DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Taller II

Rutas en Internet

13/10/2020 Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Romczyk, Geronimo	143/17	g.romczyk@hotmail.com
Segura Maag, Mariano	235/17	marianosegura90@gmail.com
López, Mauro	055/13	mauro.javier.lopez@gmail.com
Olkies, Ilan	250/17	ilanolkies@gmail.com

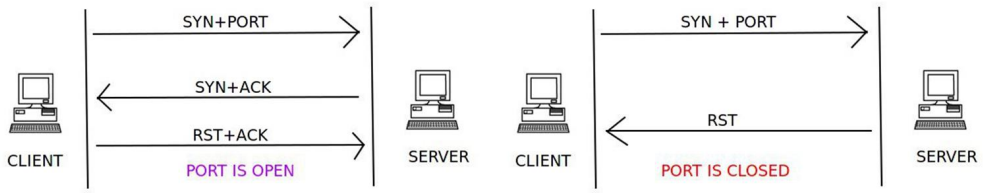
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

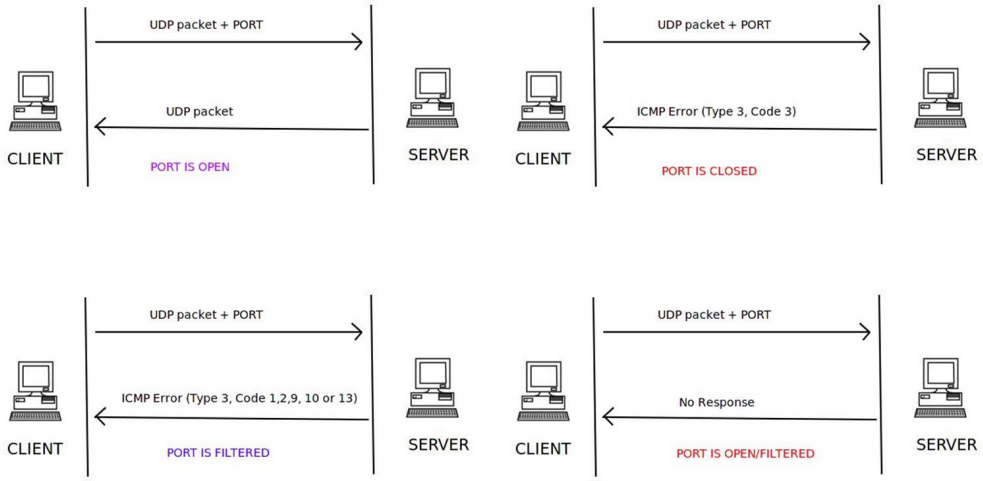
1. Introducción

En este trabajo estudiamos los protoclos a nivel transporte. El objetivo es analizar los puertos de un servidor web para identificar puertos abiertos, cerrados y si están protegidos por un firewall.

Para conectarce a un puerto de un servidor, primero tenemos que enviar un paquete TCP con la flag SYN al número del puerto, si este está abierto el servidor responde con un paquete TCP on las flags SYN+ACK, a las cuales podemos responder estableciendo una conexin con un paquete TCP con las flags ACK+RST. Si el servidor responde con RST significa que el puerto está cerrado, y en el caso que no haya respuesta del servidor, entonces nuestra petición fue bloqueda por un firewall.



A diferencia de TCP, el protocolo UDP es *connectionless*, por lo tanto el envio de paquetes se realiza sin chequear si hay un canal disponible, entonces si envio un paquete UDP a un puerto y recibo otro paquete UDP quiere decir que el puerto esta abierto, si recibo un ICMP con tipo de error 3 código 3 el puerto está cerrado y si el error es de tipo 3 y código 1, 2, 9, 10 o 13 entonces fue filtrado. Observemos que si no hay respuesta no podemos decidir si está abiero o filtrado



2. Métodos y condiciones de los experimentos

2.1. Port Scanning UDP

Definimos un paquete UDP con destino al puerto seleccionado con un $TTL = 10$.

- Si las respuesta es de tipo **none** retransmitimos 3 veces si alguno es de tipo distinto a **none** volvemos a correr el scanner, si la respuesta no cambia entonces el estado puede ser filtrado o abierto.
- Si la respuesta es UDP devolvemos que el puerto está abierto
- Si la respuesta es ICMP nos fijamos el tipo de error y código pare definir si es cerrado o filtrado

2.2. Detalles de experimentación

La experimentacion se realizará sobre 4 universidades

- Universidad de Munich
- Universidad de Auckland
- Universidad de Tokyo
- Universidad de New York

para los puertos del 1 al 1024

2.2.1. Detección de Firewall

Dado un puerto filtrado en un scan por **TCP**, esto puede decir que el puerto tiene un firewall escuchando al puerto, o un router, o un proveedor de internet decide filtrarlo por reglas de fowarding establecidas por estos.

Para detectar con mayor precisión los casos de filtrado por firewall podemos comparar que puertos(UDP) fueron filtrados o están cerrado al enviar paquetes UDP, en el caso de que tanto para **UDP** y **TCP** el paquete haya sido filtrado es probable que haya un firewall escuchando los puertos para algun servicio

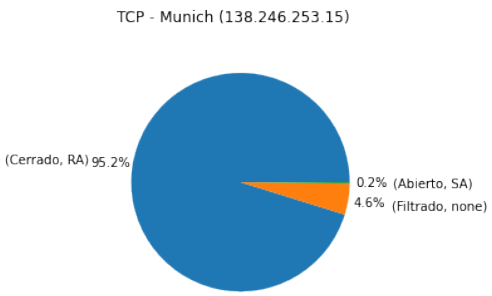
2.2.2. Puertos Comunes

Para extraer información sobre el uso de puertos podemos analizar puertos recurrentes en los request a distintos servidores

3. Resultados de los experimentos

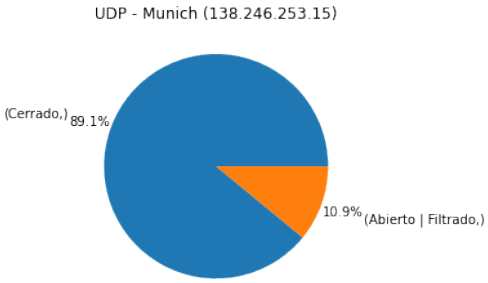
3.1. Universidad De Munich

En primer lugar podemos observar que solo los puerto 53 y 80 se encuentran abiertos. El puerto 53 correponde al servicio de **DNS** y el 80 al **HTTP**



port	TCP	TCPflag
53	Abierto	SA
80	Abierto	SA

También podemos observar que para el protocolo **UDP** el puerto 53 también se encuentra abierto, lo cual nos dice que DNS utiliza tanto TCP como UDP para brindar servicios.



port	UDP	TCP	TCPflag
53	Abierto | Filtrado	Abierto	SA

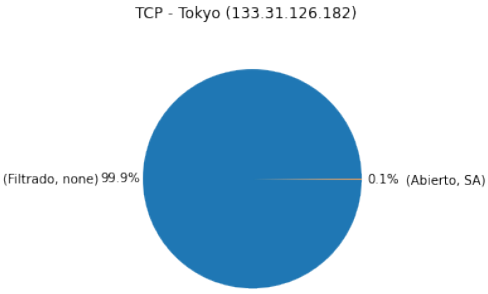
3.1.1. Firewall

Tanto el puerto 46 como 282 se encuentran filtrados para TCP y UDP por lo cual podemos asumir que son escuchados por un firewall

port	TCP	TCPflag	UDP
46	Filtrado	none	Abierto | Filtrado
282	Filtrado	none	Abierto | Filtrado

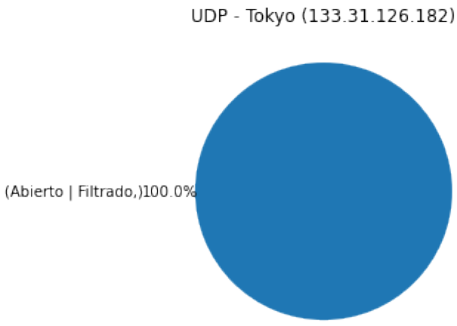
3.2. Universidad De Tokyo

Se puede ver que en el caso de la universidad de Tokyo, el unico puerto TCP abierto es el 53, que se corresponde al servicio **DNS** como mencionamos antes. Cabe destacar que, a diferencia del caso anterior, los puertos restantes no se encontraban cerrados a la hora de realizar el experimento, sino que fueron filtrados por un firewall.



port	TCP	TCPflag
53	Abierto	SA

También podemos observar que para el protocolo **UDP** el puerto 53 también se encuentra abierto, lo mismo que en el caso anterior. Cabe destacar, que para este caso, no pudimos determinar concretamente el estado de ninguno de los puertos UDP, en particular si se encontraban abiertos, o si fueron filtrados a lo largo del camino hasta Tokyo. Esto tiene sentido, ya que el recorrido hasta la Universidad de Tokyo probablemente abarque muchos mas nodos que en el caso anterior.



port	UDP	TCP	TCPflag
53	Abierto | Filtrado	Abierto	SA

3.2.1. Firewall

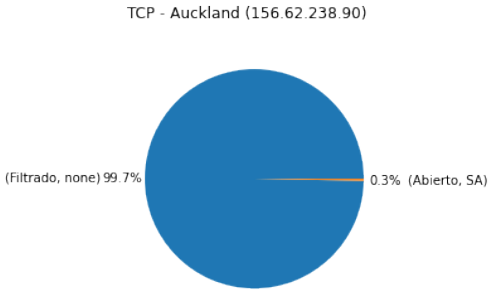
En este caso, para TCP, pudimos determinar que todos los puertos, a excepción del 53, fueron filtrados. Por este motivo, podemos suponer que dichos puertos tambien ueron filtrados para el protocolo UDP. Aqui podemos ver un resumen de la tabla de puertos filtrados.

port	TCP	TCPflag	UDP
1	Filtrado	none	Abierto | Filtrado
2	Filtrado	none	Abierto | Filtrado
3	Filtrado	none	Abierto | Filtrado
4	Filtrado	none	Abierto | Filtrado
5	Filtrado	none	Abierto | Filtrado
...	...	...	...
1020	Filtrado	none	Abierto | Filtrado
1021	Filtrado	none	Abierto | Filtrado
1022	Filtrado	none	Abierto | Filtrado
1023	Filtrado	none	Abierto | Filtrado
1024	Filtrado	none	Abierto | Filtrado

1023 rows × 3 columns

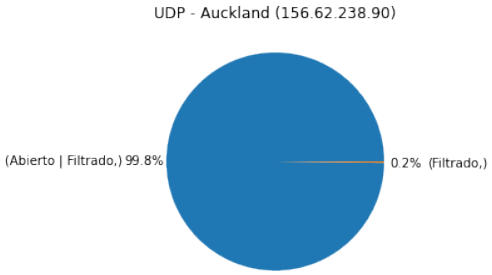
3.3. Universidad De Auckland

En el caso de la Universidad de Auckland, nos encontramos con 3 puertos abiertos para el protocolo TCP, el 53 (**DNS**), el 80 (**HTTP**) y el 443 (**HTTPS**), una version segura de HTTP.



port	TCP	TCPflag
53	Abierto	SA
80	Abierto	SA
443	Abierto	SA

En este caso, pudimos determinar unicamente que los puertos 99 y 303 del protocolo **UDP** fueron filtrados efectivamente, mientras que para los 1022 puertos restantes, no pudimos determinar su estado, ya que pueden haber estado abiertos y haber sido filtrados a lo largo del camino. Por este motivo, asumimos que aquellos puertos abiertos para el protocolo **TCP** se encontraban abiertos para **UDP** también.



port	UDP	TCP	TCPflag
53	Abierto | Filtrado	Abierto	SA
80	Abierto | Filtrado	Abierto	SA
443	Abierto | Filtrado	Abierto	SA

3.3.1. Firewall

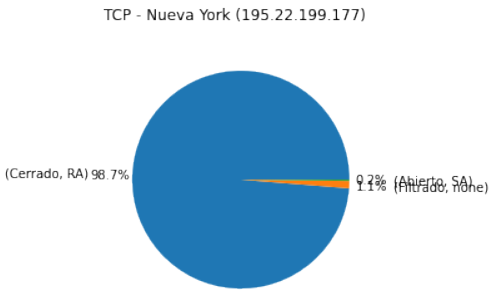
En este caso, asi como en el anterior, pudimos determinar que, para el protocolo **TCP**, todos los puertos salvo el 53, el 80 y el 443, fueron filtrados, por lo que asumimos que lo mismo aplica para los puertos del protocolo **UDP**.

port	TCP	TCPflag	UDP
1	Filtrado	none	Abierto | Filtrado
2	Filtrado	none	Abierto | Filtrado
3	Filtrado	none	Abierto | Filtrado
4	Filtrado	none	Abierto | Filtrado
5	Filtrado	none	Abierto | Filtrado
...	...	...	...
1020	Filtrado	none	Abierto | Filtrado
1021	Filtrado	none	Abierto | Filtrado
1022	Filtrado	none	Abierto | Filtrado
1023	Filtrado	none	Abierto | Filtrado
1024	Filtrado	none	Abierto | Filtrado

1021 rows × 3 columns

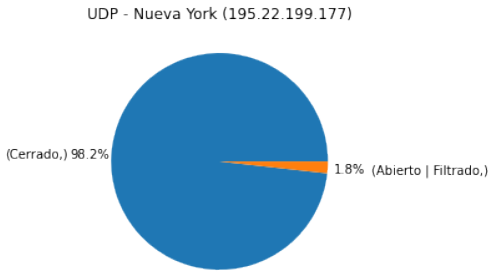
3.4. Universidad De New York

En el caso de la Universidad de Nueva York, nos encontramos con que el 98.7 % de los puertos del protocolo TCP se encontraban cerrados, un 1.1 % fueron filtrados, y los dos puertos restantes, el 179 y el 646, se encotraban abiertos. El puerto 179 corresponde al **Border Gateway Protocol (BGP)**, que se utiliza para intercambiar iformación de alcance y ruteo entre sistemas autónomos, mientras que el puerto 646 se corresponde con **Label Distribution Protocol (LDP)**, que se utiliza para el intercambio de informacion de etiquetas de mapeo entre routers con capacidad MPLS (una tecninca de ruteo).



port	TCP	TCPflag
179	Abierto	SA
646	Abierto	SA

En este caso, nos encontramos con que el 98.2 % de los puertos del protocolo **UDP** se encontraban cerrados, mientras que, para el 1.8 % restante, no pudimos determinar su estado, ya que podrian haber estado abiertos, y haber sido filtrados en el camino. En este caso, suponemos que el puerto 646 se encontraba abierto, ya que no pudimos determinar su estado, pero se encontraba abierto para el protocolo **TCP**.



port	UDP	TCP	TCPflag
646	Abierto | Filtrado	Abierto	SA

3.4.1. Firewall

En la siguiente lista podemos ver los puertos que encontramos filtrados por algun firewall para el protocolo **TCP**, y para el protocolo **UDP** no pudimos determinar si estaban abiertos o si fueron filtrados.

port	TCP	TCPflag	UDP
135	Filtrado	none	Abierto | Filtrado
137	Filtrado	none	Abierto | Filtrado
138	Filtrado	none	Abierto | Filtrado
139	Filtrado	none	Abierto | Filtrado
445	Filtrado	none	Abierto | Filtrado
514	Filtrado	none	Abierto | Filtrado

4. Conclusiones

En los primeras tres muestra de *Port scanning*, de las facultades de Munich, Auckland y Tokyo obtuvimos resultados similares. Los dos puertos abiertos son los standards que utilizan los browsers de internet para obtener las páginas web de las univercidades. Esto se debio a que la IP utilizada para experimentar era la IP obtenida del DNS de la página web. El browser web, por default siguiendo los standards, siempre buscara la pagina web HTTP hosteada en el puerto 80, los servicios de DNS en el 53, y la página por HTTPS en 443. Dados estos resultados, dedicidimos escanear un puerto distinto al obtenido de la consulta del browser para la página web. Para la univercidad de New York obtuvimos la IP de un listado de IPs que estaba dentro de una seccion interna de la página web. Esta IP, al ser escneada, dio distintos resultados: los puertos abiertos eran los 179 y 646, utilizados para servicios de distribución y redirección dentro del sistema de IPs de la facultad.

Luego, analizando los puertos con firewall, obtuvimos resultados esperados: solo los servicios *conocidos* tenian las puertas abiertas para ser consultados. El resto tenian algún nivel de protección. Esto era esperado, o algún problema de seguridad o diseño posiblemente podria afectar a los hosts en cuestión.