TP3: Port-Scanning y DNS

Introducción

En este trabajo realizaremos un Port Scanning para intentar determinar en qué estado están los puertos **bien conocidos** de los servidores de varias universidades del mundo. Los puertos bien conocidos son los que van del número 0 al 1023 y como todo puerto pueden estar en estado abierto o cerrado. Cabe aclarar que nuestros intentos por saber su estado consisten básicamente en el envío de pings que pueden no llegar nunca a destino si son filtradas por un firewall.

Métodos y condiciones de los experimentos

Implementación del código

Para determinar el estado de los puertos vamos a realizar el envío de paquetes TCP y UDP a los puertos bien conocidos de los servidores de las siguientes universidades:

- Universidad de Buenos Aires (uba.ar)
- Universidad Nacional de Córdoba (unc.edu.ar)
- Universidad de Sudáfrica (unisa.ac.za)
- Universidad de Alejandria (alexu.edu.eg)
- Universidad ITMO, Rusia (itmo.ru)
- Universidad de Reikiavik, Islandia (fs.ru.is)

El código para esta funcionalidad se implementó en el lenguaje Python utilizando la biblioteca Scapy.

Para el escaneo de puertos TCP, se envió un paquete con el flag “SYN” a todos los puertos bien conocidos de cada servidor, de manera que si se recibe la respuesta “SYN + ACK”, tenemos la confirmación de que el puerto está abierto. En cambio, si se recibe una respuesta con el flag “RESET + ACK”, significa que el puerto está cerrado. Al no recibir respuesta, podría el puerto estar cerrado o el paquete filtrado por un firewall.

Para el escaneo de puertos UDP, se envió un paquete UDP a todos los puertos bien conocidos de cada servidor, al igual que el análisis de TCP. Sin embargo, dado que la comunicación sobre UDP no tiene noción de conexión, aunque el puerto esté abierto el servicio que lo atiende puede no responder nada. Si el mensaje está siendo filtrado por un firewall puede igual no haber respuesta, por lo que encontrar puertos abiertos requiere conocimiento previo sobre los servicios que normalmente lo atienden. La única manera de detectar un puerto efectivamente cerrado es si recibiéramos un paquete ICMP de tipo *Destination-Unreachable* y subtipo *Port-Unreachable*.

Para ambos escaneos en caso de recibir un paquete ICMP de tipo *Destination-Unreachable* tomaremos cómo indicador de que el puerto se encuentra filtrado (salvo subtipo *Port-Unreachable* en UDP).

Criterios de clasificación de nmap

Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1,2,3,9,10, or 13)	filtered

Tabla 5.2 de “Nmap Reference Guide”, https://nmap.org/book/synscan.html

Response	Assigned State
Any UDP response from target port (unusual)	open
No response received (even after retransmissions)	open | filtered
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1,2,3,9,10, or 13)	filtered

Tabla 5.3 “Nmap Reference Guide”, https://nmap.org/book/scan-methods-udp-scan.html

Experimentación

Para nuestra experimentación decidimos escanear los puertos bien conocidos de las universidades antes mencionadas con nuestro script y comparar los resultados con un escaneo obtenido con la utilidad nmap. El escaneo realizado por nmap es service-aware por lo que obtenga mejores resultados en los puertos UDP y más información en los TCP.

El scan con nmap fué realizado el **2021-06-09** entre las 11:09 y las 16:09 utilizando los flags `-sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"`.

El scan con nuestro script fué realizado el **2021-06-11** entre las 18:20 y las 18:21.

Conclusiones

¿Cuántos puertos abiertos aparecen? ¿A qué servicios/protocolos (nivel de aplicación) corresponden?

Descubiertos por nuestro script

- tcp: uba.ar:80 (HTTP)
- tcp: uba.ar:443 (TLS+HTTP)
- tcp: unc.edu.ar:80 (HTTP)
- tcp: unc.edu.ar:443 (TLS+HTTP)
- tcp: unisa.ac.za:80 (HTTP)

Descubiertos por nmap

- tcp: alexu.edu.eg:25 (SMTP)
- tcp: alexu.edu.eg:53 (DNS)
- udp: alexu.edu.eg:53 (DNS)
- tcp: alexu.edu.eg:80 (HTTP)
- tcp: alexu.edu.eg:443 (TLS+HTTP)
- tcp: alexu.edu.eg:993 (TLS+IMAP)
- tcp: fs.ru.is:443 (TLS+HTTP)
- tcp: itmo.ru:80 (HTTP)
- tcp: itmo.ru:443 (TLS+HTTP)
- tcp: itmo.ru:22 (SSH)
- tcp: uba.a :80 (HTTP)
- tcp: uba.ar:443 (TLS+HTTP)
- tcp: unc.edu.ar:80 (HTTP)
- tcp: unc.edu.ar:443 (TLS+HTTP)
- tcp: unisa.ac.za:80 (HTTP)
- tcp: unisa.ac.za:443 (TLS+HTTP)

¿Cuántos puertos filtrados tenían los sitios web que se probaron?

Como mencionamos anteriormente, nuestro script no tiene manera de diferenciar los puertos UDP abiertos de los filtrados por firewall. Sin más que agregar, listamos los puertos filtrados para los que recibimos alguna respuesta:

Descubiertos por nuestro script (con respuesta)

- tcp: uba.ar:865 (filtered)

  Destination-Unreachable con subtipo Communication-Prohibited en lugar de un RST.

- udp: uba.ar:802 (filtered)

  Destination-Unreachable con subtimo Communication-Prohibited.

- tcp: unisa.ac.za:53 (closed)

Total filtrados: 12292 + 3 = 12295

Descubiertos por nmap

- tcp: itmo.ru:135 (filtered)
- tcp: itmo.ru:139 (filtered)
- tcp: itmo.ru:445 (filtered)
- tcp: unisa.ac.za (closed)
- tcp: unisa.ac.za:53 (closed)

Total filtrados: 12279 + 5 = 12284

¿Es posible darse cuenta si los hosts que se probaron están protegidos por un firewall?

Es posible tener sospechas. Por ejemplo nuestro script recibió respuestas ICMP a paquetes TCP lo cual esperaríamos para puertos filtrados. Para el caso general es imposible distinguir entre un firewall y un host comportándose cómo uno.

¿Existen otros puertos bien conocidos que puedan estar abiertos en los hosts que se probaron?

No encontramos otros puertos abiertos con nmap pero sí otros dos puertos filtrados que quedan por fuera del análisis propio de nuestro script:

- tcp: itmo.ru:1080
- tcp: itmo.ru:3128

DNS (opcional)

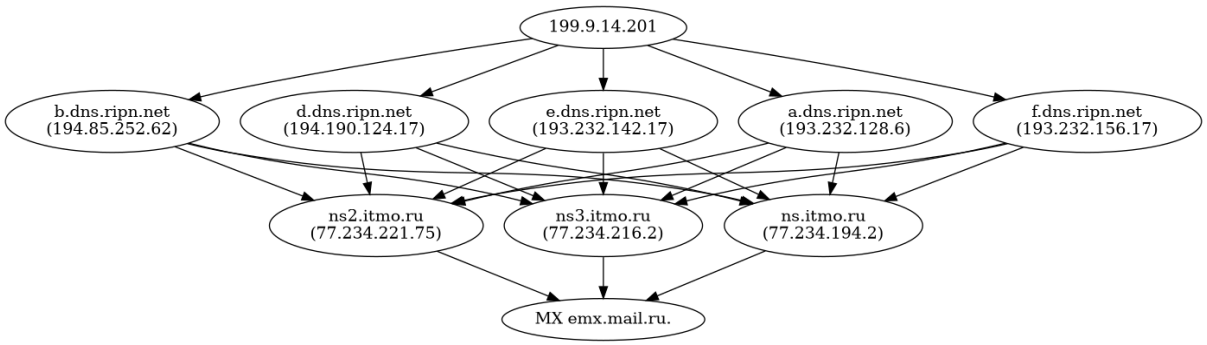
En esta última parte trabajaremos realizando sucesivas consultas DNS, a los mismos servidores de universidades elegidos en la sección anterior. con ellos analizaremos mediante consultas iterativas los registros MX (Mail exchange) de cada dominio.

Para ello modificamos el script de scapy provisto, en donde luego de realizar un llamado *“encolamos”* los hosts recibidos tanto en la Answer Section, como sus respectivos SOAs. Así mismo contabilizamos aquellas respuestas que fueron respondidas y las que no lo fueron.

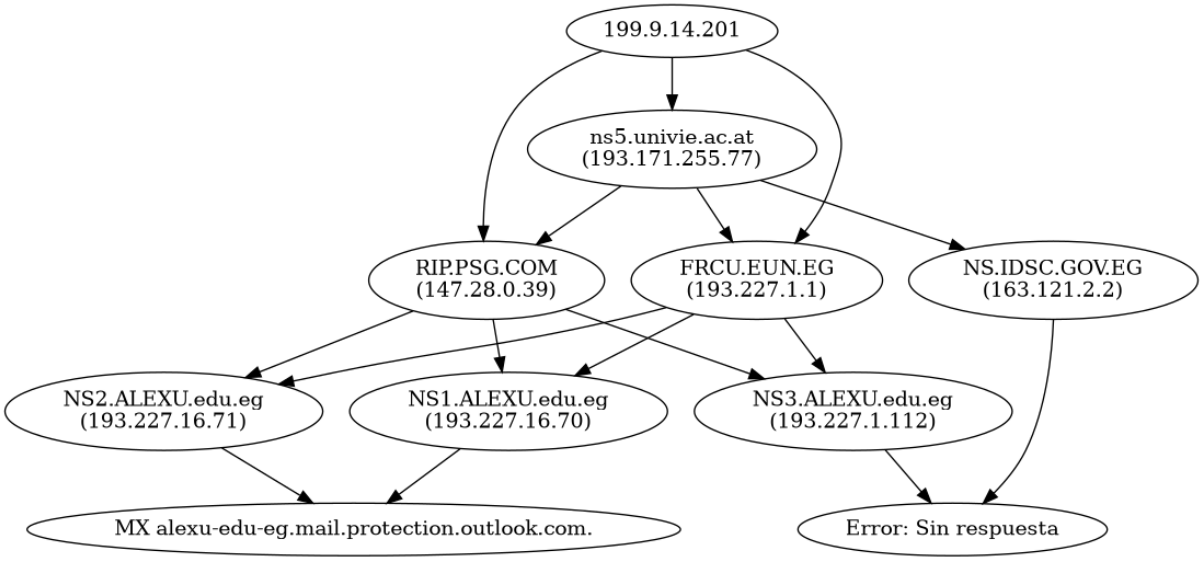
Experimentación

A continuación procederemos a mostrar los resultados de los las 6 universidades elegidas. Empezando por las extranjeras, dejando la UBA y la UNC para el final.

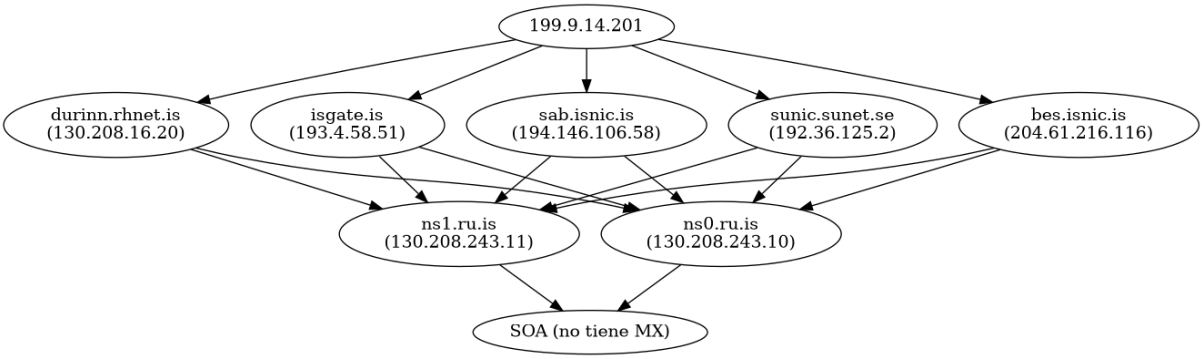
- **Dominio de la Universidad ITMO, Rusia (itmo.ru)**



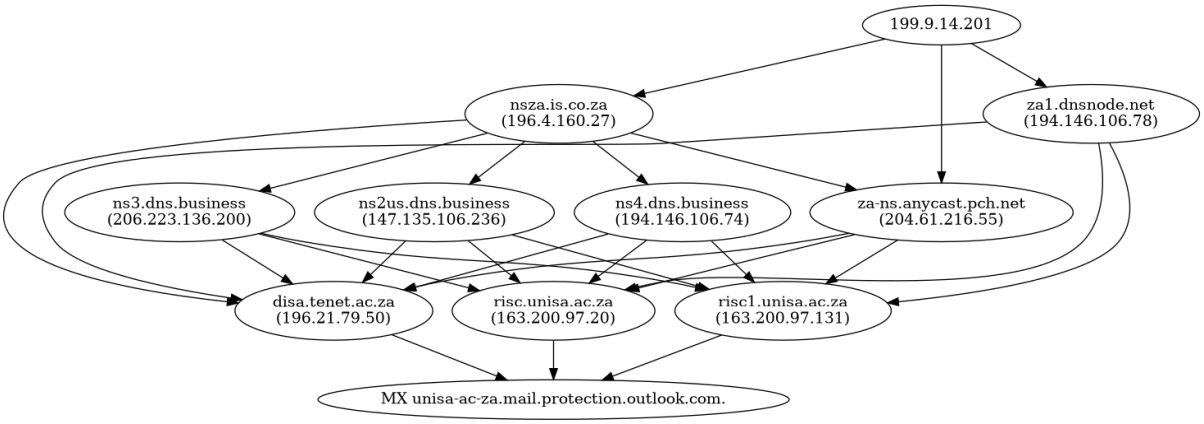
- **Dominio de la Universidad de Alejandria (alexu.edu.eg)**



- **Universidad de Reikiavik, Islandia (fs.ru.is)**

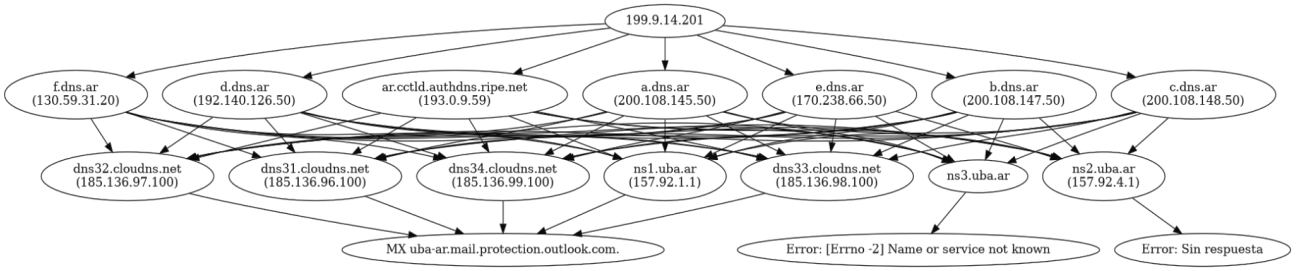


- **Universidad de Sudáfrica (unisa.ac.za)**

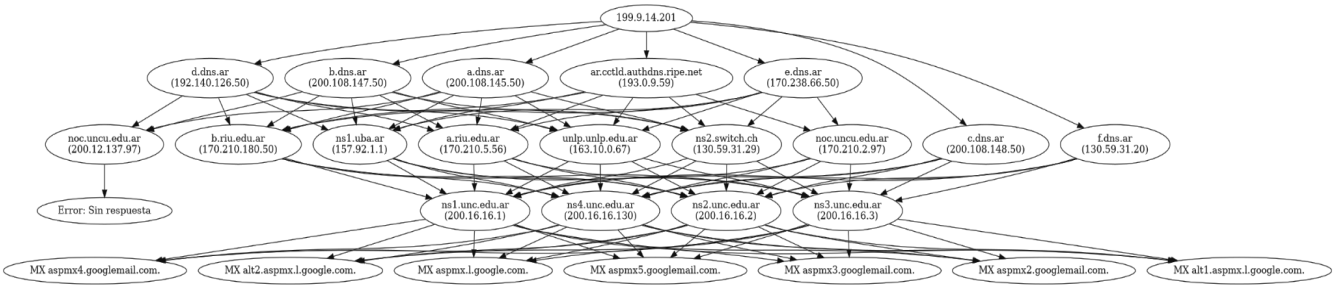


Finalmente, llegamos a los dominios de la UBA y UNC en Argentina, destacamos que los resultados obtenidos fueron mucho más *“caoticos”* de lo esperado. En el caso de la **UNC** incluso recibimos varias respuestas de MX diferentes.

- **Universidad de Buenos Aires (uba.ar)**



- **Universidad Nacional de Córdoba (unc.edu.ar)**



Conclusiones

¿Cuántos niveles de servidores DNS se recorrieron en las sucesivas consultas hasta obtener la información solicitada?

Depende del caso, sin embargo en líneas generales todos los dominios son capaces de detectar en 3 iteraciones un registro MX (almenos por alguna de sus rutas) , En el caso de Islandia, no hubo respuesta MX, lo último que recibimos es el SOA, sin Answer Section.

¿Todos los servidores DNS Autoritativos que aparecen en las sucesivas respuestas responden a las consultas realizadas?

La cantidad de NS records varían dependiendo la universidad, en general casi siempre son respondidos. Sin embargo, tenemos casos como apartados de los cuales no obtenemos respuesta.

En **Alejandria (alexu.edu.eg)**, de los dominios **NS3.ALEXU.edu.eg y NS.IDSC.GOV.EG** no obtuvimos respuesta.

En **Argentina** obtuvimos el siguiente escenario.

- **uba.ar:**
  - **ns2.uba.ar** no obtuvimos respuesta
  - **ns3.uba.ar** no resuelve a ninguna dirección IP.
- **unc.edu.ar:**
  - **noc.uncu.edu.ar** no obtuvimos respuesta.

¿Cuántos nombres de servidores de mail encontraron? ¿Tienen nombres en el mismo dominio que la universidad?

Encontramos un total de 11 servidores de mail de los cuales 7 registros MX aparecieron en la consulta de **unc.edu.ar.** Estos 7 registros apuntan a dominios de Google por lo que podemos asumir que utilizan google apps para procesar los emails universitarios.

Para el caso de Islandia **fs.ru.is** no arrojó ninguna respuesta.

Finalmente el resto de las universidad arrojaron cada una un registro MX:

- alexu.edu.eg, uba.ar, unisa.ac.za: Apuntan a subdominios de outlook.com. Por lo que entendemos que usan el servicio de email de Microsoft.
- itmo.ru: Apunta a un subdominio de mail.ru. Mail.ru es un aglomerado de empresas que tienen entre otros servicios (además de uno de los servicios de mail más populares de Runet) ICQ y VKontakte.

¿Cuántas direcciones IP distintas hay? ¿Estas direcciones IP corresponden a dispositivos que están prendidos?

Para resolver los nameservers de la authority section utilizamos el resolvedor de DNS del sistema operativo. Por lo que podría en realidad haber más IPs descubiertas (correspondientes a servidores con múltiples registros A). En la siguiente tabla detallamos la cantidad de IPs consultadas en cada una de las trazas antes mostradas.

Dominio	Cantidad de IPs
Universidad Nacional de Córdoba (unc.edu.ar)	18
Universidad de Buenos Aires (uba.ar)	13
Universidad de Sudáfrica (unisa.ac.za)	9
Universidad ITMO, Rusia (itmo.ru)	8
Universidad de Alejandria (alexu.edu.eg)	7
Universidad de Reikiavik, Islandia (fs.ru.is)	7

De las IPs que no respondieron en su momento podemos decir lo siguiente:

- *NS3.ALEXU.edu.eg*, *NS.IDSC.GOV.EG* no responden (ni vía a DNS ni ping)
- *ns2.uba.ar* responde vía ping. Haciendo más pruebas con nuestro script encontramos vimos otras situaciones en las que sí respondió vía DNS. Por lo que creemos que lo que se ve en las trazas mostradas es simplemente la pérdida de un paquete (dado que nuestro script no reenvía los paqutes)
- *noc.uncu.edu.ar* no responde en una de las IPs que posee (tiene más de un registro A)

¿Coinciden las IPs de los servidores de correo con las IPs de los servidores Web?

No. Además todos usan servicios externos (provistos por Google, Microsoft o Mail.ru) para el procesamiento de emails.