Práctica 5

Capa de Transporte - Parte I

1. ¿Cuál es la función de la capa de transporte?
2. Describa la estructura del segmento TCP y UDP.
3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?
4. Compare TCP y UDP en cuanto a:
    a. Confiabilidad.
    b. Multiplexación.
    c. Orientado a la conexión.
    d. Controles de congestión.
    e. Utilización de puertos.
    f. ¿Cuál es el campo del datagrama IP y los valores que se utilizan en este para diferenciar que se transporta TCP o UDP? (Ayuda: buscar en /etc/protocols y contrastarlo con una captura de tráfico).
5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el término datagrama. Indique cuando.
6. Describa el saludo de tres vías de TCP.
7. Investigue qué es el ISN (Initial Sequence Number). Relaciónelo con el saludo de tres vías.
8. Investigue qué es el MSS. ¿Cuándo y cómo se negocia?
9. Utilice el comando **ss** (reemplazo de netstat) para obtener la siguiente información de su PC:
    a. Para listar las comunicaciones TCP establecidas.
    b. Para listar las comunicaciones UDP establecidas.
    c. Obtener sólo los servicios TCP que están esperando comunicaciones
    d. Obtener sólo los servicios UDP que están esperando comunicaciones.
    e. Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión.
    f. Obtenga la misma información planteada en los items anteriores usando el comando **netstat**.
10. ¿Qué sucede si llega un segmento TCP con el flag SYN activo a un host que no tiene ningún proceso esperando en el puerto destino de dicho segmento (es decir, que dicho puerto no está en estado LISTEN)?
    a. Utilice **hping3** para enviar paquetes TCP al puerto destino 22 de la máquina virtual con el flag SYN activado.

b. Utilice **hping3** para enviar paquetes TCP al puerto destino 40 de la máquina virtual con el flag SYN activado.
c. ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores? ¿Puede explicar a qué se debe? (Ayuda: utilice el comando ss visto anteriormente).

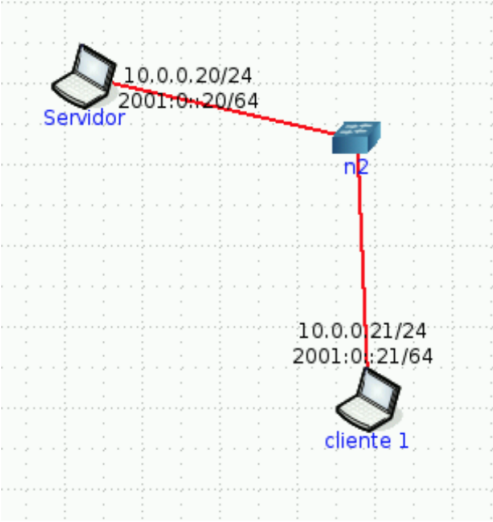
11. ¿Qué sucede si llega un datagrama UDP a un host que no tiene a ningún proceso esperando en el puerto destino de dicho datagrama (es decir, que dicho puerto no está en estado LISTEN)?

    a. Utilice **hping3** para enviar datagramas UDP al puerto destino 68 de la máquina virtual.
    b. Utilice **hping3** para enviar datagramas UDP al puerto destino 40 de la máquina virtual.
    c. ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores? ¿Puede explicar a qué se debe? (Ayuda: utilice el comando ss visto anteriormente).

12. Investigue los distintos tipos de estado que puede tener una conexión TCP.
    (Ver la página: https://thewalnut.io/app/release/73/#time=21)

13. Use CORE para armar una topología como la siguiente, sobre la cual deberá realizar:

    a. En ambos equipos inspeccionar el estado de las conexiones y mantener abiertas ambas ventanas con el comando corriendo para poder visualizar los cambios a medida que se realiza el ejercicio. Ayuda: watch -n1 'ss -nat'.
    b. En Servidor, utilice la herramienta **ncat** para levantar un servicio que escuche en el puerto 8001/TCP. Utilice la opcion -k para que el servicio sea persistente. Verifique el estado de las conexiones.



    c. Desde CLIENTE1 conectarse a dicho servicio utilizando también la herramienta ncat. Inspeccione el estado de las conexiones.
    d. Iniciar otra conexión desde CLIENTE1 de la misma manera que la anterior y verificar el estado de las conexiones. ¿De qué manera puede identificar cada conexión?

e. En base a lo observado en el item anterior, ¿es posible iniciar más de una conexión desde el cliente al servidor en el mismo puerto destino? ¿Por qué? ¿Cómo se garantiza que los datos de una conexión no se mezclarán con los de la otra?

f. Analice en el tráfico de red, los flags de los segmentos TCP que ocurren cuando:

i. Cierra la última conexión establecida desde CLIENTE1. Evalúe los estados de las conexiones en ambos equipos.

ii. Corta el servicio de ncat en el servidor (Ctrl+C). Evalúe los estados de las conexiones en ambos equipos.

iii. Cierra la conexión en el cliente. Evalúe nuevamente los estados de las conexiones.

14. Dada la siguiente salida del comando ss, responda:

```
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
tcp    LISTEN     0      128                *:22                    *:*      users:(("sshd",pid=468,fd=29))
tcp    LISTEN     0      128                *:80                    *:*      users:(("apache2",pid=991,fd=95))
udp    LISTEN     0      128       163.10.5.222:53                  *:*      users:(("named",pid=452,fd=10))
tcp    ESTAB      0      0         163.10.5.222:59736    64.233.163.120:443    users:(("x-www-browser",pid=1079,fd=51))
tcp    CLOSE-WAIT 0      0         163.10.5.222:41654     200.115.89.30:443    users:(("x-www-browser",pid=1079,fd=50))
tcp    ESTAB      0      0         163.10.5.222:59737    64.233.163.120:443    users:(("x-www-browser",pid=1079,fd=55))
tcp    ESTAB      0      0         163.10.5.222:33583     200.115.89.15:443    users:(("x-www-browser",pid=1079,fd=53))
tcp    ESTAB      0      0         163.10.5.222:45293     64.233.190.99:443    users:(("x-www-browser",pid=1079,fd=59))
tcp    LISTEN     0      128                *:25                    *:*      users:(("postfix",pid=627,fd=3))
tcp    ESTAB      0      0            127.0.0.1:22            127.0.0.1:41220  users:(("sshd",pid=1418,fd=3),
                                                                                       ("sshd",pid=1416,fd=3))
tcp    ESTAB      0      0         163.10.5.222:52952     64.233.190.94:443    users:(("x-www-browser",pid=1079,fd=29))
tcp    TIME-WAIT  0      0         163.10.5.222:36676     54.149.207.17:443    users:(("x-www-browser",pid=1079,fd=3))
tcp    ESTAB      0      0         163.10.5.222:52960     64.233.190.94:443    users:(("x-www-browser",pid=1079,fd=67))
tcp    ESTAB      0      0         163.10.5.222:50521     200.115.89.57:443    users:(("x-www-browser",pid=1079,fd=69))
tcp    SYN-SENT   0      0         163.10.5.222:52132        43.232.2.2:9500   users:(("x-www-browser",pid=1079,fd=70))
tcp    ESTAB      0      0            127.0.0.1:41220         127.0.0.1:22     users:(("ssh",pid=1415,fd=3))
udp    LISTEN     0      128          127.0.0.1:53                    *:*      users:(("named",pid=452,fd=9))
```

a. ¿Cuántas conexiones hay establecidas?

b. ¿Cuántos puertos hay abiertos a la espera de posibles nuevas conexiones?

c. El cliente y el servidor de las comunicaciones HTTPS (puerto 443), ¿residen en la misma máquina?

d. El cliente y el servidor de la comunicación SSH (puerto 22), ¿residen en la misma máquina?

e. Liste los nombres de todos los procesos asociados con cada comunicación. Indique para cada uno si se trata de un proceso cliente o uno servidor.

f. ¿Cuáles conexiones tuvieron el cierre iniciado por el host local y cuáles por el remoto?

g. ¿Cuántas conexiones están aún pendientes por establecerse?

15. Dadas las salidas de los siguientes comandos ejecutados en el cliente y el servidor, responder:

```
servidor# ss -natu | grep 110
tcp    LISTEN     0     0             *:110              *:*
tcp    SYN-RECV   0     0     157.0.0.1:110     157.0.11.1:52843

cliente# ss -natu | grep 110
tcp    SYN-SENT   0     1    157.0.11.1:52843    157.0.0.1:110
```

a. ¿Qué segmentos llegaron y cuáles se están perdiendo en la red?

b. ¿A qué protocolo de capa de aplicación y de transporte se está intentando conectar el cliente?

c. ¿Qué flags tendría seteado el segmento perdido?