



## Tarea 3

### Caso 1

*i)* Se logró ejecutar el servidor.

*ii)* El filtro para buscar paquetes UDP cuyo destino es 255.255.255.255 es:

```
ip.dst==255.255.255.255 && udp
```

*iii)* El largo del paquete es 74B y UDP 8B (+ 32B de data). El motivo de la diferencia es que la comunicación por ethernet mide 14B e internet protocol (IPv4) mide 20B, ambos necesarios para establecer la conexión a nivel de otras capas.

*iv)* El mensaje enviado es "Mi numero de la suerte es 143 \n" y su largo son 32B.

*v)* El archivo se adjunta dentro del .zip.

### Caso 2

*i)* La IP del SIDING es 146.155.4.17

*ii)* El filtro para buscar paquetes en los que el SIDING es destino u origen es:

```
ip.addr==146.155.4.17
```

*iii)*

*iv)* Los paquetes TCP Keepalive son paquetes que permiten verificar si la conexión sigue activa. Esto para lograr 2 objetivos: tomar las acciones correspondientes si un peer se desconecta (liberar un socket por ejemplo) y mantener activa la conexión para que un peer no se desconecte por inactividad.

*v)* Los paquetes con el flag RST seteado en 1 sirven para indicar que la conexión debe ser reiniciada. En general se utiliza para terminar abruptamente una conexión porque se recibió un paquete que no corresponde, es decir, avisarle al otro que debe reiniciar porque algo salió mal. Por ejemplo, puede que desde el SIDING se haya liberado el puerto que escuchaba a un alumno y, al intentar conectarse tiempo después, SIDING envía un RST para que el alumno reinicie y encuentre un puerto correcto. El filtro para buscar paquetes en los que el SIDING es destino u origen que contengan el flag RST es:

```
ip.addr==146.155.4.17 && tcp.flags.reset==1
```

*vi)* El protocolo TLS se usa en el layer de seguridad de HTTPS. Se usa para seguridad e integridad de los datos, las 2 partes intercambian los parámetros de seguridad necesarios para establecer una comunicación que no puede descifrada por terceros que estén escuchando maliciosamente.

Un resumen del funcionamiento del Handshake es:

Cliente: hola (con Vers. Num., Rand. Generated Data, Sess. Id, Cipher Suite y Compression Algorithm)

Server: hola (envía mismos tipos de datos desde el servidor)

\*envía certificado\* (cliente revisa, lo usa para encriptar el “premaster secret”)

\*fin hola\*

Cliente: \*envía “Client Key Exchange”, 2 números aleatorios encriptados con el secreto\*

\*envía mensaje que notifica que los mensajes futuros serán encriptados\*

\*envía toda la conversación encriptada\*

Server: \*envía mensaje de que los mensajes futuros serán encriptados\*

\*envía toda la conversación encriptada\*

Finalmente, si el cliente logra descryptar lo enviado por el servidor, entonces la comunicación es segura.

Tiene sentido que haya al conectarse al SIDING porque la página usa HTTPS.

Fuente: Microsoft Docs

## Caso 3

*i)* Desde el computador que se ejecuta traceroute se envían y se reciben múltiples paquetes del protocolo ICMP. Este test consiste en comprobar si una IP pertenece a la red y, además, ver a través de que host se routea el mensaje para llegar al destino, es decir, traza una ruta.

*ii)* El archivo se adjunta dentro del .zip.

*iii)* El protocolo ICMP (Internet Control Message Protocol) se usa en las comunicaciones que se ejecutan a través de IP para enviar mensajes de éxito o fallo. Es utilizado por la capa de red. Se utiliza generalmente para diagnosticar la res, por ejemplo, mediante herramientas como ping y traceroute. ICMP se manda encapsulado en un paquete de IPv4:

Header: se informa que se trata de ICMP.;

Type: Tipo de ICMP;

Code: Subtipo de ICMP;

Checksum;

Resto del header (depende del tipo de ICMP y subtipo;

Data;

Fuente: Wikipedia

*iv)* El protocolo ARP (Address Resolution Protocol) sirve para descubrir direcciones a nivel de la Capa de Enlace, por ejemplo, una dirección MAC conectada a la red y su respectiva dirección IPv4. En otras

