

microsoft.public.sqlserver.programming: Re: Strange connections, can somebody tell what to do?

Re: Strange connections, can somebody tell what to do?

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.programming/2004-05/0220.html>

From: Arjen (boah123_at_hotmail.com)

Date: 05/01/04

Date: Sat, 1 May 2004 17:51:07 +0200

Okay, clear.

Last question.

Do you know a good firewall?

Where I can block everything.

Some ports can be open like for internet and e-mail.

And maybe sql, but only for access from my home ip.

Thanks,

Arjen

"Bojidar Alexandrov" <bojo@kodar.net> schreef in bericht

news:e163NM5LEHA.3904@TK2MSFTNGP09.phx.gbl...

> *Someone is trying to break in. From name – this is a computer in a
> university in Tawan.*

>

> *If you use remote control from somewhere else – it is visible to the outer*

> *world. Also you can try to connect to the MSDE*

> *using your tools or from command prompt –*

> *telnet yourserv 1433*

> *If you get timeout error – you cannot connect, else it show a black screen*

> *and you can type data to be send to the SQL.*

>

> *It is a high securtiy risk to leave SQL Server visible from Internet.*

There

> *are many recomendations to not do so. Have a search at Microsoft or*

> *google.*

> *I recommend you to setup firewall on the site where this server is located*

> *and block access to the SQL.*

>

> *Bojidar Alexandrov*

>

> *"Arjen" <boah123@hotmail.com> wrote in message*

> *news:c70g0n\$4a1\$1@news5.tilbu1.nb.home.nl...*

Re: Strange connections, can somebody tell what to do?

microsoft.public.sqlserver.programming: Re: Strange connections, can somebody tell what to do?

> > *Hi Bojidar Alexandrov,*
> >
> > *Thanks for your answer.*
> > *I still get more of these:*
> >
> > *:ms-sql-s ox.ntntc.edu.tw:7624 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:7762 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:9728 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:11446 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:13796 FIN_WAIT_1*
> > *:ms-sql-s ox.ntntc.edu.tw:14795 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:15323 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:19427 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:22265 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:23812 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:26872 CLOSING*
> > *:ms-sql-s ox.ntntc.edu.tw:30157 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:35529 TIME_WAIT*
> > *:ms-sql-s ox.ntntc.edu.tw:39411 TIME_WAIT*
> >
> > *I'm running windows 2003 web edition with msde 2000.*
> > *I have installed the latest updates.*
> >
> > *I cannot ping OMNIBACK and ERPSERVER.*
> >
> > *I'm using remote control.*
> > *So the server must be visable for outside.*
> > *How can I check it? (If the server is visable from outside)*
> >
> > *Thanks!*
> >
> >
> >
> > *"Bojidar Alexandrov" <bojo@kodar.net> schreef in bericht*
> > *news:%23av6Ur4LEHA.1556@TK2MSFTNGP10.phx.gbl...*
> > > *Please describe your envirnoment – is your SQL Server visible*
> > > *outside??*
> > > *What*
> > > > *client you have – why these to be not normal?*
> > > >
> > > > *Most probably OMNIBACK and ERPSERVER are computers in your workgroup*
> > > > *or*
> > > > *in*
> > > > > *your lan – these are NETBIOS names of the computer. Do ping from*
> > > > > *command*
> > > > > > *prompt to this name and this will reveal their IP address and then*
> > > > > > *decide.*
> > > > > >
> > > > > > > *TIME_WAIT connection is a closing one – it was active just before some*
> > > > > > > *seconds.*
> > > > > > > > *This can mean that someone have connected to the SQL Server. If he*

Re: Strange connections, can somebody tell what to do?

microsoft.public.sqlserver.programming: Re: Strange connections, can somebody tell what to do?

> > > *sucessully breaked in is impossible to know – when you get connected*
> *then*
> > > *your are asked for the password.*
> > >
> > > *Check if your server is visible to the outer world and if that is your*
> > > *intention. If not – setup a firewall.*
> > >
> > >
> > > *Bojidar Alexandrov*
> > > *"Arjen" <boah123@hotmail.com> wrote in message*
> > > *news:c70563\$6vb\$1@news1.tilbul.nb.home.nl...*
> > > > *Hello,*
> > > >
> > > > *When I use the command netstat I can see the current connections.*
> > > > *This is what I see:*
> > > >
> > > > *1. myservername : microsoft-ds OMNIBACK:3296 ESTABLISHED*
> > > > *2. myservername : ms-sql-s ox.ntntc.edu.tw:37720 TIME_WAIT*
> > > > *3. myservername : ms-sql-s ERPSEVER:15372 TIME_WAIT*
> > > >
> > > > *What does this mean?*
> > > > *Can I set this out?*
> > > > *And who are OMNIBACK, ox.ntntc.edu.tw and ERPSEVER?*
> > > >
> > > > *Thanks!*
> > > >
> > > >
> > > >
> > > >
> > >
> > >
> >
> >
>
>