

Re: Explanation of Anonymous Named Pipes Security Policy

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-08/msg00261.html>

- *From:* "Will" <westes-usc@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 21 Aug 2006 17:38:10 -0700
-

This is really helpful and thanks.

What is SNA?

Remote management of objects in my SAM...just what every standalone Windows box in a DMZ needs! :)

I tried to empty the list, and immediately many Windows 2003 applications start to hang when you logout. So it's back to making smaller random experiments and just praying something else doesn't break later.

—

Will

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message news:eNv4tSOxGHA.4680@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Read in the Windows Server 2003 Security guide.

There you will see that the two you mention are also controlled by the setting to allow (or not) anonymous access to shares and named pipes, and if I recall correctly, the guide recommends emptying the list of shares for high sec environment.

The named pipes can be trimmed significantly for most machines.

The guide gives use information for these as

- COMNAP – SNA session access
- COMNODE – SNA session access
- SQL\QUERY – SQL instance access
- SPOOLSS – Spooler service
- LLSRPC – License Logging service
- Netlogon – Net Logon service
- Lsarc – LSA access
- Samr – SAM access
- browser – Computer Browser service

which is pretty fully informative except for maybe Samr, which is

Re: Explanation of Anonymous Named Pipes Security Policy
the protocol for remote management of objects in the Sam.