

Re: Do I need these services listening?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-03/0768.html>

rodlinkowitz_at_whale-mail.com

Date: 03/15/05

Date: 15 Mar 2005 13:19:24 -0800

Gerald Vogt wrote:

- > *rodlinkowitz@whale-mail.com* wrote:
- > > *Simply, the modem and router are -physically connected- to the first*
- > > *computer. The other computer (which I call the "client" or "secondary"*
- > > *computer) has only a cable attached to the first computer, hence it*
- > > *receives its internet connection via the first computer. Again, this is*
- > > *a standard configuration, nothing special being done here. I consider*
- >
- > *Sorry, but now you are contradicting your last message. Last time you*

- > *wrote both computers are connected to the router and the router is*
- > *connected to the modem. Now you are writing that there is no physical*

- > *connection between the second computer and the router and the second*
- > *computer is connected to the first computer (but how if the first one*

- > *does only have one ethernet card?) So again, how exactly is your wiring?*

Sorry, when I say the second computer has a "cable attached to the first computer", I was not being very specific. But by that, I mean the cable is attached to the LAN port on the router, which sits on top of the first computer. (I've just always "seen" the second computer as being attached to and dependent upon the first computer, since its the one that houses the modem and router. But of course, since this is a simple standard configuration, technically speaking, the 2nd machine is being connected to the LAN port on the router, as is the first one).

- > > *the "server" computer as having both a public IP and a private IP,*
- > > *because it contains the router, which on one side (WAN) has a public*
- >
- > *Last time I checked a RP614 is a hardware device.*

comp.security.firewalls: Re: Do I need these services listening?

> <http://www.netgear.com/products/details/RP614.php>

> *Your computer cannot contain that router...*

By "contains", I simply meant the router is physically located on top of the first computer.

Sorry for the confusion.

> *No, no server outside your network can know about your LANs private IP*

> *addresses unless you are using something that tells it to the outside,*

> *which may be a JavaScript inside your browser. Noone outside your router*

> *can send a packet to any of your inside IP addresses because the*

> *internal IP addresses are not routable and any router in between will*

> *just drop these packets.*

That's what I was starting to conclude.... I guess that means I can stop worrying about Javascript revealing my private IP. Still kinda bugs me that "they" can know that too about me.... (turning JS off simply isn't a solution, unfortunately. My wife who uses the computer would never know when to turn it on, when a particular function in a web site is "broken" because of JS).

> *That a software scan of your public IP shows open ports inside the network, however, seems not correct. But at this time I won't try any*

> *more guessing until I fully understood your configuration. Under normal*

> *circumstances the scan of your public IP address would scan the router*

> *from the inside which may show some open ports in particular port 80 if*

> *the router does have a web management interface. The router should not*

> *have open ports 25 or 110, though, as it is not running a server.*

I think we discovered via netstat (and "WhoIsConnected") that 25 & 110 were not listening to the net, because the software port monitor/analysis programs don't report that, nor do the online scanners. Only some of the (software) port scanners do.

> > *Okay, but can it hurt to block those ports I mentioned (135-139,445) on*

> > *the Netgear, or should I return it to default and just let NAT do its*

> > *thing? Maybe its purely psychological, but it makes me 'feel' more*

> > *secure to block those ports completely on the router's WAN*

> > *configuration as I did, as well as having the router block it via NAT,*

Re: Do I need these services listening?

comp.security.firewalls: Re: Do I need these services listening?

- > > *not to mention its SPI, as well as having my 4 or 5 personal firewalls*
- > > *block the ports as well. How else can I sleep at night?*
- >
- > *You can block them on your Netgear. No problem there. But why do you*
- > *have 4 or 5 personal firewalls on two computers?*

Because it helps me sleep at night? My story begins... after countless hours of research and tweaking rulesets, I thought I was pretty savvy when it came to computer network security, and that my system was all but bulletproof. Then when I witnessed an attack on my personal firewall causing it to crash on me, and my friend's home PC actually getting a DOS attack before my eyes, (which was stopped by Kaspersky, the antivirus), that's when I decided that months of researching network security to protect myself wasn't enough. If it wasn't enough that I had what research told me was one of the most respected software firewalls available, then it wasn't enough. That's when I decided I needed the Netgear, simply for use as a hardware firewall device, to avoid having a software firewall become disabled by a trojan or worm. That plus the fact that the use of the router meant I had to change my modem to an "always on" type, which made security even more of an issue.

Now if a hacker wants in and tries to disable my firewall or reboot my PC to do it, they're at least going to have a heck of a time trying to succeed. Because even if the Netgear gets struck by lightning, I still have Jetico providing firewall duties. And if they manage to disable Jetico, Kaspersky anti-hacker takes up the slack. If they also manage to blow away Kaspersky Anti-Hacker, the sideline players kick in; namely Black Ice Defender. If Black Ice Defender suddenly has a heart attack, then I will probably have Windows SP2 firewall there to "get its back". But if they manage to kill SP2's firewall, blow up the Netgear, crash Jetico, shoot down Anti-Hacker, and quiche Black Ice Defender... then I'm really screwed. Unless TrojanGuard picks up on the attack. But even if it doesn't, Kaspersky Anti-Virus, which is also running, might. After all, it stopped the network TCP Syn Flood Attack that my friend got. As for the second computer... if all of these firewalls and anti-hacking programs manage to let the attack through to the second computer... well, there's still Jetico there to prevent further damage. And of course, if the attack comes on ports 135-139 or 445, well I've blocked those off completely via the Netgear.

My purpose here in posting this thread was to tighten up security even more, by seeing if I can completely close off any listening ports.

- > *This is weird. That means that there is actually something listening on*
- > *these ports but just closes the connection again after a few seconds.*
- If
- > *there is nothing running you would get an error message. (Try*

Re: Do I need these services listening?

comp.security.firewalls: Re: Do I need these services listening?

"telnet
> 192.168.1.2 1234" with 1234 a random port that noone is listening to
for
> comparison...) This is not good. But right now I am more confused
about
> your configuration that I don't know where the problem could be.

I tried that and the IP of my two computers, using port 5066 as the
random port no.
Every time I get "Could not open connection to the host on port 5066,
Connect failed". I'm assuming this is normal. More interestingly, when
I tried telnetting smtp using the private IP of either of my two
computers, I got the same message (ie. telnet privateIP smtp = "connect
failed"). So what happened yesterday is not
being repeated today.

> Maybe you could write the output of the "ipconfig" command on both
> computers. That should clarify a lot about your setup with the
Netgear.

This is the output as done from the second computer:

Windows IP Configuration

Host Name : client
Primary Dns Suffix :
Node Type : Unknown
IP Routing Enabled. : No
WINS Proxy Enabled. : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description : Realtek RTL6145 Family PCI Fast
Ethernet NIC
Physical Address. : 00-20-CH-A9-69-4D
Dhcp Enabled. : No
IP Address. : 192.168.1.3
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DNS Servers : 192.168.1.1

4.2.2.2

> Do you have a anti-virus with e-mail scanner running? Do the open
ports
> still appear on your computers if the e-mail scanner (inbound and
> outbound) is turned off?

Yes. No. After turning Kaspersky's email guard off, and doing a quick
scan with FreePortScanner, The 25 and 110 ports are reported as closed.
These experiments have also confirmed for me that the port scanners
have varying degrees of reliability. FOR EXAMPLE... Today, Advanced

Re: Do I need these services listening?

comp.security.firewalls: Re: Do I need these services listening?

Port Scanner showed only port 25 as open, after doing a "range scan" of all addresses that end between 0 and 255 on my private LAN. But when I did a scan on only the address owned by my second computer, the one that reported those ports open, nothing showed up as open. Then when I did another range scan after closing Kaspersky's email guard, two ports showed open, but they were ports 135 and 139. This however conflicts with the above mentioned FreePortScanner, which also showed the mail ports as closed after closing Kaspersky's mail guard feature, but they showed THREE ports open: 135, 139 and 445. Running Moorer's Port Scanner doesn't show ANY ports as being open. However on the plus side, its very fast at producing these incorrect results. "pcSuper Scanner 1.1" found those same three as "FreePortScanner", and two more that it didn't, which were the Kaspersky antivirus ports. However, it didn't report the mail ports, even though I had re-opened Kaspersky's mail guard. Instead, it found a whole bunch of what it calls "TCP Client Ports", which -none- of the other port scanners reported. So many, it wouldn't even show me the entire list, because the stupid program can't be properly maximized to reveal numbers that go beyond its screen space. Plus a whole slew of UDP ports that even the port scanners never listed. This program really says "bogus" to me.