C3%A7irme-evil-twin-attack-bc95c60a516b*

[2] Wireless Network Password Cracking by Creating a Fake Access Point (Evil Twin Attack) *https://ht4mer.wordpress.com/2017/04/16/sahte-erisim-noktasi-olusturarak-kablosuz-ag-sifresi-kirma-evil-twin-attack*

[3] Understanding Evil Twin AP Attacks and How to Prevent Them *https://www.darkreading.com/ attacks-breaches/ understanding-evil-twin-ap-attacks-and-how-to-prevent-them-/a/d-id/1333240*