O LWAPP descodifica a habilitação software no 3.0 do OmniPeek e do EtherPeek de WildPackets

Índice

Introdução

O OmniPeek de WildPackets (e o EtherPeek) têm o protocolo de pouco peso do Access point (LWAPP) descodificam disponível, mas não são obstruídos dentro. Este documento explica como permitir o LWAPP descodifica e usa o software para olhar o LWAPP. Este documento usa o procedimento para o 3.0 do EtherPeek e o OmniPeek 5.0.

Nota: O procedimento para o 3.0 do OmniPeek é o mesmo que aquele do 3.0 do EtherPeek.

Nota: A única diferença entre software do OmniPeek e do EtherPeek é o lugar dos arquivos.

- O trajeto para o OmniPeek é C: Arquivos /Program/WildPackets/OmniPeek.
- O trajeto para o EtherPeek é C: Arquivos /Program/WildPackets/EtherPeek.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do EtherPeek, e 3.0 do OmniPeek e 5.0 software. Para obter informações sobre do EtherPeek, refira o EtherPeek FAQ . Para obter informações sobre do OmniPeek, refira a introdução de Omni .

Componentes Utilizados

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

- 3.0 do OmniPeek
- 3.0 do EtherPeek
- OmniPeek 5.0

Convenções

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

Altere o LWAPP descodificam o arquivo

A fim alterar o LWAPP descodifique o arquivo, adicionam “ETHR 0 0 identidades de 90 c2 AP: ; ” à função LWAPP. Este é diretamente sob o “LABL 0 0 0 protocolos de pouco peso do Access point b1 \ LWAPP: ; ” linha no arquivo de LWAPP-light_weight_… protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Altere 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;
```

Nota: Nenhuma porta é aberta no computador host em consequência deste processo. Consequentemente, esta etapa não expõe o computador host a nenhuns riscos de segurança.

Desta maneira, as duas portas 12222 e 12223 são incluídas.

Altere o arquivo Pspecs.xml

Conclua estes passos:

1. Na seção do User Datagram Protocol (UDP) do arquivo pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), adicionar estas linhas:**Nota:** Certifique-se suportar primeiramente o arquivo 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 o OmniPeek ou o EtherPeek para que suas mudanças tomem o efeito.

O LWAPP descodifica no OmniPeek 5.0

A versão 5.0 do OmniPeek é a ferramenta da captação da próxima geração para a versão 3.0 do OmniPeek. Na versão 5.0, o LWAPP descodifica é inerente à revelia. Assim, não há nenhuma necessidade para umas mudanças mais adicionais no arquivo. Contudo, está aqui um exemplo que mostre como definir um filtro de protocolo na versão 5.0 usando um endereço IP de Um ou Mais Servidores Cisco ICM NT e o número de porta:

1. Abra o aplicativo do OmniPeek 5.0.
2. Desde o início página, **arquivo do** clique **> novo** a fim abrir um indicador novo da captura de pacote de informação.Um indicador pequeno nomeado opções da captação aparece. Contém a lista de opções para uma captura de pacote de informação.
3. Da opção do **adaptador**, escolha um adaptador capturar pacotes usando esse adaptador. A descrição sobre o adaptador é mostrada abaixo enquanto você destaca o adaptador. Escolha a **conexão de área local** capturar pacotes usando o adaptador dos Ethernet locais.
4. Clique em **OK**.O indicador novo da captação aparece.
5. Clique o botão da **captação do começo**.A ferramenta começa capturar pacotes para os protocolos definidos no software. A fim ver os pacotes capturou, clica a opção dos **pacotes** abaixo do menu da **captação** à esquerda.
6. Clicar com o botão direito alguns dos pacotes capturados e o clique **faz o filtro** a fim definir um protocolo novo.O indicador do filtro da inserção aparece.
7. Dê entrada com um nome dentro da caixa do **filtro** para identificar o protocolo.Permita o **filtro de endereço**.Escolha o tipo como o **IP** capturar pacotes a e dos endereços IP de Um ou Mais Servidores Cisco ICM NT específicos.Para o **endereço1** incorpore o endereço IP de origem.Para o **endereço 2** incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT se o destino tem um IP Estático.Escolha a opção como **todo o endereço** se o destino recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT com o DHCP.A fim especificar o sentido do fluxo de pacote de informação clique os **ambos sentidos** abotoam e escolhem qualquer uma das três opções. A seta Mark no botão indica o sentido escolhido.Permita o **filtro de porta**.Escolha o tipo para a porta usada pelo protocolo, por exemplo TCP.Para a **porta 1** entre em uma porta usada na fonte.Para a **porta 2** entre em um número de porta se o destino usa uma porta bem definida padrão.Se não, escolha **toda a** opção da **porta** se o destino usa uma porta em uma base aleatória.Escolha um *sentido dos* **ambos sentidos** abotoam-se baseado em sua exigência.
8. Repita estas etapas para definir todo o protocolo personalizado novo.

Verificar

Com OmniPeek 5.0, você pode verificar da tela da captação que a ferramenta captura o protocolo LWAPP à revelia quando um evento LWAPP é provocado. Figura 1 mostra a captação do protocolo LWAPP durante o pedido da descoberta feito pelo REGAÇO.

Figura 1

Fazer duplo clique no pacote para ver os detalhes sobre o pacote.

Informações Relacionadas

- EtherPeek FAQ
- Introduzindo Omni
- OmniPeek 5.0 da transferência
- Suporte Técnico e Documentação - Cisco Systems