# جمارب ىلع LWAPP Decodes جمارب ىلع WildPacket OmniPeek و EtherPeek 3.0

#### المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>تعديل ملف فك ترميز LWAPP لي</u> <u>تعديل ملف الPSPES.xm</u> فك تشفير LWAPP في OmniPeek 5.0 <u>معلومات ذات صلة</u>

#### <u>المقدمة</u>

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.

#### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

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

#### <u>المكونات المستخدمة</u>

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

OmniPeek 3.0 •

- EtherPeek 3.0 •
- OmniPeek 5.0 •

#### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

## <u>تعدیل ملف فك ترمیز LWAPP</u>

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 light\_weight\_...ملف protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

## <u>تعديل TCP\_UDP\_Ports.dcd</u>

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

UX2fbe | LWAPP; vx2fbf | 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 الأصلى 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>
```

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

## <u>فك تشفير LWAPP في OmniPeek 5.0</u>

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 لالعنوان1 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 العزمة انقر على زر كلا الاتجاهين واختر أي من الخيارات الثلاثة. تشير علامة السهم الموجودة على الزر إلى الحزمة انقر على زر كلا الاتجاهين واختر أي من الخيارات الثلاثة. تشير علامة السهم الموجودة على الزر إلى الإتجاه الذي تم إختيار 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.
  - 8. كرر هذه الخطوات لتعريف أي بروتوكول مخصص جديد.

#### <u>التحقق من الصحة</u>

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

شكل 1

2 OmniPeek Dem	o - [Capture 4]	and the second second							CF	X	
B File Edit View	Capiture Send Monitor Tool	s Window Help .			1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	and the second second	and the second	1.12		7 ×	
Q - 0 - U		STRODES	1918	0	a Duy Now						
Packets received	received: 207 Buffer snaget 19% monocomment										
Packets filtered:	207 Filter st	tates 🗰 Accept all packets						264	AL CHOUSE		
19-											
E Capture	4 - 12 - 12 - 12		9.9	2	a se se superior de la co				1 - 1		
Deshboard	for any	Provide states	-	1.1.1.000	Relative Reve	Reistand	C. Standard C. S. S.			-	
Packets	Source	Cesonacion	riage	3424	Reading Tane	PTOROCOR	Summary			100	
Log	3 10.77.244.209	g IF Broadcast		96	0:01:10.277675	DWS	C OUERT RAME-CI	SCO-LWAPS	-CONTRO		
Filters	#POD:1A:A1:54:30:AB	Moast 802.1d BE	•	64	0:01:11.067006	002.1	L				
Expert	10.77.244.209	IF Broadcast		168	0:01:11.276397	sAurod	SEC+60909,D#C+	514 ,1+	122		
Herarchy	10.77.244.209	IF BEOBSCASE		141	0:01:11.276981	sAsrod	SEC+60909,DSt+	514 ,14	22		
Flat	3 10.77.244.209	g IF Broadcast		137	0:01:11.277584	sAsrod	200+60909,090×	214 124	71		
Application	00:1A1A1:54:30:AB	monse boz.1d BE	•	64	0:01:13.072054	002.1	i.			. ŝ.	
Web	3 10.77.244.209	IF Ecoadcast		96	0:01:13.277035	083	C QUEPT NAME+CI	300-14871	-CONTRO	÷.	
Servers	LO 22 DAT DOD	BCG2C 002.1d DE		0.4	0:01:15.077120	002+1	A comparison management	when a second			
Clients	3 10.77.244.209	g IF Broadcast		26	0:01:16.275003	000	C QUERT NAME+CI	SCO-LWAP	CONTRO	÷.	
Pages	PODIIATALIS41301AB	Whichse 002.1d BE		64	0101117.001615	902-1					
Requests	00:1A:A1:54:30:AB	Aphcese 002.10 82		64	0:01:19.088698	002.1	Longer and see the				
R Voice & Video	200118:D4:E3:A6:18	Ethernet Broadcast		64	0:01:19.275905	WAS bedrese	10.77.244.204 +	7			
Calls	10 77 244 200	ALLO ALALIS 41 JULAS			0101:20.042094	rooppack	·	114 14	1.04		
Media	10 77 244 009	IF BEOBSCARC		1.51	0101120-274975	sAarod	200-000000.0000	224 124	200		
Visuals	¥ 10.77.244.209	IF BIDedcest		1.20	0101120.275459	systog	3EC+60909,090+	319 164	100	÷.	
Apdex	3 10-11-044-003	Tr scooscast		140	0101120-275394	LANT .	200-14011164041	6663 JAN	744	Ц.	
Peer Map	BOOLING ALLOWING	Breat for id br	- C		0101121-099924	99613					
Graphs	MPOULALALIS41301AB	MC455 002.10 02		0.4	0101123.093938	00.00.00.00.00					
Statistics	0011A1A11541301AD	01100100100100100		04	0101123,401099	00-00-00-00-00					
Nodes	20011A1A11541501AD	Breast 202 1d Br			0101123-401109	00-00-00-00					
Protocols	10011A1A1154L301A5	Brook overse street	- C		0108165-102050	996-8					
Summary	20011A1A11541301A5	Margar 602 14 Re			0101127-107099	80.2.3					
	200-11-11-54-30-18	BOOM 12 - 21 - 50 - 10	-		0101107-110003	ave-a Loughaste					
	BAD: 18-D.4-F3-18-18	BU THE ALL ON OVER			0-01-30 303160	ADD Deminent	100 22 244 202				
	3500110-04104100110	Water and id be	· .		0:01:31.116975	APR PEQUERS	and the second s	· ·			
	\$200-18-D4-F3-18-18	Stebarner Broadcast	+		0-01-31 201080	100 Permet	10.00.044.000 -				
	MAD:11-11-54-30-18	Press Shi ld Br			6-01-33 122126	AV2 1		r			
	10.77.244.209	12 Broadcast		1.72	0:01:34,336021	evalor	frontibility para	514 . 1-			
	10, 77, 244, 209	TP Broadcast		132	0:01:34.336407	malog	Strieffishth Date	514 1-	6.6		
	100:14:41:54:30:48	Reast 802.14 By		64	0-01-35,126294	802.1	and a second second second	124 124			
	10.77.244.209	TP Broadcast		132	0:01:35.348150	avalor	Stree60909.Dete	514 . 1-	66		
	100:14:41:54:30-48	Brant 802, 1d Br		64	0:01:37,135293	802.1	and a second second	124 124			
	BB.0.0. 1 5 - 1 1 - F 4 - 0.0. 1 B	MAL	· •	40.1	ALALLAR PARLAR	***				~	
	C. C									×1	

انقر نقرا مزدوجا على الحزمة لعرض التفاصيل حول الحزمة.

## <u>معلومات ذات صلة</u>

- <u>الأسئلة المتداولة حول EtherPeek</u>
  - <u>التعريف بالعمر</u>
  - <u>تنزيل OmniPeek 5.0</u>
- <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما