

Re: What is this?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-10/0052.html>

From: Moe Trin (*ibuprofin_at_painkiller.example.tld*)

Date: 10/02/05

Date: Sun, 02 Oct 2005 15:08:50 -0500

In the Usenet newsgroup comp.security.firewalls, in article
<LZx%e.35034\$d5.190941@newsb.telia.net>, Anders wrote:

>I dit apt-get my own hping, and after that I had played a little with it,
>I had to look in my snort log, because I didnt get any respond from my
>firewall.
>I did find over 700 hits.
>One of the explanation for what had hapend on snort.org was this:
>
>""BAD-TRAFFIC tcp port 0 traffic
>This event is generated when TCP traffic to port 0 is detected.
>This should not be seen in normal TCP communications.

There are 12 bytes of "stuff" other than the IP addresses in an IP header
and 16 bytes of "stuff" other than port numbers in a TCP header that can be
"played" with. Only a few combinations are normally used. Fyodor of nmap
fame makes use of other combinations to explore networks. hping2 is the
manual version that lets you do even more.

>Have to be careful with this tool.

Yes

>First, I have to apologize for the "traceroute -S udp p53", the udp part
>should not be in there at all, it is an blunder made by me, I can only
>blame my self for that, did not dubbel check it,I am sorry.

OK – there are several different implementations of traceroute out there,
and they differ in which option does what. The LBL (original) version does
not have a -S option, and the version from Olaf Kirch (then Caldera, now
SuSE) uses that as the LBL -s option for [S]ource address, which should
have an IP address appended. The udp was also not a normal option.

> Michael Schiffman patch stops increment enabling user to use 1 fixed
>UDP port number (i.e. port 53)

OK – there are other tools that can do that ;-)

comp.security.firewalls: Re: What is this?

*>The probe immediately after the successful one will be denied by the ACL
>on the firewall. To possibly get further, a simple modification to
>traceroute can be done to add a command line switch to stop port
>incrementation (Figure 5). This allows us to force every probe we send to
>be acceptable to the firewall's ACL (a side effect being that we might not
>get the normal ICMP unreachable message from the ultimate destination due
>to the fact that there might actually be something listening on the other
>end).*

This fails on a properly set up firewall. If there are no name servers meant to be publicly accessible behind the firewall, there is no reason to all traffic to port 53 inbound. Where I work, we have three publicly accessible DNS servers – one in the DMZ, and two located at our upstream. All internal DNS requests go to servers behind the firewall, but as there is no reason for external hosts to know internal names, the external DNS servers are set to return "generic" answers to requests – so that when a request comes in for the name of 192.0.2.2, the answer returned is "192.0.2.2.example.com" rather than "file_server.example.com". That answer satisfies those who "must" have a "valid" hostname to put into their logs – (and if someone does the reverse lookup, and follows it with a forward lookup of 192.0.2.2.example.com, they get the 192.0.2.2 answer), but those answers don't provide useful information about the layout of our internal LAN. Creating those zonefiles is trivial – just a couple of dumb shell scripts. An external request for a public system (such as www.example.com) does return the valid IP address of the web server in the DMZ (and a reverse lookup of that IP does return the 'www.example.com'), so the public can go there, but no further.

Old guy