



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



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Ejercicio Práctico	3
2. Ejercicio de investigación	7

ÍNDICE DE FIGURAS

Figura 1: Filtros en WireShark.....	3
Figura 2: SSID identificado.....	4
Figura 3: Filtro para "Association Request"	4
Figura 4: Filtro subtipo 11.....	4
Figura 5: Fase "requisito" de conexión.....	4
Figura 6: Flujo de un "Handshake".....	5
Figura 7: Filtro EAPOL	5
Figura 8: Tipo de cifrado empleado	6
Figura 9: Bucle para construir un diccionario de claves	7
Figura 10: Comando de ejecución	7
Figura 11: Clave encontrada	7
Figura 12: Clave conocida para descifrar tráfico.....	8
Figura 13: Tráfico descifrado.....	8

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	disassociations
	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"

wlan.fc.type_subtype == 0

No.	Time	Source	Destination	Protocol	Length	Info
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer

```

Short preamble: False
Data rate: 1.0 Mb/s
Channel: 1
Frequency: 2412MHz
> [Duration: 824µs]
▼ IEEE 802.11 Association Request, Flags: .....C
  Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
    Destination address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
    Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)
    Source address: Apple_82:36:3a (00:0d:93:82:36:3a)
    BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
    .... .... 0000 = Fragment number: 0
    0000 0001 1000 .... = Sequence number: 24
    Frame check sequence: 0xed2e1921 [correct]
    [FCS Status: Good]
▼ IEEE 802.11 wireless LAN
  > Fixed parameters (4 bytes)
    > Capabilities Information: 0x0431
      Listen Interval: 0x000a
  > Tagged parameters (47 bytes)
    > Tag: SSID parameter set: Coherer
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: Coherer
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: RSN Information
  
```

Figura 2: SSID identificado

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

wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1

No.	Time	Source	Destination	Protocol	Length	Info
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer
84	5.647953	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C

Figura 3: Filtro para "Association Request"

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

wlan.fc.type_subtype == 11

No.	Time	Source	Destination	Protocol	Length	Info
78	5.643955	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
80	5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C

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.

78	5.643955	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
79	5.644038	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
80	5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C
81	5.645039	Cisco-Li_82:b2:55	Cisco-Li_82:b2:55 (00...	802.11	38	Acknowledgement, Flags=.....C
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer
83	5.646955	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
84	5.647953	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C

Figura 5: Fase "requisito" de conexión

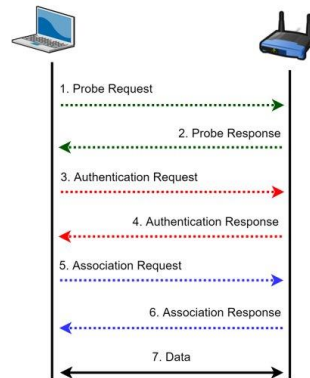


Figura 6: Flujo de un "Handshake"

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.

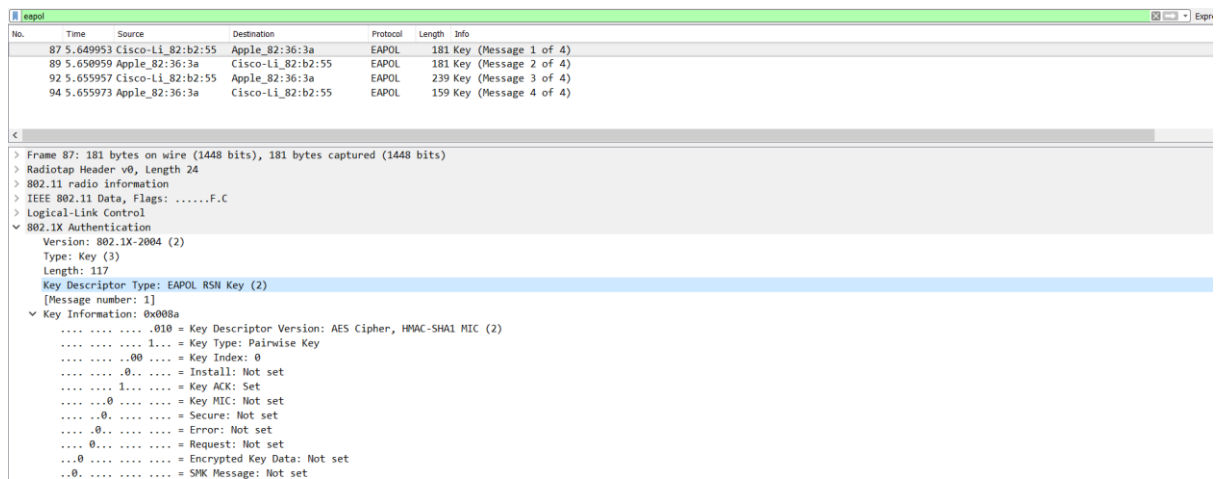


Figura 7: Filtro EAPOL

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.

No.	Time	Source	Destination	Protocol	Length	Info
95	5.656951	Cisco-Li_82:b2:55	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
96	5.734961	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C, BI=100, SSID=Cohereer
97	5.837942	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C, BI=100, SSID=Cohereer
98	5.842998	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
99	5.844024	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=p.....TC
100	5.844051	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
101	5.845998	Cisco-Li_82:b2:55	Cisco-Li_82:b2:55 (00...	802.11	38	Clear-to-send, Flags=.....C
102	5.846994	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	652	Data, SN=4047, FN=0, Flags=p.....F.C
103	5.848122	Cisco-Li_82:b2:55	Cisco-Li_82:b2:55 (00...	802.11	38	Acknowledgement, Flags=.....C
104	5.875944	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
105	5.876920	Apple_82:36:3a	IPv6mcast:ff:82:36:3a	802.11	148	Data, SN=28, FN=0, Flags=p.....TC
106	5.876930	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
107	5.889920	Apple_82:36:3a	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
108	5.890916	Apple_82:36:3a	AppleTalk-broadcast-a...	802.11	104	Data, SN=29, FN=0, Flags=p.....TC

> 802.11 radio information
 > IEEE 802.11 Data, Flags: .p.....TC
 Type/Subtype: Data (0x0020)
 > Frame Control Field: 0x0041
 .000 0000 0010 1100 = Duration: 44 microseconds
 Receiver address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
 Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)
 Destination address: AppleTalk-broadcast-address (09:00:07:ff:ff:ff)
 Source address: Apple_82:36:3a (00:0d:93:82:36:3a)
 BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
 STA address: Apple_82:36:3a (00:0d:93:82:36:3a)
 0000 = Fragment number: 0
 0000 0001 1101 = Sequence number: 29
 Frame check sequence: 0xcc9df85f [correct]
 FCS Status: Good
 > CCM parameters
 CCM Ext. Initialization Vector: 0x000000000003
 Key Index: 0

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}{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
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”).

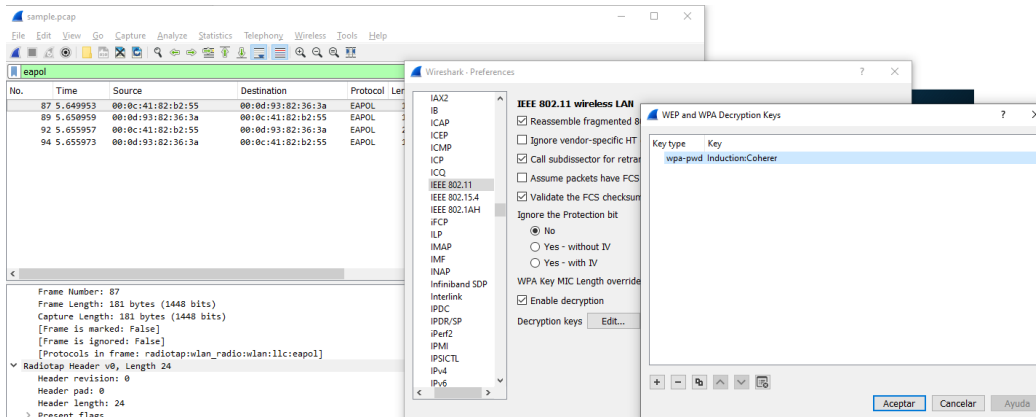


Figura 12: Clave conocida para descifrar tráfico

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).

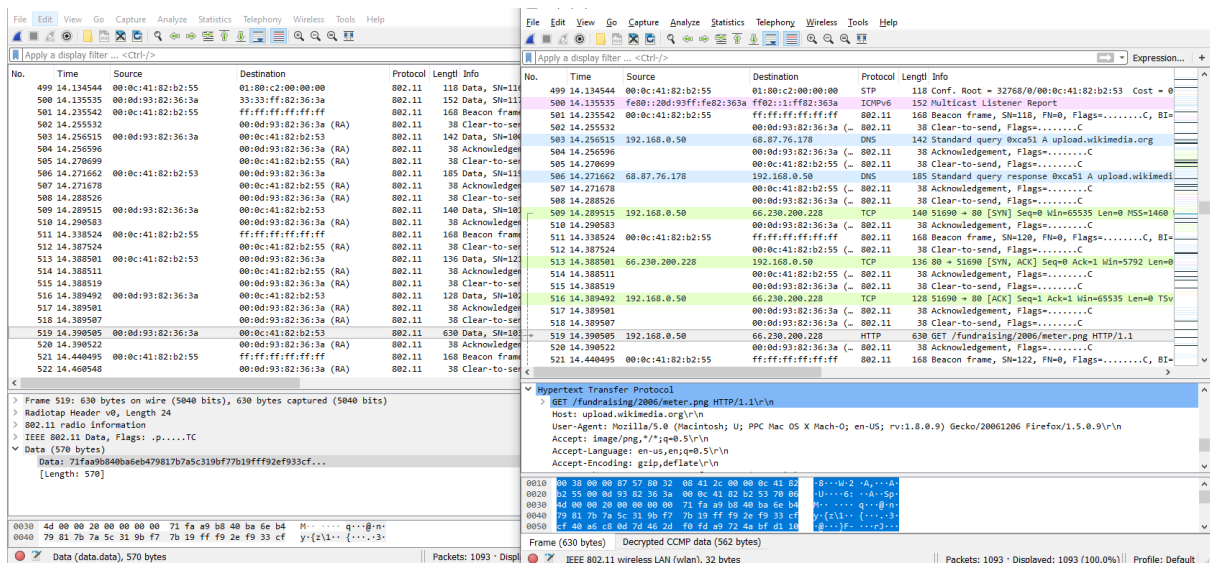


Figura 13: Tráfico descifrado