LWAPP decodifica l'abilitazione sui software WildPackets OmniPeek e EtherPeek 3.0

Sommario

Introduzione

Per i pacchetti WildPackets OmniPeek (ed EtherPeek) sono disponibili decodici Lightweight Access Point Protocol (LWAPP), ma non sono collegati. Questo documento spiega come abilitare la decodifica LWAPP e usare il software per esaminare LWAPP. Nel documento viene usata la procedura per EtherPeek 3.0 e OmniPeek 5.0.

Nota: la procedura per OmniPeek 3.0 è la stessa di EtherPeek 3.0.

Nota: l'unica differenza tra i software OmniPeek e EtherPeek è la posizione dei file.

- Il percorso di OmniPeek è C:/Program Files/WildPackets/OmniPeek.
- Il percorso di EtherPeek è C:/Programmi/WildPackets/EtherPeek.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei software EtherPeek e OmniPeek 3.0 e 5.0. Per informazioni su EtherPeek, fare riferimento alle domande frequenti su EtherPeek . Per informazioni su OmniPeek, fare riferimento a Introduzione a Omni .

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Modificare il file di decodifica LWAPP

Per modificare il file di decodifica LWAPP, aggiungere "ETHR 0 0 90 c2 AP Identity:;" alla funzione LWAPP. Si trova direttamente sotto la riga "LABEL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" in LWAPP-light_weight_...file protocol.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes).

Modificare il file TCP_UDP_Ports.dcd

Nel file TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), è necessario includere le due righe seguenti:

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

Nota: questa operazione non comporta l'apertura di porte nel computer host. Pertanto, questo passaggio non espone il computer host ad alcun rischio per la sicurezza.

In questo modo, vengono incluse le due porte 1222 e 1223.

Modificare il file Pspecs.xml

Attenersi alla seguente procedura:

1. Nella sezione UDP (User Datagram Protocol) del file pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), aggiungere le righe seguenti:**Nota:** assicurarsi di eseguire prima il backup del file originale.

```
<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. Riavviare OmniPeek o EtherPeek per rendere effettive le modifiche.

Decodifica LWAPP in OmniPeek 5.0

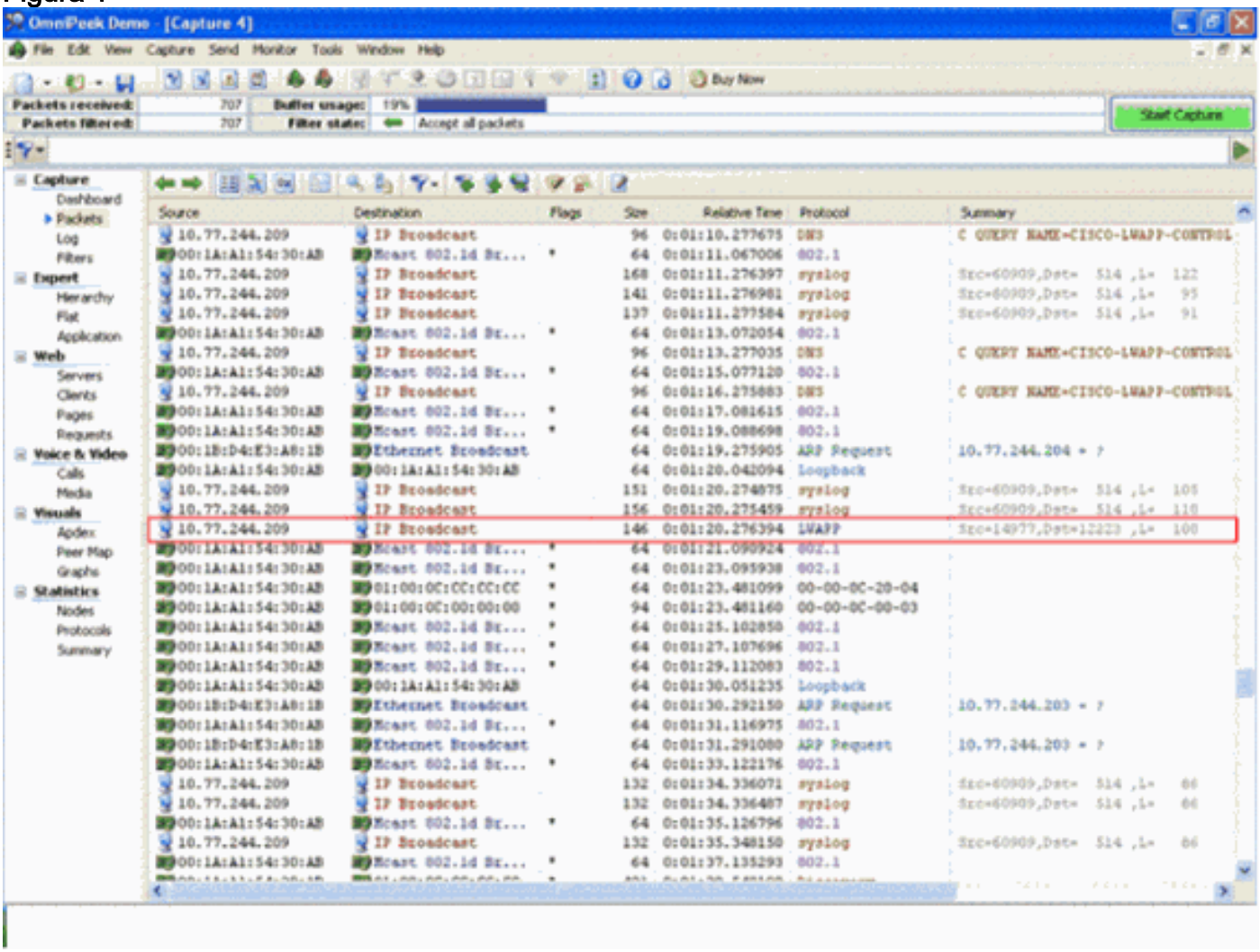
OmniPeek versione 5.0 è lo strumento di acquisizione di nuova generazione per OmniPeek versione 3.0. Nella versione 5.0, le decodificazioni LWAPP sono incorporate per impostazione predefinita. Non sono pertanto necessarie ulteriori modifiche al file. Tuttavia, l'esempio seguente mostra come definire un filtro di protocollo nella versione 5.0 utilizzando un indirizzo IP e il numero di porta:

1. Aprire l'applicazione OmniPeek 5.0.
2. Dalla pagina iniziale, fare clic su **File > Nuovo** per aprire una nuova finestra di acquisizione pacchetti.Viene visualizzata una piccola finestra denominata Opzioni di cattura. Contiene l'elenco di opzioni per l'acquisizione di un pacchetto.
3. Dall'opzione **Scheda**, scegliere una scheda per acquisire i pacchetti utilizzando quella scheda. La descrizione della scheda di rete viene mostrata di seguito quando si evidenzia la scheda di rete. Scegliere **Connessione LAN** per acquisire i pacchetti utilizzando la scheda Ethernet locale.
4. Fare clic su **OK**.Viene visualizzata la finestra Nuova cattura.
5. Fare clic sul pulsante **Avvia cattura**.Lo strumento avvia l'acquisizione dei pacchetti per i protocolli definiti nel software. Per visualizzare i pacchetti catturati, fare clic sull'opzione **Packets** sotto il menu **Capture** a sinistra.
6. Per definire un nuovo protocollo, fare clic con il pulsante destro del mouse su uno dei pacchetti acquisiti e scegliere **Crea filtro**.Viene visualizzata la finestra Inserisci filtro.
7. Immettere un nome nella casella **Filtro** per identificare il protocollo.Abilitare il filtro **Indirizzo**.Scegliere il Tipo come **IP** per acquisire i pacchetti da e verso indirizzi IP specifici.Per **Address1**, immettere l'indirizzo IP di origine.In **Indirizzo 2**, immettere un indirizzo IP se la destinazione ha un indirizzo IP statico.Selezionare l'opzione **Any Address** (Qualsiasi indirizzo) se la destinazione riceve un indirizzo IP tramite DHCP.Per specificare la direzione del flusso del pacchetto, fare clic sul pulsante **Entrambe le direzioni** e scegliere una delle tre opzioni. Il simbolo a forma di freccia sul pulsante indica la direzione scelta.Abilitare il filtro **Porta**.Selezionare il Tipo per la porta utilizzata dal protocollo, ad esempio TCP.Per la **Porta 1**, immettere una porta utilizzata nell'origine.Per **Porta 2** immettere un numero di porta se la destinazione utilizza una porta standard ben definita.In caso contrario, selezionare l'opzione **Any port** se la destinazione utilizza una porta in modo casuale.Scegliere una *direzione* dal pulsante **Entrambe le direzioni** in base alle proprie esigenze.
8. Ripetere questi passaggi per definire un nuovo protocollo personalizzato.

Verifica

Con OmniPeek 5.0, è possibile verificare dalla schermata Capture che lo strumento acquisisca il protocollo LWAPP per impostazione predefinita quando viene attivato un evento LWAPP. La figura 1 mostra l'acquisizione del protocollo LWAPP durante la richiesta di rilevamento effettuata dal LAP.

Figura 1



Fare doppio clic sul pacchetto per visualizzare i dettagli del pacchetto.

Informazioni correlate

- Domande frequenti su EtherPeek
- Presentazione di Omni
- Scarica OmniPeek 5.0
- Documentazione e supporto tecnico – Cisco Systems