

Re: Denied Packets from Internal Network

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-04/0433.html>

From: Randy C (randy_mn@hotmail.com)

Date: 04/09/02

From: "Randy C" <randy_mn@hotmail.com>

Date: Tue, 09 Apr 2002 00:34:41 GMT

I was not trying to hide any IP addies .. I forgot to add the broadcast one when I copied the log file message over. My apologies for the screwup there. It should read

```
Apr 8 time machine_name kernel: Packet log: input DENY eth1 PROTO=17
192.168.1.1:1499 255.255.255.255:63645 L=44 S=0x00 I=31239 F=0x000 T=128
(#24)
```

192.168.1.1 is for the internal network as you guessed, it is the second nic card on the Linux box/server. The other nic card is for the external network and is hardwired – IP addy. So the packet is coming from the server itself and not another machine on the network or it would have a different IP addy – at least I assume that it would have a different IP addy.

My concern is that someone is trying to route packets through and they are getting blocked .. I am just trying to figure out what might be trying to generate them. They come about every minute and the internal port address keeps going up by 3 each time.

RainbowHat .. thanks for the links you suggested.

Randy

"Randy C" <randy_mn@hotmail.com> wrote in message
news:dLhs8.139\$po4.104326@news7.onvoy.net...

>

> *I have a Caldera install on my network server. I am using a proxy server*

> *with an ipchains type firewall. I recently noticed entries in my log file*

> *that indicate my server's internal IP is trying to send out packets about*

> *every one second and the port number increases by 3 each time. Is this*

the

> *result of someone from the outside trying to route packets through my*

> *internal network and to make it look like they are coming from my system?*

>

> *The log entry looks like*

>

comp.os.linux.security: Re: Denied Packets from Internal Network

> Apr 8 time machine_name kernel: Packet log: input DENY eth1 PROTO=17
> 192.168.1.1:1499 L=44 S=0x00 I=31239 F=0x000 T=128 (#24)
>
> This repeats itself with the port changing from 1499 to 1502 to 1505 etc
..
> with the only other thing changing is the I= value .
>
> comments? suggestions? education?
>
> --
>
> Randy
>
>
>

- **Next message:** [John Thompson: "Re: Isn't this an oxymoron. linux & security?"](#)
- **Previous message:** [Mark Damrose: "Re: Giving shutdown rights to somebody"](#)
- **In reply to:** [Randy C: "Denied Packets from Internal Network"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)