

Re: [fw-wiz] terminal services

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-01/1607.html>

From: Barney Wolff (barney@pit.databus.com)

Date: 01/29/03

From: Barney Wolff <barney@pit.databus.com>
To: "Reckhard, Tobias" <tobias.reckhard@secunet.com>
Date: Wed Jan 29 12:13:19 2003

On Wed, Jan 29, 2003 at 08:26:20AM +0100, Reckhard, Tobias wrote:

>
> *Source ports are worth pretty much zilch when filtering TCP or UDP. It's not
> a good security decision to design a filter that attempts to allow (only)
> outbound DNS queries based on outbound packets having source port 53 and
> inbound packet having destination port 53. Rather, the source port (in the
> outbound direction) should be able to be pretty much anything, while the
> destination port is the one that needs to be checked. Same for NTP or any
> other service.*

I believe you've misunderstood what I wrote. If you allow queries to DNS or NTP out from high ports, you must, with a non-state-keeping filter, allow UDP inbound to high ports from port 53 or 123. But without state, you won't notice that the supposed DNS response from port 53 is going to port 1434 and is an attack packet. The solution, without state, is to allow packets in only to ports 53 and 123, and ensure that outbound requests are sent only from those ports. If you can't do that you must keep state.

> *There are protocols that use fixed client as well as server ports. IKE
> appears to be one of them (but DNS and NTP definitely aren't). You can
> configure your packet filter, stateful or not, more restrictively by
> restricting the source ports used. It may buy you some added security. Most
> of the time, that won't be much, though.*

This is just wrong – both bind's named and ntpd can be configured to send requests only from 53/123. ntpd does it by default; it's ntpdate that sends from a high port. Just to be clear, I am NOT suggesting that checking the source port of inbound packets does any good. I am suggesting that controlling the source port of your own outbound requests allows you to restrict what destination ports inbound packets may target, if you're using a simple router filter rather than a state-keeping firewall.

--

Barney Wolff <http://www.databus.com/bwresume.pdf>
I'm available by contract or FT, in the NYC metro area or via the 'Net.