Cracking WPA/WPA2 with Airgeddon using an Evil Twin Attack with a Captive Portal

Required:

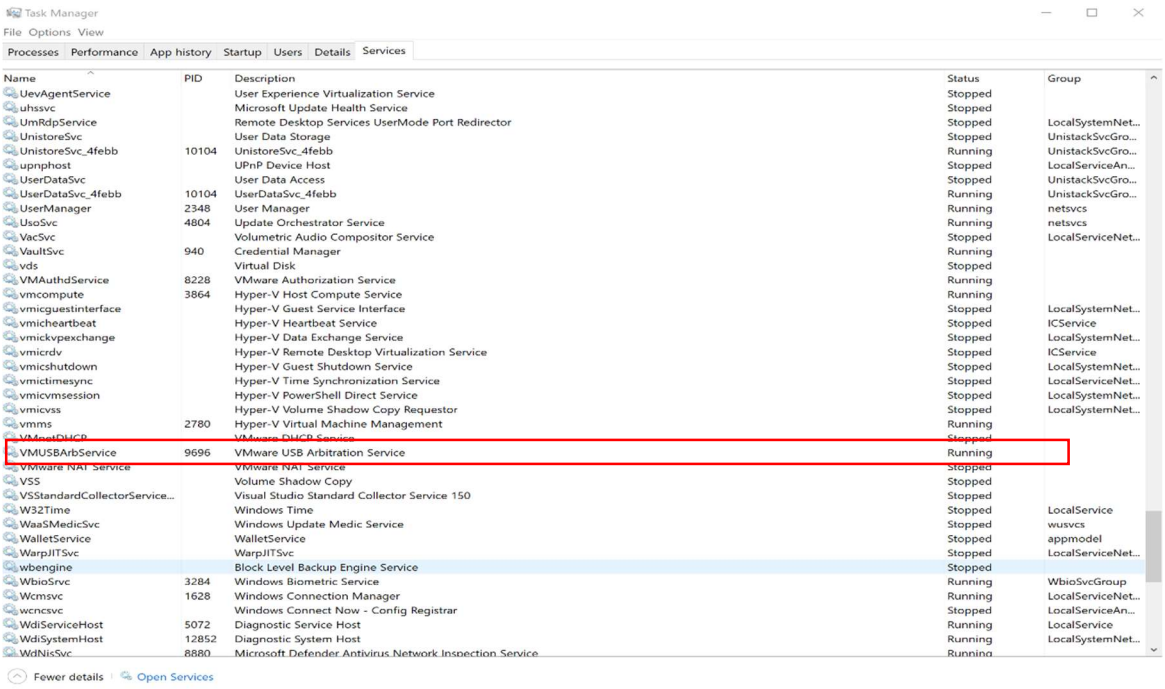
- WiFi adapter capable of packet injection
- Kali VM
- A target client (I will demonstrate using my host machine, but it could be a WiFi device capable of opening webpages)
- VMware

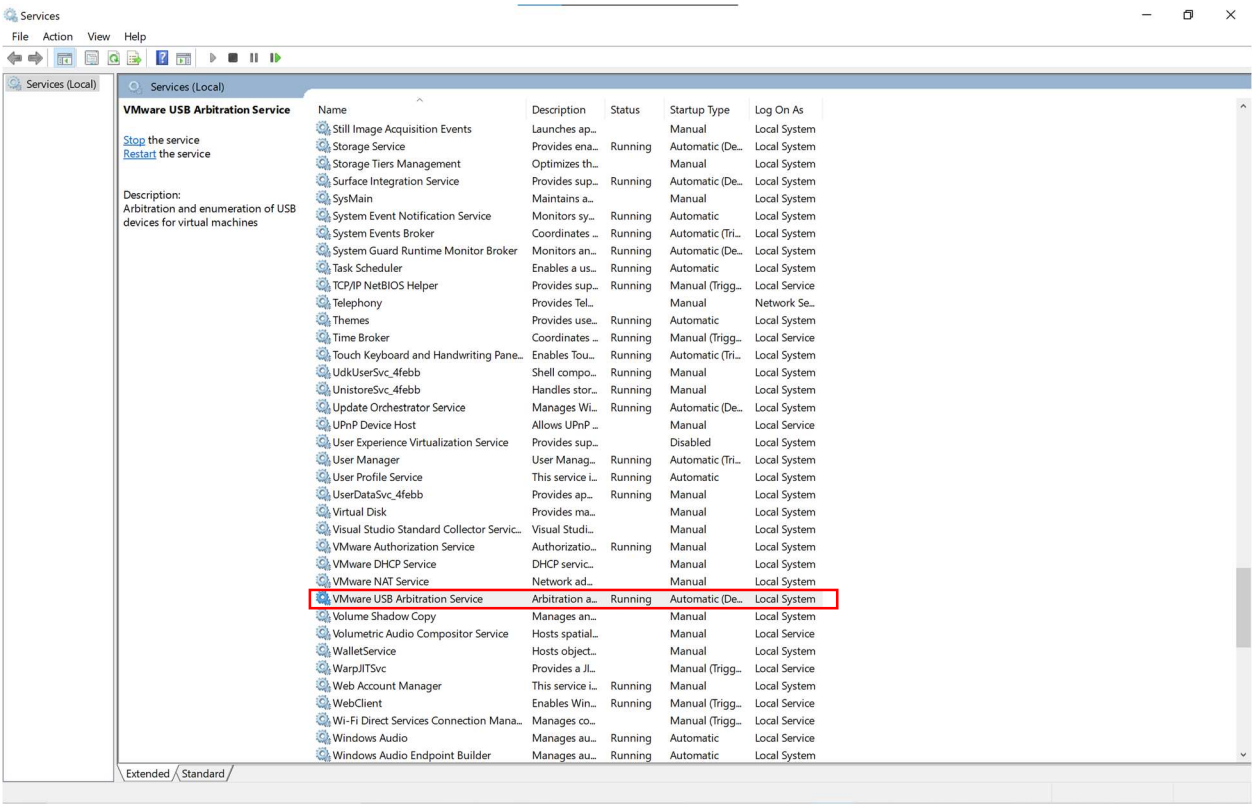
PART I: Setting up the Environment

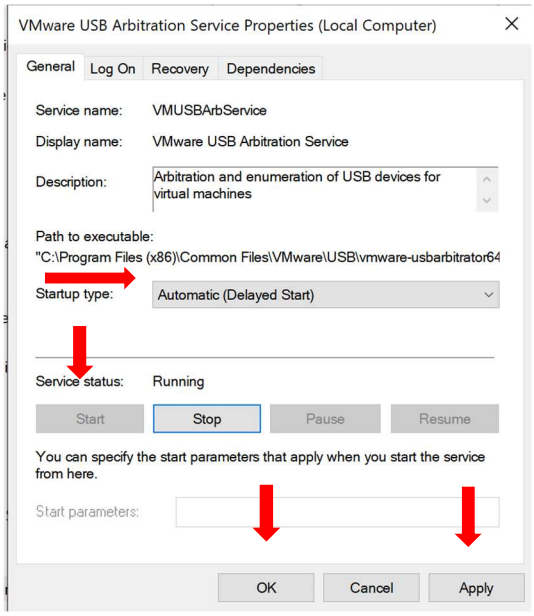
1) Plug in your external WiFi adapter to the computer

2) VMUSBArbService

   a. Check to ensure VMUSBArbService is running. To do so go to open Task Manager, then click on the Services tab. Scroll down until you find it. If it is running, you're good to go. If it is not running, right click it and select "open services". This will open a new window called Services. Scroll down until you find VMUSB Arbitration Service again, right click it and select properties. Change the Startup Type to Automatic or Automatic (Delayed Start) depending on your preference. Then click Start, Apply and Ok. Now we are good to go and should be able to use USB devices inside VMware.







3) Connect to a safe and secure WiFi network
    a. Preferably one with no one else on it as this lab will cause disruption to others using the network.

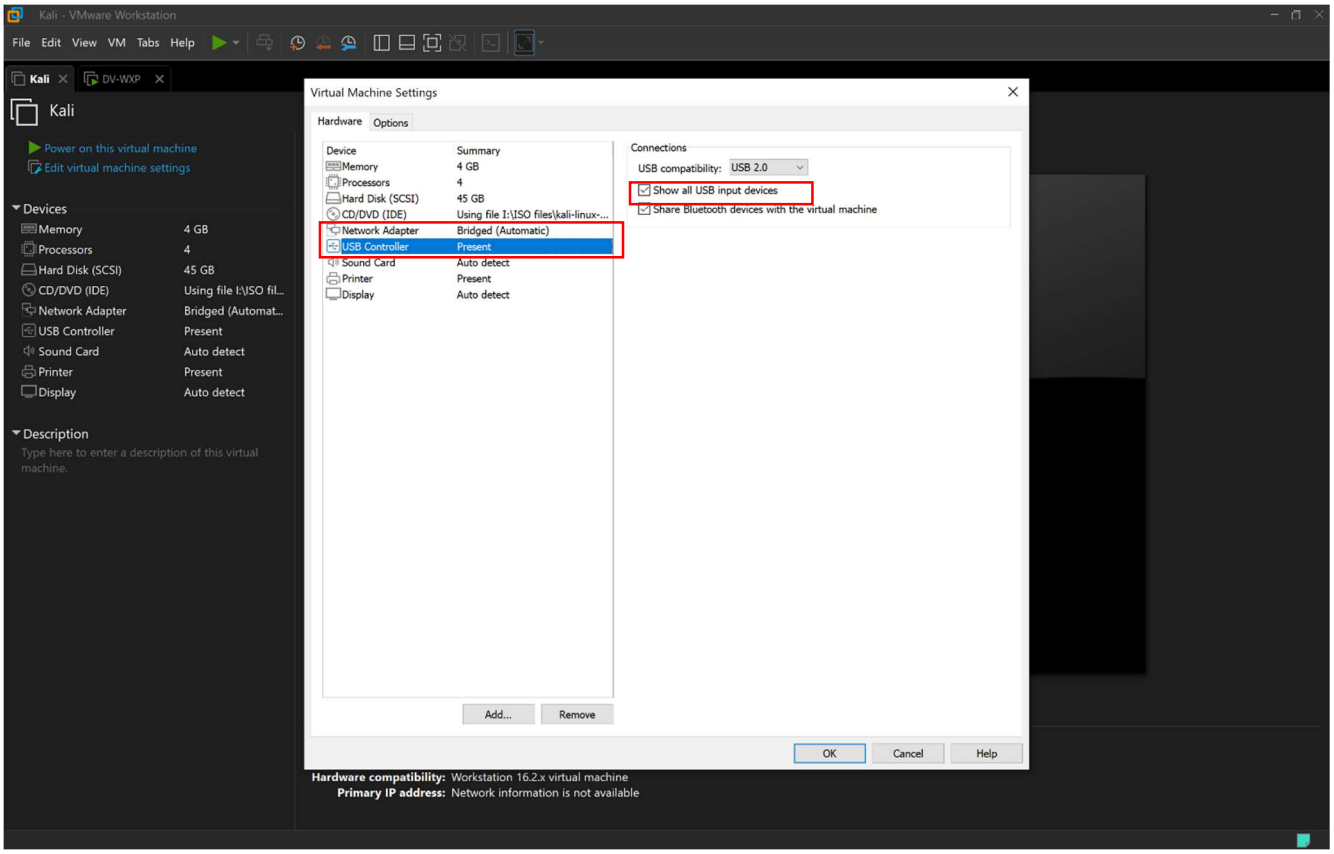
PART II: Setting Up Your Target

1) Connect your target to the network you will attack

PART III: Setting up the attack machine

1) Load Kali VM onto VMware

2) Settings
    a. Network Adapter
        i. Bridged Connection
    b. USB Controller
        i. “show all USB input devices” is checked.
        ii. If “USB Controller” is not present, click Add and add the option for “USB Controller”



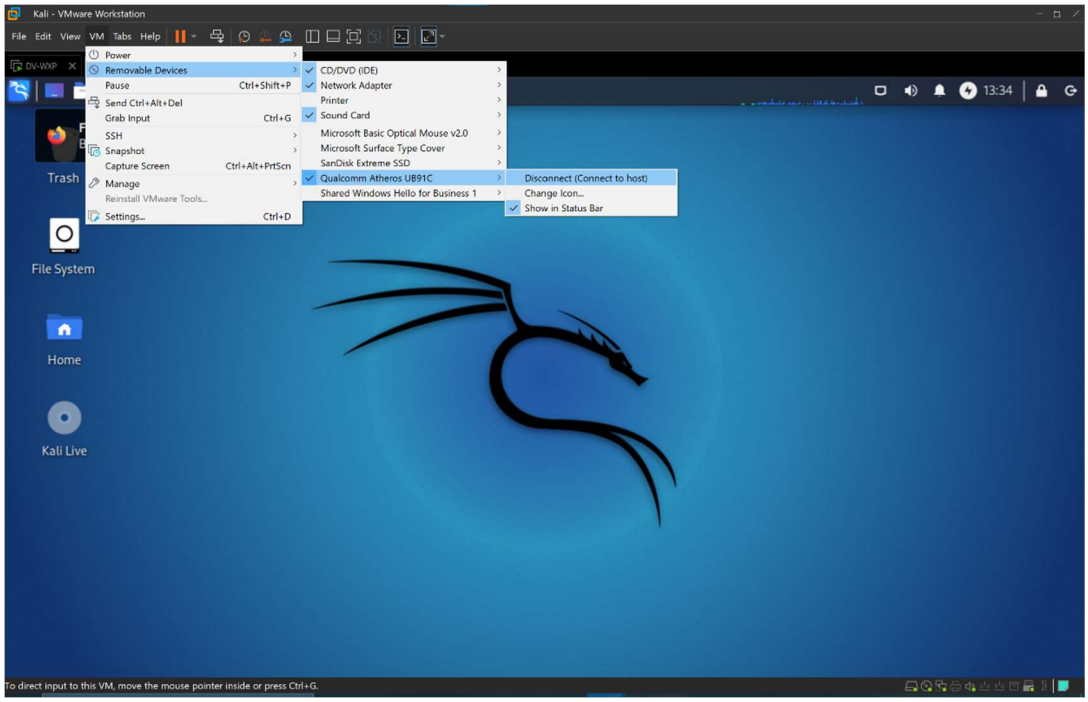
3) Boot up Kali and log in

PART IV: Downloading Airgeddon

1) On the Kali VM open a terminal and type the command:
    a. #cd /usr/share
    b. #sudo git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
        - Enter your password as required
        - (you may already have Airgeddon installed, if so that is fine. If not, continue with the installation and type “Y” when asked.)
    c. #cd Airgeddon

Part V: Plugging in the External Wifi Adapter

1) Click the VM tab on the top of the screen. Then Removable Devices, then hover over your external WiFi adapter and select Connect (Disconnect from Host). This will now enable you to use your external WiFi adapter inside the VM (Bonus trick: you can also use other USB devices if you enable them).



PART VI: Changing the MAC address on the Attack Machine (it's good OpSec)

1) Determine your wireless interface card name and shut it down

   #ifconfig

   - for me my interface card is "wlan0". Record your wireless interface card.
   - It more than likely will also be "wlan0" for you too. "eth0" is the bridged connection coming from the host machine being interpreted as a wired connection.

   #sudo ifconfig wlan0 down

   #ifconfig

```
┌──(user㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 47  bytes 7993 (7.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 9492 (9.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1014  bytes 108134 (105.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1014  bytes 108134 (105.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.177  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2603:300c:183c:e060:7492:aff1:13c2:64f0  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a4e0:4d56:d88:f6f0  prefixlen 64  scopeid 0x20<link>
        ether 00:c0:ca:99:5f:d7  txqueuelen 1000  (Ethernet)
        RX packets 27279  bytes 15860569 (15.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8628  bytes 1162497 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(user㉿kali)-[~]
└─$ sudo ifconfig wlan0 down

┌──(user㉿kali)-[~]
└─$
```

2) Changing the MAC address

#macchanger -s wlan0

#sudo macchanger -r wlan0

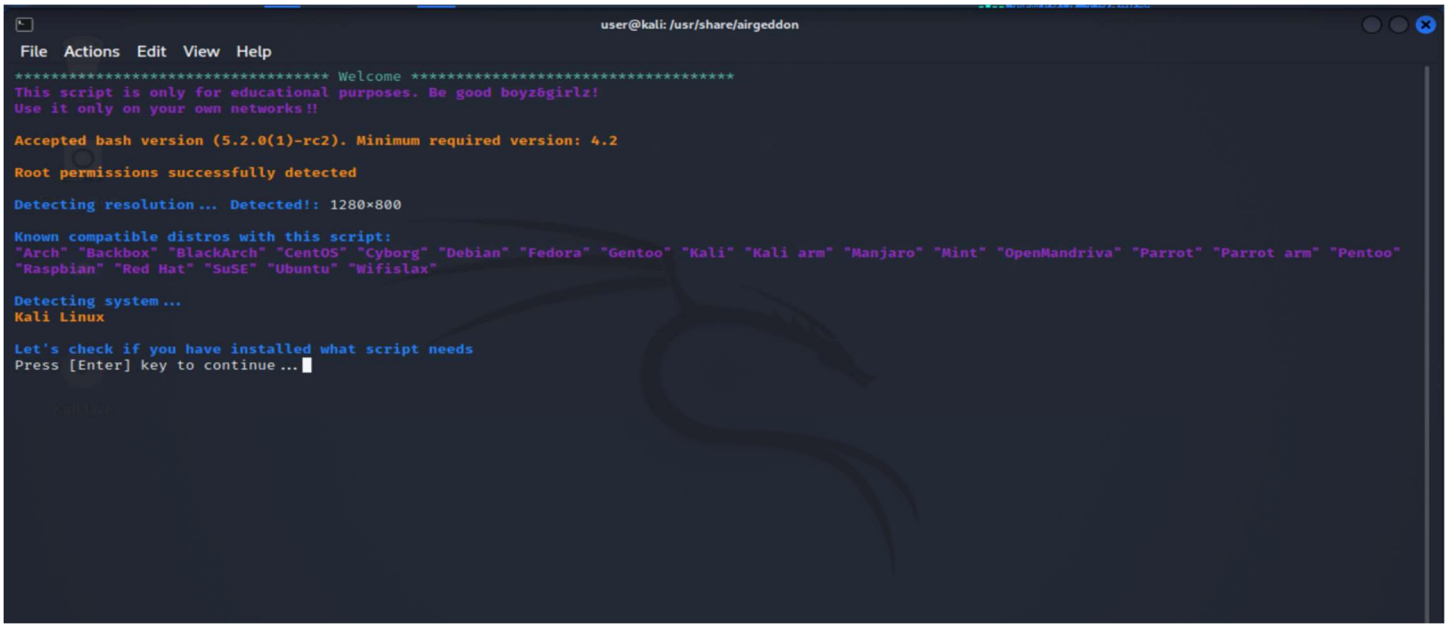
```
user@kali: ~
File  Actions  Edit  View  Help

┌──(user㉿kali)-[~]
└─$ macchanger -s wlan0
Current MAC:   00:c0:ca:99:5f:d7 (ALFA, INC.)
Permanent MAC: 00:c0:ca:99:5f:d7 (ALFA, INC.)

┌──(user㉿kali)-[~]
└─$ sudo macchanger -r wlan0
Current MAC:   00:c0:ca:99:5f:d7 (ALFA, INC.)
Permanent MAC: 00:c0:ca:99:5f:d7 (ALFA, INC.)
New MAC:       7a:7f:d5:b8:f9:91 (unknown)

┌──(user㉿kali)-[~]
└─$ macchanger -s wlan0
Current MAC:   7a:7f:d5:b8:f9:91 (unknown)
Permanent MAC: 00:c0:ca:99:5f:d7 (ALFA, INC.)

┌──(user㉿kali)-[~]
└─$
```

PART VII: Running Airgeddon

1) Run Airgeddon

#sudo ./airgeddon.sh

- After running this command, it will ask you press "Enter" to check if you have the right scripts installed
- You might be missing optional tools. Type "Y" to install.
- This process may take a few minutes and might not show when it is complete.
- After a few minutes and it seems "stuck", close the terminal, and try running Airgeddon again.
- You will be asked to press "Enter" several times you reach a new screen titled "Interface Selection".



2) Selecting the interface

   >2

   - For me I select 2, but make sure you select the correct interface card you recorded earlier

3) Putting the Interface Card in monitor mode

   >2

   - press "Enter"

4) Selecting the Evil Twin Attack Menu

   >7

5) Evil Twin Attack Option selection and start scanning for targets

   >9

   - press "Enter" to start the scan

6) Find the target

   -When you see your network SSID in the new window that you want to perform the attack on, hit "Ctrl + C" to stop the scan.

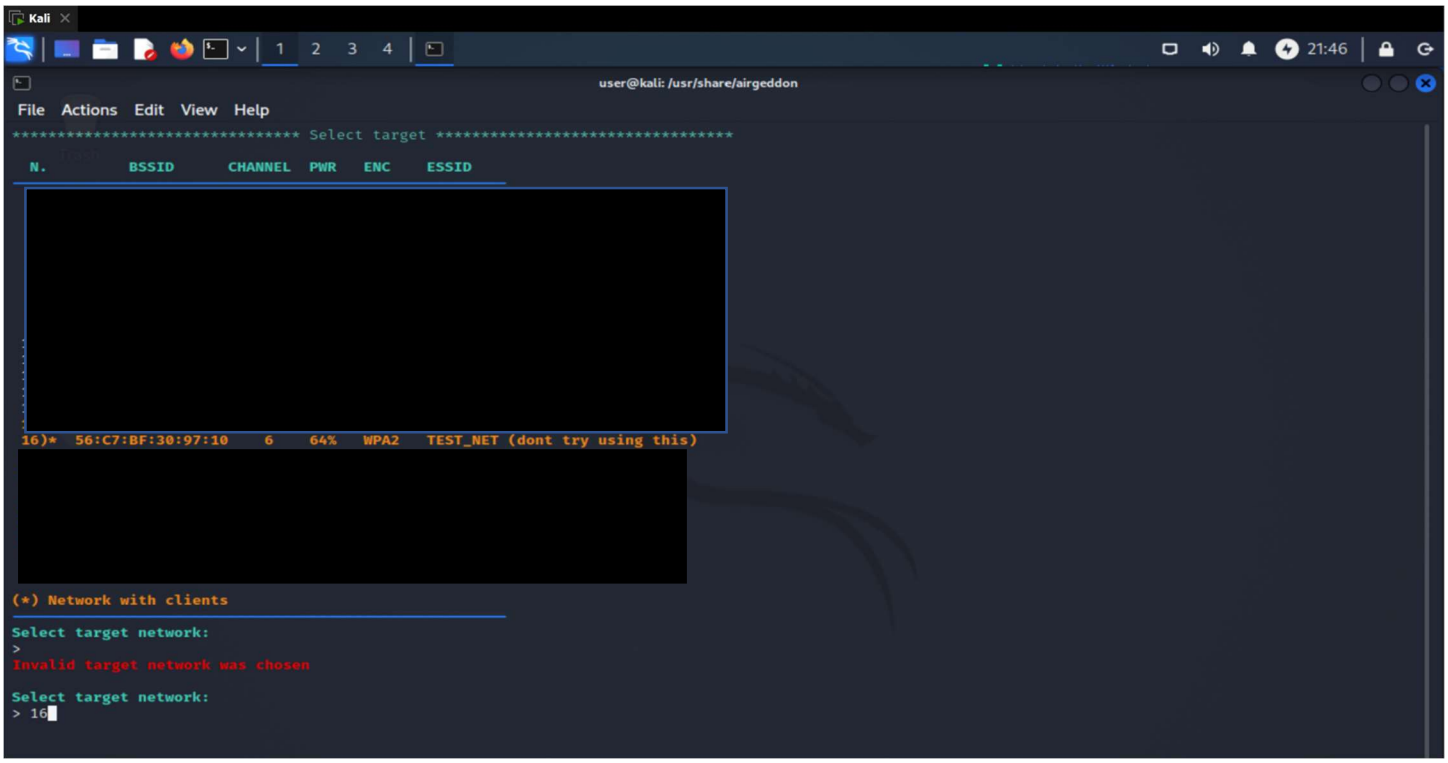
YOU MUST ONLY ATTACK YOUR OWN NETWORK

PART VIII: Picking the Target and Deauthenticating

1) Now we will find the SSID that we are targeting and selecting it for the attack.

   >16

   - for me my target number was 16. Use the number by your SSID.



2) Deauthenticate clients on the target network

   >2

3) It will ask us if we want to enable “DoS Pursuit Mode”
   a. type “N”

4) Now we will be asked to spoof our MAC address during the attack.
   a. Type “Y”

5) 5)We will then be asked if we already have a handshake capture.
   a. Type “N”

6) Then it will ask us to type the value in seconds 10-100 for a deauth attack or accept the default 20 seconds.
   a. Hit “Enter” twice.

      - This will begin deauthenticating connected clients to the network and grab a handshake. If it is unsuccessful, run it again.

      -After capturing a handshake, it will ask us where we want to save the capture file

   b. >/usr/share/airgeddon/handshake.cap
   c. >”Enter”

PART IX: Starting the Captive Portal

1) Now we are asked where to save the password when we get it. We will enter in our own path >/usr/share/airgeddon/password.txt

>"Enter"

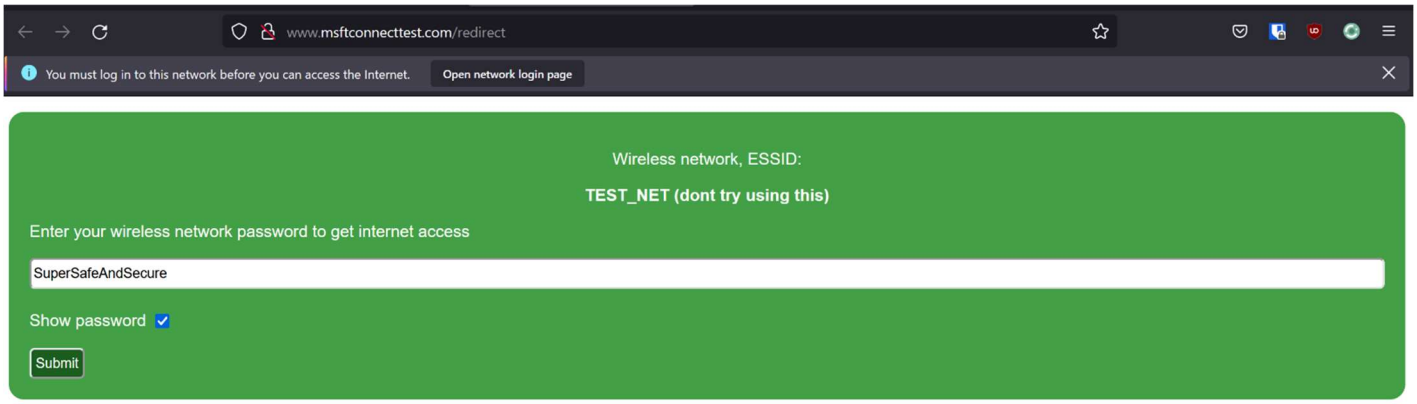
2) Choose the language of the captive portal

> 1

>"Enter"

3) The Evil Twin Attack has started, and the captive portal is made. This creates an AP with the same name (SSID) as the one we selected, but as an open connection.

4) On the target client, they will be completely unable to access the internet. Frustrated, they will check the networks and see their SSID and click on it not realizing its an Evil Twin. Upon connecting, a log-in window will pop up. They will enter in their password and bam. We have stolen their WiFi password by social engineering.



5) After confirming that the password was captured, we can hit "Enter" to stop the attack.
   a. You will be notified by the program in top right window called "Control"

PART X: Viewing the Password

1) close out of the Airgeddon
   >Ctrl + C
   >Y
   >N
2) View the password

   #ls

   #cat password.txt

-Congrats! Password successfully grabbed 😊