

## Re: Is there any way to prevent hacker trying to guess sa password?

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2005-10/0120.html>

---

*From:* Ken Schaefer (*kenREMOVE\_at\_THISadOpenStatic.com*)

*Date:* 10/17/05

Date: Mon, 17 Oct 2005 13:19:15 +1000

"Rob R. Ainscough" <robains@pacbell.net> wrote in message  
news:uhmakmA0FHA.736@tk2msftngp13.phx.gbl...

: Ken,

:

: What is scary is that opening port 1433 is some "major" security flaw ---  
it

: shouldn't be and if it is why --- because hackers can crash the service  
with

: port on

Remove the TCP/IP library, and port 1433 will not be open. Your clients will  
need to use some other mechanism to connect to SQL Server.

Having port 1433 open is completely different to guessing the "sa" password.  
If someone can crash SQL Server by connecting to port 1433, you need to open  
a case with Microsoft PSS to get that fixed.

: I think part of the problem is that you're used to "living with" the  
: security problems and the many possible solutions and working around to  
them  
: all.

Not at all – I realise that you use the most appropriate tool to do the job.  
Glass windows can be broken – do we demand that all glass window  
manufacturers now work out how to prevent an attacker from breaking your  
house's glass windows? No. You use shutters, steel bars or a burglar alarm  
system. Use the right tool for the job.

: Smaller companies don't have the luxury of hiring multiple  
: security/network "experts" in order to secure data that in most cases  
: affects the end user (our clients/consumers) and forces them to conform  
just  
: because MS can't provide a simple secure solution. Adding yet more tools  
on  
: top of the tools is not really helping the situation, just more things to

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

: configure and to manage and to purchase because of either the OS/SQL  
: weakness.

You don't need multiple security experts. Just put a very complex password  
on your "sa" account. Or don't expose port 1433 to the internet directly.  
There are lots of simple "solutions" to this problem.

:: In fact, by me posting on this very newsgroup, I'm now being flooded with  
: "security experts" wanting a job. Having numerous experts doesn't help  
make  
: a product cheaper to the end user/consumer. I shouldn't need to go to a  
: bookstore and see 150 books on securing Microsoft OS/SQL Server -- in a  
: word, I don't have time to read them all -- I'm a software engineer with  
: bigger fish to fry. If I wrote software that expected my end  
: users/consumers to go read several books on how to use my software  
: efficiently, I'd be out of business.

If you wish to use a complex piece of software like SQL Server, you should  
have some basic level of knowledge. You should expect to do some reading on  
the product, and expect to have some kind of learning curve. No one is  
suggesting you need to read 150 books.

Cheers  
Ken

:  
: Rob.  
:  
: "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message  
: news:eKgqaC6zFHA.1264@tk2msftngp13.phx.gbl...  
:>  
:> "Rob R. Ainscough" <robains@pacbell.net> wrote in message  
:> news:ukAppP0zFHA.2008@TK2MSFTNGP10.phx.gbl...  
:> : Simple option that the DBA can configure only permit login attempts  
:> every  
:> : XYZ milliseconds, attack can be user defined -- you listed the  
paramters  
:> #  
:> : of failed tries over XYZ milliseconds -- that'll cover the basic  
attacks  
:> at  
:> : least, now the SQL injection attacks and/or crash the service attacks  
:> need  
:> : to be address separately (no real DBA options here).  
:>  
:> The proper way to secure this though isn't in SQL Server per se. Whilst  
:> that  
:> might be a "nice to have" feature, I think I'd prefer the SQL Server  
:> product  
:> group to work on more important things.  
:>

Re: Is there any way to prevent hacker trying to guess sa password?

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

:> There aren't that many application servers that limit the number of  
:> logons/sec (e.g. Active Directory doesn't, IIS doesn't, SQL Server  
:> doesn't,  
:> Exchange doesn't). Instead, you should use an appropriate tool for the  
:> job.  
:> By using the most appropriate, dedicated tool, we keep things a little  
:> simpler and the network easier to manage and defend.  
:>  
:>  
:> : But one would HOPE that Microsoft are serious about security (they  
:> certainly  
:> : are having problems demonstrating this and have a serious problem with  
:> : making joe consumer feel "safe")  
:>  
:> Microsoft's putting a lot of effort into security. Check their website  
:> someday and look at all the consumer guidance they have out there now.  
:> Look  
:> at all the tools that have been coming out (MBSA, IISLockDown,  
:> AntiSpyware,  
:> Malicious Software Removal Tool). Look at the improvements in security  
in  
:> SQL Server SP3, and IIS6.0 etc  
:>  
:> : But more importantly MS strategy should  
:> : not only be to prevent, but to identify, locate, shut down and report  
to  
:> the  
:> : authorities  
:>  
:> Microsoft does have a honey pot project running. And I'm sure they have  
:> contacts with various authorities to report on the more significant  
:> issues.  
:>  
:> : But I think the point of telling the DBA, or Developer or IT person  
:> : "security isn't MS problem, it is yours" does NOBODY any good.  
:>  
:> Ultimately, security is your responsibility. There are tools out there  
:> (like  
:> firewalls, IDSes, and the stuff built into SQL Server). But how you  
:> configure it, and the processes you use to manage it are your  
:> responsibility.  
:>  
:>  
:> : MS needs to provide these tools,  
:>  
:> The tools are there – you just aren't using them. And blaming Microsoft  
:> isn't going to solve the problem.  
:>  
:>  
:> You think you are the only person in your situation? There are lots of  
:> companies running SQL Server, but they don't all seem to be having the  
:> problem you are having. You need to do a little research, and get the

Re: Is there any way to prevent hacker trying to guess sa password?

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

:> necessary info on how to configure all this stuff properly so you don't  
:> have  
:> this issue.  
:>  
:> And frankly, your lockout system is a little scary – you want to lockout  
:> the  
:> "sa" account? Sounds like a potential DoS issue to me.  
:>  
:> Cheers  
:> Ken  
:>  
:>  
:> : they need to get serious about security, they NEED to  
:> : understand that DBA's, Developer's, IT people can and do go the  
easiest  
:> : route to security — it doesn't matter what the DBA, Developer, IT  
:> person  
:> : does or doesn't do, the ultimate perception of being hacked or  
security  
:> : compromised will point to MS in the public eyes — so for MS to say it  
:> is  
:> : NOT our burden is just foolish. I realize this is falling on deaf  
ears,  
:> but  
:> : MS need to stop the ignorance — provide the tools, make them easy to  
:> use,  
:> : provide intelligent defaults to configurations.  
:> :  
:> :  
:> : "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message  
:> : news:OLaBtftzFHA.1264@tk2msftngp13.phx.gbl...  
:> :>  
:> :> "Rob R. Ainscough" <robains@pacbell.net> wrote in message  
:> :> news:ObLmEunzFHA.1040@TK2MSFTNGP14.phx.gbl...  
:> :> : Hi Ken,  
:> :> :  
:> :> : The problem is, those that should be permitted access are not  
static  
:> IPs  
:> :> : (they could be a broadband connection with a dynamic IP) — IPs  
can  
:> and  
:> :> do  
:> :> : change so that would involve a lot of maintenance to keep them  
:> updated  
:> :> not  
:> :> : to mention the end user would NOT have a clue what is wrong with  
the  
:> :> : applicaiton that no longer can communicate to the SQL Server.  
:> :>  
:> :> Fair enough.

Re: Is there any way to prevent hacker trying to guess sa password?

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

:> :>  
:> :> : Is there really NOTHING built into Win2K3 or SQL 2000 that has any  
:> :> : intelligence about prevent hacker attacks?  
:> :>  
:> :> What is a hacker attack? 3 tries in 1 second? 10,000 tries in one  
:> second?  
:> :>  
:> :> What you want is something like an IDS (Intrusion Detection System),  
:> which  
:> :> you can configure at an appropriate thresh-hold which you determine.  
:> Then  
:> :> it  
:> :> can do various stuff (like alert you, or configure a block at your  
:> :> firewall  
:> :> or whatever) when a trigger value is reached.  
:> :>  
:> :> However this is something that requires you to think carefully about  
:> it –  
:> :> to  
:> :> ensure that a legitimate user doesn't accidently lock themselves  
out.  
:> :>  
:> :>  
:> :> : I mean the pattern of a SQL  
:> :> : hacker is pretty simple -- look in the event viewer at the 20000+  
:> login  
:> :> sa  
:> :> : failed attempts (once every 10 seconds).  
:> :>  
:> :> Is this just one IP address? If so, just use TCP filtering in  
Windows  
:> :> server. 20,000 attempts to pretty obviously a hack. But what if it  
was  
:> :> only  
:> :> 5 attempts? What then?  
:> :>  
:> :> In any case, this is probably something you should use something  
else  
:> to  
:> :> secure – firewall, VPN etc.  
:> :>  
:> :> Cheers  
:> :> Ken  
:> :>  
:> :>  
:> :> What I don't like is the  
:> :> : processing time the hacker consumes with all the failed login  
:> :> : attempts --  
:> :> : with my 40 character password at one attempt every 10 seconds it  
:> would

Re: Is there any way to prevent hacker trying to guess sa password?

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

:> :> still  
:> :> : take them 5.6034833284317069404025203533663e+87 years to guess  
the  
:> :> : password -- even assuming they got lucky and hit the jackpot in  
1/2  
:> the  
:> :> time  
:> :> : that is still 2.8017416642158534702012601766831e+87 years. So am  
I  
:> :> worried  
:> :> : about using port 1433, no -- just annoyed that there doesn't  
appear  
:> to  
:> :> be  
:> :> : any tools to automatically ignore these attempts and stop using up  
:> my  
:> :> : bandwidth and resources.  
:> :> :  
:> :> : Rob.  
:> :> :  
:> :> : "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message  
:> :> : news:e1Lu4shzFHA.3408@TK2MSFTNGP09.phx.gbl...  
:> :> :> Is is absolutely required that port 1433 be open to the entire  
:> :> internet?  
:> :> :> If  
:> :> :> not, why not use a firewall or similar to block all IP addresses  
:> :> except  
:> :> :> those that should be permitted access?  
:> :> :>  
:> :> :> Cheers  
:> :> :> Ken  
:> :> :>  
:> :> :> "Rob R. Ainscough" <robains@pacbell.net> wrote in message  
:> :> :> news:%23qF1TlhzFHA.2640@TK2MSFTNGP10.phx.gbl...  
:> :> :> : Hi Sue,  
:> :> :> :  
:> :> :> : I don't suppose Microsoft provide any such easy to use tools  
to  
:> :> monitor  
:> :> :> : "patterned" network traffic -- i.e. the same IP attempting  
:> :> connection  
:> :> :> with  
:> :> :> : my SQL Server every 10 seconds? Also is there anything in SQL  
:> :> Server  
:> :> :> 2000  
:> :> :> : that can filter out an IP that attempts more than XYZ failed  
:> :> attempts  
:> :> at  
:> :> :> : login with sa?  
:> :> :> :  
:> :> :> : It seems that 95% of hacker activity/patterns are very

Re: Is there any way to prevent hacker trying to guess sa password?

microsoft.public.sqlserver.security: Re: Is there any way to prevent hacker trying to guess sa password?

similar,  
:> but  
:> :> I'm  
:> :> :> not  
:> :> :> : finding anything in the MS 2003 Server nor in MS SQL Server  
2000  
:> :> that  
:> :> :> would  
:> :> :> : help identify and prevent these patterns -- am I just missing  
:> :> something?  
:> :> :> :  
:> :> :> : If not, are there any tools out there (paid or free) that are  
:> easy  
:> :> to  
:> :> :> use  
:> :> :> : with minimal setup -- I'm a developer and don't have the time  
to  
:> :> spend  
:> :> :> on  
:> :> :> : tracking stuff like this down and I've got more important task  
:> to  
:> :> :> accomplish  
:> :> :> : with looming deadlines.  
:> :> :> :  
:> :> :> : Any recommendation, tips, hints, web sites to visit would be  
:> most  
:> :> :> : appreciated.  
:> :> :> :  
:> :> :> : Thanks, Rob.  
:> :> :> :  
:> :> :> : "Sue Hoegemeier" <Sue\_H@nomail.please> wrote in message  
:> :> :> : news:313mk1hjlkko4ncs8fajt0gn9m2gi3n4m6@4ax.com...  
:> :> :> :> Nothing built into SQL Server 2000 -- you have to get at this  
:> :> :> :> through the OS level using Network Monitor or another  
:> :> :> :> sniffer to capture the IP of the source.  
:> :> :> :>  
:> :> :> :> -Sue  
:> :> :> :>  
:> :> :> :> On Mon, 10 Oct 2005 13:01:32 -0700, "Rob R. Ainscough"  
:> :> :> :> <robains@pacbell.net> wrote:  
:> :> :> :>  
:> :> :> :>>Some hacker has set off a program to try and guess the sa  
:> password  
:> :> to  
:> :> :> my  
:> :> :> :>>SQL  
:> :> :> :>>Server that is public (1433 is open) -- I'm logging all the  
:> :> attempts  
:> :> :> :>>(about  
:> :> :> :>>6 a minute from the start of my logging til now -- several  
:> :> 100,000

Re: Is there any way to prevent hacker trying to guess sa password?

