

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











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: <u>https://www.aircrack-ng.org/doku.php?id=wpa_capture</u>

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: <u>https://www.wifi-professionals.com/2019/03/wireshark-display-filters</u>

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"







📕 wlar	.fc.type_subtype	== 0										
No.	Time	Source	Destination	Protocol	Length	Info						
	82 5.64595	3 Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association	Request,	SN=24,	FN=0,	Flags=	C, SSID=Coherer	
												,
<												
	Short pream	ble: False										
	Data rate:	1.0 Mb/s										
	Channel: 1											
	Frequency:	2412MHz										
>	[Duration:	824µs]										
✓ IE	EE 802.11 As	sociation Request,	Flags:C									
	Type/Subtyp	e: Association Requ	est (0x0000)									
>	Frame Contr	ol Field: 0x0000										
	.000 0001 0	011 1010 = Duration	: 314 microseconds									
	Receiver ad	aress: Cisco-Li_82:	D2:55 (00:0c:41:82:D2:55)								
	Destination	address: Cisco-Li_	82:02:55 (00:00:41:82:02	:55)								
	Sounce addr	auuress. Appie_oz.	(00.0d.02.02.26.2a))								
	DSS Td+ Cie	co-Li 92:52:55 (00:	(00.00.55.02.50.5a) 0c.41.02.b2.55)									
	555 10. 015	0000 = Fragment	number: 0									
	0000 0001 1	000 = Sequence	number: 24									
	Frame check	sequence: 0xed2e19	21 [correct]									
	[FCS Status	: Good]										
✓ IE	EE 802.11 wi	reless LAN										
~	Fixed param	eters (4 bytes)										
	> Capabili	ties Information: 0>	x0431									
	Listen I	nterval: 0x000a										
~	Tagged para	meters (47 bytes)										
	✓ Tag: SSI	D parameter set: Coł	herer									
	Tag N	umber: SSID paramete	er set (0)									
	Tag 1	ength: 7										
	SSID:	Coherer										
	> Tag: Sup	ported Rates 1(B), 2	2(B), 5.5(B), 11(B), 18,	24, 36,	54, [M	bit/sec]						
	> Tag: RSN	Information										

Figura 2: SSID identificado

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

wian.fc.type_subtype == 0 or wian.fc.type_subtype == 1									
No.	Time	Source	Destination	Protocol	Length Info				
	82 5.6459	53 Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	1 103 Association Request, SN=24, FN=0, Flags=C, SSID=Coherer				
	84 5.6479	53 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.	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 (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 (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 (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 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.

GOBIERNO GE ESPAÑA GE ESPAÑA	SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL	\$in cib e_	UAVUDA EN CIBERSEGURIDAD
Apply a display filter <ctrl-></ctrl->			
No. Time Source Destination	Protocol Length Info		
95 5.656951 Apple_82:36:3a (00:00.	802.11 38 Acknowledgement, Flags=	A Flags C BT 100 SSTD Cabanan	
97 5 837942 (isco-Li 82:b2:55 Broadcast	802.11 108 Beacon frame SN=4045, FN	0, Flags= C RI=100, SSID=Coherer	
98 5.842998 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=	pTC	
100 5.844051 Apple_82:36:3a (00:0d.	802.11 38 Acknowledgement, Flags=	c	
101 5.845998 Cisco-Li_82:b2:55 (00.	802.11 38 Clear-to-send, Flags=	c	
102 5.846994 Cisco-Li_82:b2:53 Apple_82:36:3a	802.11 652 Data, SN=4047, FN=0, Flag	=.pF.C	
103 5.848122 Cisco-Li_82:b2:55 (00.	802.11 38 Acknowledgement, Flags=	c	
104 5.8/5944 Apple_82:36:38 (00:00.	802.11 38 Clear-to-send, Flags=		
105 5.876920 Apple_82:30:38 IPV0Mcdst_TT:82:30:38 106 5.976030 Apple_82:30:38	802.11 140 Data, SN=20, FN=0, Flags=	pic	
107 5.889920 Apple 82:36:3a (00:0d.	802.11 38 Clear-to-send. Flags=		
108 5.890916 Apple 82:36:3a AppleTalk-broadcast-a.	802.11 104 Data, SN=29, FN=0, Flags=	pTC	
100 F 000034	000 11 00 A.I.S. J.J.S. F1		
N DOD 44 and/o information			
> 802.11 radio information			
Type/Subtype: Data (0x0020)			
> Frame Control Field: 0x0841			
.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: AppleIalk-broadcast-address (09:0	0:07:11:11:11)		
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]			
CCMP parameters			
Key Index: 0			









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.



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 second	ds 51.66%									
	KEY FOUND! [Induction]									
Master Key : A2 2A	2 88 FC F0 CA AA CD A9 A9 F5 86 33 FF 35 E8 99 A 01 D9 C1 0B A5 E0 2E FD F8 CB 5D 73 0C E7 BC									
Transient Key : Bl 82 15 CE	L CD 79 27 16 76 29 03 F7 23 42 4C D7 D1 65 11 2 A6 44 13 3B FA 4E 0B 75 D9 6D 23 08 35 84 33 5 79 8D 51 1B EA E0 02 83 13 C8 AB 32 F1 2C 7E 8 71 C8 93 48 26 69 DA AF 0E 92 23 FE 1C 0A ED									
EAPOL HMAC : A4 root@kali:/media/sf_Share	4 62 A7 02 9A D5 BA 30 B6 AF 0D F3 91 98 8E 45 b#									



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").

📕 sample.pcap	- 🗆 X	
Eile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		
🛋 🗏 💿 📙 🗅 🗙 🗖 🔍 🗢 🗢 🕾 🗑 🛓 🚍 🔍 Q. Q. N		
Reapol	Wireshark - Preferences ? ×	
No. Time Source Destination Protocol Pro	Image: Second	? ×
Header revision: 0 Header pad: 0 Header length: 24 > Present flags		Ayuda

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).

1						_					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						File	Edit View G	Capture Analyze Statistics	Telephony <u>W</u> ireless <u>T</u>	ools <u>H</u> elp	
4	(🔳 🧟 🛞 📙 🛅	। 🗙 🖸 । ९. 👳 🖷 🖗	👲 📃 📃 ପ୍ ପ୍ ସ୍ 🎹			4 =	1 🕢 🔒	ै 🔀 🗳 🧣 🗢 🗳 👔	🎍 📃 📃 ପ୍ର୍ର୍	题	
	Apply a display filter	<ctrl-></ctrl->				App	ply a display filte	r <ctrl-></ctrl->			Expression +
N	o. Time	Source	Destination	Protocol	Lengti Info	No.	Time	Source	Destination	Protocol	Length Info
	499 14,134544	00:0c:41:82:b2:55	01:80:c2:00:00:00	802.11	118 Data, SN=116		400 14 124544	00.0c.41.82.b2.55	01:00:02:00:00:00	стр	118 Conf. Boot - 22768/0/00:00:41:82:62:52 Cort - 0
	500 14,135535	00:0d:93:82:36:3a	33:33:ff:82:36:3a	802.11	152 Data, SN=117		500 14 125525	forga 20d. 02ff . for 2 2625	ff031.ff03.2625	TCMDuc	152 Multicast Listenen Depert
	501 14,235542	00:0c:41:82:b2:55	ff:ff:ff:ff:ff	802.11	168 Beacon frame		500 14.155555	00.04.41.92.62.50	44.44.44.44.44.44	202 11	162 Person frame Challe Elane C PT-
	502 14,255532		00:0d:93:82:36:3a (RA)	802.11	38 Clear-to-ser		501 14.255542	00.00.41.02.02.33	00.04.02.03.36.3. /	802.11	28 Class to cond Element C
	503 14,256515	00:0d:93:82:36:3a	00:0c:41:82:b2:53	802.11	142 Data, SN=100		502 14.255552	102 168 0 50	60:00:95:02:50:58 (002.11	140 Steaded avery Guerri A unlead vibinedia and
	584 14.256596		00:0d:93:82:36:3a (BA)	802.11	38 Acknowledger	_	505 14.250515	192.100.0.50	00.07.70.170	002 11	142 Standard query oxcasi A upioad.wikimedia.org
	505 14.270699		00:0c:41:82:b2:55 (BA)	802.11	38 Clean-to-ser		504 14.250590		00:00:95:02:50:58 (002.11	38 Acknowledgement, Flags
	506 14.271662	00:0c:41:82:b2:53	00:00:93:82:36:38	802.11	185 Data, SN=119		505 14.270099	(0.03.3(.430	00:00:41:02:02:55 (002.11	38 Clear-to-send, Flags=C
	507 14 271678		00:0c:41:82:b2:55 (RA)	802 11	38 Acknowledge		506 14.271662	68.87.76.178	192.108.0.50	UNS 000	165 Standard query response 0xca51 A upioad.wikimedi
	508 14 288526		00:0d:93:82:36:3a (RA)	802 11	38 Clear-to-ser		507 14.2/16/8		00:00:41:82:02:55 (802.11	38 Acknowledgement, Flags=
	500 14 280515	00-04-03-82-36-3a	00-0c-41-82-b2-53	802 11	140 Data SN-101		508 14.288526		00:00:93:82:36:3a (802.11	38 Clear-to-send, Flags=C
	510 14 200583	00100133102130130	00:0d:93:82:36:3a (PA)	802 11	38 Acknowledge	Г	509 14.289515	192.168.0.50	66.230.200.228	ICP	140 51690 + 80 [SYN] Seq=0 W1n=65535 Len=0 MS5=1460
	510 14.250585	00.0	60:00:95:02:50:58 (NA)	802.11	168 Basson face		510 14.290583		00:0d:93:82:36:3a (802.11	38 Acknowledgement, Flags=C
	512 14.303524	00.00.41.02.02.33	00.0.0.01.02.62.55 (04)	002.11	200 Deacon thank		511 14.338524	00:0c:41:82:52:55	**:**:**	802.11	168 Beacon frame, SN=120, FN=0, Flags=C, BI=
	512 14.30/524	00.0.0.0	00:0C:+1:82:02:35 (RA)	002.11	36 Clean-Co-ser		512 14.387524		00:0c:41:82:b2:55 (802.11	38 Clear-to-send, Flags=C
	515 14.500501	00:00:41:62:02:55	00:00:95:82:56:58	002.11	100 Data, SN=121	1	513 14.388501	66.230.200.228	192.168.0.50	TCP	136 80 → 51690 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
	514 14.300511		00:00:41:82:02:55 (RA)	002.11	56 ACKNOWLEdger		514 14.388511		00:0c:41:82:b2:55 (802.11	38 Acknowledgement, Flags=C
	515 14.388519		00:00:93:82:36:38 (RA)	802.11	38 Clear-to-ser		515 14.388519		00:0d:93:82:36:3a (802.11	38 Clear-to-send, Flags=C
	516 14.389492	00:00:93:82:36:38	00:00:41:82:02:53	802.11	128 Data, SN=102	1	516 14.389492	192.168.0.50	66.230.200.228	TCP	128 51690 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSv
	517 14.389501		00:00:93:82:36:3a (RA)	802.11	38 ACKNOWLEdger		517 14.389501		00:0d:93:82:36:3a (802.11	38 Acknowledgement, Flags=C
	518 14.389507		00:0d:93:82:36:3a (RA)	802.11	38 Clear-to-ser		518 14.389507		00:0d:93:82:36:3a (802.11	38 Clear-to-send, Flags=C
	519 14.390505	00:0d:93:82:36:3a	00:0c:41:82:b2:53	802.11	630 Data, SN=103	-	519 14.390505	192.168.0.50	66.230.200.228	HTTP	630 GET /fundraising/2006/meter.png HTTP/1.1
	520 14.390522		00:0d:93:82:36:3a (RA)	802.11	38 Acknowledger		520 14.390522		00:0d:93:82:36:3a (802.11	38 Acknowledgement, Flags=C
	521 14.440495	00:0c:41:82:b2:55	ff:ff:ff:ff:ff	802.11	168 Beacon frame		521 14.440495	00:0c:41:82:b2:55	ff:ff:ff:ff:ff	802.11	168 Beacon frame, SN=122, FN=0, Flags=C, BI= 🗸
	522 14.460548		00:0d:93:82:36:3a (RA)	802.11	38 Clear-to-ser	<					>
<						✓ Нур	pertext Trans	fer Protocol			A
	Frame 519: 630 by	tes on wire (5040 bits),	. 630 bytes captured (5040 bits)		>	GET /fundrai:	ing/2006/meter.png HTTP/1.	1\r\n		
>	Radiotap Header v	/0, Length 24				Host: upload.wikimedia.org\r\n					
>	802.11 radio info	ormation					User-Agent: 1	lozilla/5.0 (Macintosh; U;	PPC Mac OS X Mach-O;	en-US; rv	:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9\r\n
	IEEE 802.11 Data,	Flags: .pTC					Accept: image	/png,*/*;q=0.5\r\n			
×	Data (570 bytes)						Accept-Langu	ge: en-us.en;a=0.5\r\n			
	Data: 71faa9b8	40ba6eb479817b7a5c319bf7	7b19fff92ef933cf				Accept-Encod	ng; gzip.deflate\r\n			
	[Length: 570]										
						0010	00 38 00 00	87 57 80 32 08 41 2c 00 0	0 0c 41 82 ·8···W·2	·A,···A·	^
							b2 55 00 0d	93 82 36 3a 00 0c 41 82 b	2 53 70 06 .06:	···A···Sp·	
								00 00 00 00 /1 Ta ay 08 4	0 ba 6e 64 M·· ···	d	
6	030 44 00 00 20 0	0 00 00 00 71 fa a9 b8	40 ha 6e h4 M····· g···0			0040	cf 40 a6 c8	od 7d 46 2d f0 fd a9 72 4	a bf d1 10 .03F-		
0	040 79 81 7b 7a 5	c 31 9b f7 7b 19 ff f9	2e f9 33 cf y-{z\1 {3			Eram	a (620 bitor)	Decryreted CCMP data (562 byt	(200		
-	Data (data da	ta) 570 hitor		1	Packete: 1002 : Dical	-riam	e (050 dytes)	Decrypted CCMP data (362 byt	es)		
Data (data.data), 570 bytes								wireless LAN (wlan), 32 bytes			Packets: 1093 · Displayed: 1093 (100.0%) Profile: Default

Figura 13: Tráfico descifrado