

Re: MS patch-scanner for Win-NT, 2K, IIS, SQL

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-08/0221.html>

From: Laura A. Robinson (larobins@bellatlantic.net)

Date: 08/16/01

Message-ID: <05b801c1268e\$fd99070\$0b00010a@lauradominion.com>

From: "Laura A. Robinson" <larobins@bellatlantic.net>

To: "Adcock, Matt" <Matthew.Adcock@GSCCCA.ORG>, "'Jean-Pierre Harvey '" <jean-pierre.harvey@edivi>

Subject: Re: MS patch-scanner for Win-NT, 2K, IIS, SQL

Date: Thu, 16 Aug 2001 16:06:51 -0400

Again, you need to read more carefully. You not only cannot *browse* for virtual servers in a cluster, you cannot *search* for them:

Note the following additional implications to virtual server access because of the non-integration with Active Directory:

a.. Clients cannot browse or search for cluster virtual servers in a NetBIOS-less environment. The Computer Browser service uses NetBIOS to distribute and maintain the browse list. For more information about the Computer Browser service in Windows 2000, see the following article in the Microsoft Knowledge Base:

Q188001 Description of the Microsoft Computer Browser Service

To configure a NetBIOS-less environment, the client must have the WINS client property set or inherited from the DHCP server. To determine if this setting on each network adapter is NetBIOS-less or inherited from the DHCP server, view the setting in Network and Dial-up Connections. In the properties for the Internet Protocol (TCP/IP) for each network adapter, view the Wins tab after clicking Advanced. This shows three options:

Enable NetBIOS over TCP/IP

Disable NetBIOS over TCP/IP

Use NetBIOS setting from the DHCP Server

b.. Clients cannot use Kerberos to authenticate a connection to a cluster virtual server. If Kerberos cannot be used, the clients attempt to authenticate with NTLM authentication.

c.. Directory-enabled programs cannot publish under the virtual server's computer object in a cluster. Instead, they are often published under the node's computer object on which the service or resource was installed. For example, Message Queuing Server (MSMQ) is published under all nodes on which the service was installed. The cluster resource creation creates a computer object for the virtual server it is dependent on but does not publish the service there. Another example is the printer; it is published under the node's computer object that ran the Add Printer Wizard.

d.. Administrators of the cluster cannot use the browse functionality of Cluster Administrator to find the cluster name on a network adapter that has NetBIOS over TCP/IP disabled, even if the two computers are on the same subnet.

As I said, you are free to make your own decisions. I made a very simple statement regarding two limitations in Windows 2000 with regards to NetBIOS being required for functionality. I have backed those simple statements with factual documentation. I'm really not sure where your bellicosity is coming from, but it's unnecessary and uncalled for.

Laura

----- Original Message -----

From: "Adcock, Matt" <Matthew.Adcock@GSCCCA.ORG>

To: "Laura A. Robinson" <larobins@bellatlantic.net>; "Jean-Pierre Harvey" <jean-pierre.harvey@edivision.com.au>; "Adcock, Matt" <Matthew.Adcock@GSCCCA.ORG>; "Stadler, Brian T" <bstadler@ukans.edu>; <flynnngn@jmu.edu>

Cc: "Focus on Microsoft Mailing List" <FOCUS-MS@SECURITYFOCUS.COM>; <bugtraq@SECURITYFOCUS.COM>

Sent: Thursday, August 16, 2001 3:55 PM

Subject: RE: MS patch-scanner for Win-NT, 2K, IIS, SQL

> *The situation described is not a problem, it's by design. Without NetBIOS, > browsing in any form doesn't work right anymore. That's because NetBIOS is > the basis of browsing. You have to use the AD search tools, not the methods > you're all used to.*

>
> Matt

>
> -----Original Message-----

> From: Laura A. Robinson

> To: Jean-Pierre Harvey; 'Adcock, Matt'; 'Stadler, Brian T'; <flynnngn@jmu.edu>

> Cc: Focus on Microsoft Mailing List; <bugtraq@SECURITYFOCUS.COM>

> Sent: 08/15/2001 9:10 PM

> Subject: Re: MS patch-scanner for Win-NT, 2K, IIS, SQL

>
> Jean-Pierre,

>
> *Your question regarding the NetBIOS helper service came up amongst some > colleagues and myself when Windows 2000 was still in beta, and the short > answer, as I recall, is this: the NetBIOS helper service is a service > that*

> *assists in name resolution, not just NetBIOS name resolution.*

> *Essentially,*

> *it's more of a misnamed service than anything else.*

>

> Laura

>

> ----- Original Message -----

> From: "Jean-Pierre Harvey" <jean-pierre.harvey@edivision.com.au>

> To: "Adcock, Matt" <Matthew.Adcock@GSCCCA.ORG>; "Laura A. Robinson"

> <larobins@bellatlantic.net>; "Stadler, Brian T" <bstadler@ukans.edu>;

> <flynnngn@jmu.edu>

> Cc: "Focus on Microsoft Mailing List" <FOCUS-MS@SECURITYFOCUS.COM>;

> <bugtraq@SECURITYFOCUS.COM>

> Sent: Wednesday, August 15, 2001 8:59 PM

> Subject: RE: MS patch-scanner for Win-NT, 2K, IIS, SQL

>

>

>> All,

>>

>> Microsoft do not recommend implementing Win2K without NetBIOS. AD does
>> require NetBIOS features to function correctly:

>>

>> When you are running AD, you can successfully disable NetBIOS from the
> WINS

>> tab of the TCP/IP properties without breaking anything as long as you
> have

> a

>> fairly vanilla implementation. Just don't try disabling the TCP/IP

> Netbios

>> Helper Service, then things will start to break. Of course, this means
> that

>> if an anonymous user has an IP address he/she can still enumerate
> shares,

>> users etc by default. Yes, even if it is disabled in the TCP/IP

> properties

>> of network adapter.

>>

>> Setting the security policy for anonymous users to "no access without
>> explicit anonymous permissions" will give an access denied error when
>> attempting to connect using a null session.

>>

>> Does anyone else find this whole situation a bit strange? Surely if
> you

>> disable NetBIOS over TCP/IP one would expect not to have NetBIOS
> running

>> over TCP/IP.... this does not appear to be the case, since the "helper
>> service" still (pretends to?) use NetBIOS over TCP/IP, or at least
> retains

>> the classic default insecure NetBIOS features allowing anonymous
>> enumeration.

>>

>> JP

>>

>> -----Original Message-----

>> From: Adcock, Matt [mailto:Matthew.Adcock@GSCCCA.ORG]

SecurityFocus Microsoft: Re: MS patch-scanner for Win-NT, 2K, I

> > Sent: Thursday, August 16, 2001 8:13 AM
> >
> > Sorry, but logons don't require NetBIOS in Win2K. As I stated before,
> the
> > directory and OS don't need it at all in a pure 2K environment. Win2K
> > DNS/LDAP can completely replace WINS in a pure environment. WINS was
> a
> > failed implementation of internal DNS, and MS has gone back to a more
> pure
> > directory services implementaion with Win2K DNS/LDAP. From
> > <http://support.microsoft.com/support/kb/articles/Q299/9/77.ASP>:
> >
> > <quote>
> > Windows 2000 uses NetBIOS over TCP/IP to communicate with prior
> versions
> of
> > Windows NT and other clients, such as Microsoft Windows 95. Careful
> testing
> > should be done before disabling NetBIOS over TCP/IP in any production
> > environment. Programs and services that depend on NetBIOS no longer
> function
> > after you disable NetBT services, so it is important that you verify
> that
> > your clients and programs no longer need NetBIOS support before you
> disable
> > it.
> > </quote>
> >
> > I did not mean to imply that it's necessarily a good idea to remove it
> > completely. See
> >
> > <http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/WIN>
> DOWS
> > 2000/en/server/help/sag_WINS_und_NetbiosConceptsNode.htm for a
> discussion
> of
> > where disabling NetBIOS is appropriate and how it affects Win2K
> machines.
> >
> > You're right about the apps, but as far as the OS is concerned,
> NetBIOS is
> > just for backwards compatibility and completely unnecessary.

-
- **Previous message:** [Patrick S. Harper: "RE: Properly securing IIS \(Was: Accessing mail from the web\)"](#)
 - **Maybe in reply to:** [Gary Flynn: "Re: MS patch-scanner for Win-NT, 2K, IIS, SQL"](#)
 - **Next in thread:** [Souza, Chris: "RE: MS patch-scanner for Win-NT, 2K, IIS, SQL"](#)
 - **Next in thread:** [Stadler, Brian T: "RE: MS patch-scanner for Win-NT, 2K, IIS, SQL"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)