

Administrivia: Are you seeing portscans from source 127.0.0.1 source port 80?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-10/0132.html>

From: Dan Hanson (dhanson_at_securityfocus.com)

Date: 10/28/03

Date: Tue, 28 Oct 2003 08:59:56 -0700 (MST)

To: incidents@securityfocus.com

I am posting this in the hopes of dulling the 5-6 messages I get every day that are reporting port scans to their network all of which have a source IP of 127.0.0.1 and source port 80.

It is likely Blaster (check your favourite AV site for a writeup, I won't summarize here).

The reason that people are seeing this has to do with some very bad advice that was given early in the blaster outbreak. The advice basically was that to protect the Internet from the DoS attack that was to hit windowsupdate.com, all DNS servers should return 127.0.0.1 for queries to windowsupdate.com. Essentially these suggestions were suggesting that hosts should commit suicide to protect the Internet.

The problem is that the DoS routine spoofs the source address, so when windowsupdate.com resolves to 127.0.0.1 the following happens.

Infected host picks address as source address and sends Syn packet to 127.0.0.1 port 80. (Sends it to itself) (This never makes it on the wire, you will not see this part)

TCP/IP stack receives packet, responds with reset (if there is nothing listening on that port), sending the reset to the host with the spoofed source address (this is what people are seeing and mistaking for portscans)

Result: It looks like a host is port scanning ephemeral ports using packets with source address:port of 127.0.0.1:80

Solution: track back the packets by MAC address to find the infected machine. Turn off NS resolution of windowsupdate.com to 127.0.0.1.

Hope that helps

D

SecurityFocus Incidents: Administrivia: Are you seeing portscans from source 127.0.0.1 source port 80?

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at http://www.securityfocus.com/sponsor/RSA_incidents_031023 and use priority code SF4.
