

Re: Random unprivileged TCP ports below 5000 kind-of open for a fraction of a second

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-12/0142.html>

From: alfaentomega (alfaentomega@yahoo.com)

Date: 12/27/02

Date: Fri, 27 Dec 2002 00:27:47 -0800 (PST)

From: alfaentomega <alfaentomega@yahoo.com>

To: Fyodor <fyodor@insecure.org>

----- Fyodor <fyodor@insecure.org> wrote:

>

> *This may be a problem with your Linux kernel. When Nmap (or many other applications, such as Telnet) does a connect() call, the OS is supposed to choose a good source port to bind to for the connection. When you connect() to a ephemeral port (1024-4999 or so) on localhost, there is a chance that the system will decide to use as a source port the very port you are connecting to.*

Thanks, now I understand.

When I got your answer on December 24th, I typed:

```
while ;; do p=$RANDOM; nc -vzp $p localhost $p; done
```

just after I read this paragraph, and I instantly stopped worrying when I saw a familiar "Connection reset by peer" every time the random port was available. I had no time to write an answer back then, but thanks for giving me a peace of mind as a Xmas gift. :)

> *In a bizarre twist, the application then ends up "connecting to itself"! I consider this to be a Linux kernel bug, but my reports to the linux-kernel list (and offers to fix the problem) have been unheeded.*

Very interesting stuff, I didn't know about it. I made few (actually few million) tests and it seems that it's no longer possible to telnet to your own socket, at least on my 2.2.20 kernel with Debian version of Linux NetKit telnet 0.17-18.

But, while the usual error is

```
"telnet: Unable to connect to remote host: Connection refused"
```

there is sometimes a different error

```
"telnet: Unable to connect to remote host: Connection reset by peer"
```

SecurityFocus Incidents: Re: Random unprivileged TCP ports below 5000 kind-of open for a fraction of a second

every few thousands tries, when (obviously) the source and target ports are the same.

So there doesn't seem to be any workaround in telnet, which would retry a connection when the source and target ports are the same and the ip is local (otherwise there would always be only "Connection refused").

It looks like there's a workaround (?) in the kernel, which doesn't pick another port in the case of collision before connection by connect() (which was the first solution I thought about), but gives "Connection reset by peer" instead of picking new source port, trying to connect, and giving "Connection refused."

I'm a little bit confused right now, but I think that even when the source and remote port is the same and such a connection is made, the correct error returned should be "Connection refused," like for any other port, which is not open for listening. This would be consistent with e.g. trying to connect to the port from which some other outgoing connection is already made. Is there any reason why the error should be different here?

I'm not quite sure if I understand your linux-kernel post you linked to. Did "nc -p 2000 localhost 2000" actually make a connection to itself on the kernel you wrote the bug report about? Because now on my kernel (2.2.20) it doesn't (Connection reset by peer), neither does telnet when it gets the same source as target port, but the Nmap scan still shows that the port is open in such a case. Does it get the same "Connection reset by peer" error and assumes (very reasonably in my opinion) that that port had to be open, if the connection was reset by peer?

- > *So the short summary is that it is just a Linux bug which the*
- > *developers argue is a feature that they don't intend to fix.*
- > *I do have a workaround in place for Nmap versions released in the*
- last*
- > *two or three years -- what version of Nmap are you using and what are*
- > *the exact command-line arguments?*

I'm using Debian version of Nmap 2.54.31.BETA-1. This is the latest version available in Debian 3.0 Woody, the current stable release.

Could you briefly say how does your workaround work? Do you check if the source and target ports were the same (only if the target IP is local, I suppose) and retry then?

- > *New versions of the Nmap Security Scanner can be found at*
- > *<http://www.insecure.org/nmap/>*

Yes, I know. I was too paranoid (after my last compromise) to use anything network/security-related which is not part of the official Debian stable release, and it seems like my paranoia lost me. (Who

SecurityFocus Incidents: Re: Random unprivileged TCP ports below 5000 kind-of open for a fraction of a second

would have thought?)

Thanks a lot for your reply, you saved my Xmas. :) Because I was almost sure my system had to be compromised and I was scared because I had really no idea how and what was actually happening.

By the way, I think Nmap is a great tool, it's my personal scanner of choice. I don't have much experience in such tools, but I've tried and examined the interface and features of every port scanner there's available in Debian, and I've chosen Nmap which I find the best in every field, I'm serious. You did a really great job. Thanks.

I'm starting to learn more about network and systems security-related stuff, and after I'll learn enough theory, I'm planning to learn more practical knowledge from Nmap's source code. I don't think I'm ready yet and I'll probably start from something simpler, like netcat, but Nmap is so far a program which I think I'll learn the most from.

Oh, and by the way -- Merry Xmas, everyone:
nmap -sX -iR -p1-
;)

Thanks.
-Alfaentomega.

Do you Yahoo!?
Yahoo! Mail Plus – Powerful. Affordable. Sign up now.
<http://mailplus.yahoo.com>

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>