Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

IIC2333 — Sistemas Operativos y Redes — 1' 2021

Tarea 4

Caso 1: Servidor UDP

- El filtro aplicado es: *udp and ip.dst* == 255.255.255.255.
- El tamaño del paquete completo es de 75 bytes. De estos, 8 corresponden al header del protocolo UDP (capa de Transporte). La diferencia entre el tamaño total del paquete y el usado por el protocolo UDP se debe a que en el paquete se incluyen también los headers que son utilizados por las capas de Aplicación, Presentación, Sesión, Red y Enlace (36 bytes), aparte de los datos del mensaje en sí (31 bytes).
- El largo del mensaje emitido por el servidor es de 31 bytes. El mensaje es: *Mi numero de la suerte es: 58*.
- Se adjunta un archivo en la entrega que evidencia el mensaje UDP recibido (*server_PDU.pcapng*).

```
0000  00 04 00 01 00 06 08 00  27 f0 43 a7 00 00 08 00   ........ '·C·····
0010  45 00 00 3b 20 e7 40 00  40 11 0d bd 0a 00 02 0f   E··; ·@· @·......
0020  ff ff ff ff be dc 22 b8  00 27 0c 47 4d 69 20 6e   ......"· ·'·GMi n
0030  75 6d 65 72 6f 20 64 65  20 6c 61 20 73 75 65 72   umero de  la suer
0040  74 65 20 65 73 3a 20 35  38 20 0a                  te es: 5 8 ·
```

Figura 1: Captura de mensajes UDP

Caso 2: Conexión a SIDING

- La IP de la plataforma es 146.155.4.17.
- El filtro aplicado es: *ip.addr* == 146.155.4.17.
- Se envían paquetes del protocolo TCP de tipo [SYN] y [ACK]. Estos efectúan el *handshake* entre nuestro computador y el servidor del SIDING según el protocolo TCP, de forma que se pueda abrir la conexión y garantizar que la información intercambiada no se perderá de ninguna forma.
- Estos paquetes permiten que el servidor sepa si el usuario se ha desconectado, así como también intentar preservar la conexión. Se envían de forma periódica para verificar el estado del enlace entre el cliente y el servidor.
- RST es un flag que usa el protocolo TCP para reiniciar la conexión al detectar paquetes entrantes en un puerto no válido (por ejemplo, en un socket ya cerrado). Cuando se recibe uno y se desea reanudar la conexión, se vuelven a enviar los paquetes iniciales para realizar el *handshake* nuevamente. Estos paquetes de reset se pueden analizar con el filtro siguiente:

  ip.addr == 146.155.4.17 *and tcp.flags.reset* == 1.
- TLS (Transport Layer Security) es un protocolo criptográfico enfocado en establecer una conexión segura a través de la red (seguridad enfocada al área de privacidad y protección de los datos).

  El *handshake* de este protocolo tiene los siguientes pasos:

  1. El cliente envía un mensaje *ClientHello* que especifica un conjunto de cifrados y bytes aleatorios.
  2. El servidor responde con un mensaje *ServerHello*, que selecciona los parámetros de la conexión según lo enviado por el cliente anteriormente.
  3. Se intercambian certificados de seguridad.
  4. Se negocia una clave secreta común, la que se pasa por una función que utiliza los bytes aleatorios enviados en el primer paso.

  El uso de un protocolo de este tipo en una plataforma como SIDING es necesario para garantizar que los datos que se intercambiarán entre el servidor y un alumno estén protegidos y se dificulte la aparición de un intermediario que modifique o robe la información.

Caso 3: Red Local y Diagnóstico de Red

- Nuestras IPs públicas son 201.189.92.80 y 45.239.121.202. Ejecutando el comando *traceroute* desde la primera hacia la segunda, se obtiene el siguiente output:

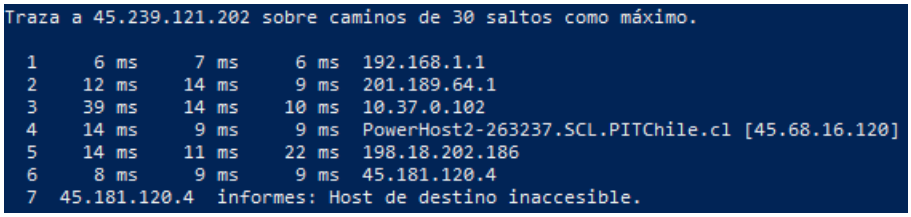

Figura 2: Output de traceroute

Al revisar los paquetes que son capturados por Wireshark, se puede ver que aparecen muchos del protocolo ICMP. Este test consiste en enviar paquetes para chequear el ping con cada uno de los dispositivos que se encuentran en el camino entre ambas IPs, buscando trazar la ruta que toman los paquetes hasta llegar a la dirección IP de destino (o hasta que no puedan acceder a alguna red). En este caso se logró llegar hasta la IP 45.181.120.4 y no se pudo seguir avanzando.

- Se adjunta un archivo en la entrega que evidencia la aparición de los paquetes ICMP (*traceroute.pcapng*).
- El protocolo ICMP se usa para el envío de mensajes de diagnóstico o errores. En general, las aplicaciones no mandan este tipo de paquetes, sino que se suelen utilizar cuando un paquete no puede encontrar al destinatario, algún host o servicio no está disponible, o bien, se desea realizar un diagnóstico de la red.
- El protocolo ARP se usa para que un dispositivo dentro de una red pueda conocer la dirección MAC de otro dispositivo conectado a la misma red, dado que ya conoce su IP.
- Se realizó la conexión por navegador a la dirección 192.168.0.1. En Wireshark se aplicó el filtro dhcp para obtener sólo los mensajes de este protocolo. Al ingresar al sitio se capturan 2 mensajes correspondientes a este protocolo, lo que indica que DHCP está activado.
- Se adjunta un archivo en la entrega que evidencia la aparición de los paquetes DHCP (*dhcp.pcapng*).
- Al ejecutar *nslookup* hacia la IP de SIDING se obtienen paquetes UDP y DNS en Wireshark. Esto ocurre debido a que el test se realiza enviando una request al servidor DNS asociado para poder obtener la IP asociada a un dominio, o bien, el dominio asociado a una IP. En este caso se obtiene el dominio del SIDING a partir de su IP. Estos paquetes suelen enviarse en UDP, razón por lo que se capturaron paquetes tanto UDP como DNS en el programa.