

Re: How to Stealth POP3 Port 110 using NIS2000?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-02/1254.html>

From: Eirik Seim (eirik@peter.mi.uib.no)

Date: 02/13/02

From: eirik@peter.mi.uib.no (Eirik Seim)

Date: 13 Feb 2002 16:31:32 GMT

In article <rpta8.24957\$A44.1456793@news2.calgary.shaw.ca>, Nameless wrote:

> "Eirik Seim" <eirik@peter.mi.uib.no> wrote in message

> news:slrna6kj9u.i6m.eirik@peter.mi.uib.no...

>> What do you want to protect by 'stealth-ports' ?

>>

>> Your privacy? If so, would you (or anyone?) please explain in detail

>> how a stealthed port protects your privacy, 'cause I really don't get it.

>> And I've been building firewalls for a while.

>

> I can't answer that as I am no expert on firewalls. I am a novice

> trying to become more familiar with their function, capabilities,

> limitations, and use. I probably wouldn't be having the kind of

> problems I am currently having with NIS2000 if I knew more about them.

> Learning more about firewalls (and in particular NIS2000, which I have)

> is what I'm trying to do by asking the experts on this newsgroup.

The only thing you risk when not stealthing port 110 is for people to find out that you have no POP3 server running. Same goes for all the other ports. If anyone, be it an application scanning random ip addresses or a determined hacker wanting to break into YOUR computer, tries to connect to a port where you have no listening service, he won't get anywhere.

Any other opinions?

>>> Maybe so. Yet who is to say that your talk isn't "stupid and

>>> technically incorrect"? Am I to take your word for it against all

>>> that

>>> I've read from arguably far more reliable and knowledgeable sources?

>>>

>>> What sources? grc.com? Did you try reading some real papers on real

>>> firewalls, from sites like CERT or COAST?

>>>

>>> Much of my albeit limited knowledge of firewalls has been gleaned from

>>> grc.com plus the help files associated with my firewall program. I've

>>> read numerous newsgroup postings (current and archived) on firewalls,

>>> "stealthing", etc. and various other articles on the net. I am

>>> unfamiliar with CERT or COAST, but I will seek these sites out on the

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

- > *net and read what they have to say. Perhaps they offer a different*
- > *perspective on the subject. I take it you (and "Wolfgang") share some*
- > *degree of contempt for viewpoints expressed on grc.com?*

I can't answer for Wolfgang, but I've never used Gibson's site for anything. My impression is that he presents "network security" for those who don't care to understand network security. But I might be wrong, of course.

- >> >> > *Why can't I see evidence of probes? [?]*
- >> *What kind of probes?*
- > *I've created a firewall rule (top of the list) that records a log of*
- > *every inbound TCP connection to port 110. Each time I check my e-mail,*
- > *for instance, this rule makes a note of it in the log. When I scan my*
- > *ports using "Shields Up" at grc.com, it supposedly scans port 110 but it*
- > *doesn't trigger this new rule and so no log entry is created. If I*
- > *modify this new rule to actually block port 110 (thinking this should*
- > *"stealth" the port), it nevertheless shows up as only "closed" according*
- > *to "Shields Up". Port 80 is always "stealthed". Perhaps I'm*
- > *overlooking something?*

I'll have to agree with that other poster who mentioned something about your ISP could be filtering these connections. You might be able scan your computer from another machine in your own LAN (if any), to see if it is really 'stealth', and not some obscure bug.

– Eirik

--

Eirik Seim
eirik.seim@mi.uib.no
<http://www.mi.uib.no/~eirik>

System Administrator
Math. Department
University of Bergen

-
- **Next message:** Wolfgang Kueter: "Re: How to Stealth POP3 Port 110 using NIS2000?"
 - **Previous message:** ^Caladin: "Astaro --> Anyone Have any insight?"
 - **In reply to:** Nameless: "Re: How to Stealth POP3 Port 110 using NIS2000?"
 - **Next in thread:** Wolfgang Kueter: "Re: How to Stealth POP3 Port 110 using NIS2000?"
 - **Reply:** Wolfgang Kueter: "Re: How to Stealth POP3 Port 110 using NIS2000?"
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]