

Re: [fw-wiz] OT? New compromise.

Re: [fw-wiz] OT? New compromise.

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2007-03/msg00083.html>

- *From:* Victor Williams <vbwilliams@xxxxxxxxxxx>
 - *Date:* Wed, 28 Mar 2007 15:55:46 -0500
-

I guess what I was alluding to was that the two ports are KNOWN to be used by two applications that are often targeted. MSN IM is a known vector of being attacked as well as mounting an attack.

It didn't seem to me the OP was aware that that's what commonly used those ports. For me, I would start looking at how many of the "virusey" workstations were running IM clients (by default, on purpose, or un-beknownst to the end-user), and go from there...that may quicken the revealing of a rootkit or other malware. Likewise, start looking at default junk that sets to start when the OS starts in the registry.

Fedora 4 loads more stuff than you think with the default install...likewise, unless you specifically disallow it, there's all kinds of crap that is turned on by default...one of them being root being able to login directly over an SSH session. So, not really puzzling to me why a Fedora box would be showing signs of being compromised as well. I've seen it happen the same percentage as Windows boxes.

Stian Øvrevåge wrote:

On 3/28/07, J. Oquendo <sil@xxxxxxxxxxxxxxxxxxx> wrote:

St John, Richard wrote:

Once you determine there might be an issue, I think there used to be a program called openports which would run on the machine and relate any LISTENING or ESTABLISHED ports to the actual file that has the port open. This would then give you the service/process/program waiting for traffic on that port.

Re: [fw-wiz] OT? New compromise.

Re: [fw-wiz] OT? New compromise.

On Windows

```
/c:\netstat -an |find /i "listening"/
```

Why download when you can use existing tools...

Ever heard of rootkits?

And I also think that even if port so and so is listed as belonging to this and that innocent application is fairly irrelevant. I know for sure if I wrote a virus/worm (if that's what it is) like this I'd pick ports that would blend in. From what I understand a large anomaly is what made Jim do some digging, statistics is a wonderful thing, and I'm pretty certain that statistic anomalies like this is not coincidental. The anomaly itself need not be caused by any party that means harm. But the other signs (though vague) of foul play indicates, imho, that it might well be.

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxx

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>