

Re: Norton Firewall question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-01/1365.html>

From: NeoSadist (*neosad1st_at_charter.net*)

Date: 01/17/04

Date: Fri, 16 Jan 2004 18:10:52 -0700

doug the red wrote:

> *When my computer receives an attack how can I tell which is the*
> *destination port?*

Incoming means that the destination port is the port it wants on your PC. So if Norton is saying you're being attacked on port 80, that should be the destination port. Norton could be over-simplifying things by telling you the port without destination / source specification, so let me give you an example:

My computer asks for a web page

My computer sends a SYN tcp packet originating on MY port 80

Therefore the packet looks like outgoing destination port 80, source port 3072.

The server gets the packet, which was going over port 3072 while on the internet, but when it gets to the last hop gets reassembled to arrive on the server's port 80.

To the server, it looks like source port 3072, destination port 80 incoming.

The server sends back information to my port 80. The packet looks to the server as outgoing source port 3072 destination port 80.

My machine gets the data as source port 3072 destination port 80, which it sees as incoming port 80 information.

The destination port is the port you either want them to see the request on, or is the port they want you to see the data on.

Here's an example firewall log:

```
18:02:19 kernel IN=eth1 OUT= MAC=00:40:d0:0b:f6:39:00:0a:8b:6e:3c:8c:08:00
SRC=213.48.73.94 DST=24.241.184.247 LEN=48 TOS=0x00 PREC=0x00 TTL=111
ID=6196 DF PROTO=TCP SPT=36945 DPT=4091 WINDOW=16384 RES=0x00 SYN URGP=0
```

This is from IPTables (smoothwall). You see that this packet, logged by the kernel, came in over ethernet adapter #1 (network card #2), from that MAC address, from 213.48.73.94. Its destination was me (24.241.184.247), the protocol was TCP, the source port was 36945 (random port while being sent), the destination port (the port it was delivered to on my machine) is 4091, and it was a connection request (SYN flag).

comp.security.firewalls: Re: Norton Firewall question

I know how you might feel right now: this stuff is complex. I also feel that the personal firewall market has to cater to people who don't know and don't care to know how the firewall works: they just want it TO work. It's understandable why you don't know these things: probably no one bothered to teach you. My examples are simplified, but they're about as close as I can get to explaining the thing. For now, when NPF tells you it's an attack on port 80, that means it was coming to you over destination port 80. I don't know if NPF's logs get that specific.

--

This restaurant was advertising breakfast any time. So I ordered french toast in the renaissance.

- Steven Wright, comedian