

Re: Firewall trapping outbound probes to TCP 1120 from W2K gateway box

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-03/1335.html>

From: Karl Levinson [x y] mvp (levinson_k@excite.com)

Date: 03/11/03

From: "Karl Levinson [x y] mvp" <levinson_k@excite.com>

Date: Tue, 11 Mar 2003 08:10:46 -0500

Might not necessarily be anything malicious. Depending on the way your network is set up, it could be absolutely normal for your gateway computer to see messages between two internal computers and block this. I might check both the source and destination machine using IPCONFIG /ALL or WINIPCFG to confirm that the subnet mask and DNS server IP addresses are correct, as these could cause internal traffic to be sent incorrectly to your gateway.

As you may know, Windows chooses an ephemeral port above 1024 as the source port when opening connections such as windows networking on TCP 139, and the port number usually increases with each new connection. Eventually a "suspicious" port number like 1243 is used as the source port. Also, when the reply comes back, a firewall or IDS system may tell you that the responding computer is scanning destination port 1243, when really it's just a normal reply.... e.g. what looks like the destination port and IP address are really the computer that started the connection.

I might check both computers to determine whether it is normal for one computer to be initiating communications with the other.

You might also:

1) try using a sniffer [or the www.sygate.com personal firewall] to inspect the packet contents and try to determine what it is. An IDS like Snort might not be a bad thing to start thinking about too. Also www.mynetwatchman.com or www.dshield.org free software can help you by letting you see whether a particular internet IP address is also scanning other networks besides yours.

2) Check this out:

<http://securityadmin.info/faq.htm#hacked> [start here]

<http://securityadmin.info/faq.htm#re-secure>

<http://securityadmin.info/faq.htm#harden> [important too]

microsoft.public.win2000.security: Re: Firewall trapping outbound probes to TCP 1120 from W2K gateway box

IMHO formatting and reinstalling does nothing to help if