UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Práctica 7
Fail2ban, ClamaV, Postfix y Logwatch

ASIGNATURA

Administración de Sistemas Unix/Linux

ALUMNO

Alexis de Jesus Arizmendi López - 318176110

PROFESOR

Yeudiel Hernández Torres

AYUDANTES

Virgilio Castro Rendón
Raúl Ríos Ciriaco

Fail2ban

1. `sudo aptitude update`

   Actualiza los índices de los repositorios de paquetes. Este paso asegura que la información esté al día antes de instalar cualquier paquete.

2. `sudo aptitude install fail2ban`

   Instala la herramienta Fail2Ban, utilizada para prevenir ataques de fuerza bruta y proteger servicios como SSH.

3. `cd /etc/fail2ban`

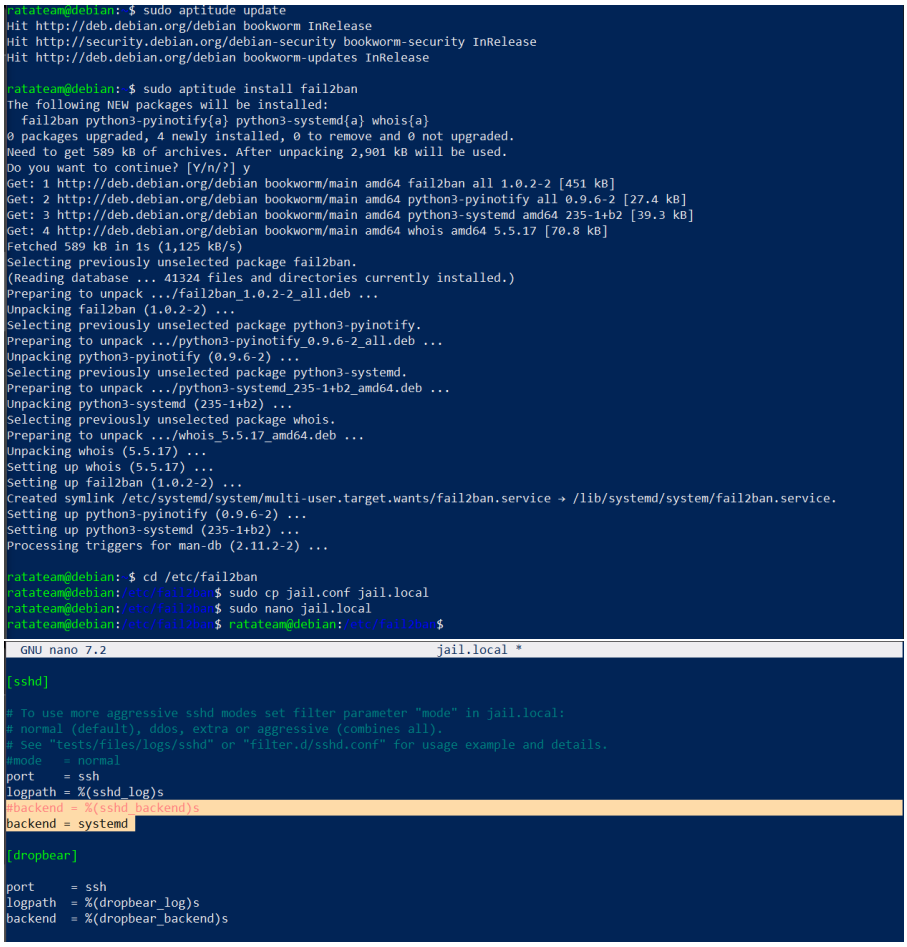
   Cambia el directorio de trabajo al de configuración de Fail2Ban.

4. `sudo cp jail.conf jail.local`

   Crea una copia de seguridad del archivo de configuración principal de Fail2Ban, asegurando que las modificaciones no sean sobrescritas en futuras actualizaciones.

5. `sudo nano jail.local`

   Abre el archivo `jail.local` en el editor `nano` para realizar ajustes específicos en la configuración de Fail2Ban.



6. `sudo systemctl restart fail2ban`

   Reinicia el servicio de Fail2Ban para aplicar los cambios realizados en la configuración.

7. `sudo systemctl status fail2ban`

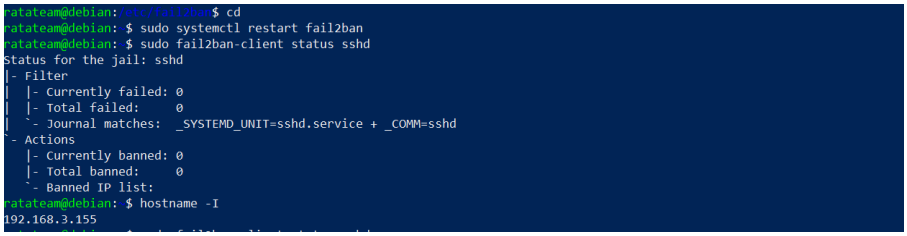
   Verifica nuevamente el estado de Fail2Ban después del reinicio.

8. `sudo systemctl start fail2ban`

   Inicia el servicio Fail2Ban si estaba detenido.

9. `sudo fail2ban-client status sshd`

   Verifica nuevamente el estado del servicio Fail2Ban.



10. `sudo fail2ban-client set sshd unbanip [IP]`

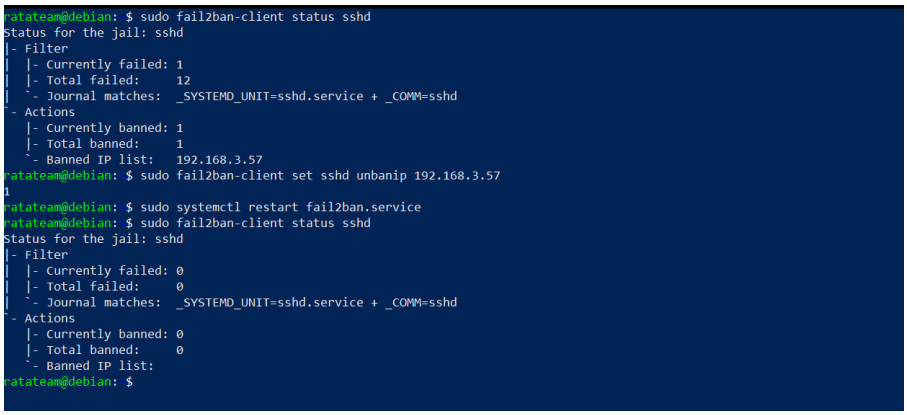
    Desbloquea manualmente una dirección IP específica que había sido bloqueada para el servicio SSH.

11. `sudo fail2ban-client status sshd`

    Revisa nuevamente el estado de Fail2Ban en el servicio SSHD para verificar los cambios después de desbloquear una IP.

12. `sudo systemctl restart fail2ban.service`

    Reinicia el servicio Fail2Ban, asegurando que cualquier cambio o ajuste adicional se aplique correctamente.



ClamaV

1. `sudo aptitude install clamav clamav-daemon`

   Instala ClamAV y su componente `clamav-daemon` para la protección antivirus.

2. `sudo dpkg-reconfigure clamav-daemon`

   Reconfigura el paquete clamav-daemon, lo que te permite ajustar configuraciones específicas del servicio, como opciones de escaneo en tiempo real o configuración de red.

3. `sudo systemctl status clamav-freshclam.service`

   Verifica el estado del servicio clamav-freshclam, que se encarga de actualizar automáticamente la base de datos de firmas de virus en ClamAV.

4. `sudo systemctl enable clamav-freshclam.service`

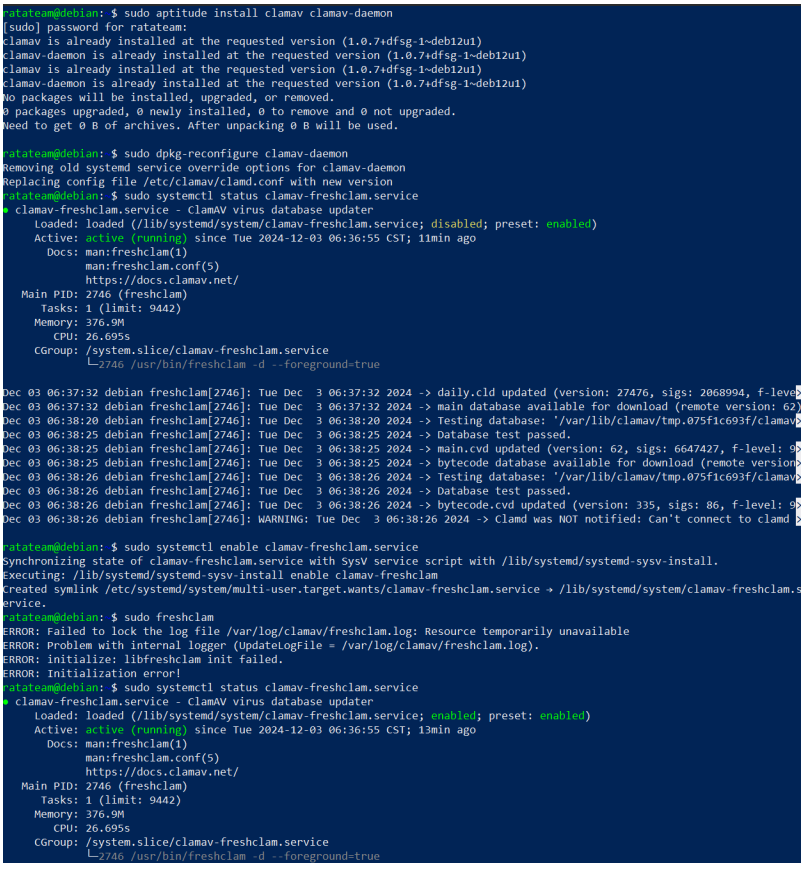
   Activa el servicio clamav-freshclam para iniciar automáticamente al arrancar el sistema.

5. `sudo systemctl start clamav-freshclam.service`

   Inicia el servicio clamav-freshclam si aún no está activo.

6. `sudo freshclam`

   Ejecuta manualmente la actualización de la base de datos de virus de ClamAV usando freshclam, en caso de que el servicio no esté activo o para forzar una actualización.



7. `sudo systemctl stop clamav-freshclam.service`

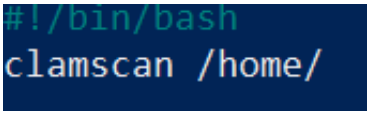
   Detiene el servicio clamav-freshclam como superusuario, similar al comando anterior.

8. `sudo systemctl start clamav-freshclam.service`

   Reinicia el servicio clamav-freshclam después de cualquier actualización o ajuste manual.

9. `sudo nano /etc/cron.daily/clamavscan.sh`

   Crea o edita el archivo de script clamavscan.sh en el directorio de tareas diarias. Este archivo puede contener instrucciones para realizar un escaneo diario con ClamAV.



10. `clamscan /home/`

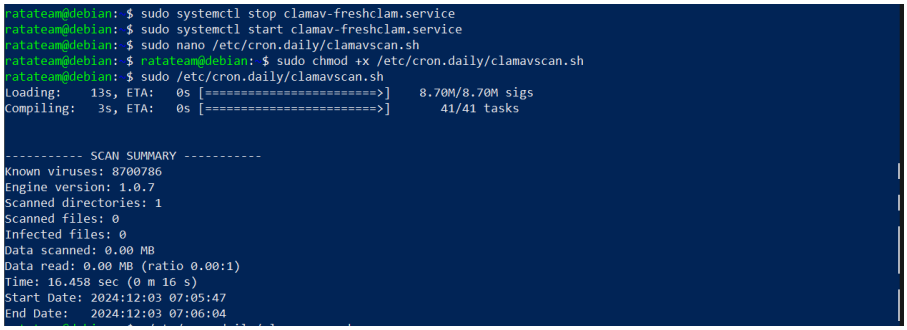
    Ejecuta el comando clamscan, que es la herramienta de escaneo de ClamAV, sobre el directorio /home/. Esto significa que ClamAV analizará todos los archivos y subdirectorios dentro de /home/ en busca de virus y malware. Al finalizar, ClamAV mostrará un resumen con la cantidad de archivos analizados, posibles infecciones y otros detalles.

11. `sudo chmod +x /etc/cron.daily/clamavscan.sh`

    Asigna permisos de ejecución al script clamavscan.sh para que el sistema pueda ejecutarlo automáticamente cada día.

12. `sudo /etc/cron.daily/clamavscan.sh`

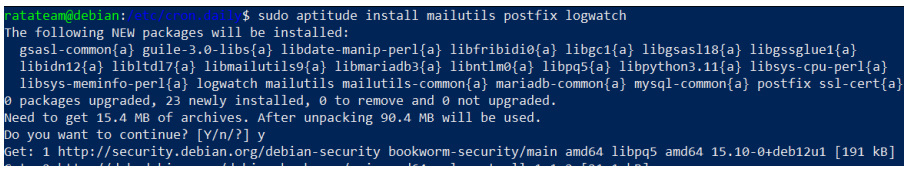
    Ejecuta el script clamavscan.sh manualmente para verificar que funcione correctamente. Esto debería iniciar un escaneo antivirus si el script está bien configurado.



Postfix y Logwatch

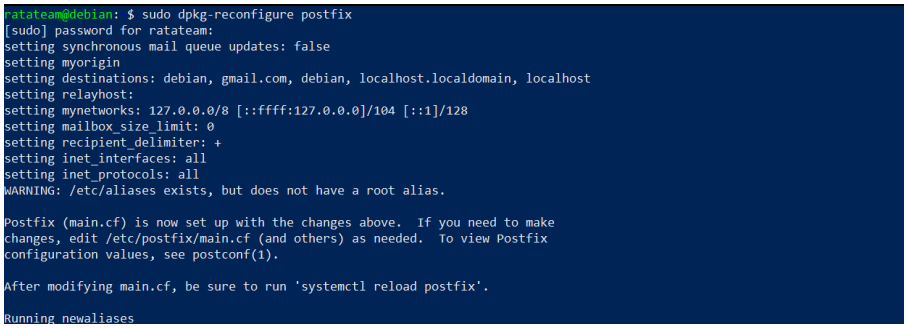
1. `sudo aptitude install mailutils postfix logwatch`

   Instala los paquetes `mailutils`, `postfix` y `logwatch` para la configuración de correo y generación de informes de monitoreo.



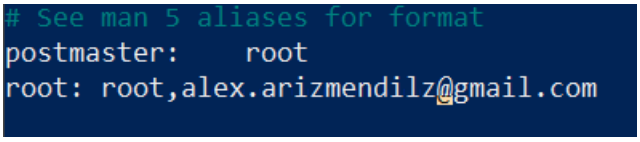
2. `sudo dpkg-reconfigure postfix`

   Reconfigura Postfix para ajustar su funcionamiento según las necesidades del servidor.



3. `sudo nano /etc/aliases`

   Configura alias de correo para redirigir mensajes a las direcciones adecuadas.



4. `sudo newaliases`

   Actualiza la base de datos de alias para que los cambios realizados en el archivo `aliases` tengan efecto.

5. `sudo mkdir /var/cache/logwatch`

   Crea un directorio de caché para Logwatch. Esto almacena datos temporales y ayuda a Logwatch a manejar archivos grandes de registro.

6. `sudo cp /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/`

   Copia el archivo de configuración principal de Logwatch (logwatch.conf) al directorio de configuración en /etc. Aquí puedes personalizar los ajustes de los informes generados.

7. `sudo nano /etc/logwatch/conf/logwatch.conf`

   Abre el archivo logwatch.conf en nano para ajustar configuraciones, como el nivel de detalle del informe, el rango de tiempo y la dirección de correo a la cual se enviará el

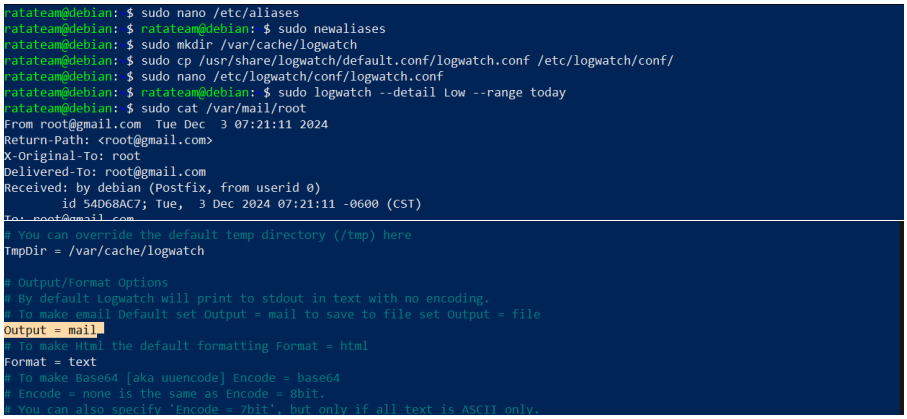
informe.

8. `sudo logwatch --detail Low --range today`

   Ejecuta manualmente Logwatch para generar un informe con los eventos del sistema del día.

9. `sudo cat /var/mail/root`

   Muestra el contenido del buzón de correo de root, donde pueden llegar informes generados por Logwatch si no se han configurado alias de correo adicionales.



10. `sudo nano /etc/cron.daily/00logwatch`

    Abre el archivo de tareas diarias 00logwatch con nano. logwatch genera informes de actividad del sistema y registros importantes, y en este archivo puedes configurar o ajustar su frecuencia y contenido.

11. `sudo nano /etc/cron.weekly/00logwatch`

    Abre el archivo de tareas semanales 00logwatch para configurar escaneos e informes semanales del sistema.