

Re: Blocking port scans on local network

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0006.html>

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 11/30/04

Date: Tue, 30 Nov 2004 19:35:30 GMT

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/05sconfg.mspx>

— 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 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 al