LWAPP는 WildPackets OmniPeek 및 EtherPeek 3.0 소프트웨어에서 지원 기능을 디코딩합니다.

목차

소개

WildPackets OmniPeek(및 EtherPeek)은 LWAPP(Lightweight Access Point Protocol) 디코딩을 사용할 수 있지만 연결되지 않습니다. 이 문서에서는 LWAPP 디코딩을 활성화하고 소프트웨어를 사용하여 LWAPP를 보는 방법에 대해 설명합니다. 이 문서에서는 EtherPeek 3.0 및 OmniPeek 5.0에 대한 절차를 사용합니다.

참고: OmniPeek 3.0의 절차는 EtherPeek 3.0의 절차와 동일합니다.

참고: OmniPeek와 EtherPeek 소프트웨어의 유일한 차이점은 파일의 위치입니다.

- OmniPeek의 경로는 C:/Program Files/WildPackets/OmniPeek입니다.
- EtherPeek의 경로는 C:/Program Files/WildPackets/EtherPeek입니다.

사전 요구 사항

요구 사항

EtherPeek, OmniPeek 3.0 및 5.0 소프트웨어에 대해 알고 있는 것이 좋습니다. EtherPeek에 대한 자세한 내용은 EtherPeek FAQ를 참조하십시오 . OmniPeek에 대한 자세한 내용은 Introducing Omni 를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

LWAPP 디코드 파일 수정

LWAPP 디코딩 파일을 수정하려면 LWAPP 함수에 "ETR 0 0 90 c2 AP Identity:;"을 추가합니다. 이것은 LWAPP-light_weight_의 "LAPL 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" 줄 바로 아래에 있습니다.protocol.dcd 파일(C:\Program Files\WildPackets\EtherPeek\Decodes).

TCP_UDP_Ports.dcd 수정

TCP_UDP_Ports.dcd(C:\Program Files\WildPackets\EtherPeek\Decodes) 파일에서 다음 두 행을 포함해야 합니다.

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

참고: 이 프로세스의 결과로 호스트 컴퓨터에 포트가 열려 있지 않습니다. 따라서 이 단계에서는 호스트 컴퓨터가 보안 위험에 노출되지 않습니다.

이러한 방식으로 12222와 12223 2개의 포트가 포함됩니다.

Pspecs.xml 파일 수정

다음 단계를 완료하십시오.

1. pspecs.xml(C:\Program Files\WildPackets\EtherPeek\1033) 파일의 UDP(User Datagram Protocol) 섹션에서 다음 행을 추가합니다.**참고:** 먼저 원본 파일을 백업해야 합니다.

```
<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. 변경 사항을 적용하려면 OmniPeek 또는 EtherPeek를 다시 시작하십시오.

OmniPeek 5.0의 LWAPP 디코딩

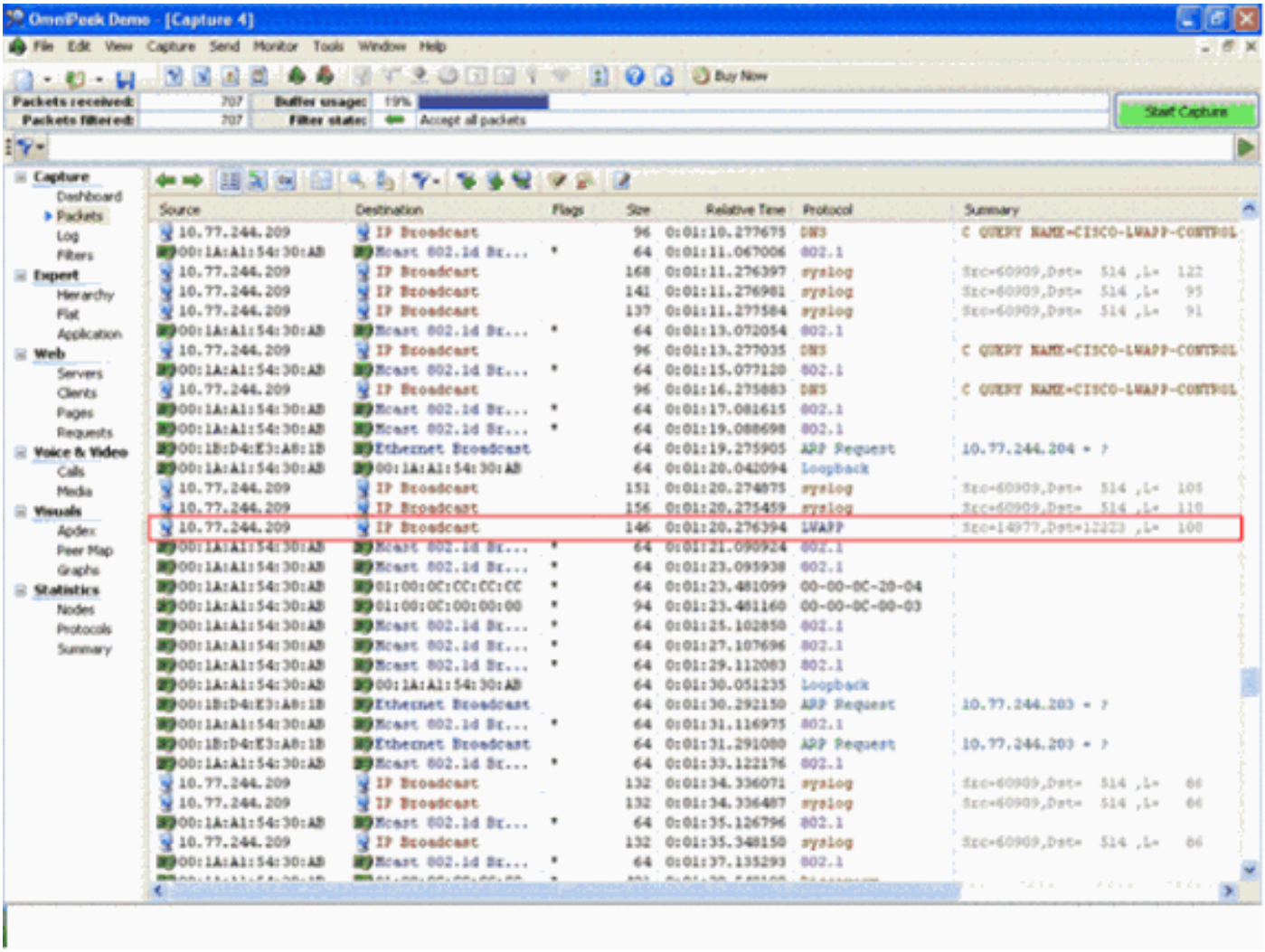
OmniPeek 버전 5.0은 OmniPeek 버전 3.0의 차세대 캡처 툴입니다. 5.0 버전에서는 기본적으로 LWAPP 디코딩이 내장되어 있습니다. 따라서 파일에서 더 이상 변경할 필요가 없습니다. 그러나 IP 주소 및 포트 번호를 사용하여 5.0 버전에서 프로토콜 필터를 정의하는 방법을 보여 주는 예는 다음과 같습니다.

1. OmniPeek 5.0 응용 프로그램을 엽니다.
2. Start(시작) 페이지에서 **File(파일) > New(새로 만들기)**를 클릭하여 New Packet Capture Window(새 패킷 캡처 창)를 엽니다.Capture Options라는 작은 창이 나타납니다. 여기에는 패킷 캡처에 대한 옵션 목록이 포함됩니다.
3. Adapter 옵션에서 해당 어댑터를 사용하여 Capture Packets를 캡처할 어댑터를 선택합니다. 어댑터에 대한 설명은 어댑터를 강조 표시할 때 아래에 표시됩니다. 로컬 이더넷 어댑터를 사용하여 패킷을 캡처하려면 Local Area Connection을 선택합니다.
4. **확인을 클릭합니다**.New Capture(새 캡처) 창이 나타납니다.
5. Start Capture(캡처 **시작)** 버튼**을** 클릭합니다.툴은 소프트웨어에 정의된 프로토콜에 대한 패킷을 캡처하기 시작합니다. 캡처된 패킷을 보려면 왼쪽의 **Capture** 메뉴 아래**에 있는 Packets** 옵션을 클릭합니다.
6. 캡처된 패킷 중 하나를 마우스 오른쪽 버튼으로 클릭하고 **Make Filter**를 클릭하여 새 프로토콜을 정의합니다.Insert Filter 창이 나타납니다.
7. 프로토콜을 식별하려면 **Filter** 상자 안에 이름을 입력합니다.**주소** 필터를 활성화합니다.Type as **IP**를 선택하여 특정 IP 주소 간에 패킷을 캡처합니다.**Address1**에 소스 IP 주소를 입력합니다.**주소 2**의 경우 대상에 고정 IP가 있는 경우 IP 주소를 입력합니다.목적지가 DHCP를 통해 IP 주소를 수신하는 경우 Option as **Any Address**를 선택합니다.패킷 흐름의 방향을 지정하려면 **Both directions** 버튼을 클릭하고 세 가지 옵션 중 하나를 선택합니다. 단추의 화살표 표시는 선택한 방향을 나타냅니다.포트 필터를 활성화합니다.프로토콜에서 사용하는 포트의 Type(유형)을 선택합니다(예: TCP).포트 **1**에 소스에 사용된 포트를 입력합니다.목적지에서 잘 정의된 표준 포트를 사용하는 경우 **Port 2**에 포트 번호를 입력합니다.그렇지 않으면 목적지가 임의의 기준으로 포트를 사용하는 경우 Any **port** 옵션을 선택합니다.요구 사항에 따라 **Both Directions** 버튼에서 *방향*을 선택합니다.
8. 새 사용자 지정 프로토콜을 정의하려면 이 단계를 반복합니다.

다음을 확인합니다.

OmniPeek 5.0을 사용하면 LWAPP 이벤트가 트리거될 때 Capture Screen에서 툴이 기본적으로 LWAPP 프로토콜을 캡처하는지 확인할 수 있습니다. 그림 1은 LAP에서 수행한 검색 요청 중 LWAPP 프로토콜 캡처를 보여줍니다.

그림 1



패킷에 대한 세부 정보를 보려면 패킷을 두 번 클릭합니다.

관련 정보

- EtherPeek FAQ
- 옴니 소개
- OmniPeek 5.0 다운로드
- 기술 지원 및 문서 – Cisco Systems