

Re: Network Services accessed after account disabled

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-11/0004.html>

From: DickieRay (*DickieRay_at_discussions.microsoft.com*)

Date: 10/31/05

Date: Mon, 31 Oct 2005 13:51:03 -0800

The test box has NetBIOS over TCP/IP disabled. Hmmmm.

The funny thing is that we don't remember this behavior ever happening when we were using NT Domain. We only started seeing it after we upgraded to AD.

"Karl Levinson, mvp" wrote:

> *I don't know. I'm not sure whether there is a setting to control the
> timeout in Netbios. I seem to remember from years past that when a logon
> token is generated, it stays working for many hours, even with Windows 2000.
> For your clients and servers that only need to support connections from
> Windows 2000 and newer, you may need to disable Netbios over TCP/IP in the
> network card settings under TCP/IP, advanced. Since this setting is
> presumably set per network adapter and not per computer, I'm not sure
> whether it's very easy to automate this remotely via Group Policy or script.
> Test it first to see whether it fixes the problem.*
>
> *In ethereal, netbios would generate TCP 139 and maybe UDP 138. I think
> kerberos would involve TCP/UDP ports 88 and/or 445. Things are slightly
> complicated by the difficulty of running ethereal on a computer while you
> log in, so you could either sniff on the server ,or sniff while you connect
> to a server after logging in and being locked out, or plug two computers
> into a hub and sniff from one while logging into Windows on the other.*
>
>
> *"DickieRay" <DickieRay@discussions.microsoft.com> wrote in message
> news:E5C884B8-AA93-4F96-AD22-6C0ADEE68506@microsoft.com...
>> Thank you for your reply, Karl. That makes a lot of sense.*
>>
>> *Would you be able to point me to the settings for these cached
>> authentication time-outs?*
>>
>> *I'm familiar with Ethereal, but wouldn't know what to look for exactly.*
>>
>> *Thanks again.*
>>

microsoft.public.win2000.security: Re: Network Services accessed after account disabled

> > "Karl Levinson, mvp" wrote:
> >
> > > *That article seems to apply to Kerberos. Is it possible that NTLM or LM*
> > > *authentication is being negotiated, and that different timeouts for*
> *cached*
> > > *logons occur under those conditions? Examining the settings or using*
> *the*
> > > *www.ethereal.com sniffer might help determine this.*
> > >
> > >
> > > "DickieRay" <DickieRay@discussions.microsoft.com> wrote in message
> > > *news:1E3540EE-F90D-4BF0-A5C0-99C6187A2798@microsoft.com...*
> > > > *Thanks for responding, Joe.*
> > > >
> > > > *Yes, we do have enforce logon restrictions enabled.*
> > > >
> > > > "Joe Richards [MVP]" wrote:
> > > >
> > > > > *Do you have enforce logon restrictions enabled?*
> > > > >
> > > > >
> > > > >
> > > > > --
> > > > > *Joe Richards Microsoft MVP Windows Server Directory Services*
> > > > > *www.joeware.net*
> > > > >
> > > > >
> > > > > *DickieRay wrote:*
> > > > > > *Though all of the DCs on our Windows2000 native-mode domain are*
> > > *updated with*
> > > > > *the latest Service Packs and security patches, we continue to see*
> *the*
> > > > > *behavior described in KB 274064.*
> > > > >
> > >
> > >
> > >
>
>
>