Instituto Politécnico Nacional

ESCOM

Ingeniería en

Sistemas Computacionales

Redes de Computadoras

Torres Abonce Luis Miguel

Olguin Castillo Brayan Mauricio

Grupo: 5CM4

Practica 2: Wireshark

Profesor. Ing. Juan J. Alcaraz Torres.

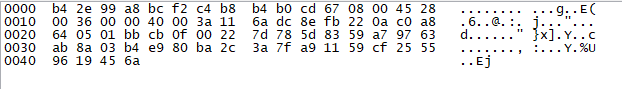
Introducción.

En esta práctica realizamos la captura de 10 paquetes con el programa llamado wireshark, de estos debemos de rellenar los encabezados de TCP (Capa de transporte), UDP(Capa de transporte), IP(Capa de red) Ethernet 2 (Capa de enlace de datos).

Wireshark es una herramienta de análisis de tráfico de red que se utiliza para capturar y examinar paquetes de datos en una red. Se utiliza a menudo para depurar problemas de red, detectar intrusiones y violaciones de seguridad, y realizar análisis de rendimiento. Wireshark es gratuito y de código abierto, y está disponible para Windows, MacOS y Linux.

Al utilizar Wireshark, puede ver información detallada sobre cada paquete capturado, incluyendo su origen y destino, el tipo de paquete, el tamaño y el contenido. Esto le permite analizar la actividad de red y entender cómo se están transmitiendo los datos en su red. Wireshark también incluye una serie de características avanzadas, como la capacidad de filtrar y decodificar paquetes de acuerdo con diferentes criterios, lo que le permite investigar problemas de red más a fondo.

Desarrollo

1.

UDP

0 7 8 15 16 23 24 31

+--------+--------+--------+--------+

| Source port |Destination port |

| 01bb | cb0f |

+--------+--------+--------+--------+

| Leght | checksum |

| 0022 | 7d 78 |

+--------+--------+--------+--------+

| data octets |

| 26 |

+---------------- ...---------------|

IP

|  |  |  |
| --- | --- | --- |
| 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 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|version=42 | IHL=4 | Type of service=28|Total Length=0036 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Identification=0000 | flags=40 | fragment offset=00 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live= 3a | Protocol=11 |Header Checksum=6adc |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=8e fb 22 0a |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address = c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Ethernet 2

+---------+---------+---------+----------

|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b0 cd 67|Type=08 00|Data...

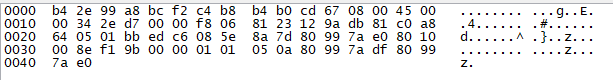
+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWare

2.



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=01 bb | Destination Port= ed c6 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Sequence Number=08 5e 8a 7d |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Acknowledgment Number= 80 99 7a e0 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Data | |U|A|P|R|S|F| |

| Offset| Reserved |R|C|S|S|Y|I| Window= 00 8e |

| | |G|K|H|T|N|N| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Checksum=f1 9b | Urgent Pointer |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Options=01 01 05 0a 80 99 7a df 80 99 7a e0 | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| data |

+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++++

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 2 3 4 5 6 7 8 9 0 1 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Version=45|IHL=45|Type of Service=|Total Length=00 34 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Identification=2e d7 |Flags=00|Fragment Offset=00 00 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live=f8 | Protocol=06| Header Checksum=81 23 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=12 9a db 81 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address=c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Trama Ethernet 2 (Capa de Enlace de Datos)

+---------+---------+---------+----------

|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b4 b0 cd 67|Type=08 00|Data...

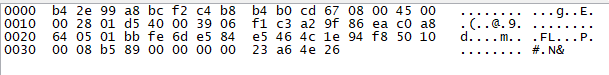
+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWar

3.

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=01 bb | Destination Port= fe 6d |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Sequence Number=e5 84 e5 46 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Acknowledgment Number= 4c 1e 94 f8 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Data | |U|A|P|R|S|F| |

| Offset| Reserved |R|C|S|S|Y|I| Window= 00 08 |

| | |G|K|H|T|N|N| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Checksum=b5 89 | Urgent Pointer |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| data |

+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++++

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 2 3 4 5 6 7 8 9 0 1 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Version=45|IHL=45|Type of Service=|Total Length=00 28 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Identification=01 d5 |Flags=40|Fragment Offset=40 00 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live=39 | Protocol=06| Header Checksum=f1 c3 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=a2 9f 86 ea |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address=c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Trama Ethernet 2 (Capa de Enlace de Datos)

+---------+---------+---------+----------

|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b4 b0 cd 67|Type=08 00|Data...

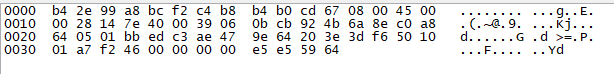
+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWar

3.



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=01 bb | Destination Port= ed c3 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Sequence Number=ae 47 9e 64 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Acknowledgment Number= 20 3e 3d f6 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Data | |U|A|P|R|S|F| |

| Offset| Reserved |R|C|S|S|Y|I| Window= 01 a7 |

| | |G|K|H|T|N|N| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Checksum=f2 46 | Urgent Pointer |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| data |

+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++++

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 2 3 4 5 6 7 8 9 0 1 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Version=45|IHL=45|Type of Service=|Total Length=00 28 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Identification=14 7e |Flags=40|Fragment Offset=40 00 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live=39 | Protocol=06| Header Checksum=0b cb |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=92 4b 6a 8e |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address=c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Trama Ethernet 2 (Capa de Enlace de Datos)

+---------+---------+---------+----------

|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b4 b0 cd 67|Type=08 00|Data...

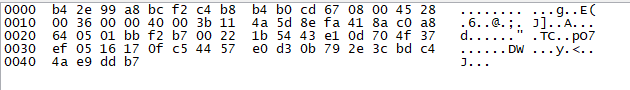
+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWar

4.



UDP

0 7 8 15 16 23 24 31

+--------+--------+--------+--------+

| Source port |Destination port |

| 01bb | f2 b7 |

+--------+--------+--------+--------+

| Leght | checksum |

| 0022 | 1b 54 |

+--------+--------+--------+--------+

| data octets |

| 26 |

+---------------- ...---------------|

IP

|  |  |  |
| --- | --- | --- |
| 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 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|version=45 | IHL=4 | Type of service=28|Total Length=00 36|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Identification=00 00 | flags=40|fragment offset=40 00|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live= 3b | Protocol=11 |Header Checksum=4a 5d|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=8e fb 22 0a |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address = c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Ethernet 2

+---------+---------+---------+----------

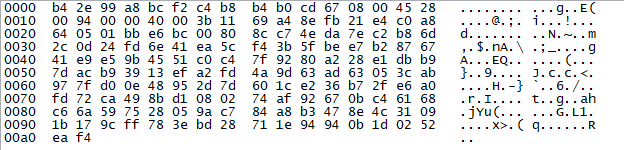
|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b0 cd 67|Type=08 00|Data...

+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWare

5. 

UDP

0 7 8 15 16 23 24 31

+--------+--------+--------+--------+

| Source port |Destination port |

| 01 bb | e6 bc |

+--------+--------+--------+--------+

| Leght | checksum |

| 00 80 | 8c c7 |

+--------+--------+--------+--------+

| data octets |

| 26 |

+---------------- ...---------------|

IP

|  |  |  |
| --- | --- | --- |
| 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 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|version=45 | IHL=45 |Type of service=28|Total Length=00 94|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Identification=00 00 | flags=40|fragment offset=40 00|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live= 3b | Protocol=11 |Header Checksum=69 a4|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=8e fb 22 0a |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address = c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Ethernet 2

+---------+---------+---------+----------

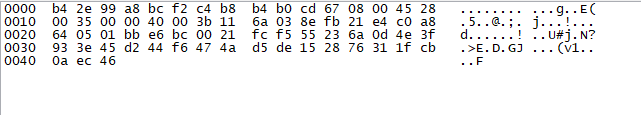
|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b0 cd 67|Type=08 00|Data...

+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWare

6. 

UDP

0 7 8 15 16 23 24 31

+--------+--------+--------+--------+

| Source port |Destination port |

| 01 bb | e6 bc |

+--------+--------+--------+--------+

| Leght | checksum |

| 00 21 | fc f5 |

+--------+--------+--------+--------+

| data octets |

| 26 |

+---------------- ...---------------|

IP

|  |  |  |
| --- | --- | --- |
| 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 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|version=45 | IHL=45 |Type of service=28|Total Length=00 35|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Identification=00 00 | flags=40|fragment offset=40 00|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live= 3b | Protocol=11 |Header Checksum=6a 03|

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source Address=8e fb 22 0a |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address = c0 a8 64 05 |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Ethernet 2

+---------+---------+---------+----------

|Dst=b4 2e 99 a8 bc f2|Src=c4 b8 b0 cd 67|Type=08 00|Data...

+---------+---------+---------+----------

<-- 6 --> <-- 6 --> <-- 2 --> <-46-1500->

Type 0x80 0x00 = TCP/IP Type 0x06 0x00 = XNS

Type 0x81 0x37 = Novell NetWare

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 pagina www.escom.ipn.mx

d) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

e) ¿Cuál es la IP destino?

Destination: 148.204.58.225

f) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

3. Análisis de una IP de la pagina www.saes.escom.ipn.mx

g) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

h) ¿Cuál es la IP destino?

Destination: 148.204.56.240

i) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

4. Análisis de una IP 148.204.56.254

j) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

k) ¿Cuál es la IP destino?

Destination: 148.204.56.254

l) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

5. Análisis de una IP 148.204.61.254

m) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

n) ¿Cuál es la IP destino?

Destination: 148.204.61.254

o) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

6. Análisis de una de la pagina www.ipn.mx

p) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

q) ¿Cuál es la IP destino?

Destination: 104.214.26.43

r) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

7. Análisis de una de la pagina www.google.com.mx

s) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

t) ¿Cuál es la IP destino?

Destination: 142.251.34.99

u) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

8. Análisis de una de la pagina www.facebook.com

v) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67

w) ¿Cuál es la IP destino?

Destination: 157.240.25.35

x) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

9. Análisis de una de la pagina twitter.com

y) ¿Cuál es la MAC destino?

Destination: c4:b8:b4:b0:cd:67 (c4:b8:b4:b0:cd:67)

z) ¿Cuál es la IP destino?

Destination: 104.244.42.129 (104.244.42.129)

aa) En el campo Protocol ¿Cuál es el valor del campo?

Protocol: ICMP (1)

11. ¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

Puede mostrar la dirección MAC actual de los hosts locales porque esa información está disponible en el tráfico que se está monitoreando, pero la MAC de los hosts remotos por el contario no se está monitoreando ese trafico

12. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?

Es importante porque permite detectar y solucionar problemas de red, proteger la red de ataques externos y optimizar su rendimiento.

Conclusión

En esta practica pudimos aprender a manejar de una manera básico la detección y análisis de paquetes con la herramienta wireshark, esto aplicando un comando ping en la consola de nuestro sistema operativo para rastrear este paquete y analizarlo por encabezados, ya sea por UDP, TCP, IP o Ethernet 2. Ubicando la información ya sea de manera hexadecimal que es un poco más difícil o viendo directamente todas las variables en el programa.