Herramientas básicas en TCP/IP
Ping, ARP

Alfredo Abad

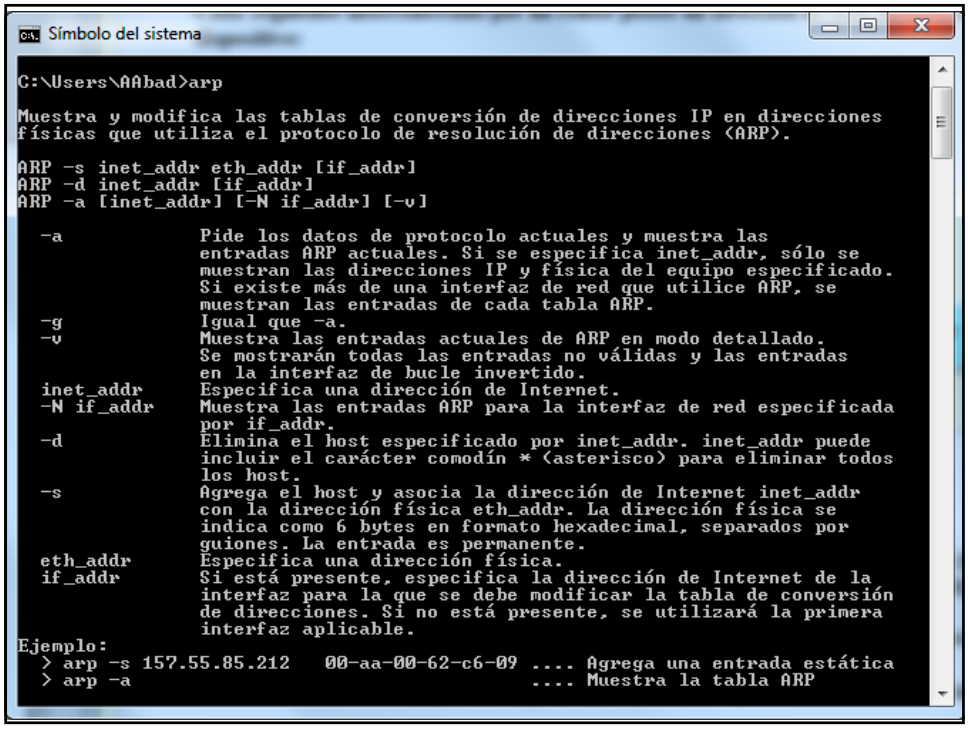
UA: 13-ago-2018

PARP403-PingArp.pptx

Objetivo de la práctica

- Se tratará de utilizar distintas herramientas estándar en los sistemas operativos de red para la pila de protocolos TCP/IP
  - Se necesitarán al menos dos nodos de red ejecutando TCP/IP, que denominaremos en sentido figurado Tu-ID1 (pc1) y Tu-ID2 (pc2), que pueden ser Windows o Linux o mezclas de ambos
  - Deberás tener a mano las direcciones IP (nivel 3) y MAC (nivel 2 o direcciones físicas) de cada una de las máquinas que intervengan en la práctica
  - Las direcciones IP de las máquinas deben estar en la misma subred
    - En el caso de que estén en distinta subred, necesitarás un enrutador que interconecte las dos subredes
- Instala un sniffer (Wireshark, por ejemplo) en cada uno de estos dos sistemas para capturar todo el tráfico generado durante la ejecución de la práctica

TRABAJANDO CON ARP



Operación con la caché de ARP

- Visualiza en primer lugar las direcciones ip1, ip2, mac1 y mac2
  - Regístralas por escrito y tenlas a mano durante toda la práctica
- Asegúrate de que tienes activado y capturando un sniffer (puede servir Wireshark o el monitor de red de Windows) tanto en pc1 como en pc2
- Consulta el estado inicial de la caché de ARP con «arp –a» tanto en pc1 como en pc2 registrando el resultado
- Haz ping desde pc1 a pc2
  - Consulta de nuevo la caché de ARP en ambos nodos
  - ¿En qué han variado? ¿Por qué? Justifica las respuestas
- Borra la entrada de caché en pc1 del nodo pc2 con arp –d ip2
  - ¿Ha variado la caché de pc1? Y, ¿la de pc2? ¿Por qué?
  - ¿Qué tienes que hacer para volver a recuperar el registro de pc2 en la caché ARP de pc1?

Operación con ARP

- Ahora haz ping a una dirección inexistente en la red (por ejemplo, 10.10.1.1)
  - Comprueba que ping no obtiene ningún resultado, pero registra la información que te proporciona
  - Consulta en la caché ARP si hay alguna entrada que contenga 10.10.1.1
- Añade una dirección MAC ficticia (por ejemplo, 00:00:00:01:02:03) a la caché ARP en pc1 y asóciala a la IP ficticia anterior (puedes utilizar la orden «arp –s 10.10.1.1 00-00-00-01-02-03» desde una consola con los derechos elevados
- Ahora haz ping a la dirección 10.10.1.1
  - El mensaje proporcionado por ping, ¿es el mismo que el anterior?
  - Consulta de nuevo la cache ARP buscando alguna entrada que contenga 10.10.1.1
  - ¿Por qué, a pesar de que ARP tiene una entrada para el destino, ping sigue sin funcionar?

Poisoning de ARP

- Ahora borra las entradas creadas para 10.10.1.1 y la entrada de pc2 en la caché ARP y comprueba que lo has hecho correctamente
- Después añade una entrada para 10.10.1.1 asociándola a la dirección MAC de pc2 (observa que pc2 no tiene la dirección 10.10.1.1)
- Ahora haz ping a 10.10.1.1 desde pc1
  - ¿Qué ocurre? ¿Por qué? Justifica las respuestas

Reflexionando sobre las capturas

- Repasa ahora las capturas en pc1 y pc2 de las operaciones anteriores
- ¿Localizas los paquetes arp y ping de cada uno de las actividades anteriores?
  - Justifica las conclusiones a las que llegas con pantallas de las capturas de tus justificaciones
- ¿Cuántos datagramas intervienen en la resolución ARP?
  - Describe la secuencia de tramas involucradas en la resolución justificando todas las direcciones MAC e IP que intervienen en el proceso
  - ¿Qué tipo de paquetes identifican los envíos ping? ¿Y las resoluciones ARP?
- Habrás observado que al hacer un ping a una dirección real, pero desconocida por ARP se ejecuta automáticamente una resolución ARP y se da de alta en su caché
  - Cuando ejecutas el ping de nuevo inmediatamente después, podrás notar que no se hace una nueva resolución
  - ¿Por qué a pesar de hacer lo mismo no se ejecuta la resolución ARP?

Para investigar

- Repite la práctica utilizando pc1 y pc2 como máquinas GNU/Linux virtualizadas sobre VirtualBox
- Localiza las diferencias, si las hay, entre Windows y Linux al utilizar los comandos ping y arp

Para entregar

- Una vez finalizada la práctica deberás entregar:
  - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
  - Las pantallas más significativas que demuestren la ejecución
  - Las respuestas documentadas a todas las cuestiones que se plantean en la ejecución de la práctica
- Nomenclatura identificativa de práctica:
  - **PARP403-PingARP**