

Re: all port scan attack notifications

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2006-06/msg00084.html>

- *From:* "Ray" <noemails@please>
 - *Date:* Fri, 9 Jun 2006 11:30:12 -0400
-

Here's my opinion:

As long as you have verified from the outside that you don't have anything exposed that shouldn't be, and you periodically re-confirm that, it's a non-issue. You will be port-scanned from all over the world all the time. Get used to it.

The threats you have to be really worried about are the ones where someone has painted a target on your back specifically. Those attackers are not going to use something as simple and noisy as a regular port scan. They may scan you, but it may only be one port a day and if they're good, the source IP will be rotated so you don't know it's the same attacker.

Detecting these types of attacks is expensive and time-consuming because they require 100% monitoring and the ability to correlate an astronomical number of events to find the pattern. For most companies, it's a better tactic to throw as many hurdles in front of any attacker as you can.

If you don't do any business with Asia-Pacific, set an ACL on the router between ISA & your ISP and drop those routes out. Minimize your footprint on the Internet by using the bare minimum number of IP's. Make sure you use a split DNS system to minimize mapping of your internal network. Use DMZ techniques to limit damage. Have multiple layers of virus inspection. Use an HTTP virus scanner on ISA. Set all of your users as Restricted Users no matter how much they whine and moan. Block all outbound traffic except for that which is specifically allowed (for example, don't allow SMTP outbound except from the IP address of your mail server).

If someone is targeting you specifically, they will find a way in eventually. Your main job is to minimize the damage and improve the detection time when that happens.

Good luck,

Ray

"Rob" <Rob@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:792B4524-83A0-4EC8-8CAD-1B8A6050F649@xxxxxxxxxxxxxxxxxxxx

Re: all port scan attack notifications

Thanks Ray,
can you recomend any other method?
cheers

"Ray" wrote:

They're probably false alarms. ISA's port scan detection has been plagued with this since day 1. Turn it off and forget about it (and use another method of detection).

Ray

"Rob" <Rob@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:520D36C2-73A6-47F9-A9E6-FB4CD04BA941@xxxxxxxxxxxxxxxxxxxx

Hi,
I've been getting notifications about all port scan attacks.
From these I do some investigation and block the offending IP if necessary (if I can tell it's a ISP dial-up/ broadband I). I've recently had some thru that on investigation turn out to be from a companies mail server. Why would a mail server be doing an all port scan attack – surely it would only want to connect to port 25? Or is this just default text in the notification and there is not an actual 'attack'?
Any pointers gladly received.
thanks