Práctica 4

Capa de Aplicación - Correo electrónico

Correo electrónico

1. ¿Qué protocolos se utilizan para el envío de mails entre el cliente y su servidor de correo? ¿Y entre servidores de correo?

2. ¿Qué protocolos se utilizan para la recepción de mails? ¿Incluiría a HTTP en dichos protocolos? Enumere y explique características y diferencias entre las alternativas posibles.

3. Utilizando la VM y teniendo en cuenta los siguientes datos, abra el cliente de correo (Icedove) y configure dos cuentas de correo. Una de las cuentas utilizará POP para solicitar al servidor los mails recibidos para la misma mientras que la otra utilizará IMAP.

   Al crear cada una de las cuentas, seleccionar Manual config y luego de configurar las mismas según lo indicado, ignorar advertencias por uso de conexión sin cifrado.

   Datos para POP

   - Cuenta de correo: alumnopop@redes.unlp.edu.ar
   - Nombre de usuario: **alumnopop**
   - Contraseña: **alumnopoppass**
   - Puerto: **110**

   Datos para IMAP

   - Cuenta de correo: alumnoimap@redes.unlp.edu.ar
   - Nombre de usuario: **alumnoimap**
   - Contraseña: **alumnoimappass**
   - Puerto: **143**

   Datos comunes para ambas cuentas

   - Servidor de correo entrante (POP/IMAP):
     - Nombre: **mail.redes.unlp.edu.ar**
     - SSL: **None**
     - Autenticación: **Normal password**
   - Servidor de correo saliente (SMTP):
     - Nombre: **mail.redes.unlp.edu.ar**

- Puerto: **25**
- SSL: **None**
- Autenticación: **Normal password**

a. Verificar el correcto funcionamiento enviando un email desde el cliente de una cuenta a la otra y luego desde la otra responder el mail hacia la primera.

b. **Análisis del protocolo SMTP**

   i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnopop@redes.unlp.edu.ar envía un correo a alumnoimap@redes.unlp.edu.ar

   ii. Utilice el filtro SMTP para observar los paquetes del protocolo SMTP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta. Ayuda: filtre por protocolo SMTP y sobre alguna de las líneas del intercambio haga click derecho y seleccione Follow TCP Stream...

   iii. Desde una terminal de comandos, utilice los comandos observados en el punto anterior para enviar un mail de manera manual. Después de hacerlo, verifique que haya recibido el correo. Para conectarse al servidor deberá utilizar el comando:
   telnet mail.redes.unlp.edu.ar 25

c. **Análisis de encabezados**

   i. Desde una terminal de comandos envíe un mail de manera manual al puerto 25 del servidor mail.redes.unlp.edu.ar utilizando, en la directiva del envelop **mail from:** una cuenta de correo diferente de la cuenta de correo utilizada en el encabezado **From:**

      a′ Verifique en el correo recibido la cuenta que el usuario percibe como el remitente del correo.

      b′ Analice los fuentes del correo para ver si es posible observar tanto la información indicada tanto en la directiva del envelop **mail from:** como en el encabezado **From:**.

   ii. Usando el cliente de correo, **icedove** del usuario alumnopop@redes.unlp.edu.ar envíe un correo electrónico alumnoimap@redes.unlp.edu.ar el cual debe tener: un asunto, datos en el body y una imagen adjunta.

      a′ Verifique los fuentes del correo recibido para entender como se utiliza el header Çontent-Type: multipart/mixed"para poder realizar el envío de distintos archivos adjuntos.

      b′ Extraiga la imagen adjunta del mismo modo que lo hace el cliente de correo a partir de los fuentes del mensaje.

d. **Análisis del protocolo POP**

   i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnoimap@redes.unlp.edu.ar le envía una correo a alumnopop@redes.unlp.edu.ar y mientras alumnopop@redes.unlp.edu.ar recepciona dicho correo.

ii. Utilice el filtro POP para observar los paquetes del protocolo POP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta.

e. **Análisis del protocolo IMAP**

i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnopop@redes.unlp.edu.ar le envía una correo a alumnoimap@redes.unlp.edu.ar y mientras alumnoimap@redes.unlp.edu.ar recepciona dicho correo.

ii. Utilice el filtro IMAP para observar los paquetes del protocolo IMAP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta.

f. **IMAP vs POP**

i. Marque como leídos todos los correos que tenga en el buzón de entrada de alumnopop y de alumnoimap. Luego, cree una carpeta llamada POP en la cuenta de alumnopop y una llamada IMAP en la cuenta de alumnoimap.
Asegurese que tiene mails en el inbox y en la carpeta recientemente creada en cada una de las cuentas.

ii. Con el rol de administrador del sistema (root), ejecute el cliente de correos. Para esto, abra una consola de comandos y ejecute: **sudo icedove**
De esta forma, iniciará el cliente de correo con el perfil del superusuario (diferente del usuario con el que ya configuró las cuentas antes mencionadas).
Luego configure las cuentas POP e IMAP de los usuarios alumnopop y alumnoimap como se describió anteriormente pero desde el cliente de correos ejecutado con el usuario root.
Luego responda:

a′ ¿Qué correos ve en el buzón de entrada de ambas cuentas? ¿Están marcados como leídos o como no leídos? ¿Por qué?

b′ ¿Qué pasó con las carpetas POP e IMAP que creó en el paso anterior?

iii. En base a lo observado. ¿Qué protocolo le parece mejor? ¿POP o IMAP? ¿Por qué? ¿Qué protocolo considera que utiliza más recursos del servidor? ¿Por qué?

4. **(Ejercicio de promoción) Utilizando la herramienta Swaks, envíe un correo electrónico con las siguientes características:**

NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.

- Dirección destino: Dirección de correo de alumnoimap@redes.unlp.edu.ar
- Dirección origen: Dirección de correo de uno de los integrantes del grupo

- Asunto: SMTP-<Número de grupo>
- Archivo adjunto: PDF del enunciado de la práctica
- Cuerpo del mensaje: Nombres de los integrantes del grupo

a. Analice tanto la salida del comando swaks como los fuentes del mensaje recibido para responder las siguientes preguntas:

   i. ¿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.

   ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.

   iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?

   iv. ¿Cuál es el software utilizado como servidor de correo electrónico?

   v. Adjunte la salida del comando swaks y los fuentes del correo electrónico.

5. **(Ejercicio de promoción) Descargue de la plataforma la captura de tráfico smtp.pcang y la salida del comando swaks smtp.swaks para responder y justificar los siguientes ejercicios.**

   NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.

   a. ¿Por qué el contenido del mail no puede ser leido en la captura de tráfico?

   b. Recupere el archivo adjunto a partir de la salida del comando de swaks para indicar de qué personaje se trata.

6. Investigue que son los registros SPF, para que se usan y cómo se configuran.

7. Realice una consulta de DNS por registros TXT al dominio info.unlp.edu.ar y entre dichos registros evalúe la información del registro SPF. ¿Por qué cree que aparecen muchos servidores autorizados?

Ejercicio de parcial.

8. Suponga que el servidor de correo mail1.example.com tiene para enviar un correo a pepe@gmail.com. Indique y justifique en todos los casos:

   - Primer consulta de DNS que debe hacer mail1.example.com.
   - Suponiendo que la consulta anterior devuelve varios resultados, ¿de qué forma elegiría mail1.example.com el servidor al cuál entregar el correo? ¿Y si ese servidor no estuviera disponible?
   - Considerando que la consulta anterior retorna un listado de nombres de servidores de correo para gmail.com, ¿será necesario realizar una consulta de DNS adicional? En caso de responder afirmativamente, indique el registro por el cuál se realizará la consulta.

- Cuál será el protocolo de aplicación, el protocolo de transporte y el puerto que mail1.example.com usará para entregar el correo al destinatario pepe@gmail.com.