

Re[2]: Exchange 2003

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-03/0078.html>

From: Marius Huse Jacobsen (*mahuja_at_c2i.net*)

Date: 03/12/04

Date: Fri, 12 Mar 2004 17:03:46 +0100

To: John Swope <johns@akorn.net>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hello,

I have an idea what's going on.

The calls go, both ways, to and from udp/137 on both sides in both cases.

That means, that when the server tries to find out information on the client, it makes an outbound connection. When the query is finished, however, there is nothing that tells the firewall that it's over. When you "create a connection" back to the server, the firewall sees you as sending further responses to the server.

In other words, it would match any "established" rule, after the server was allowed to make an outgoing connection.

Thursday, March 4, 2004, 6:08:49 AM, you wrote:

JS> I noticed the Exchange server was performing 3 NBT broadcasts to try to
JS> resolve the LMHOST name of my box. Naturally it did not work because I'm a
JS> Unix box not running Samba.

JS> So, could the exchange server in your case be doing the same? Would it
JS> explain the results? Is the PIX allowing all traffic from Exchange to
JS> external network? I realize that I was seeing broadcast traffic and one of
JS> the posts in the thread mentioned the boxes are separated by a PIX, just
JS> throwing this in as something worth checking...

>>Nbtstat command is sending packets to udp 137 port of destination. As far as
>>I see, firewall is accepting udp packets, if there is an established tcp
>>>connection from same source to same destination as in udp connection
>>request. I think there is a configuration problem in the customer firewall.
>>For further analysis I requested firewall configuration and logs.

SecurityFocus Penetration: Re[2]: Exchange 2003

>>

>>> *Before I run the portscan, I have controlled the server with "nbtstat" command of windows. It returned error messages as below.*

>>> *Host not found.*

>>> *After the port scan is finished, in order to see the banner information of mail server, I opened the connection to port 25 using telnet command (telnet EXCH_IP 25). Same time when I run "nbtstat -A" command from another window by mistake and I saw that below output.*

>>>

>>> *nbtstat -A EXCH_IP*

>>>

>>> *Local Area Connection:*

>>> *Node IpAddress: [MY_MACHINE] Scope Id: []*

>>>

>>> *NetBIOS Remote Machine Name Table*

>>>

>>> *Name Type Status*

>>> -----

>>> *If there isn't any connection to open port of the server you can't see this nbtstat outputs.*

>>>

>>> *Has any body faced with same situations before?*

Best regards,

Marius mailto:mahuja@c2i.net

-----BEGIN PGP SIGNATURE-----

iQA/AwUBQFHRYJfZ2CSWpu1rEQJMpQCghvmsmggvOkLuVvMVgQ/8i1bF83UAn10s
IMU5XaXpfzxwrrLFmsgt8orc
=yj5t

-----END PGP SIGNATURE-----

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
