скрипт блокировки спамеров на www средствами ipfw table и nginx

Автор: ProFTP.
Оригинал: http://www.lissyara.su/articles/freebsd/www/spam_blosking_with_using_ipfw_table/

задача: закрыть спам на сайтах.

есть черный список (black list) ip на сайте http://www.stopforumspam.com/ (есть и другие списки), список часто обновляется. В blacklist входя прокси-сервера, взломанные машины через которые боты пытаються спамить на все www сразу...

проще всего добаавить в ipfw таблицу, после блокировки максимум 1 спам сообщение за несколько суток или за неделю.

ipfw table:add deny ip from table(1) to any

```
ee /root/spamstop.pl#!/usr/bin/perl

# use File::Pid;
# my $pidfile = File::Pid->new( { file => '/var/run/x0.pid', } );
# my $pid = $pidfile->running;
# die "Service already running: $pidn" if $pid;
# $pidfile->write;
## можно раскомментировать, это для того чтобы скрипт
## одновременно повторно не запустился

use LWP::Simple;

my $spam = get("http://www.stopforumspam.com/downloads/bannedips.csv");

# system("ipfw table 1 flush > /dev/null &") if (defined $spam);


open( IP, "ipfw table 1 list |" );
$/ = '';    # Включить режим чтения абзацев
my $use_ip = <IP>;
close IP;

# IP которые уже присутствуют в таблице не удаляются
# а добавляются новые тех которых нету
my %seen;
@seen{ return_ip($spam) } = ();
delete @seen{ return_ip($use_ip) };
```

```
#print keys %seen;

foreach (keys %seen) {
 print $_;
 system("exec ipfw table 1 add ".$_ );
# system("exec ipfw table 1 add $_ > /dev/null &");

}

sub return_ip {
 # print $_[0];
 my $hash;
 $hash->{$1}++
 while $_[0] =~ /(d+.d+.d+.d+)/smg xor
 grep { $_ > 255 } split /./,
 $1;
 return keys %$hash;

}

# $pidfile->remove;
## можно раскомментировать, это для того чтобы скрипт
## одновременно повторно не запустился

exit;
```

crontab:8 0 * * * root /root/spamstop.pl

или запускать скрипт, через каждых 3 часа:0 */3 * * * root /root/spamstop.pl

можно при старте системы добавить этот скрипт в /usr/local/etc/rc.d/

скрипт выполняется не быстро, 4-10 минут, грузит процессор, можно попробовать вариант быстрого добавления в ipfw таблицу ЧСВ python биндинг для ipfw бацаю

```
ipfw -a list | grep table
00150   1317     65171 deny ip from table(1) to any
```

========
========
========

вариант помягче:
http://forum.lissyara.su/viewtopic.php?f=14&t=16531#p159781

теперь в фаерволле у меня правило:
```
00530 fwd 127.0.0.1,8013 tcp from table(1) to me dst-port 80
```

а 127.0.0.1:8013 слушает nginx
(основной вебсервер апач на 80 порту, а nginx только для быстрого отлупа "форум-спамера")

вот конфиг nginx
```
#user  nobody;
worker_processes  1;
#error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;
#pid        logs/nginx.pid;
events {
worker_connections  10;
}
http {
include       mime.types;
default_type  application/octet-stream;
#log_format  main  '$remote_addr - $remote_user [$time_local] $request '
#                  '"$status" $body_bytes_sent "$http_referer" '
#                  '"$http_user_agent" "$http_x_forwarded_for"';
#access_log  logs/access.log  main;
sendfile        on;
#tcp_nopush     on;
#keepalive_timeout  0;
keepalive_timeout  1;
#gzip  on;
server {
listen       127.0.0.1:8013;
server_name  localhost;
#charset koi8-r;
#access_log  logs/host.access.log  main;
error_page  400 401 403 404 500 502 503 504 =200  /index.html;
location / {
root   /usr/local/www/nginx;
index  index.html index.htm;
}
}
}
```

а в index.html что-то типа этого

```
<html>
<head>
<title>Welcome to zztop!</title>
</head>
<body bgcolor="white" text="black">
<center><h1>You are seing this page, because you are in blacklist.
</h1></center>
<center><h2>Visit http://www.stopforumspam.com/ to check you IP,
or contact me: email@was.here</h2></center>
<center><h3>Best regards, St. Me.</h3></center>
</body>
</html>
```

Результат:
- nginx как "легкий" веб-сервер отлично и быстро отдает статику типа маленького html файлика, в котором написано что пользователь в стоп-листе
- если пользователь оказывается в стоп-листе, то он не тупо отфаерволивается, а редиректится на nginx, где его посылают, но красиво :)
- в апач запросы спамера не попадут вообще, т.е. он их не будет обрабатывать, и 1) нагружаться; 2) позволять роботам постить спам