GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Seminario web 7 "Seguridad wifi pública"

Ejercicios

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1. EJERCICIO PRÁCTICO

El objetivo del ejercicio es investigar el contenido de un fichero .pcap, el cual contiene tramas 802.11 como resultado de la conectividad de un determinado dispositivo a un punto de acceso. Los usuarios deberán investigar su contenido y contestar a las siguientes preguntas:

- ¿Cuál es el nombre (SSID) del AP al cual se conecta el cliente?
- Identifica las tramas de asociación y autenticación intercambiadas entre el AP y el cliente.
- Localiza el *handshake* a 4 pasos e indica que tipo de cifrado se ha utilizado (TKIP o CCMP).

Resolución del ejercicio:

Los usuarios deberán de repasar las fases involucradas en la conexión de una estación con un AP. Un buen recurso para abordar este ejercicio es: https://www.aircrack-ng.org/doku.php?id=wpa_capture

El nombre del SSID utilizado por el cliente puede obtenerse fácilmente si se filtran las tramas de gestión relacionadas con los "*Probe requests*" o directamente se observan las tramas de asociación.

Algunos filtros de interés desde Wireshark para el protocolo 802.11 pueden encontrarse en el siguiente recurso: https://www.wifi-professionals.com/2019/03/wireshark-display-filters

management frames	wlan.fc.type == 0	all management frames
	wlan.fc.type_subtype == 0	association requests
	wlan.fc.type_subtype == 1	association response
	wlan.fc.type_subtype == 2	re-association request
	wlan.fc.type_subtype == 3	re-association response
	wlan.fc.type_subtype == 4	probe requests
	wlan.fc.type_subtype == 5	probe responses
	wlan.fc.type_subtype == 8	beacons
	wlan.fc.type_subtype == 9	atims
	wlan.fc.type_subtype == 10	disassosiations
	wlan.fc.type_subtype == 11	authentications
	wlan.fc.type_subtype == 12	deauthentications
	wlan.fc.type_subtype == 13	actions

Figura 1: Filtros en WireShark

Estableciendo filtros relacionados con “probe request” y/o “association requests”, obtenemos rápidamente la respuesta a la primera pregunta. El SSID solicitado es “Coherer”

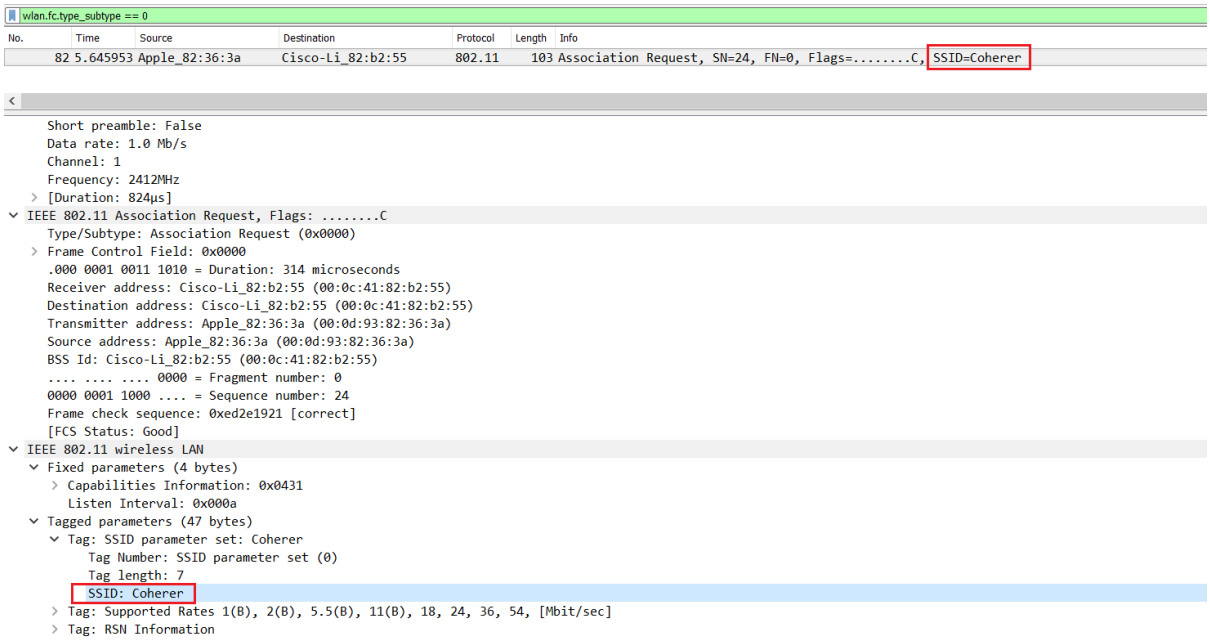

Figura 2: SSID identificado

El “Association Request” y la respuesta del AP (“Association Response”) pueden obtenerse estableciendo el siguiente filtro.

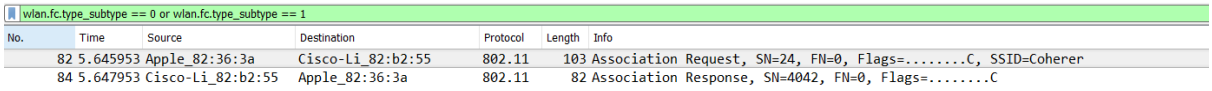

Figura 3: Filtro para "Association Request"

De forma similar, las tramas de autenticación pueden obtenerse con el subtipo 11:

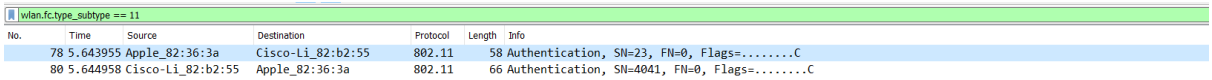

Figura 4: Filtro subtipo 11

Puede observarse, tal y como se describió en el seminario web, que las tramas de autenticación preceden a las de asociación y que dicha fase es un requisito para poder conectarse a una red.

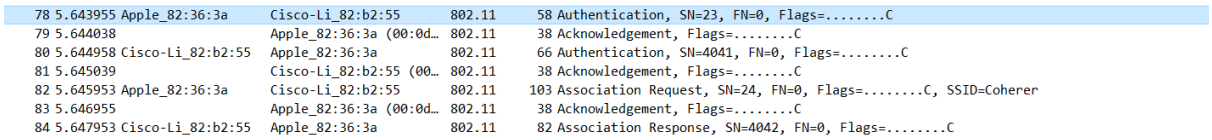

Figura 5: Fase "requisito" de conexión

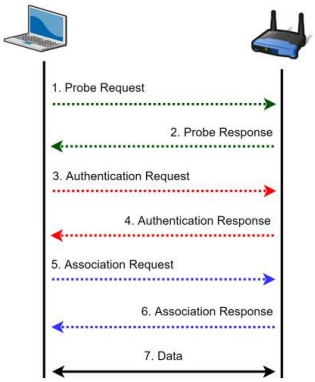

Figura 6: Flujo de un "Handshake"

Respecto al tercer punto, se hacen dos preguntas. La primera de ellas solicita identificar el *handshake* a 4 pasos. Para ello podemos emplear el filtro “EAPOL”, el cual nos mostrará las 4 tramas responsables de la negociación. Fíjese que es el AP el encargado de iniciar el mismo.

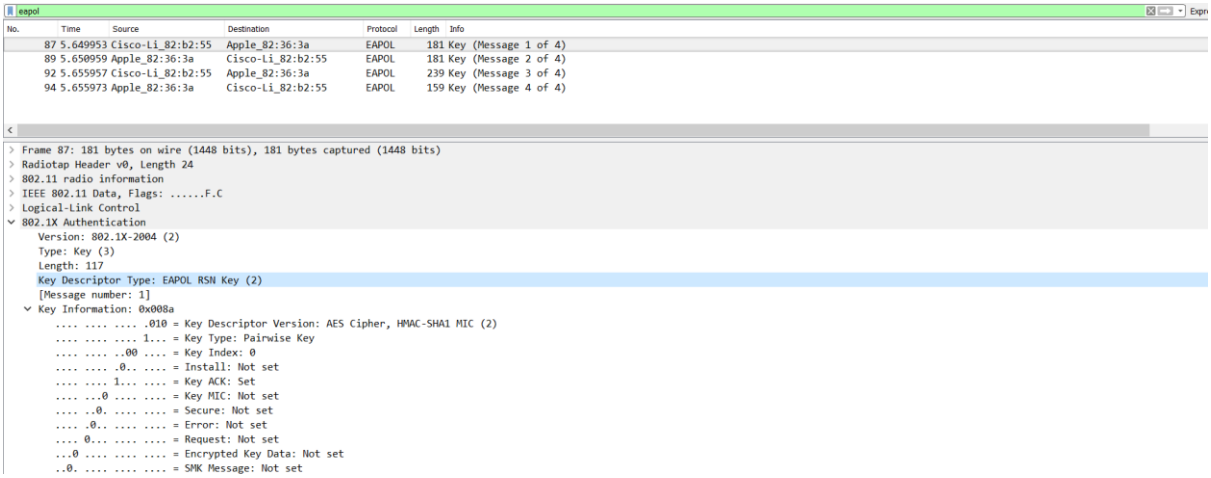

Figura 7: Filtro EAPOL

Respecto a la segunda pregunta (qué tipo de cifrado se emplea), como se puede ver en la siguiente trama (correspondiente a los datos intercambiados entre el AP y la estación una vez se autentica y se asocia en la red), es CCMP.

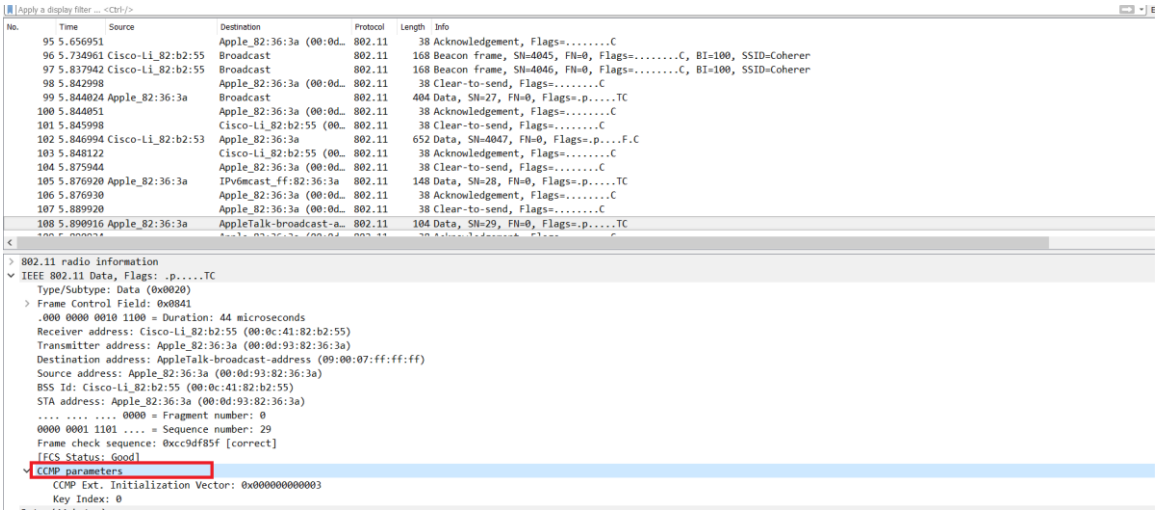

Figura 8: Tipo de cifrado empleado

2. EJERCICIO DE INVESTIGACIÓN

A raíz del estudio del .pcap anterior, los alumnos deberán investigar la forma de romper la contraseña para poder acceder al tráfico cifrado del mismo. Recuérdese que el .pcap contiene el *handshake* a cuatro pasos y, por tanto, es susceptible de ser descifrado si se ha empleado una contraseña débil.

Pista: es posible en este caso que la contraseña sea "induction" bien en mayúsculas/minúsculas o una combinación de ambas.

Resolución del ejercicio:

En el curso se ha mencionado en diversas ocasiones la *suite* de herramientas *aircrack-ng*. Los alumnos deberán investigar la forma de aplicar fuerza bruta mediante alguna de sus herramientas. A raíz de la pista, se ha creado un diccionario de palabras utilizando "induction" y sus variaciones en mayúsculas y minúsculas.

```
root@kali:/media/sf_Share# for w in {i,I}{n,N}{d,D}{u,U}{c,C}{t,T}{i,I}{o,O}{n,N};do echo $w;done > dict.txt
root@kali:/media/sf_Share# head dict.txt
induction
inductioN
inductiOn
inductiON
inductIon
inductIoN
inductIOn
inductION
inducTion
inducTioN
root@kali:/media/sf_Share#
```

Figura 9: Bucle para construir un diccionario de claves

Posteriormente se ha ejecutado *aircrack-ng* de la siguiente manera:

```
root@kali:/media/sf_Share# aircrack-ng -w /tmp/dict.txt -b 00:0C:41:82:b2:55 sample.pcap
```

Figura 10: Comando de ejecución

Con el parámetro -b se indicará la MAC del AP y con -w el diccionario creado anteriormente.

```
                          Aircrack-ng 1.5.2

      [00:00:00] 264/511 keys tested (2096.50 k/s)

      Time left: 0 seconds                                      51.66%

                           KEY FOUND! [ Induction ]


      Master Key     : A2 88 FC F0 CA AA CD A9 A9 F5 86 33 FF 35 E8 99
                       2A 01 D9 C1 0B A5 E0 2E FD F8 CB 5D 73 0C E7 BC

      Transient Key  : B1 CD 79 27 16 76 29 03 F7 23 42 4C D7 D1 65 11
                       82 A6 44 13 3B FA 4E 0B 75 D9 6D 23 08 35 84 33
                       15 79 8D 51 1B EA E0 02 83 13 C8 AB 32 F1 2C 7E
                       CB 71 C8 93 48 26 69 DA AF 0E 92 23 FE 1C 0A ED

      EAPOL HMAC     : A4 62 A7 02 9A D5 BA 30 B6 AF 0D F3 91 98 8E 45
root@kali:/media/sf_Share#
```

Figura 11: Clave encontrada

De forma instantánea obtendremos la contraseña ("Induction"). Posteriormente para descifrar el tráfico desde Wireshark nos dirigiremos a "Edición->Preferencias" y, dentro del

protocolo IEEE 802.11, añadiremos la clave en el siguiente formato: "*wpa_key*:*SSID*" (es decir: "Induction:Coherer").

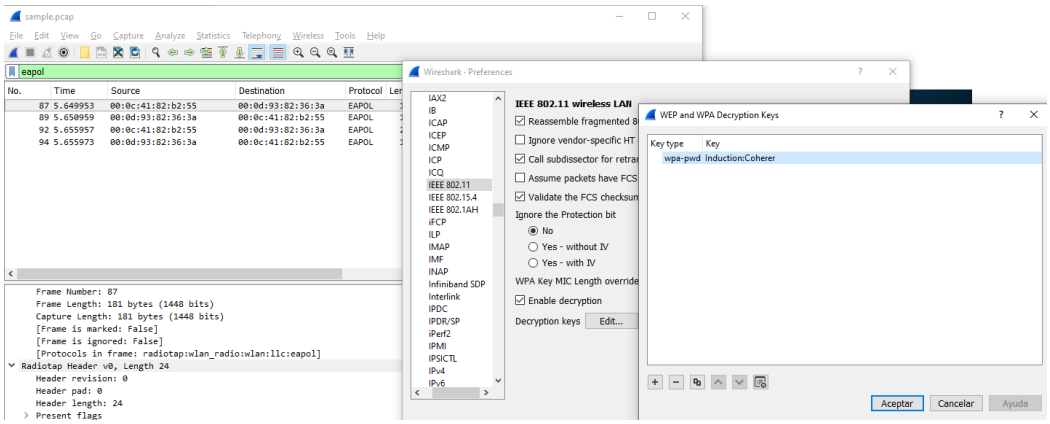

Figura 12: Clave conocida para descifrar tráfico

Tras aceptar el cuadro de diálogo, podremos acceder a la información cifrada. En la siguiente imagen se observa la captura antes de descifrar (imagen de la izquierda) y una vez descifrado (imagen de la derecha). Obsérvese que ya es posible acceder en claro a la información remitida por el cliente y el AP (por ejemplo, tráfico HTTP).

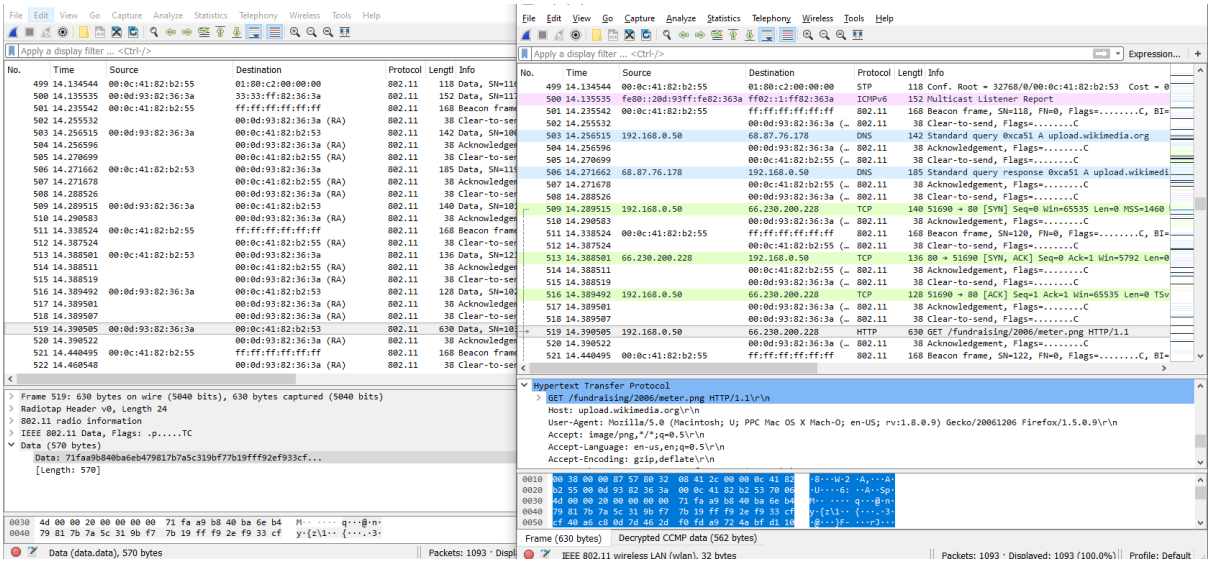

Figura 13: Tráfico descifrado