

## Re: Capture IP Address

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2005-11/0141.html>

---

**From:** John (*IDontLikeSpam\_at\_Nowhere.com*)

**Date:** 11/21/05

Date: Mon, 21 Nov 2005 11:41:01 -0800

Hmmm...I apologize if this is a novice observation but I just noticed something interesting that I thought I would share...

I have some MS Access front end databases linked to SQL Server 2000 databases as the backend (tables) on our internal network. I create new SQL logins for every user that requests access to the database and capture every user action through SQL Profiler. In analyzing the Profiler trace logs I noticed some Login Failed attempts to our Master database which really raised my concern. The interesting part is that the Login Failed attempt kept saying user 'Admin'. I know that we don't have a specific user name to any of our databases named 'Admin' especially to our Master. I just did a test and went to open my linked table through MS Access to SQL Server 2000 and that the Profiler logged the event as a Login Failed attempt to the Master database even though the linked table is to one of my other defined databases. Then the dsn odbc login pop up comes up and then I log in with my valid specified user name and password which is not 'Admin' and am able to login successfully. All of the Login Failed attempts with 'Admin' throughout my trace logs have a successful login immediately after with a valid user name. So it appears that when accessing a SQL Server table through a link from MS Access it by default tries to access the Master database with the default user name of 'Admin' and then prompts the user for the valid login name and password. So maybe these weren't hack attempts (which I am truly hoping)?

Would be interested if someone could confirm to me if this whole process is accurate?

Thanks in advance.

-J

"John" <IDontLikeSpam@Nowhere.com> wrote in message  
news:%23pr5wns7FHA.3808@TK2MSFTNGP10.phx.gbl...

> *Keeping up to date with database security can get so stressful makes me  
> sick to gut.*

>

> *Thank you very much Russ for your helpful post. I really appreciate it.*

>

microsoft.public.sqlserver.security: Re: Capture IP Address

> -J  
>  
> "Russell Stevens" <rustyprogrammer@online.nospam> wrote in message  
> news:u3mohmk7FHA.3976@TK2MSFTNGP15.phx.gbl...  
>> John,  
>>  
>> If you are getting hack in attempts, just go to the command prompt and  
>> type  
>>  
>> netstat -n  
>>  
>> The SQL attacks will be on 1433 and will be listed as time wait (assuming  
>> you check when you are being hacked).  
>>  
>> Russ Stevens  
>>  
>>  
>  
>