

Event ID 576/538 – Guest Logon

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-10/msg00190.html>

- *From:* carmen <carmen.2z52bu@xxxxxxxxxxxxxx>
 - *Date:* Sun, 28 Oct 2007 06:08:31 +0530
-

Recently, I got a message when I logged onto my pc that the event viewer logs were full.

When I took a look in the security logs in event viewer, I saw pages and pages of Event ID 576, followed by 538 using the guest id. In terms of timing, the 538 was always about 1 second after the 576.

What would cause these messages and if it was a hacker, was it successful or not and what would he have had access to?

At the bottom of this message are the details of the 538 and 576.

Some details of my pc:

1. My pc is running XP Pro fully patched. I don't use any Peer to Peer file sharing programs.
2. I have run Computer Associates, Macafee and Kaspersky Anti virus. No virus found.
3. I have run Adaware, Windows defender, and trial Trojan Hunter – No malware found
4. Remote desktop was enabled on the pc but was hardened so that after 3 failed logon attempts, the system would lock the account out for 30 minutes.
I was also not using the default port for Remote Desktop so that it couldn't be detected in a random port scan.
5. This pc (Computer A) was not behind a hardware firewall, but did have Sygate firewall running. Sygate was configured to accept incoming connections from only 1 IP address (Computer B), which was the IP address

Event ID 576/538 – Guest Logon

from the pc from which I would start the remote desktop. I know this would work because if I did try and ping Computer A from Computer B, I would get a response. If however, I tried to ping Computer A from any other IP address, I would get timeout messages.

6. File and print sharing was enabled, but no shares were created.

Net

share from a dos prompt shows only the default shares were enabled.

7. Event viewer did not show any failed guest logons.

Here are the messages:

Event ID 576

Special privileges assigned to new logon:

User Name:

Domain:

Logon ID: (0x0,0x1EC738B8)

Privileges: SeChangeNotifyPrivilege

For more information, see Help and Support Center at

<http://go.microsoft.com/fwlink/events.asp>.

Event ID 538

User Logoff:

User Name: Guest

Domain: WORK

Logon ID: (0x0,0x1EC7356E)

Logon Type: 3

carmen

carmen's Profile: <http://forums.techarena.in/member.php?userid=33855>

View this thread: <http://forums.techarena.in/showthread.php?t=842244>

<http://forums.techarena.in>

.