

Re: Event 680

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-03/msg00107.html>

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 16 Mar 2006 11:39:08 -0600
-

About the best you can do is to go into your firewall logs and look for IP addresses that correspond in time to the failed logon events on the server and if you find IP addresses that seems to be causing the problem add them to your firewalls blocked list. For that to work well you would need to have logging enabled on your firewall and the time on the firewall and server would be in synch. Also make sure your server does not have any ports/services available to internet users that it should not have. Since your server is Windows 2003 and if you have Service Pack 1 installed on it you could use the Security Configuration Wizard to help you secure the server by configuring it based on it's role to make sure unnecessary services are not enabled and to help configure the Windows Firewall if you want to use that also. --- Steve

<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.msp>
--- Windows 2003 Security Configuration Wizard

"Shahin" <Shahin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:F49279ED-D607-4061-8E4B-9BE55E58F980@xxxxxxxxxxxxxxxxxxxx>

Dear Steven,

This person try to gain Access to Administrator Account from outside, so I can just see the name of his/her PC.

Any idea how can I find some info on this?

Thanks,

Shahin.

"Steven L Umbach" wrote:

Does the Event ID show the name of the source computer assuming type 3 logon is being attempted? If so that could be a starting point and you could try

Re: Event 680

to ping the computer name or look at DHCP leases, dns records, or wins records for the IP address of the computer. --- Steve

"Shahin" <Shahin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:1CAF08E0-EE19-4F43-922F-3CF751ACC58B@xxxxxxxxxxxxxxxxxxxx

Hi,

I have a question regarding security logs, I get a lot of event 680 on one of my windows 2003 servers, as you know this event has to do with Failure on logon, with account Administrator. Now I would like to know if there is a tool that I can use to get some info on this person. Some thing like IP of the person or some thing useful?

Thanks,
Shahin.