

Re: NT 4 server firewall?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-01/0878.html>

From: Lars M. Hansen (*badnews_at_hansenonline.net*)

Date: 01/15/05

Date: Sat, 15 Jan 2005 07:54:49 -0500

On Fri, 14 Jan 2005 20:58:22 -0600, zn spoketh

>
>*And what happens when another Microsoft worm breaks out and starts
>exploiting some bug in the OS. How many times has that happened during
>the last several years? There is always a window where the virus is
>breaking out but new definitions either haven't been prepared or haven't
>made it to the clients yet. A software firewall would help protect
>against this.*

:

But the firewall doesn't protect you from this. Since you need to keep the ports for "normal" windows operation open anyways due to domain traffic, the firewall cannot block these ports, so if the worm hits (from the inside, because your network firewall protects you from outside attacks), then you are out of luck anyways.

>
>
>> *There are no software you can put on a SQL server that will protected
>> it more than it already should be by employing the "best practices"
>> available for securing said server.*
>>
>> *There's nothing worse than upper management second-guessing the
>> security measures put in place by competent administrators. If you
>> really don't trust the administrator, then have someone come in to
>> audit the server and the firewall/routers.*
>
>*You guys have an inferiority complex. Just because you are competent sure
>doesn't mean that every network administrator is.*
>
>*Have you ever dealt with large campus, multiprotocol networking hardware?
>Problems happen -- ports get left open accidentally, firmware may not get
>updated quickly, leaving potential exploits.*

Then do as I suggested: Hire in a Computer/Network security firm to audit your setup. If you really think that your network admin is incompetent, then have someone audit his work as well, then fire him if

he's truly clueless.

>
>> *Just because your senior management read an interesting article in
>> some magazine about "software firewalls" in some know-it-all business
>> magazine doesn't mean that it'll do anything for you...*
>
>*That's just a silly comment. There is no problem running packet filtering
>software on Unix and it's very commonplace. All that I asked about was
>software for doing the same on Windows. Software firewalls are just
>another level of security.*

No, it is not. Software firewalls are mostly a waste of system resources. They cannot protect you from the things you think you need protection from. A software firewall on a SQL server would NOT in any way, shape or form have protected it from the SQLSlammer worm because the firewall would have leave port 1433 and 1434 open so that people can actually use the SQL server.

Windows NT server comes with built-in packet filtering, but that's not going to do you much good anyways. See, out of the 130000+ ports (UDP and TCP combined), only a few are open. On a Windows NT server, that would normally be 135, 137, 138 and 139, plus whatever ports the Oracle database leaves open (sorry, too lazy to look it up). The rest are all closed. Adding a packet filter on the machine itself to further "close" that which is already closed does not add another level of security, it just adds more complexity. And, you can't close the ports that are listening, because that would kill your database server...

As for packet filter software on Unix/Linux, it's just as useless as well, unless you are actually using it as a firewall. There's no point in having IPTables block port 4567 if there's nothing there in the first place...

I don't know your setup, but it sounds like you have some good stuff between the internet and the server, and if you are really in the need for a packet filter on the server in question, that can just as easily be implemented on the switch the computer is connected to, or on a router the separates your valuable servers from the rest of your LAN.

Lars M. Hansen

<http://www.hansenonline.net>

(replace 'badnews' with 'news' in e-mail address)