

# 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.

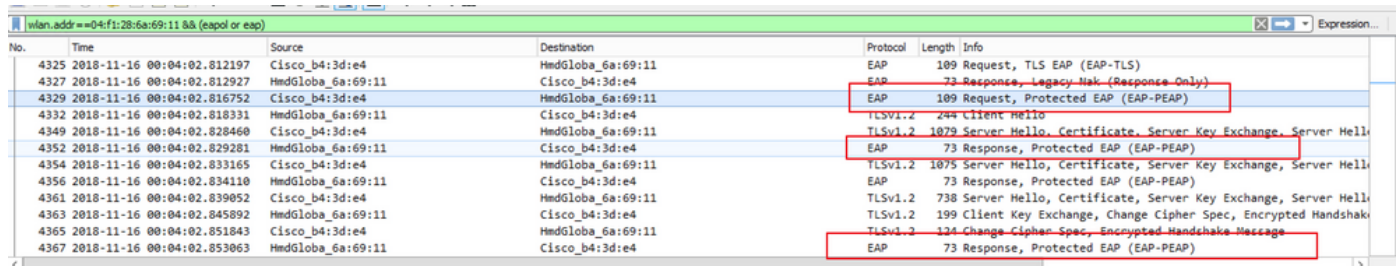
- Servidor Radius (FreeRADIUS o ISE)
- Dispositivo de captura de señal aérea
- Dispositivo Apple MacOS/OS X o Linux

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.

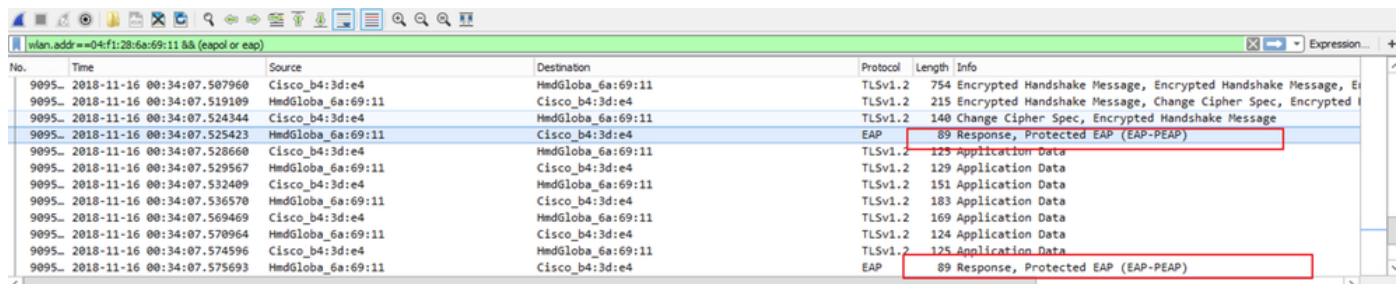
## Antecedentes

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.



No.	Time	Source	Destination	Protocol	Length	Info
4325	2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	EAP	109	Request, TLS EAP (EAP-TLS)
4327	2018-11-16 00:04:02.812927	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	EAP	73	Response, Legacy Nak (Response Only)
4329	2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	EAP	109	Request, Protected EAP (EAP-PEAP)
4332	2018-11-16 00:04:02.818331	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	244	Client Hello
4349	2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	1079	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4352	2018-11-16 00:04:02.829281	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)
4354	2018-11-16 00:04:02.833165	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	1075	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4356	2018-11-16 00:04:02.834110	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)
4361	2018-11-16 00:04:02.839052	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	738	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4363	2018-11-16 00:04:02.845892	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	199	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4365	2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	124	Change Cipher Spec, Encrypted Handshake Message
4367	2018-11-16 00:04:02.853063	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)



No.	Time	Source	Destination	Protocol	Length	Info
9095_	2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	754	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message
9095_	2018-11-16 00:34:07.519109	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	215	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
9095_	2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	140	Change Cipher Spec, Encrypted Handshake Message
9095_	2018-11-16 00:34:07.525423	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	89	Response, Protected EAP (EAP-PEAP)
9095_	2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	125	Application Data
9095_	2018-11-16 00:34:07.529567	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	129	Application Data
9095_	2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	151	Application Data
9095_	2018-11-16 00:34:07.536570	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	183	Application Data
9095_	2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	169	Application Data
9095_	2018-11-16 00:34:07.570964	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	124	Application Data
9095_	2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSv1.2	125	Application Data
9095_	2018-11-16 00:34:07.575693	HmdGlobo_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



**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 [función de registro de paquetes WLC](#), 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)

 radius_novlan.pcap	Pcap N...apture	22 KB	Today at 11:56 am
--	-----------------	-------	-------------------

### Tcpdump ISE (B)

 radius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm	850 KB	Pcap N...apture
---	-----------------------	--------	-----------------

### Combinado (A+B)

 radius_novlan_merged.pcapng	Pcapn...Capture	927 KB	Today at 12:28 pm
---	-----------------	--------	-------------------

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 = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

PMK:

```
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key =

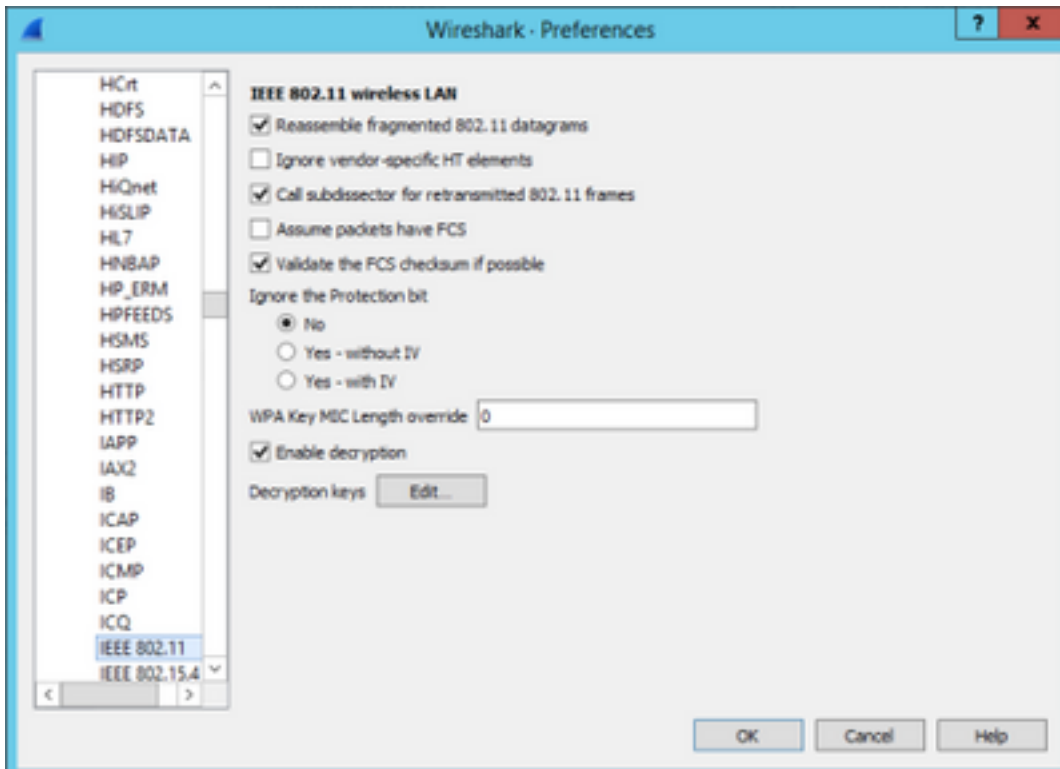
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d79848816a3793c5a4dfb1cfb b0e

PMK :

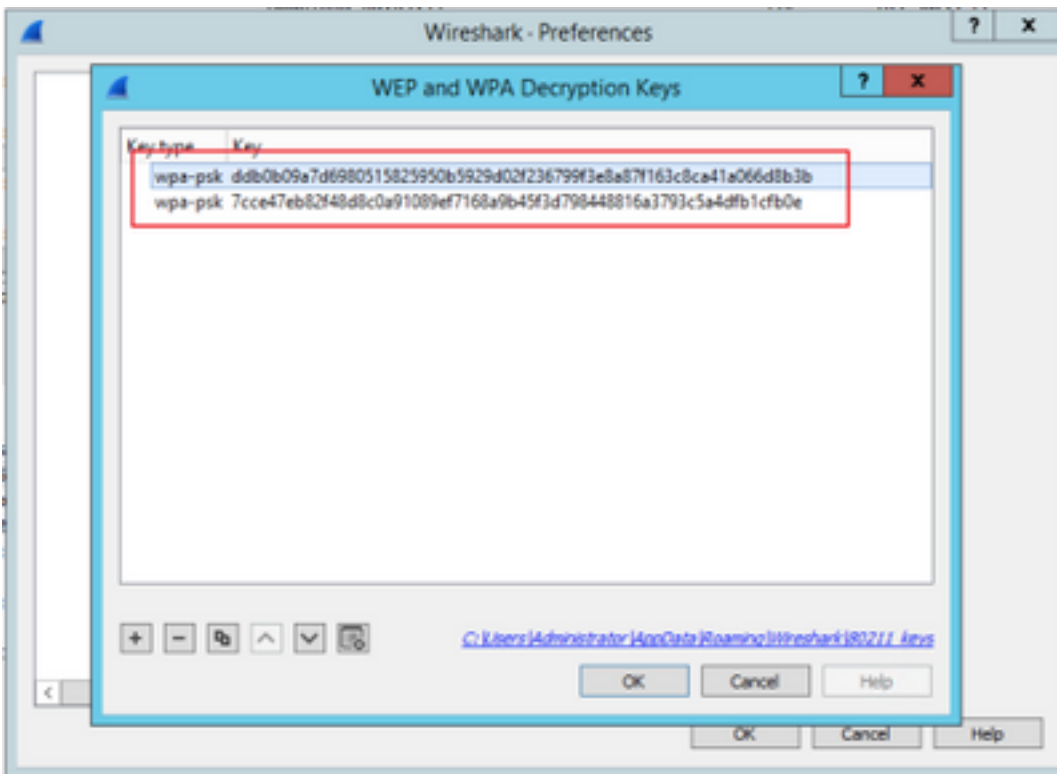
7cce47eb82f48d8c0a91089ef7168a9b45f3d79848816a3793c5a4dfb1cfb0e

### 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 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+).



### Ejemplo de un paquete 802.11 descifrado

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] Seq=3999908
397882	2018-11-16 00:17:08.098444	104.17.57.239	172.16.255.13	TCP	154	80 → 37553 [ACK] Seq=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] Seq=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) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
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/logo.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
  IEEE 802.11 QoS Data, Flags: .p.....TC
  Logical-Link Control
  Internet Protocol Version 4, Src: 172.16.255.13, Dst: 40.127.66.24
  Transmission Control Protocol, Src Port: 45658, 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 00 04 d9 a4 00 00 00 00 04 01 00  ....
0020 9e 09 0b 22 1f 00 06 00 65 00 00 04 00 00 00  ....
0030 88 41 30 00 80 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 af f4 c2 2f 90 d1 14 52 a5 8b 2e 57 27 3a  .... /-R...W':
0060 d8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 34 39 ca  T-U.....49-
0070 5c 08 7a 36 57 cd e2 43 89 86 f5 92 24 17 d0 db  \z6m-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  #l{..... 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 screenshot displays the Wireshark interface with a packet capture of IEEE 802.11 QoS Data. The packet list pane shows several packets, with packet 397886 highlighted in yellow. The packet details pane shows the structure of the IEEE 802.11 QoS Data frame, including the Radiotap Header, radio information, and the Data field. The packet bytes pane shows the raw hex and ASCII data of the captured frame.

**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 muestran 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

- [Twaking EAP's débil link - succión de PMK WiFi de RADIUS con pmkXtrat](#)
- [Cómo descodificar la clave MS-MPPE-Recv de Radius](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)