

Redes y Comunicaciones

Ulises Jeremias Cornejo Fandos,¹ Federico Ramón Gasquez,² and Lihuel Pablo Amoroso³

¹13566/7, Licenciatura en Informatica, Facultad de Informatica, UNLP

²13598/6, Licenciatura en Informatica, Facultad de Informatica, UNLP

³13497/2, Analista Programador Universitario, Facultad de Informatica, UNLP

compiled: September 18, 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.

Se adjuntan con la entrega los .pcap asociados a los datos filtrados en el directorio *filtered*.

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.unlp.edu.ar
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 vacía y no existe ningún 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 vacía y no existe ningún 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 primera 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 envía el servidor como respuesta al EHLO es:

- mail
- PIPELINING
- SIZE 10240000
- VRFY
- ETRN
- STARTTLS
- AUTH PLAIN LOGIN
- AUTH=PLAIN LOGIN

- ENHANCEDSTATUSCODES
- 8BITTIME
- DSN
- SMTPUTF8

STARTTLS

STARTTLS es una extensión a los protocolos de comunicación de texto plano, que ofrece una forma de mejorar desde una conexión de texto plano a una conexión cifrada (TLS o SSL) en lugar de utilizar un puerto diferente para la comunicación cifrada.

PIPELINING

La extensión pipelining significa que, durante la conexión, el cliente no siempre necesita esperar una respuesta antes de enviar la siguiente solicitud. Específicamente, el cliente no necesita esperar por respuestas de RSET, MAIL, RCPT, o un mensaje codificado.

El servidor puede demorar la respuesta mientras sigue recibiendo nuevas solicitudes, pero en general esto no ocurre. El servidor no debería nunca esperar por el input del cliente hasta haber terminado todas las solicitudes pendientes, y debe responderlas en orden. Es responsabilidad del cliente evitar el deadlock.

SIZE

La extensión size tiene 2 propósitos:

- Avisar al servidor de un estimado del tamaño del mensaje antes de que el mismo sea transmitido.
- Avisar al cliente de que los mensajes superando cierto tamaño no será aceptado.

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

Se envía el mail de forma segura utilizando TLS.

6. Ejercicio 6

Con respecto al segundo correo electrónico

a) ¿Cuál es el nombre del servidor de correo origen?

El primer comando que necesitamos enviar al servidor de correo es EHLO o HELO. Este es un saludo básico que inicia la comunicación entre el cliente de telnet y el servidor SMTP. También se pasa el DNS PTR para la dirección IP desde la que nos conectamos, como se determinó previamente.

Luego, el nombre del servidor de correo origen es 'mail.linti.unlp.edu.ar' y lo sabemos dado que se envía como parámetro del comando EHLO.

b) ¿Cuál es el MESSAGE-ID del correo enviado? ¿Quién asigna dicho valor?

En la fila 20 de los datos filtrados para el protocolo SMTP, paquete nro. 113 del total de los paquetes del .pcap, se puede ver en el campo Internet Message Format el MESSAGE-ID del mail enviado y este es:

`<94c3492a-4bf1-c0c8-c059-c2cb2216d2f8@linti.unlp.edu.ar>`

El Message-Id es generado por el user agent de mail o el servidor SMTP origin.

c) ¿Cuál es el producto que implementa el servidor de correo origen y cuál el destino?

El cliente utilizado para el envío del mail es Thunderbird, *Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Thunderbird/52.9.1*. Luego, el producto que implementa el servidor de correo origen es Exim en su versión 4.80, y el servidor de mail destino implementa Postfix sobre un GNU Debian.

d) Analice y explique los comandos SMTP y las correspondientes respuestas que se presentan en la captura.

- EHLO, para abrir una sesión, en el caso de que el servidor soporte extensiones definidas en el RFC 1651. En ambos casos de utilización de este comando, el servidor responde con un listado de comandos extra soportados por el mismo. Entre estas opciones está PIPELINING la cual permite que se ejecuten los comandos MAIL FROM, RCPT TO y DATA sin esperar una respuesta del servidor inmediata entre cada uno de ellos. Se explican luego cada uno de los comandos.
- STARTTLS, Los servidores de correo electrónico y los clientes que usan el protocolo SMTP normalmente se comunican usando texto sin formato a través de Internet. La comunicación a menudo pasa por uno o más enrutadores que el servidor y el cliente no controlan ni confían en ellos. Esta comunicación se puede controlar y también es posible modificar los mensajes que se envían a través de los enrutadores.

Para mejorar la seguridad, se puede usar una conexión encriptada TLS (Seguridad de la capa de transporte) al comunicarse entre el servidor de correo electrónico y el cliente. TLS es más útil cuando se necesita cifrar un nombre de usuario y contraseña de inicio de sesión (enviados por el comando AUTH). TLS se puede utilizar para encriptar todo el mensaje de correo electrónico, pero el comando no garantiza que todo el mensaje permanezca encriptado todo el camino hasta el receptor; algunos servidores de correo electrónico pueden decidir enviar el mensaje de correo electrónico sin cifrado. Pero al menos el nombre de usuario y la contraseña utilizados con el comando AUTH permanecerán encriptados. Usar el comando STARTTLS junto con el comando AUTH es una forma muy segura de autenticar usuarios.

En respuesta a esto, el servidor envía 220 2.0.0 Ready to start TLS.

- MAIL FROM, para indicar quien envía el mensaje.
- RCPT TO, para indicar el destinatario del mensaje.
- DATA, para indicar el comienzo del mensaje, éste finalizará cuando haya una línea únicamente con un punto.
- QUIT, para cerrar la sesión.

Como respuesta, el servidor envía 221 2.0.0 BYE.

En el caso de los comandos ejecutados para el envío de mail, como se menciona anteriormente se ejecuta en un pipe, y el servidor envía los tres códigos en una única respuesta 250 2.1.0 Ok — 250 2.1.5 Ok — 354 End data with <CR><LF>.<CR><LF>.

e) ¿Qué diferencia hay entre la entrada “MAIL FROM” y “From” que se observa en la captura?

Para explicar la diferencia entre ambas podemos pensar en el siguiente ejemplo:

Cuando vos envía una carta, la envías en un sobre. El sobre contiene tu mensaje. La dirección de devolución escrita en el correo postal es la misma que la dirección de devolución “MAIL FROM:” y la “RCPT TO:” dará la dirección del destinatario. Esto es parte de la información del sobre.

El contenido del mensaje, dentro del sobre de la carta, es como el cuerpo de su mensaje. En el sentido del correo electrónico, también puede tener la información del campo del encabezado, como “Subject:” “Date:”, “To:” y “From:”.

Luego, el comando “MAIL FROM” especifica la dirección para propósitos de devolución (ejemplo: problemas con la entrega de correo). Por otro lado, el campo de encabezado “De:” le dirá quién es el autor del mensaje.

f) Indicar cuáles cabeceras fueron agregadas por el MUA.

El MUA agrega las cabeceras de User Agent y Message ID.

g) Analice las cabeceras MIME y responda:

- 1) ¿Qué tipo de archivo fue adjuntado al correo electrónico?
Se adjunta un archivo de tipo imagen con formato *.jpeg*.
- 2) ¿Quién es el personaje que se encuentra en la foto?



Fig. 2. Imagen enviada como archivo adjunto en el mail.