

Offline NT Password Reset Procedure

2010-08-19

Michael Spence

Preamble:

This procedure was procured from <http://pogostick.net/~pnh/ntpasswd> . This procedure has been tested by myself on an XP machine and seems reliable. There is an associated Disc, which I have in my possession. It is labeled "Offline NT Password Reset" and is dated 2010-08-19.

The following is the instructions from the website on running the procedure. In my test, I only used the default values, and only reset the Administrator password. I believe that this should be the only process which should need to be performed. From the administrator account, you will be able to reset all local passwords.

Overview

1. Get the machine to boot from CD (or floppy)
3. Load drivers (usually automatic, but possible to run manual select)
4. Disk select: tell which disk contains the Windows system. Optionally...load drivers.
5. PATH select, where on the disk is the system?
6. File select, which parts of registry to load, based on what you want to do.
7. Password reset or other registry edit.
8. Write back to disk (you will be asked)

DON'T PANIC!! - Most questions can usually be answered with the default answer which is given in [brackets]. Just press enter/return to accept the default answer.

The walkthrough and instructions is now on its own page!

What can go wrong?

Lots of things can go wrong, but most faults won't damage your system.

The most critical moment is when writing back the registry files to NTFS.

The most common problem is that the computer was not cleanly shut down, and my disk won't write correctly back. (it says: read only filesystem). If so, boot into Windows Safe Mode (F8 before windows logo appears) and shut down from the login window. You may have to do that twice in a row.

Also, see the FAQ for help with other common problems.