

Re: Backgroun dnoise

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/11178.html>

From: Leonid Rosenboim (My_1st_name@Consultant.Com)

Date: 10/10/02

From: "Leonid Rosenboim" <My_1st_name@Consultant.Com>

Date: Thu, 10 Oct 2002 11:55:50 +0200

Wolfgang is right, and I really dont understand the reason for ignorant people to try and solve other people's problems for free.

Anyway, background noise is a problem with all firewalls.

Especially when a routing outage happens somewhere, and you have connections effected by that outhage, as short as it may be, there are going to be very late packets which where part of a valid connection, but where stuck in routers' queue or in temporary routing loops, that eventually get delivered, after the firewall/NAT has alredy timed that session out.

It happens with ZomeArlam, it happens with the Intel Wireless Gateway I got at home, and it happens with Cisco IOS/FW, as well as Checkpoint FW-1. Even if session timeout is set at 2 minutes (the recommended timeout in many RFCs), there will still be these false alarms.

The cost of setting session timeouts too long is high – there would be a need for much more memory to keep track for terminated session for a longer period, and thus the total number of entries in the session tables would need to be increased.

— HTH

Leonid Rosenboim Visit: <http://www.masada2000.org/>

Consultant Email: my first name at consultant dot com

"Wolfgang Kueter" <wolfgang@shconnect.de> wrote in message news:ao2nit\$vj4\$1@news.shlink.de...

> *taharka wrote:*

>

> > *The following link is a security report on that addy at mynetwatchman.com*

comp.security.firewalls: Re: Backgroun dnoise

> > : <http://www.mynetwatchman.com/LID.asp?IID=8254594>
> > Looks like this guys been at it for a while.
> >
> > Here is the info on that addy's ISP:
> >
> > 206.13.29.12 (dns1-la.lsan03.pacbell.net)
> >
> > [a lot of totally irrelevat stuff deleted]
> >
> > Port 1099:RATs: Blood Fest Evolution, RAT
> > Download portref.zip from: wilders.org for a full port reference
listing.
> >
> > If the firewall is blocking internet access to that addy, there is
nothing
> > to worry about. Probably that nasty ole NETBIOS/e-mail worm looking for
> > open shares.
> >
> > Sorry, complete nonsense. I might sound harsh, but your posting shows that
> > you are completely clueless. Instead of posting some whois entries you
> > should simply have looked at the ports and protocols used:
> >
> > It is udp, it is directed to Port 1099 and uses source port 53 coming from
> >
> > wk@heart-of-gold:~/patch/rh73> host 206.13.29.12
> > 12.29.13.206.IN-ADDR.ARPA domain name pointer dns1-la.lsan03.pacbell.net
> >
> > which looks much like a DNS server. And something like
> >
> > wk@heart-of-gold:~> nslookup www.google.com dns1-la.lsan03.pacbell.net
> > Server: dns1-la.lsan03.pacbell.net
> > Address: 206.13.29.12
> >
> > Non-authoritative answer:
> > Name: www.google.com
> > Address: 216.239.35.101wk@heart-of-gold:~/patch/rh73> nslookup
> > www.google.com dns1-la.lsan03.pacbell.net
> > Server: dns1-la.lsan03.pacbell.net
> > Address: 206.13.29.12
> >
> > Non-authoritative answer:
> > Name: www.google.com
> > Address: 216.239.35.101
> >
> > even shows you that it is a DNS server.
> >
> > So what this stupid piece of firewall simulation did, was simply to
> > misinterpret a late DNS answer packet as an attack.
> >
> > The only question here is what is more stupid, this firewall simulation
> > giving false alarms or you, who is not able to distinguish between a late

- > *DNS answer and an attack.*
 - >
 - > *Read a book about network protocols.*
 - >
 - > *Wolfgang*
-

- *Next message:* [kim: "Check it out"](#)
- *Previous message:* [Linux Newbie: "iptables vs cisco pix ???"](#)
- *In reply to:* [Wolfgang Kueter: "Re: questionable access to my computer – please help"](#)
- *Next in thread:* [Wolfgang Kueter: "Re: Backgroun dnoise"](#)
- *Reply:* [Wolfgang Kueter: "Re: Backgroun dnoise"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)