Redes y Comunicaciones

Ulises Jeremias Cornejo Fandos[1]

[1] *Licenciatura en Informatica - 13566/7, Facultad de Informatica, UNLP*

compiled: September 16, 2018

1. Ejercicio 1

Descargue la captura .pcap del servidor **http://redes.catedras.linti.unlp.edu.ar/smtp/smtp.pcap** Para ello la petición GET deberá contener el header *x-custom-redes2018*.

Para descargar el archivo *.pcap* se utiliza el comando curl ejecutando los siguientes comandos en la terminal.

```
$ URL=http://redes.catedras.linti.unlp.edu.ar/smtp/smtp.pcap
$ curl -H "x-custom-redes2018: value" $URL --output smtp.pcap
```

2. Ejercicio 2

Extraiga de la consulta .pcap descargada las consultas DNS y los datos correspondientes a SMTP.

3. Ejercicio 3

Analizar consultas DNS realizadas por el servidor SMTP origen.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	163.10.10.61	163.10.5.78	DNS	81	Standard query 0x0ef8 MX demo.info.unlp.edu.ar
2	0.000712	163.10.5.78	163.10.10.61	DNS	174	Standard query response 0x0ef8 MX demo.info.unlp.edu.ar MX 5 mail2.demo.info.unlp.edu.ar MX 10 mail.demo.info
3	0.001016	163.10.10.61	163.10.5.78	DNS	87	Standard query 0x5cc6 AAAA mail2.demo.info.unlp.edu.ar
4	0.001636	163.10.5.78	163.10.10.61	DNS	132	Standard query response 0x5cc6 AAAA mail2.demo.info.unlp.edu.ar SOA ada.info.unlp.edu.ar
5	0.001730	163.10.10.61	163.10.5.78	DNS	87	Standard query 0xcdc3 A mail2.demo.info.unlp.edu.ar
6	0.002071	163.10.5.78	163.10.10.61	DNS	121	Standard query response 0xcdc3 A mail2.demo.info.unlp.edu.ar A 163.10.20.254 NS ada.info.unlp.edu.ar
7	0.002178	163.10.10.61	163.10.5.78	DNS	86	Standard query 0x63c6 AAAA mail.demo.info.unlp.edu.ar
8	0.002679	163.10.5.78	163.10.10.61	DNS	131	Standard query response 0x63c6 AAAA mail.demo.info.unlp.edu.ar SOA ada.info.unlp.edu.ar
9	0.002753	163.10.10.61	163.10.5.78	DNS	86	Standard query 0x2060 A mail.demo.info.unlp.edu.ar
10	0.003058	163.10.5.78	163.10.10.61	DNS	120	Standard query response 0x2060 A mail.demo.info.unlp.edu.ar A 163.10.20.18 NS ada.info.unlp.edu.ar

Fig. 1. Consultas DNS realizadas por el servidor SMTP origen.

a) ¿Cuál es el servidor DNS recursivo que utiliza el servidor SMTP origen?

Mirando la primer consulta DNS realizada, podemos observar que el servidor DNS recursivo al cual hace la consulta tiene como IP 163.10.5.78.

b) ¿Cuáles son las consultas DNS que realiza?

Las consultas DNS realizadas son las siguientes:

1. Primero se hace una consulta DNS al servidor con IP 163.10.5.78 para obtener el servidor de mail de ‘demo.demo.info.unlp.edu.ar‘ haciendo una consulta DNS de tipo MX.
   En la respuesta de la misma se obtienen los datos de dos servidores de mail. Los mismos son ‘mail2.demo.info.unlp.edu.ar‘ y ‘mail.demo.info.unlp.edu.ar‘ con preferencias 5 y 10 respectivamente.

2. Posteriormente, se pide conocer la IP del servidor de mail con mayor nivel de preferencia, 5. Entonces se hace una consulta DNS de tipo AAAA al mismo servidor que en el caso anterior para conocer la IPv6 del servidor de mail ‘mail2.demo.info.unlp.edu.ar‘.
   Dado que la respuesta de la consulta es vacia y no existe ningun error en la conexión, podemos saber que el mismo no tiene una IPv6 asociada.

3. Se procede a consultar por la IPv4 del servidor ‘mail2.demo.info.unlp.edu.ar‘ haciendo una consulta DNS de tipo A. En la respuesta de la consulta podemos ver que se obtiene la ip 163.10.20.254.

4. Posteriormente, se pide conocer la IP del servidor de mail con nivel de preferencia 10. Entonces se hace una consulta DNS de tipo AAAA al mismo servidor que en el caso anterior para conocer la IPv6 del servidor de mail ‘mail.demo.info.unlp.edu.ar‘.
   Dado que la respuesta de la consulta es vacia y no existe ningun error en la conexión, podemos saber que el mismo no tiene una IPv6 asociada.

5. Se procede a consultar por la IPv4 del servidor ‘mail.demo.info.unlp.edu.ar‘ haciendo una consulta DNS de tipo A. En la respuesta de la consulta podemos ver que se obtiene la ip 163.10.20.18.

c) ¿Alguna de las respuestas es de tipo autoritativa?

Mirando el flag *Authoritative* de las respuestas a cada una de las consultas podemos ver que ninguna de ellas son de tipo autoritativo.

4. Ejercicio 4

Análisis de SMTP

a) ¿A qué servidor SMTP se conecta el servidor de correo origen? ¿Por qué?

Observando la primer fila de los datos correspondientes a SMTP podemos ver que el servidor de mail con el que se logra establecer la conexión tiene ipv4 163.10.20.18, es decir, que se conecta con el servidor ‘mail.demo.info.unlp.edu.ar‘.

b) ¿Cuántas comunicaciones SMTP se observan en la captura?

Se observan dos comunicaciones SMTP.

5. Ejercicio 5

Sobre el primer correo electrónico

a) ¿A qué corresponde la información enviada por el servidor destino como respuesta al comando EHLO? Elija dos de las opciones del listado e investigue la funcionalidad de la misma.

La información que envia el servidor como respuesta al EHLO es:

- mail
- PIPELINING
- SIZE 10240000
- VRFY
- ETRN
- STARTTLS
- AUTH PLAIN LOGIN
- AUTH=PLAIN LOGIN
- ENHANCEDSTATUSCODES
- 8BITTIME
- DSN
- SMTPUTF8

b) ¿Por qué el contenido del primer mail no puede ser leído?

Se envia el mail de forma segura utilizando TLS.

6. Ejercicio 6