Índice

Actividad 2 – POSTFIX - Mecanismos de Autenticación (SASL) y políticas de aceptación.

1. Introducción

SASL es el acrónimo de "**Simple Authentication and Security Layer**" que significa "Capa de Seguridad y Autenticación Simple". SASL es el método por defecto que nos permite añadir autenticación a los protocolos no seguros como SMTP. Se trata de un servicio independiente que Postfix utilizará para llevar a cabo las autenticaciones.

2. Integración SASL en PostFix

En sus versiones modernas, **postfix soporta 2 tipos de autenticación**; Cyrus SASL y Dovecot SASL. Podemos comprobar las versiones soportadas ejecutando la siguiente orden:

```
:~$ postconf –a
cyrus
dovecot
```

Como nosotros estamos configurando una servicio de correo electrónico a través de IMAP, lo aconsejable es utilizar la **implementación integrada con Dovecot;** Dovecot **SASL,** y será en la que nos centremos a lo largo de la práctica.

2.1 Instalación y configuración

Configuración de Dovecot

El servicio paquete `dovecot-imapd`, instalado en la práctica anterior, dispone de un plugin para implementar SASL y y permite a Postfix autenticar con él. Para habilitarlo

basta con buscar el fichero de configuración `/etc/dovecot/conf.d/10-master.conf`, buscar el siguiente **bloque de código**, descomentarlo e introducir las siguientes opciones:

```
#Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
   mode = 0666
   user = postfix
   group = postfix
}
```

De esta forma **estamos definiendo un nuevo socket UNIX** que se **mantendrá a la espera de peticiones de autenticación** del usuario **postfix**.

Configuración de Postfix

Por su parte, **en** la configuración de **PostFix**, **deberemos** indicar la **ruta del socket** y **habilitar** la **autenticación** para ello, editaremos el fichero `/etc/postfix/main.cf` y añadiremos las siguientes líneas:

/etc/postfix/main.cf

```
# Autenticación SASL
smtpd_sasl_type = dovecot
smtpd_sasl_auth_enable = yes
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
```

2.2 Cambio del puerto por defecto del servidor SMTP

En muchas ocasiones, los proveedores de acceso a internet (ISP) **cierran el puerto**

25 como medida preventiva para evitar el **envío de spam** a través de sus red. Esto es así porque, al ser el puerto por defecto y **no proveer autenticación** algunas spammers tratan de buscar servidore abiertos **openRelay**, para poder enviar sus mensajes.

En estas estas circunstancias necesitamos habilitar el **envío de correos** por el **puerto 587.** La configuración de los **puertos de escucha de postfix** se lleva a cabo a través del fichero `/etc/postfix/master.cf.` Buscaremos, la siguiente directiva

/etc/postfix/master.cf

```
// Directiva original que escucha por el puerto 25
smtp      inet  n       -       y       -       -       smtpd
```

y la sustituiremos por:

/etc/postfix/master.cf

```
// Los sustituimos por la siDirectiva modificada que escucha por el puerto 587
587       inet  n       -       y       -       -       smtpd
```

Una vez modificado, **reiniciaremos el servicio de postfix** y abriremos **el puerto** correspondiente en el **firewall.**

El **tercer parámetro** resulta de gran relevancia, ya que nos indica si el servidor postfix **se ejecutará en una jaula** (chroot) dentro de la rura `/var/spool/postfix`. Al ejecutarse en una jaula, **cualquier ruta** que especifiquemos dentro de los **archivos de configuración** tomará como base este directorio, de forma que si especificamos `/private/auth`, realmente se estará especificando que el archivo se ubica en `/var/spool/postfix/private/auth`

Para finalizar, **configuraremos el cliente** (MUA) para que haga uso del **nuevo puerto**. Si hacemos uso de roundcube, esto se realiza a través del fichero `/var/www/roundcube/config/config.inc.php`. En la **siguiente página** puedes consultar todas las **opciones de configuración** del cliente.

2.3 Definición políticas anti-spam para la aceptación de los mensajes.

Para finalizar, es conveniente modificar **nuestra política de aceptación de mensajes** para hacer el **servidor más seguro frente al spam**:

/etc/postfix/main.cf

```
# Políticas de recepción de mensajes
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination, reject_unknown_client_hostname, reject_rbl_client zen.spamhaus.org
```

De esta forma, estaremos definiendo que:

- Aceptaremos **recibir mensajes que sean enviados desde nuestras redes** (en nuestra configuracióon, sólo la propia máquina en la que está el servidor).
- En caso contrario, aceptaremos recibir mensaje de conexiones autenticadas.
- En caso contrario, rechazaremos los correos que no vayan destinados a nosotros mismos (o que no vayan destinados a dominios que hayamos autorizado. **(no hemos autorizado ninguno).**
- En caso contrario, rechazaremos mensajes de clientes cuya IP no se resuelva a un nombre. **(IP inversa)**
- En caso contrario, comprobamos que el cliente nos parezca fiable, para lo cual nos basamos **en una base de datos externa** de spam. (**Spamhaus**)

Actividad 1 – Preguntas propuestas

Contesta razonadamente a las siguientes preguntas

- Busca en la documentacion oficial de postfix, la funcionalidad de cada una de las **directivas que hemos aplicado en el servidor de postfix** para habilitar la **autenticación mediante SASL** y define la función que llevan a cabo.

- ¿Que diferencia existe entre Dovecot SASL y Cirus SASL?

- ¿Qué es spamhaus? ¿Qué funcionalidad nos proporciona?

Actividad 2 – Arquitectura a configurar

- Securiza el **servidor postfix** instalado para que **solo permita** el envío de correos a usuarios autenticados mediante SASL. Una vez realizado, reconfigura **roundcube** para que utilize **autenticación por smtp.**

```
$config['smtp_user'] = '%u';
$config['smtp_pass'] = '%p';
```

– Configura **postfix** para que atienda solo peticiones por el **puerto 587**.

Actividad 3 – Envío de correos al exterior

- ¿Que **directiva de postfix** permite indicar las redes desde las cuales se permitirá enviar **correos al exterior**? ¿Qué modificación deberías hacer para poder enviar correos al exterior desde roundcube? Prueba a enviarte correos a tu cuenta de gmail.

3. Bibliografía / Webgrafía

- Documentación oficial de PostFix. http://www.postfix.org/documentation.html. PostFix Web Site.
- Servidor IMAP. https://sio2sio2.github.io/doc-linux/07.serre/03.mail/03-imap/index.html#Linuxnomición
- Archivo de configuración Roundcube. https://github.com/roundcube/roundcubemail/blob/master/config/defaults.inc.php. Roundcube