



Practica: Captura y Analisis de paquetes con Wireshark..

Cuando dos aplicaciones se comunican a través de la red, éstas generan PDU's con datos de aplicación que es necesario encapsular dentro de otros PDU's de capas inferiores y poder dar así un buen tratamiento a los datos enviados. Dos de las principales capas son la capa de red (Internet) y la capa de Transporte, en las cuales se manejan datos sensibles, tales como las direcciones lógicas de los dispositivos de red que contienen dichas aplicaciones y los identificadores de estas aplicaciones (# de puerto).

Wireshark es una herramienta muy conocida dentro de los analizadores de protocolos (*sniffers*) que permite leer la información contenida dentro de los distintos PDU's de un paquete que viaja por la red. A continuación mostraremos un ejemplo de una trama (Capa 2) capturada con Wireshark.

Observe la siguiente trama capturada con la herramienta wireshark :

```

0000 00 21 9b ea 8a 7c 00 19 e4 b9 64 b1 08 00 45 00 !...|...d...E.
0010 00 28 7e 2d 40 00 1c 06 41 9a bb 8d 01 92 c0 a8 -@.<. A.....
0020 01 41 00 50 c4 1f 9e bb 03 f9 fe f5 dd bd 11 .A.P....P.
0030 1a 99 00 00 00 00 00 00 00 00 00 00

```

Ésta trama puede ser desencapsulada de la siguiente manera:

- Trama Ethernet2 (Capa de Enlace de Datos)
 - MAC Destino: 00:21:9b:ea:8a:7c
 - MAC Origen: 00:19:e4:b9:64:b1
 - Tipo de trama: IP(0x800)
 - Trailer: 000000000000
- Paquete IP (Capa de Red)
 - Versión: 4
 - Longitud encabezado: 5 (palabras de 32 bits=20 bytes)
 - TOS: 0
 - Longitud total del paquete: 40 palabras de 32 bits(0028)=160 bytes
 - Identificador: 32301(0x7e2d)
 - Banderas: No fragmentar (0x04)
 - Offset: 0(0x00)
 - TTL: 60 (0x3c)
 - Protocolo: TCP (0x06) //RFC 1340
 - Checksum: 0x419a



- IP Origen: 187.141.1.146 (bb8d0192)
- IP destino: 192.168.1.65 (c0a80141)
- Segmento TCP (capa de Transporte)
 - Puerto Origen: 80 (0x0050) //http RFC 1340
 - Puerto Destino: 50207 (0xc41f)
 - Número de secuencia: 2663056377 (0x9ebb03f9)
 - Número de acuse: 4277525949 (0xfef5ddbd)
 - Longitud de encabezado: 20 bytes (0x05)
 - Banderas: 0x11 (ACK + FIN)
 - 0_____: Reducción de ventana por congestión
 - _0_____: ECN-Echo (Notificación explícita de congestión)
 - __0_____: Urgente
 - ___1_____: ACK
 - ____0_____: PUSH
 - ____0 : RESET
 - ____0_: SYN
 - _____1: FIN
 - Tamaño ventana: 6809 (0x1a99)
 - Checksum: 0xd259

Desarrollo:

Uso de Wireshark para examinar las tramas de Ethernet

Paso 1: Revisar las descripciones y las longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

**Paso 2: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP**

En la tabla siguiente, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción						
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.						
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada como 12 dígitos hexadecimales, 0-9, A-F. Un formato común es 12:34:56:78:9A:BC. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC); los seis últimos números hexadecimales corresponden al número de serie de la NIC. La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast.						
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)							
Tipo de trama	0x0806	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior que admite Ethernet II. Dos tipos comunes de trama son: <table><tr><th>Valor</th><th>Descripción</th></tr><tr><td>0x0800</td><td>Protocolo IPv4</td></tr><tr><td>0x0806</td><td>Protocolo de resolución de direcciones (ARP)</td></tr></table>	Valor	Descripción	0x0800	Protocolo IPv4	0x0806	Protocolo de resolución de direcciones (ARP)
Valor	Descripción							
0x0800	Protocolo IPv4							
0x0806	Protocolo de resolución de direcciones (ARP)							
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 y 1,500 bytes.						
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica						



Analizar las tramas y paquetes de las siguientes direcciones:

I. Capture por lo menos 10 paquetes utilizando Wireshark y para cada uno de ellos rellene los siguientes encabezados

1. Análisis de una IP de una **máquina de laboratorio**
2. Análisis de una IP de la página www.escom.ipn.mx
3. Análisis de una IP de la página www.saes.escom.ipn.mx
4. Análisis de una IP 148.204.56.254
5. Análisis de una IP 148.204.61.254
6. Análisis de una de la pagina www.ipn.mx
7. Análisis de una de la pagina www.google.com.mx
8. Análisis de una de la pagina www.facebook.com
9. Análisis de una de la pagina _____
10. Análisis ARP 148.204.56.255
11. Análisis de una IP **148.204.1.2**

Encabezado IP (Capa de red)

0				1				2				3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
Version				IHL				Type of Service				Total Length											
								Identification				Flags				Fragment Offset							
								Time to Live								Protocol							
								Source Address															
								Destination Address															
								Options								Padding							

**Trama Ethernet 2 (Capa de Enlace de Datos)**

```

+-----+-----+-----+-----+
|  Dst   |  Src   |  Type  |  Data...|
+-----+-----+-----+-----+
<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->
Type 0x80 0x00 = TCP/IP
Type 0x06 0x00 = XNS
Type 0x81 0x37 = Novell NetWare

```

Encabezado TCP (capa de Transporte)

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
|          Source Port          |          Destination Port          |
+-----+-----+-----+-----+
|          Sequence Number      |
+-----+-----+-----+-----+
|          Acknowledgment Number      |
+-----+-----+-----+-----+
|  Data |  Reserved | U|A|P|R|S|F|          Window          |
| Offset|           | R|C|S|S|Y|I|           |
|       |           | G|K|H|T|N|N|           |
+-----+-----+-----+-----+
|          Checksum              |          Urgent Pointer          |
+-----+-----+-----+-----+
|          Options                |          Padding                |
+-----+-----+-----+-----+
|          data                   |
+-----+-----+-----+-----+

```

Encabezado UDP (capa de Transporte)

```

0          7 8          15 16          23 24          31
+-----+-----+-----+-----+
|          Source Port          |          Destination Port          |
+-----+-----+-----+-----+
|          Length                |          Checksum                |
+-----+-----+-----+-----+
|          data octets ...      |
+-----+-----+-----+-----+

```



De las capturas de los paquetes de los encabezados anteriores responde las preguntas:

1. Análisis de una **IP** de una **máquina de laboratorio**
 - a) ¿Cuál es la MAC destino?
 - b) ¿Cuál es la IP destino?
 - c) En el campo Protocol ¿Cuál es el valor del campo?

2. Análisis de una **IP** de la página **www.escom.ipn.mx**
 - d) ¿Cuál es la MAC destino?
 - e) ¿Cuál es la IP destino?
 - f) En el campo Protocol ¿Cuál es el valor del campo?

3. Análisis de una **IP** de la pagina **www.saes.escom.ipn.mx**
 - g) ¿Cuál es la MAC destino?
 - h) ¿Cuál es la IP destino?
 - i) En el campo Protocol ¿Cuál es el valor del campo?

4. Análisis de una **IP 148.204.56.254**
 - j) ¿Cuál es la MAC destino?
 - k) ¿Cuál es la IP destino?
 - l) En el campo Protocol ¿Cuál es el valor del campo?

5. Análisis de una **IP 148.204.61.254**
 - m) ¿Cuál es la MAC destino?
 - n) ¿Cuál es la IP destino?
 - o) En el campo Protocol ¿Cuál es el valor del campo?

6. Análisis de una de la pagina **www.ipn.mx**
 - p) ¿Cuál es la MAC destino?
 - q) ¿Cuál es la IP destino?
 - r) En el campo Protocol ¿Cuál es el valor del campo?

7. Análisis de una de la pagina **www.google.com.mx**
 - s) ¿Cuál es la MAC destino?
 - t) ¿Cuál es la IP destino?
 - u) En el campo Protocol ¿Cuál es el valor del campo?



8. Análisis de una de la pagina **www.facebook.com**
 - v) ¿Cuál es la MAC destino?
 - w) ¿Cuál es la IP destino?
 - x) En el campo Protocol ¿Cuál es el valor del campo?
9. Análisis de una de la pagina _____
 - y) ¿Cuál es la MAC destino?
 - z) ¿Cuál es la IP destino?
 - aa) En el campo Protocol ¿Cuál es el valor del campo?
10. Análisis de una **IP 148.204.1.2**
 - bb) ¿Cuál es la MAC destino?
 - cc) ¿Cuál es la IP destino?
 - dd) En el campo Protocol ¿Cuál es el valor del campo?
11. Capturar una trama ARP (mandar un ping a la **IP 148.204.56.255**) y rellenar los campos

Reflexión

12. ¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?
13. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?