

RE: [despammed] [fw-wiz] Blocking IRC

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-01/0088.html>

From: Eric Appelboom (eric_at_mweb.com)

Date: 01/24/04

To: "Jose Eduardo B. Nunes Martins" <jemart@student.dei.uc.pt>, <firewall-wizards@honor.icsalabs.com>
Date: Sat, 24 Jan 2004 14:26:10 +0200

Yep, but play with the strings till they suit your enviroment.
Using snort with flexresp is better option than iptables sm as it is very easy to do
And very accurate as you can match on the direction of the flow.
The snort irc sigs are very good.....you can always just run without the resp: rst_all optin to test
Flexresp is your friend! Unless you fsckup and start reseting all your folks connections :)

I you really want fun play with flexresp2 or the older hogwash(inline)

Cheers
Eric

-----Original Message-----

From: Jose Eduardo B. Nunes Martins [<mailto:jemart@student.dei.uc.pt>]
Sent: 24 January 2004 12:00 AM
To: [firewal wizards@honor.icsalabs.com](mailto:firewal_wizards@honor.icsalabs.com)
Subject: RE: [despammed] [fw-wiz] Blocking IRC

Is it my mistake or does this drops ALL packets with the specified strings?
Would an HTML page with those strings have his (or some of his) packet dropped?

On Mon, 19 Jan 2004, Eric Appelboom wrote:

```
>Or if you really want to be classy using just IPTables use string  
>matching support  
>  
>iptables -I INPUT -j DROP -p tcp -d 0.0.0.0/0 -m string --string "JOIN  
>\": \#"  
>iptables -I INPUT -j DROP -p tcp -d 0.0.0.0/0 -m string --string  
>"PRIVMSG "  
>  
>  
>http://www.securityfocus.com/infocus/1531  
>
```

Firewall-Wizards: RE: [despammed] [fw-wiz] Blocking IRC

>Cheers

>Eric

>

>-----Original Message-----

>From: Eric Appelboom

>Sent: 19 January 2004 10:54 AM

>To: 'Vishwanath V'; firewall-wizards@honor.icsalabs.com

>Subject: RE: [despammed] [fw-wiz] Blocking IRC

>

>Use snort with flexresp

>

>RULE-LOCKED:alert tcp \$HOME_NET any -> !\$SAFE_IRC any (msg:"CHAT IRC

>channel join"; flow:to_server,established; content:"JOIN \: \#";

>nocase; offset:0; classtype:misc-activity; sid:1729; rev:2; resp:

>rst_all;) RULE-LOCKED:alert tcp \$HOME_NET any -> !\$SAFE_IRC any

>(msg:"CHAT IRC message"; flow:to_server,established; content:"PRIVMSG

>"; nocase; offset:0; classtype:misc-activity; sid:1463; rev:3; resp:

>rst_all;)

>

>

>I defined !\$SAFE_IRC as IRC server I don't block.

>This also block IRC over nonstandard ports.

>

>Regards

>Eric

>

>-----Original Message-----

>From: Vishwanath V [mailto:thelinuxguyis@yahoo.co.in]

>Sent: 14 January 2004 12:47 PM

>To: firewall-wizards@honor.icsalabs.com

>Subject: [despammed] [fw-wiz] Blocking IRC

>

>Hi guys,

>I just joined the list.

>I need some help wrt iptables.

>I have a linux gateway machine acting as a IP_masq/firewall.

>My policy is a basic deny all.

>I wana block machnies on my LAN from using irc client.

>

>Thanks in advance.

>Visu

>

>

>_ Yahoo! India Mobile: Download the latest polyphonic ringtones.

>Go to <http://in.mobile.yahoo.com>

>

>firewall-wizards mailing list

>firewall-wizards@honor.icsalabs.com

><http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

>

>-----

RE: [despammed] [fw-wiz] Blocking IRC

Firewall-Wizards: RE: [despammed] [fw-wiz] Blocking IRC

>Filtered by despammed.com. Tracer: /headers/TAA027571074475835
>Consider a PayPal donation to help Despammed stay a step or two ahead
>of the bad guys.
>A new PayPal donation button is now on the home page. Thanks!
>
>
>

>firewall-wizards mailing list
>firewall-wizards@honor.icsalabs.com
><http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
>

--

JoseM

"Compaq are the most poorly designed PCs I've ever seen.." - Andrew
<http://7mares.terravista.pt/zemartins>
<telnet://sponge.org:6969>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

Filtered by despammed.com. Tracer: 1074896594 Consider a PayPal
donation to help Despammed stay a step or two ahead of the bad guys.
A new PayPal donation button is now on the home page. Thanks!

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>