

Re: May this be an hacker attack?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-06/1303.html>

From: Lars M. Hansen (badnews@hansenonline.net)

Date: 06/19/02

From: Lars M. Hansen <badnews@hansenonline.net>

Date: Wed, 19 Jun 2002 01:30:53 GMT

On Wed, 19 Jun 2002 01:37:47 +0200, Wizard spoketh

>Hi everybody.

>

>My linux firewall logged two times a port scanning from a private network IP

>like 172.16.x.x. What I know is that that address shouldn't be used in a

>public network.

>Here is an extract from the firewall's log file:

>Jun 1 02:21:06 firewall kernel: from_pub: IN=eth0 OUT=

>MAC=00:40:c7:95:6c:fa:00:01:c9:2e:f4:54:08:00 SRC=172.16.3.4 DST=<my public

>IP> LEN=92 TOS=0x00 PREC=0x00 TTL=244 ID=4473 DF PROTO=TCP SPT=119

>DPT=1363 WINDOW=8760 RES=0x00 ACK PSH URGP=0

>

>I verified my linux box and didn't find trojan-like processes, nor opened

>ports or connections. I think my box is safe.

>My internal network uses IP like 192.168.x.x, I'm the only user in this

>site, so I can exclude internal attacks.

>With tracepath i can hop the first public node, but the second filters my

>traffic.

>Here's what I suppose: my provider misconfigured the node where I'm

>connected, passing through illegal traffic but the

>second node filters correctly. Someone connected to my same node noticed the

>bug and plays at the hacker, scanning

>through the unfiltered node.

>Someone has an idea of what's going on? Am I arguing in the right way?

>

>Thanks everybody for your suggestions.

>

>Wizard

>

Since private IP addresses are only blocked on routers (or should be), it is possible that someone on the same node as you have misconfigured something on their end, which is causing these private IP address to get out onto the wire. Since it doesn't pass any routers, it doesn't get dropped.

comp.security.firewalls: Re: May this be an hacker attack?

Since you are running a firewall, and it obviously blocked the nntp probe, I wouldn't lose any sleep over it.

Lars M. Hansen

<http://www.hansenonline.net>

(replace 'badnews' with 'lars' in e-mail address)

- *Next message:* [VermiciousKnid: "Re: SonicWALL Basic Support?"](#)
- *Previous message:* [Douglas: "Re: Sonicwall SOHO – How fast does it route?"](#)
- *In reply to:* [Wizard: "May this be an hacker attack?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)