

Re: Anonymous, Guest login problems!!!

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-10/3421.html

From: celi (*celi_at_volcanomail.com*)

Date: 10/19/03

Date: 18 Oct 2003 20:35:26 -0700

Hi, I had seen those in my log and knew they were system events, but they happen like 15 during a period of 3-4 minutes, always success audits in the security log for either anonymous, nt authority/network or NT authority/system local service logons, event IDs 528, 538, 540. I never see failures and it's filling up my log!

Exactly what you said sounds like it could be an impersonation. They will flood the log for like 10 minutes, then do it again a couple of hours later. It seems to happen more when I boot up, but after that, there is no pattern to it. How can I make sure it's not just the system? (Have Norton AV, firewall from ms). Online scanning systems (like src) say my ports are "stealthed" but when i run the cmd: netstat -ano, I see 135, 445 and 1025 'listening.

Also, my LAN settings have disabled NetBios over the connection, but there may be a background service running elsewhere (?)

WORSE, at boot up I see the following Event ID 612, where the System seems to have changed auditing policies. How could that be? Administrators are the only ones with permission to log or change policy, as set in the local security policy. the user name is the computername and a \$ sign, like a clone, but there doesn't seem to be any changes to the policy help please!!!

Event ID 612

from NT AUTHORITY\SYSTEM

Audit Policy Change:

New Policy:

Success Failure

- + + Logon/Logoff
- + Object Access
- + Privilege Use
- + + Account Management
- + + Policy Change
- + System
- - Detailed Tracking
- - Directory Service Access

microsoft.public.windowsxp.security_admin: Re: Anonymous, Guest login problems!!!

+ + Account Logon

Changed By:

User Name: computername\$
Domain Name: workgroupname
Logon ID: (0x0,0x3E7)

>From Anonymous

Successful Network Logon:

User Name:
Domain:
Logon ID: (0x0,0x60E2A)
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name:
Logon GUID: {00000000-0000-0000-0000-000000000000}

"Steven L Umbach" <sumbach@ameritech.net> wrote in message
news:<rX_fb.24940\$ev2.6053467@newssrv26.news.prodigy.com>...

> *Windows is actually a pretty secure product if you configure it correctly*
> *for your needs and pay attention to things like security updates that are*
> *common to all operating systems, including linux [Sendmail has been keeping*
> *my son busy as of late]. I did a quick search on Google for "linux*
> *vulnerabilities" and came up with 579,000 matches.*

>
> *To answer your question. The event ID's that you are finding are not "guest"*
> *logons, but normal null sessions that are created by the operating system*
> *that is used for some networking functions including maintaining the browse*
> *list. If you do not need file and print sharing, then uninstall it and you*
> *should see those events decrease. Null sessions are a vulnerability if*
> *allowed from the internet which you would find as exposed netbios/cifs*
> *ports – particularly 139 and 445. If you see more than a few failed logons*
> *in rapid succession using known non default accounts in your security log ,*
> *that may mean that someone has enumerated your computer through those ports.*
> *See KB link below that explains a bit about anonymous/null connections in*
> *Windows 2000. --- Steve*

>
> <http://support.microsoft.com/?kbid=246261>

>
> "loduricano" <loduricano@aol.com> wrote in message
> news:037901c38b74\$c8b66650\$a401280a@phx.gbl...
> > *I know that M\$Windoze is crap regarding security, but I*
> > *have to use it in one of the boxes at home. I use a custom*
> > *version of Linux.*

> >
> > *Here is the problem: I get anonymous and guest logons on it.*
> > *All the accounts have strong passwords, including the Guest*
> > *account. The guest account is also disabled! I have tried*
> > *deleting the guest account but it's not possible to delete*
> > *built-in accounts. I have also run at one time or another*

Re: Anonymous, Guest login problems!!!

microsoft.public.windowsxp.security_admin: Re: Anonymous, Guest login problems!!!

> > Syquest, McAfee, Sygate Pro and Zone Alarm Pro with the
> > same results. I just installed the latest Zone Alarm Pro
> > right now, and did a complete scan using the Sygate
> > security scan. I also did a full scan from outside the
> > firewall, over the LAN with NMap and other utilities. All
> > the ports are stealthed! I also changed the ruleset of ZO
> > to block ports 135, 137-139, 445 and others.
> >
> > So you tell me, how come I STILL have anonymous and guest
> > logons? And what can I do to stop them?
> >
> > Here is a dump of the logs:
> >
> > Event Type: Success Audit
> > Event Source: Security
> > Event Category: Logon/Logoff
> > Event ID: 540
> > Date: 10/5/2003
> > Time: 7:26:28 AM
> > User: NT AUTHORITY\ANONYMOUS LOGON
> > Computer: *****
> > Description:
> > Successful Network Logon:
> > User Name:
> > Domain:
> > Logon ID: (0x0,0x11029)
> > Logon Type: 3
> > Logon Process: NtLmSsp
> > Authentication Package: NTLM
> > Workstation Name:
> > Logon GUID: {00000000-0000-0000-0000-000000000000}
> >
> > For more information, see Help and Support Center at
> > <http://go.microsoft.com/fwlink/events.asp>.
> >
> >
> > Any help is appreciated.
> >
> > Cheers,
> >
> > cl.
> >
> > -----
> > Who's fault it is that the whole internet is crawling with
> > Messenger (port 1026/udp) spam from China?
> >

Re: Anonymous, Guest login problems!!!