Fail2ban para HTTP

Anti - DoS con fail2ban (WebSites [ports:80/443])

Implementacion de anti-DoS con fail2ban en Sistema Operativo Debian 9

Instalar los paquetes “fail2ban” y “iptables-persistent”

```
~$ sudo apt-get install iptables-persistent fail2ban
```

Modificar la configuracion por defecto de fail2ban y agregar las siguientes lineas al archivo mencionado

```
~$ vim /etc/fail2ban/jail.conf
```

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
[http-get-dos]
enabled = true
port = http,https
filter = http-get-dos
# Cambiar a la ruta de los logs de Apache/Nginx/etc..
logpath = /var/log/*apache2*/*access.log
maxretry = 300
findtime = 300
#ban por 5 minutos
bantime = 600
action = iptables[name=HTTP, port=http, protocol=tcp]
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Crear un archivo en la ruta correspondiente con el siguiente contenido

```
~$ vim /etc/fail2ban/filter.d/http-get-dos.conf
```

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
# Fail2Ban archivo de configuracion
[Definition]
# Opcion: failregex
# Se debe configurar el maxretry y findtime en jail.conf muy cuidadosamente para evitar los falsos positivos.
failregex = ^<HOST> -.*"(GET|POST).*
# Optcion: ignoreregex (El IP de este campo no sera bloqueado)
ignoreregex =
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Reiniciar el servicio de fail2ban

```
~$ sudo systemctl restart fail2ban.service
```

Para revisar las IP bloqueados

```
~$ sudo iptables -nvL
```

Remover IP “banneada”

```
//Desplegara las reglas que creamos en este caso seria http-get-dos
~$ sudo fail2ban-client status
//Elimina la IP "banneada"
~$ sudo fail2ban-client set http-get-dos unbanip <IP_ADDRESS>
```

Revision #3
Created 10 marzo 2023 11:35:50 by Franz Rojas
Updated 3 abril 2025 12:30:23 by Vladimir Urquiola