

Re: How to Stealth POP3 Port 110 using NIS2000?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-02/1237.html>

From: Joseph V. Morris (jvmorris@erols.com)

Date: 02/13/02

From: "Joseph V. Morris" <jvmorris@erols.com>

Date: Wed, 13 Feb 2002 09:50:17 -0500

Nameless,

There's a potentially simple answer for what you're seeing

"Nameless" <nameless@noname.com> wrote in message
news:aoda8.19392\$Cg5.1074668@news1.calgary.shaw.ca...

|

| According to the firewall log, that port is not even being probed.

A lot of ISPs BLOCK unsolicited inbound POP3 requests at the border routers, apparently. POP3 was one of the ports that was NEVER probed by GRC on my machine (if I recall correctly and the last time that I bothered to run Shields Up). The response that GRC is reporting is, therefore, coming from your ISP's routers, not from you. And many industrial-strength routers aren't going to support Stealthing ports for the simple reason that it's not an industry standard response. (Find me a reference to Stealth in the RFCs; I can't.)

The reason for this is quite simple. Under most ISP's TOS/AUP, you're not supposed to be running a POP server. Consequently, there's no need to forward such requests to the IP address assigned to you (not to mention the minor problem of the vulnerabilities associated with running such a server).

Check out the NIS rules for POP3 and SMTP for your e-mail client software. You're only going to see a PERMIT rule for outbound. In other words, YOU have to initiate the conversation -- either to send mail or to receive it. (And once you've initiated the conversation, the response packets are allowed in.) NIS, NPF, and AtGuard all block any communication that is not explicitly PERMITTED. In NIS and NPF, the event you would probably see is "Unused Port Blocking". In AtGuard, I think it would show as "Implicit Block Rule".

What version of NIS 2000 are you running? NIS 1.0 or NIS 2.0? I don't believe NIS 1.0 ever invoked a patch to "Stealth Unused Ports", but I think it may have been added via Live Update at some point to NIS 2.0. (I jumped from NIS FE 1.0 to NIS FE 2.5, so I'm not completely positive what

happened with NIS 2.0.)

Finally, if you're running any kind of NAT router — hardware or software (like ICS in Win 98 SE) — there's a very good chance that the response you're seeing could be coming from your router. Most of them block unsolicited inbound POP3 and SMTP communications, or can be configured to do so.

| This problem persists whether I have NAV e-mail scanning enabled or
| disabled. Apparently, long ago there was a problem with this port being
| left completely open. But that was later fixed with a new LiveUpdate
| (mine is up to date).

Yes, the original version of the NAV e-mail scanner DID function as a server that would also receive unsolicited inbound requests. But, I think they fixed this quite some time ago. In this instance, it was listening for unsolicited inbound and consequently could not be Stealthed (but it could be CLOSED).

| By the way, is it possible (or desirable) to have two firewall programs
| active on a PC? I've read lots of good things about Zone Alarm and am
| wondering whether it would be compatible with NIS.

This is a matter of personal opinion. I don't think it's desirable; if you don't know how to set up one personal software firewall (PSF), it's very unlikely that you will know how to correctly set up two. Furthermore, the firewalls are burrowing further and further into and under the winsock and TCP/IP stack to protect against newly emerging threats. The possibility of a conflict that effectively nullifies some aspect of the firewall protection for both PSFs is therefore increasing. (And, of course, you'd never know — until . . .) In other words, it's quite conceivable that your protection could actually decline as a consequence of running two firewalls. However, AFAIK, there's no known conflict between most versions of ZA/ZAP and the early versions of NIS/NPF. There WAS, at one time, a conflict between one particular ZA/ZAP build and one of the later versions of NIS/NPF, but, IIRC, ZoneLabs fixed that quite some time ago.

| One other thing, is there an easier way to rearrange the firewall rules
| in NIS2000 rather than choosing one rule at a time and clicking the
| up/down arrows over-and-over-and-over again!?

Not yet. Maybe in NIS/NPF 5.0. There's been a lot of talk about an enhanced ruleset editor/browser, primarily to rectify the unmitigated disaster represented by the rules editor GUI in NIS 3.0/4.0. One of the obvious enhancements would be to implement multiple rule selection and drag and drop functionality.

--

Regards,

Joseph V. Morris
jvmorris@erols.com

comp.security.firewalls: Re: How to Stealth POP3 Port 110 using NIS2000?

ICQ #29438199

This is a NEWSGROUP message; except for privacy reasons, please respond therein; an e-mail COPY is always appreciated, of course. Almost all electrons used in the creation of this message were recycled. No electrons used in the production of this message were harmed or mistreated in any manner.

- *Next message:* [Jules Dubois: "Re: Tiny or Zone Alarm?"](#)
- *Previous message:* [Wolfgang Kueter: "Re: How to Stealth POP3 Port 110 using NIS2000?"](#)
- *In reply to:* [Nameless: "How to Stealth POP3 Port 110 using NIS2000?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)