قم بتكوين Wireshark و FreeRADIUS من أجل فك تشفير 802.11 WPA2-enterprise/EAP/dot1x عبر الهواء لمشاللاسلكي

المحتويات

المقدمة

يصف هذا المستند طريقة فك تشفير Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) وأ 802.1x (dot1x) Encrypted Wireless over-Air (OTA) Sniffer مع أي أساليب لبروتوكول المصادقة المتوسع (EAP).

من السهل نسبيا فك تشفير ميزة التقاط 802.11 OTA القائمة على PSK/WPA2-الشخصي بناء على EAP رباعي الإتجاه عبر LAN (EAPoL). ومع ذلك، الهدف دائما بالمفتاح المشترك مسبقا (PSK) من منظور أمان. إن سحق كلمة المرور ذات الترميز الثابت مسألة وقت الأكثر.

وبالتالي، تختار العديد من المؤسسات dot1x مع خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS) كحل أمان أفضل لشبكاتهم اللاسلكية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FreeRADIUS مع **Radsniff** مثبت
- Wireshark/Omnipeek أو أي برنامج قادر على فك تشفير حركة مرور البيانات اللاسلكية 802.11

- امتياز أن يحصل على السر مشترك بين شبكة منفذ نادل (NAS) ومصادقة
- القدرة على التقاط حزمة RADIUS بين NAS والمصادقة من طلب الوصول الأول (من NAS إلى المصدق) إلى آخر قبول وصول (من المصدق إلى NAS) خلال جلسة EAP
- القدرة على إجراء عمليات الالتقاط عبر الهواء (OTA) التي تحتوي على مصافحة EAPoL رباعية الإتجاه

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

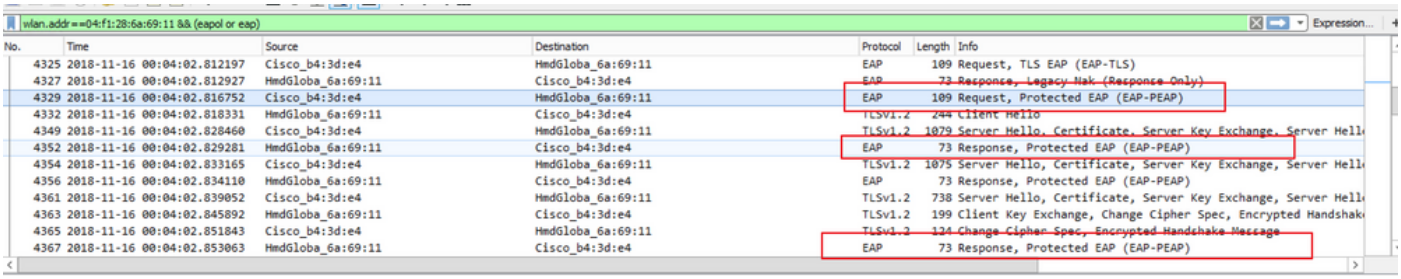
- خادم RADIUS (FreeRADIUS أو ISE)
- جهاز التقاط عبر الهواء
- جهاز Apple MacOS/OS X أو Linux

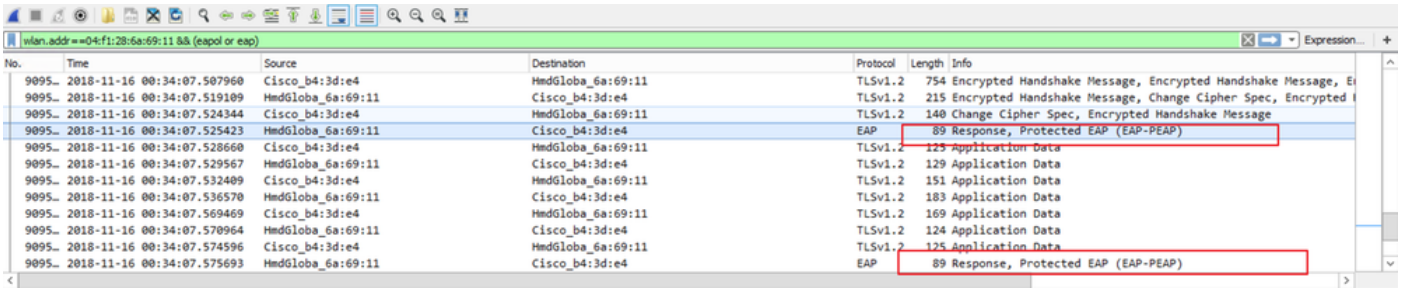
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

في هذا المثال، يتم اشتقاق مفتاحين أساسيين من حزم RADIUS التي تم التقاطها من ISE 2.3، حيث أن مهلة جلسة المعمل على SSID هذا هي 1800 ثوان، والتقاط المعطى هنا هو 34 دقيقة (2040 ثوان) طويلة.

كما هو موضح في الصورة، يستخدم EAP-PEAP كمثال، لكن يمكن تطبيق ذلك على أي مصادقة السلكية تستند إلى dot1x.





الإجراء

الخطوة 1. فك تشفير PMK (آت) من حزمة قبول الوصول.

ركضت الradsniff مقابل قبض نصف قطر بين NAS والمصادقة in order to استخرجت PMK. السبب وراء إستخراج حزمتين لقبول الوصول أثناء الالتقاط هو أن مؤقت مهلة جلسة العمل تم تعيينه على 30 دقيقة على هذا SSID المحدد والاستيلاء هو 34 دقيقة طويلة. يتم إجراء

المصادقة مرتين.

```
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 = 0x52656175746853657373696f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373a4953452d322d332f333238323731323338
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 = 0x52656175746853657373696f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373a4953452d322d332f333238323731323338
2f33303434

EAP-Message = 0x03910004

Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9

MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb2988741259284701 14d009b5fb

MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e<<<<<<<<<<<<<<<<<<PMK

Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

ملاحظة: يرجى إزالة أي عمامة شبكة LAN الظاهرية (VLAN) من التقاط حزمة Radius، وإلا، فإن **Radsniff** لا يتعرف على ملف PCAP الداخل. لإزالة أي عمامة VLAN، على سبيل المثال، يمكن استخدام editcap.

تلميح: بشكل عام، يمكن حساب وقت تشغيل الأمر **Radsniff** مقابل ملف RADIUS PCAP

كمقياس للثواني. مهما، إن **الJRadsniff** التصق في هذه دولة يبدي في السجل، رجاء تعاقب هذا ربط التقاط (a) مع آخر ربط أطول (B) بين ال نفسه NAS و مصدق. بعد ذلك، قم بتشغيل الأمر radsniff مقابل الحزمة المتتالية (A+B). المتطلب الوحيد للتقاط الحزمة (B) هو أن أنت يستطيع أن يركض ال radsniff أمر ضده وأن يرى نتيجة.

```
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)
```

في هذا المثال، يتم تجميع تسجيل مستوى التحكم في وحدة تحكم الشبكة المحلية اللاسلكية (WLC) (A) الذي يتم التقاطه عبر ميزة تسجيل حزم WLC، مع التقاط أطول من ميزة ISE TCPdump (B). يتم إستخدام تسجيل حزم WLC كمثال لأنه عادة صغير الحجم للغاية.

تسجيل حزم WLC (A)

تفريغ ISE (B)

مدمجة (A+B)

ثم قم بتشغيل **الراديوس** مقابل PCAP المدمج (A+B) وستتمكن من رؤية مخرجات التصحيح.

```
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>
```

الخطوة 2. إستخراج PMK (وحدات).

يتم بعد ذلك حذف حقل 0x في كل **MS-MPPE-Recv-Key** من خرج المحتوى و PMKs المطلوب لفك تشفير حركة المرور اللاسلكية.

MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

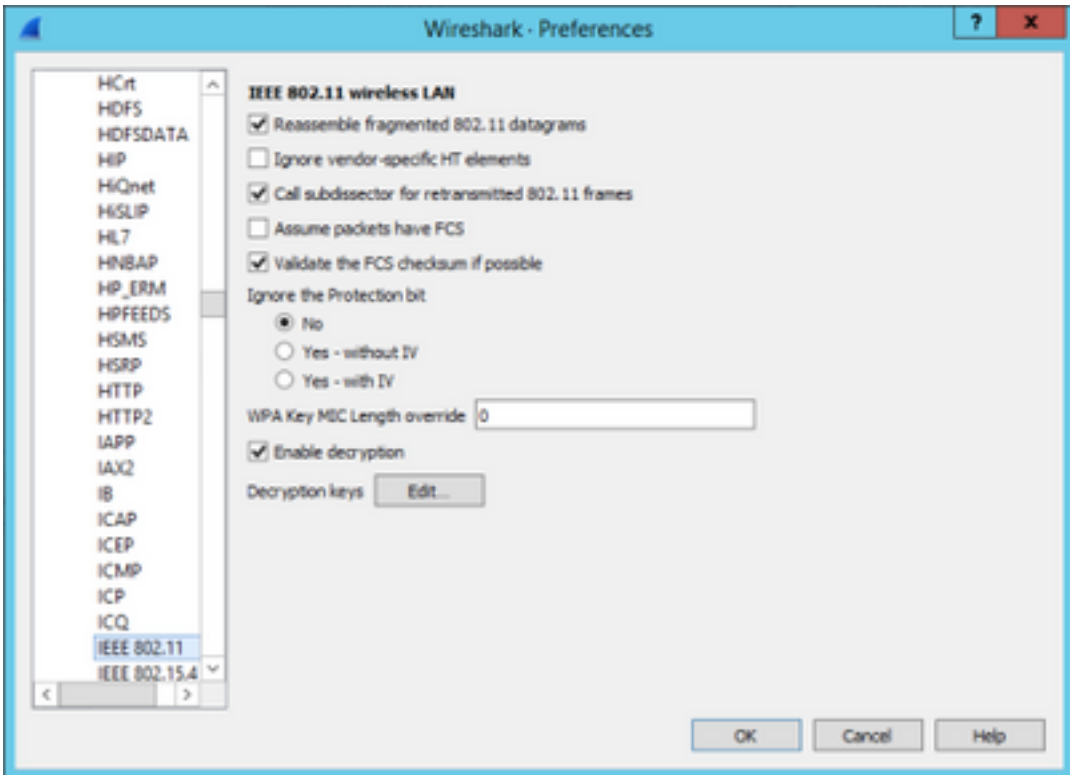
```
PMK:
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1cfb0e

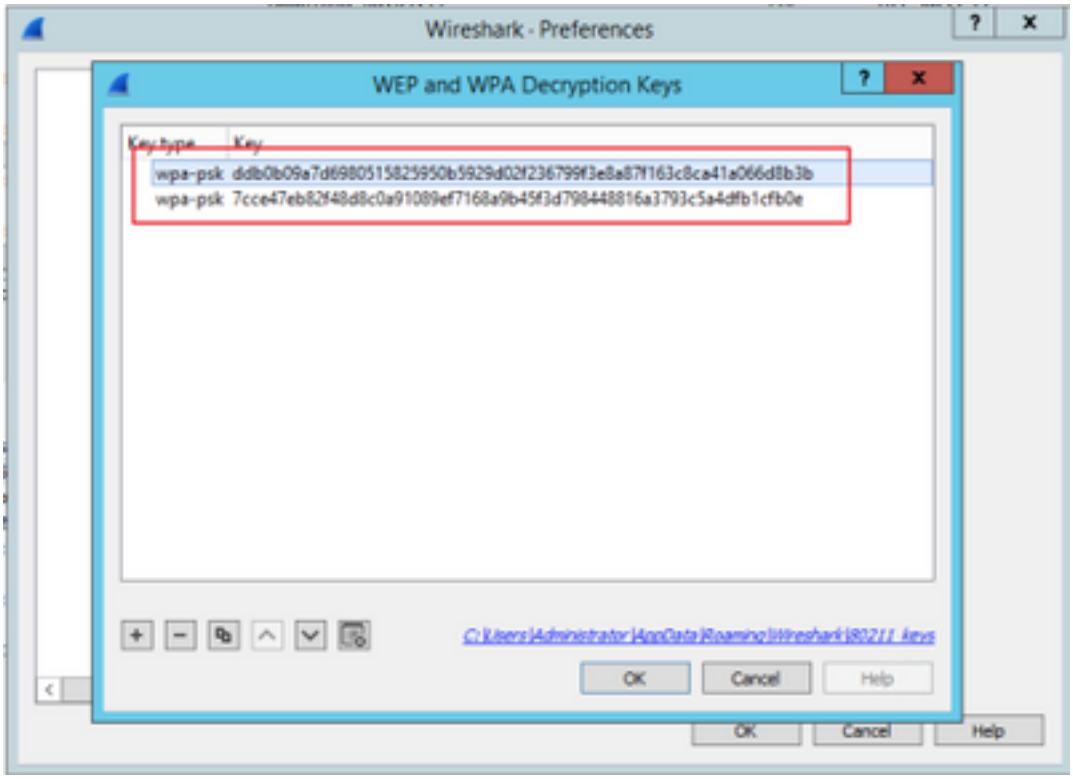
```
PMK:
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e
```

الخطوة 3. فك تشفير OTA sniffer.

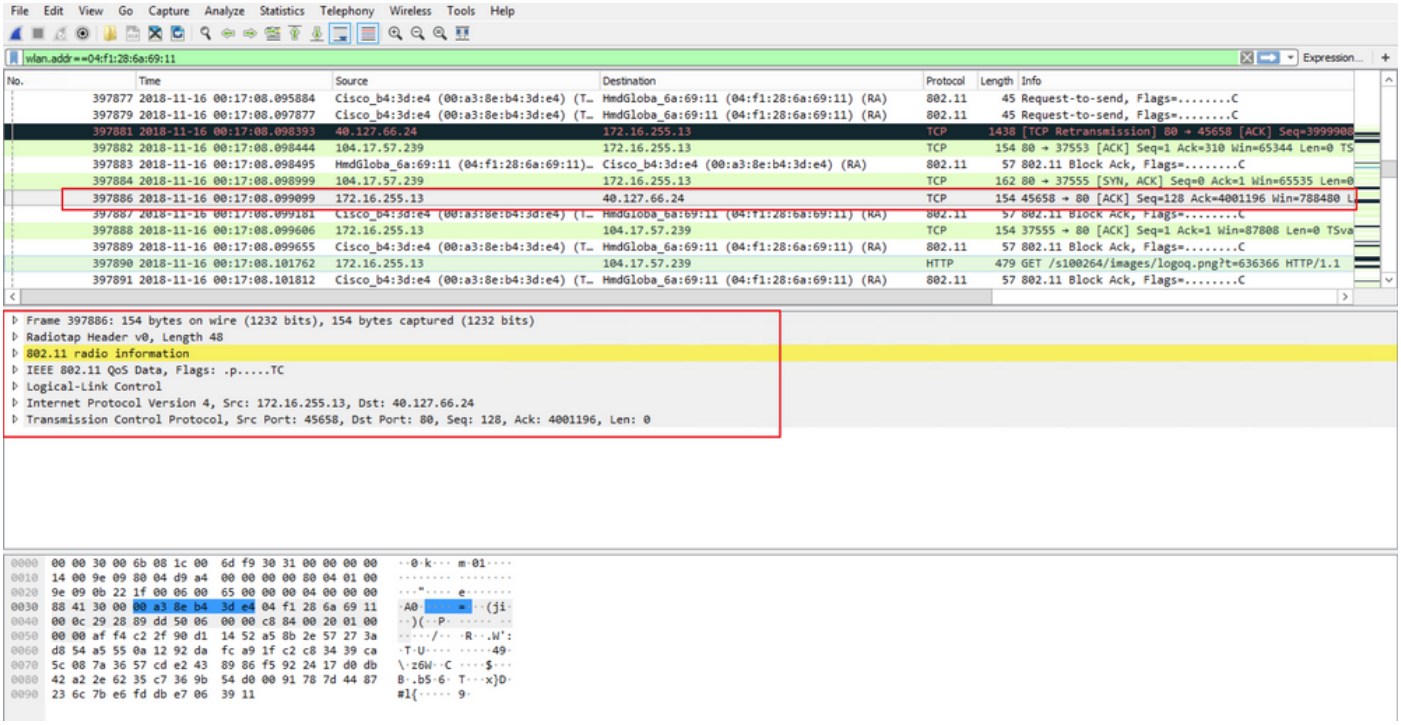
انتقل إلى **Wireshark > تفضيلات > بروتوكولات > IEEE 802. 11. ثم اضغط على تمكين فك التشفير** وانقر على زر **تحرير** الموجود بجوار **مفاتيح فك التشفير**، كما هو موضح في الصورة.



بعد ذلك، يرجى تحديد **WPA-PSK** كنوع المفتاح، ووضع PMKs المشتقة في حقل **المفتاح**، ثم انقر على **موافق**. بعد إكمال هذا، يجب فك تشفير التقاط OTA ويمكنك رؤية معلومات الطبقة الأعلى (3+).

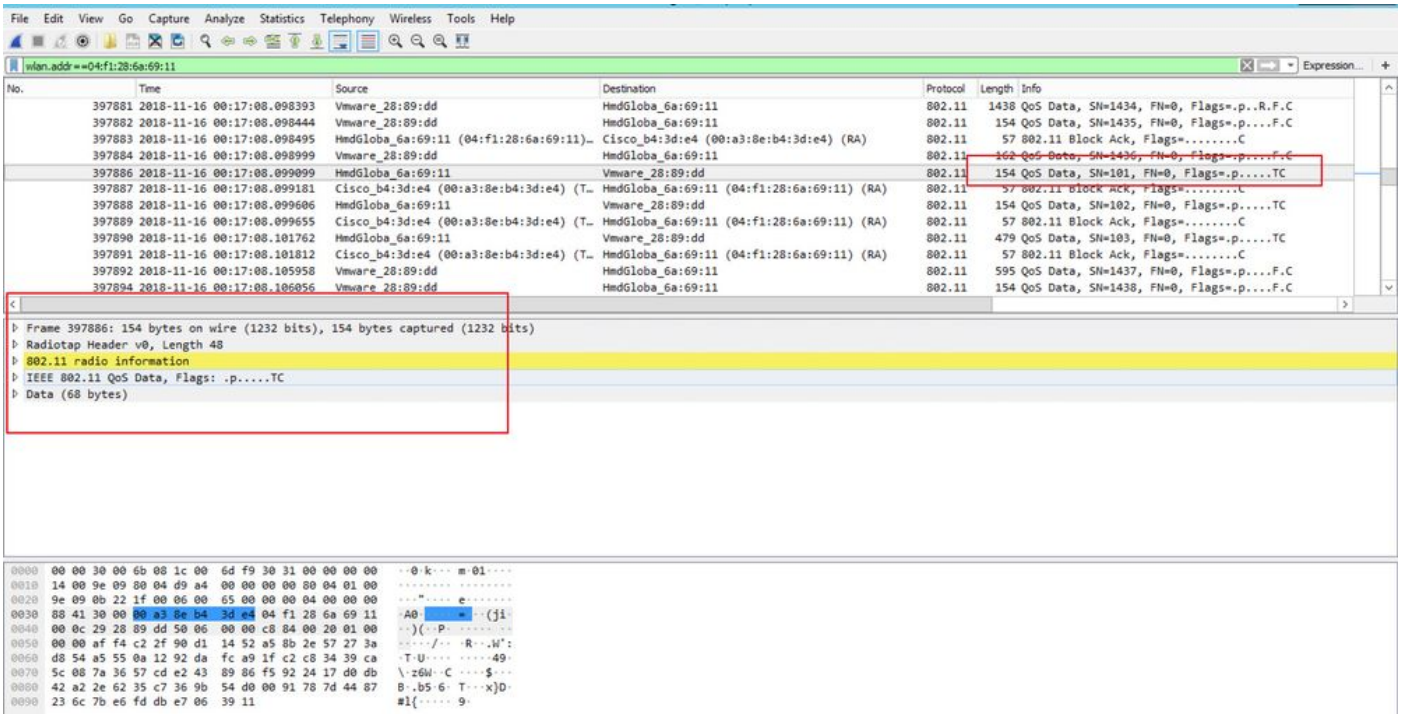


مثال على حزمة 802.11 التي تم فك تشفيرها



إذا قمت بمقارنة النتيجة الثانية حيث لم يتم تضمين PMK، مع النتيجة الأولى، حيث يتم تضمين PMK، يتم فك تشفير الحزمة 397886 كبيانات جودة الخدمة 802.11.

مثال على حزمة 802.11 المشفرة



تحذير: قد تواجه مشكلة مع Wireshark في فك التشفير، وفي هذه الحالة، حتى في حالة توفير PMK الصحيح، (أو في حالة إستخدام PSK، يتم توفير كل من SSID و PSK)، الا يقوم Wireshark بفك تشفير التقاط OTA. الحل البديل هو إيقاف تشغيل Wireshark ثم تشغيله عدة مرات حتى يمكن الحصول على معلومات طبقة أعلى وعدم عرض حزم 802.11 كبيانات جودة الخدمة، أو استخدام كمبيوتر/نظام آخر حيث يتم تثبيت Wireshark.

تلميح: تم إرفاق رمز C++ يسمى pmkXtract في المنشور الأول في المعلومات ذات الصلة. تمت محاولات التحويل البرمجي بنجاح وتم الحصول على ملف تنفيذي، ولكن يبدو أن البرنامج التنفيذي الا يقوم بفك التشفير بشكل صحيح لبعض الأسباب المعروفة. بالإضافة إلى ذلك، يتم نشر سيناريو Python الذي يحاول إستخلاص PMK في منطقة التعليقات على مدة النشر الأولى، والتي يمكن إستكشافها بشكل أكبر إذا كان القارئ مهتمين.

معلومات ذات صلة

- [تحويل إرتباط EAP الضعيف - إمتصاص WiFi PMKs خارج RADIUS باستخدام PMKxtract]
- [كيفية فك تشفير RADIUS MS-MPPE-Recv-Key]
- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).