Activation du décodage LWAPP sur les logiciels WildPackets OmniPeek et EtherPeek 3.0

Contenu

Introduction

WildPackets OmniPeek (et EtherPeek) ont le point d'accès léger Protocol (LWAPP) décode disponible, mais eux ne sont pas branchés. Ce document explique comment activer le LWAPP décode et emploie le logiciel pour regarder LWAPP. Ce document utilise la procédure pour EtherPeek 3.0 et OmniPeek 5.0.

Remarque: La procédure pour OmniPeek 3.0 est identique que celle d'EtherPeek 3.0.

Remarque: La seule différence entre les logiciels d'OmniPeek et d'EtherPeek est l'emplacement des fichiers.

- Le chemin pour OmniPeek est C : Fichiers /Program/WildPackets/OmniPeek.
- Le chemin pour EtherPeek est C : Fichiers /Program/WildPackets/EtherPeek.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de l'EtherPeek, et logiciel d'OmniPeek 3.0 et 5.0. Pour les informations sur EtherPeek, référez-vous à la Foire aux questions d'EtherPeek . Pour les informations sur OmniPeek, référez-vous à introduire Omni .

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Modifiez le LWAPP décodent le fichier

Afin de modifier le LWAPP décodez le fichier, ajoutent « ETHR 0 0 identités de 90 C2 AP : ; » à la fonction LWAPP. C'est directement sous le « LABL 0 0 0 points d'accès léger b1 Protocol \ LWAPP : ; » ligne dans le fichier de LWAPP-light_weight_… protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modifiez TCP_UDP_Ports.dcd

Dans le fichier TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), vous devez inclure ces deux lignes :

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

Remarque: Aucun port n'est ouvert sur l'ordinateur hôte en raison de ce processus. Par conséquent, cette étape n'expose l'ordinateur hôte à aucun risque de sécurité.

De cette façon, les deux ports 12222 et 12223 sont inclus.

Modifiez le fichier Pspecs.xml

Procédez comme suit :

1. Dans la section de Protocole UDP (User Datagram Protocol) du fichier pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), ajoutez ces lignes :**Remarque:** Veillez à sauvegarder le fichier d'origine d'abord.
```
<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. Redémarrez OmniPeek ou EtherPeek pour que vos modifications les prennent effet.

LWAPP décodent dans OmniPeek 5.0

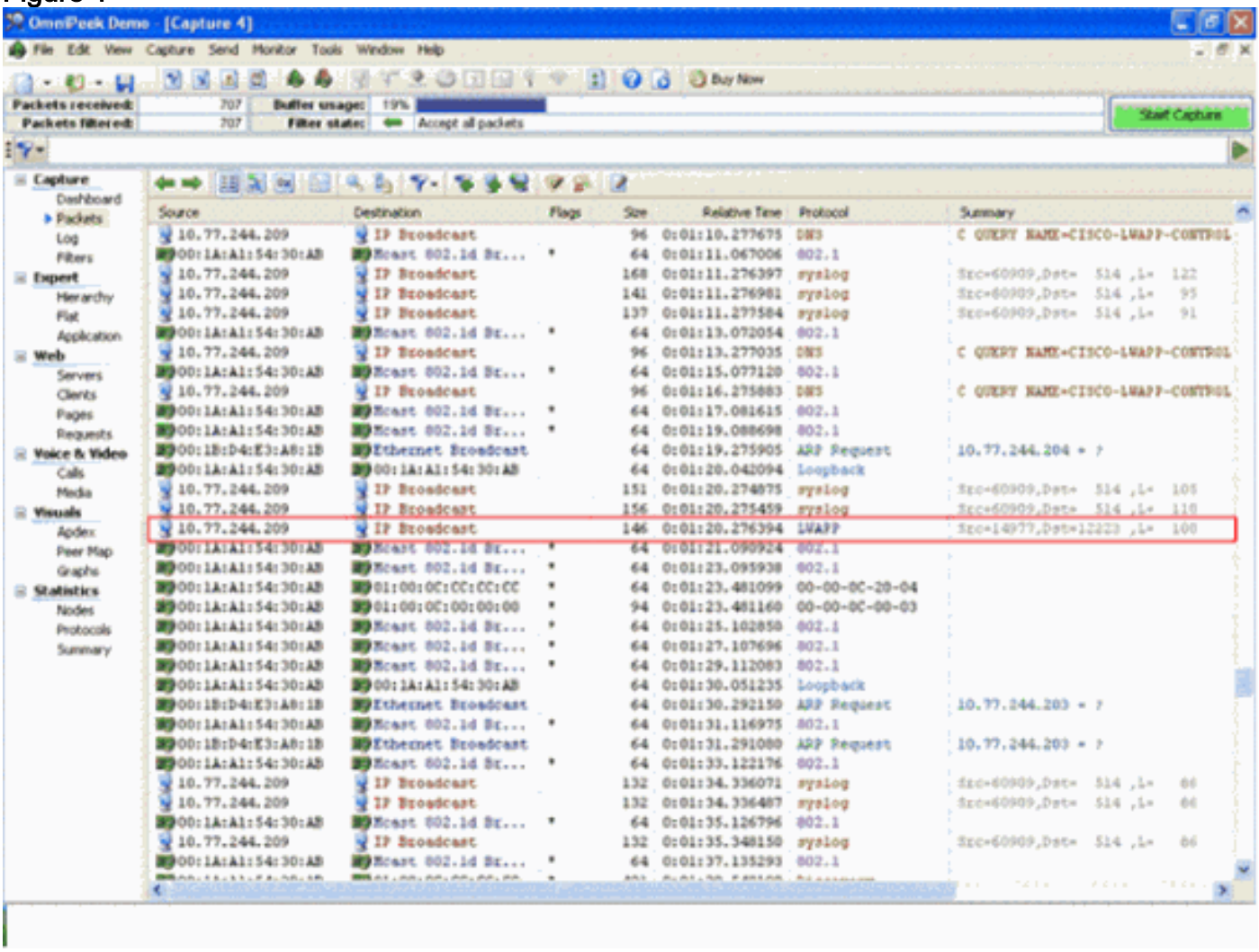
La version 5.0 d'OmniPeek est l'outil de saisie de nouvelle génération pour la version 3.0 d'OmniPeek. Dans la version 5.0, LWAPP décode est incorporé par défaut. Ainsi, il n'y a aucun besoin d'autres de changements du fichier. Cependant, voici un exemple qui affiche comment définir un filtre de Protocol dans la version 5.0 utilisant une adresse IP et le numéro de port :

1. Ouvrez l'application d'OmniPeek 5.0.
2. Dès le début page, **fichier de** clic **> nouveau** afin d'ouvrir une nouvelle fenêtre de capture de paquet.Une petite fenêtre nommée des options de capture apparaît. Il contient la liste d'options pour une capture de paquet.
3. De l'option d'**adaptateur**, choisissez un adaptateur pour capturer des paquets utilisant cet adaptateur. La description au sujet de l'adaptateur est affichée ci-dessous pendant que vous mettez en valeur l'adaptateur. Choisissez la **connexion au réseau local** pour capturer des paquets utilisant l'adaptateur local d'Ethernets.
4. Cliquez sur **OK**.La nouvelle fenêtre de capture apparaît.
5. Cliquez sur le bouton de **capture de début**.Les débuts d'outil pour capturer des paquets pour les protocoles définis en logiciel. Afin de visualiser les paquets capturés, cliquez sur l'option de **paquets** au-dessous du menu de **capture** du côté gauche.
6. Les paquets l'uns des de clic droit les ont capturé et le clic **font le filtre** afin de définir un nouveau protocole.La fenêtre de filtre d'insertion apparaît.
7. Écrivez un nom à l'intérieur de la case de **filtre** pour identifier le protocole.Activez le filtre d'**adresse**.Choisissez le type comme **IP** pour capturer des paquets à et des adresses IP spécifiques.Pour **adresse1 l'**entrer l'adresse IP source.Pour l'**Address2** écrivez une adresse IP si la destination a un IP statique.Choisissez l'option en tant que **n'importe quelle adresse** si la destination reçoit une adresse IP par le DHCP.Afin de spécifier la direction de l'écoulement de paquet cliquez sur les **les deux directions** boutonnent et choisissent l'un ou l'autre des trois options. La marque de flèche sur le bouton indique la direction choisie.Activez le filtre de **port**.Choisissez le type pour le port utilisé par le protocole, par exemple TCP.Pour le **port 1** entrez dans un port utilisé dans la source.Pour le **port 2** introduisez un numéro de port si la destination utilise un port bien défini standard.Autrement, choisissez la **n'importe quelle** option de **port** si la destination utilise un port sur une base aléatoire.Choisissez une *direction les* **des deux directions** se boutonnent basé sur votre condition requise.
8. Répétez ces étapes pour définir n'importe quel nouveau protocole fait sur commande.

Vérifiez

Avec OmniPeek 5.0, vous pouvez vérifier de l'écran de capture que l'outil capture le protocole LWAPP par défaut quand un événement LWAPP est déclenché. La figure 1 affiche la saisie de protocole LWAPP pendant la demande de détection faite par le RECOUVREMENT.

Figure 1



Double-cliquer sur le paquet pour visualiser les détails au sujet du paquet.

Informations connexes

- Foire aux questions d'EtherPeek
- Introduire Omni
- Téléchargement OmniPeek 5.0
- Support et documentation techniques - Cisco Systems