

Re: Have firewall/internal network, but still receiving probes from AOL user -- how?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-12/0367.html>

From: harry wong (wong_at_aol.com)

Date: 12/07/03

Date: Sun, 07 Dec 2003 11:40:20 GMT

No matter what hardware or software firewall you have, whenever you're connected to the internet, your ISP is going to assign an IP address to you. You are always going to have folks who go trolling for trojans (hitting on a range of ip addresses) which is what is probably happened here. My only surprise is that it only occurred once.

What you really should be worried about is going to a shady website that will install various forms of spyware (with a trojan slipstreamed on perhaps) that will get through anything without a restrictive ruleset. And you better have a few layers of AV/spyware/antitrojan protection on your machine to catch slips.

Not that I want to make you paranoid.

"Anonymous User" <googleTrashBin@yahoo.com> wrote in message news:39af109b.0312070134.5389ee79@posting.google.com...

- > *I checked my software-firewall's log (Sygate Personal) today, and*
- > *noticed that it showed what looked like someone at AOL hitting of my*
- > *ports. I didn't write down the info before clearing the log,*
- > *unfortunately, but *did* note that it was IP 172.198.145.77, which*
- > *traceroute showed to be "ACC6914D.ipt.aol.com"*
- > *(could always be spoofed, I suppose).*
- >
- > *I don't know a whole lot about setting up firewalls, but I know that*
- > *my DSL modem can function as a rudimentary firewall, and I have it set*
- > *up to act as one, and assign internal IP's with DHCP, and using NAT.*
- >
- > *I'd think that with such a setup, I'd be safe. How could someone get*
- > *through both hardware and software firewalls (Sygate was allowing the*
- > *access), know my internal IP (okay, it's a typical one for an internal*
- > *network), etc.?*
- >
- > *Or am I somehow mistaken in this, and I'm not seeing what I *think**
- > *I'm seeing?*