

Security Tips

Disabling “null” Sessions

Introduction

The concept of a NULL session is to provide a null username and a null password, which grants the user the “guest” access. Even with just “guest” level access, it is still possible to gather lots of data useful in breaking into a system. Furthermore any functions which can be performed remotely via a null session can be executed by anyone, from anywhere, and you won't be able to determine who did it. Therefore it is recommended that you restrict null session access to the minimum level necessary to meet your needs.

By default Windows systems will allow anyone to connect as a 'guest' user. There is usually no operational need to allow this service. If the clients you deal with are all running Windows 2000 or higher, you probably have little need to allow null sessions on your server machines. Null sessions should only be necessary to support Windows NT 4.0 and Windows 9X clients and possibly some unfortunately-designed third-party software.

Disabling NULL Sessions

Turning this feature off is actually quite simple.

The easiest way to stop NULL sessions is by disabling "File and Print Sharing" on all network devices, after logging on as an Administrator. On XP go to Control Panel > Network Connections > Properties for each adapter. On Windows 2000 go to Control Panel > Network and Dial-up Connections and select the proper connection. Right click on the connection and select 'Properties'. You can uncheck the option, though uninstalling would of course provide better security against accidentally turning it on.

However, should you actually need to run “File and Print Sharing”, then there is another way to disable NULL sessions. To do this you need to access the system registry, by running `regedit.exe`

Use Registry Editor to view the following registry entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

The key you want to edit is **RestrictAnonymous**. Change the value to a 1 or 2. A setting of 1 indicates that null connections are allowed but sensitive data is blocked being sent via the connection (only option available in NT4). A setting of 2 will disallow any NULL connections; this may conflict with some third party software. There are a few hacking tools that will work on a level 1 setting and retrieve information. Reboot the machine when done.

Windows XP also supports these settings, but they are now displayed in the "Security Policy" GUI as "Network access: Do not allow anonymous enumeration of SAM accounts" and "Network access: Do not allow anonymous enumeration of SAM accounts and shares". Set both of these to "enable".

References

<http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP> (Windows 2000/XP)

<http://support.microsoft.com/support/kb/articles/q143/4/74.asp> (Windows NT)