

Re: Port 1214 – Is It Used For A Specific Purpose?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-11/6805.html>

From: Eric Anderson (anderson@centtech.com)

Date: 11/26/01

Date: Mon, 26 Nov 2001 11:41:55 -0600
From: Eric Anderson <anderson@centtech.com>
To: Drew Tomlinson <drew@mykitchentable.net>

The only time I have seen mass 1214 ports probes is when running mp3 p2p clients, like morpheous or kazaa.

Eric

(Sorry if someone mentioned this already, I missed a chunk of mail)

Drew Tomlinson wrote:

>
> ----- Original Message -----
> From: "Ian Smith" <smithi@nimnet.asn.au>
> To: "Drew Tomlinson" <drew@mykitchentable.net>
> Cc: <freebsd-security@FreeBSD.ORG>
> Sent: Monday, November 26, 2001 6:49 AM
> Subject: Re: Port 1214 – Is It Used For A Specific Purpose?
>
> > On Sun, 25 Nov 2001, Drew Tomlinson wrote:
> >
> > > I was looking over my firewall logs this morning and noticed that
> > > there
> > > are many attempts to connect to TCP port 1214 from different
> > > addresses.
> >
> > Good replies re the specific gadget, but you'll be seeing similar
> > scans
> > for any number of mystery ports to every accessible address in your
> > net.
> >
> > > [..]
> >
> > > P.S. 192.168.10.2 is my outside interface to my firewall. I know
> > > it is
> > > a private address but it's OK as my ADSL modem/router gets a public
> > > address from my ISP via DHCP and performs NAT for the rest of my
> > > machines.

FreeBSD–Security: Re: Port 1214 – Is It Used For A Specific Purpose?

> > >
> > > *ipfw: 65500 Deny TCP 141.157.125.23:1042 192.168.10.2:1214 in via*
> *ed1*
> > [..]
> > > *ipfw: 65500 Deny TCP 172.191.120.23:2453 192.168.10.2:1214 in via*
> *ed1*
> >
> > *I don't understand why a firewall, upstream on ed1 as you describe it,*
> > *would be passing TCP setup for this port on to you in the first place,*
> > *unless it's a service that's been specifically allowed?*
> >
> > *Perhaps I misunderstand the topology – is this your local ipfw*
> *logging?*
>
> *My network setup is like this:*
>
> *ISP*
> |
> | *IP is DHCP (RFC 1918 & draft–manning nets*
> | *inbound blocked here)*
> |
> | *ADSL Modem/Router (provides DNS & NAT)*
> | *192.168.10.1 RFC 1918 & draft–manning nets*
> | *outbound blocked here)*
> |
> | *192.168.10.2 (ed1)*
> |
> | *Firewall (FBSB/IPFW Box)*
> |
> | *192.168.1.2 (ed0)*
> |
> | *Internal Network 192.168.1.0/24*
>
> *The ADSL modem/router (3Com OCR 812) is set to forward all packets to*
> *the FBSB box. The modem/router has limited filtering capabilities*
> *unless I can figure out how to write what the manual terms as "generic*
> *packet filters" where one actually calculates the offset and examines*
> *then next "n" bytes (bits?). But irregardless of the type of filter,*
> *there is no logging as far as I can tell. I setup the FBSB box as a*
> *firewall for finer control and so that I could see what's happening via*
> *log files. In other words, the modem/router is mostly a modem. Because*
> *I have been unsuccessful in setting it up as a bridge (which is what I*
> *think I really want), I left NAT running on the router as there's no*
> *reason to NAT twice.*
>
> *Ultimately, I would like the modem/router to be a modem only and pass*
> **everything* (isn't this what a bridge does?) to ed1 on my FBSB box so I*
> *may filter it there. When I originally signed up for DSL, the modem my*
> *telco offered would only work with Windows as there was no "dial–up"*
> *software for PPPoA. Thus I went for the router as it does the "dial–up"*
> *internally.*

FreeBSD-Security: Re: Port 1214 – Is It Used For A Specific Purpose?

>
> *I've fiddled with my setup several times and this is the best I could*
> *come up with. However I'm always open to suggestions.*
>
> *Thanks,*
>
> *Drew*
>
> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> *with "unsubscribe freebsd-security" in the body of the message*

--

Eric Anderson anderson@centtech.com Centaur Technology
An unbreakable toy is useful for breaking other toys.

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message