

Re: false portscan alarm

Re: false portscan alarm

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-10/msg00376.html>

- *From:* "Spack" <news@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 18 Oct 2006 16:09:59 +0100
-

GEO wrote on Wed, 18 Oct 2006 13:47:10 GMT:

On Wed, 18 Oct 2006 08:41:04 +0100, "Spack" <news@xxxxxxxxxxxxxxxxxxx> wrote:

On Tue, 17 Oct 2006 13:23:40 +0200, mikahan wrote:

I receive regular notification from my personal firewall about port scanning made by www.microsoft.com. This is the information from my log

2006-09-12 09:20 port scan from
207.46.18.30 TCP (1700, 1730, 1734,
1733, 1168, 1165)

207.46.18.30 is www.baytest5.microsoft.com

Which is just one of a large cluster of servers running www.microsoft.com.

Does it mean that Microsoft try to hack me ?
:-)
What is the reason of that traffic ?

Looking up those ports at
http://isc.sans.org/port_details.php?port=1730 (example)
would seem to indicate www.baytest5.microsoft.com has

Re: false portscan alarm

some malware
hunting for more exploitable systems.

Or those packets are simply responses to connections initiated from the user end and closed prematurely. For instance, the user opened a browser to www.microsoft.com, and it took a while for the MS server to respond, and the browser and/or the "personal firewall" had decided to close those ports prematurely. Each of those "port scans" could be a response to a request for various files used by a web page – images, scripts, etc – which each have a local source port above 1024 opened outgoing to port 80 on the web server, so the response data will come back to those source ports.

This is just the usual sort of completely harmless and normal activity that these so called "personal firewalls" like to warn people about when there is absolutely no reason to. It breeds fear in the computer illiterate, encouraging them to spend money on more "personal security" products, which is probably one of the reasons that these "personal firewalls" spew this rubbish.

I would disagree with your explanation since I have no firewall, and don't connect to MS, and yesterday I was receiving UDP packets from the same range of addresses (207.46.18.xx). Today I have received UDP packets from 204.16.208.74.

Either the explanation that ' www.baytest5.microsoft.com has some malware hunting for more exploitable systems' is correct, or they have managed to spoof the IP address.

Geo

I've had a dig through my own PIX logs, and while there is nothing for today or yesterday, I am seeing UDP packets from IPs in the same range in earlier logs. Something strange is going on here, as at least one of those IPs belongs to a Window NT4 server so definitely doesn't have anything installed that would talk to MS, and one is to an IP that has all outbound access denied except to one IP in the PIX DMZ, so could never initiate a connection to anywhere on the internet.

I need to go and rebuild my honeypot/sniffer machine and get it back outside my firewall so I can capture a few of these packets.

Dan

.

Re: false portscan alarm