Subject: iptables on VE0 to prevent SSH Attacks?
Posted by phpfreak on Wed, 01 Feb 2006 15:18:34 GMT
View Forum Message <> Reply to Message

Had an interesting scenario this morning. We had a brute force scan network wide and it was hitting all of the VE's on a single server. When this happened, we had about 250 sshd processes running and visible in TOP on the host machine. Of course this spiked the load considerably.

I tried to drop the offending host's IP address on venet0 on the host machine (VE0) but it had no effect.

Is there any simple way to have a firewall rule on the host machine that can affect all of the VE's in a case like this?

Please let us know.

Thanks,

Subject: Re: iptables on VE0 to prevent SSH Attacks?
Posted by phpfreak on Wed, 01 Feb 2006 15:40:25 GMT
View Forum Message <> Reply to Message

I found the answer, sorry for the confusion. To help anyone else, if you need to drop an IP from all your VE's, just do something like this:

```
iptables -A FORWARD -i eth0 -s 65.254.39.146 -j DROP
```

Problem solved.

Subject: Re: iptables on VE0 to prevent SSH Attacks?
Posted by kir on Wed, 01 Feb 2006 15:56:42 GMT
View Forum Message <> Reply to Message

Nice hit.

Could you post this tip to HowTo forum?

Subject: Re: iptables on VE0 to prevent SSH Attacks?
Posted by phpfreak on Wed, 01 Feb 2006 15:58:46 GMT

View Forum Message <> Reply to Message

surely!

Subject: Re: iptables on VE0 to prevent SSH Attacks?

Posted by almahdi on Fri, 17 Feb 2006 18:07:25 GMT

View Forum Message <> Reply to Message

You may want to limit the number of times each IP connects per second to SSH..

Most of those Attacks are script based, there is an easy way to block them, we've been using it for a while on our servers.

```
----
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent   --set

iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent   --update --seconds 60 --hitcount 4 -j DROP
----
```

This will limit incoming connections to port 22 to no more than 3 attemps in a minute. Any more will be dropped.

You can adjust the numbers yourself to limit connections further.

Subject: Re: iptables on VE0 to prevent SSH Attacks?

Posted by kir on Fri, 17 Feb 2006 18:35:28 GMT

View Forum Message <> Reply to Message

Yet another approach that I use is to put sshd on a different port.

The good thing is it is very easy to do - just add "Port XXXX" line to your /etc/ssh/sshd_config file/, restayou will never ever be attacked, since most people just blindly try default port and do not do port scanning.

The bad (well, not that bad, just a bit inconvenient) thing is you have to remember this new port number and either put it into your ~/.ssh/config or into ssh command line argument. If you use the same machine to ssh from this is not really a problem - you put it into ssh config once and forget about it. But if you use a lot of machines this can be, well, not very convenient.