

Re: How to Stealth POP3 Port 110 using NIS2000?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-02/1246.html>

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

Date: 02/13/02

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

Date: Wed, 13 Feb 2002 10:43:04 -0500

Nameless,

"Nameless" <nameless@noname.com> wrote in message news:rpta8.24957
|. . . I probably wouldn't be having the kind of
| problems I am currently having with NIS2000 if I knew more about them.

Well, actually you would because each vendor, in its own inimitable
fashion, chooses to get a bit obscure about exactly how it does what it
does. (And this is as true of ZA/ZAP as it is of NIS/NPF.)

| 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.

. . . .

If you want to learn more about what NIS actually does, I would suggest
you visit Albert Janssen's site at www.capimonitor.nl and download some of
his freeware add-on utilities for NIS/NPF/AG. Specifically, I would
recommend his AtGuard/NIS Rules Viewer and (assuming you're running an
older version of NIS), his Firewall Log Analyzer (only works up through
NIS/NPF 2.5, last time I checked).

| 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,
| "stealthng", etc. and various other articles on the net. . . .

Steve Gibson is a popularizer. He serves a potentially useful purpose for
individuals new to the concept of internet security, but he is hardly the
end-all, be-all of internet security. This would be like assuming that
Carl Sagan was the ultimate authority among astronomers. (Both Steve and
Carl have provided very valuable services, but) Steve uses a lot
of hype to make his points. Sometimes the hype tends to mislead people.
And most of the time, Steve will never admit it when he makes a boo-boo.
The page may disappear or be quietly re-written, but some of the
information on his website is so outdated (and undated) that those very
self-same novice users reach very wrong conclusions. For example, Steve
was in love with Black Ice Defender BID (prior to Zone Alarm's release).

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

Somehow, Steve missed the point that BID was really an intrusion detection system (IDS), not a firewall. (He got a lot of help misunderstanding that when marketers started writing the copy for the BID website.) To this day, I am not at all sure that Steve understands firewalls like AtGuard, NIS/NPF, Tiny, Outpost, Sygate, etc.

| . . . I am
| unfamiliar with CERT or COAST, but I will seek these sites out on the
| 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?

Well, two sites you definitely want to look at, then, would be
www.cert.org and www.sans.org . (There are many more.) These get to be a
bit heavy (technical) at times, but they're also low hype.

. . . .

| >>> What about asking those questions the vendor of that software?
| >>
| >> Thanks for the tip. I may just do that.

There's no point in asking Symantec; they have some of the worst technical
support out there, especially for their firewall products (not that this
is unique in the PSF market, however).

. . . .

| . . . Another product may be a good idea and that's where I'm
| considering the free ZoneAlarm. One of my questions was whether I might
| expect it and NIS2000 to work okay together, since I don't want to give
| up NIS2000 until I'm comfortable with an alternative and satisfied that
| the alternative is at least as good as what I've currently got.

Well, AFAIK, they will work together. However, ZA (free) is hardly what
I would characterize as tighter than the default rules that NIS would
install for a particular application. Indeed, ZA (free) actually goes the
other direction. For a given client application, once you've allowed it,
you've just given outbound permission for that application to use all
local IP addresses, all local services (ports), to all remote IPs and
all remote services (ports). Use Albert's app and take a look at your
NIS rules for an application. I think you'll find that they are typically
far more restrictive. Indeed, most NIS users are complaining about the
fact that the NIS rules are still too slack! <g> (You can use Albert's
Firewall Log Analyzer to determine where you personally can tighten them
up further for your particular situation.)

--

Regards,
Joseph V. Morris
jvmorris@erols.com
ICQ #29438199

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

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:* [c5d: "blocking svchost"](#)
- *Previous message:* [Dr. Bob: "Re: Tiny or Zone Alarm?"](#)
- *In reply to:* [Nameless: "Re: How to Stealth POP3 Port 110 using NIS2000?"](#)
- *Next in thread:* [Eirik Seim: "Re: How to Stealth POP3 Port 110 using NIS2000?"](#)
- *Next in thread:* [Wolfgang Kueter: "Re: How to Stealth POP3 Port 110 using NIS2000?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)