

Re: physical security

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-10/1628.html

From: Ulf B. Simon-Weidner [MVP] (*nospam2-ulf_at_usw-consulting.com*)

Date: 10/24/04

Date: Sun, 24 Oct 2004 03:49:18 -0700

"Z" <z@z.com> wrote in message

news:#IYsPZuEHA.1452@TK2MSFTNGP11.phx.gbl:

> *Mike,*

>

> *The main question is: Are there tools to hack the ntds.dit? Are there*

> *tools*

> *which allows to raw read / write the ntds.dit? Why is it important? For*

> *example if I am a hacker and I have a physical access I will capture the*

>

> *incoming network traffic even restart the DC and stole the ntds.dit if any*

>

> *POC tools are not available now. In my environment I will implement the*

> *IPSec, so I will mitigate the risk.*

>

> *BTW: in Windows Server 2003 the syskey is enabled by default (method 1) if*

> *remember correctly. Is it helps me?*

>

Hello Z,

You do not need tools to hack the dit-db, and ipsec just helps you to prevent sniffing.

If I have physical access to your server I'm able to hack into it with cheap and easy tools. I just need access to the harddrive on a low level with a NTFS-Driver and I'm able to change the system so that I'd be able to log on as local Admin. Afterwards there are ways how to restart the domain and create my own domain admin, and now I've got access to everything. To retrieve the passwords I'll just need to start some brute force software to retrieve the pwds.

Hacking into the ntds.dit directly would be way to painful and would not provide a lot of results since passwords are not stored in reversable encryption anyways.

Syskey is by default set on every windows machine to use a local stored

syskey, the other available options allow you to save the key just on a disc or to type in the key everytime the machine starts. The other two options help you against attack of the local sam but they are not very practical in a remote office (or useless if you keep the disc in the server).

Things you need to do to delay the time you get after one of your DCs is stolen:

1. prevent the storage of lm-hases of passwords, then change every password in the domain.
2. use complex and long passwords, beyond 20 chars are good passwords. Just use Phrases instead of words. The attacker will be able to get into the local system very fast, and they have access to all data on that DC. If he wants to attack the rest of the domain, he needs one of the existing domain administrative accounts or he needs to get the domain back into the domain. To prevent him to get the other accounts fast prevent lm-hash and use long and complex passwords, this will give you some time to change the passwords on the domain after the DC is missing.
3. as passwords for your service accounts you can use very long ones and completly randomly generated, you can create a script which changes the account password and the credentials for the service at the same time, no need to store the password anywhere else. If you need to use the password, change it again randomly.
4. educate your users to use complex and long passphrases as well
5. implement and test processes to change all passwords (including those of service accounts) in a short time
6. implement a process which defines what to do when a DC is stolen, e.g. delete the computer account of that DC immediatelly (to prevent him getting back on the network after it might have been hacked and a additional administrator created), change passwords of all accounts, perform a metadata cleanup of your domain.
7. Never ever put back a missing DC into your domain without 100% reinstallation

If you follow those steps then if your DC is stolen they get all data on that DC, however if you prevent them to hack the domain accounts fast (done by step 1. to 4. above) you have some time (few days instead of seconds) to proceed with the other steps (5 and 6) to prevent them getting into the rest of the network.

And take care of point 7 – very important.

--

Gruesse - Sincerely,
Ulf B. Simon-Weidner

MVP-Book "Windows XP - Die Expertentipps": <http://tinyurl.com/44zcz>
Weblog: <http://msmvps.org/UlfBSimonWeidner>
WebSite: <http://www.windowsserverfaq.org>