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

Contenido

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 Preguntas Frecuentes sobre EtherPeek . Para obtener información sobre OmniPeek, consulte Introducción de Omni .

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 Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

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:

1. 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-C</SName>
 <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

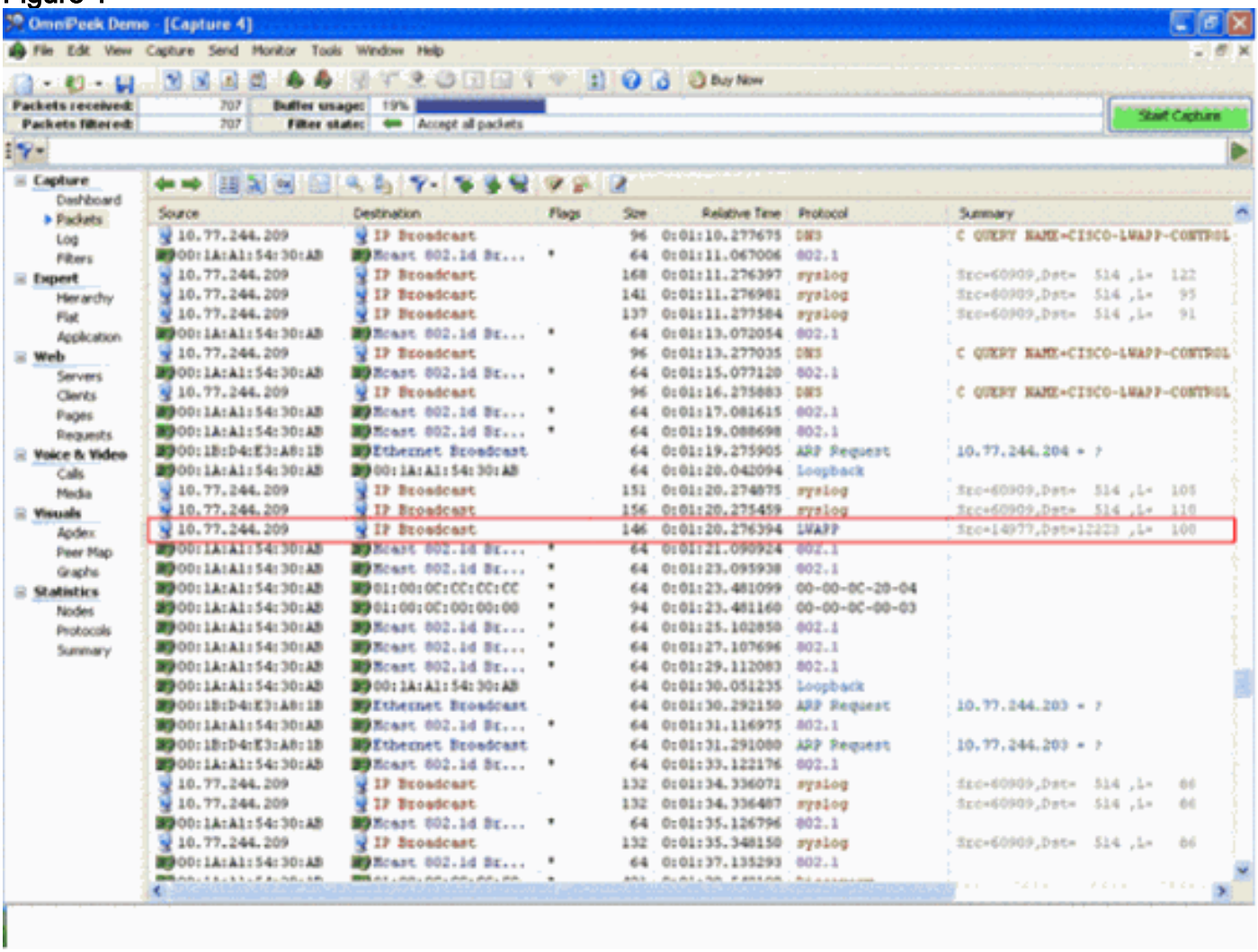
OmniPeek versión 5.0 es la herramienta de captura de última generación para OmniPeek versión 3.0. En la versión 5.0, los decodificadores LWAPP se incorporan de forma predeterminada. Por lo tanto, no es necesario realizar ningún cambio adicional en el archivo. Sin embargo, aquí hay un ejemplo que muestra 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.
2. 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. La Figura 1 muestra la captura del protocolo LWAPP durante la Solicitud de Detección realizada por el LAP.

Figure 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