O LWAPP decodifica a ativação em software WildPackets OmniPeek e EtherPeek 3.0

Contents

Introduction

O WildPackets OmniPeek (e EtherPeek) tem decodificações Lightweight Access Point Protocol (LWAPP) disponíveis, mas não estão conectados. Este documento explica como habilitar os decodificadores do LWAPP e usar o software para examinar o LWAPP. Este documento usa o procedimento para EtherPeek 3.0 e OmniPeek 5.0.

Observação: o procedimento para o OmniPeek 3.0 é o mesmo do EtherPeek 3.0.

Observação: a única diferença entre os softwares OmniPeek e EtherPeek é a localização dos arquivos.

- O caminho para o OmniPeek é C:/Program Files/WildPackets/OmniPeek.
- O caminho para o EtherPeek é C:/Program Files/WildPackets/EtherPeek.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos softwares EtherPeek e OmniPeek 3.0 e 5.0. Para obter informações sobre o EtherPeek, consulte as Perguntas Frequentes do EtherPeek . Para obter informações sobre o OmniPeek, consulte Introdução ao Omni .

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Modificar o arquivo de decodificação LWAPP

Para modificar o arquivo de decodificação LWAPP, adicione "ETHR 0 90 c2 AP Identity:;" à função LWAPP. Isso está diretamente abaixo da linha "LABL 0 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" no LWAPP-light_weight_...arquivo protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modificar TCP_UDP_Ports.dcd

No arquivo TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), você deve incluir estas duas linhas:

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

Observação: nenhuma porta é aberta no computador como resultado desse processo. Portanto, esta etapa não expõe o computador host a riscos de segurança.

Dessa forma, as duas portas 12222 e 12223 estão incluídas.

Modificar o arquivo Pspecs.xml

Conclua estes passos:

1. Na seção User Datagram Protocol (UDP) do arquivo pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), adicione estas linhas:**Nota:** Certifique-se de fazer o backup do arquivo original primeiro.

```
<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 o OmniPeek ou o EtherPeek para que as alterações entrem em vigor.

Decodificação LWAPP no OmniPeek 5.0

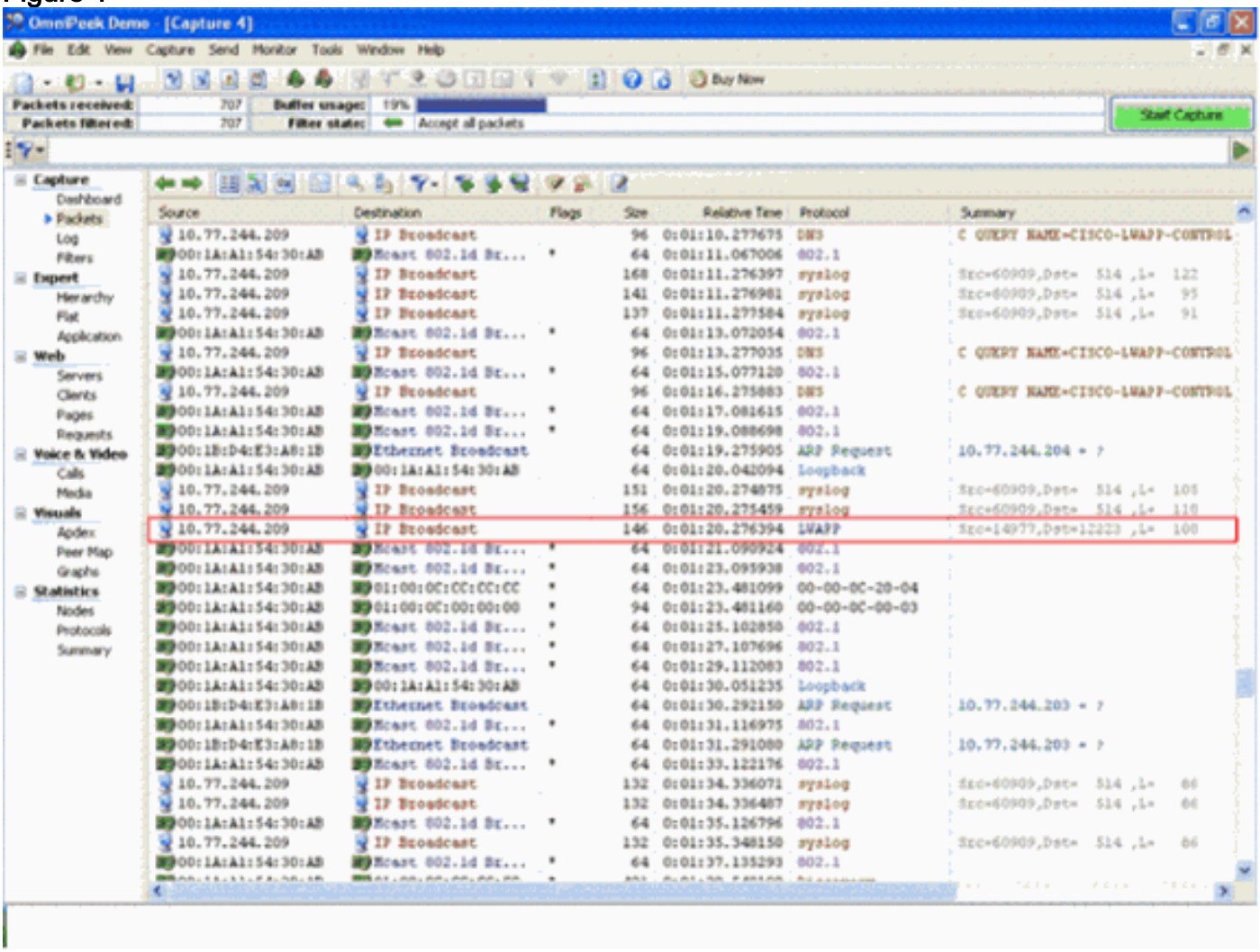
O OmniPeek versão 5.0 é a ferramenta de captura de próxima geração para o OmniPeek versão 3.0. Na versão 5.0, os decodificadores LWAPP são incorporados por padrão. Assim, não há necessidade de mais alterações no arquivo. No entanto, aqui está um exemplo que mostra como definir um filtro de Protocolo na versão 5.0 usando um endereço IP e o número da porta:

1. Abra o aplicativo OmniPeek 5.0.
2. Na página Iniciar, clique em **Arquivo > Novo** para abrir uma nova janela de captura de pacote.Uma pequena janela chamada Opções de captura é exibida. Contém a lista de opções para uma captura de pacote.
3. Na opção **Adaptador**, escolha um adaptador para Capturar pacotes usando esse adaptador. A descrição sobre o adaptador é mostrada abaixo quando você realça o adaptador. Escolha **Conexão de Área Local** para capturar pacotes usando o adaptador ethernet local.
4. Click **OK**.A janela Nova captura é exibida.
5. Clique no botão **Start Capture (Iniciar captura)**.A ferramenta começa a capturar pacotes para os protocolos definidos no software. Para visualizar os pacotes capturados, clique na opção **Pacotes** abaixo do menu **Captura** à esquerda.
6. Clique com o botão direito do mouse em qualquer pacote capturado e clique em **Make Filter (Criar filtro)** para definir um novo protocolo.A janela Inserir filtro é exibida.
7. Digite um nome dentro da caixa **Filtro** para identificar o protocolo.Ative o filtro **de endereço**.Escolha o Tipo como **IP** para capturar pacotes de e para endereços IP específicos.Para o **Endereço1**, insira o endereço IP de origem.Para o **Endereço 2**, insira um endereço IP se o destino tiver um IP estático.Escolha a Opção como **Qualquer Endereço** se o destino receber um endereço IP por meio do DHCP.Para especificar a direção do fluxo do pacote, clique no botão **Ambas as direções** e escolha uma das três opções. A marca de seta no botão indica a direção escolhida.Ative o filtro **de porta**.Escolha o Tipo para a porta usada pelo protocolo, por exemplo, TCP.Para a **porta 1**, insira uma porta usada na origem.Para a **porta 2**, insira um número de porta se o destino usar uma porta padrão bem definida.Caso contrário, escolha a opção **Qualquer porta** se o destino usar uma porta aleatoriamente.Escolha uma *direção* no botão **Ambas as direções** com base no seu requisito.
8. Repita essas etapas para definir qualquer novo protocolo personalizado.

Verificar

Com o OmniPeek 5.0, você pode verificar na tela Capture que a ferramenta captura o protocolo LWAPP por padrão quando um evento LWAPP é acionado. A Figura 1 mostra a captura do protocolo LWAPP durante a solicitação de descoberta feita pelo LAP.

Figure 1



Clique duas vezes no pacote para ver os detalhes sobre o pacote.

Informações Relacionadas

- Perguntas frequentes do EtherPeek
- Introdução ao Omni
- Download do OmniPeek 5.0
- Suporte Técnico e Documentação - Cisco Systems