

Re: Help with identifying scan/attack

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-06/0125.html>

Valdis.Kletnieks_at_vt.edu

Date: 06/16/03

To: Derrick Teo <deric@deric.NET>
Date: Mon, 16 Jun 2003 00:48:58 -0400

On Fri, 13 Jun 2003 18:35:43 +0800, Derrick Teo <deric@deric.NET> said:

> *I would very much appreciate some help in identifying the nature of*
> *a scan/attack on one of my servers earlier today.*
>
> *Snort picked up a series of packets of a wide range of protocols*
> *with seemingly random (and mostly invalid) source and destination IPs. This*
> *carried out continuously for about an hour. During this time, there was*
> *massive lag and packet loss (roughly 2000ms ping with 50% loss) to even*
> *hosts on the same (100MBit) switch even though MRTG showed only less than 5%*
> *of the link in use.*

Hmm.. and I'll bet that the problem was seen ONLY on the one switch, and that MRTG is measuring the load on the OTHER end of the wire...

> *After the scan/attack stopped, ping times immediately*
> *went back to normal.*
>
> *Has anyone else seen anything like this before?*
>
> *Excerpts of logs follow:*
> -----
> *Jun 13 15:29:16 nemesis snort: [116:1:1] (snort_decoder) WARNING: Not IPv4*
> *datagram! {IP} 16.0.155.69 -> 11.254.0.0*
> *Jun 13 15:29:19 nemesis snort: [116:1:1] (snort_decoder) WARNING: Not IPv4*
> *datagram! {TCP} 0.0.136.8:0 -> 0.1.0.0:0*
> *Jun 13 15:29:50 nemesis /kernel: arp: unknown hardware address format*
> *(0xd004)*
> *Jun 13 15:29:50 nemesis /kernel: arp: runt packet*

This smells like a hardware problem, especially given the last 2 lines quoted.

My first guess is a bad crimp on an RJ-45 or a kinked/bad cable. My second guess is a tech used a Cat-3 jumper cable where Cat-5 was called for, and the resulting signal quality loss caused lots of stray/spurious packets. I've also seen similar fun on an over-length thinwire or thickwire subnet, where late

SecurityFocus Incidents: Re: Help with identifying scan/attack

collision detection caused fun and games with mangled packets.

Usually, such 'jabbering' results in an extremely high congestion level on the net – and the Snort packets you are seeing logged every 15–20 seconds are the statistically tiny percentage of jabbered mangled packets that happen to be valid 802.3 packets, while your interface card is probably throwing away thousands of totally borked packets per second because they have failed even the rudimentary framing requirements at the wire level (the 802.3 standard does specify a link-level checksum, among other things).

The only saving grace for debugging these is that the problem hardware is almost always on the same physical segment as the problem is manifesting, as the problem is confined to a single thinwire/thickwire segment or twisted-pair connected with a low-end hub that operates at layer-2. A layer-3 switch that does filtering on MAC addresses or a router will stop these, simply because the hardware doesn't accept the broken packets for forwarding.

And yes, I've even seen cases where a broken cable ran under a window, and it would fail/work based on whether the window was open (the resulting temperature difference caused the wires to expand/contract just enough to make/break). We finally had to TDR(*) the cable to find THAT one...

/Valdis

(*) TDR – Time Domain Reflectometer – basically, send a pulse down a thinwire/thickwire cable, and every network tap or other break sends back an echo. Think of it as sonar for Ethernet. ;)

-
- application/pgp-signature attachment: [stored](#)