

Re: increase in smb scans

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-03/0067.html>

From: Hugo van der Kooij (hvdkooij@vanderkooij.org)

Date: 03/08/02

Date: Fri, 8 Mar 2002 23:41:59 +0100 (CET)
From: Hugo van der Kooij <hvdkooij@vanderkooij.org>
To: Incidents Mailing List <incidents@securityfocus.com>

On Fri, 8 Mar 2002, Nathan W. Labadie wrote:

> *Has anyone else noticed a _huge_ increase in SMB scans? I'm seeing sweeps
> of various subnets 5-10 times a day. This started around two weeks ago...
> they appear to be looking for open \\<netbios-name>\C shares. My guess is
> that they are looking for machines previously infected with Nimda, but I
> could be wrong. It shows up as "NETBIOS SMB C access" under snort, and
> "Tree Connect AndX Request" when the tpcdump is viewed with ethereal.*

What has puzzled me is that I get netbios-ns request from all over the world on a ADSL link. (Just 1 IP address.) They seem to get in at random moments from random machines.

This is not what I normally get from netbios-ns. You can have a peek at this traffic on <http://hvdkooij.xs4all.nl/fwlog/> and choose for "Overview based on: source IP address and destination port" to get a grasp of what I mean.

This odd thing started from March 4. Before that I see the occasional bursts from badly configured machines doing netbios name lookups for my machine instead of using DNS.

To me this does not seem extremely alarming at the moment but just something I have not seen before.

Hugo.

--

All email sent to me is bound to the rules described on my homepage.
hvdkooij@vanderkooij.org<http://hvdkooij.xs4all.nl/>
Don't meddle in the affairs of sysadmins,
for they are subtle and quick to anger.

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>

SecurityFocus Incidents: Re: increase in smb scans

- **Previous message:** Matt Zimmerman: "Re: sshd: PAM pam_set_item: NULL pam handle passed"
- **In reply to:** Nathan W. Labadie: "increase in smb scans"
- **Next in thread:** Nathan W. Labadie: "Re: increase in smb scans"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]