

Re: Apparent NetBIOS Attack – How Dangerous?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0284.html>

From: Karl Levinson, mvp (levinson_k_at_despammed.com)

Date: 12/13/04

Date: Mon, 13 Dec 2004 08:25:59 -0500

... for more information on how to secure this and what can break at the various settings, go to www.nsa.gov/snac and download the Windows 2000 group policy guide, think it's the third document, and search it for "restrictanonymou.s." For Win 2000, restrictanonymou.s=1 is usually safe, though it doesn't block all enumeration, just blocks some details from being seen. Restrictanonymou.s=2 is only safe if you have no Windows 9x or ME or NT systems, for example. RestrictAnonymou.s=2 only exists in Windows 2000, for XP and 2003 you use RestrictAnonymou.s and RestrictAnonymou.sSAM, both of which can be either 0 or 1. Search www.google.com for RestrictAnonymou.sSAM if you need more information on XP and 2003 settings.

More information on why this happens and what can be seen are at www.securityfriday.com There is a presentation / article on netbios null sessions, and the free getacct tool lets you see what the hackers can see.

I concur that it sounds like you have no firewall or a misconfigured firewall and you should not be surprised that hackers can get into your domain controllers. Windows is not secure until you secure it. www.microsoft.com/technet/security, www.nsa.gov/snac and www.securityadmin.info/faq.asp#harden have hardening guides for Win 2000.

"Roger Abell [MVP]" <mvpNoSpam@asu.edu> wrote in message news:uKNKGxM4EHA.924@TK2MSFTNGP14.phx.gbl...

> *Aside from failing to use a firewall, you possibly do not have policies set*

> *to that you Do not all anonymous enumeration of SAM accounts and shared*

> *This allows a remote to easily list out your account names and groups,*

> *and attracts further effort due the appearance of an easy meal.*

> *The anonymous enumeration settings can be found in the security*

> *setting options of the local security policy, although slightly differently*

> *worded depending on OS version.*

>

> --

> *Roger Abell*

> *Microsoft MVP (Windows Server System: Security)*

> *MCDBA, MCSE W2k3+W2k+Ni4*

microsoft.public.win2000.security: Re: Apparent NetBIOS Attack – How Dangerous?

> "Thomas" <email@isin.my.message.com> wrote in message
> news:cpira1\$hp\$1@ngspool-d02.news.aol.com...
> >I have been noticing, after checking Windows 2000's Event Viewer's
security
> > protocol, that some individual (from the Internet) is attempting to log
> > into
> > our computer. The attempts --fortunately all failed, so far-- start
> > occurring a few minutes after I establish a PPPoE Internet connection,
and
> > cease after some time. When the attacks begin, they occur for several
> > minutes, sometimes every two or three seconds, sometimes every 10-60
> > seconds, sometimes just once or twice.
> >
> > In the Event Viewer, the alerts look like the following one:
> >
> > The logon to account: <Local account name here>
> > by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> > from workstation: 0WEWCKG1
> > failed. The error code was: 3221225578
> >
> > The error type is 681.
> >
> > Strangely, the individual basically uses every account available in our
> > system. That is, if we have the accounts Administrator, Peter, Thomas,
> > Jane,
> > then the user attempts to login with one or more of these accounts. How
is
> > it possible that our full account list is known to someone on the
> > Internet?
> >
> > As the login attempts occur after packets are sent to local port 137
> > (NetBIOS), I have disabled NetBIOS over TCP/IP, but the login attacks
> > still
> > won't stop. The user still obtains our account list, and the failed
logins
> > still appear on the Event Viewer security protocol.
> >
> > What can be done in order to remedy this situation? If the subject
> > discovers
> > the password for one account, would it be possible for him to eventually
> > "login" successfully, in spite of NetBIOS over TCP/IP being disabled? In
> > that instance, how much access does he actually have, and how much
damage
> > can he do? In advance, I appreciate any information you can provide.
> >
> > Regards,
> >
> > Thomas
> >
> >
> >
>

Re: Apparent NetBIOS Attack – How Dangerous?

microsoft.public.win2000.security: Re: Apparent NetBIOS Attack – How Dangerous?

>