

Re: FIRED IT ADMIN HAS LOCKED US OUT OF SBS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-09/msg01968.html>

- *From:* Magnetoram <Magnetoram@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 14 Sep 2007 02:20:02 -0700
-

Mathew...WOW The most intelligent and appreciated post I have ever received in a newsgroup. Thank You VERY Much my Professional Colleague Your post is what I wish I always received. When comments about caps are posted and the obvious of calling the police, I then am taking time to reveiw useless info. I know maybe someone might not think to call the Police, but if you have risen to an Administrator this would be a given. This environment runs Novell, NT Server and SBS. I have all credentials at this time and will be looking for support to migrate out of Novell and NT add a member @K3 server and run all LOB apps on these. Do you have a Novell background?

"Matthew X. Economou" wrote:

"Teneo" ==
Teneo
<not@xxxxxxxx>
writes:

Teneo> Interesting post and Im now gonna be a party pooper... ;-)
Teneo> We must be careful of requests like this, it could be a
Teneo> member of staff wanting info and we have a duty to the
Teneo> industry to be careful what we supply / advise.

Questions asked in good faith should be answered in good faith.

0. Before doing anything, retain trustworthy legal counsel and information security expertise. Ask for and follow their advice, especially when it comes to evidence handling and data recovery.

1. Try to preserve as much evidence as possible. While the likelihood of successful prosecution is low, the organization will want to go to the authorities with as much evidence as possible. Make certain to keep both an electronic and a printed log of each step taken, along with the associated data. If a console login on the SBS server is possible, even as an unprivileged user, try to run

Re: FIRED IT ADMIN HAS LOCKED US OUT OF SBS

something like Helix (to capture things like active network connections) before cutting power to the server and to the Internet connection.

2. Back up the server to tape, CD/DVD, or a separate hard drive after powering it down. Buy all new hard drives for the server, and copy the contents of the existing drives onto the new ones (a bit-for-bit copy is ideal). Seal the old drives and put them under lock and key, along with the rest of the physical evidence. (A second bitwise duplicate may also be worth the time and expense, especially if deleted files must be recovered and one's backups prove to be unreliable.)

3. Depending on the time constraints imposed by the business, choose whether to crack or reset the Directory Services restore mode (DSRM) password, and whether to crack or reset the Active Directory domain Administrator account password. If you can verify that the outgoing admin did not encrypt any important data files using Windows EFS, you can forego password cracking (which is relatively slow). There's also a good chance the admin forgot to change the DSRM password, which makes breaking back into SBS much easier. I would try the following:

- Use something like BartPE to inspect the system and data volumes for encrypted files.

- If there are no encrypted files, just reset the DSRM account password using something like Peter Nordahl's password recovery diskette. Otherwise, boot into Directory Services restore mode and try old domain Administrator account's passwords. It's likely still the original password from when the server was built. Also try the blank (empty) password, just in case. If nothing works, using something like BartPE to copy the SAM, and using something like L0phtcrack to crack the Administrator password.

- Boot into Directory Services restore mode and use INSTSRV and SRVANY to get execute a command as NT AUTHORITY\SYSTEM. (See the associated Petri IT Knowledgebase article at http://www.petri.co.il/reset_domain_admin_password_in_windows_server_2003_ad.htm.)

- Again, if there are no encrypted files, just reset the domain Administrator account with the "net user administrator <password> /domain" command (as described in the aforementioned article). Otherwise, script the creation of another domain account with administrator privileges with something like CSVDE or LDIFDE, log in with that account, use something like pwdump2 to extract password data from Active Directory, and use something like l0phtcrack to crack the domain Administrator password.

4. After regaining access to the server, don't just reset the

Re: FIRED IT ADMIN HAS LOCKED US OUT OF SBS

Administrator account. Instead, create a new administrator account and configure it as an EFS key recovery agent, in case the old IT admin encrypted important files. (I'm uncertain as to whether this will allow you to recover files encrypted before the creation of the second EFS KRA account, so check with Microsoft CSS or some other expert for an authoritative answer. Microsoft CSS may be able to answer whether you can safely reset the domain Administrator password with "net user" and still use the EFS key recovery certificate.)

5. Call the police, but be aware of their limitations. Not every police department can handle electronic crimes, and the FBI has limited investigational capacity. Proving that a crime was committed could be very difficult.

6. Other nastiness may be lurking on the server, so check for backdoors (user accounts and remote control software), timebombs, etc. Unfortunately, it may be better to rebuild the server from scratch, once you have verified the integrity of your data (including email, database contents, etc.) Even here, one have several options, including attempting a partial swing migration (although great care must be taken to ensure that your temporary domain controller is itself not compromised).

7. Implement the two-man rule for all privileged accounts, so that this doesn't happen again.

In the end, the original poster must balance the need to preserve evidence with the imperative to restore normal business operations. And while it is entirely reasonable to decide to forego prosecution in order to minimize down-time, the final decision should be up to the business's senior management (with input from HR, IT, and the lawyers).

Best wishes and good luck,
Matthew

—

A: Because it messes up the order in which people normally read text.

Q: Why is top-posting such a bad thing?