

Iptables Log Analyzer

Autor: Luiz Cezar Quaquio

Convenções utilizadas neste documento:

- O símbolo "#" significa que o comando deve ser executado como root;
- O símbolo "\$" significa que o comando deve ser realizado como usuário;
- O símbolo ">" é o prompt do MySQL.

Para o Iptables Log Analyzer funcionar é necessário os seguintes pacotes instalados:

- Apache
- MySQL
- PHP5
- Perl

Baixe o arquivo do Iptables Log Analyzer e descompacte:

```
$ wget -c http://www.gege.org/iptables/iptables_logger_v0.4.tar.gz  
$ tar zxvf iptables_logger_v0.4.tar.gz
```

Configure o banco de dados conforme abaixo:

```
$ mysql -u root -p  
> create database iptables  
> grant create,select,insert,update on iptables.* to iptables_admin@localhost identified by 'xx';  
> grant select,insert,update on iptables.* to iptables_user@localhost identified by 'xx';  
> grant create temporary tables on iptables.* to iptables_user@localhost identified by 'xx';
```

Depois, é só efetuar os seguintes comandos :

```
$ cd iptables  
$ mysql -u root -p iptables < sql/db.sql
```

Prepare o arquivo **feed_db.pl**, que fará a leitura dos logs do iptables :

```
$ cd ../scripts  
$ vi feed_db.pl
```

Deixe desse jeito:

```
my $dsn = 'DBI:mysql:iptables:localhost';  
my $db_user_name = 'iptables_admin';  
my $db_password = 'xxxx';  
my $log_file = '/var/log/messages';  
my $pid_file = "/var/run/iptableslog.pid"  
my($log_tag)="IPTABLES";
```

A variável **\$log_file**, é a linha onde o seu firewall grava os logs. A maioria grava direto no messages, mas em alguns casos (com edição do syslog-ng e syslog comum), você pode jogar os logs do iptables para um arquivo específico e a variável **\$log_tag** coloque o que o seu Iptables loga em -log-prefix.

Mova os arquivos **feed_db.pl** e **iptableslog**:

```
# mv fee_db.pl /usr/local/bin/  
# mv iptableslog /etc/init.d/
```

Edite a linha 22 do arquivo **iptableslog** e deixe conforme abaixo:

```
# vi /etc/init.d/iptableslog
```

Altere para:

```
start-stop-daemon --start --quiet --pidfile /var/run/$NAME.pid --exec $DAEMON &
```

O próximo passo tem que saber em qual diretório de sua distribuição o apache tem seu SERVER ROOT setado, ou seja, onde está configurado o diretório padrão de arquivos web no seu server.

No Debian ficará dessa maneira :

```
$ cd ..  
# cp -R web /var/www/iptables
```

Dentro do diretório onde estão os arquivos web edite o arquivo config.php:

```
# cd /var/www/iptables  
# vi config.php
```

Deixe assim:

```
# Host do banco de dados MySQL  
$db_host="localhost";  
# Usuario da base mysql  
$db_user="iptables_user";  
# Senha da sua base mysql MySQL database  
$db_password="suporte";  
# Nome da database  
$db_name="iptables";  
# Endereço url da sua instalação, do tipo http://seuservidor.com.br/iptables  
$url_base="/iptables/";
```

Inclua o arquivo *iptableslog* na inicialização do sistema, no Debia seria:

```
# update-rc.d iptablelog defaults
```

Inicie o arquivo para capturar os dados:

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

Tudo pronto acesse do seu navegador favorito:

```
http://<ipdamaquina>/iptables
```

*** DICA ***

Se o Iptables Log Analyzer não capturar o mês corretamente e no banco de dados a data ficar toda zerada (0000-00-00 00:00:00) não aparecerá nada na tela inicial, por isso é necessário fazer algumas alterações no script de captura do Iptables Log Analyzer. Edite o arquivo *feed_db.pl*:

```
# vi /caminho/feed_db.pl
```

Abaixo da linha com o texto *\$year += 1900;*, linha 107, coloque o seguinte:

```
use strict;  
my($monthnum);  
if ($m{shift(@entry_split)} == ""){  
    my ($second, $minute, $hour, $dayOfMonth, $month, $yearOffset, $dayOfWeek, $dayOfYear,  
$daylightSavings) = localtime();  
    $monthnum = $month + 1;  
}  
else {  
    $monthnum = $m{shift(@entry_split)};  
}  
$entry{'date'}="$year-".$monthnum."-".shift(@entry_split)." ".shift(@entry_split);
```

Comente a antiga linha que recebe a data com “#” no início:

```
#$entry{'date'}="$year-".$m{shift(@entry_split)}."-".shift(@entry_split)." ".shift(@entry_split);
```

Referências:

<http://www.ataliba.eti.br/node/1441>