

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

Windows NT/2000/XP/2003 operating systems keep their passwords into an encrypted form called "hashes". Passwords cannot be retrieved directly from hashes. To recover passwords it is necessary to compute hashes by possible passwords and compare them to the existing hashes. Password auditing includes check of possible ways to retrieve user accounts information. Result of password recovery is passwords in case-sensitive form.

## Obtaining Password Hashes

There are several ways to obtain password hashes, depending on their location and existing access. Password hashes can be obtained from SAM file or its backup, directly from local or remote computer registry, from registry or Active Directory on local or remote computer by means of DLL injection, from a network sniffer.

## Obtaining Password Hashes from SAM File

User accounts, which also contain users names and their passwords, are kept in the Windows NT/2000/XP/2003 registry and exactly in the SAM file (Security Account Manager). This file can be found on the disk in the %SystemRoot%\system32\config directory, emergency repair disk or on a backup tape.

It is impossible to gain access to the SAM file located in the %SystemRoot%\system32\config directory, while Windows NT/2000/XP/2003 is running because it is used by the operating system. If there is a physical access to the machine, it is possible to copy the SAM file by booting operating system copy or another operating system. If Windows NT/2000/XP/2003 is installed to the disk with NTFS file system, accessing it from MS-DOS or Windows 95/98/Me will require additional software. In MS-DOS can be used such programs as NTFSDOS and NTFSDOS Professional, in Windows 95/98/Me - NTFS for Windows 98 (by Mark Russinovich and Bryce Cogswell). Accessing from Linux operating system will require an NTFS support turned on. It is also possible to boot from a floppy disk and copy SAM file, having launched a program to access NTFS in advance. After this you need to import from SAM file. Extracting password hashes from a SAM file was first developed and applied in SAMDump program (by Dmitry Andrianov). During a SAM file import operation, obtaining of user accounts information is performed. The import from SAM file is similar to the obtaining of password hashes using pwdump method, except for the fact that instead of Windows API functions, supporting the registry operations, their emulations are used. During the import from SAM file by SAMDump, all non-Latin characters, contained in the user names, will be distorted. LCP program is free of this disadvantage.

The way to obtain a SAM file in Windows NT operating system, which does not require a computer rebooting, is copying it from %SystemRoot%\repair directory or emergency repair disk. Every time when an emergency repair disk in Windows NT is created by RDISK program, a SAM file packed and saved to a sam.\_ file, which is in fact backup copy of a SAM file. A sam.\_ file is an archive in the cabinet format. This file can be unpacked by the command "expand sam.\_ sam". The disadvantage of this method is that some passwords might have been changed since the emergency repair disk creation and sam.\_ file might be outdated. LCP program has a built-in ability to import SAM file from a sam.\_ file without using the expand program. A sam.\_ file is preliminary unpacked while import of user accounts list process and then the actual SAM file import is performed.

A SAM file is also copied when a complete backup copy is created. If there is an access to a backup copy, a SAM file can be recovered from %SystemRoot%\system32\config directory to a different machine and after all extract password hashes from it. The disadvantage of this method is also that passwords might have been changed since the last time of backup copy creation.

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

There is the SYSKEY tool, which first appeared in Service Pack 3 for Windows NT. SYSKEY additionally encrypts password hashes of user accounts, which makes import from SAM file by SAMDump useless. SYSKEY can be used in one of the following variants:

- generated startup key is saved encrypted to registry on the local hard disk;
- to derive startup key the startup password chosen by the administrator is used
- generated startup key is saved to the floppy disk, which should be inserted during operating system start.

Storing of the startup key in the registry is by default used. For more details regarding SYSKEY tool see article KB143475 Windows NT System Key Permits Strong Encryption of the SAM.

For extra protection, the SYSKEY tool should be activated manually after required Service Pack installation in Windows NT. In Windows 2000/XP/2003 operating systems the SYSKEY tool primary installed and activated.

Import from SAM file with additionally SYSKEY encryption, was first realized in SAMInside program (by PolASoft and Ocean). The SYSKEY algorithm was first published by FlashSky from Xfocus Team. To import from SAM file, while startup key is stored in the registry, it is required to copy SAM and SYSTEM files from %SystemRoot%\system32\config directory and then open them. If there is not enough space on a floppy disk, files can be compressed before copying. Backup files copies can also be found in the %SystemRoot%\repair directory, in case they have been archived there before. While keeping startup key on the floppy disk, StartKey.Key file is also required for import from SAM file.

LCP makes import from SAM file with or without additional encryption at any startup key storing variant possible.

## Obtaining Password Hashes From Operating System Registry

Obtaining password hashes from operating system registry requires direct access to the registry. Information import requires administrative privileges at the computer, which passwords dump you need create. If it is not a local computer, a remote access to the registry and required privileges must be permitted. Obtaining hashes through this method was first performed in pwdump program (by Jeremy Allison). During information import using this method by pwdump program, user names containing non-Latin characters will be distorted. It is recommended to use LCP for obtaining password hashes from the registry.

In case that SYSKEY program is activated, password hashes will be additionally encrypted. It makes import by pwdump program useless, because it is impossible to recover passwords from additionally encrypted hashes. In LCP program obtaining password hashes from registry is enhanced by support of additional encryption, therefore it is recommended to use LCP.

## Obtaining Password Hashes by DLL Injection

This method was first developed and realized in pwdump2 program (by Todd A. Sabin). Obtaining password hashes by pwdump2 method is possible with no regards to the SYSKEY program activated or not. To create a passwords dump by pwdump2 method, you need the SeDebugPrivilege. By default, only Administrators have this right, so administrator privileges are required for use of this method. Pwdump2 method is applicable to a local machine only.

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

Pwdump2 method uses DLL injection for passwords dump creation. One process forces another process (lsass.exe), using its process identifier, to load a DLL (samdump.dll) and execute some code from the DLL in the other process's (lsass.exe's) address space. In this case, samdump.dll is loaded into lsass (system service LSASS - Local Security Authority Subsystem), it uses the same internal API that msv1\_0.dll uses to access the password hashes. This means it can get the hashes without doing any of the hard work of pulling them out of the registry and decrypting them. The program neither knows nor cares what the encryption algorithms or keys are.

There is a mistake in pwdump2 program version supporting Active Directory, which prevents obtaining password hashes if in operating system there are accounts with non-Latin characters in user names. This mistake is fixed in the LCP program, therefore it is recommended to use it for obtaining password hashes by this method.

The method used in pwdump2 program was further developed to obtain password hashes not only from a local but a remote computer also in pwdump3/pwdump3e programs (by Phil Staubs). An executive service file and DLL file are copied to the remote computer. After copying process completed, a new service, equal to pwdump2 program on a local computer, is created and started. After obtaining password hashes, the service and files previously copied are deleted. The transfer of user accounts information is performed through a registry key on a remote computer. This key is temporarily created and permanently deleted after the copying process is completed. In pwdump3e program an additional encryption of transferred data by Diffie-Hellman algorithm is performed. This is done on purpose to prevent illegal access to the transferred data in case of network capture. This method also requires administrative privileges at the computer, which user accounts information you need to obtain.

During information import using this method by pwdump3/pwdump3e programs, user names containing non-Latin characters will be distorted. It is recommended to use LCP for obtaining password hashes by DLL injection.

In case you do not have administrative privileges at the local computer, it is possible to use a vulnerability of Windows NT/2000/XP/2003 operating systems, which in fact allows to change a screen saver, launched in case of logon absence for the particular amount of time (it is 15 minutes for Windows NT/2000 and 10 minutes for Windows XP/2003 by default) to a different program. To perform this, you need to change %SystemRoot%\system32\logon.scr to desired executive file (cmd.exe for example), which will be launched by the operating system instead of screen saver with system privileges. This change can be done by method used to copy a SAM file. You can get an access with write capability to a NTFS disk by NTFSDOS Professional or NTFS for Windows 98 programs. After this you need obtain hashes by pwdump2 or pwdump3/pwdump3e methods.

## Network Capture of Authentication Packets

Even in case when SYSKEY program is installed and activated and there is no required access to a remote or local computer, there is still a possibility to obtain password hashes of user accounts. By this possibility we mean network capture of authentication packets - sniffing. A client machine is exchanging authentication packets with a server each time it is required to prove a user privileges. It is only required that a targeting computer is in the same network segment as yours. A built-in sniffer of LC5, works at machines with Ethernet adapter and supports Windows NT/2000/XP/2003 and Windows 95/98/Me. LC5 program needs to be launched in the network capture mode and left for a certain amount of time to gather required password hashes. The captured data needs to be saved to a file. After this, you need to import LC5 session file in LCP.

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

To prevent obtaining password hashes by this method, Microsoft has developed an enhancement to the authentication mechanism called NTLMv2. Its usage becomes possible after Service Pack 4 for Windows NT installation. For more details regarding NTLMv2 usage see article KB147706 How to Disable LM Authentication on Windows NT.

## Passwords Recovering

A password can be derived in different ways: dictionary attack, brute force attack, hybrid of dictionary and brute force attacks, precomputed hashes attack.

Within a dictionary attack, hashes are gradually computed for each single word or word modifications from a dictionary and compared with the password hashes of each particular user. In case of the complete hashes match a password is found. An advantage of this method is its high speed, a disadvantage - only very simple passwords, which are based on the existing words of the used dictionary, can be retrieved by this method.

Brute force uses a character set and computes a hash for each possible password, compiled out of these characters. While using this method you can be sure that a password will be recovered in case that it contains the characters from the current character set. The only disadvantage of this method is a huge amount of time that might be required to retrieve a password. The more characters are contained in selected character set - the more time will be spent on passwords retrieving.

While passwords recovering by hybrid of dictionary and brute force attacks, characters are added to the right and/or left of the words or words modifications. A hash is computed for each assembled combination and compared with the users password hashes.

To perform precomputed hashes attack, hashes are precomputed and password/hash pairs are stored for all possible combination of the chosen character set. Available password hashes are being searched among precomputed hashes. An advantage of this method is its very high speed, a disadvantages are long time to precompute hashes and huge amount of disk space needed for their storing.

After obtaining password hashes, you can start passwords recovering. There are two basic file types containing password hashes: PwDump (passwords dump) and Sniff files.

Each string of a PwDump file is compiled in the following format:

**"UserName:RID:LMhash:NThash:FullName,Description:HomeDirectory:"**

Each of seven-characters password halves is encrypted independently from the other in LM hash due to DES algorithm (former federal standard of the USA), NT hash is compiled as a result of the whole password encryption due to MD4 algorithm (by RSA Security, Inc.). LM hash contains password information in case-insensitive form (in upper case), NT hash - in case-sensitive form. There is a unique user account identifier - RID (relative identifier) right after a user name, which is not used for hashes computing. Identifier of a built-in administrator account is equal to 500, a guest account - 501. LM hash is used for compatibility with other operating systems (LAN Manager, Windows for Workgroups, Windows 95/98/Me, etc.). Its presence simplifies passwords recovering. If the NT password length exceeds 14 characters, LM hash corresponds to the empty password. In case of LM hash presence, the password recovering is initially performed due to LM hash. When LM password is found, NT hash will be used to determine the NT password.

Each string of a Sniff file is compiled in the following format:

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

## "UserName:3:ServerChallenge:LMresponse:NTresponse"

LM response is compiled as a result of LM hash encryption, NT response - as a result of NT hash encryption. Encryption is performed due to DES algorithm, so that it is possible to recover LM and NT passwords only in case of the whole password check out. Besides, a separate server challenge is used in every single case. Therefore passwords recovering by Sniff file is required much more time.

The first program for recovering of Windows NT passwords was L0phtCrack (called now LC5) by Peiter Mudge Zatkan and Chris Wysopal from L0pht Heavy Industries, Inc. (now @stake, Inc.). If non-Latin characters in password are used then password will probably not be recovered with LC5, it is recommended to use LCP for passwords recovering.

### Changing Users Passwords Without Their Recovering

In case recovering of Windows NT/2000/XP/2003 users passwords is not required, it is possible to change them having access to a local computer. Users passwords changing is performed in Offline NT Password & Registry Editor program (by Petter Nordahl-Hagen). To do this, you need to boot from Linux floppy disk and choose a user to change password. After input of the password, password hash will be computed and SAM file will be changed in system disk. The program supports Windows NT/2000/XP/2003 even in case SYSKEY is activated.

### Additional Possibilities Of Obtaining Passwords Information

In case there are computers with Windows 3.11, Windows for Workgroups or Windows 95/98/Me installed in network, there are additional possibilities of obtaining passwords information.

Users passwords caching is performed to the %WinDir%\<UserName>.pwl (PassWord List) files in such operating systems by default. Passwords are kept encrypted in case-insensitive form (in upper case). Passwords encrypting algorithm was changed starting from Windows 95 OSR2, because detected mistake was corrected. Therefore passwords recovering from old PWL files is much easier.

In this case you can use programs like Glide (by Frank Andrew Stevenson), PWL\_Key (by Arthur Ivanov), PwIHack (by Vladimir Kalashnikov), PwITool (by Vitas Ramanchauskas and Eugene Korolev). For passwords recovering from newer PWL files you can use PwIHack or PwITool.

If passwords caching is permitted, there is a possibility to determine passwords during a user session in PwIView program (by Vitas Ramanchauskas and Eugene Korolev). This program can show the cached passwords on the local machine for the current user using undocumented Windows API functions.

In case a Windows NT/2000/XP/2003 user is at the same time a user in Windows 3.11, Windows for Workgroups or Windows 95/98/Me and his password is already retrieved (for Windows 3.11, Windows for Workgroups or Windows 95/98/Me), his password for Windows NT/2000/XP/2003 can be easily retrieved by LCP. It is necessary to specify characters of the recovered Windows 3.11, Windows for Workgroups or Windows 95/98/Me password as known password characters.

Recommendations for Windows 3.11, Windows for Workgroups and Windows 95/98/Me administrator  
At the computers with Windows 3.11, Windows for Workgroups and Windows 95/98/Me installed:

- disable passwords caching in Windows 3.11 and Windows for Workgroups.
- Add to %WinDir%\system.ini file the following parameter:

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

## [NETWORK]

### PasswordCaching=no

- disable passwords caching in Windows 95/98/Me. Locate DisablePwdCaching binary value in the registry by registry editor and set to 1 (if value does not exist, add it) to the following registry key:

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network**

- delete all PWL files from the disk and reboot operating system after disabling of passwords caching;
- change your operating system to Windows NT/2000/XP/2003 in case your computer meets the hardware requirements.

## Recommendations for Windows NT/2000/XP/2003 Administrator

At the computers with Windows NT/2000/XP/2003 installed:

- make case of a computer inaccessible to opening. It will prevent possible disconnect of a hard disk with operating system or connection of other disk;
- permit to boot only from a hard disk in Setup to prevent booting from other devices;
- set a password to Setup, preventing changing boot settings;
- Windows NT/2000/XP/2003 should be the only operating system installed on the computer. That makes impossible copying and changing files from other operating systems;
- use NTFS file system only and refuse using FAT and FAT32;
- make sure that Windows NT has Service Pack 3 or later installed and SYSKEY is activated;
- refuse storing the startup key in the registry, changing startup key storing in the SYSKEY program to a use of the startup password or storing on a floppy disk;
- use a Windows 2000/XP/2003 built-in ability of files encryption through EFS (Encrypting File System), which is part of NTFS5;
- prevent the remote registry management by stopping appropriate service;
- prohibit SeDebugPrivilege privilege. In the "Local Security Policy" click "Security Settings\Local Policies\User Rights Assignment" and remove all users and groups from the list in the properties of the "Debug programs" policy;
- delete administrative shares ADMIN\$, C\$ etc., which allow a user with administrative privileges to connect them through the network. Add AutoShareWks (for Workstation and Professional versions) or AutoShareServer (for Server version) DWORD value and set to 0 to the following registry key:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

**Range: 0-1, default - 1.**

**0 - do not create administrative shares;**

**1 - create administrative shares.**

- For more details regarding deleting administrative shares see article KB314984 HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers (for Workstation and Professional versions) and KB318751 HOW TO: Remove Administrative Shares in Windows 2000 (for Server version);
- prevent or restrict at maximum the number of shares;
- restrict anonymous access in Windows NT/2000 operating systems, which allows to get access to the information about users, security policy and shares. In Windows NT/2000 add RestrictAnonymous DWORD value to the following registry key:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**

**Range: 0-2, default - 0 for Windows NT/2000, 1 - for Windows XP/2003.**

**0 - do not restrict, rely on default permissions;**

**1 - do not allow enumeration of accounts and user names;**

**2 - no access without explicit anonymous permissions (not available in Windows NT).**

- For more details regarding restricting anonymous access see article KB143474 Restricting Information Available to Anonymous Logon Users (for Windows NT) and KB246261 How to Use the RestrictAnonymous Registry Value in Windows 2000 (for Windows 2000);
- prevent storage of the LM hashes in Windows 2000/XP/2003 operating systems to embarrass passwords recovering for an intruder, forcing him to use NT hashes. Add NoLMHash DWORD value and set to 1 to the following registry key:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**

**Range: 0-1, default - 0.**

**0 - store LM hashes;**

**1 - do not store LM hashes.**

- For more details regarding preventing storage of the LM hashes see article KB299656 How to Prevent Windows from Storing a LAN Manager Hash of Your Password in Active Directory and Local SAM Databases;
- in case there are no Windows for Workgroups and Windows 95/98/Me clients in the network, it is recommended to disable LM authentication. It will embarrass passwords recovering for an intruder if authentication packets are captured. In case there are such clients, you can allow usage of LM authentication only by server request. You can do it by activation of enhancement to NTLM called NTLMv2. Add the following values to the registry:

**LMCompatibilityLevel DWORD value to the key**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**

**Range: 0-5, default - 0.**

**0 - send LM and NT responses, never use NTLMv2 authentication;**

**1 - use NTLMv2 authentication if negotiated;**

**2 - send NT response only;**

# Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003

By Unknown

3 - use NTLMv2 authentication only;

4 - domain controller refuses LM authentication;

5 - domain controller refuses LM and NT authentication (accepts only NTLMv2).

NtlmMinClientSec or NtlmMinServerSec DWORD value to the key

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0

Range: the logical OR of any of the following values:

0x00000010 - message integrity;

0x00000020 - message confidentiality;

0x00080000 - NTLMv2 session security;

0x20000000 - 128 bit encryption.

- For more details regarding NTLMv2 usage see article KB147706 How to Disable LM Authentication on Windows NT;
- in case there are only Windows 2000/XP/2003 clients in the network, it is recommended to use Kerberos authentication protocol;
- hide the user name of the last logged on user in the logon dialog box. Add DontDisplayLastUserName string value and set to 1 to the following registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Range: 0-1, default - 0.

0 - display last user name;

1 - do not display last user name.

- For more details regarding hiding the user name see article KB114463 Hiding the Last Logged On Username in the Logon Dialog;
- disable the logon screen saver, launched in case of logon absence for the particular amount of time. Set ScreenSaveActive string value to 0 to the following registry key:

HKEY\_USERS\DEFAULT\Control Panel\Desktop

- For more details regarding disabling of the logon screen saver see article KB185348 HOW TO: Change the Logon Screen Saver in Windows;
- observe the following rules at a choice of Windows NT/2000/XP/2003 passwords:
- do not choose password or password part, which appears dictionary word or its modification;
- Windows NT password should be at least 7 characters long (14 characters at maximum), a Windows 2000/XP/2003 password - more than 14 characters (128 characters at maximum);
- password should contain characters from the maximum possible character set. Do not use A-Z characters only, try to include letters, numerals and special symbols into the password (if the password length less or is equal to 14, similar characters should be in each of seven-characters password halves);
- password characters being letters should be uppercase and lowercase letters. It will complicate passwords recovering with NT hashes;

# **Theory And Practice Of Password Auditing and Recovery In Windows NT/2000/XP/2003**

**By Unknown**

- install service packs and hotfixes of operating system in due time;
- rename administrator and guest accounts, disable guest account;
- administrator account should not be on the other computer as a regular account;
- have only one account with administrative privileges;
- adjust account policy (account lockout after invalid logon attempts, maximum password age, minimum password length, complexity requirements for the password, enforcing of the password history etc.);
- turn on logon failure audit;
- use programs from Microsoft Security Tool Kit, such as HFNetChk and Microsoft Baseline Security Analyzer (by Shavlik Technologies LLC for Microsoft). These tools can scan for missing hotfixes and security vulnerabilities;
- regularly perform passwords audit by LCP program or similar.