Informe

Trabajo Práctico TD4

Bacigalupo, Guillermina - Ferrari, Sofia - Milde, Manuel

Ejercicios :

3.1. Ejecutar su **traceroute** trazando las rutas a 5 universidades de diferentes continentes. Responder las siguientes preguntas:

a. ¿Qué porcentaje de hosts intermedios envían mensajes de ttl-zero-during-transit? Investigar y dar posibles razones para este comportamiento.

El mensaje "ttl-zero-during-transit" es un mensaje de error enviado por un router cuando detecta que el valor del TTL (Time To Live) en un paquete IP llegó a cero, esto se utiliza ya que sea setea a dicho campo de los paquetes IP con un número finito para evitar se queden indefinidamente en la red. Por lo que dada la ejecución de nuestro traceroute a las 5 universidades de diferentes continentes vamos a encontrar que el porcentaje de hosts intermedios que envían este mensaje lo calcularemos de la siguiente manera.

- Vamos a recibir este mensaje la cantidad de veces que mandemos un paquete (y recibamos una respuesta). Por lo tanto, si consideramos que por ejemplo el ttl establecido es igual a 30, y encontramos al host destino en el ttl número 21 (y que de todos los paquetes anteriormente recibimos respuesta) vamos a realizar la siguiente cuenta:

  (cantidad de paquetes enviados en los que recibimos el mensaje "ttl-zero-during-transit" / cantidad de paquetes enviado) x 100 = 95,24%

  Notemos además que este es el porcentaje máximo de mensajes de "ttl-zero-during-transit" que podríamos recibir en caso de encontrar al host destino ya que aunque el ttl donde lo encontremos sea menor o mayor a 21 si de todos los anteriores recibimos respuesta siempre vamos a obtener un 95,24%. En el caso de no recibir respuesta de todos los paquetes enviados el porcentaje va a ser menor.

Las razones por las que podríamos no recibir respuesta son múltiples, puede deberse por un lado a la configuración de seguridad de algunos routers, estos suelen tener firewalls que descartan ciertos mensajes ICMP para evitar que la red sea rastreada o para protegerse de ataques. También puede suceder que se esté ejecutando el traceroute a través de una VPN las cuales están compuestas por nodos que no responden a estos mensajes para mantenerse privadas y por razones de seguridad. Sin embargo, la razón más común es simplemente que algunos routers no están configurados para responder a los mensajes ICMP por razones ya sea de rendimiento (ya sea para priorizar el tráfico real o para evitar consumir recursos y la congestión/sobrecargas en la red) como de seguridad (ya que se aplican ciertas políticas para evitar rastreos y ataques como mencionamos anteriormente).

Para el caso particular de la implementación del traceroute en las 5 universidades de diferentes continentes obtuvimos que :

- **Asia : Nanyang Technological University**

  Encontramos que :

  mensajes "ttl-zero-during-transit" recibidos = 9

  paquetes enviados = 10

  Por lo tanto el porcentaje de mensajes es de 95,24%

- **Europa : Cambridge University**

  Encontramos que :

  mensajes "ttl-zero-during-transit" recibidos = 9

  paquetes enviados = 31

  Por lo tanto el porcentaje de mensajes es de 29,03%

- **America : Massachusetts Institute of Technology**

  Encontramos que :

  mensajes "ttl-zero-during-transit" recibidos = 8

  paquetes enviados = 10

  Por lo tanto el porcentaje de mensajes es de 80%

- **Africa : University of Cape Town**

  Encontramos que :

  mensajes "ttl-zero-during-transit" recibidos = 13

  paquetes enviados = 31

  Por lo tanto el porcentaje de mensajes es de 41,93%

- **Oceania : University of Melbourne**

  Encontramos que :

  mensajes "ttl-zero-during-transit" recibidos = 9

  paquetes enviados = 10

Por lo tanto el porcentaje de mensajes es de 95,24%

b. Para cada una de las rutas descubiertas, analizar la diferencia entre los RTT de diferentes saltos (es decir, la diferencia entre los RTT de dos hosts sucesivos en una ruta). ¿Hay algún salto grande entre el RTT de un host de la ruta y el siguiente? ¿A que creen que se puede deber?

Analizando las rutas previamente descubiertas, se puede notar que en cada uno de los casos ocurre un salto grande entre RTT de dos hosts sucesivos. Esto se puede deber a distintos motivos, entre ellos:

- La distancia geográfica entre dos hosts, donde cuanto mayor sea la distancia, mayor será el RTT en consecuencia de la latencia inherente en la transmisión de datos a través de cables o satélites.
- La congestión de la red, donde los paquetes pueden sufrir demoras de tránsito, resultando en valores de RTT altos.
- Los saltos a través de enlaces de menor calidad (ej: conexiones inalámbricas o enlaces de menor capacidad) puede que deriven a altos valores de RTT por la latencia o la pérdida de paquetes.
- Los saltos a través de routers con capacidad limitada de manejo de paquetes, causando delays de procesamiento de los mismos.
- Sobrecarga o alto volumen de tráfico de los servidores de destino, donde los tiempos de respuesta pueden ser más altos.

A pesar de no poder determinar exactamente a qué se deben estos saltos, si observamos con atención, notamos un patrón interesante. La mayoría de las veces, estos picos ocurren después de que se envían varios paquetes sin obtener respuesta. Además, es curioso que las direcciones IP de los hosts en cuestión suelen pertenecer a proveedores de servicios de internet (ISP/MOB), lo que hemos confirmado a través de sitios web como https://es.ipshu.com.

Ahora bien, cuando se trata de los traceroutes que involucran universidades en continentes distintos de América, los picos en los RTT se vuelven más notables y variados. Esto nos lleva a pensar que la distancia geográfica entre los hosts puede estar desempeñando un papel importante. La razón de que los saltos en los tiempos de respuesta sean más notorios en estos casos sugiere que otros factores, como la infraestructura de red global y las rutas de tráfico internacionales, también pueden influir en la variabilidad de los RTT en este contexto. En resumen, aunque no podemos ofrecer una explicación definitiva, estos hallazgos nos indican que la falta de respuesta a paquetes y la geografía de la red son factores que contribuyen a la variabilidad en los tiempos de respuesta en las trazas de ruta.

3.2 Ejecutar ambos **Port Scanners** desarrollados sobre las páginas web de 3 universidades distintas.

- Realizar un análisis estadístico sobre el porcentaje de puertos cerrados, abiertos y filtrados. Para realizar el análisis sugerimos graficar e intentar explicar los resultados obtenidos.
- ¿Encontraron patrones en los estados de los puertos en diferentes servidores? ¿A qué se debe?
- Analizar las diferencias en los resultados de escanear un mismo servidor con los dos diferentes scanners desarrollados.
- **nmap**[2] es una herramienta conocida que permite realizar Port Scanning. Comparar los resultados de escanear servidores usando **nmap** con los del Port Scanner que desarrollaron

Soluciones

a)

Para realizar este análisis, nos basamos en lo especificado por el enunciado del Trabajo Práctico, utilizamos la función -h en nuestro Port Scanner. Como objeto de estudio, se analizaron los primeros mil puertos TCP de los servidores en donde están almacenadas las páginas de las siguientes universidades:

- MIT: Massachusetts Institute of Technology
- UNT: Nanyang Technological University
- UNSa: Universidad Nacional de Salta

De estas se obtuvieron estos resultados

- MIT

  El 99.8% son puertos Filtered, el 0.2% son puertos Open y 0% son puertos Close. Los puertos 80 y 443 estaban abiertos.

- UNT

  El 99.8% son puertos Filtered, el 0.2% son puertos Open y 0% son puertos Close. Los puertos 80 y 443 estaban abiertos.

- UNSa

  El 99.7% son puertos Filtered, el 0.3% son puertos Open y 0% son puertos Close. Los puertos 80, 443 y 22 estaban abiertos.

En el gráfico se puede ver el porcentaje de puertos filtrados (rojo), abiertos (verde) y cerrados (azul).

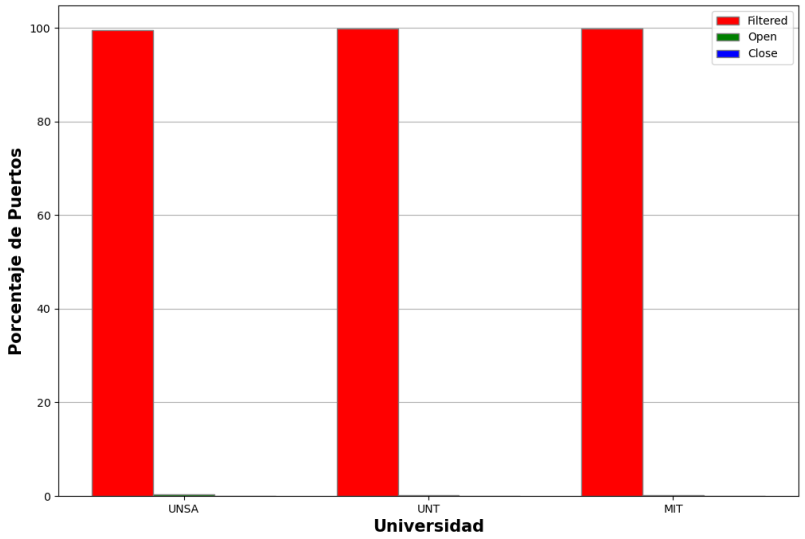
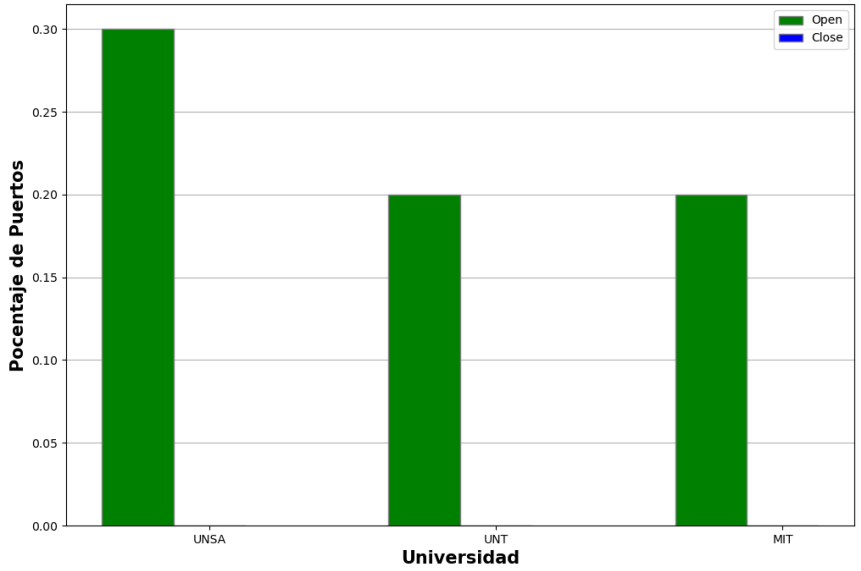


Gráfico con resultados comparados entre universidades



Detalle de los valores Open (apenas visibles en el primer gráfico)

b)

Los patrones que encontramos entre servidores fueron las apariciones de los puertos 80 y 443 en todas las ejecuciones del Port Scanner, utilizados frecuentemente para el uso de protocolos HTTP. La única excepción fue la del puerto 22 (ssh) en el caso de UNSA, debido a esto podemos asumir que la plataforma en línea de esta universidad es vulnerable a inicios de sesión sin autorización por parte de atacantes que busquen información de los usuarios.

c)

Utilizamos el servidor de UTDT como dirección de destino para comparar las funciones de nuestro port scanner.

Las imágenes de abajo muestran los resultados de ambas operaciones tanto con la función con payload (-f), como sin payload (-h).

Usando la función -h

```
Escaneando www.utdt.edu para ver puertos TCP

Puerto 80 OPEN
Puerto 443 OPEN

Escaneo completado

El 99.8% son puertos Filtered y el 0.2% son puertos Open. (CLOSE:0.0%)
```

Usando la función -f (con payload)

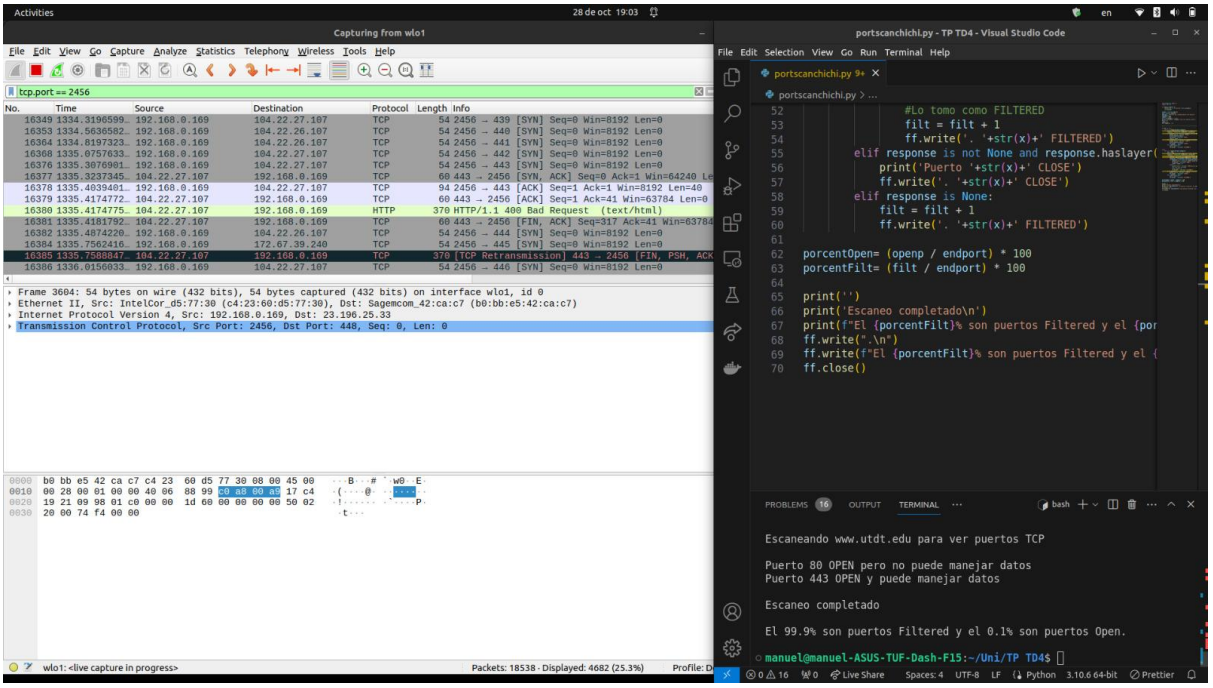
```
Escaneando www.utdt.edu para ver puertos TCP

Puerto 80 OPEN pero no puede manejar datos
Puerto 443 OPEN y puede manejar datos

Escaneo completado

El 99.9% son puertos Filtered y el 0.1% son puertos Open.
```

Mensaje de la consola



Captura de pantalla completa con el detalle de la ejecución de Wireshark para detectar errores.

Teniendo en cuenta que en la ejecución del parámetro -f, el puerto 80 no recibió el payload, podemos concluir que el servidor de UTDT está bien preparado en cuestiones de seguridad, ya que justamente este puerto es más vulnerable a ataques. En cambio el puerto 443, mejor preparado para situaciones complejas, está abierto para establecer una conexión, ya que usa https..

d)

Para comparar nuestro Port Scanner con nmap, utilizamos el servidor de MIT como referencia.

Nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-29 20:27 -03
Nmap scan report for www.mit.edu (23.43.185.92)
Host is up (0.0037s latency).
Other addresses for www.mit.edu (not scanned): 2600:1419:1200:182::255e 2600:1419:1200:186::255e
rDNS record for 23.43.185.92: a23-43-185-92.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.60 seconds
```

Nuestro Port Scanner (-h)

```
Puerto 80 OPEN
Puerto 443 OPEN

Escaneo completado

El 99.8% son puertos Filtered y el 0.2% son puertos Open. (CLOSE:0.0%)
```

En base a las imágenes, podemos sacar las siguientes conclusiones. Las diferencias son notables, podemos obtener mucha más información por medio de nmap, no solamente sobre los puertos sino también la dirección IP del host, el tipo de servicio (http o https) y más detalles.

También vemos que coinciden los puertos escaneados, dándonos a entender que nuestro Port Scanner funciona correctamente ya que tuvimos los mismos resultados.