Tarea 4

IIC2333 - Sistemas Operativos y Redes

Francisco Guíñez y Pedro Rioja

Caso 1: Servidor UDP

- Cree un filtro de forma que solo se capturen paquetes cuya IP de destino sea 255.255.255.255 y que el protocolo sea UDP. ¿Cuál es este filtro?
  - **Respuesta:** `udp && ip.dst == 255.255.255.255`
- ¿Cuál es el tamaño en bytes del paquete completo? ¿Cuántos de estos corresponden a UDP? ¿A qué se debe esta diferencia?
  - **Respuesta:** El tamaño del paquete completo es **74 bytes**, de los cuales **8 bytes corresponden a UDP**. Esta diferencia se debe a que los paquetes deben incluir más información aparte de UDP, en este caso tenemos 14 bytes para Ethernet, 20 bytes para IPv4 y 32 bytes para data.
- ¿Cuál es el mensaje que emite el servidor? ¿Cuál es su largo en bytes en el paquete?
  - **Respuesta:** El mensaje que emite es `Mi numero de la suerte es: 780` con un largo de **32 bytes**. *Nota: El número de alumno sin dígito verificador ingresado fue **1664113** correspondiente a Francisco Guíñez.*

Caso 2: Conexión a SIDING

- ¿Cuál es esta IP?
  - **Respuesta:** 146.155.4.17
- Crear un filtro en Wireshark, de forma que solo se capturen paquetes cuyo origen o destino es la IP de la plataforma SIDING. ¿Cuál es este filtro?
  - **Respuesta:** `ip.addr == 146.155.4.17`
- Con el filtro activado y el visor de paquetes capturados vacío, realizar la conexión a la plataforma SIDING a través de su navegador web de preferencia. Debiesen aparecer aproximadamente 6 paquetes capturados al inicio de la conexión. ¿Qué es lo que está ocurriendo? ¿A qué corresponden estos paquetes?

- **Respuesta:** Lo que está ocurriendo es que se está estableciendo la conexión con el servidor por medio de un TCP *handshake* protegido con TLS. Entonces, los paquetes corresponden al proceso mencionado con el siguiente detalle:
    a. TCP - Un paquete `SYN` desde el cliente al servidor
    b. TCP - Un paquete `SYN, ACK` del servidor al cliente
    c. TCP - Un paquete `ACK` del cliente al servidor
    d. TLS - Un paquete `Client Hello` del cliente al servidor
    e. TLS - Un paquete `Server Hello` con el certificado desde el servidor al cliente
    f. TLS - Un paquete del cliente al servidor con un mensaje de protocolo de enlace ya cifrado

- Si espera unos momentos sin hacer nada en su navegador comenzará a recibir paquetes de tipo TCP Keepalive. ¿Qué significan estos paquetes? ¿Por qué se envían?

    - **Respuesta:** Son paquetes sin datos con el flag `ACK` activado, el recibirlos significa que la conexión con el servidor sigue funcionando correctamente. En general, estos paquetes se envían por 2 razones:
        a. Saber si la conexión sigue funcionando
        b. Evitar una desconexión por inactividad

    Fuente: The Linux Document Project

- Al navegar por la plataforma, observarán que Wireshark detecta paquetes del protocolo TCP de tipo RST. ¿A qué se deben estos paquetes? ¿Qué está ocurriendo? Creen un filtro de Wireshark de forma que solo muestre estos paquetes. ¿Cuál es este filtro?

    - **Respuesta:** Estos paquetes se deben a que ha habido un problema en la comunicación, por lo que se necesita RST para volver a intenter la obtención de información. Por lo tanto, dado que todos los paquetes de este tipo se envían del cliente al servidor, lo que está ocurriendo es que nosotros como cliente estamos haciendo un nuevo intento por conseguir información faltante para obtener la información de la página solicitada. Para visualizar estos paquetes debemos usar el filtro `tcp.flags.reset == 1` . Opcionalmente, si queremos asegurarnos de que los paquetes mostrados corresponden explusivamente a SIDING, podemos usar el filtro `ip.addr == 146.155.4.17 && tcp.flags.reset == 1`

- Expliquen qué es el protocolo TLS y para qué se usa. Describan además el

Handshake Protocol de TLS. ¿Tiene sentido que aparezcan paquetes de este protocolo al conectarse a la plataforma SIDING? ¿Por qué?

- **Respuesta:** El *Transport Layer Security* (TLS) es un protocolo que se encarga de que la comunicación sea segura por medio de la criptografía. Se utiliza ampliamente en las comunicaciones por internet, para por ejemplo la mensajería electrónica, servicios que requieren inicio de sesión, navegación web en general, incluso ha sido utilizado para crear servicios VPN. El *Handshake Protocol* de TLS ocurre justo después de establecida la conexión (comunmente por medio de TCP, como en el caso de Siding) y resumidamente consiste en que:

  a. Cliente y servidor se saludan, proceso en el cual ambos aportan una serie de números pseudo-aleatorios para producir las llaves.
  b. Luego, el servidor envía un certificado al cliente, con esta información el cliente confirma la identidad del servidor
  c. El cliente procede a enviar el *premaster secret* con un último grupo de números pseudo-aleatorios, el cual se encripta con la llave pública del servidor por lo que solo puede ser leído por él.
  d. Con los números pseudo-aleatorios generados, cliente y servidor generan las llaves de sesión.
  e. Se envían mutuamente mensajes *Finished* ya encriptados con la llave de sesión.

  Una vez hecho esto el servidor ofrece un certificado que el cliente debe verificar. Posteriormente, cuando esa verificación se ha llevado a cabo, se genera una sesión. Se crea una clave a través de la cual se intercambian datos a través de esa sesión.

  Por todo lo dicho anteriormente, *si tiene sentido* que aparezcan paquetes de este protocolo al conectarse a la plataforma, porque permite cifrar las comunicaciones entre los estudiantes y SIDING desde el comienzo, permitiendo comunicaciones seguras.

Caso 3: Red Local y Diagnóstico de Red

- Determinen las IPs públicas de sus redes locales. En consola ejecuten un test traceroute desde uno de sus equipos a la IP pública del compañero. Observen lo que ocurre en Wireshark. ¿Qué está pasando? ¿En qué consiste este test?

  - **Respuesta:** Lo que está ocurriendo es que se están intentando enviar una

serie de paquetes ICMP de un computador a otro, con los cuales traceroute nos muestra los saltos que hay que dar para comunicar a los dos equipos. Sin embargo en el octavo salto podemos notar que se deja de obtener respuesta, lo que implica que realmente unos de los pasos intermedios está bloqueando la comunicación y no se llega realmente a la IP de destino. Esto muy seguramente ocurre porque el proveedor de internet bloquea el intento de comunicación por seguridad.

El test consiste en enviar una serie de paquetes ICMP a una dirección de destino, donde el primer paquete tiene un valor de *Time To Live* (TTL) igual a 1, y se aumenta en 1 este valor en cada nuevo paquete. Cada vez que se excede el TTL obtenemos la IP del salto en el que se encontraba, por lo que en la práctica esto nos muestra el recorrido de un paquete a traves de diferentes IPs hasta llegar a su destino. En nuestro caso, el *output* fue el siguiente:

```
traceroute to 190.161.68.43 (190.161.68.43), 64 hops max, 52 byte packet
 1  192.168.1.254 (192.168.1.254)  26.920 ms  2.904 ms  2.734 ms
 2  * * *
 3  192.168.4.53 (192.168.4.53)  16.927 ms  14.341 ms  15.598 ms
 4  192.168.4.54 (192.168.4.54)  17.051 ms  16.131 ms  15.701 ms
 5  190.196.124.212 (190.196.124.212)  19.007 ms  16.015 ms  15.914 ms
 6  192.168.99.30 (192.168.99.30)  17.253 ms  18.677 ms  16.859 ms
 7  192.168.15.130 (192.168.15.130)  22.796 ms  21.470 ms  22.695 ms
 8  192.168.15.58 (192.168.15.58)  22.616 ms  23.686 ms  23.944 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
...
```

- **Nota:** Se adjunta el archivo `traceroute.pcapng` que contiene los paquetes capturados en el punto anterior. Nuestras IPs públicas son `201.186.130.212` (Francisco Guíñez) y `190.161.68.43` (Pedro Rioja), el test fue realizado desde el primer equipo hacia el segundo con el comando `traceroute 190.161.68.43` . Para facilitar la visualización de los paquetes de interés, se le puede aplicar el filtro `icmp` , por ejemplo.
- Describan qué es el protocolo ICMP y para qué se usa generalmente.
  - **Respuesta:** Es un protocolo que forma parte de la Capa de Red y está orientado a realizar controles y diagnósticos del funcionamiento de la

capa. Por lo mismo, es utlizado generalmente para conocer si existen errores al intentar comunicarse con un servidor, o directamente identificar si el servidor buscado existe o no. Todos los mensajes ICMP continen un tipo y un código, las diferentes combinaciones de estos dos parámetros nos permiten describir mejor el ICMP que estamos recibiendo.

- Si no utilizan ningún filtro, cada cierto tiempo van a recibir un paquete de protocolo ARP. ¿Cuál es la finalidad de este protocolo?
  - **Respuesta:** El protocolo ARP trabaja a nivel de Capa de Enlace y sirve para obtener la dirección MAC que en ese momento está relacionada a una IP en particular. Dada esta finalidad, se reciben paquetes de este tipo constantemente para mantener actualizadas las relaciones entre direcciones IP y direcciones físicas.
- Indiquen utilizando Wireshark si el servicio DHCP está habilitado en sus redes locales. Esto lo pueden comprobar observando lo que ocurre en Wireshark cuando se conectan a sus redes locales. Describan lo que realizaron para llegar a su respuesta.
  - **Respuesta:** El servicio DHCP **si está habilitado** en la red local. Para llegar a esta respuesta pusimos Wireshare a capturar paquetes con la el equipo sin conexión a internet, luego lo conectamos a una red Wi-Fi. Al realizar este proceso podemos ver que los primeros paquetes capturados corresponden a la conexión a la red local, entre estos paquetes podemos usar el filtro `dhcp` para ver el proceso de asignación de IP. Se destaca la recepción de un paquete *DHCP Acknowledge*, que nos avisa que la información fue recibida correctamente.
- En consola ejecuten un test nslookup hacia la IP de la plataforma SIDING. ¿Qué está ocurriendo? ¿Qué objetivo tiene este test?

  - **Respuesta:** Al ejecutar el comando `nslookup 146.155.4.17` , podemos ver en Wireshark que lo que está ocurriendo es que aparecen 2 paquetes DNS que relacionan la IP entregada con el nombre intrawww.ing.puc.cl.

    El objetivo de este test es corroborar que efectivamente el DNS está relacionando correctamente nombres e IPs. Es más, nos permite también realizar el ejercicio inverso a lo solicitado, el comando `nslookup intrawww.ing.puc.cl` nos entregará la IP 146.155.4.17.