



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.

```
ratateam@debian: $ sudo aptitude update
Hit http://deb.debian.org/debian bookworm InRelease
Hit http://security.debian.org/debian-security bookworm-security InRelease
Hit http://deb.debian.org/debian bookworm-updates InRelease

ratateam@debian: $ sudo aptitude install fail2ban
The following NEW packages will be installed:
  fail2ban python3-pyinotify(a) python3-systemd(a) whois(a)
0 packages upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 589 kB of archives. After unpacking 2,901 kB will be used.
Do you want to continue [Y/n/?] y
Get: 1 http://deb.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2 [451 kB]
Get: 2 http://deb.debian.org/debian bookworm/main amd64 python3-pyinotify all 0.9.6-2 [27.4 kB]
Get: 3 http://deb.debian.org/debian bookworm/main amd64 python3-systemd amd64 235-1+b2 [39.3 kB]
Get: 4 http://deb.debian.org/debian bookworm/main amd64 whois amd64 5.5.17 [70.8 kB]
Fetched 589 kB in 1s (1,125 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 41324 files and directories currently installed.)
Preparing to unpack .../fail2ban_1.0.2-2_all.deb ...
Unpacking fail2ban (1.0.2-2) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../python3-pyinotify_0.9.6-2_all.deb ...
Unpacking python3-pyinotify (0.9.6-2) ...
Selecting previously unselected package python3-systemd.
Preparing to unpack .../python3-systemd_235-1+b2_amd64.deb ...
Unpacking python3-systemd (235-1+b2) ...
Selecting previously unselected package whois.
Preparing to unpack .../whois_5.5.17_amd64.deb ...
Unpacking whois (5.5.17) ...
Setting up whois (5.5.17) ...
Setting up fail2ban (1.0.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
Setting up python3-pyinotify (0.9.6-2) ...
Setting up python3-systemd (235-1+b2) ...
Processing triggers for man-db (2.11.2-2) ...

ratateam@debian: $ cd /etc/fail2ban
ratateam@debian:/etc/fail2ban$ sudo cp jail.conf jail.local
ratateam@debian:/etc/fail2ban$ sudo nano jail.local
ratateam@debian:/etc/fail2ban$ ratateam@debian:/etc/fail2ban$
```

GNU nano 7.2 jail.local *

```
[sshd]
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), dos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = ssh
logpath = %($sshd_log)s
#backend = %($sshd_backend)s
backend = systemd

[dropbear]
port = ssh
logpath = %(dropbear_log)s
backend = %(dropbear_backend)s
```

```
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.

```
ratateam@debian: ~ /var/lib/fail2ban $ cd
ratateam@debian: $ sudo systemctl restart fail2ban
ratateam@debian: $ sudo fail2ban-client status sshd
status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 0
| |- Total banned: 0
| |- Banned IP list:
ratateam@debian: $ hostname -I
192.168.3.155
```

```
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.

```
ratateam@debian: $ sudo fail2ban-client status sshd
status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 12
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 1
| |- Total banned: 1
| |- Banned IP list: 192.168.3.57
ratateam@debian: $ sudo fail2ban-client set sshd unbanip 192.168.3.57
1
ratateam@debian: $ sudo systemctl restart fail2ban.service
ratateam@debian: $ sudo fail2ban-client status sshd
status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 0
| |- Total banned: 0
| |- Banned IP list:
ratateam@debian: $
```

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 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.

```
ratacam@debian: $ sudo aptitude install clamav clamav-daemon
[sudo] password for ratacam:
clamav is already installed at the requested version (1.0.7+dfsg-1~deb12u1)
clamav-daemon is already installed at the requested version (1.0.7+dfsg-1~deb12u1)
clamav is already installed at the requested version (1.0.7+dfsg-1~deb12u1)
clamav-daemon is already installed at the requested version (1.0.7+dfsg-1~deb12u1)
No packages will be installed, upgraded, or removed.
0 packages upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B of archives. After unpacking 0 B will be used.

ratacam@debian: $ sudo dpkg-reconfigure clamav-daemon
Removing old systemd service override options for clamav-daemon
Replacing config file /etc/clamav/clamd.conf with new version
ratacam@debian: $ sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; disabled; preset: enabled)
   Active: active (running) since Tue 2024-12-03 06:36:55 CST; 1min ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
      Main PID: 2746 (freshclam)
         Tasks: 1 (limit: 9442)
        Memory: 376.9M
          CPU: 26.695s
         CGroup: /system.slice/clamav-freshclam.service
                   └─2746 /usr/bin/freshclam -d --foreground=true

Dec 03 06:37:32 debian freshclam[2746]: Tue Dec  3 06:37:32 2024 -> daily.cld updated (version: 27476, sigs: 2068994, f-level: 62)
Dec 03 06:37:32 debian freshclam[2746]: Tue Dec  3 06:37:32 2024 -> main database available for download (remote version: 62)
Dec 03 06:38:25 debian freshclam[2746]: Tue Dec  3 06:38:25 2024 -> Testing database: '/var/lib/clamav/tmp.075f1c693f/clamav'
Dec 03 06:38:25 debian freshclam[2746]: Tue Dec  3 06:38:25 2024 -> Database test passed.
Dec 03 06:38:25 debian freshclam[2746]: Tue Dec  3 06:38:25 2024 -> main.cvd updated (version: 62, sigs: 6647427, f-level: 62)
Dec 03 06:38:25 debian freshclam[2746]: Tue Dec  3 06:38:25 2024 -> bytecode database available for download (remote version: 62)
Dec 03 06:38:26 debian freshclam[2746]: Tue Dec  3 06:38:26 2024 -> Testing database: '/var/lib/clamav/tmp.075f1c693f/clamav'
Dec 03 06:38:26 debian freshclam[2746]: Tue Dec  3 06:38:26 2024 -> Database test passed.
Dec 03 06:38:26 debian freshclam[2746]: Tue Dec  3 06:38:26 2024 -> bytecode.cvd updated (version: 335, sigs: 86, f-level: 62)
Dec 03 06:38:26 debian freshclam[2746]: WARNING: Tue Dec  3 06:38:26 2024 -> Clamd was NOT notified: Can't connect to clamd

ratacam@debian: $ sudo systemctl enable clamav-freshclam.service
Synchronizing state of clamav-freshclam.service with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-freshclam
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.

ratacam@debian: $ sudo freshclam
ERROR: Failed to lock the log file /var/log/clamav/freshclam.log: Resource temporarily unavailable
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
ratacam@debian: $ sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-12-03 06:36:55 CST; 1min ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
      Main PID: 2746 (freshclam)
         Tasks: 1 (limit: 9442)
        Memory: 376.9M
          CPU: 26.695s
         CGroup: /system.slice/clamav-freshclam.service
                   └─2746 /usr/bin/freshclam -d --foreground=true
```

```
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.

```
#!/bin/bash  
clamscan /home/
```

```
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.

```
ratateam@debian: $ sudo systemctl stop clamav-freshclam.service  
ratateam@debian: $ sudo systemctl start clamav-freshclam.service  
ratateam@debian: $ sudo nano /etc/cron.daily/clamavscan.sh  
ratateam@debian: $ ratateam@debian: $ sudo chmod +x /etc/cron.daily/clamavscan.sh  
ratateam@debian: $ sudo /etc/cron.daily/clamavscan.sh  
Loading: 13s, ETA: 0s [=====>] 8.70M/8.70M sigs  
Compiling: 3s, ETA: 0s [=====>] 41/41 tasks  
  
----- SCAN SUMMARY -----  
Known viruses: 8700786  
Engine version: 1.0.7  
Scanned directories: 1  
Scanned files: 0  
Infected files: 0  
Data scanned: 0.00 MB  
Data read: 0.00 MB (ratio 0.00:1)  
Time: 16.458 sec (0 m 16 s)  
Start Date: 2024:12:03 07:05:47  
End Date: 2024:12:03 07:06:04
```

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.

```
ratateam@debian: /etc/cron.daily$ sudo aptitude install mailutils postfix logwatch
The following NEW packages will be installed:
  gsasl-common{a} guile-3.0-libs{a} libdate-manip-perl{a} libfribidio0{a} libgc1{a} libgsasl18{a} libgssglue1{a}
  libidn12{a} libltdl17{a} libmailutils9{a} libmariadb3{a} libntl10{a} libpq5{a} libpython3.11{a} libsys-cpu-perl{a}
  libsys-meminfo-perl{a} logwatch mailutils mailutils-common{a} mariadb-common{a} mysql-common{a} postfix ssl-cert{a}
0 packages upgraded, 23 newly installed, 0 to remove and 0 not upgraded.
Need to get 15.4 MB of archives. After unpacking 90.4 MB will be used.
Do you want to continue? [Y/n/?] y
Get: 1 http://security.debian.org/debian-security bookworm-security/main amd64 libpq5 amd64 15.10-0+deb12u1 [191 kB]
...[redacted]
```

2. sudo dpkg-reconfigure postfix

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

```
ratateam@debian: $ sudo dpkg-reconfigure postfix
[sudo] password for ratateam:
setting synchronous mail queue updates: false
setting myorigin
setting destinations: debian, gmail.com, debian, localhost.localdomain, localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [:1]/128
setting mailbox size limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with the changes above. If you need to make
changes, edit /etc/postfix/main.cf (and others) as needed. To view Postfix
configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
```

3. sudo nano /etc/aliases

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

```
# See man 5 aliases for format
postmaster:    root
root:   root,alex.arizmendiz@gmail.com
```

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.

```
ratateam@debian: $ sudo nano /etc/aliases
ratateam@debian: $ ratateam@debian: $ sudo newaliases
ratateam@debian: $ sudo mkdir /var/cache/logwatch
ratateam@debian: $ sudo cp /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/
ratateam@debian: $ sudo nano /etc/logwatch/conf/logwatch.conf
ratateam@debian: $ ratateam@debian: $ sudo logwatch --detail Low --range today
ratateam@debian: $ sudo cat /var/mail/root
From root@gmail.com Tue Dec 3 07:21:11 2024
Return-Path: <root@gmail.com>
X-Originial-To: root
Delivered-To: root@gmail.com
Received: by debian (Postfix, from user id 0)
          id 54D68AC7; Tue, 3 Dec 2024 07:21:11 -0600 (CST)
To: root@gmail.com
# You can override the default temp directory (/tmp) here
TmpDir = /var/cache/logwatch

# Output/Format Options
# By default logwatch will print to stdout in text with no encoding.
# To make email Default set Output = mail to save to file set Output = file
Output = mail
# to make html the default formatting Format = html
Format = text
# To make Base64 [aka uuencode] Encode = base64
# Encode = none is the same as Encode = 8bit.
# You can also specify 'Encode = 7bit', but only if all text is ASCII only.
```

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.

```
#!/bin/bash

#Check if removed-but-not-purged
test -x /usr/share/logwatch/scripts/logwatch.pl || exit 0

#execute
/usr/sbin/logwatch --output mail

#Note: It's possible to force the recipient in above command
#Just pass --mailto address@a.com instead of --output mail
```