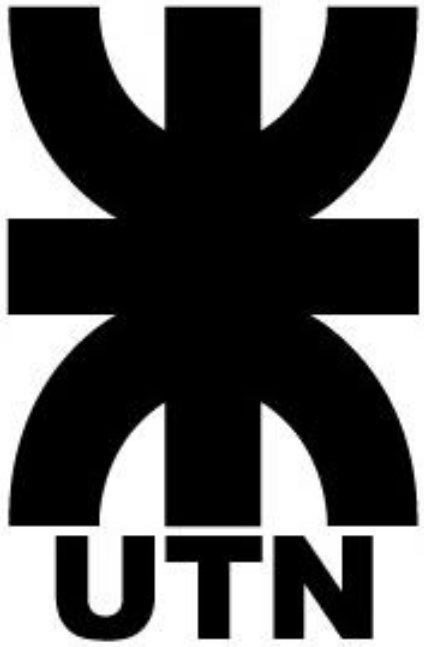
Universidad Tecnológica Nacional



Facultad Regional Delta

Laboratorio de redes de información

2024

Trabajo Práctico N°4| Capa de Transporte

Alumno: Gonzalez, Tomas

Profesor: Carrizo Carlos

Contenido

No se encontraron entradas de tabla de contenido.

Consignas

Temas: TCP/UDP, DNS, TELNET.

Herramientas a utilizar: PC con Windows, aplicación Wireshark

1) Desde una PC con Windows:

· Abra la aplicación Wireshark e inicie el monitoreo sobre la placa de red con el modo promiscuo desactivado.

· Investigue y utilice el comando telnet para verificar si el servidor web que hostea la facultad tiene abierto el puerto 80 o 443.

· Una vez ejecutada la verificación detenga el monitoreo de Wireshark.

a) Busque en Wireshark los paquetes de inicio de conexión TCP. Documéntelos.

b) Determine el puerto origen y destino de la conexión. Documéntelo.

c) Seleccione el primer paquete de conexión TCP y haga un seguimiento del Stream TCP. Para tal efecto seleccione el paquete, haga click al botón derecho y seleccione la opción “Follow - TCP Stream”.

Analice y comente la salida visualizada.

Si el transporte utilizado por el servicio es UDP, ¿cómo puedo verificar de forma remota si el puerto está abierto?

Resolución

En esta práctica, se utilizará el comando TELNET para conocer el estado de los puertos. Mediante el comando TELNET (que se utiliza para la conexión remota), con el cual se intentara realizar la conexión con los distintos servicios, cabe aclarar que con el comando solo podremos iniciar una sesión (en caso de que el puerto este abierto), pero no podremos intercambiar información con el servicio corriendo en ese puerto (ya que TELNET no podría enviar datos, por ejemplo, al puerto 25 que es de SMTP)
Luego de esta introducción, se procede a iniciar la captura con la aplicación Wireshark.
En la CMD de Windows se ingresa el comando

```
C:\Users\Tomi>telnet 200.80.60.166 80
```

Donde la dirección 200.80.60.166 es la dirección IP del servidor web que hostea la facultad y 80 es el puerto que estamos probando para saber si esta abierto o cerrado. En Wireshark obtenemos:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	255.255.255.255	UDP	246	59727 → 6667 Len=204
2	5.019023	192.168.1.4	255.255.255.255	UDP	246	59727 → 6667 Len=204
3	6.146335	192.168.1.12	200.80.60.166	TCP	66	56791 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	6.165528	200.80.60.166	192.168.1.12	TCP	66	80 → 56791 [SYN, ACK] Seq=0 Ack=1 Win=32430 Len=0 MSS=1410 SACK_PERM=1 WS=128
5	6.165671	192.168.1.12	200.80.60.166	TCP	54	56791 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
6	7.213606	2803:9800:90b4:8405…	2603:1056:1400:1::1	TLSv1.2	109	Application Data
7	7.308626	2603:1056:1400:1::1	2803:9800:90b4:8405…	TCP	74	443 → 54772 [ACK] Seq=1 Ack=36 Win=16382 Len=0
8	10.035174	192.168.1.4	255.255.255.255	UDP	246	59727 → 6667 Len=204
9	11.570116	192.168.1.5	255.255.255.255	UDP	82	9487 → 9478 Len=40

Donde se localizan los 3 paquetes que corresponden al inicio de sesión entre TELNET y el servidor web que hostea la facultad. Como se observa, la conexión fue exitosa, con lo cual quiere decir que existe un servicio asociado a ese puerto corriendo por detrás (al ser el puerto 80, correspondiente a HTTP, quiere decir que están corriendo servicios de comunicación entre recursos webs)

En cuanto al puerto, se observa que se utiliza el puerto 56791 desde el lado del cliente, y, como se menciono antes, el puerto 80 del lado del servidor.

Utilizando la función TCP – Follow Stream

```
qHTTP/1.1 400 Bad Request
Date: Mon, 08 Jul 2024 02:42:36 GMT
Content-Type: text/html
Content-Length: 150
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

En la captura se observa, que como TELNET no es un cliente HTPP, la comunicación esta está establecida, pero al momento de intentar enviar datos, se observan error de “bad request”, ya que el servidor HTTP no puede interpretar los comandos enviados por TELNET, que no es un navegador web.

Por último, respecto a la pregunta
“Si el transporte utilizado por el servicio es UDP, ¿cómo puedo verificar de forma remota si el puerto está abierto?”
Se llego a la conclusión que se puede:

- Utilizar Wireshark para ver si el envió y recepción de paquetes dirigidos hacia el puerto en cuestión es exitosa.
- Utilizar alguna herramienta de escaneo como puede ser **Nmap** (multiplataforma), **Angry IP Scanner** (Windows) o **SoftPerfect ScanIP** (Windows), **Advanced port Scanner**.
  Ejemplo de comando nmap en Windows: nc -v -u -w 1 direccionIP Puerto
  Ejemplo de comando Advanced port Scanner: advancedportscanner.exe -v -udp -a ip_remota puerto_UDP