TEMA 5 – BOLETÍN DE EJERCICIOS

Cristóbal Suárez Abad

SERVICIOS DE RED E INTERNET - 2º ASIR

4. (E) EMAIL Server. Objetivo: crear un servidor de envío de correo electrónico funcional. Para ello, debes configurar un servidor de correo personalizando una imagen docker de IRedMail en tu Servidor Docker, bajo el nombre de dominio **que elijas**, teniendo en cuenta los apartados que se detallan a continuación:

i. Configura la zona de tu dominio en el servidor DNS del aula:

a. Conteniendo el registro MX apuntando hacia ***mail.tudominio.tld***

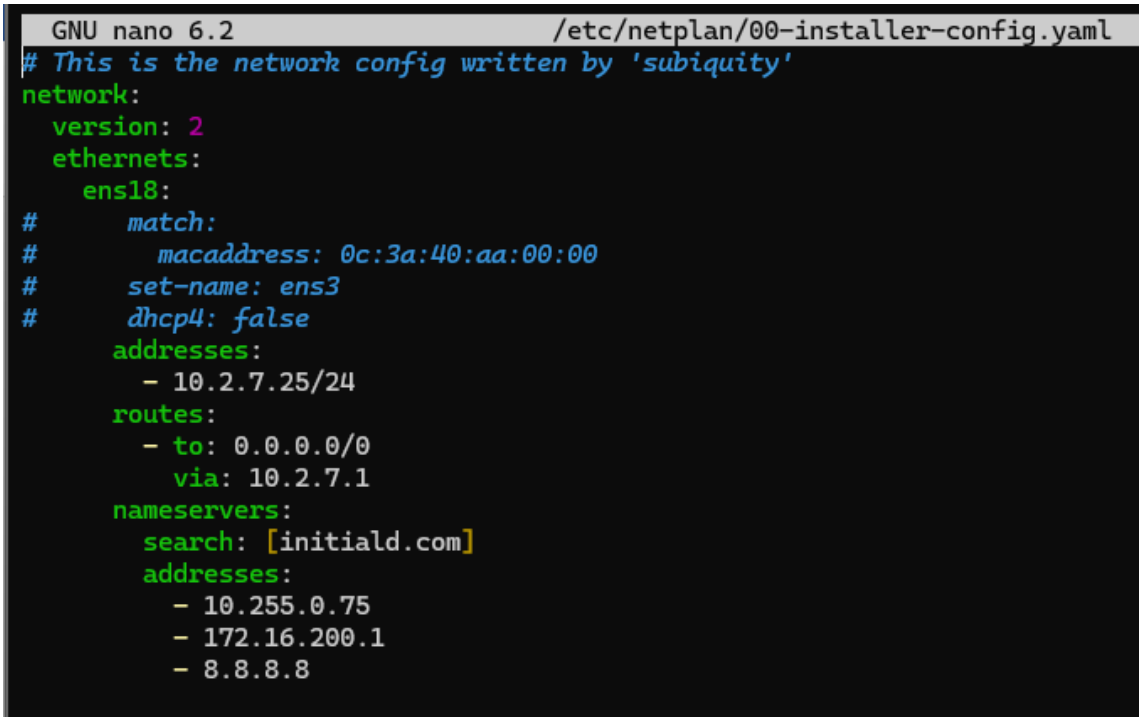
b. De manera que dicho nombre resuelva como la **ip tu servidor** de correo (será la misma del servidor Docker) y viceversa.

//Configuración de named.conf.local

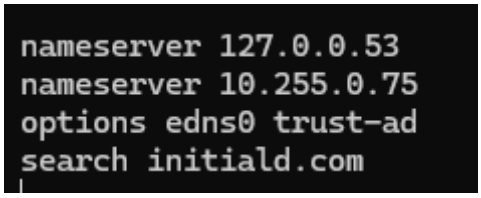
```
// Archivo para busquedas directas
zone "initiald.com" {
  type master;
  file "db.initiald.com";     // Debe estar en /var/cache/bind/
  allow-update { none; };
};

// Configuración de db.initiald.com
Bind data file
; PLANTILLA DE AYUDA PARA DNS
; GUARDAR COMO db.initiald.com
; BIND data file for initiald.com
;
$TTL    1D
@ IN SOA dnsdjfr.institutodh.net. root.institutodh.net. (
        2025112701 ; Serial Basado en el dia e incrementando
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Default TTL

; Servidores DNS del dominio
        IN      NS              dnsdjfr.institutodh.net.

; Correo
        IN      MX 10   mail.initiald.com.

; Directas
mail IN A 10.2.7.25

; Alias o sinonimo
mx IN CNAME mail
smtp IN CNAME mail
```

ii.Configuración de un servidor de correo SMTP usando **IRedMail**:

a. Configura la **Ip estática** de tu servidor Docker y elige como DNS del profesor (10.255.0.75).



También en el archivo "/etc/resolv.conf". ¿Esto se hace dentro del contenedor o en servidor Docker? Lo he puesto en ambos.



b. Baja la imagen del servidor de correo iRedMail y siguiendo estas instrucciones ejecútalo para que:

i. Configura el **FQDN** (nombre completo ***mail.tudominio.tld***). Ver ayuda en dockerhub.

ii. Define los dominios para los que se acepta correo entrante y reenvío. Ver ayuda en DockerHub. Comprueba dentro del contenedor el valor de la variable ***mydestinations*** de la configuración de postfix.

Creamos un directorio para iRedMail:

mkdir iredmail

Nos situamos en él. Creamos el archivo con los siguientes datos:

echo HOSTNAME=mail.initiald.com >> iredmail-docker.conf

echo FIRST_MAIL_DOMAIN=initiald.com >> iredmail-docker.conf

echo FIRST_MAIL_DOMAIN_ADMIN_PASSWORD=12345 >> iredmail-docker.conf

echo MLMMJADMIN_API_TOKEN=$(openssl rand -base64 32) >> iredmail-docker.conf

echo ROUNDCUBE_DES_KEY=$(openssl rand -base64 24) >> iredmail-docker.conf

Creamos una serie de ficheros para el contenedor.

mkdir -p data/{backup-mysql,clamav,custom,imapsieve_copy,mailboxes,mlmmj,mlmmj-archive,mysql,sa_rules,ssl,postfix_queue}

Creamos un archivo .sh que usaremos para crear el contenedor.

```
docker run \
  --rm \
   -d \
  --name iredmail \
  --env-file iredmail-docker.conf \
  --hostname mail.initiald.com \
  -p 80:80 \
  -p 443:443 \
  -p 110:110 \
  -p 995:995 \
  -p 143:143 \
  -p 993:993 \
  -p 25:25 \
  -p 465:465 \
  -p 587:587 \
```

***-v /iredmail/data/backup-mysql:/var/vmail/backup/mysql ***
***-v /iredmail/data/mailboxes:/var/vmail/vmail1 ***
***-v /iredmail/data/mlmmj:/var/vmail/mlmmj ***
***-v /iredmail/data/mlmmj-archive:/var/vmail/mlmmj-archive ***
***-v /iredmail/data/imapsieve_copy:/var/vmail/imapsieve_copy ***
***-v /iredmail/data/custom:/opt/iredmail/custom ***
***-v /iredmail/data/ssl:/opt/iredmail/ssl ***
***-v /iredmail/data/mysql:/var/lib/mysql ***
***-v /iredmail/data/clamav:/var/lib/clamav ***
***-v /iredmail/data/sa_rules:/var/lib/spamassassin ***
***-v /iredmail/data/postfix_queue:/var/spool/postfix ***
iredmail/mariadb:stable

Ahora ejecutamos el archivo, pero debemos hacerlo como ROOT (no vale hacer un sudo).

sh iredmail.sh

Para entrar en el contenedor

docker exec -ti iredmail /bin/bash

Una vez dentro del contenedor, comprobamos el valor de “mydestination”.

cat /etc/postfix/main.cf | grep mydestination

```
tricTions $sender_dependent_relayhost_maps
mydestination = $myhostname, localhost, localhost.localdomain
    $mydestination
```

cat /etc/postfix/main.cf | grep hostname

```
myhostname = mail.initiald.com
mydestination = $myhostname, localhost, localhost.localdomain
root@mail:/#
```

ATENCIÓN: **ClamAV** puede petarte el disco porque se pone a hacer actualizaciones, etc. Para evitarlo, no hay otra forma de pararlo que cambiarle el nombre.

Renombra el clam: **/usr/sbin/clamd**

Le pones cualquier NOMBRE Y YA ESTÁ. usa mv.

iii. Usa el filtro Amavis para crear una lista negra de manera que no se acepte correo entrante del correo spammer@l.io y desde otro dominio que tu elijas.

Listamos los plugins: ls -l /opt/iredapd/plugins/

```
root@mail:/# ls -l /opt/iredapd/plugins/
total 152
-r-x------ 1 iredapd iredapd     0 Aug 27  2021 __init__.py
drwx------ 2 root    root     4096 Dec  6 17:12 __pycache__
-r-x------ 1 iredapd iredapd 13634 Aug 27  2021 amavisd_wblist.py
-r-x------ 1 iredapd iredapd 17355 Aug 27  2021 greylisting.py
-r-x------ 1 iredapd iredapd  2843 Aug 27  2021 ldap_force_change_password.py
-r-x------ 1 iredapd iredapd 11749 Aug 27  2021 ldap_maillist_access_policy.py
-r-x------ 1 iredapd iredapd   986 Aug 27  2021 reject_null_sender.py
-r-x------ 1 iredapd iredapd 16180 Aug 27  2021 reject_sender_login_mismatch.py
-r-x------ 1 iredapd iredapd   788 Aug 27  2021 reject_to_hostname.py
-r-x------ 1 iredapd iredapd  4313 Aug 27  2021 senderscore.py
-r-x------ 1 iredapd iredapd  8665 Aug 27  2021 sql_alias_access_policy.py
-r-x------ 1 iredapd iredapd  2795 Aug 27  2021 sql_force_change_password.py
-r-x------ 1 iredapd iredapd  4843 Aug 27  2021 sql_ml_access_policy.py
-r-x------ 1 iredapd iredapd 30090 Aug 27  2021 throttle.py
-r-x------ 1 iredapd iredapd  3324 Aug 27  2021 wblist_rdns.py
-r-x------ 1 iredapd iredapd  3849 Aug 27  2021 whitelist_outbound_recipient.py
root@mail:/# ls -l /opt/iredapd/plugins/
```

Ahora debemos introducir en el listado de plugins activos el que vamos a crear más adelante, para ello modificamos el archivo de configuración:

nano /opt/iredapd/settings.py

Nos vamos a la sección “Enabled plugins” he introducimos: “wblist_admin”

```
# Enabled plugins.
plugins = ['wblist_admin', 'rejec
```

Ahora nos situamos en la carpeta de plugins:

/opt/iredapd/tools

python3 wblist_admin.py --add --blacklist spammer@l.io @.

```
root@mail:/opt/iredapd/tools# python3 wblist_admin.py --add --blacklist spammer@l.io @.
* Establishing SQL connection.
* Add inbound blacklist for account: @.
* Add senders: spammer@l.io, @.
root@mail:/opt/iredapd/tools#
```

Es probable que no tengamos Python en el contenedor.

apt install python

pip install web.py

apt-get install python3-pip

Ahora introducimos otro nombre en la lista negra.

python3 wblist_admin.py --add --blacklist neo@policia.es @.

```
root@mail:/opt/iredapd/tools# python3 wblist_admin.py --add --blacklist neo@policia.es @.
* Establishing SQL connection.
* Add inbound blacklist for account: @.
* Add senders: neo@policia.es, @.
root@mail:/opt/iredapd/tools#
```

Para ver a quien tenemos en la lista negra o blanca, usamos:

https://docs.iredmail.org/amavisd.wblist.html

“python3 wblist_admin.py --list --whitelist”

```
root@mail:/opt/iredapd/tools# python3 wblist_admin.py --list --whitelist
* Establishing SQL connection.
* List all inbound whitelist for account: @.
10.2.3.25
root@mail:/opt/iredapd/tools#
```

“python3 wblist_admin.py --list --blacklist"

```
root@mail:/opt/iredapd/tools# python3 wblist_admin.py --list --blacklist
* Establishing SQL connection.
* List all inbound blacklist for account: @.
@.
neo@policia.es
spammer@l.io
root@mail:/opt/iredapd/tools#
```

ATENCIÓN: Es posible que también tengamos que establecer en la white list para poder enviar-recibir correos desde determinadas direcciones:

Ejemplo servidor de Andrés:

python3 /opt/iredapd/tools/wblist_admin.py --add --whitelist 10.2.3.25

ATENCIÓN: Parece ser que cuando activamos las blacklist-whitelist, le da el siroco y te bloquea también tu propio servidor, por lo que no puedes mandar correos entre usuarios de tu dominio. Solución básica: pon el localhost en la whitelist.

python3 /opt/iredapd/tools/wblist_admin.py --add --whitelist 127.0.0.1

Configura SpamAssasin para que califique como spam los mensajes que tengan tus ***iniciales*** en el Asunto. Aporta pruebas en el siguiente ejercicio.

Fuera del contenedor, en el servidor, nos situamos en **/iredmail/data/sa_rules/3.004004/updates_spamassassin_org**

Allí hay un archivo “local.cf” que usaremos como plantilla para nuestra tarea, lo copiamos.

cp local.cf csa.cf

Introducimos:

 # --- Configuración para bloquear 'CSA' en el Asunto ---
 # 1. Definición de la Regla (Pattern Match):
 # Busca 'CSA' (insensible a mayúsculas/minúsculas) en el campo Subject.
header SUBJECT_HAS_MY_INITIALS Subject =~ /CSA/i
 # 2. Descripción:
describe SUBJECT_HAS_MY_INITIALS Asunto contiene mis iniciales (CSA)
 # 3. Puntuación (Score):
 # Una puntuación de 10.0 es suficiente para marcar el correo como spam
score SUBJECT_HAS_MY_INITIALS 10.0

```
# --- Configuración para bloquear 'CSA' en el Asunto ---

# 1. Definición de la Regla (Pattern Match):
# Busca 'CSA' (insensible a mayúsculas/minúsculas) en el campo Subject.
header      SUBJECT_HAS_MY_INITIALS       Subject =~ /CSA/i

# 2. Descripción:
describe    SUBJECT_HAS_MY_INITIALS       Asunto contiene mis iniciales (CSA)

# 3. Puntuación (Score):
# Una puntuación de 10.0 es suficiente para marcar el correo como spam
score       SUBJECT_HAS_MY_INITIALS       10.0
```

Recargamos la configuración:

Tienes que reiniciar el contenedor:

docker restart (nombre contenedor)

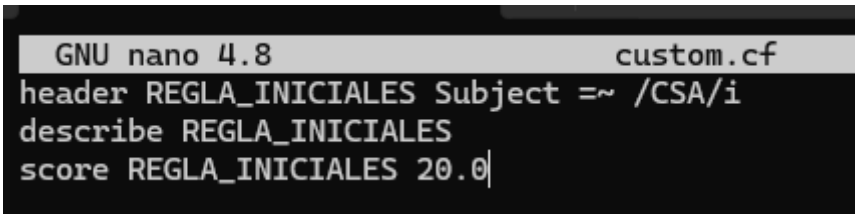
Estilo Andres:

nano /opt/iredmail/custom/spamassassin/custom.cf

header REGLA_INICIALES Subject =~ /CSA/i

describe REGLA_INICIALES

score REGLA_INICIALES 20.0



service amavis restart

iv. Para evitar los intentos de adivinación de contraseñas, iRedMail usa ***fail2ban***. Muestra las líneas de configuración que provocan el baneo de los atacantes. Muestra los logs de un baneo por múltiples fallos de autenticación. (Ayuda: mira /etc/fail2ban)

https://docs.iredmail.org/fail2ban.sql.html

"When some (bad) client triggers the ban, Fail2ban will perform actions defined in action = parameter in jail config file. For example, in jail dovecot (/etc/fail2ban/jail.d/dovecot.local):"

cat /etc/fail2ban/jail.d/dovecot.local

```
root@mail:/opt/iredapd# cat /etc/fail2ban/jail.d/dovecot.local
#
# This file is managed by iRedMail Team <support@iredmail.org> with Ansible,
# please do __NOT__ modify it manually.
#

[dovecot]
backend = polling
journalmatch =
enabled = true
filter  = dovecot
logpath = /var/log/dovecot/*.log tail
action  = iptables-multiport[name=dovecot, port="110,995,143,993,4190", protocol=tcp]
          banned_db[name=dovecot, port="110,995,143,993,4190", protocol=tcp]
root@mail:/opt/iredapd#
```

Log:

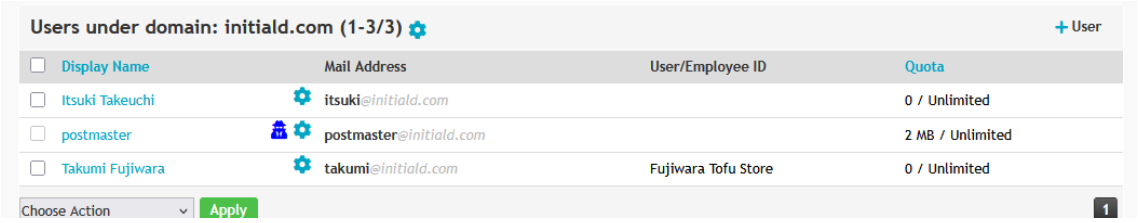
cat /var/log/dovecot/dovecot.log

```
root@mail:/opt/iredapd# cat /var/log/dovecot/dovecot.log
Dec  8 10:24:15 mail dovecot: master: Dovecot v2.3.7.2 (3c910f64b) starting up for pop3, imap, sieve, lmtp
root@mail:/opt/iredapd#
```

c. Configura el servidor para que utilice cifrado (SSL/**TLS**). Simplemente comprueba que los puertos de los servicios cifrados están activos y averigua dónde se encuentran los certificados que está usando (ficheros .key, .crt) ¿cómo podrías configurar un certificado válido?

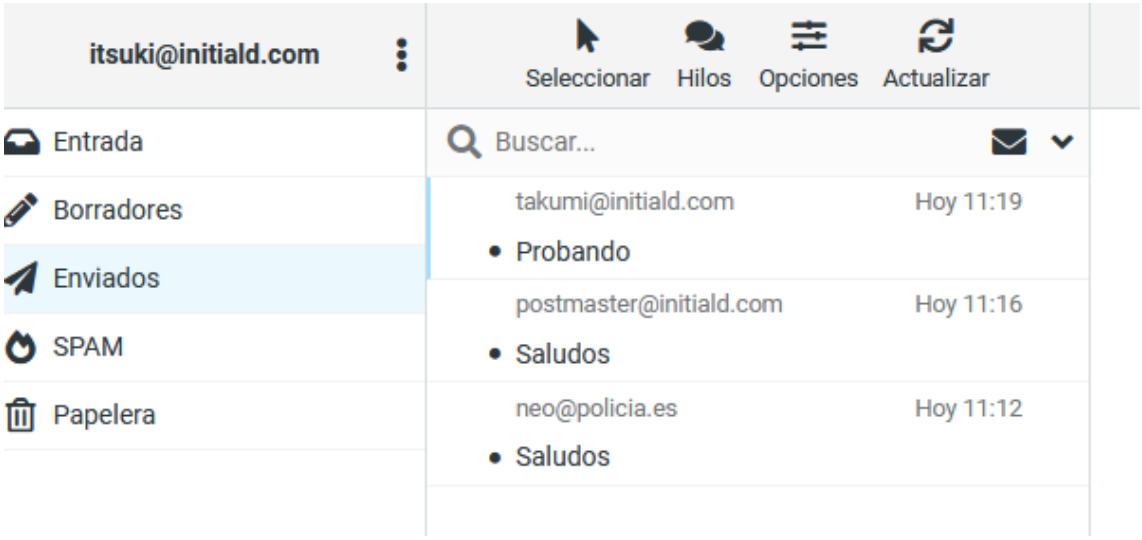
d. Añade algunas cuentas de usuario mediante el panel de administración de iRedMail (usuario *postmaster@tudominio*, web: *https://ip/iredadmin*)

https://10.2.7.25/iredadmin



iii. Realiza las siguientes pruebas de funcionamiento con el cliente ***webmail (roundcube)*** conectándote al propio servidor vía web.

a. Correo entre usuarios locales del servidor. Crea los que sean necesarios, relacionados con tu nombre de dominio. Aporta los logs que muestran el envío y la entrega del correo. Aporta los envíos, la comprobación de correo, y las respuestas.



cat /var/log/mail.log | grep takumi

Dec 8 11:19:08 mail amavis[754]: (00754-11) Passed UNCHECKED {RelayedTaggedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:57158 ESMTP/ESMTP <itsuki@initiald.com> -> <takumi@initiald.com>, (), Queue-ID: 4dPzyD6svnz4wCr, Message-ID: <4433b8b71d7ac1a31ae8e9ca2b2d7f87@initiald.com>, mail_id: BmaPn_gP0iuE, b: dIqQKJ3AU, Hits: -, size: 539, queued_as: 4dPzyN25bwz4wCx, Subject: "Probando", From: <itsuki@initiald.com>, User-Agent: Roundcube_Webmail, helo=localhost, 7278 ms

Dec 8 11:19:08 mail amavis[754]: (00754-11) Passed UNCHECKED, <itsuki@initiald.com> -> <takumi@initiald.com>, Hits: -, tag=2, tag2=6.2, kill=6.9, queued_as: 4dPzyN25bwz4wCx, L/Y/Y/Y

Dec 8 11:19:08 mail postfix/amavis/smtp[2740]: 4dPzyD6svnz4wCr: to=<takumi@initiald.com>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.4, delays=0.12/0.02/0.01/7.3, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dPzyN25bwz4wCx)

Dec 8 11:19:08 mail postfix/pipe[2767]: 4dPzyN25bwz4wCx: to=<takumi@initiald.com>, relay=dovecot, delay=0.13, delays=0.02/0.02/0/0.08, dsn=2.0.0, status=sent (delivered via dovecot service)

b. Correo desde un usuario local a un usuario de otro servidor de clase. Aporta los logs del envío.

cat /var/log/mail.log | grep neo@policia.es

Dec 8 11:12:59 mail amavis[754]: (00754-09) Passed UNCHECKED {RelayedTaggedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:57518 ESMTP/ESMTP <itsuki@initiald.com> -> <neo@policia.es>, (), Queue-ID: 4dPzq75ht6z4wCL, Message-ID: <4a113654809908c70965a3bdb7cd8c0a@initiald.com>, mail_id: ccaZOxDC8ymN, b: Jz8Y-NPCl, Hits: -, size: 536, queued_as: 4dPzqH1MTyz4wCr, Subject: "Saludos", From: <itsuki@initiald.com>, User-Agent: Roundcube_Webmail, helo=localhost, 7328 ms

Dec 8 11:12:59 mail amavis[754]: (00754-09) Passed UNCHECKED, <itsuki@initiald.com> -> <neo@policia.es>, Hits: -, tag=2, tag2=6.2, kill=6.9, queued_as: 4dPzqH1MTyz4wCr, L/Y/Y/Y

Dec 8 11:12:59 mail postfix/amavis/smtp[2601]: 4dPzq75ht6z4wCL: to=<neo@policia.es>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.5, delays=0.15/0.03/0.01/7.3, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dPzqH1MTyz4wCr)

Dec 8 11:13:05 mail postfix/smtp[2621]: 4dPzqH1MTyz4wCr: to=<neo@policia.es>, relay=mail.policia.es[10.2.3.25]:25, delay=6.6, delays=0.03/0.04/6.4/0.19, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 4dPzqP5QYrz3wsl)

c. Correo desde un usuario local a un destinatario exterior. Aporta los logs del envío.

No me deja:

cat /var/log/mail.log | grep cristobal

Dec 8 11:29:15 mail amavis[754]: (00754-12) Passed UNCHECKED {RelayedTaggedInternal}, ORIGINATING/MYNETS LOCAL [127.0.0.1]:59992 ESMTP/ESMTP <itsuki@initiald.com> -> <cristobal2590@institutodh.net>, (), Queue-ID: 4dQ09v4gqrz4wCx, Message-ID: <71ab28957ce301f0f6ea5747ad00af67@initiald.com>, mail_id: xM4X_Z3bcJzd, b: dIqQKJ3AU, Hits: -, size: 559, queued_as: 4dQ0B272Ytz4wCw, Subject: "Probando", From: <itsuki@initiald.com>, User-Agent: Roundcube_Webmail, helo=localhost, 7283 ms

Dec 8 11:29:15 mail amavis[754]: (00754-12) Passed UNCHECKED, <itsuki@initiald.com> -> <cristobal2590@institutodh.net>, Hits: -, tag=2, tag2=6.2, kill=6.9, queued_as: 4dQ0B272Ytz4wCw, L/Y/Y/Y

Dec 8 11:29:15 mail postfix/amavis/smtp[2923]: 4dQ09v4gqrz4wCx: to=<cristobal2590@institutodh.net>, relay=127.0.0.1[127.0.0.1]:10026, delay=7.4, delays=0.13/0.02/0.01/7.3, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 4dQ0B272Ytz4wCw)

Dec 8 11:29:18 mail postfix/smtp[2942]: 4dQ0B272Ytz4wCw: to=<cristobal2590@institutodh.net>, relay=none, delay=3.1, delays=0.03/0.03/3.1/0, dsn=4.4.1, status=deferred (connect to mail.institutodh.net[10.5.0.71]:25: **No route to host**)

d. Aporta la prueba de recepción de correo de otro compañero de clase.

Los logs se borran con cada reinicio del servidor iredmail.

e. Envía los correos necesarios para las pruebas del apartado anterior.