

Re: [Full-disclosure] Strange interactions between tunnelling and SMB under the proprietary Microsoft Windows environment

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-03/msg01776.html>

- *From:* Laurent LEVIER <llevier@xxxxxxxxxxxxx>
 - *Date:* Thu, 30 Mar 2006 09:21:10 +0200
-

Hi Marc,

At 07:52 30/03/2006, Marc SCHAEFER wrote:

However, accessing \\192.168.1.2\c\$ did go through the Ethernet interface, and *not the tunnel*, and strangely half-using the private addresses!

This recalls me an old behavior from Microsoft products I was using to detect Internet rogue backdoors on my company's network.

When a windows is multi-homed, it sends packets towards broadcast @IP of each of its addresses to fill his computer browser tables.

Here I am talking about this behavior:

- Internal @IP -> Internal NIC -> Internal @IP broadcast
- Internal @IP -> Internal NIC -> External @IP broadcast
- External @IP -> External NIC -> Internal @IP broadcast
- External @IP -> External NIC -> External @IP broadcast

So you can imagine how this was useful. I was routing internal networks on Internet towards a probe that was also receiving Intranet routers anti-spoofing realtime logs.

When the probe was receiving a packet from outside targetting an internal @IP broadcast, I was correlating with antispoof logs of packets coming from an @IP compatible with this external broadcast towards the broadcast of the source @IP of the packet received from the outside and gotcha.

I dont know if Windoze keeps behavior like this.
Possibly this is related?

Brgrds

Laurent LEVIER
Systems & Networks Security Expert, CISSP CISM

Full-Disclosure – We believe in it.

Re: [Full-disclosure] Strange interactions between tunnelling and SMB under the proprietary Microsoft Windows environ

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Re: [Full-disclosure] Strange interactions between tunnelling and SMB under the proprietary Microsoft Windows