GUÍA DE SEGURIDAD

Boletín Nro.: 2016-02
Fecha de publicación: 25/08/2016
Tema: Instalación y configuración de Fail2ban adaptado a Zimbra

Fail2ban es una aplicación escrita en Python, para la prevención de intrusos en un sistema, que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta. Funciona en sistemas POSIX que tengan interfaz con un sistema de control de paquetes o un firewall local, como iptables o TCP Wrapper.
Fail2ban monitorea los registros (*logs*) de los programas que se especifiquen en busca de las reglas definidas por el usuario para poder aplicar una determinada penalización (bloqueo de la aplicación en un determinado puerto, bloquearla para todos los puertos, bloquear la cuenta afectada etc.), también definida por el usuario. Ante una cantidad predefinida (por el usuario) de intentos fallidos, fail2ban determina la acción a tomar sobre la IP que originó el problema. Las acciones son configurables mediante scripts de Python.
De esta manera se reduce no solo la sobrecarga de red provocada por los ataques, sino también la probabilidad de que un ataque de fuerza bruta tenga éxito.

Instrucciones:

1) Instalar el paquete fail2ban
   Para Centos: *
   ```
   # yum install fail2ban
   ```
   Para Ubuntu:
   ```
   # apt-get install fail2ban
   ```

   En caso de que utilice otra distribución de Linux, puede instalarlo manualmente, descargándolo desde: https://github.com/fail2ban/fail2ban
   * Obs.: debe contar con los repositorios EPAL (Fedora Extra Packages for Enterprise Linux)
   ```
   # yum install epel-release
   ```


CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

2) Crear el archivo **/etc/fail2ban/filter.d/zimbra.conf** con el siguiente contenido

```
#Fail2Ban configuration file
#
# Author:
#
# $Revision: 1 $
#

[Definition]

# Option:  failregex
# Notes.:  regex to match the password failures messages in the logfile. The
#          host must be matched by a group named "host". The tag "<HOST>" can
#          be used for standard IP/hostname matching and is only an alias for
#          (?::::f{4,6}:)?(?P<host>[\w\-.^_]+)
# Values:  TEXT
#
failregex = \[ip=<HOST>;\] account - authentication failed for .* \(no such account\)$
                        \[ip=<HOST>;\] security - cmd=Auth; .* error=authentication failed for .*, invalid password;$
                        ;oip=<HOST>;.* security - cmd=Auth; .* protocol=soap; error=authentication failed for .* invalid
password;$
                        \[oip=<HOST>;.* SoapEngine - handler exception: authentication failed for .*, account not
found$
                        WARN .*;ip=<HOST>;ua=ZimbraWebClient .* security - cmd=AdminAuth; .* error=authentication
failed for .*;$
                        NOQUEUE: reject: RCPT from .*\[<HOST>\]: 550 5.1.1 .*: Recipient address rejected:
                        warning: .*\[<HOST>\]: SASL .* authentication failed: authentication failure

# .*\[ip=<HOST>;\] .* - authentication failed for .* \(invalid password\)
#
# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
```


CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

3) Crear el archivo **/etc/fail2ban/jail.local** con el siguiente contenido:

```
[DEFAULT]
ignoreip = 127.0.0.1/8
# ---
# cert@cert.gov.py
# si existe <maxretry> intentos fallidos en <findtime> banearlo por <bantime>
#---
bantime = 3600
findtime = 3600
maxretry = 5
backend = auto

[zimbra-account]
enabled = true
filter = zimbra
action = iptables-allports[name=zimbra-account]
sendmail[name=zimbra-account, dest=destino@midominio.gov.py]
logpath = /opt/zimbra/log/mailbox.log
# cert@cert.gov.py: <bantime> por 10 minutos cuando se ingresa mal el password via webmail
bantime = 600

[zimbra-audit]
enabled = true
filter = zimbra
action = iptables-allports[name=zimbra-audit]
sendmail[name=zimbra-audit, dest=destino@midominio.gov.py]
logpath = /opt/zimbra/log/audit.log

[zimbra-recipient]
enabled = true
filter = zimbra
action = iptables-allports[name=zimbra-recipient]
sendmail[name=zimbra-recipient, dest=destino@midominio.gov.py]
logpath = /var/log/zimbra.log
# cert@cert.gov.py: <bantime> = -1 es banear en forma permanente
bantime = -1

[postfix]
enabled = true
filter = postfix
action = iptables-multiport[name=postfix, port=smtp, protocol=tcp]
sendmail-buffered[name=Postfix, dest=destino@midominio.gov.py]
logpath = /var/log/zimbra.log
# cert@cert.gov.py: <bantime> = -1 es banear en forma permanente
bantime = -1
```

* Obs.: en el campo "dest" debe poner el correo electrónico de la persona que va a recibir las alertas de bloqueos de IPs.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

4) Editar el archivo **/etc/fail2ban/action.d/sendmail.conf** y modificar la línea:

Fail2Ban" | /usr/sbin/sendmail -f <sender> <dest>

por:

Fail2Ban" | /opt/zimbra/postfix/sbin/sendmail -f <sender> <dest>

5) Inicializar el servicio: **/etc/init.d/fail2ban start**

6) Verificación de funcionamiento:
   a) **fail2ban-client status**
   b) **fail2ban-client status zimbra-recipient**

Cuando está operativo en la parte de **Actions -> Banned IP list** estarán los IPs bloqueados

```
[root@correo fail2ban]# fail2ban-client status
Status
|- Number of jail:    4
`- Jail list:    postfix, zimbra-account, zimbra-audit, zimbra-recipient


[root@correo fail2ban]# fail2ban-client status zimbra-recipient
Status for the jail: zimbra-recipient
|- Filter
|  |- Currently failed:    0
|  |- Total failed:    5
|  `- File list:    /var/log/zimbra.log
`- Actions
   |- Currently banned:    29
   |- Total banned:    29
   `- Banned IP list:    103.237.147.20 103.3.46.15
```

Obs.: Para verificar los intentos fallidos y bloqueos vía webmail, el comando es:
fail2ban-client status zimbra-account

Información adicional:

http://www.fail2ban.org

https://www.vavai.net/2011/10/tips-improving-zimbra-mail-server-security-with-fail2ban/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 | + 595 962 271071
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py