Fundamentos de sistemas y arquitecturas

Práctica 2: Redes de comunicación. Spoofing ARP.

Daniel Pérez Efremova

Índice

Ejercicio 1

En esta sección se presentan las dos máquinas virtuales y los pasos seguidos para recabar las direcciones IP y MAC de las máquinas y los routers. En la Tabla se describen las direcciones. Se aprecia que las direcciones IP de las máquinas son

	VM1	VM2	Router
IP	172.16.228.128	172.16.228.129	172.16.228.2
MAC	00:0c:29:82:82:ee	00:0c:29:fb:44:8e	00:50:56:ff:2f:3a

Tabla 1: Tabla de direcciones

distintas. En el Anexo se pueden encontrar dos capturas. La Figura 1 contiene las consultas por consola de las direcciones. La Figura 2 contiene los pings mutuos de las máquinas.

Ejercicio 2

En la Figura 3 se muestra el resultado del ataque. En la máquina MV1 se ataca la MV2 (172.16.228.129) acaparando el router (172.16.228.2). Al mismo tiempo, desde la MV2 se observa que antes del ataque el router tenía su dirección MAC correctamente definida (00:50:56:ff:2f:3a), sin embargo, al iniciar el ataque su dirección MAC se corresponde con la de MV1 (00:0c:29:82:82:ee). Al hacer un *arping* desde MV2 al router, se observa que responde la MV1 con la IP del router (172.16.228.2) pero con la dirección MAC de MV1 (00:0c:29:82:82:ee).

Ejercicio 3

En la Figura 4 se ve como se lanzan los dos ataques. En las Figuras 5, 6, 7 y 8, se ven las capturas de tráfico asociado a la resolución DNS.

En primer lugar, en la Figura 5 se ve como la MV2 pasa el paquete al router. Sin embargo, debido al ataque, en el nivel ethernet vemos que el destino es la MV1.

Después, en la Figura 6 se ve que la MV1 envía la resolución al router, aunque a nivel IP parece que lo ha hecho la MV2.

En la Figura 7 se ve la respuesta de la resolución. Se ve como el verdadero router, con dirección MAC 00:50:56:ff:2f:3a, envía la respuesta a la MV1, con MAC 00:0c:29:82:82:ee. Aunque a nivel de IP parece que la comunicación es entre el verdadero router y MV2.

Finalmente, en la Figura 8 vemos como la MV1, con MAC 00:0c:29:82:82:ee

envía la respuesta a la MV2 con MAC 00:0c:29:fb:44:8e, suplantando la identidad del router. Aunque aparentemente, según las direcciones IP, la comunicación es entre el router y MV2.

A la derecha de las imágenes se puede observar el resultado del lookup, donde MV2 no es consciente de que su paquete ha sido interceptado, ya que se proporciona por consola la IP del router real en los valores de Server.

Cabe señalar que la petición y respuesta a la resolución DNS deberían haberse enviado en un único paquete y no en dos, como se observa en wireshark, por lo que el tráfico duplicado es un indicio bastante sospechoso del ataque. Se añade en Anexos una resolución DNS correctamente realizada sin sufrir ningún ataque y desde MV1 (Figura 9).

En conclusión, queda probado que la MV1 se ha hecho pasar por el router con respecto a la MV2 y también se ha hecho pasar por MV2 con respecto al router, interceptando todo el tráfico entre ambos nodos de la red. Sin embargo, este ataque se puede detectar y trazar fácilmente con wireshark prestando atención a las direcciones MAC de los remitentes y destinatarios de los paquetes así como a la cantidad de paquetes que circulan.

Ejercicio 4

Un servidor DNS traduce un nombre de dominio (humano) en una dirección IP numérica que se pueda usar para enrutar paquetes. El protocolo es recursivo hasta que se encuentra una respuesta válida, almacenando en caché el último servidor que da la respuesta. En el momento es que se suministra un servidor falso para procesar las peticiones, se le considera infectado (DNS spoofing).

Mediante un spoofing de ARP, se puede forzar a que el servidor DNS almacene en caché una IP distinta a la que tiene la víctima para procesar las peticiones.

Una vez que la dirección IP (Gateway) de la víctima se ha suplantado, por ejemplo con un ARP spoofing, se está realizando un DNS spoofing.

Anexo

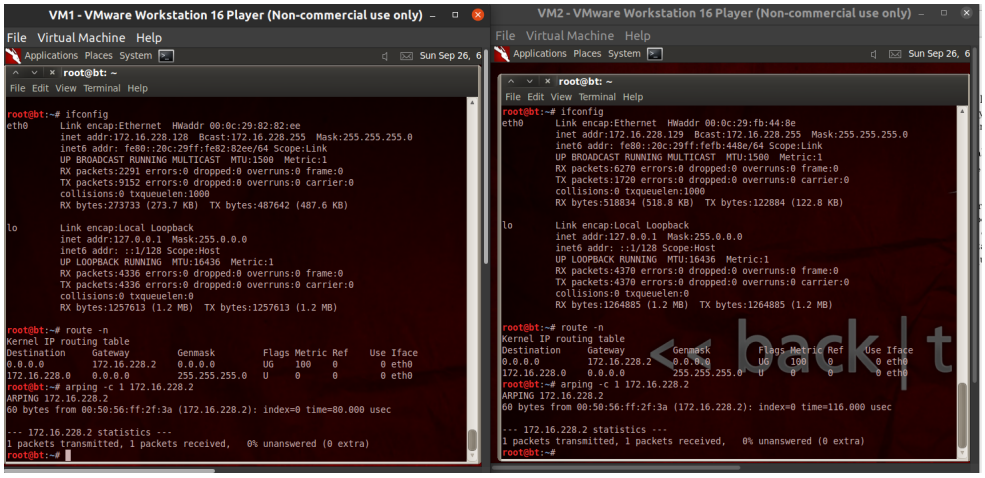

Figura 1: Direcciones de red de las máquinas virtuales

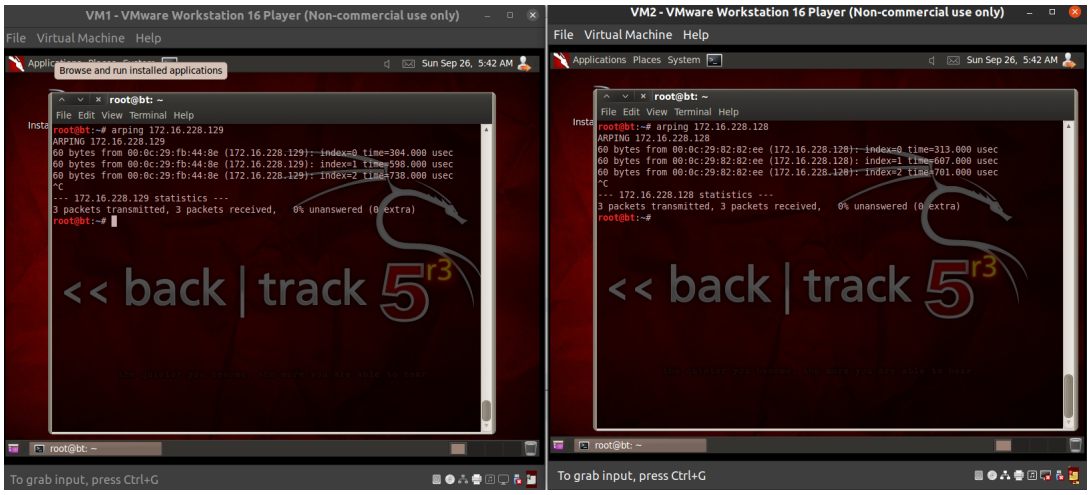

Figura 2: Comprobación de la conectividad a nivel 2 entre máquinas virtuales

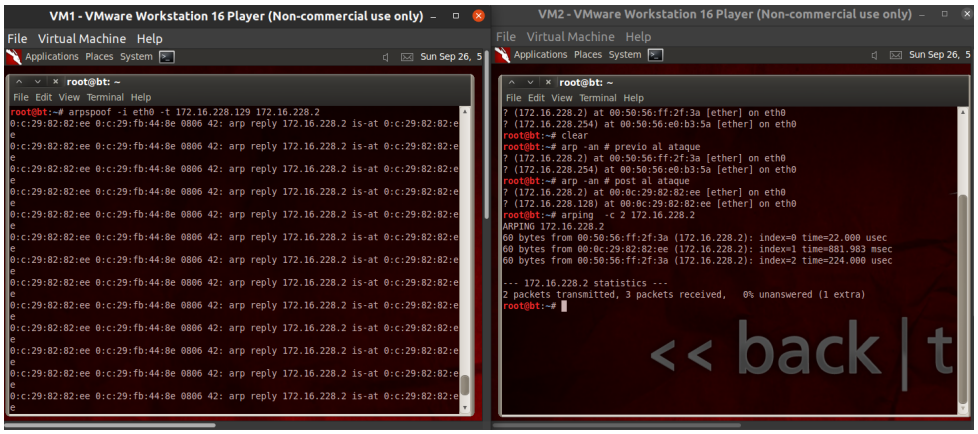

Figura 3: Comprobación de la identidad (suplantada) del router

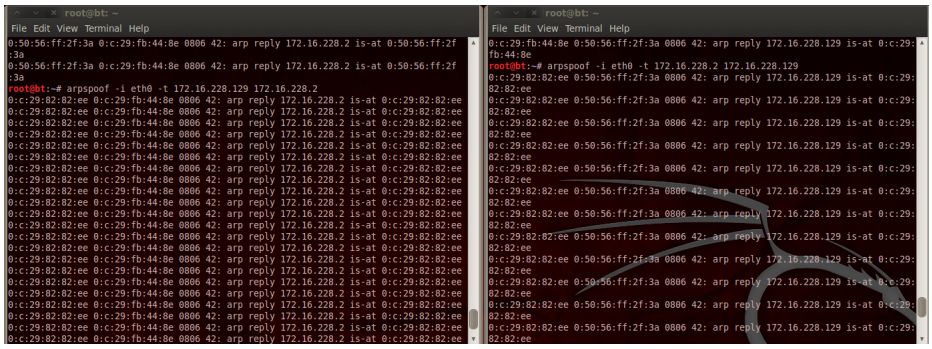

Figura 4: Intercepción del tráfico entre el router y MV2

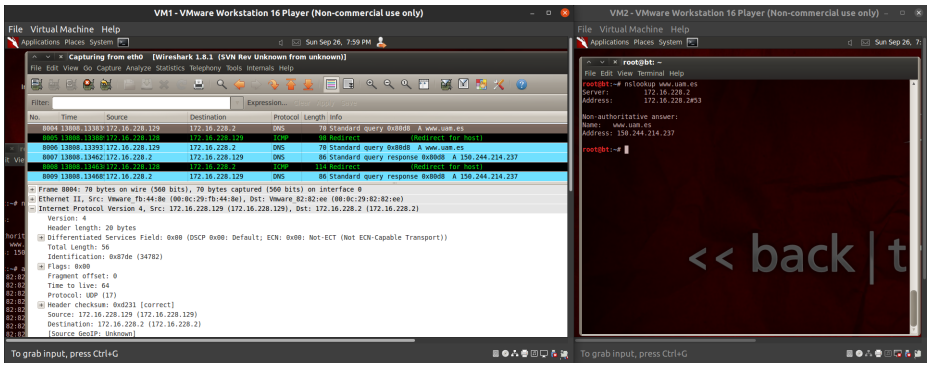

Figura 5: Intercepción del tráfico entre el router y MV2 (paso 1)

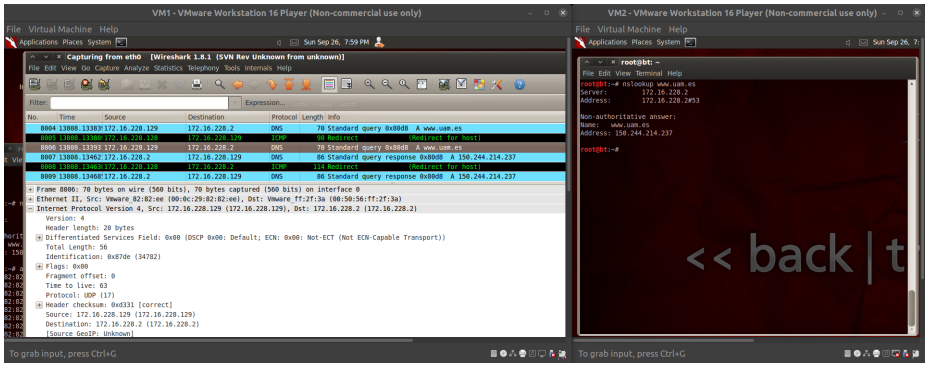

Figura 6: Intercepción del tráfico entre el router y MV2 (paso 2)

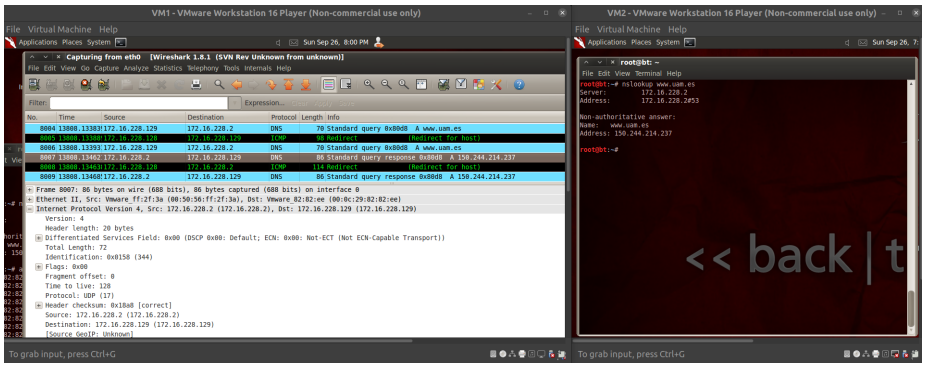

Figura 7: Intercepción del tráfico entre el router y MV2 (paso 3)

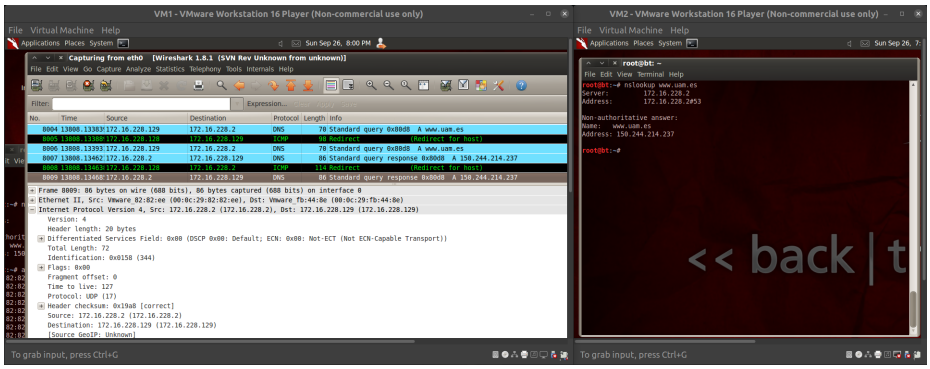

Figura 8: Intercepción del tráfico entre el router y MV2 (paso 4)

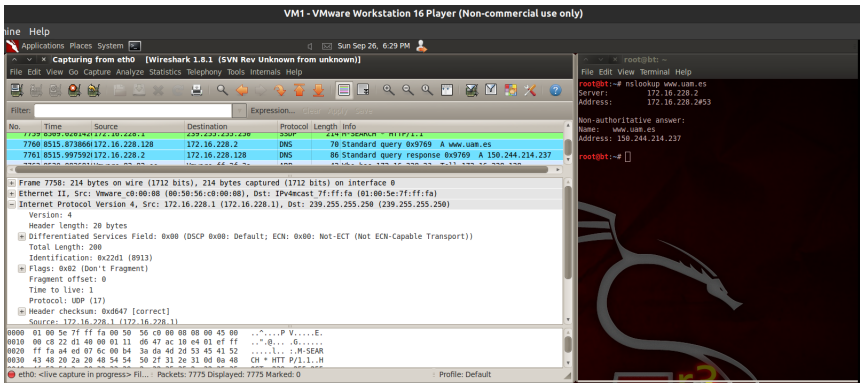

Figura 9: Resolución correcta DNS