Tema 8.8.2.8.EnriqueGomezTagle

martes, 27 de febrero de 2024 21:14

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

---

¿Qué característica significativa tiene el contenido del campo de dirección de destino?

Todos los hosts en la LAN recibirán esta trama de difusión. 192.168.1.1 (host) enviará una difusión a la fuente.

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?

Necesita la MAC destino. Con ARP broadcast obtiene la MAC del host.

¿Cuál es la dirección MAC del origen en la primera trama?

f4:8c:50:62:62:6d

¿Cuál es el identificador de proveedor (OUI) de la NIC del origen?

Intel Cor (Intel Corporation)

¿Qué porción de la dirección MAC corresponde al OUI?

Primeros 3 octetos

¿Cuál es el número de serie de la NIC del origen?

62:62:6d

d. En el prompt en Node: H3, introducir **ip address** para verificar la dirección IPv4 y registrar la dirección MAC.

Host-interfaz	Dirección IP	Dirección MAC
H3-eth0	10.0.0.13	6e:81:b8:8c:be:0d

e. En el cursor de Node: H3, introduzca **netstat -r** para mostrar la información del gateway predeterminado.

```
[root@secOps ~]# netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 10.0.0.1 0.0.0.0 UG 0 0 0 H3-eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 H3-eth0
```

¿Cuál es la dirección IP del gateway predeterminado correspondiente al host H3?

10.0.0.1

¿Cuál es la dirección MAC de la NIC de la PC?

6e:81:b8:8c:be:0d

¿Cuál es la dirección MAC del gateway predeterminado?

f2:df:19:8b:9f:d0

d. Pueden hacer clic en la flecha que se encuentra al principio de la segunda línea para obtener más información sobre la trama de Ethernet II.

¿Qué tipo de trama se muestra?

IPv4 (0X0800) o una trama IPv4

e. En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

¿Cuál es la dirección IP de origen?

10.0.0.13

¿Cuál es la dirección IP de destino?

10.0.0.1

g. Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.

¿Qué dispositivo y qué dirección MAC se muestran como dirección de destino?

Dispositivo Host 3 y dirección MAC 6e:81:b8:8c:be:0d

Paso 7: Examinar los nuevos datos del panel de la lista de paquetes de Wireshark.

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y de destino?

Fuente: 6e:81:b8:8c:be:0d

Destino: f2:df:19:8b:9f:d0

¿Cuáles son las direcciones IP de origen y de destino que contiene el campo de datos de la trama?

Fuente: 10.0.0.13

Destino: 172.16.0.90

Comparen estas direcciones con las direcciones que recibió en el paso 5. La única dirección que cambió es la dirección IP de destino.

¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

Las tramas de capa 2 nunca abandonan la LAN. El origen usa la MAC del Gateway. Cuando el gateway recibe, quita la info de capa 2 y luego crea un nuevo encabezado con la MAC del siguiente salto.

Reflexión

En Wireshark, no se muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

7 octetos de 1010 alternados y el octeto de inicio de trama 10101011