Instalación de Fail2ban

Sumario

Introducción a Fail2ban

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. Se distribuye bajo licencia GNU y típicamente funciona en sistemas POSIX que tengan interfaz con un sistema de control de paquetes o un firewall local (como iptables o TCP Wrapper).

Funcionamiento

Habitualmente las computadoras sufren **Ataques de fuerza bruta** (especialmente servidores SSH,FTP, etc) con el fin de descifrar las contraseñas y acceder a ellas. En este punto es indispensable una buena política de contraseñas. Sin embargo, los ataques por fuerza bruta también consumen un gran ancho de banda, disparan el volumen de los *logs* de nuestro sistema y ocupan ciclos de CPU que podrían dedicarse a tareas útiles.

Fail2ban busca en los registros (*logs*) de los programas que se especifiquen las reglas que el usuario decida para poder aplicar una penalización. La penalización puede ser bloquear la aplicación que ha fallado en un determinado puerto, bloquearla para todos los puertos, etc. Las penalizaciones, así como las reglas, son definidas por el usuario.

Habitualmente, si las IP de ataque se prohíben por un lapso prudencial de tiempo, la sobrecarga de red provocada por los ataques baja, y también se reduce la probabilidad de que un ataque de fuerza bruta basada en diccionarios tenga éxito.

Ante una cantidad predefinida (por el usuario) de intentos fallidos, fail2ban determina la acción a tomar sobre la IP que originó el problema. Puede simplemente notificar por e-mail del suceso, denegar el acceso a la IP atacante, bloquearla en determinado puerto y habilitarla en otros (modificando las entradas correspondientes en iptables, o el firewall local que corresponda), etc. Puede asimismo levantar las prohibiciones después de un determinado periodo, por si el problema no obedeciera a un ataque sino simplemente a errores del usuario intentando loguearse. Las acciones son configurables mediante scripts de Python.

Instalación de Fail2ban

```
# Instalación de fail2ban
apt-get install fail2ban

cd /etc/fail2ban
cp jail.conf jail.local
nano /etc/fail2ban/jail.local

[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host
ignoreip = 127.0.0.1/8 10.0.0.6

# 60 minutos = 60*60 = 3600
findtime= 1800

# 6 horas de ban = 3600*6 = 21600
bantime  = 21600
maxretry = 3

.......

#
# Destination email address used solely for the interpolations in
# jail.{conf,local} configuration files.
destemail = ceca@iessanclemente.net
sendername = Fail2Ban-Alertas
```

```
.......

# email action. Since 0.8.1 upstream fail2ban uses sendmail
# MTA for the mailing. Change mta configuration parameter to mail
# if you want to revert to conventional 'mail'.
mta = mail

.......

# Choose default action.  To change, just override value of 'action' with the
# interpolation to the chosen action shortcut (e.g.  action_mw, action_mwl, etc) in jail.local
# globally (section [DEFAULT]) or per specific section
#action = %(action_)s

# Para notificación por mail.
action = %(action_mwl)s

[ssh]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3

[dropbear]
enabled  = false
port     = ssh
filter   = sshd
logpath  = /var/log/dropbear
maxretry = 3

[ssh-ddos]
enabled  = false
port     = ssh
filter   = sshd-ddos
logpath  = /var/log/auth.log
maxretry = 3

# Ejecutar estas líneas para añadir el host en los correos que llegan de fail2ban.

find /etc/fail2ban/action.d/ -type f -exec sed -i 's/\[Fail2Ban\]/\[Fail2Ban@\<hostname\>\]/g' {} \;
files=$(grep -ir hostname /etc/fail2ban/action.d/ | awk -F ':' '{print $1}' | sort -u); for f in $files; do echo "hostname = \`/bin/h

# Revisar el fichero o añadir más información en los mails en:

nano /etc/fail2ban/action.d/mail.conf
```

Borrado de una IP Baneada

```
#El comando para borrar una IP baneada es el siguiente:

fail2ban-client set JAILNAMEHERE unbanip IPADDRESS

# Para averiguar el nombre del JAIL iremos a /etc/fail2ban/jail.local y podremos ver todas las configuraciones. Por ejemplo para ssh

# Si tecleamos:
iptables -L -n

# Se nos muestran las IP's baneadas y en qué cadena están, por ejemplo la cadena f2b-sshd. (sshd será el nombre del jail).

# Por ejemplo eliminar una IP del ban, en el jail de SSH haremos:

fail2ban-client set sshd unbanip 125.56.49.22
```

Veiga (discusión) 09:14 8 feb 2018 (CET)