

Configurare Wireshark e FreeRADIUS per decrittografare 802.11 WPA2-Enterprise/EAP/dot1x over-the-air Wireless Sniffer

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Procedura](#)

[Passaggio 1. Decrittografare le chiavi PMK dal pacchetto di accettazione dell'accesso.](#)

[Passaggio 2. Estrarre i file PMK.](#)

[Passaggio 3. Decrittografare lo sniffer OTA.](#)

[Esempio di pacchetto 802.11 decrittografato](#)

[Esempio di pacchetto 802.11 crittografato](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come decrittografare gli sniffer OTA (Wireless Over-The-Air) crittografati Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) o 802.1x (dot1x) con qualsiasi metodo EAP (Extensible Authentication Protocol).

È relativamente facile decrittografare l'acquisizione 802.11 OTA basata su PSK/WPA2-personal a condizione che vengano acquisiti tutti gli handshake EAP over LAN (EAPoL) a quattro vie. Tuttavia, non è sempre consigliabile utilizzare una chiave già condivisa (PSK) dal punto di vista della protezione. Cancellare una password hardcoded è solo una questione di tempo.

Molte aziende scelgono quindi il dot1x con il servizio RADIUS (Remote Authentication Dial-In User Service) come soluzione di protezione migliore per le reti wireless.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FreeRADIUS con **radsniff** installato
- Wireshark/Omnipeek o qualsiasi software in grado di decrittografare il traffico wireless 802.11
- Privilegio per ottenere il segreto condiviso tra Network Access Server (NAS) e Authenticator.

- Capacità di acquisire l'acquisizione di pacchetti radius tra NAS e autenticatore dalla prima richiesta di accesso (da NAS a autenticatore) all'ultima accettazione di accesso (da autenticatore a NAS) durante la sessione EAP
- Capacità di eseguire l'acquisizione OTA (Over-the-Air) contenente handshake EAPoL a quattro vie

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

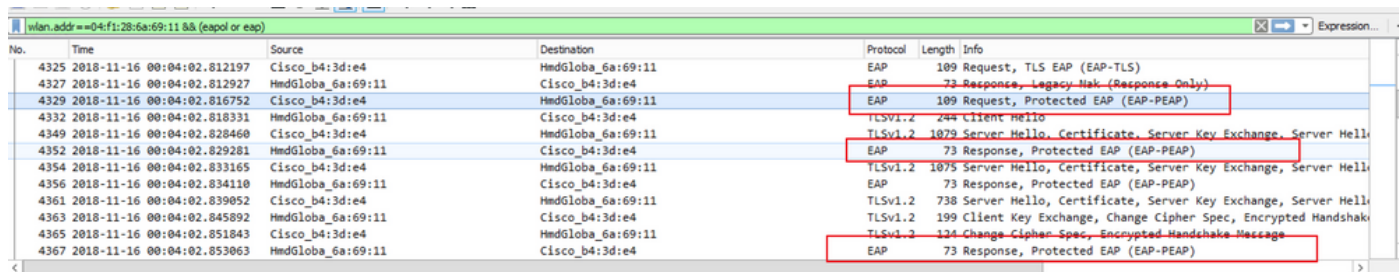
- Server Radius (FreeRADIUS o ISE)
- Dispositivo di acquisizione over-the-air
- Dispositivo Apple macOS/OS X o Linux

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

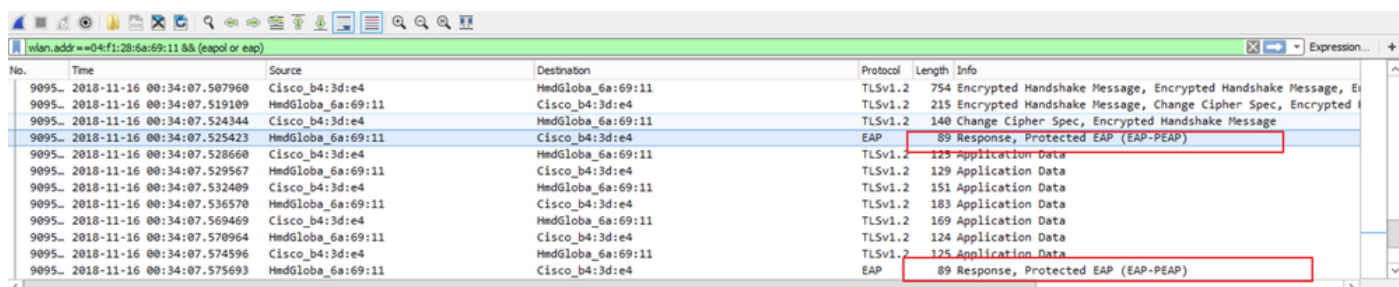
Premesse

Nell'esempio, due chiavi master Pairwise (PMK) vengono derivate da pacchetti Radius acquisiti da ISE 2.3, poiché il timeout della sessione su questo SSID è di 1800 secondi e l'acquisizione qui specificata è lunga 34 minuti (2040 secondi).

Come mostrato nell'immagine, EAP-PEAP è usato come esempio, ma può essere applicato a qualsiasi autenticazione wireless basata su 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	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	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 Hell
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 Hell
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 Hell
4362	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 Handshak
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, E
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
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)

Procedura

Passaggio 1. Decrittografare le chiavi PMK dal pacchetto di accettazione dell'accesso.

Suggerimento: In genere, il runtime del comando **radsniff** rispetto a un file pcap RADIUS può essere conteggiato come una scala di secondi. Tuttavia, se il **radsniff** è bloccato in questo stato indicato nel log, collegare in serie questa acquisizione pacchetto (A) con un'altra acquisizione pacchetto più lunga (B) tra lo stesso NAS e l'autenticatore. Eseguire quindi il comando **radsniff** sul pacchetto a cascata (A+B). L'unico requisito dell'acquisizione del pacchetto (B) è la possibilità di eseguire il comando **radsniff** su di esso e visualizzare un risultato dettagliato.


```
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)
```

Nell'esempio, il control plane logging (A) del Wireless Lan Controller (WLC), acquisito tramite la funzione di [registrazione dei pacchetti WLC](#), viene acquisito in cascata con una durata maggiore dal protocollo TCPdump (B) di ISE. La registrazione dei pacchetti WLC è usata come esempio perché di solito è di dimensioni molto piccole.

Registrazione pacchetti WLC (A)

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

ISE Tcpdump (B)

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

Unito (A+B)

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

Eseguire quindi il **radsniff** sulla cuffia unita (A+B) per visualizzare l'output dettagliato.

```
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>
```

Passaggio 2. Estrarre i file PMK.

Viene quindi presentata l'eliminazione del campo 0x in ogni **MS-MPPE-Recv-Key** dall'output dettagliato e le PMK necessarie per la decodifica del traffico wireless.

MS-MPPE-Recv-Key =

0xdb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

PMK:

ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

MS-MPPE-Recv-Key =

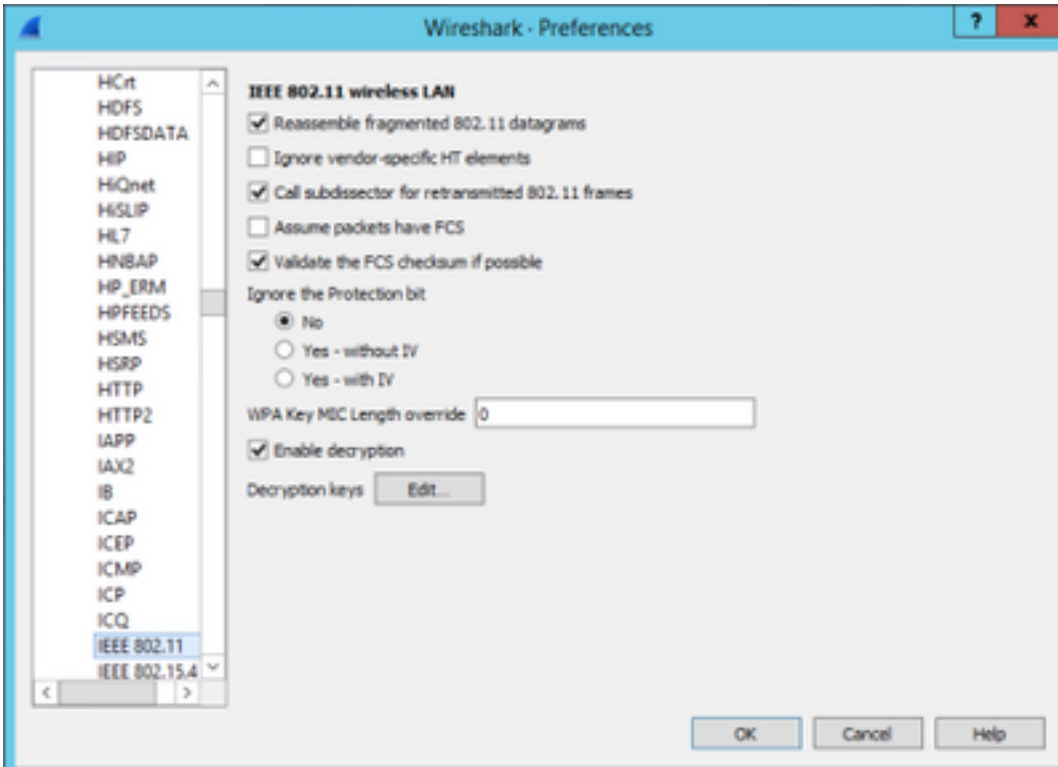
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

PMK :

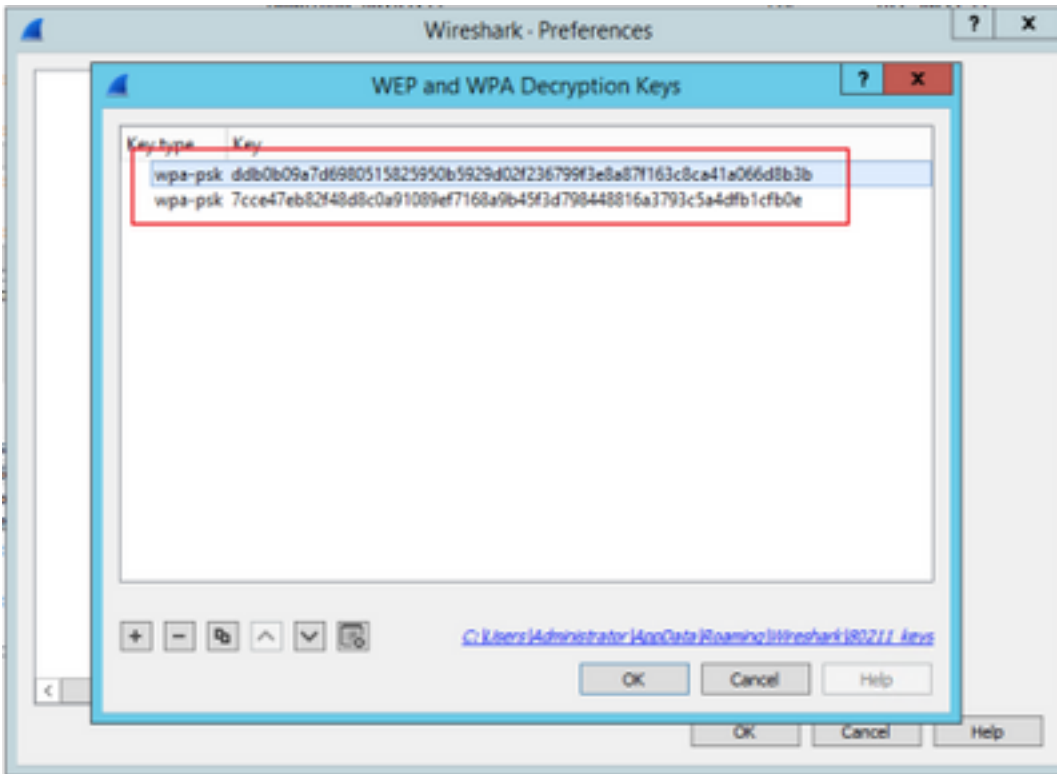
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Passaggio 3. Decrittografare lo sniffer OTA.

Passare a **Wireshark > Preferenze > Protocolli > IEEE 802.11**. Quindi selezionare **Abilita decrittografia** e fare clic sul pulsante **Modifica** accanto a **Chiavi di decrittografia**, come mostrato nell'immagine.



Selezionare quindi **wpa-psk** come tipo di chiave, inserire le PMK derivate nel campo **Chiave** e fare clic su **OK**. Al termine, l'acquisizione OTA deve essere decrittata ed è possibile visualizzare informazioni sul livello superiore (3+).



Esempio di pacchetto 802.11 decrittografato

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...	HmdGlobo_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...	HmdGlobo_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	HmdGlobo_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...	HmdGlobo_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...	HmdGlobo_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...	HmdGlobo_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-
  
```

Se si confronta il secondo risultato dove PMK non è incluso, con il primo risultato, dove PMK è incluso, il pacchetto 397886 viene decrittato come dati QoS 802.11.

Esempio di pacchetto 802.11 crittografato

The screenshot displays the Wireshark interface with a packet capture of 802.11 QoS Data. The packet list pane shows several packets, with packet 397886 highlighted. The packet details pane shows the structure of the 802.11 radio information, including IEEE 802.11 QoS Data and Data (68 bytes). The packet bytes pane shows the raw hex and ASCII data.

Attenzione: È possibile che si verifichino problemi con Wireshark in fase di decrittografia e in tal caso, anche se viene fornito il PMK corretto (o se viene utilizzato il PSK, vengono forniti sia il SSID che il PSK), Wireshark non decifra l'acquisizione OTA. Per ovviare al problema, spegnere e riaccendere Wireshark alcune volte fino a quando non si ottengono informazioni sul layer più elevato e i pacchetti 802.11 non vengono più visualizzati come dati QoS, oppure utilizzare un altro PC/Mac con Wireshark installato.

Suggerimento: un codice C++ chiamato pmkXtract è allegato al primo post in Informazioni correlate. I tentativi di compilazione sono stati completati correttamente e viene ottenuto un file eseguibile, ma il programma eseguibile non sembra eseguire correttamente la decrittografia per motivi sconosciuti. Inoltre, uno script Python che tenta di estrarre PMK è pubblicato nell'area commenti al primo post, che può essere ulteriormente esplorato se i lettori sono interessati.

Informazioni correlate

- [Modificare il collegamento debole di EAP - risucchiare i PMK WiFi da RADIUS con pmkXtract](#)
- [Come decodificare il raggio MS-MPPE-Recv-Key](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)