

## Re: NtLmSsp -- Login

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-07/0868.html>

---

**From:** Steven Umbach [MVP] ([n9rou\\_at\\_comcast.com](mailto:n9rou_at_comcast.com))

**Date:** 07/13/03

Date: Sun, 13 Jul 2003 00:51:22 GMT

The anonymous logon/null session is used by Windows operating system for communications among computers on a network for a variety of reasons including browser list communications, certain rras processes, and downlevel clients for password changes. As long as you have a properly configured firewall that also blocks netbios and 445 ports to the internet these events should not be of any great concern – go to <http://scan.sygate.com/> to check. However if you see a large number of failed audits from known user accounts, then somebody may have used a null session to enumerate your users and groups – possibly from your lan. Logon type three is a network logon. --- Steve

<http://is-it-true.org/nt/atips/atips155.shtml> --- Logon event ID explanations.

<http://support.microsoft.com/?kbid=246261> --- Describes some anonymous account uses.

<http://www.somarsoft.com/> --- Dumpsec tool that can exploit null session.

"Greg" <[greg\\_68@hotmail.com](mailto:greg_68@hotmail.com)> wrote in message  
news:#5F#WpMSDHA.2128@TK2MSFTNGP12.phx.gbl...

> I was looking through the security section of the event viewer and found a  
> login and was hoping someone could tell me how the login was done (remote  
> login or local login).:

>

> Successful Network Logon:

> User Name:

> Domain:

> Logon ID: (0x0,0xA3B6)

> Logon Type: 3

> Logon Process: NtLmSsp

> Authentication Package: NTLM

> Workstation Name:

> Logon GUID: -

> Caller User Name: -

> Caller Domain: -

> Caller Logon ID: -

> Caller Process ID: -

> Transitted Services: -

microsoft.public.win2000.security: Re: NtLmSsp -- Login

- > *Source Network Address:* –
- > *Source Port:* –
- >
- > *The event viewer title for this event shows Anonymous login. What login*
- > *process is NtLmSsp?*
- >
- > *Thanks.*
- >
- >