Configure o Wireshark e o FreeRADIUS para descriptografar o Sniffer sem fio 802.11 WPA2-Enterprise/EAP/dot1x over-the-air

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Procedimento](#)
[Etapa 1. Descriptografar PMK(s) do pacote Access-accept.](#)
[Etapa 2. Extraia PMK(s).](#)
[Etapa 3. Descriptografar o Sniffer OTA.](#)
[Exemplo de um pacote 802.11 descriptografado](#)
[Exemplo de um pacote 802.11 criptografado](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como descriptografar o sniffer de Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) ou 802.1x (dot1x) criptografado sem fio por via aérea (OTA), com qualquer método EAP (Extensible Authentication Protocol).

Érelativamente fácil descriptografar a captura OTA 802.11 baseada em PSK/WPA2-Personal, desde que sejam capturados os handshakes EAPover LAN (EAPoL) completos de quatro vias. No entanto, a chave pré-compartilhada (PSK) nem sempre é recomendada do ponto de vista da segurança. Decifrar uma senha codificada é apenas uma questão de tempo.

Portanto, muitas empresas escolhem o dot1x com Remote Authentication Dial-In User Service (RADIUS) como uma melhor solução de segurança para sua rede sem fio.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FreeRADIUS com o **radsniff** instalado
- Wireshark/Omnipeek ou qualquer software capaz de descriptografar o tráfego sem fio 802.11
- Privilégio de obter o segredo compartilhado entre o Network Access Server (NAS) e o Authenticator
- Capacidade de capturar a captura de pacote raio entre o NAS e o autenticador da primeira

solicitação de acesso (do NAS para o autenticador) para a última aceitação de acesso (do autenticador para o NAS) durante toda a sessão EAP
- Capacidade de executar captura OTA (Over-the-Air) contendo handshakes EAPoL de quatro vias

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

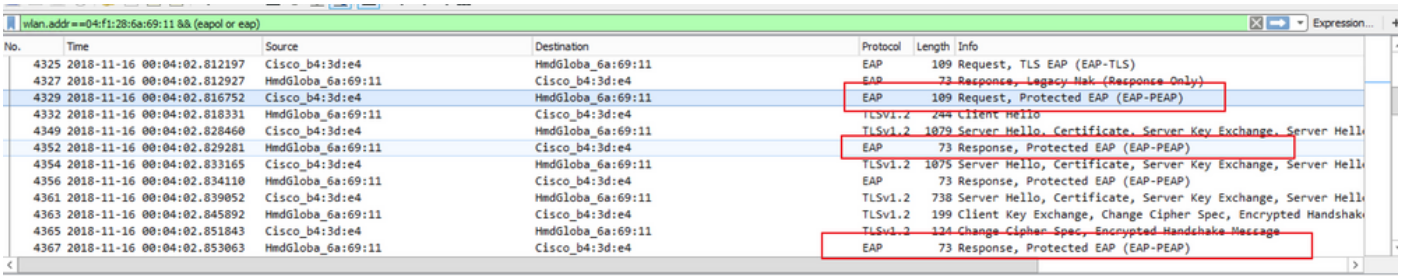
- Servidor Radius (FreeRADIUS ou ISE)
- Dispositivo de captura over-the-Air
- Apple macOS/OS X ou dispositivo Linux

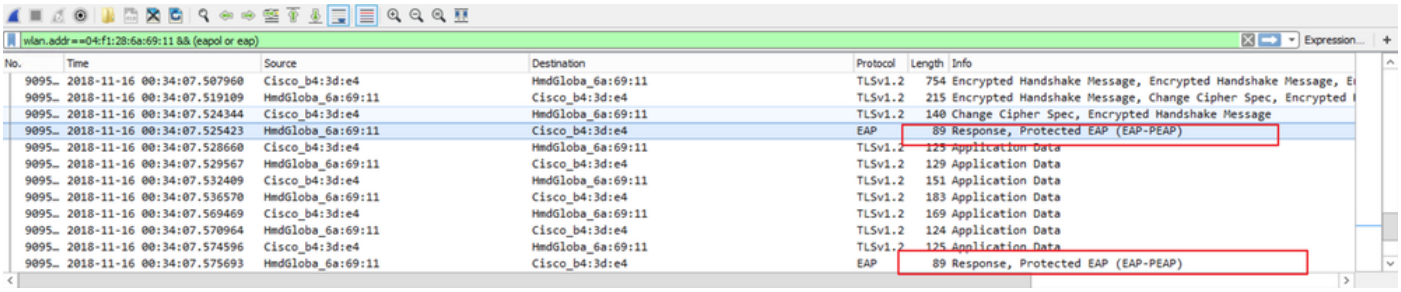
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Neste exemplo, duas PMKs (Pairwise Master Keys) são derivadas de pacotes Radius capturados do ISE 2.3, já que o tempo limite da sessão neste SSID é de 1800 segundos, e a captura fornecida aqui tem 34 minutos (2040 segundos).

Como mostrado na imagem, o EAP-PEAP é usado como exemplo, mas isso pode ser aplicado a qualquer autenticação sem fio baseada em dot1x.





Procedimento

Etapa 1. Descriptografar PMK(s) do pacote Access-accept.

Execute o **radsniff** contra a captura de raio entre o NAS e o Authenticator para extrair o PMK. A razão pela qual dois pacotes aceitos pelo acesso são extraídos durante a captura é que o temporizador de tempo limite da sessão é definido como 30 minutos neste SSID específico e a captura tem 34 minutos de duração. A autenticação é executada duas vezes.

```
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 =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f333238323731323338
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 =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f333238323731323338
2f33303434

EAP-Message = 0x03910004

Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9

MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb

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

Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

Note: Remova qualquer marca de LAN virtual (VLAN) da captura de pacote Radius; caso contrário, **radsniff** não reconhece o arquivo pcap de entrada. Para remover qualquer marca de VLAN, por exemplo, editcap pode ser usado.

Tip: Geralmente, o tempo de execução do comando **radsniff** em um arquivo pcap RADIUS pode ser contado como uma escala de segundos. No entanto, se o **radsniff** estiver preso nesse estado mostrado no registro, faça a cascata dessa captura de pacote (A) com outra

captura de pacote (B) mais longa entre o mesmo NAS e o mesmo Autenticador. Em seguida, execute o comando radsniff no pacote em cascata (A+B). O único requisito da captura de pacotes (B) é que você pode executar o comando radsniff contra ele e ver um resultado detalhado.

```
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)
```

Neste exemplo, o registro de plano de controle (A) do Wireless Lan Controller (WLC) capturado por meio do recurso de registro de pacotes da WLC, é em cascata com uma captura mais longa do TCPdump (B) do ISE. O registro de pacotes da WLC é usado como exemplo, porque geralmente é muito pequeno.

Registro de pacote (A) da WLC

Tcpdump ISE (B)

Mesclado (A+B)

Em seguida, execute o **radsniff** contra o pcap mesclado (A+B) e você poderá ver a saída verbosa.

```
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>
```

Etapa 2. Extraia PMK(s).

A exclusão de um campo 0x em cada **MS-MPPE-Recv-Key** da saída verbosa e os PMKs necessários para o decodificador de tráfego sem fio são então apresentados.

MS-MPPE-Chave-Recv = 0xdb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41ca066d8b3b

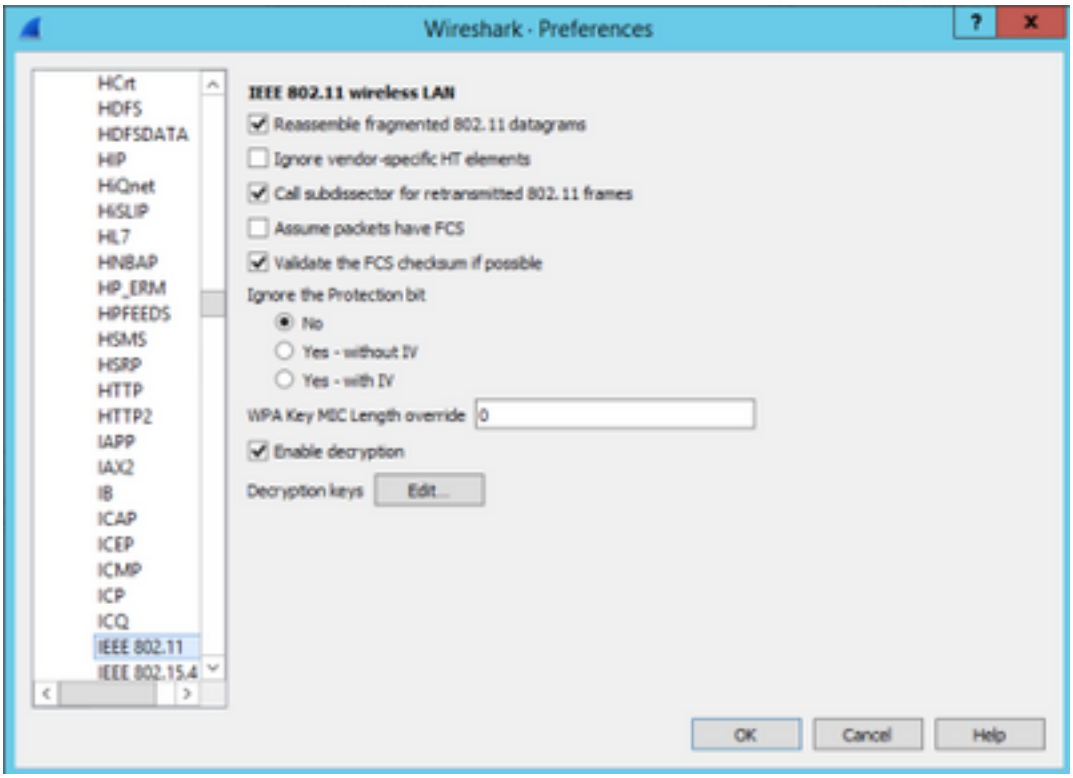
```
PMK:
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1ccb0e

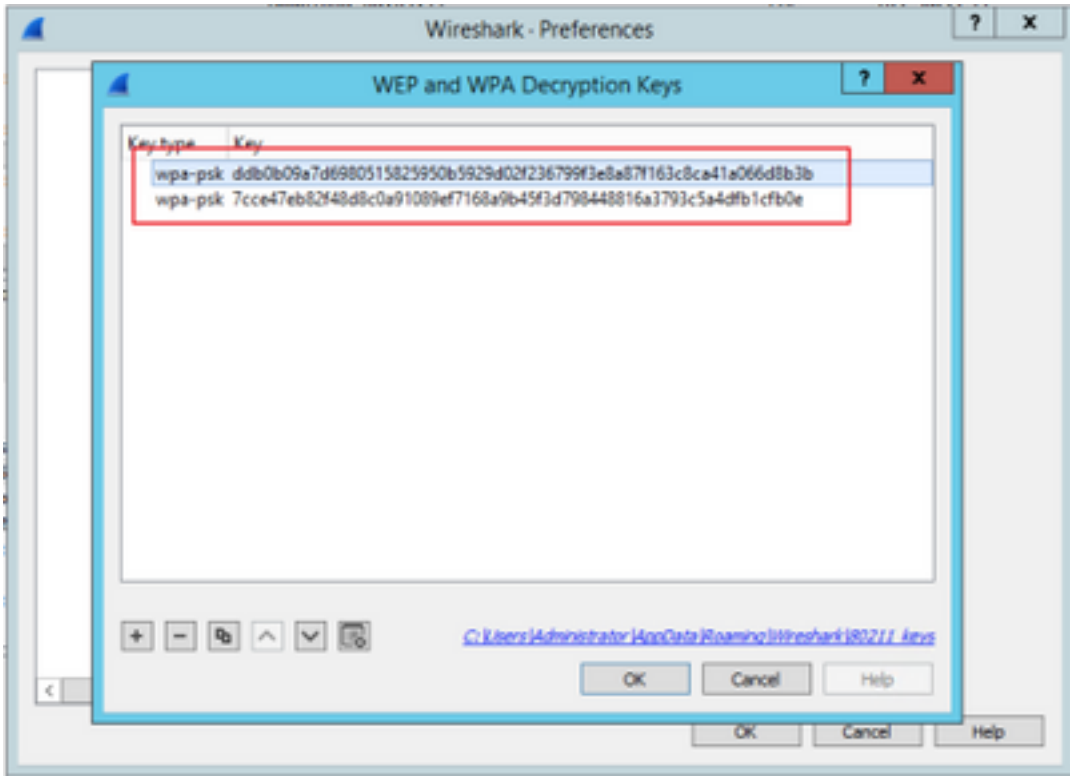
PMK:
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Etapa 3. Descriptografar o Sniffer OTA.

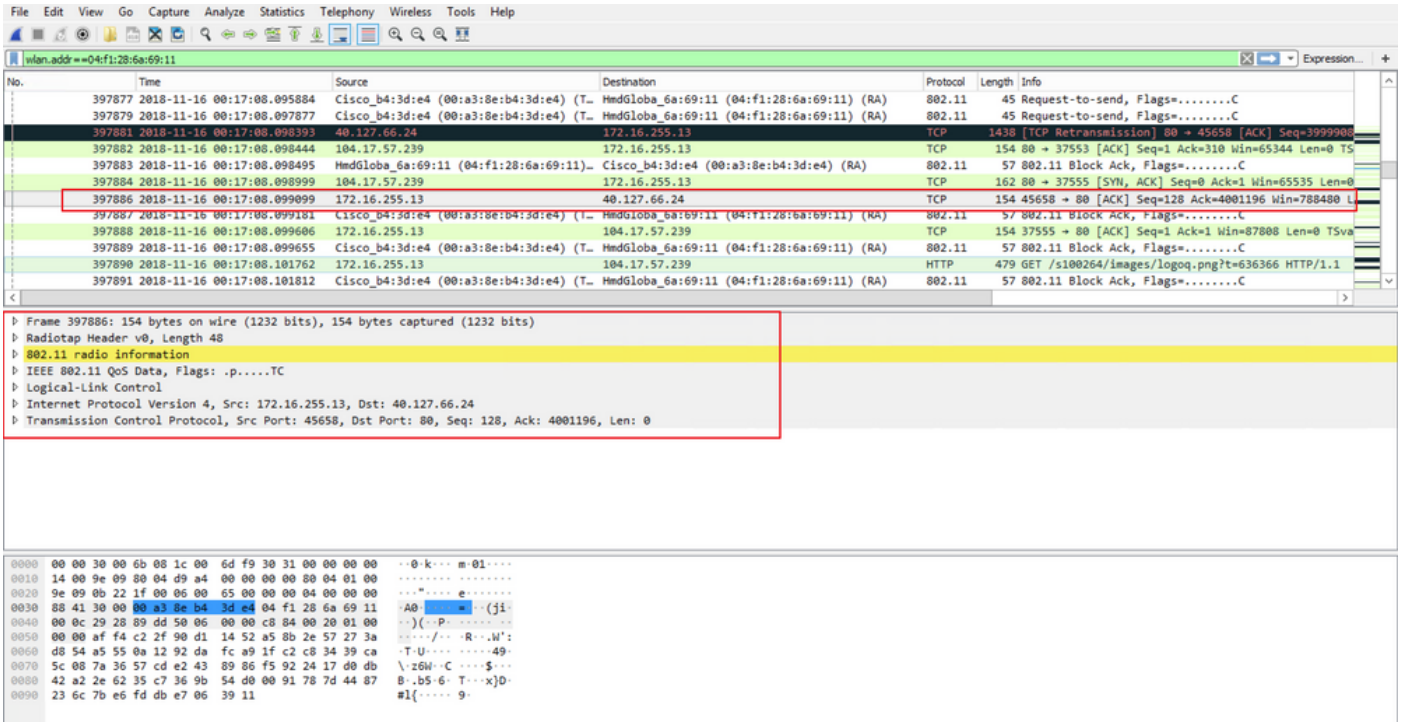
Navegue até **Wireshark > Preferences > Protocols > IEEE 802.11.** Em seguida, marque **Enable Decryption (Ativar descriptografia)** e clique no botão **Edit (Editar)** ao lado de **Decryption Keys (Chaves de descriptografia)**, como mostrado na imagem.



Em seguida, selecione **wpa-psk** como o tipo de chave, coloque os PMKs derivados no campo **Key** e clique em **OK**. Depois que isso for concluído, a captura OTA deverá ser descriptografada e você poderá ver informações da camada superior (3+).

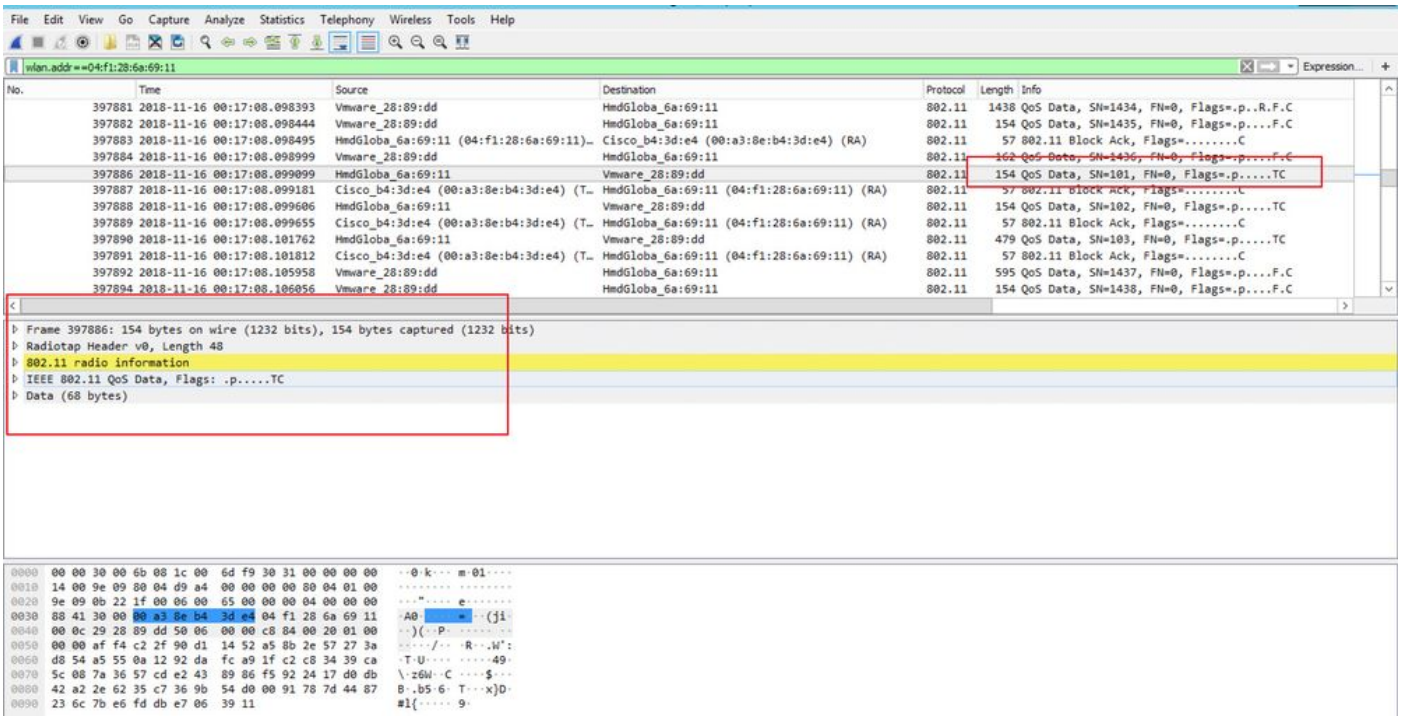


Exemplo de um pacote 802.11 descriptografado



Se você comparar o segundo resultado em que o PMK não está incluído, com o primeiro resultado, em que o PMK está incluído, o pacote 397886 é descriptografado como dados de QoS 802.11.

Exemplo de um pacote 802.11 criptografado



Caution: Você pode encontrar um problema com o Wireshark na descriptografia e, nesse caso, mesmo se o PMK correto for fornecido (ou se a PSK for usada, o SSID e a PSK forem fornecidos), o Wireshark não descriptografa a captura OTA. A solução alternativa é desligar o Wireshark e ligá-lo algumas vezes até que as informações da camada mais alta possam ser obtidas e os pacotes 802.11 não sejam mais mostrados como dados de QoS, ou usar

outro PC/Mac onde o Wireshark está instalado.

Dica: um código C++ chamado pmkXtract está anexado à primeira publicação em Informações Relacionadas. As tentativas de compilação foram bem-sucedidas e um arquivo executável é obtido, mas o programa executável não parece executar a descriptografia corretamente por alguns motivos desconhecidos. Além disso, um script Python que tenta extrair PMK é publicado na área de comentários da primeira publicação, que pode ser explorada se os leitores estiverem interessados.

Informações Relacionadas

- Ajustando o link fraco do EAP - extraindo PMKs Wi-Fi do RADIUS com pmkXtract
- Como decodificar MS-MPPE-Recv-Key RADIUS
- Suporte Técnico e Documentação - Cisco Systems