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

Contenido

Introducción

El OmniPeek de WildPackets (y el EtherPeek) tienen protocolo del Lightweight Access Point (LWAPP) decodifica disponible, solamente ellos no se enchufan. Este documento explica cómo habilitar el LWAPP decodifica y utiliza el software para mirar el LWAPP. Este documento utiliza el procedimiento para el 3.0 y el OmniPeek 5.0 del EtherPeek.

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

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

- La trayectoria para el OmniPeek es C: Archivos/WildPackets/OmniPeek /Program.
- La trayectoria para el EtherPeek es C: Archivos/WildPackets/EtherPeek /Program.

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del EtherPeek, y 3.0 del OmniPeek y 5.0 softwares. Para la información sobre el EtherPeek, refiera al EtherPeek FAQ . Para la información sobre el OmniPeek, refiera a introducir el Omni .

Componentes Utilizados

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

- 3.0 del OmniPeek
- 3.0 del EtherPeek
- OmniPeek 5.0

Convenciones

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

Modifique el LWAPP decodifican el archivo

Para modificar el LWAPP decodifique el archivo, agregan “ETHR 0 0 identidades de 90 c2 AP: ; ” a la función del LWAPP. Esto está directamente bajo los “LABL 0 0 0 protocolos \ el LWAPP del Lightweight Access Point b1: ; ” línea en el archivo de LWAPP-light_weight_… protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modifique TCP_UDP_Ports.dcd

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

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

Nota: No se abre ningunos puertos en la computadora host como resultado de este proceso. Por lo tanto, este paso no expone la computadora host a ninguna riesgos de seguridad.

De esta manera, los dos puertos 12222 y 12223 son incluidos.

Modifique el archivo Pspecs.xml

Complete estos pasos:

1. En la sección del User Datagram Protocol (UDP) del archivo pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), agregue estas líneas:**Nota:** Aseegurese sostener el archivo original primero.
```
<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. Recomience el OmniPeek o el EtherPeek para que sus cambios tomen el efecto.

El LWAPP decodifica en el OmniPeek 5.0

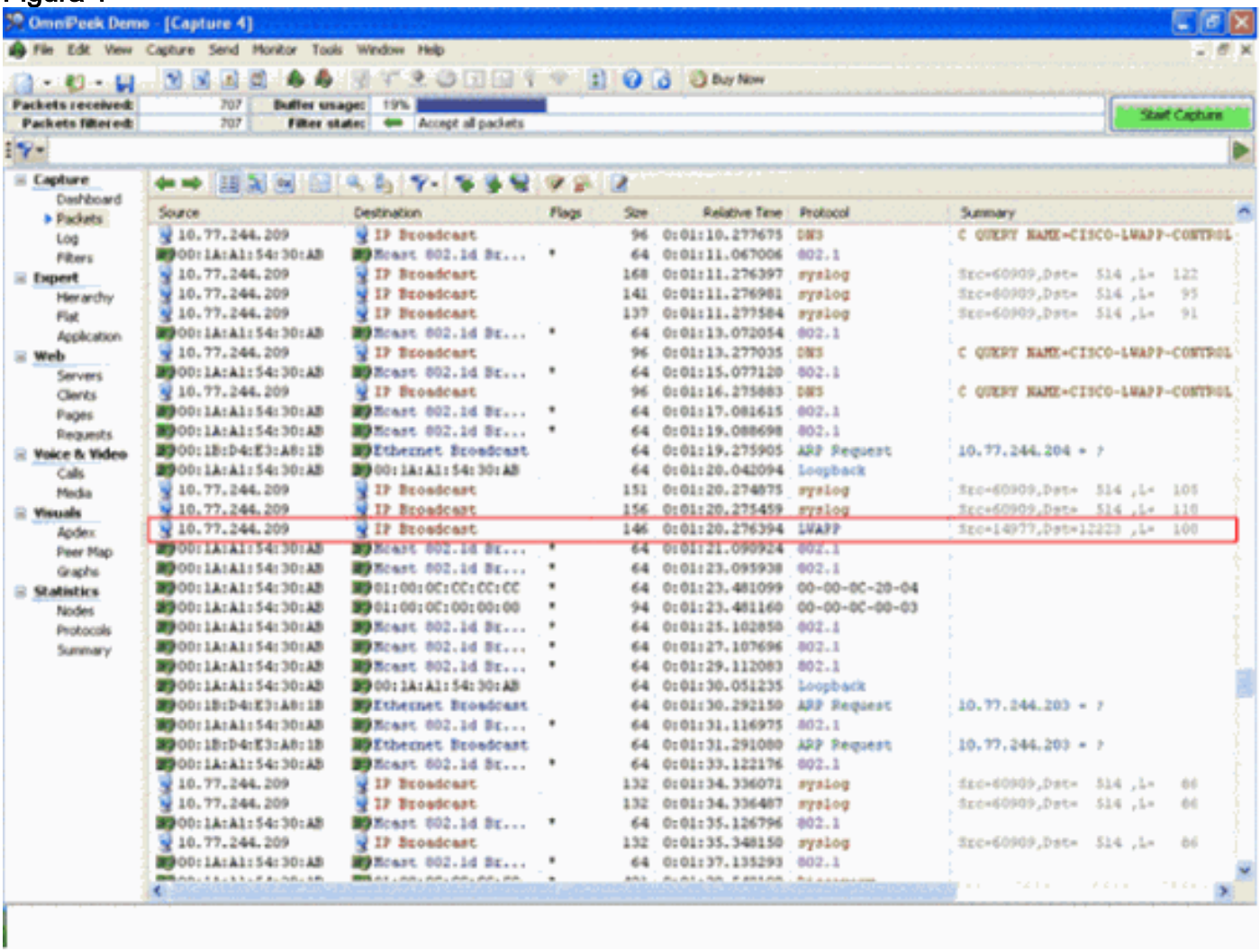
La versión 5.0 del OmniPeek es la herramienta de la captura de la última generación para la versión 3.0 del OmniPeek. En la versión 5.0, el LWAPP decodifica es incorporado por abandono. Así, no hay necesidad de un cambios cualquier más otra en el archivo. Sin embargo, aquí está un ejemplo que muestra cómo definir un filtro del protocolo en la versión 5.0 usando una dirección IP y el número del puerto:

1. Abra la aplicación del OmniPeek 5.0.
2. Desde el principio página, clic en Archivo **> nuevo** para abrir una nueva ventana de la captura de paquetes.Una pequeña ventana nombrada las opciones de la captura aparece. Contiene la lista de opciones para una captura de paquetes.
3. De la opción del **adaptador**, elija un adaptador para capturar los paquetes usando ese adaptador. La descripción sobre el adaptador se muestra abajo mientras que usted resalta el adaptador. Elija la **conexión de área local** para capturar los paquetes usando el adaptador de los Ethernetes locales.
4. Haga clic en OK.La nueva ventana de la captura aparece.
5. Haga clic el botón de la **captura del comienzo**.La herramienta comienza a capturar los paquetes para los protocolos definidos en el software. Para ver los paquetes capturó, hace clic la opción de los **paquetes** debajo del menú de la **captura** a la izquierda.
6. Los paquetes uces de los del click derecho capturaron y el tecleo **hace el filtro** para definir un nuevo protocolo.La ventana del filtro del separador de millares aparece.
7. Ingrese un nombre dentro del rectángulo del **filtro** para identificar el protocolo.Habilite el **filtro de direcciones**.Elija el tipo como **IP** para capturar los paquetes a y desde los IP Addresses específicos.Para el **address1** ingrese la dirección IP de origen.Para el **direccionamiento 2** ingrese un IP Address si el destino tiene a IP estático.Elija la opción como **cualquier direccionamiento** si el destino recibe una dirección IP con el DHCP.Para especificar la dirección del flujo de paquetes haga clic a las **ambas direcciones** abotonan y eligen cualquiera de las tres opciones. La marca de la flecha en el botón indica la dirección elegida.Habilite el **filtro del puerto**.Elija el tipo para el puerto usado por el protocolo, por ejemplo TCP.Para el **puerto 1** ingrese un puerto usado en la fuente.Para el **puerto 2** ingrese un número del puerto si el destino utiliza un puerto bien definido estándar.Si no, elija la **cualquier** opción del **puerto** si el destino utiliza un puerto sobre una base al azar.Elija una *dirección de las* **ambas direcciones** abotonan basado en su requisito.
8. Relance estos pasos para definir cualquier nuevo protocolo personalizado.

Verificación

Con el OmniPeek 5.0, usted puede verificar de la pantalla de la captura que la herramienta capture el protocolo del LWAPP por abandono cuando se acciona un lwapp event. El cuadro 1 muestra la captura del protocolo del LWAPP durante la petición de la detección hecha por el REVESTIMIENTO.

Figura 1



El doble hace clic en el paquete para ver los detalles sobre el paquete.

Información Relacionada

- EtherPeek FAQ
- Introducción del Omni
- OmniPeek 5.0 de la descarga
- Soporte Técnico y Documentación - Cisco Systems