

## Re: Blocking port scans on local network

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0013.html>

---

**From:** TBONE (TBONE\_at\_discussions.microsoft.com)

**Date:** 11/30/04

Date: Tue, 30 Nov 2004 14:19:02 -0800

Thanks Steve and BitWise!

The link and Steve's suggestions are a big help.

"Steven L Umbach" wrote:

- > You can implement enumeration of SAM accounts and shares with probably no
- > ramifications, especially since you have no downlevel clients. However even
- > after you enable it you will find that you can still extract a lot of info
- > from computers. You would have to enable the setting for "no access without
- > explicit anonymous permissions" to really block access to that info. Such
- > setting may however cause problems but on a pure W2K domain you may be able
- > to pull it off. It would cause the most potential problems when implemented
- > on domain controllers via Domain Controller Security Policy depending of
- > configuration but it should not for instance not allow W2K computer users to
- > logon to the domain or change passwords. The browse list [My Network Places]
- > may or may not become disrupted as the pdc fsmo is also the domain master
- > browser. See the links below for more details.
- >
- > <http://support.microsoft.com/?kbid=246261>
- > <http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/05sconfig.msp>
- > -- see the explanation and recommendation of the security option for
- > additional restrictions for anonymous connections in this security guide.
- >
- > Another thing to consider is that NO non domain computer can connect to any
- > domain computer that has a "require" ipsec policy assigned to it. However I
- > do not recommend applying ipsec policy wide scale without some testing of
- > policy ahead of time as you could shut down the domain. In particular domain
- > controllers MUST be exempt from ipsec policy that involves communications
- > between domain computers and domain controllers as the domain controllers
- > are the kerberos key distribution centers. The way to configure the policy
- > would be to add the domain controllers by their static IP addresses to the
- > ipsec policy in a rule that would have a permit filter action for all
- > traffic between domain controllers and domain members affected by the ipsec
- > policy. However even such a policy would allow them to scan your domain
- > controllers.
- >
- > If you decide not to implement no access without explicit anonymous

microsoft.public.win2000.security: Re: Blocking port scans on local network

> permissions on your domain controller tell them that you can not because of  
> the problems it will cause in your domain. Security is about managing risk  
> and if it reduces or interferes with the functionality of your domain then  
> that may not be acceptable. Having said all that here are a couple of tips.  
> Since you do not have any downlevel clients in your domain make sure you  
> have disabled the storage of lm hashes on at least your domain controllers.  
> Set the security option in Domain Security Policy for "lan manager  
> authentication level" to at least send ntlmv2 Responses only or send  
> ntlmv2/refuse lm. Do not set it to "refuse lm/ntlm without testing as it can  
> break rras or Exchange. Check that the root/drive folders do not have  
> excessive permissions for everyone group. Also run the MBSA tool on your  
> servers [you can do remote scans] to make sure not needed service are  
> disabled on computers such as telnet and www. Remember IIS is installed and  
> enabled by default in W2K. The Windows 2000 Security Hardening Guide I  
> referred to in the link above is a great read. Good luck! --- Steve  
>  
> <http://support.microsoft.com/?kbid=299656> -- disable lm hash.  
>  
> "TBONE" <TBONE@discussions.microsoft.com> wrote in message  
> news:90B459FD-1A87-45CD-9EEF-DDEB5587C67F@microsoft.com...  
>> Thanks BitWise.  
>>  
>> That pointed me in the right direction. The main jist seemed to suggest a  
>> registry change. There was a broken link posted by Mark Minasi that I'd  
>> like  
>> to read but can't( <http://www.minasidownloads.com/nws0312.htm> ) It also  
>> brings up a related question concerning Local and Domain Security Policy.  
>> This does the same as the registry change and can be applied across the  
>> entire domain. I'll explain...  
>>  
>> There is a policy under Security Options in both the Local and Domain  
>> Security Policy snap-in called "Additional restrictions for anonymous  
>> connections" that can restrict SAM account and share enumerations. Do you  
>> (or  
>> does anyone) know of any negative ramifications if I choose to restrict  
>> 'enumeration of SAM accounts and shares"? I am running in a pure Windows  
>> 2000  
>> environment (Clients and Servers).  
>>  
>> If I am running pure a W2K domain, will I see any changes in browsing or  
>> other network services? Will this prevent non-domain users and machines  
>> from  
>> retrieving SAM and share information?  
>>  
>> Thanks again!  
>>  
>> "BitWise" wrote:  
>>  
>>> Most likely they are connecting with null sessions, which is quite easy  
>>> to  
>>> do. A good read on null sessions is at [www.minasi.com](http://www.minasi.com). You'll need to

> >> *register, but it's free. Search there for 'null sessions'.*  
> >>  
> >> *"TBONE" wrote:*  
> >>  
> >> > *We have some wonderful auditors in our building who will be testing our*  
> >> > *network security (Sarbanes–Oxlely is the bane of my existence).*  
> >> >  
> >> > *I noticed that one of the auditors had a copy of SolarWinds Engineering*  
> >> > *Edition Toolset. I suspect that they will be scanning my network etc...*  
> >> > *I ran*  
> >> > *one of the SolarWinds browsing utilities on my domain controller and*  
> >> > *was*  
> >> > *suprised at the information it returned. Specifically, it returned all*  
> >> > *of the*  
> >> > *users accounts in my domain! It did not return any specific information*  
> >> > *on*  
> >> > *those accounts but, a simple account list was still a great suprise to*  
> >> > *me.*  
> >> > *All of this while using an account not in my domain and on a machine*  
> >> > *that is*  
> >> > *not a member of my domain.*  
> >> >  
> >> > *The auditors do not log into my domain and their machines are not*  
> >> > *members of*  
> >> > *my domain. HOWEVER, their machines are issued an IP address from my*  
> >> > *DHCP*  
> >> > *server and they can access the Internet.*  
> >> >  
> >> >  
> >> > *QUESTION:*  
> >> >  
> >> > *Is there a way to block access to my servers (Port Scans etc..) from*  
> >> > *machines that are not member of the domain without adversely affecting*  
> >> > *my*  
> >> > *users? Using domain or group policy in the solution would be desirable.*  
> >> >  
> >> > *If not, what measures can I take that will limit them to Internet*  
> >> > *access only?*  
> >> >  
> >> > *Any and all suggestions would be greatly appreciated.*  
> >> >  
> >> > *Thank you,*  
> >> > *--*  
> >> > *TBONE*  
>  
>  
>