24 mar 2013

Instalando Fail2ban com Asterisk

Escrito por Jean Carlos Coelho.

Fail2ban é um serviço que monitora os logs de diversos serviços em busca de uma expressão regular específica definida em suas configurações. Assim o atacante que efetuar diversas tentativas de acesso em um determinado serviço (no nosso caso Asterisk)

por X vezes em um pequeno intervalo de tempo, será automaticamente bloqueado através do iptables (Linux), por 3600 segundos (padrão).

Lembrando que a idéia aqui é explanar a adição de serviços customizados (como Asterisk), uma vez que pode

ser criado regras para qualquer tipo de serviço exposto para a internet (que trabalhe com processos de autenticação), ou até mesmo ativar o que já vem por padrão no produto. Você precisa apenas saber o que coletar nos logs do serviço, para criar suas expressões regulares.

Download

Para dar início as configurações, vamos efetuar o download do produto no seguinte endereço:

Link do Projeto: http://www.fail2ban.org/wiki/index.php/Downloads

Link de Download: http://sourceforge.net/projects/fail2ban/files/

Neste documento estaremos usando a versão fail2ban-0.8.4.tar.bz2você pode efetuar o download de uma versão mais atual, lembre-se de sempre usar um source estável. Após o baixar o pacote, precisaremos descompactar o arquivo, para isso precisaremos do pacote bzip2, caso esteja inexistente no seu sistema, você deverá instalar este pacote, no Debian, basta seguir estes procedimentos:

```
# apt-get update

# apt-get install bzip2
```

Para descompactar o pacote:

```
# tar -xvf fail2ban-0.8.4.tar.bz2
```

Após descompactar o pacote, o ideal é que o arquivo README seja lido com atenção, adiantando o processo, um requisito do produto (contido no leia-me, seria a versão do Python >= ao 2.3). Instale-o:

```
# apt-get update

# apt-get install python (ou python2.4)
```

Agora estamos prontos para instalação e configuração! Lembre-se sempre de ler a documentação do produto para desenvolver novas features ou modificar qualquer item não incluso neste manual durante o procedimento de instalação.

Instalação

```
# cd fail2ban-0.8.4

# python setup.py install
```

Feito isso, o produto estará instalado no seu sistema operacional, no diretório: /usr/share/fail2ban ou em/usr/local/share/fail2ban. Não vamos editar nada neste diretório. O que interessa neste momento é a verificação da existência dos arquivos binários no nosso PATH, O comando a seguir deverá exibir a versão do produto:

```
# fail2ban-server -V


Fail2Ban v0.8.4


Copyright (c) 2004-2008 Cyril Jaquier

Copyright of modifications held by their respective authors.

Licensed under the GNU General Public License v2 (GPL).


Written by Cyril Jaquier < cyril.jaquier@fail2ban.org>.

Many contributions by Yaroslav O. Halchenko < debian@onerussian.com>.
```

Repita o procedimento para os outros executáveis para confirmar suas existências:

```
# fail2ban-client -V

# fail2ban-regex -V
```

OBS:Caso não consiga visualizar as informações do produto, você deverá adicionar o PATH dos executáveis ao seu .bashrcou adicioná-los ao PATH do usuário root.

OBS: As novas versões do produto, criam as pastas automaticamente, sem a necessidade da execução dos dois procedimentos abaixo, antes de executad estes procedimentos, verifique se as pastas já existem em seu sistema, caso sim, prossiga para script de inicializaçãoe configurações.

Agora vamos criar os diretórios de configurações do serviço. No Debian as configurações padrão seriam:

```
# mkdir -p /etc/fail2ban

# chown root.root /etc/fail2ban -R
```

Copie o conteúdo da pasta “config”no diretório de instalação do produto para: /etc/fail2banda seguinte forma:

```
# cp -arv /root/fail2ban-0.8.4/config/* /etc/fail2ban
```

Script de Inicialização

O pacote source não contém o script de inicialização automática (RC’s), portanto é necessário copiá-lo no site do projeto e salvá-lo em nosso sistema operacional, crie o arquivo “/etc/init.d/fail2ban” e no link abaixo, copie o script de inicialização:

http://www.fail2ban.org/wiki/index.php/MANUAL_0_8

O Script está no Item 2.2 “Installing from sources on a GNU/Linux system”

Apenas alguns ajustes serão necessários neste script, vamos precisar organizar o PATH (caso necessário. No meu caso, os executáveis estão em /usr/local/bin), edite no arquivo “/etc/init.d/fail2ban”as seguintes linhas:

```
(Linha 19 ADD) PATH=/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/bin/

(Linha 25 EDIT)DAEMON=/usr/local/bin/$NAME-client
```

Salve e saia do arquivo, aplique permissões de execução para o arquivo:

```
# cd /etc/init.d/

# chmod +x fail2ban
```

Inicie o serviço e verifique o status de funcionamento:

```
# /etc/init.d/fail2ban start

[ ok ] Starting authentication failure monitor: fail2ban.


# netstat -nlp | grep fail2ban

LISTENING 10580 5111/python /var/run/fail2ban/fail2ban.sock


# tail -f /var/log/fail2ban.log

fail2ban.server : INFO Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.4
```

Agora que o serviço está ativo em execução, vamos definir sua inicialização automática no Sistema Operacional:

```
# cd /etc/init.d/

# update-rc.d -f fail2ban defaults

update-rc.d: using dependency based boot sequencing
```

```
#
```

Configuração

Por padrão as configurações do fail2ban estão no arquivo “jail.conf”localizado em: “/etc/fail2ban/”, para começar a monitorar o Asterisk, devemos adicionar no final deste arquivo as seguintes configurações:

```
#
# Asterisk - Opens Tecnologia
#
[asterisk]
enabled = true
filter = asterisk
action = iptables-allports[name=asterisk, protocol=all]
sendmail-whois[name=Asterisk, dest= TI@EMPRESA.com.br, sender= security@CLIENTE.com.br]
logpath = /var/log/asterisk/full
maxretry = 5
bantime = 172800
```

Outra configuração importante no arquivo “/etc/fail2ban/jail.conf”, seria:

ignoreipela é responsável por não bloquear a própria máquina, a rede interna do cliente, ou qualquer IP Externo que deva conectar ao serviço Asterisk ou qualquer outro serviço monitorado pelo fail2ban, sendo assim, configure da seguinte forma:

```
ignoreip = 127.0.0.1 192.168.0.0/24 200.200.200.200 100.100.100.100
```

Com a configuração do Asterisk criada em “/etc/fail2ban/jail.conf”e o ignoreip devidamente setado para não bloquear nossas redes, precisamos agora criar o arquivo responsável pela leitura de logs do Asterisk.

Dentro de “/etc/fail2ban/filter.d”crie o arquivo “asterisk.conf”

ATENÇÃO: O nome do arquivo criado na pasta “/etc/fail2ban/filter.d/”deve ser IGUAL ao nome dado na opção “filter”para cada serviço no “jail.conf”, ou seja, se eu tenho uma filter chamada asterisk, meu arquivo deve ser chamar asterisk.confdentro da pasta “/etc/fail2ban/filter.d/”

```
# cd /etc/fail2ban/filter.d

# vi asterisk.conf
```

As expressões regulares para monitoramento do asterisk 1.4 e 1.8 estão na página seguinte, vamos relembrar o funcionamento do serviço (lógica):

- O fail2ban escuta os logs do asterisk através da instrução Asterisk no arquivo “jail.conf”
- A escuta dos logs espera as expressões regulares configuradas em “asterisk.conf” dentro da pasta “filter.d”
- Caso alguma linha do log case com as expressões regulares do arquivo asterisk.conf na pasta “filter.d”, é executado a instrução “iptables-allports” e “sendmail-whois”, configurado no “jail.conf” para o Asterisk;
- O valor <HOST> coletado pelo “asterisk.conf” é bloqueado no iptables em todas as interfaces da central IP (bloqueio total do IP agressor) e um email é enviado para os responsáveis pela central, após o timeout padrão da instrução Asterisk (bantime), o IP é liberado.

```
# Fail2Ban configuration file

#

#

# $Revision: 250 $

#
```

```
[INCLUDES]

[Definition]

#_daemon = asterisk

# 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>\S+)

# Values: TEXT

#

# Asterisk 1.4 use the following failregex

failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - No matching peer found

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Username/auth name mismatch

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Device does not match ACL

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Peer is not supposed to register

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - ACL error (permit/deny)

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Device does not match ACL

NOTICE.* <HOST> failed to authenticate as '.*'$

NOTICE.* .*: No registration for peer '.*' \(from <HOST>\)

NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)

NOTICE.* .*: Failed to authenticate user .*@<HOST>.*


# In Asterisk 1.8 use the same as above, but after <HOST> add :.* before the single quote.
This is because in Asterisk 1.8, the log file includes a port number which 1.4 did not.
```

```
# Option: ignoreregex

# Notes.: regex to ignore. If this regex matches, the line is ignored.

# Values: TEXT

#

ignoreregex =
```

Salve o arquivo, reinicie o serviço e seja feliz! :)

Autor: Jean Carlos Coelho

Revisão: 01 - 21/03/2013

Ambientes: Debian Etch / Squeeze / Wheezy

Adicionar comentário

Nome (obrigatório)

E-mail (obrigatório)

Website

1000 caracteres

Notifique-me de comentários futuros

Atualizar

Enviar

JComments

Tweetar +1 Like

RSS

Entradas do Feed

escreva

Você tem um artigo que gostaria de publicar ?

Quer saber como ?

1. Envie-nos um E-mail solicitando sua liberação (não esqueça de informar seu

nome de login).

2. Uma vez liberado, faça o Login.

3. Clique aqui e escreva seu artigo.