ELCOMSOFT
PROACTIVE SOFTWARE

AN EFFECTIVE APPROACH TO RESTORING SYSTEM ACCESS IN WINDOWS

WHITEPAPER

ELCOMSOFT
PROACTIVE SOFTWARE

CONTENTS

INTRODUCTION

In order to protect important data, we use a large variety of methods and technologies, especially when the data in question is confidential and essential for day-to-day operations of a business and for making important management decisions.

“If you have the information, you own the world” has become the basic tenet of our times, where control over data is of the utmost significance. The loss of access to important data can have a very negative impact on the company’s business.

It is under these conditions that any system administrator in the corporate setting is occasionally faced with the problem of restoring access to a client computer, resulting from the loss of the operating system password.

Unfortunately, this kind of problem is frequently resolved by the administrator using the brute force method, without using any special software for resetting and restoring passwords. The subject of this white paper is how to properly and more effectively resolve such problems.

EVERYONE LOSES PASSWORDS

Setting a system password is one of the most common, and as we tend to believe, the safest method for protecting data from unauthorized users. As is often the case, this too has a downside.

Our goal is to set a “difficult” password, to make it harder to guess and gain unauthorized system access, but then we forget it, and find ourselves in an awkward situation, caught in a trap of our own making. After this, we may have completely lost system access.

Life is full of unpredictable twists and turns: the system user may, for example:

- forget the password, having made it too complicated and become unable to remember it after a business trip or a vacation;
- make a mistake when changing the password, having entered the wrong character, followed the wrong scheme, or selected too complex a variant from the outset;
- be obstructive, pretending to have “lost” the password (for example, before dismissal, if there had been a conflict with company management or coworkers);
- leave the company or disappear without leaving system access information, (due to negligence or intentionally in retaliation to the employer).

When no other accounts exist in the system, due to security measures, and this is most often the case, the system becomes fully inaccessible.

The loss of a system password is especially inconvenient, since it results in loss of access not only to one or several files, applications, and services, but it puts an entire workstation out of use, with all of the associated consequences.

WHAT ARE THE CONSEQUENCES OF LOSING A SYSTEM PASSWORD?

POTENTIAL COSTS

Research conducted by Datamonitor[1] showed, that internal costs for one request for assistance from the company helpdesk with regard to problems with passwords, are between USD 10 and USD 40 (depending on the size of the company). On average, USD 25 or 57 minutes of time spent on resolving the issue by a qualified IT professional every day. Over the course of a year, the average costs exceed USD 150 thousand for large companies with over two thousand employees.

But this includes only expenses related to the time spent by hired IT professionals, not counting the costs resulting from the interruption of other business processes, potential loss of contract and reputation.

The problem is not as critical if the password in question is for an "empty" workstation of an average company manager. Here, the losses may be limited to the time spent by the system administrators on restoring the system to its original state and partial revenue loss from the employee's inactivity during that time.

But what if access is lost to the server with a client database, company accounting records, or to the CEO's laptop? This situation may create a host of internal problems, bring company operations to a standstill, and may lead to significant material and operational costs. Here, it is impossible to calculate exactly the total losses to the business, and so there is only one solution – these types of risks must be minimized.

WHY NOT SIMPLY RESET THE PASSWORD?

If the computer is part of a domain, its personal password can be reset by the network administrator. In this case, the problem is quickly resolved and the password will not need to be restored. This simple approach is the first solution that comes to mind, but taking it could bring serious consequences with it.

For example, what is the best approach if the computer was using EFS (Encrypted File System) or other services, directly tied into the account for which the password has been lost?

The problem is that the EFS-protected files on the drive, are encrypted using the FEK (File Encryption Key), with is stored in the files attributes. The FEK is encrypted using the master-key, which, in turn, is encrypted by the keys of those users that have access to the file. User keys themselves are encrypted by the password hashes of those same users. For this reason, if the user password is reset in the domain, you will lose access to EFS-encrypted data.

If the computer is not part of a domain, the local administrator password cannot be reset.

[1] "The ROI case for smart cards in the enterprise," Datamonitor, November 2004

Reinstalling the operating system to resolve the problem of a lost password is a brute force approach that should not be used. It can lead to the loss of important data and extraneous internal costs.

When the system password is lost, it is much wiser to attempt to restore the lost password using special software discussed below.

HOW TO RESTORE SYSTEM ACCESS?

AVAILABLE SOLUTIONS

To launch the application for restoring the system password, you would need to somehow gain full access to the hard drive of the "problem" computer.

This can be achieved in the following ways:

1. Boot under a different account with Administrator privileges (if it exists).
2. Physically disconnect the hard drive and install it on a different workstation running decryption software.
3. Boot using a different operating system, installed on the same computer, if available.
4. Boot using an operating system off a special bootable CD-ROM or other removable media such as USB flash drive.

The approach using a removable media is the most convenient, since it allows support personnel to quickly and surely boot into the computer with administrator privileges and complete access to the hard drive.

USING A WINPE BOOTABLE DISK

The preferred bootable disk to use in this case is the Microsoft Windows Preinstallation Environment (WinPE) disk. This tool offers the minimal functionality of a standard Windows XP operating system, which substitutes itself for DOS and allows for system setup in automatic mode.

WinPE is used to create a boot-disk configured for the problem at hand, which is then used by the administrator to automate software setup or system restore after system failure, when routine booting becomes impossible. This is precisely the problem in our case!

Using the boot disk the technician can quickly create a restore disk, then boot the problem computer without a hitch, gain access to the content of the hard drive and run a special program to reset the password, still using the same CD-ROM.

It is best to use a ready-made reset disk with WinPE, as the administrator then does not need to create it or delve into the intricacies of WinPE.

If the computer does not have CD drive, as in a laptop for example, then you can use a specially prepared reset USB flash drive.

FREE SOLUTIONS BASED ON LINUX/UNIX

Free “open source” solutions based on Linux/UNIX can serve as an alternative to WinPE, however these can hardly be considered convenient or reliable tools. The format of freely distributed software does not guarantee any kind of acceptable quality, update releases, or technical support, while intelligible documentation is frequently absent altogether.

Furthermore, existing Linux-based solutions, such as Offline NT Password & Registry Editor, Bootdisk / CD (http://home.eunet.no/pnordahl/ntpasswd/bootdisk.html), unlike solutions based on WinPE, do not offer a convenient and user-friendly graphic interface. The user must possess specialized knowledge if using these alternatives. For example, the user must know where the password hashes are located, and execute a fairly large number of “manual” command line operations.

The compatibility of Linux-based solutions leaves much to be desired. In particular, for SATA/RAID/SCSI devices, users would have to find drivers to use with Linux on the Internet and then also load them manually.

An experienced user could potentially succeed, but the majority would not. In addition, when using Linux the user may encounter problems not only with the hard drive, but even with a USB keyboard.

For this reason, paid solutions based on WinPE are more suitable for resolving the problem of restoring Windows system access, as they offer higher quality, the familiar Windows interface, and do not require time-consuming troubleshooting before being usable. In addition, in the case of WinPE you are guaranteed technical product support from the manufacturer.

ELCOMSOFT SYSTEM RECOVERY – A SIMPLE WAY TO RESTORE SYSTEM ACCESS

KEY FEATURES

Elcomsoft System Recovery (ESR) is one such specialized software tool for restoring Windows system passwords, which can be used to regain access to a Windows machine within an extremely short timeframe, complete with the needed user permissions.

The system administrator would also not need to spend much time on restoring system functionality and data access. It is as simple as booting the machine from the WinPE booting CD, run ElcomSoft System Recovery, and go back to other tasks.

A separate utility, on the boot disk, can be used to create a bootable USB flash drive, if needed. This can be especially useful when the "problem" computer does not have a CD-drive (for example, if it is a laptop).

A bootable USB flash drive can be very convenient, if the goal is not to reset the passwords, but to use ESR to backup system files that contain password hashes for the purpose of recovery of plaintext passwords later on a different computer.

ESR first tries to restore passwords using a predefined attack (dictionary and direct search). In addition, some passwords can be extracted from cache, system services, autologon (if it is configured), and so on. Different combinations are tried (dictionary attack), for example, when the password is the same as the username with one or two digits appended at the end.

All this makes it fairly effective in restoring the lost password. This procedure does not take more than a few minutes. As a result, in many cases there is no need to reset the password, which ensures the security of all data on the machine.

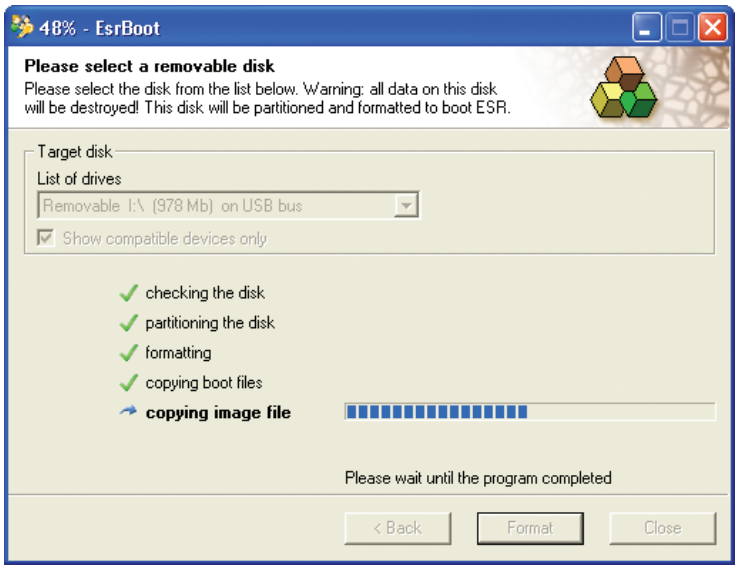

Fig. 1. Creating the booting USB flash drive.

SPECIAL FEATURES OF ELCOMSOFT SYSTEM RECOVERY

Here are some of the special features that come with Elcomsoft System Recovery:

- The ESR package includes a ready-to-use boot disk (CD or USB flash drive), which is compatible with any machine running a Windows operating system.
- ESR is based on Windows PE (Preinstallation Environment), licensed from Microsoft.
- ESR is compatible with Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 and Windows Vista.
- ESR supports all US and localized versions of Windows, as well as usernames and passwords in different languages.
- ESR supports all RAID arrays and SCSI drives (using Windows drivers).
- ESR automatically identifies all operating systems installed on the machine, making the choice of the operating system from a list relatively straightforward.
- ESR gives the option of giving administrator privileges to another user on the machine, with a known password. This way, there is no need to reset or restore the lost password.
- ESR extracts password hashes from SAM/SYSTEM files or the **Active Directory** database for both the domain administrator and domain users. This option is **not available from competing products on the market**. The collected hashes are written to a text file for later analysis and restoring using more advanced methods, such as the rainbow attack, that takes longer using a different product, for example the Proactive Password Auditor from ElcomSoft.

Using ESR you can easily:

- Obtain a list of all local user accounts and their descriptions; find out ones that have administrator privileges.
- Review the user account privileges (with the exception of those set using local and group security policies).
- Uncover accounts with empty passwords.
- Assign administrator privileges to any user account.
- Enable/unlock disabled/locked user accounts.
- Instantly restore passwords for special/system accounts (such as IUSR_, HelpAssistant, and others).
- Reset and change passwords for any local or Active Directory user accounts.

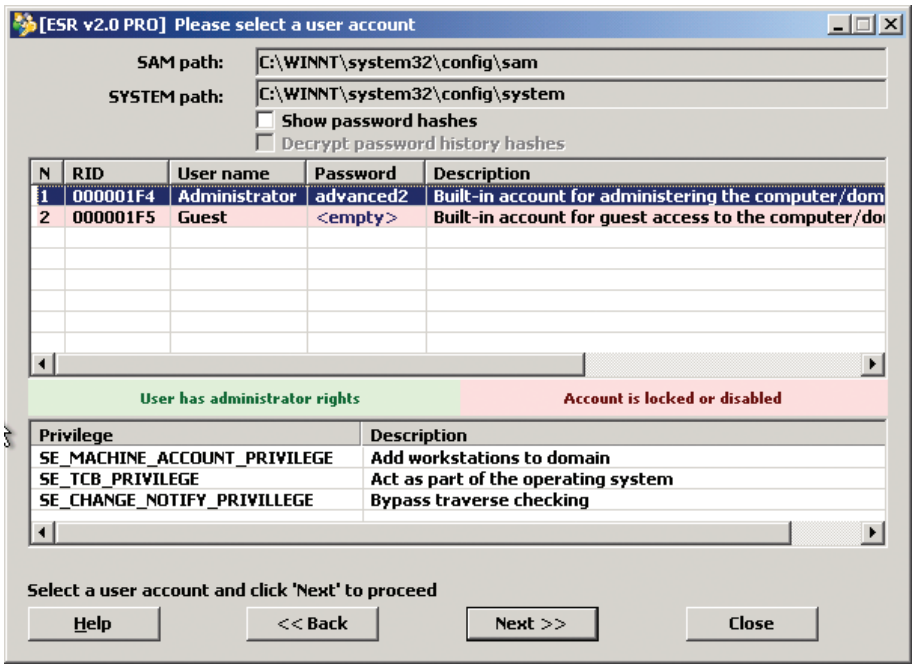

Fig. 2. Selecting an account from a list to reset or change the password or perform other tasks.

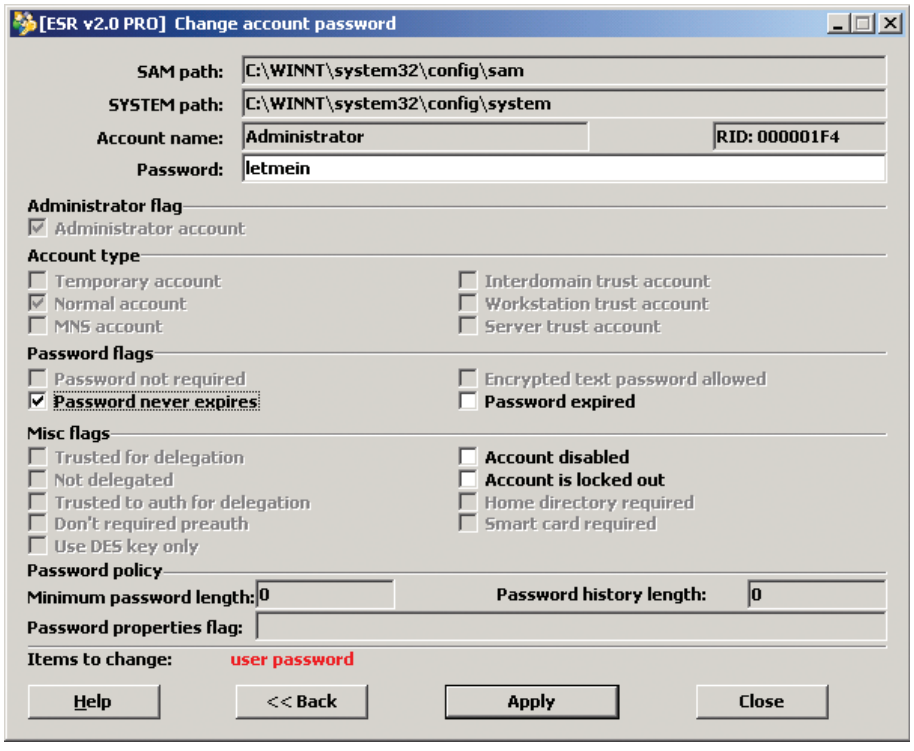

Fig. 3. Changing a user password.

ESR is available in three different versions: Basic, Standard and Professional. The differences between the versions are listed in the table below:

	ESR Basic	ESR Std	ESR Pro
Windows versions support			
Supports Windows Vista	●	●	●
Supports Windows NT/2000/XP workstations	●	●	●
Supports Windows NT/2000/XP servers	●	●	●
Supports non-US Windows versions	●	●	●
General features			
Multilingual user interface	●	●	●
Based on Windows PE	●	●	●
Supports all RAID/SCSI/SATA devices	●	●	●
Automatic mode (list of installed systems)	●	●	●
Manual mode (browse for Registry files)	●	●	●
Password reset CD	●	●	●
Creates a password reset USB flash drive	●	●	●
Reset local Administrator password	●	●	●
Enable/unlock Administrator account	●	●	●
Advanced features			
Reset password to other user accounts	●	●	●
Highlight accounts with Administrator rights	●	●	●
Look up account privileges	●	●	●
Enable/unlock disabled/locked accounts	●	●	●
Give Administrator privileges to any user account	●	●	●
Recover passwords for some system accounts	●	●	●
Reset Domain Administrator password	●	●	●
Reset AD users password	●	●	●
Dump password hashes for local accounts	●	●	●
Dump password hashes for AD accounts	●	●	●
Show LM/NTLM hashes	●	●	●

Advanced features			
Show password history hashes	●	●	●
Test short and simple passwords	●	●	●
SAM database editor	●	●	●
License, maintenance, delivery, price			
Licensed for business use	●	●	●
One year of free updates	●	●	●
Delivery	Download (ISO)	Express mail	Express mail
Price	US $49	US $199	US $599

The Basic version is distributed online without the ready-to-use boot disk, which can be created from the archive using the ISO-9660 disk image. The Standard and Professional versions are delivered with the boot disk and can be used to create the bootable USD flash drive.

Read more about Elcomsoft System Recovery product details here.

ABOUT ELCOMSOFT

Founded in 1990 in Moscow, Russia, ElcomSoft is a leader in the password/system recovery and forensics market. Thanks to one-of-a-kind technologies, ElcomSoft's products have garnered wide recognition both in Russia and abroad.

ElcomSoft's clients include many well known international companies from the following sectors:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

ElcomSoft is a Microsoft Gold Certified Partner, Intel Software Partner, as well as a member of the Russian Cryptology Association, the Computer Security Institute (CSI), and the Association of Shareware Professionals (ASP).

ElcomSoft is an acknowledged expert in the password/system recovery and forensics market. The company's technological achievements and opinion leadership is quoted in many authoritative publications. For example: "Microsoft Encyclopedia of Security", "The art of deception" (Kevin Mitnick), "IT Auditing: Using Controls to Protect Information Assets" (Chris Davis), "Hacking exposed" (Stuart McClure).

Visit our website to find out more.

ADDRESS:
Elcomsoft
Zvezdny bulvar 21, office 541
129085 Moscow, Russian Federation

FAX:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

WEBSITES:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr