

Re: Is port 37 safe to let out?

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-06/0058.html>

From: Menno Duursma (*pan_at_desktop.lan*)

Date: 06/07/05

Date: Tue, 07 Jun 2005 12:07:15 +0200

On Mon, 06 Jun 2005 20:54:30 -0700, Mikhail Zotov wrote:

> *Menno Duursma* wrote:

>> *On Sun, 05 Jun 2005 21:41:41 -0700, Anthony Ewell* wrote:

>> > *matt_left_coast* wrote:

>> >> *Anthony Ewell* wrote:

>>

>> >>> *I am getting a lot of port 37 (time) outbound connection attempts*

>> >>> *on my iptables firewall.*

I'd be interesting to find out: how come?

>> >>> *Is it safe to "let it (port 37) out?"*

>>

>> *Maybe,*

Probably.

>> *but i wouldn't.*

Unless for some reason you need this to work (in which case, you may want to restrict it some.)

Apperently some box behind it your firewall wants to know how the clock is set on some outside host for some reason. And trys to use the RFC868 Time Protocol to do so. Better to just sync one or two server boxen to pool.ntp.org or something, and have them provide "time" services for LAN connected machines.

Who knows: maybe it's actually an attempt of one of your users/machines to create/get a tunnel through your firewall.

>> *Unless you are on a LAN and have some box setup with ntpd (or a cron*

>> *job running "ntpddate") which provides "time" broadcasts*

s/broadcasts/services/

Sorry this may well be incorrect (although Google tells there are Time implementations which can send/recive broadcasts, i don't see it in the

RFC.) But i might have been thinking BSD TSP (time synchronization protocol) here. Which uses UDP port 525 instead:
<http://www.linuxvalley.it/encyclopedia/ldp/manpage/man8/timed.8.php>

My bad.

Thanks for pointing out my error Mikhail.

>> *to the subnet you're on, for other machines – yours – to sync with.*

Which you (cron) would do with "netdate" probably.

>> >> *Outbound means you are trying to connect to a time server on the internet.*

>>

>> *No it doesn't.*

Well, your correct (ofcourse) sorry again. However a "time server on the internet" would generally be providing an (S)NTP service, rather than the Time Protocol one. As the former is much more accurate.

>> >> *If you want to sync to the atomic clocks, you need to let the packet out.*

>>

>> *No you don't (or atleast not unless you have some atomic clocks within your subnet/broadcast domain providing a time service to you (unlikely.))*

>

> *Menno, could you please explain your point.*

The basic "time" service isn't very accurate, unless both client and server know about some extension to it. And even then, only when used over a relatively lo-latency (LAN) network.

--

-Menno.