Elcomsoft Rescues Idiot

A few weeks ago I had just awoken from a Sunday afternoon nap when I was confronted with "Your password expires in 7 days. Would you like to change you password?" system message. It had been asking for several days, so I complied and hastily gave it a new, valid password. So far, so good. Well, some time passed while I was working on documenting some user procedure. The course of documenting eventually forced me to reboot my laptop to emulate what the user would see. I get to the login screen and type in what I thought was my new password - several times, and many, many variations there of. For the life of me, I could not remember what I had entered a couple hours earlier! Being that my Active Directory server sits 2 feet from my laptop, I think "no problem, I'll log into the server as Administrator and reset my user password"...

Well, it turns out that it had been quite a while since I had actually logged in as Administrator, my regular user account has admin rights on the whole domain, so I never had to. I had forgotten this password as well, and I will tell you - what a horrible, sinking feeling when you realize you are locked out of your primary server. As this machine serves as my ad/file/smtp/imap/http/svn/j2ee/mssql/etc server, this was a major blow. The machine was up and running, I just could not get in to administer most of the server's functionality or, more importantly, do any backups. So, what does one do?

This server, "Bessie", is like my extended brain. She is the aggregation of my computing knowledge from the last decade on a single machine. Most of the data lives in a separate, RAID 5 volume, which is backed up periodically, so that was fairly safe. It is the actual configuration I wanted to save. I built this machine from parts and it is a bit unique. I have spent countless hours configuring this (convoluted) system, and reinstalling Window simply was not an option, or at least not an option I wanted to consider. Bessie runs **Windows Server 2003 R2 Standard x64 Edition** installed on a RAID 1 volume. She is also a primary Active Directory domain controller. Both of these facts made her rescue a bit harrowing...

I spent a lot of time on Google searching for an answer. There were lots of options (even the free variety) had this been a regular desktop system (this is a good start). The fact that the operating system is installed on RAID 1 volume, and security was handled by Active Directory ruled out all but Elcomsoft System Recovery Pro. It was rather pricy ($600), and took forever to be delivered from Czechoslovakia, but ultimately did the trick.

Published by Wyatt
Sun Nov 18 07:02:49 EST 2007
http://blog.wylovan.com/pebble/wyatt/2007/11/18/1195387369343.html