WiFiChallenge LAB

Como aprender hacking wifi sin morir en el intento

2022 - Raúl Calvo Laorden

/RootedCON

whoami

Raúl Calvo Laorden

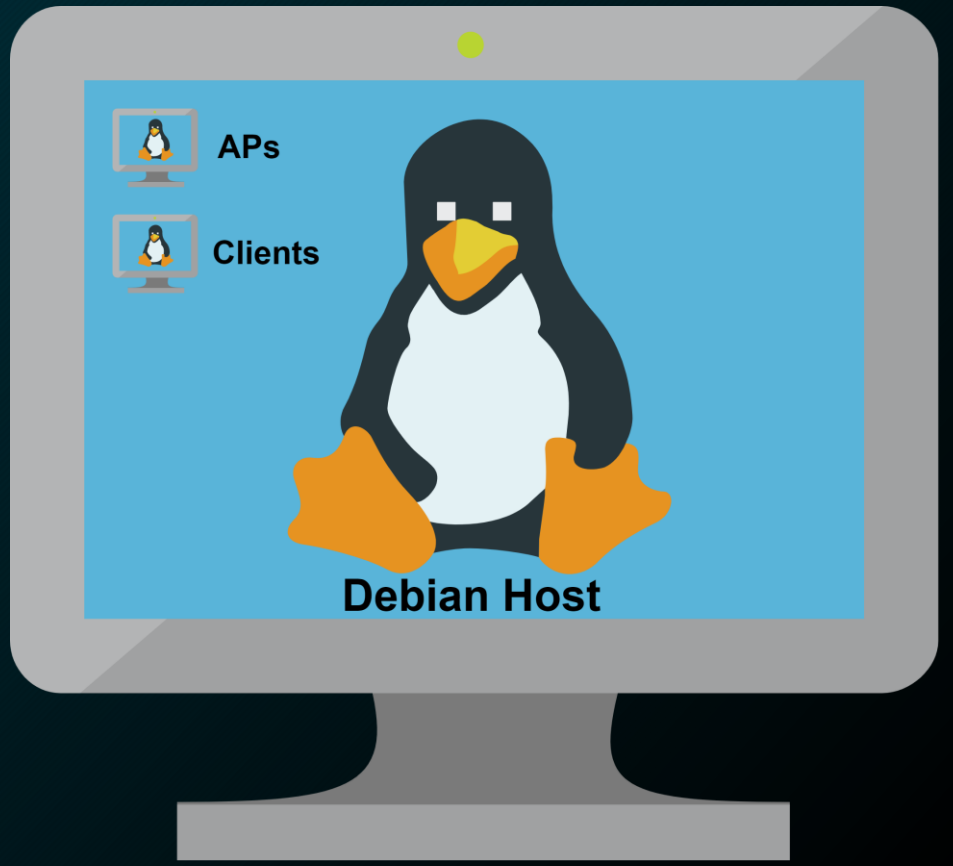
- Pentester en Telefónica
- Graduado en Ingeniería informática
- Fan de las cosas inalámbricas

¿Por qué?

- El hardware WiFi tiende a dar bastantes problemas
  - Chipset, monitor mode, drivers, etc.
- Se necesita un gran número de antenas
  - Mínimo 3 para atacar a cada tipo de red con clientes
- No hay laboratorios wifi virtualizados gratis
  - ¿Alternativas? Pentester Academy
- Entorno “realista” para aprender
  - Simulación de clientes
  - Todo tipo de redes (OPN, PSK, WEP y MGT)
- Probar herramientas

Cómo montar un laboratorio WiFi virtualizado

- mac80211_hwsim
- vwifi de Raizo62 (https://github.com/Raizo62/vwifi)
- Virtualización anidada/múltiples equipos
  - Host (Host VM)
  - APs (VM anidada)
  - Clients (VM anidada)
- ¿Y si utilizamos Docker?
  - No, mac80211_hwsim es un módulo kernel



Problemas encontrados

- Las máquinas virtuales dan MUCHOS problemas
  - Sobre todo si se anidan
  - Hay equipos en los que no funciona sin motivo aparente
- Solo para VMware
  - VirtualBox da problemas
- Los snapshot hechos en Intel no funcionan en AMD

WiFiChallenge Lab - Virtual Machine


Applications Places System
Wed Mar 9, 14:36
user's Home
MATE Terminal
WiFiChallenge
LAB
Menu

WiFiChallenge Lab - Virtual Machine - VMs

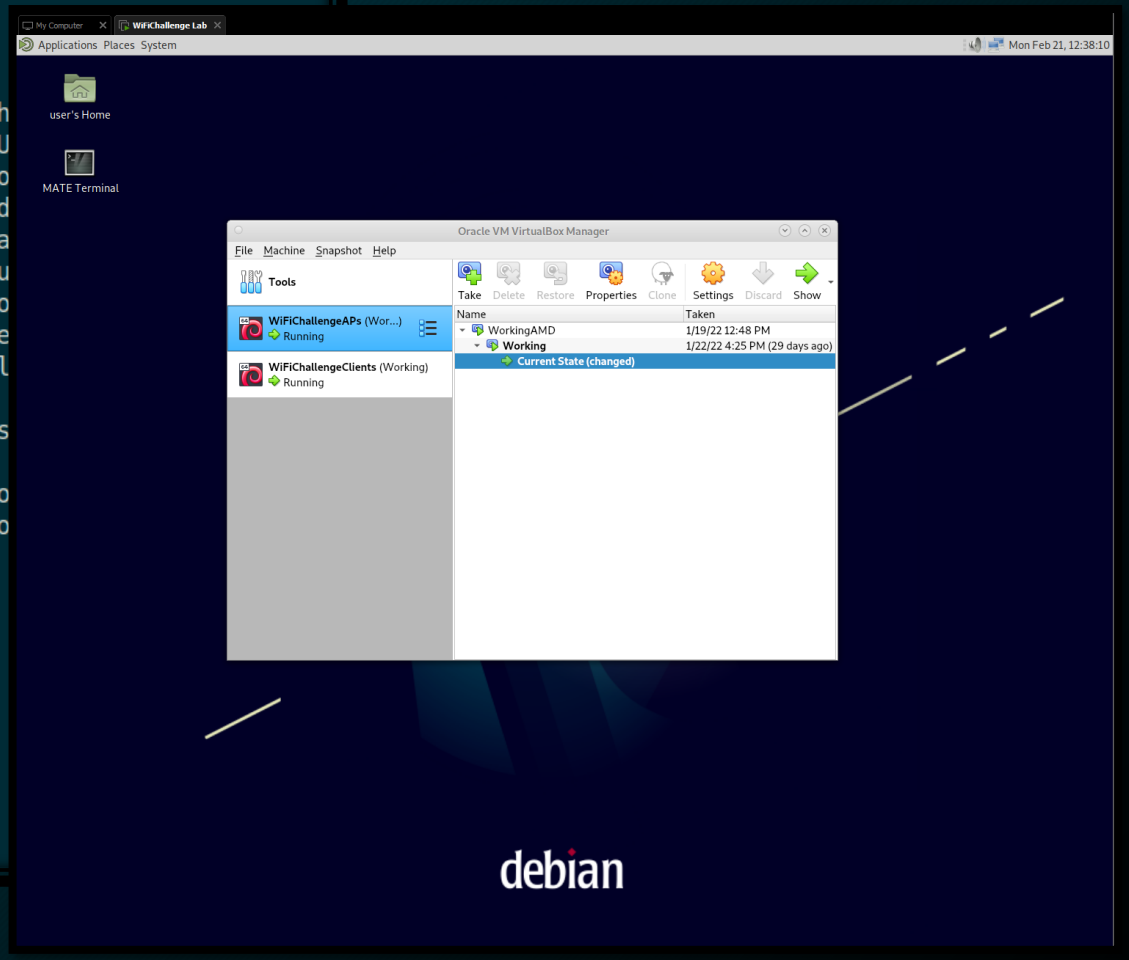
```
CH 44 ][ Elapsed: 30 s ][ 2022-02-21 12:17

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

F0:9F:C2:71:22:11  -38      158        0    0   1   54   WEP  WEP         <length
8A:B7:65:D1:B5:FD  -38      158        0    0   1   54   WPA2 CCMP   PSK  WIFI-JU
F0:9F:C2:71:22:22  -38      158      142    1   1   54   WPA2 CCMP   PSK  wifi-mo
F0:9F:C2:71:22:33  -38      146        0    0   1   54   WPA2 CCMP   PSK  wifi-ad
9E:BD:9B:7C:05:F9  -38      146        0    0   1   54   WPA2 CCMP   PSK  MiFibra
F0:9F:C2:71:22:00  -38      145      153    0   1   54   OPN              wifi-gu
F0:9F:C2:71:22:55  -41      134       48    0  44   54e  WPA2 CCMP   MGT  wifi-co
F0:9F:C2:71:22:66  -41      133       12    0  44   54e  WPA2 CCMP   MGT  wifi-re
F0:9F:C2:71:22:77  -41      154        1    0  44   54e  WPA2 CCMP   MGT  wifi-gl

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   78:C1:A7:BF:72:66  -42    0 -54     80         6         wifi-o
(not associated)   B4:99:BA:6F:F9:55  -42    0 -54     80         6         wifi-o
F0:9F:C2:71:22:22  28:6C:07:6F:F9:33  -36   18 -18      0         4
F0:9F:C2:71:22:22  28:6C:07:6F:F9:44  -36   18 -18      2       135
F0:9F:C2:71:22:00  B0:72:BF:B0:78:88  -36   18 -18      0        52
F0:9F:C2:71:22:00  80:18:44:BF:72:77  -36   18 -18      0        46
F0:9F:C2:71:22:00  B0:72:BF:44:B0:99  -36   18 -18      0        50
F0:9F:C2:71:22:55  10:F9:6F:07:6C:00  -39  54e-54e      0        14
F0:9F:C2:71:22:55  10:F9:6F:BA:6C:11  -39  54e-54e      3        30
F0:9F:C2:71:22:66  10:F9:6F:AC:53:10  -42  54e-54e      5        12
F0:9F:C2:71:22:77  10:F9:6F:BA:18:22  -39    0 -54e     0         1
```



¿Por qué no hacer un CTF?

- Serie de retos específicos con pistas
- "Guiado" para gente nueva
- Algo de competición para los que saben

WiFiChallenge Lab - CTF

- URL:

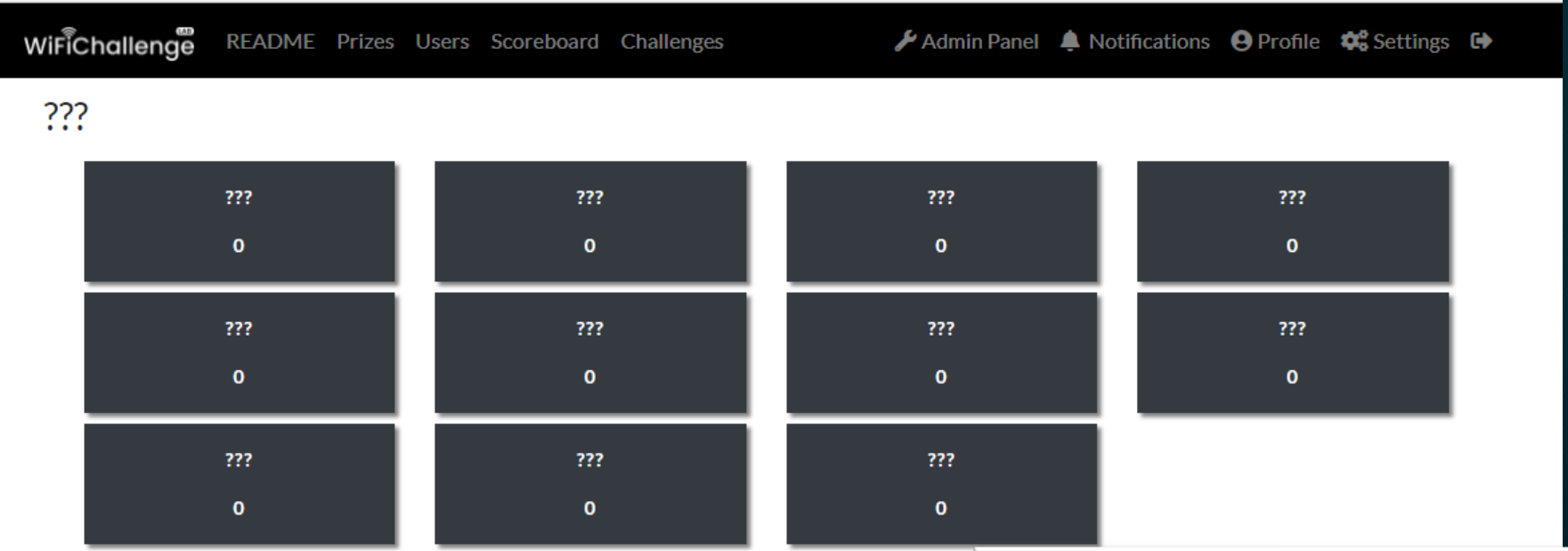
  wifichallengelab.com

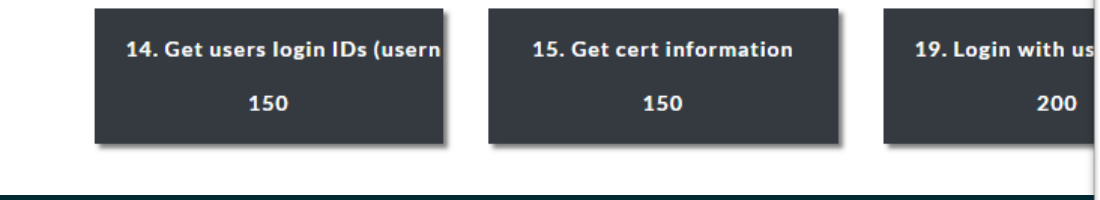
- Duración:

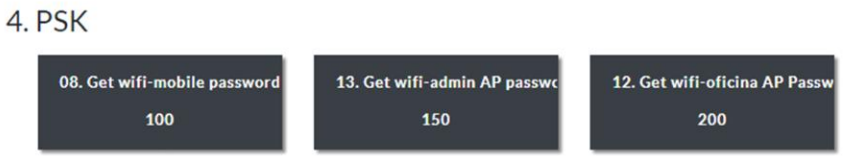
  Del 11 de Marzo al 15 de Mayo

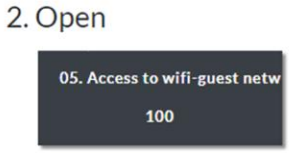
- Contacto

  contact@wifichallengelab.com

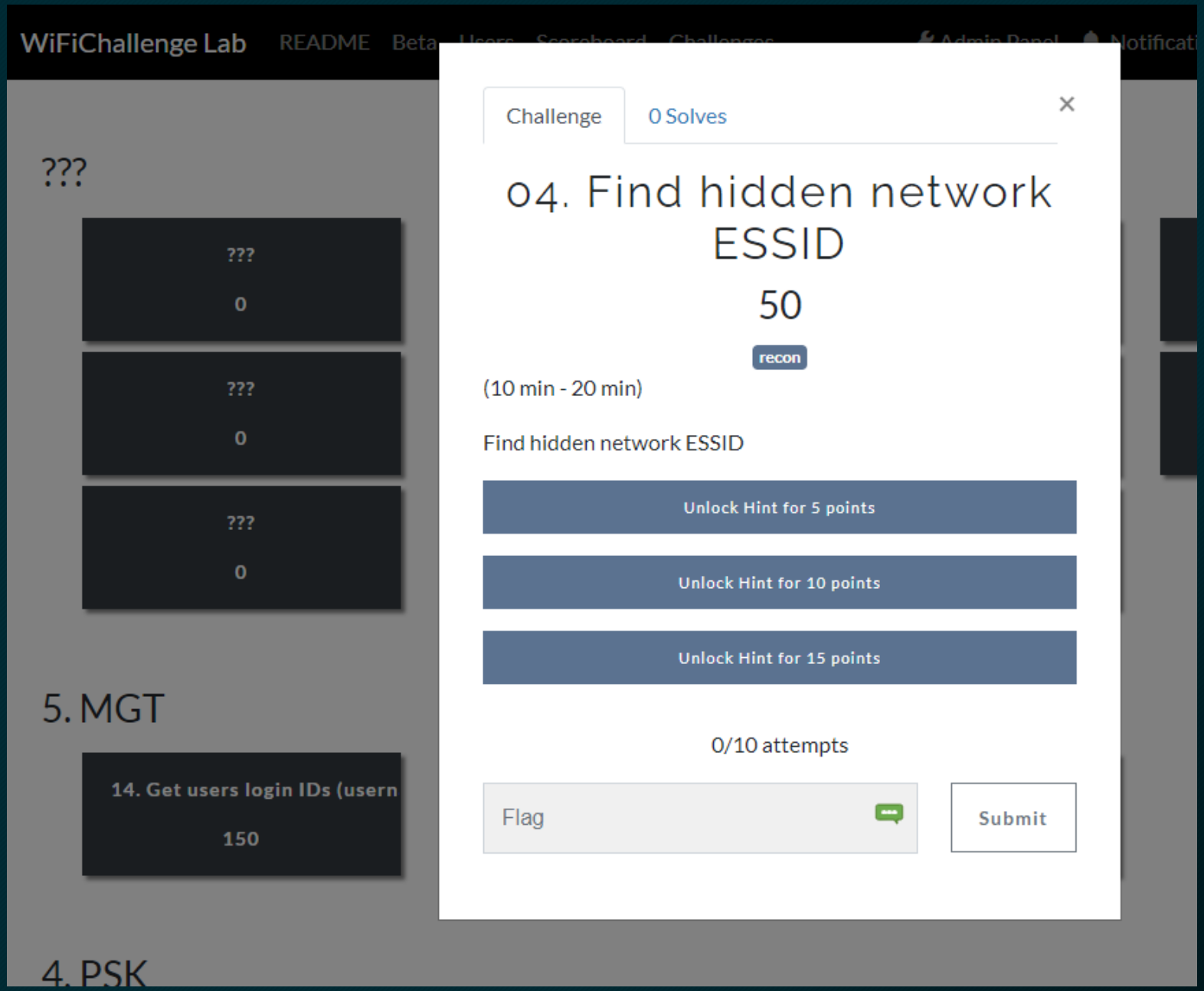








WiFiChallenge Lab - CTF



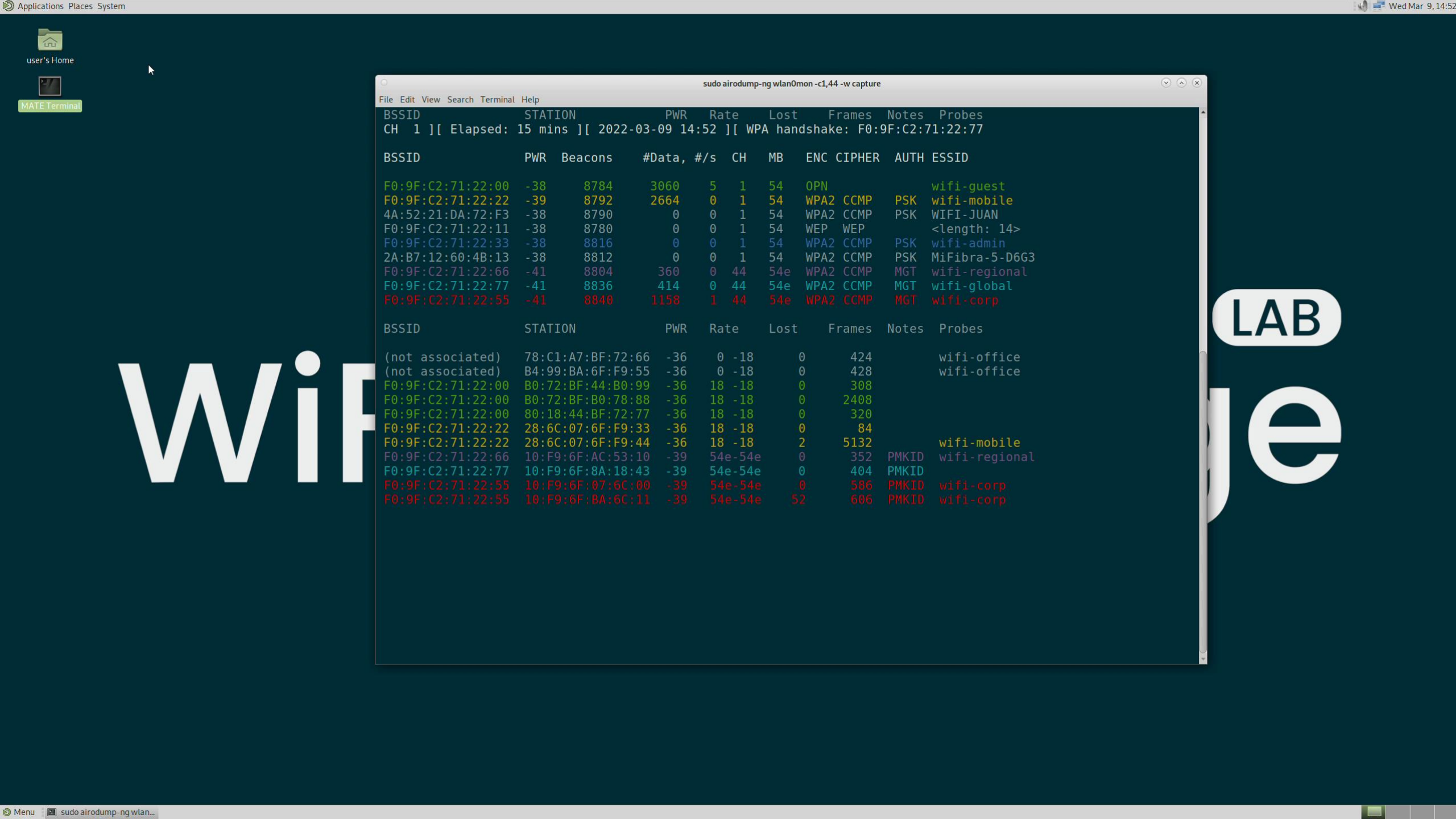
/Rooted

WiFiChallenge Lab - CTF

¿Cómo reutilizar el código del laboratorio?

- Open Source
- El código para crear el laboratorio se publicará cuando acabe el CTF
- Está documentado el proceso de crear el laboratorio
- changeFlags.sh - Script para cambiar las flags
- Habrá una versión como el CTF pero sin cifrar, para modificaciones

Parte práctica
Obtención de información pasivamente


Applications Places System
Wed Mar 9, 14:52
user's Home
MATE Terminal
sudo airodump-ng wlan0mon -c1,44 -w capture
File Edit View Search Terminal Help
BSSID STATION PWR Rate Lost Frames Notes Probes
CH 1][Elapsed: 15 mins][2022-03-09 14:52][WPA handshake: F0:9F:C2:71:22:77
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
F0:9F:C2:71:22:00 -38 8784 3060 5 1 54 OPN wifi-guest
F0:9F:C2:71:22:22 -39 8792 2664 0 1 54 WPA2 CCMP PSK wifi-mobile
4A:52:21:DA:72:F3 -38 8790 0 0 1 54 WPA2 CCMP PSK WIFI-JUAN
F0:9F:C2:71:22:11 -38 8780 0 0 1 54 WEP WEP <length: 14>
F0:9F:C2:71:22:33 -38 8816 0 0 1 54 WPA2 CCMP PSK wifi-admin
2A:B7:12:60:4B:13 -38 8812 0 0 1 54 WPA2 CCMP PSK MiFibra-5-D6G3
F0:9F:C2:71:22:66 -41 8804 360 0 44 54e WPA2 CCMP MGT wifi-regional
F0:9F:C2:71:22:77 -41 8836 414 0 44 54e WPA2 CCMP MGT wifi-global
F0:9F:C2:71:22:55 -41 8840 1158 1 44 54e WPA2 CCMP MGT wifi-corp
BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) 78:C1:A7:BF:72:66 -36 0 -18 0 424 wifi-office
(not associated) B4:99:BA:6F:F9:55 -36 0 -18 0 428 wifi-office
F0:9F:C2:71:22:00 B0:72:BF:44:B0:99 -36 18 -18 0 308
F0:9F:C2:71:22:00 B0:72:BF:B0:78:88 -36 18 -18 0 2408
F0:9F:C2:71:22:00 80:18:44:BF:72:77 -36 18 -18 0 320
F0:9F:C2:71:22:22 28:6C:07:6F:F9:33 -36 18 -18 0 84
F0:9F:C2:71:22:22 28:6C:07:6F:F9:44 -36 18 -18 2 5132 wifi-mobile
F0:9F:C2:71:22:66 10:F9:6F:AC:53:10 -39 54e-54e 0 352 PMKID wifi-regional
F0:9F:C2:71:22:77 10:F9:6F:8A:18:43 -39 54e-54e 0 404 PMKID
F0:9F:C2:71:22:55 10:F9:6F:07:6C:00 -39 54e-54e 0 586 PMKID wifi-corp
F0:9F:C2:71:22:55 10:F9:6F:BA:6C:11 -39 54e-54e 52 606 PMKID wifi-corp
LAB
Menu
sudo airodump-ng wlan...

Agradecimientos

- Raizo62 por vwifi
- Todos los beta testers del laboratorio
- Especialmente a:
  - @Cyb3rR0nin
  - Manuel López Torrecillas
  - Juanma García
  - HENKO

Muchas gracias
Nos vemos en el CTF

¿Preguntas?