LWAPP decodifica la habilitación en el software OmniPeek y EtherPeek 3.0 de WildPackets

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Modificar el archivo de descodificación LWAPP Modificar TCP_UDP_Ports.dcd Modificar el archivo Pspecs.xml Decodificación del LWAPP en OmniPeek 5.0 Verificación Información Relacionada

Introducción

WildPackets OmniPeek (y EtherPeek) tienen decodificadores de protocolo de punto de acceso ligero (LWAPP) disponibles, pero no están conectados. Este documento explica cómo habilitar los decodificadores del LWAPP y utilizar el software para ver el LWAPP. Este documento utiliza el procedimiento para EtherPeek 3.0 y OmniPeek 5.0.

Nota: El procedimiento para OmniPeek 3.0 es el mismo que el de EtherPeek 3.0.

Nota: La única diferencia entre los softwares OmniPeek y EtherPeek es la ubicación de los archivos.

- La ruta para OmniPeek es C:/Program Files/WildPackets/OmniPeek.
- La ruta para EtherPeek es C:/Archivos de programa/WildPackets/EtherPeek.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de los softwares EtherPeek y OmniPeek 3.0 y 5.0. Para obtener información sobre EtherPeek, refiérase a <u>Preguntas Frecuentes sobre EtherPeek</u>. Para obtener información sobre OmniPeek, consulte <u>Introducción de Omni</u>.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Modificar el archivo de descodificación LWAPP

Para modificar el archivo de decodificación LWAPP, añada "ETHR 0 90 c2 AP Identity:;;" a la función LWAPP. Esto se encuentra directamente debajo de la línea "LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" en el LWAPP-light_weight_...protocol.dcd file (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modificar TCP_UDP_Ports.dcd

En el archivo TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), debe incluir estas dos líneas:

0x2fbe | LWAPP; 0x2fbf | LWAPP;

Nota: Como resultado de este proceso, no se abre ningún puerto en el equipo host. Por lo tanto, este paso no expone al equipo host a ningún riesgo de seguridad.

De esta manera, se incluyen los dos puertos 12222 y 1223.

Modificar el archivo Pspecs.xml

Complete estos pasos:

 En la sección Protocolo de datagramas de usuario (UDP) del archivo pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), agregue estas líneas:Nota: Asegúrese primero de realizar una copia de seguridad del archivo original.

```
<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 Control</LName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
</PSpec>
</PSpec>
```

2. Reinicie OmniPeek o EtherPeek para que sus cambios surtan efecto.

Decodificación del LWAPP en OmniPeek 5.0

OmniPeek versión 5.0 es la herramienta de captura de última generación para OmniPeek versión 3.0. En la versión 5.0, los decodificadores LWAPP se incorporan de forma predeterminada. Por lo tanto, no es necesario realizar ningún cambio adicional en el archivo. Sin embargo, aquí hay un ejemplo que muestra cómo definir un filtro de protocolo en la versión 5.0 usando una dirección IP y el número de puerto:

- 1. Abra la aplicación OmniPeek 5.0.
- En la página Inicio, haga clic en Archivo > Nuevo para abrir una nueva ventana de captura de paquetes.Aparece una pequeña ventana denominada Opciones de captura. Contiene la lista de opciones para una captura de paquetes.
- 3. En la opción **Adapter**, elija un adaptador para capturar paquetes con ese adaptador. A continuación se muestra la descripción del adaptador cuando lo resalta. Elija **Local Area Connection** para capturar paquetes usando el adaptador Ethernet local.
- 4. Click OK.Aparece la ventana Nueva captura.
- 5. Haga clic en el botón **Iniciar captura**.La herramienta comienza a capturar paquetes para los protocolos definidos en el software. Para ver los paquetes capturados, haga clic en la opción **Paquetes** debajo del **menú Capturar** a la izquierda.
- 6. Haga clic con el botón derecho en cualquiera de los paquetes capturados y haga clic en **Make Filter** para definir un nuevo protocolo.Aparecerá la ventana Insertar filtro.
- 7. Ingrese un nombre dentro del cuadro Filtro para identificar el protocolo.Habilite el filtro Dirección.Elija el tipo como IP para capturar paquetes hacia y desde direcciones IP específicas.Para la Dirección 1, ingrese la dirección IP de origen.Para la Dirección 2, introduzca una dirección IP si el destino tiene una IP estática.Elija la opción como Cualquier dirección si el destino recibe una dirección IP a través de DHCP.Para especificar la dirección del flujo de paquetes, haga clic en el botón Both direction y elija una de las tres opciones. La marca de flecha del botón indica la dirección elegida.Habilite el filtro de puerto.Elija el tipo para el puerto utilizado por el protocolo, por ejemplo TCP.Para el Puerto 1, ingrese un puerto usado en el origen.Para el Puerto 2 ingrese un número de puerto si el destino utiliza un puerto estándar bien definido.De lo contrario, elija la opción Any port si el destino utiliza un puerto aleatoriamente.Elija una *dirección* del botón Ambas direcciones según sus requerimientos.
- 8. Repita estos pasos para definir cualquier nuevo protocolo personalizado.

Verificación

Con OmniPeek 5.0, puede verificar desde la pantalla de captura que la herramienta captura el protocolo LWAPP de forma predeterminada cuando se activa un evento LWAPP. <u>La Figura 1</u> muestra la captura del protocolo LWAPP durante la Solicitud de Detección realizada por el LAP.

OmniPeek Dem	o - [Capture 4]				antes at managed					
Prin Edit View	Capture Send Monitor Tool	s Wedow Help		1	1.00				- 0	
🗋 - 😫 - 🖬		BIJ SODDI	2.3	0	Duy Now				Same	
Packets received	707 Buffer usage: 19%							Start Caphare		
Packets fatered	207 Filler of	reset - woods in backets								
- Fashing		10. 3. 1 m 1 m 10 m		-						
Dashboard										
Packets	Source	Destination	Flags	Size	Relative Time	Protocol	Summary			
Log	3 10.77.244.209	IP Buoadcast		96	0:01:10.277675	DWS	C OTERY RATE-CI	SCO-LWAPP	-CONTROL	
Fitters	POD:1A:A1:54:30:AB	MCast 802.1d Br	•	64	0:01:11.067006	002.1	1			
Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	syslog	SEC=60909,D#C=	514 ,1+	122	
Herarchy	10.77.244.209	IF Broadcast		141	0:01:11.276981	sAsrod	Sic+60909,D#t+	514 ,1+	- 22	
Flat	3 10.77.244.209	IF Broadcast		137	0:01:11.277584	sistod	\$£0+60909,D9t+	214 .14	91	
Application	00:1A:A1:54:30:AB	My Reast 802.1d Dr	•	64	0:01:13.072054	002.1	i i			
Web	10.77.244.209	IP Ecoadcast	-	96	0:01:13.277035	08/3	C QUERT NAME+CI	3CO-LWAP7	-CONTROL	
Servers	B900:1A:A1:54:30:AB	Boast 802.1d Br	•	64	0:01:15.077120	-802.1				
Clerks	3 10.77.244.209	IF Broadcast		96	0:01:16.275883	DBI3	C QUERT NAME+CI	SCO-LWAPP	-CONTROL	
Pages	#900:1A:A1:54:30:AB	MyRcast 002.14 Br		64	0:01:17.081615	002.1				
Requests	B900:1A:A1:54:30:AB	My Mcast 802.1d Sr	•	64	0:01:19.088698	802.1				
🖻 Voice & Video	BP00:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:19.275905	ARP Request	10.77.244.204 +	7		
Calls	2900:1A:A1:54:30:AB	20011A1A11541301A5		-64	0:01:20.042094	Loopback				
Media	10.77.244.209	IP Broadcast		151	0:01:20.274975	syslog	SEC+60909,D95+	514 ,14	105	
R Visuals	10.77.244.209	IP Broadcast		156	0:01:20.275459	syslog	SEC+60909,Det+	514 .14	110	
Apdex	3 10.77.244.209	3 IS Broadcast		146	0:01:20.276394	14499	SEC+14977,D9t+1	2223 yike	100	
Peer Map	2900:1A1A1:54:30:AB	MRCASE 802.18 Br		64	0:01:21.090924	02.1				
Graphs	#00:1A:A1:54:30:AB	My Mcast 602.1d Br	•	64	0:01:23.095938	002.1				
Statistics	B900:1A:A1:54:30:AB	B01:00:0C:CC:CC:CC	•	64	0:01:23.481099	00-00-00-20-04				
Nodes	#900:1A:A1:54:30:A8	B 01:00:0C:00:00:00		-94	0:01:23.461160	00-00-00-00-03				
Protocols	2900:1A:A1:54:30:A5	Moast 002.14 St	.*	64	0:01:25.102850	002-1				
Summary	#900:1A:A1:54:30:AB	BRANK BO2.1d BE	•	64	0:01:27.107696	802.1				
	B00:1A:A1:54:30:AB	Monst 802.1d Sr	•	64	0:01:29.112083	802-1				
	200:1A:A1:54:30:AB	10011A1A11541301A8		64	0:01:30.051235	Loopback				
	POD:18:D4:E3:A8:18	BEthernet Broadcast		- 64	0:01:30.292150	APP Request	10.77.244.203 -	7		
	#90011A1A11541301AB	Micast 002.1d Sc		64	0:01:31.116975	802.1				
	#900:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:31.291080	APP Request	10,77,244,203 -	2		
	200:1A:A1:54:30:AB	BRCAST 802.14 St		64	0:01:33.122176	802.1				
	10.77.244.209	IF Broadcast		132	0:01:34.336071	syslog	frc-60909,Det-	514 ,1-	66	
	10.77.244.209	TP Broadcast		132	0:01:34.336487	syslog	Szc=60909,Dyt=	\$14 .1-	66	
	#900:1A:A1:54:30:AB	MCast 002.1d Br		64	0:01:35.126796	802.1				
	10.77.244.209	IP Scoadcast		132	0:01:35.348150	syslog	Szc-60909,Dst-	514 .1-	66	
	#900:1A:A1:54:30:A5	BCast 802.1d Br		64	0:01:37.135293	602.1				
	BRAD. 11.11.1.1.1.0.0.00.00			49.5		A.1				
									>	

Haga doble clic en el paquete para ver los detalles del paquete.

Información Relacionada

- Preguntas frecuentes sobre EtherPeek
- Presentación de Omni
- Descargar OmniPeek 5.0
- Soporte Técnico y Documentación Cisco Systems