Práctica 2: Antivirus y antispam en servidor de correo corporativo

Objetivos

Implantar un sistema de filtrado de malware y spam en un servidor de correo electrónico CentOS

Preparación

Necesitas importar la máquina virtual Centos 7 disponible en esta misma actividad. Este servidor tiene ya instalado Postfix como servidor MTA y Dovecot como servidor de POP3/IMAP4

Enunciado

1. Descárgate la máquina virtual **Centos 7 mail server** e impórtala en VirtualBox. Comprueba que la conexión de red de la máquina esté en modo puente con la tarjeta de red del anfitrión para que se encuentre en la misma red que tu equipo.

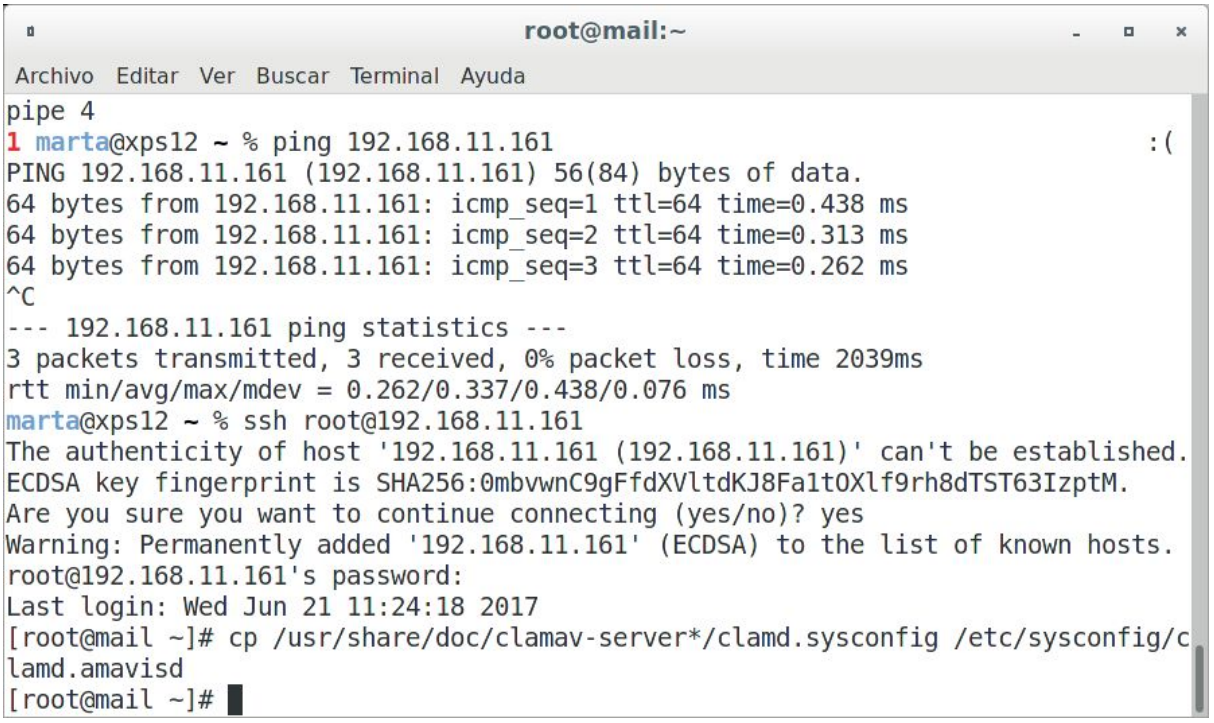
2. En este servidor existen los siguientes usuarios con sus contraseñas, que se han elegido sencillas para facilitar la realización de la práctica (aunque obviamente no es nada recomendable en un entorno de producción):

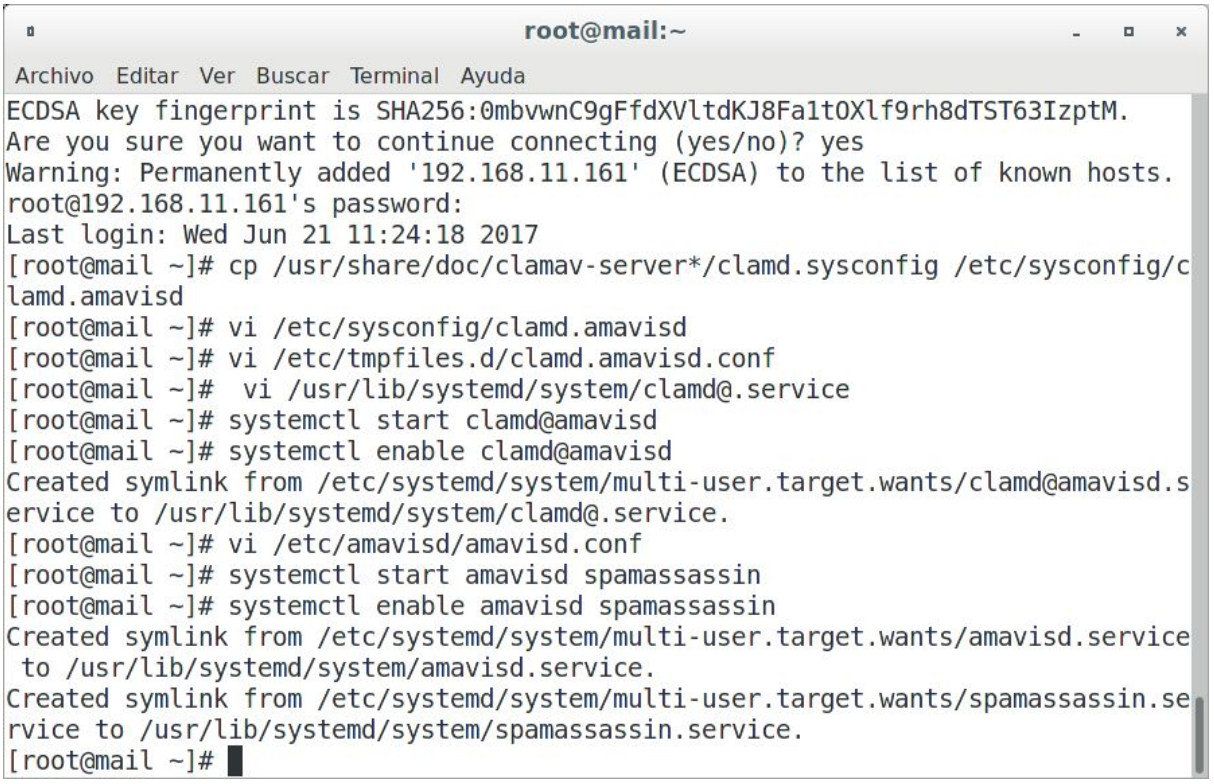
   root/cursoseg
   correo1/cursoseg
   correo2/cursoseg

3. Una vez ya tienes acceso como root, instala el antivirus **ClamAV** y **Amavis-new**, que es el conector de Postfix (servidor de correo SMTP) con el antivirus ClamAv y el antispam SpamAssassin. Para ello puedes seguir las indicaciones de esta página, adaptando algunos datos como el **hostname** y el **dominio** que en este caso son **mail.cursoseg.lan** y **cursoseg.lan** respectivamente:

   Instalación y configuración de Virus Scanning + Postfix + ClamAv en Centos 7

Os va a convenir copiar y pegar, así que os recomiendo acceder desde un terminal de la máquina real por ssh:





(Si sois lo bastante imprudentes como para usar Windows, podéis hacerlo con Putty)

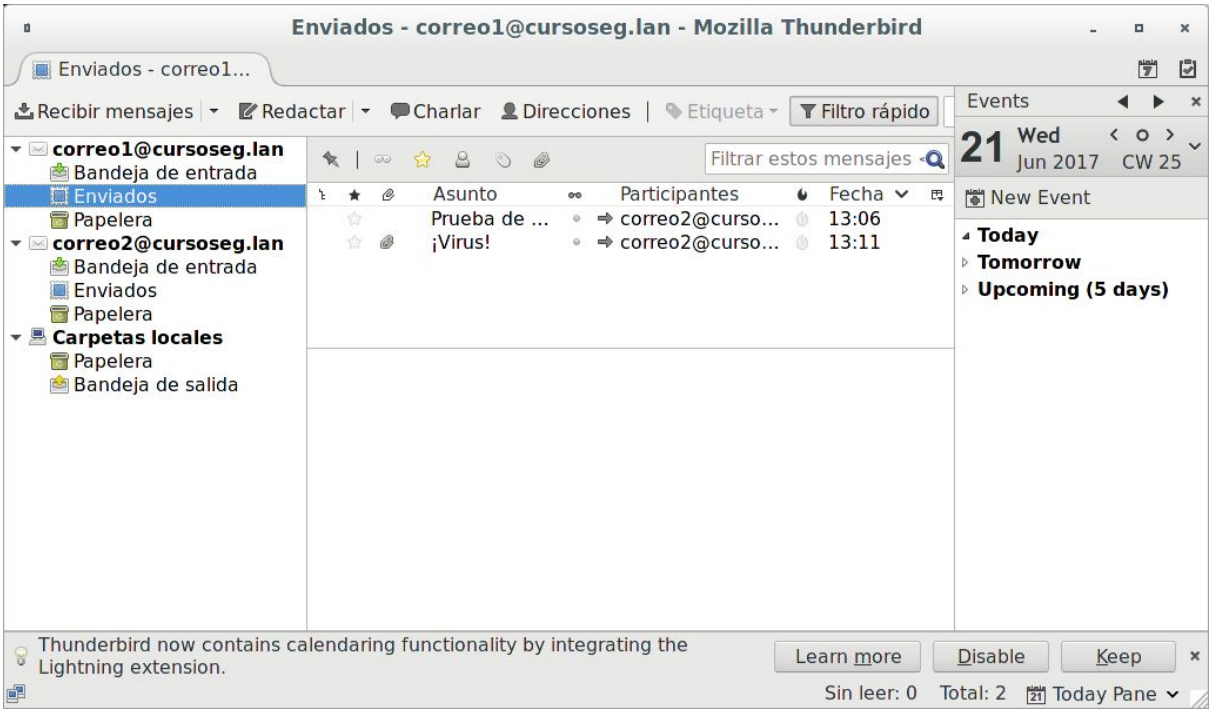
4. Una vez realizada la instalación, puedes hacer una prueba con un cliente de correo enviando emails entre las dos siguiente cuentas de correo ya configuradas en el servidor y que debes configurar en un programa de correo electrónico como por ejemplo Thunderbird, Opera Mail o la aplicación Correo de Windows 10:

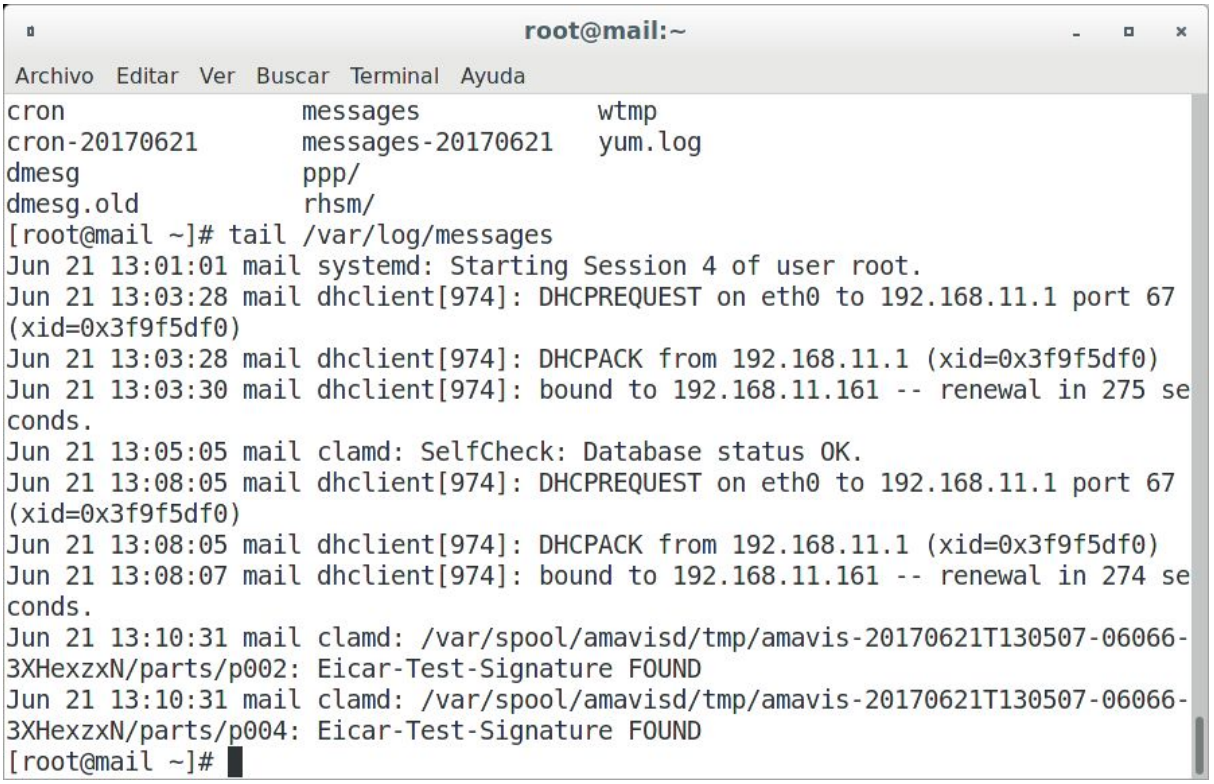
- **correo1@cursoseg.lan** usuario pop3:correo1 contraseña:cursoseg servidor SMTP/POP3: la ip que obtenga Centos en tu red
- **correo2@cursoseg.lan** usuario pop3:correo2 contraseña:cursoseg servidor SMTP/POP3: la ip que obtenga Centos en tu red

En ambos casos, la conexión se configura sin SSL/TLS (algo que tampoco se recomienda) y el servidor SMTP no requiere autenticación. En un entorno de producción es necesario activar SSL/TLS en SMTP y POP3/IMAP4, así como la autenticación SMTP.

5. Entrega una memoria de la práctica realizada, incluyendo las pruebas realizadas. Puedes usar el virus de muestra Eicar de la práctica anterior para adjuntarlo en los correos de prueba.

Debéis verificar que se pueden enviar correos entre las cuentas pero que son bloqueados si contienen un virus (Eicar):


Enviados - correo1@cursoseg.lan - Mozilla Thunderbird
Enviados - correo1...
Recibir mensajes
Redactar
Charlar
Direcciones
Etiqueta
Filtro rápido
correo1@cursoseg.lan
Bandeja de entrada
Enviados
Papelera
correo2@cursoseg.lan
Bandeja de entrada
Enviados
Papelera
Carpetas locales
Papelera
Bandeja de salida
Filtrar estos mensajes
Asunto
Participantes
Fecha
Prueba de ...
correo2@curso...
13:06
¡Virus!
correo2@curso...
13:11
Events
21 Wed Jun 2017 CW 25
New Event
Today
Tomorrow
Upcoming (5 days)
Thunderbird now contains calendaring functionality by integrating the Lightning extension.
Learn more
Disable
Keep
Sin leer: 0
Total: 2
Today Pane


root@mail:~
Archivo Editar Ver Buscar Terminal Ayuda
cron messages wtmp
cron-20170621 messages-20170621 yum.log
dmesg ppp/
dmesg.old rhsm/
[root@mail ~]# tail /var/log/messages
Jun 21 13:01:01 mail systemd: Starting Session 4 of user root.
Jun 21 13:03:28 mail dhclient[974]: DHCPREQUEST on eth0 to 192.168.11.1 port 67
(xid=0x3f9f5df0)
Jun 21 13:03:28 mail dhclient[974]: DHCPACK from 192.168.11.1 (xid=0x3f9f5df0)
Jun 21 13:03:30 mail dhclient[974]: bound to 192.168.11.161 -- renewal in 275 se
conds.
Jun 21 13:05:05 mail clamd: SelfCheck: Database status OK.
Jun 21 13:08:05 mail dhclient[974]: DHCPREQUEST on eth0 to 192.168.11.1 port 67
(xid=0x3f9f5df0)
Jun 21 13:08:05 mail dhclient[974]: DHCPACK from 192.168.11.1 (xid=0x3f9f5df0)
Jun 21 13:08:07 mail dhclient[974]: bound to 192.168.11.161 -- renewal in 274 se
conds.
Jun 21 13:10:31 mail clamd: /var/spool/amavisd/tmp/amavis-20170621T130507-06066-
3XHexzxN/parts/p002: Eicar-Test-Signature FOUND
Jun 21 13:10:31 mail clamd: /var/spool/amavisd/tmp/amavis-20170621T130507-06066-
3XHexzxN/parts/p004: Eicar-Test-Signature FOUND
[root@mail ~]#