تمكين LWAPP Decodes جمارب على EtherPeek 3.0 و WildPacket OmniPeek

المحتويات

المقدمة

تتضمن WildPacket OmniPeek (و EtherPeek) أدوات فك تشفير بروتوكول نقطة الوصول (LWAPP) خفيفة الوزن متوفرة، ولكنها غير موصلة. يشرح هذا المستند كيفية تمكين عمليات فك تشفير LWAPP واستخدام البرنامج للنظر إلى LWAPP. يستخدم هذا المستند إجراء EtherPeek 3.0 و OmniPeek 5.0.

ملاحظة: الإجراء الخاص ب OmniPeek 3.0 هو نفس الإجراء الخاص ب EtherPeek 3.0.

ملاحظة: الفرق الوحيد بين برامج OmniPeek و EtherPeek هو موقع الملفات.

- مسار OmniPeek هو c:/Program Files/WildPacket/OmniPeek.
- مسار EtherPeek هو c:/program files/wildPacket/EtherPeek.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من EtherPeek، و OmniPeek 3.0 و 5.0 برمجية. أحلت لمعلومة على EtherPeek، EtherPeek سؤال . لمزيد من المعلومات حول OmniPeek، ارجع إلى تقديم OMNI .

المكونات المستخدمة

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

- OmniPeek 3.0

- EtherPeek 3.0
- OmniPeek 5.0

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تعديل ملف فك ترميز LWAPP

لتعديل ملف فك تشفير LWAPP، أضف "ETHR 0 0 90 c2 AP identity"::؛ إلى وظيفة LWAPP. يوجد هذا مباشرة تحت بند "LABL 0 0 0 B1 Lightweight Access Point Protocol\LWAPP"::؛ في LWAPP- ملف C:\Program Files\WildPackets\EtherPeek\Decodes...light_weight (protocol.dcd).

تعديل TCP_UDP_Ports.dcd

في الملف TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes)، يجب تضمين هذين السطرين:

```
;0x2fbe | LWAPP
;0x2fbf | LWAPP
```

ملاحظة: لم يتم فتح أي منافذ على الكمبيوتر المضيف كنتيجة لهذه العملية. لذلك، لا تعرض هذه الخطوة الكمبيوتر المضيف لأي مخاطر أمنية.

بهذه الطريقة، يتم تضمين المنفذين 1222 و 12223.

تعديل ملف PSPES.xml

أكمل الخطوات التالية:

1. في قسم بروتوكول مخطط بيانات المستخدم (UDP) من الملف pspes.xml (C:\Program Files\WildPackets\EtherPeek\1033)، أضف الأسطر التالية:**ملاحظة:** تأكد من إجراء نسخ إحتياطي للملف الأصلي أولا.

```
<"PSpec Name="LWAPP>
<PSpecID>6677</PSpecID>
<LName>LWAPP</LName>
<SName>LWAPP</SName>
<Desc>LWAPP</Desc>
<Color>color_1</Color>
<CondSwitch>12222</CondSwitch>
<CondSwitch>12223</CondSwitch>
<"PSpec Name="LWAPP Data>
<PSpecID>6688</PSpecID>
<LName>LWAPP Data</LName>
<SName>LWAPP-D</SName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12222) || (DestPort == 12222)]]></CondExp>
<PSpec/>

<"PSpec Name="LWAPP Control>
<PSpecID>6699</PSpecID>
<LName>LWAPP Control</LName>
```

```
                                        <SName>LWAPP-C</SName>
                                         <DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
                                                <PSpec/>
                                                    <PSpec/>
```

2. قم بإعادة تشغيل OmniPeek أو EtherPeek حتى تصبح التغييرات التي قمت بها نافذة المفعول.

فك تشفير LWAPP في OmniPeek 5.0

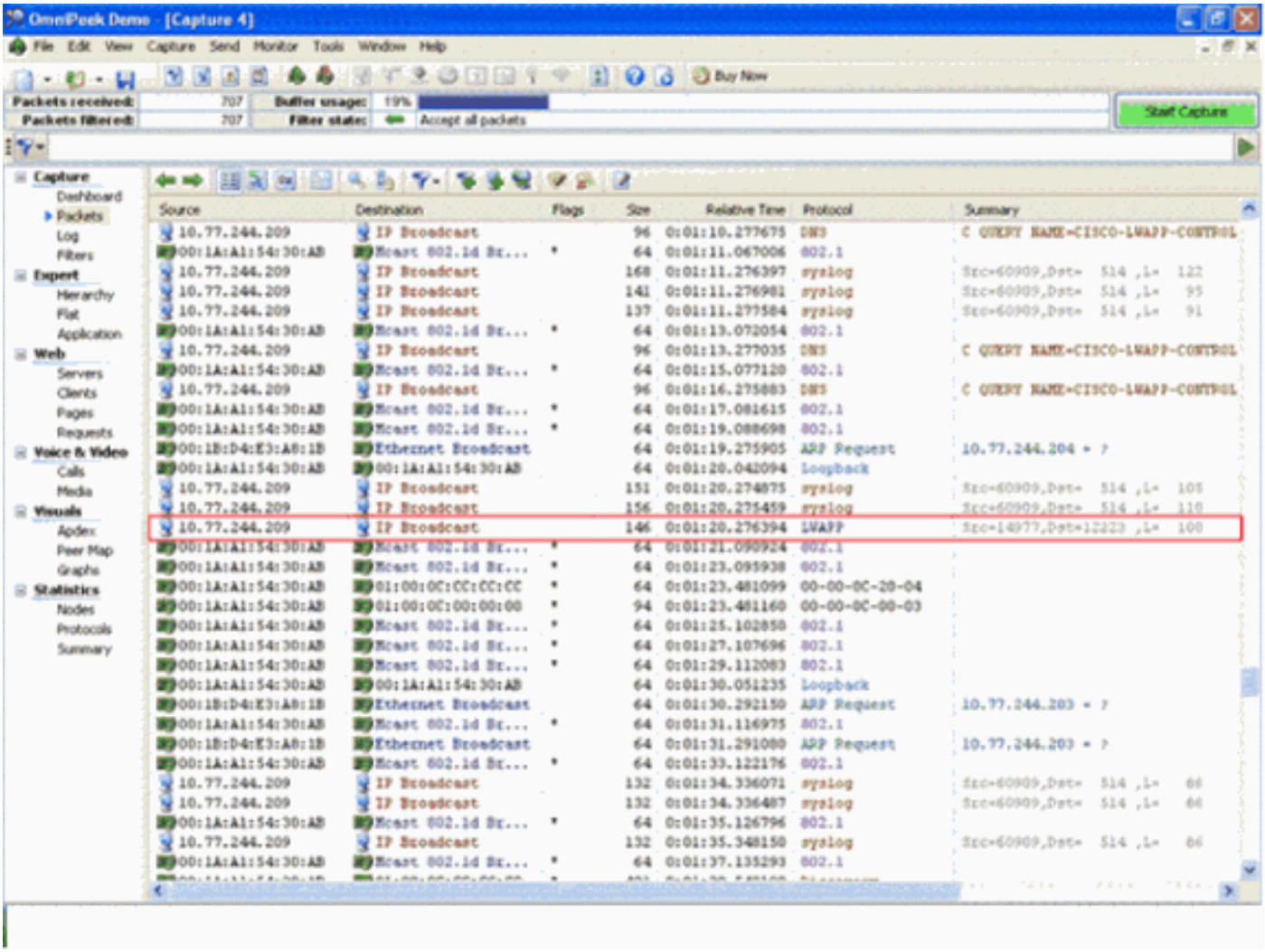
OmniPeek الإصدار 5. 0 هو أداة الالتقاط من الجيل التالي ل OmniPeek الإصدار 3. 0. في الإصدار 5.0، يتم إنشاء وحدات فك تشفير LWAPP بشكل افتراضي. وبالتالي، لا حاجة إلى أي تغييرات أخرى في الملف. ومع ذلك، هنا مثال يوضح كيفية تحديد عامل تصفية بروتوكول في الإصدار 5.0 باستخدام عنوان IP ورقم المنفذ:

1. افتح تطبيق OmniPeek 5. 0.
2. من صفحة البداية، انقر فوق **ملف > جديد** لفتح نافذة جديدة لالتقاط الحزم.تظهر نافذة صغيرة اسمها خيارات الالتقاط. وهو يحتوي على قائمة من الخيارات لالتقاط الحزمة.
3. من خيار **المحول**، أختر محول لالتقاط الحزم باستخدام ذلك المحول. يرد أدناه وصف بشأن المحول وأنت تبرز المحول. أختر **توصيل المنطقة المحلية** لالتقاط الحزم باستخدام مهايئ الإيثرنت المحلي.
4. وانقر فوق **OK**.تظهر نافذة Capture (التقاط) جديد.
5. انقر على زر **بدء الالتقاط**.تبدأ الأداة في التقاط الحزم للبروتوكولات المحددة في البرنامج. لعرض الحزم الملتقطة، انقر فوق خيار **الحزم** أسفل قائمة **الالتقاط** على اليسار.
6. انقر بزر الماوس الأيمن فوق أي من الحزم الملتقطة وانقر فوق **إنشاء مرشح** لتحديد بروتوكول جديد.تظهر نافذة إدراج مرشح.
7. أدخل اسما داخل مربع **عامل التصفية** لتعريف البروتوكول.قم بتمكين عامل تصفية **العنوان**.أخترت النوع **ك IP** أن على قبض ربط إلى ومن عنوان خاص.**دخلت** لا**لعنوان**1 المصدر عنوان.**للعنوان 2** أدخل عنوان IP إذا كانت الوجهة بها IP ثابت.أخترت الخيار كأي **عنوان** إن الغاية يستلم عنوان من خلال DHCP.لتعيين إتجاه تدفق الحزمة انقر على زر **كلا الاتجاهين** واختر أي من الخيارات الثلاثة. تشير علامة السهم الموجودة على الزر إلى الإتجاه الذي تم إختياره.قم بتمكين عامل تصفية **المنفذ**.أخترت النوع للميناء يستعمل بالبروتوكول، مثلا TCP.بالنسبة **للمنفذ 1** أدخل منفذا مستخدما في المصدر.بالنسبة للمنفذ **2** أدخل رقم منفذ إذا كانت الوجهة تستخدم منفذ معياري محدد جيدا.وإلا، أخترت **ال any ميناء** خيار إن الغاية يستعمل ميناء على أساس عشوائي.أختر *إتجاها* من الزر **كلا الاتجاهين** استنادا إلى متطلباتك.
8. كرر هذه الخطوات لتعريف أي بروتوكول مخصص جديد.

التحقق من الصحة

باستخدام OmniPeek 5.0، يمكنك التحقق من خلال شاشة الالتقاط من أن الأداة تلتقط بروتوكول LWAPP بشكل افتراضي عند تشغيل حدث LWAPP. الشكل 1 يوضح التقاط بروتوكول LWAPP أثناء طلب الاكتشاف الذي تم إجراؤه بواسطة نقطة الوصول في الوضع Lightweight (LAP).

شكل 1



انقر نقرا مزدوجا على الحزمة لعرض التفاصيل حول الحزمة.

معلومات ذات صلة

- الأسئلة المتداولة حول EtherPeek
- التعريف بالعمر
- تنزيل OmniPeek 5.0
- 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).