

## Re: nessus scan

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-06/0968.html>

---

**From:** BOFH ([bofh1234\\_at\\_hotmail.com](mailto:bofh1234_at_hotmail.com))

**Date:** 06/24/04

Date: Thu, 24 Jun 2004 14:35:13 -0500

Thank you for the information. I think that this needs to be documented somewhere in a KB article. This looks like a little change from the way windows 2000 server did things.

BOFH1234

"Steven L Umbach" <n9rou@nsc Comcast.net> wrote in message news:svECc.103532\$eu.72794@attbi\_s02...

> *Null sessions do not really enable guest access to resources. They are used  
> for various networking processes including maintaining the browse list,  
> downlevel trusts, and for changing passwords before a user logs onto the  
> computer in certain cases. Null sessions can allow unauthenticated access  
to  
> enumerate share, user, group, and other information. This information can  
be  
> used to mount an attack against a computer or a domain though a properly  
> configured firewall will prevent untrusted networks from obtaining that  
> information. Null sessions do NOT allow unauthenticated access to data on  
> shares. Enabling the "guest account" will allow unauthenticated access to  
> shares that have everyone permissions including ntfs permissions and the  
> user right to access this computer from the network. The setting of 1 is  
> good compromise for most domain controllers as 2 will even cause problems  
> when XP Pro users try to change their domain passwords at logon. Setting  
it  
> at 2 may be fine for domain workstations and servers if you are not using  
> downlevel clients to access those servers. If you have a properly  
configured  
> firewall, and account lockout policy, enforce complex passwords, and  
enable  
> auditing for account logons events and account management on domain  
> controllers and logon events on your servers, I would not be too concerned  
> about leaving null access at 1. I am not that familiar about null  
> access to ldap. I suggest also posting to the win2000.Active\_directory  
> newsgroup about that issue. --- Steve*

>

>

<http://www.microsoft.com/technet/Security/topics/hardsys/tcg/tcgch05.mspx> ---

> - read more about null/anonymous access at the link including potential

Re: nessus scan

> *impact.*  
>  
> <http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/05sconfig.msp>  
> -- and here under additional restrictions for anonymous access under  
> security options  
>  
> "BOFH" <bofh1234@hotmail.com> wrote in message  
> news:u7XJWpgWEHA.204@TK2MSFTNGP10.phx.gbl...  
>> As a part of our new policy to port scan everything several times a year  
>> using nessus, we have come across a couple of things when scanning our  
>> fully patched windows 2003 enterprise servers:  
>>  
>> 1. It was possible to log into the remote host using a NULL session.  
The  
>> concept of a NULL session is to provide a null username and a null  
> password,  
>> which grants the user the 'guest' access.  
>>  
>> To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261  
>> (Windows 2000).  
>> Note that this won't completely disable null sessions, but will prevent  
> them  
>> from connecting to IPC\$  
>> Please see <http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html>  
>>  
>> I have set the restrictanonymous registry key to 1 and 2 (with reboots  
>> between the changes) and every scan I run I always get the above  
message.  
>> Is there a way to disable 'guest' access? Is there some KB Article I  
> missed  
>> that discusses NULL sessions and windows 2003?  
>>  
>> 2. How do I disable NULL BIND on my LDAP servers? I am not running  
>> exchange.  
>>  
>> Thank you for your time,  
>>  
>> BOFH1234  
>>  
>>  
>  
>