Configure Wireshark y FreeRADIUS para descifrar el analizador inalámbrico 802.11 WPA2-Enterprise/EAP/dot1x sobre-the-air

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Procedimiento Paso 1. Descifrar PMK de Access-accept Packet. Paso 2. Extraer PMK(s). Paso 3. Descifrar el sniffer de OTA. Ejemplo de un paquete 802.11 descifrado Ejemplo de un paquete 802.11 cifrado Información Relacionada

Introducción

Este documento describe cómo descifrar el analizador Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) u 802.1x (dot1x) del rastreador inalámbrico sobre el aire (OTA) cifrado, con cualquier método de protocolo de autenticación extensible (EAP).

Es relativamente fácil descifrar la captura de OTA 802.11 basada en PSK/WPA2-personal siempre y cuando se capturan los apretadores de manos EAP a través de LAN (EAPoL) completos de cuatro direcciones. Sin embargo, la clave precompartida (PSK) no siempre se recomienda desde el punto de vista de la seguridad. Corregir una contraseña codificada es sólo cuestión de tiempo.

Por lo tanto, muchas empresas eligen dot1x con Remote Authentication Dial-In User Service (RADIUS) como una mejor solución de seguridad para su red inalámbrica.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- RADIUS libre con radsniff instalado
- Wireshark/Omnipeek o cualquier software capaz de descifrar el tráfico inalámbrico 802.11
- Privilegio para obtener el secreto compartido entre el servidor de acceso a la red (NAS) y Authenticator

- Capacidad para capturar la captura de paquetes RADIUS entre NAS y el autenticador desde la primera solicitud de acceso (desde NAS hasta Authenticator) hasta la última aceptación de acceso (desde Authenticator hasta NAS) durante toda la sesión EAP
- Capacidad para realizar capturas sobreaéreas (OTA) que contienen apretones de manos EAPoL de cuatro vías

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor Radius (FreeRADIUS o ISE)
- Dispositivo de captura de señal aérea
- Dispositivo Apple MacOS/OS X o Linux

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En este ejemplo, dos Pirwise Master Keys (PMK) se derivan de los paquetes Radius capturados desde ISE 2.3, ya que el tiempo de espera de la sesión en este SSID es de 1800 segundos y la captura dada aquí es de 34 minutos (2040 segundos) de largo.

Como se muestra en la imagen, EAP-PEAP se utiliza como ejemplo, pero esto se puede aplicar a cualquier autenticación inalámbrica basada en dot1x.

2	_					
]	wlan.a	ddr==04:f1:28:6a:69:11 && (eapol or eap)		🔀 🔜 💌 Expression	4
P	lo.	Time	Source	Destination	Protocol Length Info	Ŀ
	432	5 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, TLS EAP (EAP-TLS)	
	432	7 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Legacy Nak (Response Only)	ч.
	432	9 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, Protected EAP (EAP-PEAP)	
	433	2 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	ILSVI.2 244 Client Hello	P.
	434	9 2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 1079 Server Hello. Certificate. Server Key Exchange. Server Hello	
	435	2 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	
	435	4 2018-11-16 00:04:02.833165	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 1075 Server Hello, Certificate, Server Key Exchange, Server Hello	
	435	5 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	
	436	1 2018-11-16 00:04:02.839052	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 738 Server Hello, Certificate, Server Key Exchange, Server Hello	
	436	3 2018-11-16 00:04:02.845892	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2 199 Client Key Exchange, Change Cipher Spec, Encrypted Handshak	
	436	5 2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 124 Change Cipher Spec, Encrypted Handshake Message	
	436	7 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)	•
	-					

1	(= 2	🔘 🎉 🛅 🗙 🛅 ९ 👳 👳	🕾 🗿 🎩 📃 Q. Q. Q. M				
	wlan.ad	dr==04:f1:28:6a:69:11 && (eapol or eap))			🔀 📼 💌 Expression	+
N	io.	Time	Source	Destination	Protocol	Length Info	^
Т	9095_	2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	754 Encrypted Handshake Message, Encrypted Handshake Message, En	
	9895_	2018-11-16 00:34:07.519109	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	215 Encrypted Handshake Message, Change Cipher Spec, Encrypted I	
1	9095_	2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	140 Change Cipher Spec, Encrypted Handshake Message	
П	9095	2018-11-16 00:34:07.525423	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)	
Т	9095	2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	125 Application Data	
	9095_	2018-11-16 00:34:07.529567	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	129 Application Data	
	9895_	2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	151 Application Data	
	9095_	2018-11-16 00:34:07.536570	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	183 Application Data	
	9095	2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	169 Application Data	
	9095	2018-11-16 00:34:07.570964	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	124 Application Data	-
	9095_	2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	125 Application Data	
	9095_	2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)	¥

Procedimiento

Paso 1. Descifrar PMK de Access-accept Packet.

Ejecute el **radsniff** contra la captura de RADIUS entre NAS y Authenticator para extraer PMK. La razón por la que se extraen dos paquetes de aceptación de acceso durante la captura es que el

temporizador de tiempo de espera de sesión se establece en 30 minutos en este SSID en particular y la captura es de 34 minutos de largo. La autenticación se realiza dos veces.

```
FRLU-M-51X5:pcaps frlu$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -
s <shared-secret between NAS and Authenticator> -x
<snip>
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
2f33303432
EAP-Message = 0x03c50004
Message-Authenticator = 0x38c67b9ba349842c9624889a45cabdfb
MS-MPPE-Send-Key = 0xa464cc15c0df8f09edc249c28711eb13a6db2d1a176f1196edcc707579fd6793
MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b<<<<<<<<<<<>PMK
Authenticator-Field = 0x6cd33b4d4dde05c07d9923e17ad6c218
<snip>
2018-11-16 11:39:01.470000 (48) Access-Accept Id 183
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
2f33303434
EAP-Message = 0x03910004
Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9
MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb
MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfblcfb0e<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

Nota: Quite cualquier etiqueta LAN virtual (VLAN) de la captura de paquetes Radius; de lo contrario, **radsniff** no reconoce el archivo pcap de entrada. Para quitar cualquier etiqueta VLAN, por ejemplo, <u>editcap</u> se puede utilizar.

Consejo: Generalmente, el tiempo de ejecución del comando **radsniff** contra un archivo PCAP RADIUS se puede contar como una escala de segundos. Sin embargo, si el **radsniff** está atascado en este estado mostrado en el registro, por favor ponga en cascada esta captura de paquetes (A) con otra captura de paquetes más larga (B) entre el mismo NAS y Authenticator. A continuación, ejecute el comando radsniff contra el paquete en cascada (A+B). El único requisito de captura de paquetes (B) es que puede ejecutar el comando radsniff en su contra y ver el resultado detallado.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Cisco123 -x

Logging all events

Sniffing on (/Users/frlu/Downloads/radius_novlan.pcap)

En este ejemplo, el registro del plano de control del controlador de LAN inalámbrica (WLC) (A) que se captura a través de la <u>función de registro de paquetes WLC</u>, se coloca en cascada con una captura más larga del TCPdump (B) de ISE. El registro de paquetes WLC se utiliza como ejemplo porque generalmente es de tamaño muy pequeño.

Registro de paquetes WLC (A)



A continuación, ejecute el **radsniff** contra el pcap combinado (A+B) y podrá ver el resultado detallado.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -s
<shared-secret between NAS and Authenticator> -x

<snip>

```
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000
```

<snip>

Paso 2. Extraer PMK(s).

Elimine el campo 0x en cada **MS-MPPE-Recv-Key** de la salida detallada y luego se presentan los PMK necesarios para el descódigo del tráfico inalámbrico.

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a 066d8b3b PMK:

 $7 \verb+cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e$

Paso 3. Descifrar el sniffer de OTA.

Vaya a Wireshark > Preferences > Protocols > IEEE 802.11. A continuación, marque Enable Decryption y haga clic en el botón Edit situado junto a Decryption Keys, como se muestra en la imagen.

A	Wireshark · Preferences	? X
HCrt HDFS HDFSDATA HIP HKQnet HSLIP HL7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 IAPP IAX2 IB ICAP ICP ICP ICQ IEEE 802.11 KCQ	 ► EEE 802.11 wireless LAN Reassemble fragmented 802.11 datagrams Ignore vendor-specific HT elements Call subdissector for retransmitted 802.11 frames Assume packets have FCS Validate the FCS checksum if possible Ignore the Protection bit. No Yes - without IV Yes - with IV WPA Key MIC Length override © Enable decryption Decryption keys Edt. 	Help

A continuación, seleccione **wpa-psk** como tipo de clave, coloque los PMK derivados en el campo **Key** y luego haga clic en **OK**. Después de completar esto, se debe descifrar la captura OTA y se puede ver información de capa superior (3+).

WEP and WPA Decryption Keys ? X	
Key-type Key wpa-psk ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b wpa-psk 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e	
+ - B A V B Cillers Handate to Handate Reaming littresheri (2021) Keys	
	WEP and WPA Decryption Keys ? X Key type Key wpa-psk ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b wpa-psk wpa-psk 7cce47eb82448d8c0a91099ef7168a9b4563d799448816a3793c5a4dfb1cfb0e wpa-psk + Image: Classical Administrator HonOlate Reserve Different Reserve Differen

Ejemplo de un paquete 802.11 descifrado

File Edit View Go Capture Analyze Statistics	Telephony Wireless Tools Help			
🚄 🔳 🧟 🔘 🎴 🛅 🗙 🛅 🍳 👄 🕾 🗟 🗿	📃 📃 Q, Q, Q, 🔢			
wlan.addr==04:f1:28:6a:69:11				🔀 🗪 💌 Expression 🕇
No. Time	Source	Destination	Protocol	Length Info
397877 2018-11-16 00:17:08.095884	Cisco b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba 6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45 Request-to-send, Flags=C
397879 2018-11-16 00:17:08.097877	Cisco b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba 6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45 Request-to-send, Flags=C
397881 2018-11-16 00:17:08.098393	40.127.66.24	172.16.255.13	TCP	1438 [TCP Retransmission] 80 + 45658 [ACK] Seg=3999988
397882 2018-11-16 00:17:08.098444	104.17.57.239	172.16.255.13	TCP	154 80 → 37553 [ACK] Seg=1 Ack=310 Win=65344 Len=0 TS
397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57 802.11 Block Ack, Flags=C
397884 2018-11-16 00:17:08.098999	104.17.57.239	172.16.255.13	TCP	162 80 + 37555 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0
397886 2018-11-16 00:17:08.099099	172.16.255.13	40.127.66.24	TCP	154 45658 → 80 [ACK] Seq=128 Ack=4001196 Win=788480 L
397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (1_	HmdGloba_6a:69:11 (04:11:28:6a:69:11) (RA)	802.11	5/ 802.11 Block Ack, Flags=
397888 2018-11-16 00:17:08.099606	172.16.255.13	104.17.57.239	TCP	154 37555 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSva
397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
397890 2018-11-16 00:17:08.101762	172.16.255.13	104.17.57.239	HTTP	479 GET /s100264/images/logoq.png?t=636366 HTTP/1.1
397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C
<				>
Frame 397886: 154 bytes on wire (1232 bits).	, 154 bytes captured (1232 bits)			
Radiotap Header v0, Length 48				
802.11 radio information		and the second		
IEEE 802.11 QoS Data, Flags: .pTC				
Logical-Link Control				
Internet Protocol Version 4, Src: 172.16.25	5.13, Dst: 40.127.66.24			
▷ Transmission Control Protocol, Src Port: 450	558, Dst Port: 80, Seq: 128, Ack: 4001196	, Len: 0		
0000 00 00 30 00 6b 08 1c 00 6d f9 30 31 00	00 00 00 ··0·k··· m·01····			
0010 14 00 9e 09 80 04 d9 a4 00 00 00 00 80	04 01 00			
0020 9e 09 0b 22 1f 00 06 00 65 00 00 00 04	00 00 00 ····"···· e·····			
0030 88 41 30 00 00 a3 8e b4 3d e4 04 f1 28	6a 69 11 · A0· · · · · · · (ji·			
0040 00 0c 29 28 89 dd 50 06 00 00 c8 84 00	20 01 00 ···)(··P······			
0050 00 00 at t4 c2 2t 90 d1 14 52 a5 8b 2e	57 27 3a			
0000 uo 34 ab 55 0a 12 92 0a TC a9 1T C2 C8 0070 5c 08 7a 36 57 cd e2 43 89 86 45 92 24	17 d0 db \.z6W.C\$			
0080 42 a2 2e 62 35 c7 36 9b 54 d0 00 91 78	7d 44 87 B b5.6. T x D.			
0090 23 6c 7b e6 fd db e7 06 39 11	#1{9.			
	-			

Si compara el segundo resultado donde no se incluye el PMK, con el primer resultado, donde se incluye el PMK, el paquete 397886 se descifra como datos de QoS 802.11.

Ejemplo de un paquete 802.11 cifrado

The Sarce Desthation Protocol Length 397881 2018-11-16 00:17:08.098333 Ymare 22:09:dd HedGloba_5a:69:11 802.11 1438 Qc5 Data, Sh=1434, FHe0, Flags=, p,F.C 397883 2018-11-16 00:17:08.098455 HedGloba_5a:05:11 (04:f1:28:6a:09:11)	-00	dr==04:f1:28:6a:69:11				×	Ð
397681 2012-11-16 00:17:08.098393 Vmare 23:09:dd HedGloba_66:69:11 802.11 1438 0c5 Data, SH=344, FH=0, Flags=.pF,C 397682 2013-11-16 00:17:08.098495 HedGloba_66:69:11 002.11 57 802.11 154 0c5 Data, SH=343, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.098495 HedGloba_66:09:11 Outsched 002.11 57 802.11 164 0c5 Data, SH=35, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.098495 HedGloba_66:09:11 Vmare 23:89:dd 002.11 57 802.11 164 0c5 Data, SH=343, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.09918 Cisco_b4:3d:e4 (00:a3:eb:13) Vmare 23:89:dd 002.11 57 802.11 164 0c5 Data, SH=343, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.09918 Cisco_b4:3d:e4 (00:a3:eb:13) Vmare 23:89:dd 002.11 57 802.11 164 0c5 Data, SH=10, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.09918 Cisco_b4:3d:e4 (00:a3:eb:13) Vmare 23:89:dd 002.11 57 802.11 164 0c5 Data, SH=10, FH=0, Flags=.p,F,C 397682 2013-11-16 00:17:08.09918 Cisco_b4:3d:e4 (00:a3:eb:13) Vmare 23:89:dd 002.11 57 802.11 160 0ch Ack, Flags=.p,TC 397692 2013-11-16 00:17:08.09017 HedGloba_60:0911 Vmare 23:89:dd THedGloba_60:6911 802.11		Time	Source	Destination	Protocol	Length Info	
97782 2018-11-16 00:17:08.09844 Memore 22:09:04 Memore 23:09:01 082.11 154 QoS Data, SH-1435, FH-0, Flags-,, C 97785 2018-11-16 00:17:08.09999 Memore 22:09:04 Mediciba_5a:69:11 082.11 154 QoS Data, SH-1435, FH-0, Flags-,, C 97785 2018-11-16 00:17:08.099999 Memore 22:09:04 Mediciba_5a:69:11 082.11 154 QoS Data, SH-1435, FH-0, Flags-,, TC 39786 2018-11-16 00:17:08.09909 Memore 22:09:04 Mediciba_6a:69:11 082.11 154 QoS Data, SH-1435, FH-0, Flags-,, TC 39786 2018-11-16 00:17:08.09909 Mediciba_6a:69:11 Wmare 28:09:04 082.11 154 QoS Data, SH-1435, FH-0, Flags-,, TC 39786 2018-11-16 00:17:08.099018 (isco_Histore 4:10:10:00:10:10:10:10:10:10:10:10:10:10:		397881 2018-11-16 00:17:08.098393	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	1438 QoS Data, SN=1434, FN=0, Flags=.pR.F.C	
397883 2018-11-16 00:17:08.099495 Huddloba_6a:69:111 (04:f1:22:6a:69:11) 802.11 57 802.11 Block Ack, Flags=C 397884 2018-11-16 00:17:08.099999 Huddloba_6a:69:11 Wumare_28:89:dd 802.11 154 Qc5 Data, SN=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.099999 Huddloba_6a:69:11 Wumare_28:89:dd 802.11 154 Qc5 Data, SN=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.099959 Huddloba_6a:69:11 Wumare_28:89:dd 802.11 154 Qc5 Data, SN=101, FN=0, Flags=.pTC 397882 2018-11-16 00:17:08.09955 Cisco_bi:3d:e4 (00:a3:ee:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.pTC 397885 2018-11-16 00:17:08.09955 Cisco_bi:3d:e4 (00:a3:ee:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=.pTC 397895 2018-11-16 00:17:08.100122 Cisco_bi:3d:ee:43:de:4 (00:a3:ee:69:11 (04:f1:28:6a:69:11) (RA) 802.11 45 Qc5 Data, SN=104, FN=0, Flags=.pTC 397895 2018-11-16 00:17:08.100122 Cisco_bi:3d:ee:43:de:4 (00:a3:ee:69:11 (04:f1:28:6a:69:11) (RA) 802.11 55 Qc5 Data, SN=143, FN=0, Flags=.pFC 767882 2018-11-16 00:17:08.100556 Wumare_28:89:dd Huddloba_6a:69:11 802.11 56 Qc5 Data, SN=143, FN=0, Flags=.pFC 767882 2018-11-16 00:17:08.100556 Wumare_28:89:164 Huddloba_6a		397882 2018-11-16 00:17:08.098444	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1435, FN=0, Flags=.pF.C	
397884 2018-11-16 00:17:08.098999 Wmare_28:89:dd HudGloba_6a:69:11 802.11 160 cp 50 tots, 58-1435, frieb, f		397883 2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)_	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397886 2018-11-16 00:17:08.099099 HmdGloba_5:09:11 Wmare_28:09:1d 082.11 154 QoS Data, Sh=101, FN=0, Flags=, p,,TC 397887 2018-11-16 00:17:08.099055 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (THmdGloba_5a:65:11) (B4:f1:28:6a:69:11) (B4) 082.11 154 QoS Data, Sh=02, FN=0, FLags=, p,,TC 397888 2018-11-16 00:17:08.099055 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (THmdGloba_5a:65:11 (B4:f1:28:6a:69:11) (B4) 082.11 154 QoS Data, Sh=02, FN=0, FLags=, p,,TC 397889 2018-11-16 00:17:08.017:08.010526 Cisco_b4:3d:e4 (00:a3:08:b4:3d:e4) (THmdGloba_5a:65:011) (B4:f1:28:6a:69:11) (B4:f1:28:6a:69:12) (B4:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:		397884 2018-11-16 00:17:08.098999	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	162 QoS Data, SN-1436, FN-0, FlagspF.C	_
397887 2018-11-16 00:17:08.099181 Cisco_b4:3d:re4 (00:a3:8::b4:3d:re4) (T. HmdGloba_Ga:69:11) (R4) 802.11 57 802.11 Block Ack, Flagst 397888 2018-11-16 00:17:08.099665 Cisco_b4:3d:re4 (00:a3:8::b4:3d:re4) (T. HmdGloba_Ga:69:11) (R4) 802.11 154 QoS Data, Sh=02, FN=0, FlagsC 397889 2018-11-16 00:17:08.109655 Cisco_b4:3d:re4 (00:a3:8::b4:3d:re4) (T. HmdGloba_Ga:69:11) (R4) 802.11 57 802.11 Block Ack, FlagsC 397890 2018-11-16 00:17:08.101762 HmdGloba_Ga:69:11 Wmare_Z8:89:dd 802.11 57 802.11 Block Ack, FlagsC 397891 2018-11-16 00:17:08.10555 Wmare_Z8:89:dd HmdGloba_Ga:69:11 802.11 57 802.11 Block Ack, FlagsC 397892 2018-11-16 00:17:08.10555 Wmare_Z8:89:dd HmdGloba_Ga:69:11 802.11 57 802.11 Block Ack, FlagsC 397892 2018-11-16 00:17:08.106055 Wmare_Z8:89:dd HmdGloba_Ga:69:11 802.11 55 QoS Data, Sh=1437, FN=0, Flags,F.C Frame 3978861 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) HmdGloba_Ga:69:11 802.11 15 4 QoS Data, Sh=1436, FN=0, Flags,F.C Prame 3978862 114 Gob 50 Mure (1232 bits), 154 bytes captured (1232 bits) HmdGloba_Ga:69:11 802.11 16 4 QoS Data, Sh=1436, FN=0, Flags,F.C Pata (68 bytes) HmdGloba_Ga:69:11 802.11 16 Hore		397886 2018-11-16 00:17:08.099099	HmdGloba 6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=101, FN=0, Flags=.pTC	
397882 2018-11-16 00:17:08.099665 Hedloba_6a:69:11 Vmare_28:89:dd 902.11 154 doS Data, SN-102, FN+0, Flags=,TC 397898 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T		397887 2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T.	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=	-
397889 2018-11-16 00:17:08.099655 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11] (04:f1:28:6a:69:11) (8A) 802.11 57 802.11 Block Ack, Flags=C 39789 2018-11-16 00:17:08.101621 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11) (8A:f1:28:6a:69:11) (8A) 802.11 57 802.11 Block Ack, Flags=.,C 397891 2018-11-16 00:17:08.101621 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_ HmdGloba_a6:69:11) (8A:f1:28:6a:69:11) (8A) 802.11 57 802.11 Block Ack, Flags=.,C 397892 2018-11-16 00:17:08.106055 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=.,,C 397892 2018-11-16 00:17:08.106055 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=.,,C 97894 2018-11-16 00:17:08.106055 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=.,,C 97894 2018-11-16 00:17:08.106055 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=.,,C 97894 2018-11-16 00:17:08.106055 Vmware_28:89:dd HmdGloba_a6:69:11 802.11 57 802.11 Block Ack, Flags=.,,C 98.10 to formation If add of add add add add add add add add add ad		397888 2018-11-16 00:17:08.099606	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	154 QoS Data, SN=102, FN=0, Flags=.pTC	
397890 2018-11-16 00:17:08.101762 Hedlobs_6a:69:11 Vmvare_28:89:dd 802.11 479 Qx5 Data, SN=103, FN=0, Flags=,, TC 397891 2018-11-16 00:17:08.101812 Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T		397889 2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397891 2018-11-16 00:17:08.101812 Cisco_b4:30:r46 (00:33:8e:b4:3d:e4) (THmdGloba_6a:69:11) (04:f1:28:6a:69:11) (8A) 802.11 578 802.11 Block Ack, Flags=C 397892 2018-11-16 00:17:08.106955 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 555 (05 Data, SN=1437, FH=0, Flags=.pF.C Frame 39786: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Nadiotap Header v0, Length 48 802.11 154 0c5 Data, Flags:.pFC Data (68 bytes) Data (68 bytes)		397890 2018-11-16 00:17:08.101762	HmdGloba_6a:69:11	Vmware_28:89:dd	802.11	479 QoS Data, SN=103, FN=0, Flags=.pTC	
397892 2018-11-16 00:17:08.105958 Vmmare_28:89:dd HmdGloba_6a:69:11 802.11 595 QoS Data, SN=1437, FN=0, Flags=, pF.C 397892 2018-11-16 00:17:08.105055 Vmmare 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1437, FN=0, Flags=, pF.C Frame 397866: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) N=0 Flags=, pF.C B02.11 radio information Iffee 802.11 QoS Data, Flags: .pTC Iffee 802.11 QoS Data, Flags: .pTC Data (66 bytes) Iffee 90 20:00 cb 08 1c 00 cd ff 9 30 31 00 00 00 00 ···O·k··· m·01···· Iffee 90 20:00 cb 08 1c 00 cd ff 9 30 31 00 00 00 00 ···O·k··· m·01····		397891 2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57 802.11 Block Ack, Flags=C	
397894 2018-11-16 00:17:08.106056 Vmware 28:89:dd HmdGloba_6a:69:11 802.11 154 QoS Data, SN=1438, FM+0, Flags=.pF.C Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Bits) 802.11 radio information EEE 802.11 radio information 154 QoS Data, Flags: .pTC Data (66 bytes) 154 QoS Data, SN=1438, FM+0, Flags=.pF.C 90 00 00 6b 08 1c 00 6d f9 30 31 00 00 00 00 ···O·k··· m·01···· 154 QoS Data, SN=1438, FM+0, Flags=.pF.C 18 14 00 5e 00 80 04 d9 af 00 00 00 00 08 08 04 01 00 ······ ········· 19 40 09 c0 03 00 6b 08 1c 00 6d f9 30 31 00 00 00 00 ··············· ····································		397892 2018-11-16 00:17:08.105958	Vmware_28:89:dd	HmdGloba_6a:69:11	802.11	595 QoS Data, SN=1437, FN=0, Flags=.pF.C	
Prame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) Radiotap Header v0, Length 48 B02.11 radio information IEEE 802.11 QoS Data, Flags: .pTC Data (66 bytes) 00 00 00 6b 08 1c 00 6d f9 30 31 00 00 00 00 00 00 00 00 00 00 00 00 00		397894 2018-11-16 00:17:08.106056	Vmware 28:89:dd	HmdGloba_6a:69:11	802.11	154 QoS Data, SN=1438, FN=0, Flags=.pF.C	
0 00 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 00 00 00 k··· m·01···· 1 14 00 9c 00 30 04 d9 a4 00 00 00 00 00 04 01 00 00 00 00 00 00 00 00 00 00 00 00	ata	02.11 QoS Data, Flags: .pTC (68 bytes)					
	Data	102.11 QoS Data, Flags: .pTC 68 bytes)					
	1EEE 1 Data 0 00 00 10 14 20 90 30 88	00.11 QoS Data, Flags: .pTC (68 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 a4 00 00 00 80 09 9b 22 1f 00 06 06 55 00 00 04 f1 28	90 00 00 · · · · · · · · · · · · · · · ·				
40 00 0c 29 28 89 dd 50 06 00 08 84 00 20 01 00 ···························	00 00 00 00 10 14 20 90 40 00	00.11 QoS Data, Flags: .pTC (68 bytes) 00 30 00 65 06 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 60 00 08 09 05 22 16 00 65 00 65 00 00 00 04 41 30 00 00 a3 06 54 34 00 00 00 88 24 0 c 29 28 39 d5 00 60 00 00 68 48 00	00 00 00 ·····························				
40 00 0c 29 28 89 dd 50 06 00 0a 84 00 20 01 00 ···························	1EEE 1 Data Data 19 14 19 94 19 94 1	00.11 QoS Data, Flags: .pTC (68 bytes) 00 30 00 65 06 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 00 00 80 09 05 22 1f 00 06 06 65 00 00 04 f1 28 0c 29 28 89 dd 50 06 00 00 c8 84 00 00 af f4 c2 2f 90 d1 14 52 af 58 52	60 00 00 00 · 0·k··· m·01···· 64 01 00 · c · c · c · c · c · c · c · c · c				
Main 000 4C 22 28 83 dd 55 06 00 00 c6 54 00 20 01 00 ···)(· P ······························	IEEE 0 Data 0 000 00 010 14 020 90 030 08 030 08 000 08 000 08 000 08 000 08 000 000	00.11 QoS Data, Flags: .pTC (68 bytes) 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 9e 09 80 04 d9 a4 00 00 00 80 09 9b 22 1f 00 06 00 65 00 00 04 41 30 00 00 a3 0e b4 41 30 00 00 a8 0e 04 41 30 00 00 a8 0e 04 41 30 00 00 a8 0e 04 41 30 c 29 28 89 dd 50 06 00 00 c8 84 00 00 af f4 c 2 f9 0d 1 14 52 a5 8b 2c 4 a5 55 0a 12 92 da fc a9 1f c 2c 65	00 00 00 00 .0 k m 01 04 01 00				
440 00 0c 29 28 89 dd 50 00 0c 29 28 89 dd 50 00 0c 29 28 89 dd 50 00 0c 14 52 65 0c 20 10 0c () P	IEEE 0 Data 0 Data 0 000 000 010 14 020 90 030 08 040 00 040 00000000	00.11 QoS Data, Flags: .pTC (68 bytes) 00 30 00 65 08 1c 00 6d f9 30 31 00 00 9e 09 30 04 d9 a4 00 60 00 80 09 05 22 16 00 66 06 56 00 00 00 4 41 30 00 00 a3 06 54 30 40 4 f1 28 0c 29 28 39 d5 06 06 00 00 64 40 00 af f4 c2 2f 90 d1 14 52 a5 85 26 84 a 35 7c dc 24 38 98 6f 59 22 44 13 26 67 26 75 66 46 46 55 92 24	00 00 00 00 -0 k m 01 04 01 00 - 0 k m 01 04 01 00 - 0 - c - (j1 00 100 0] (-P 57 27 3a - (J 33 9 ca - (J 34 9 ca - (J 57 27 3a - (J 49 - (J 49 - (J) 7 d d 57 - (K) 7 d d 57 - (K) 17 d d 57 - (K				

Precaución: Puede encontrarse con un problema con Wireshark en el descifrado y, en ese caso, incluso si se proporciona la PMK adecuada (o si se utiliza PSK, se proporcionan SSID y PSK), Wireshark no descifra la captura OTA. La solución temporal es apagar Wireshark y encenderlo varias veces hasta que se pueda obtener información de capa superior y los paquetes 802.11 ya no se muestren como datos de QoS o para utilizar otro PC/Mac donde esté instalado Wireshark.

Sugerencia: un código de C++ denominado pmkXtrt se adjunta en el primer post de Información Relacionada. Los intentos de compilación se realizaron correctamente y se obtuvo un archivo ejecutable, pero el programa ejecutable no parece realizar el descifrado correctamente por algunas razones desconocidas. Además, un guión en Python que intenta extraer PMK es publicado en el área de comentarios en el primer post, que puede ser explorado más adelante si los lectores están interesados.

Información Relacionada

- <u>Tweaking EAP's débil link succión de PMK WiFi de RADIUS con pmkXtrat</u>
- <u>Cómo descodificar la clave MS-MPPE-Recv de Radius</u>
- Soporte Técnico y Documentación Cisco Systems