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

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Modificare il file di decodifica LWAPP Modificare il file TCP\_UDP\_Ports.dcd Modificare il file Pspecs.xml Decodifica LWAPP in OmniPeek 5.0 Verifica Informazioni correlate

### **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 <u>domande frequenti su EtherPeek</u>. Per informazioni su OmniPeek, fare riferimento a <u>Introduzione a Omni</u>.

#### 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 <u>Cisco sulle convenzioni</u> 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:

 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.
- 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.
- 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 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.

🕅 OmniPeek Dem	e - [Capture 4]								
File Edit View	Capiture Send Monitor Tool	s Wedow Help		1.0	and the second	1.1.4	and the second	1.12	. 0
() - () - U		STRODES	100	:) 0	3 Duy Now				
Packets received	707 Buffer um	age: 19%			and the second second			54	et Caphana
S-	TUT PROFILE	anti - incode a bacara					the loss beauty the states	Q	
Carbon Carbon	An and Apple and Sold (Col)		Lange and						
Capture		- B Y	A. 8.	1.1					
b Enclusive	Source	Destination	Flags	Sze	Relative Time	Protocol	Sumary		
Log	10.77.244.209	IP Broadcast		96	0:01:10.277675	083	C OTERY BARE-CI	SCO-LWAPS	-CONTROL
Filters	#900:1A:A1:54:30:AB	BROAFT 802.14 Br		64	0:01:11.067006	002.1			
= Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	syslog	SEC-60909,D#t=	514 .1-	1.2.2
Herarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	syslog	SEC-60909,D#t+	514 ,1+	95
Flat	10.77.244.209	IP Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t-	514 .14	91
Accilcation	#00:1A:A1:54:30:AB	BReast 802.1d Br		64	0:01:13.072054	002.1			
web	10.77.244.209	17 Excedeast		96	0:01:13.277035	08/5	C OTERT NAME-CI	300-14821	-CONTROL
Servers	B00:1A:A1:54:30:A8	BReast 802.1d Br		64	0:01:15.077120	802.1			
Clerits	10.77.244.209	17 Scondcast		96	0:01:16.275883	04/5	C QUERT NAME-CI	SCO-LWAP	-CONTROL
Papers	#900:1A:A1:54:30:AB	## Heast 002.1d Br		64	0:01:17.081615	002.1			
Reports	B00:1A:A1:54:30:AB	Mast 002.1d Sr		64	0:01:19.088698	802.1			
Voice & Video	200:18:D4:E3:A8:18	Ethernet Scondcast		64	0:01:19.275905	ARP Request	10.77.244.204 +		
Calls	2900:1A:A1:54:30:AB	200:1A:AI:54:30:AB		64	0:01:20.042094	Loopback			
Media	10.77.244.209	IP Broadcast		151	0:01:20.274075	syslog	SEC+60909,D91+	514 .14	105
C Visuals	10.77.244.209	IP Broadcast		156	0:01:20.275459	syslog	Scc+60909,Det+	514 .14	110
Acdex	10.77.244.209	IF Stoadcast		146	0:01:20.276394	LVAPP	15co+14977,Det+1	2223 .1.4	100
Peer Mac	290011A1A11541301A8	BEASt 002.18 St		64	0:01:21.090924	607.1			
Graphs	BO0:1A:A1:54:30:AB	BRCast 002.1d Br		64	0:01:23.095938	002.1			
Relative	#900:1A:A1:54:30:AB	33:33:33:30:00:00:00		64	0:01:23.481099	00-00-00-20-04			
Nodes	\$900:1A:A1:54:30:AB	B01:00:0C:00:00:00		94	0:01:23.481160	00-00-00-00-03			
Puntocrais	#900:1A:A1:54:30:A5	BO Mcast 802.14 St		64	0:01:25.102850	602.1			
Summary	#900:1A:A1:54:30:A5	BReast 802.1d Br		64	0:01:27.107696	802.1			
	#900:1A:A1:54:30:A8	BReast 802.1d Sr		64	0:01:29,112083	802.1			
	#00:1A:A1:54:30:AB	\$900:1A:A1:54:30:A8		64	0:01:30.051235	Loopback			
	#900:18:D4:E3:A0:18	Ethernet Broadcast		64	0:01:30.292150	ARP Request	10.77.244.203 -	7	
	#900:1A:A1:54:30:AB	BReast 002.1d Br		64	0:01:31,116975	802.1			
	\$900:18:D4:E3:A8:18	BEthemet Broadcast		64	0:01:31.291080	ARP Request	10.77.244.203 -	2	
	200:1A:A1:54:30:A8	BReast 802.14 Sr		64	0:01:33,122176	602.1	,		
	10.77.244.209	IF Broadcast		132	0:01:34.336071	systop	frc-60909.Det-	314 .1-	66
	10,77,244,209	IP Broadcast		132	0:01:34,336487	syslog	Spin60909.Deta	\$14 .1+	64
	#200:1A:A1:54:30:48	BO Mcast 002.14 Br		64	0:01:35,126796	802.1			
	10,77,244,209	IP Spoadcast		132	0:01:35,348150	syslog	Src+60909,Data	514 .1-	66
	#900:1A:A1:54:30:A5	BCast 002.1d Br		64	0:01:37.135293	802.1			
	manager and a state of a state of the				P. 01. 10 P.811.00	******			
							Server and the server se		2

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

## Informazioni correlate

- Domande frequenti su EtherPeek
- Presentazione di Omni
- <u>Scarica OmniPeek 5.0</u>
- Documentazione e supporto tecnico Cisco Systems