

RE: Anon Logon Events 538/540

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-03/0364.html

From: Frances [MSFT] (v-franhe_at_microsoft.com)

Date: 03/04/05

Date: Fri, 04 Mar 2005 10:07:33 GMT

Hello,

Thanks for your post.

According to your message, I understand you have event 538/540.

The event 540 logs the Successful Network Logon and the event 538 logs the Successful Network Logoff. Please rest assured they are not security issues, only for the network communication authentications. Some network applications use the ANONYMOUS LOGON process to create a communication channel with your computer. Therefore, these security logs can be ignored.

The information on this particular security event can be found within the following documentation:

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/518.asp>

Anonymous logon means that it is a null session. NT Auth/Anonymous is just a pseudonym for a Null Session. The NTAAuth/Anonymous isn't really an account; it just means that no credentials were supplied. There are many conditions known to cause a null session connection which makes it difficult to tell the exact cause of these particular events. This Anonymous logon instance was caused by the service NTLMSPP. For more information about the NTLMSPP, please refer to the following link:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/com/security_9qgg.asp

If the logon authenticates with NTLM, it will show the workstation name. The computer name HOD is not the real computer name, I assume the machine may be infected with virus, so it is masked under the identity of HOD for the machine name.

Please don't worry about it.

As for your question, I would like to answer them in order.

Q1: I can't seem to find any log info concerning the IPs of these remote connections. Does XP store these someplace?

A: Since it will take much disk space to have the logs, Windows don't have related logs concerning the IPs of the remote connections. However, you can download a tool named Network Monitor and use it to capture the data you desire.

About Network Monitor 2.0

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/about_network_monitor_2_0.asp

To obtain a time-bombed version of Network Monitor, visit the following Microsoft Web site: