

Re: IP address spoofing

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-09/0366.html>

From: Moe Trin (*ibuprofin_at_painkiller.example.tld*)

Date: 09/11/04

Date: Fri, 10 Sep 2004 20:44:33 -0500

In article <8a22k0597p4n0p5k605nqg0h10vuqvpq8c@4ax.com>, JC wrote:

> *On Thu, 09 Sep 2004 19:20:20 -0500, ibuprofin@painkiller.example.tld*

> *(Moe Trin) wrote:*

>> *1. Ever heard of "denial of service"?*

>

> *I would have expected a much higher frequency than say 10 per day.*

>

> *In the last 2.5 days I have received 872 UDP packets from 14 IP addresses all*

> *belonging to one Washington ISP. Even this, while annoying, doesn't appear to*

> *be sufficiently frequent to be an actual "denial of service" attack.*

Yeah, that sounds more like the (unfortunately) increasing background noise of the Internet now.

Technically, any "unwanted" packet (or action on your part) is an added burden – and that is denying you the use of that bandwidth or time. It would be nice if there was no unwanted packets or actions needed on your part, but that's life.

>> *2. Ever heard of UDP?*

>

> *These are mostly UDP packets being dropped.*

Likely a lot of it is messenger spam. You don't need a firewall to stop that – just disable that "feature" on your O/S. As far as 'wasting bandwidth' over the wire, there really isn't that much you can do because UDP is connectionless. The packet is sent – you will receive it, and the only difference being where does it get ignored – at the firewall, or the O/S or whatever.

>> *One could also be playing with your head, if they know you are logging*

>> *everything – I supposed wasting your time chasing shadows could also be*

>> *called a denial of service attack.*

>

> *That is possible. I am retired now*

Isn't it wonderful? ;–)

*>and have a bit of spare time in the yawning to check out the log.
>However, The perpetrator would need to be aware of this prior to
>starting the probes for this to be a factor.*

It's a fairly safe bet. Many home users who do have a firewall do have logging turned on, and all to many of them are actually wasting time reading those logs. Most don't have a clue what the logs mean, nevermind what the information is. Your firewall stopped it, and that's about all you need to know. Where it came from? A lot of it's coming from zombie boxes run by home users on wider bandwidth links (DSL or cable) that are taken over by the spammers. In most cases, these owners really shouldn't be using a computer, much less one connected to the Internet. They don't want to take the time to learn how to use it, and more importantly, how to protect it. Worse still, shooting a few hundred thousand owners of zombie boxes would have no effect, because the rest of the owners are to stupid to be using the computer in the first place, and wouldn't "get the message".

*>I doubt that the CIA et al are interested in me and it is entirely
>possible that they would be able to get through the firewall without
>raising any alarms via some "backdoor" so I discount that idea.*

Actually, it's relatively easy to prevent infection over the wire, and that includes installation of nasty stuff by those non-existent agencies. But if they really were interested in you – you'd better have 24 hour a day guards that you trust totally, to prevent someone from gaining physical access ;-)

*>I also realise that I am not the sole target for these probes. I
>approach the ISP on 2 grounds – the probes are filling up my logs and
>they are also contributing to internet traffic. If they can be stopped
>then that reduces the size of my logs and makes the internet easier to
>use which are both pluses in my book.*

As mentioned – UDP is connectionless, so if someone actually does send this crap, it's going to waste bandwidth and CPU cycles all the way up to the point where it gets dropped. If you are lucky, your ISP might be convinced to drop UDP messenger spam at their perimeter. One of my ISPs drops all packets on ports 135, 137–139, 445, and 1025–1029 inbound AND outbound. My primary ISP won't do that.

Old guy