

Microsoft SQL Server password cracking

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-07/0003.html>

From: Barry Dorrans (barryd@VIRTUEAPPLICATIONS.COM)

Date: 07/09/02

Date: Tue, 9 Jul 2002 09:59:37 +0100
From: Barry Dorrans <barryd@VIRTUEAPPLICATIONS.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Note : This email has gone to both NTBUGTRAQ and incidents.org – please direct your replies to the list you are subscribed too.

Some of you will have seen the register article on SQL server password cracking, <http://www.theregister.co.uk/content/4/26086.html>

As usual, Mr Greene's reporting is accurate to a point, but leaves out any mitigating circumstances, and in this case the mitigating circumstance makes the password cracker a not useful tool. Judging from my attempts to get Microsoft security articles fixed before, I don't hold out much hope for accuracy either. So I thought I'd fire off this email to the lists in order to halt some worries.

The password cracker relies on getting access to the hashes that SQL users store old style usernames and passwords. These are stored within a SQL database on the servers, and can be retrieved. However, they can ONLY be retrieved by users who already have SA rights. This is the information that theregister, and Mr Greene leaves out. The hashes are stored in sysxlogins, which is not available to your average joe user.

Now of course there are numerous people out there who haven't set SA passwords, as the spread of the SQL worm last month showed, but for anyone with an ounce of sense this password cracker will not create problems. It CANNOT work by simply pointing it at an MS SQL server.

As I recommended when the SQL worm started (the last time I attempted to correct theregister, again, never corrected), you should consider using NT usernames and passwords. I also suggest that you make sure that logging of failed SQL logins is turned on (this is off by default) – open SQL enterprise manager, right click on your server, choose properties and then choose security.

For those of you not in a domain or AD environment, you can still use NTLM security by mirroring usernames and passwords, see my incidents.org post archived at <http://www.incidents.org/archives/intrusions/msg12880.html>

NT-Bugtraq: Microsoft SQL Server password cracking

Regards,

Barry

- ***Previous message:*** [Gerhard Poul: "RCS public file sharing vulnerability"](#)
- ***Next in thread:*** [Deus, Attonbitus: "Re: Microsoft SQL Server password cracking"](#)
- ***Reply:*** [Deus, Attonbitus: "Re: Microsoft SQL Server password cracking"](#)
- ***Reply:*** [Bill Barrett: "Re: Microsoft SQL Server password cracking"](#)
- ***Reply:*** [Deus, Attonbitus: "Re: Microsoft SQL Server password cracking"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)