

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.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.16.1.el7.x86_64 on an x86_64

mail login: root
Password:
Last login: Fri May 12 01:18:46 on tty1
[root@mail ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:82:d6:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.161/24 brd 192.168.11.255 scope global dynamic eth0
        valid_lft 540sec preferred_lft 540sec
    inet6 fe80::a00:27ff:fe82:d63e/64 scope link
        valid_lft forever preferred_lft forever
[root@mail ~]#
[root@mail ~]# _
```

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:

```
root@mail:~
Archivo Editar Ver Buscar Terminal Ayuda
pipe 4
1 marta@xps12 ~ % ping 192.168.11.161
PING 192.168.11.161 (192.168.11.161) 56(84) bytes of data.
64 bytes from 192.168.11.161: icmp_seq=1 ttl=64 time=0.438 ms
64 bytes from 192.168.11.161: icmp_seq=2 ttl=64 time=0.313 ms
64 bytes from 192.168.11.161: icmp_seq=3 ttl=64 time=0.262 ms
^C
--- 192.168.11.161 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.262/0.337/0.438/0.076 ms
marta@xps12 ~ % ssh root@192.168.11.161
The authenticity of host '192.168.11.161 (192.168.11.161)' can't be established.
ECDSA key fingerprint is SHA256:0mbvwnC9gFfdXVltdKJ8FaItOXlf9rh8dTST63IzptM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.11.161' (ECDSA) to the list of known hosts.
root@192.168.11.161's password:
Last login: Wed Jun 21 11:24:18 2017
[root@mail ~]# cp /usr/share/doc/clamav-server*/clamd.sysconfig /etc/sysconfig/c
lamd.amavisd
[root@mail ~]#
```

```
root@mail:~  
Archivo Editar Ver Buscar Terminal Ayuda  
ECDSA key fingerprint is SHA256:0mbvwnC9gFfdXVltdKJ8Fa1t0Xlf9rh8dTST63IzptM.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.11.161' (ECDSA) to the list of known hosts.  
root@192.168.11.161's password:  
Last login: Wed Jun 21 11:24:18 2017  
[root@mail ~]# cp /usr/share/doc/clamav-server*/clamd.sysconfig /etc/sysconfig/c  
lamd.amavisd  
[root@mail ~]# vi /etc/sysconfig/clamd.amavisd  
[root@mail ~]# vi /etc/tmpfiles.d/clamd.amavisd.conf  
[root@mail ~]# vi /usr/lib/systemd/system/clamd@.service  
[root@mail ~]# systemctl start clamd@amavisd  
[root@mail ~]# systemctl enable clamd@amavisd  
Created symlink from /etc/systemd/system/multi-user.target.wants/clamd@amavisd.s  
ervice to /usr/lib/systemd/system/clamd@.service.  
[root@mail ~]# vi /etc/amavisd/amavisd.conf  
[root@mail ~]# systemctl start amavisd spamassassin  
[root@mail ~]# systemctl enable amavisd spamassassin  
Created symlink from /etc/systemd/system/multi-user.target.wants/amavisd.service  
to /usr/lib/systemd/system/amavisd.service.  
Created symlink from /etc/systemd/system/multi-user.target.wants/spamassassin.se  
rvice to /usr/lib/systemd/system/spamassassin.service.  
[root@mail ~]# █
```

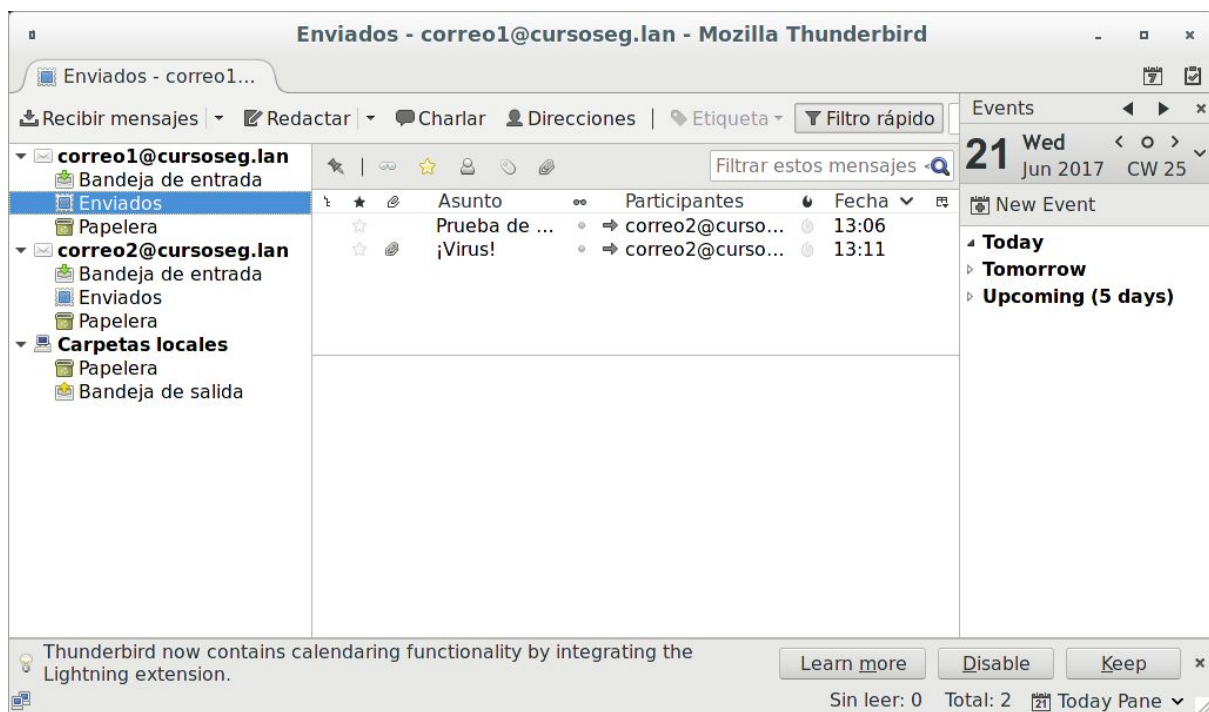
(Si sois lo bastante imprudentes como para usar Windows, podéis hacerlo con Putty)

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):



```
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/amavis/tmp/amavis-20170621T130507-06066-
3XHexzxN/parts/p002: Eicar-Test-Signature FOUND
Jun 21 13:10:31 mail clamd: /var/spool/amavis/tmp/amavis-20170621T130507-06066-
3XHexzxN/parts/p004: Eicar-Test-Signature FOUND
[root@mail ~]#
```