

Re: UDP Port Sweep question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2004-12/0077.html>

From: Ron (iago_at_valhallalegends.com)

Date: 12/29/04

Date: Wed, 29 Dec 2004 11:05:28 -0600

To: CraftedPacket@securitynerds.org

I often see UDP_PORT_SWEEP hits from virus scan servers. Virus scanners will look for their clients on a udp port, and trigger the signature. We just set up a rule to ignore antivirus boxes' udp probes.

Of course, it may also be something totally different, but that's one thing that could cause it.

Billy Dodson wrote:

>I monitor 3 different sensors which are continuously pounded with network
>reconnaissance of all types. These sensors all belong to financial
>institutions. One thing that jumped out at me are "UDP Port Sweeps"
>events from about 15 different IP addresses which all belong to either IBM
>or Sequent (which was bought by IBM). I see these same IP addresses doing
>the same thing on all three sensors. I have contacted the clients and
>they do not deal with IBM or Sequent in any way. Are there legitimate type
>traffic
>that would cause these events to fire? It is odd to me that I see them on
>all 3 sensors for 3 different companies but all happen to be in the
>financial industry. Thanks in advance for your input.
>
>
>
>