LWAPP расшифровывает включение на программном обеспечении WildPackets OmniPeek и EtherPeek 3.0

Содержание

Введение

WildPackets OmniPeek (и EtherPeek) имеет Протокол LWAPP, декодирует доступный, но они не включены. Этот документ объясняет, как включить LWAPP, декодирует, и используйте программное обеспечение для рассмотрения LWAPP. Этот документ использует процедуру для EtherPeek 3.0 и OmniPeek 5.0.

Примечание: Процедура для OmniPeek 3.0 совпадает с процедурой EtherPeek 3.0.

Примечание: Единственной разницей между программными обеспечениями OmniPeek и EtherPeek является местоположение файлов.

- Путь для OmniPeek является C:/Program Files/WildPackets/OmniPeek.
- Путь для EtherPeek является C:/Program Files/WildPackets/EtherPeek.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с EtherPeek, и OmniPeek 3.0 и 5.0 программными обеспечениями. Для получения информации о EtherPeek обратитесь к часто задаваемым вопросам EtherPeek. Для получения информации о OmniPeek обратитесь к Представлению Omni.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Модифицируйте LWAPP, декодируют файл

Для изменения LWAPP, декодируют файл, добавляют "ETHR 0 0 90 идентичности c2 AP:"; к функции LWAPP. Это непосредственно находится под "точкой доступа LABL 0 0 0 b1 Легкого веса Protocol\LWAPP:"; линия в LWAPP-light_weight_... protocol.dcd файл (C:\Program Files\WildPackets\EtherPeek\Decodes).

Модифицируйте TCP_UDP_Ports. dCD –

В файле TCP_UDP_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes), необходимо включать эти две линии:

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

Примечание: Никакие порты не открыты на главном компьютере в результате этого процесса. Поэтому этот шаг не представляет главный компьютер никаким угрозам безопасности.

Таким образом эти два порта 12222 и 12223 включены.

Модифицируйте файл Pspecs.xml

Выполните следующие действия:

1. В разделе Протокола UDP файла pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033), добавьте эти линии:**Примечание:** Удостоверьтесь, что выполнили резервное копирование исходный файл сначала.
```
<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. OmniPeek перезапуска или EtherPeek для ваших изменений для вступления в силу.

LWAPP декодирует в OmniPeek 5.0

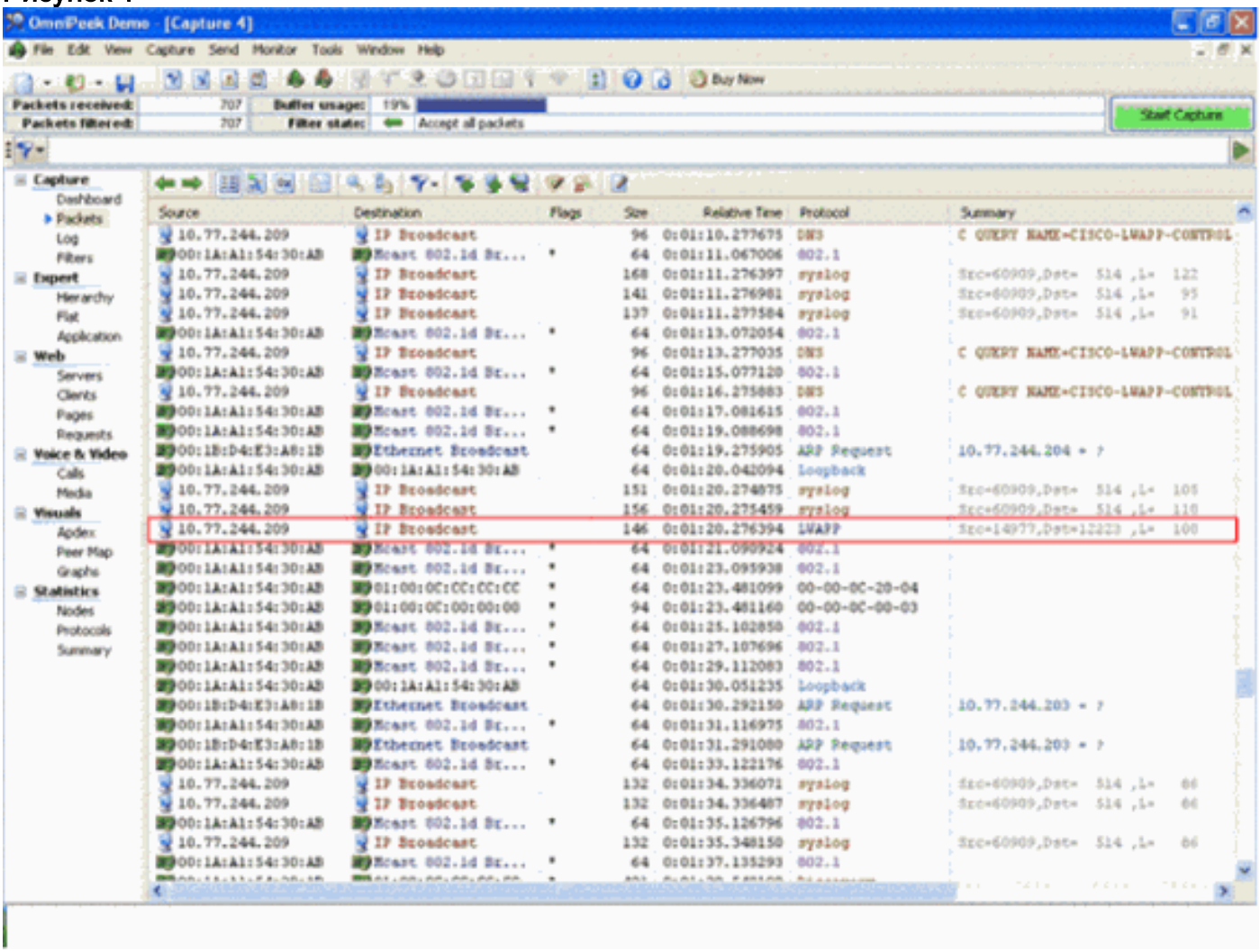
Версия 5.0 OmniPeek является программным средством перехвата следующего поколения для версии 3.0 OmniPeek. В 5.0 версиях декодирования LWAPP встроены по умолчанию. Таким образом нет никакой потребности в дальнейших изменениях в файле. Однако вот пример, который показывает, как определить Фильтр протокола в 5.0 версиях с помощью IP-адреса и Номера порта:

1. Откройте приложение OmniPeek 5.0.
2. От Начальной страницы нажмите **File> New** для открытия Нового Окна Захвата пакета.Появляется маленькое окно под названием Опции Перехвата. Это содержит список опций для захвата пакета.
3. От **опции Adapter** выберите адаптер для Получения Пакетов с помощью того адаптера. Описание об адаптере показывают ниже, поскольку вы выделяете адаптер. Выберите **Local Area Connection** для получения пакетов с помощью адаптера локального Ethernet.
4. **Нажмите кнопку OK.**Окно New Capture появляется.
5. Нажмите кнопку **Start Capture**.Программное средство начинает перехватывать пакеты для протоколов, определенных в программном обеспечении. Для просмотра перехваченных пакетов нажмите опцию **Packets** ниже меню **Capture** слева.
6. Щелкните правой кнопкой по любому из перехваченных пакетов и нажмите **Make Filter** в заказе определить новый протокол.Окно Insert Filter появляется.
7. Введите имя в **Блоке фильтров** для определения протокола.Включите **Фильтр адреса**.Выберите Type в качестве **IP** для получения пакетов к и от определенных IP-адресов.Поскольку **Address1** вводит IP - адрес источника.Если у назначения есть статическое ip, для **Адреса 2** вводят IP-адрес.Выберите Option в качестве **Любого Адреса**, если назначение получает IP-адрес через DHCP.Чтобы указать, что направление потока пакетов нажимает кнопку **Обоих направлений** и выбирает любую из этих трех опций. Стрелка Марк на кнопке указывает на выбранное направление.Включите **Фильтр портов**.Выберите Type для порта, используемого протоколом, например TCP.Для **порта 1** вводят порт, используемый в источник.Если назначение использует стандартный четко определенный порт, для **порта 2** вводят номер порта.В противном случае выберите **Любую** опцию **порта**, если назначение использует порт на случайной основе.Выберите *направление* из кнопки **Both Directions** на основе вашего требования.
8. Повторите эти шаги для определения любого нового настраиваемого протокола.

Проверка

С OmniPeek 5.0 можно проверить с Экрана Перехвата, что программное средство перехватывает протокол LWAPP по умолчанию, когда инициировано Событие lwapp. Рисунок 1 показывает перехват протокола LWAPP во время Запроса на обнаружение, сделанного LAP.

Рисунок 1



Двойной щелчок на пакете, чтобы посмотреть детали о пакете.

Дополнительные сведения

- Часто задаваемые вопросы EtherPeek
- Представление Omni
- OmniPeek 5.0 загрузки
- Cisco Systems – техническая поддержка и документация