

Re: Telnet, Ping and Port 1025

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-09/0236.html>

From: Malke (malke_at_nospoonnotreally.com)

Date: 09/04/04

Date: Sat, 04 Sep 2004 14:25:29 -0700

C & C Antiques and Collectables wrote:

> *In article <jrqdnVP6c84rIqTcRVn-vw@scnresearch.com>, Don Taylor wrote ...*

>

>> *>Lanwench [MVP - Exchange] wrote ...*

>> *>> Put a firewall in place....if you're on XP, you can just enable the built-in one.*

>> *>> C & C Antiques and Collectables wrote:*

>> *>> > I just run a security check on my system at Symantec. It reported risks from Telnet, Ping and open port number 1025. Can anyone help me close these these holes in my systems security please?*

>> *>>*

>> *>I do have Norton AV and Firewall installed, both are updated daily. It was Norton's own on-line security check that revealed the Telnet, Ping and 1025 holes in XP Home.*

>>

>> *Norton doesn't seem, by default, to lock down all ports. But if you don't see a need for a particular service then you can add a rule yourself that will block incoming and/or outgoing packets for any particular port.*

>>

>> *For telnet it isn't clear whether you have that open for incoming or for outgoing, or perhaps both, directions. For incoming, unless you specifically need to have the telnet server running and the port open to accept telnet connections from outside I'd certainly think that blocking that port number would be reasonable.*

>>

>> *For ping there are occasional "ping flood" attacks, where some little net vandal will flood your machine with a few thousand pings a second. If you don't need to have the ability for someone to check and see whether your machine is up then you can turn that off with little loss.*

>>

>> *The 1025, and I think 1029, seem to have become popular for some net vandal's probing several months back. Both*

>> *those are used for some sort of checking of network*
>> *status. I began seeing a handful of those a minute and*
>> *finally put both those into my block list, but let the*
>> *little "norton flag" wave at me to let me know that they*
>> *are still coming in on a regular basis.*
>>
>> *You can also include a rule "all that is not permitted*
>> *is prohibited" and that is convenient to just blanket*
>> *block the twits that are out there just rattling your*
>> *door to see if they can get in. And it is possible with*
>> *any and all of these to have the rule add a line to your*
>> *logs/stats, just so that every few days you can go peek*
>> *at the totals and watch for any spike in activity.*
>>
>> *I do support for a few small business users. It amazes*
>> *me that isp's, both small and large, have slowly been*
>> *inching towards blocking virus and spam but that they*
>> *let vandals send any kind of net packets in that they*
>> *want. For example, AOL has finally got antivirus tools*
>> *running, congrats to them, but I watch the trojan*
>> *packets hammering right through their system, trying to*
>> *find any customer who is at risk and who can be subverted.*
>>
>> *The net isn't what it used to be 25 years ago.*
>> *In hindsight, we never should have let the public know*
>> *about the net, that would have been for the best.*
>>
> *Well, thank you Don... a comprehensive answer if ever I read one!*
> *I have closed both 1025 and 1029 ports and set Norton to let me know*
> *when my new rule is fired. I am however uncertain precisely how to set*
> *up my system to shut down the Telnet and Ping problems. I do not*
> *knowingly use either of these.*
>

Thanks for asking such an interesting question. I was going to tell you to just disable Telnet in services (Run>services.msc), but I wasn't sure about ping. So I Googled for "disable ping" and found this really great page from MS Technet which shows how you can use the Windows Firewall advanced settings. Scroll all the way down and you'll see where you can take the checkmark out of "allow incoming echo request" i.e., ping. If you're not using the Windows Firewall but have a third-party one, see if it gives you that option. Here's the url:

<http://www.microsoft.com/technet/community/columns/cableguy/cg0204.msp>

Malke

--
MS MVP - Windows Shell/User
Elephant Boy Computers
www.elephantboycomputers.com
"Don't Panic!"