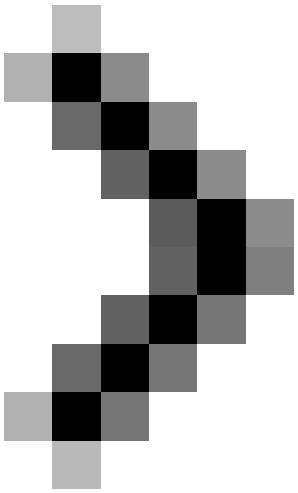
How can Windows passwords be cracked - Part 2

There is no more precautionary measure than using a strong password and changing it often.

In this article, I will show you some ways to crack passwords with different tools, then take measures to help you protect your passwords against such crack types. so.



How can Windows passwords be cracked - Part 1
In the first part of this series, we introduced you to password hashes as well as the mechanisms that Windows uses to create and save those values. In that section, we also point out the weaknesses of each method and the *avenues* may be exploited by attackers to crack those passwords. In this second and final section, we will show you some ways to crack passwords using various free tools, thus providing some tips on how to prevent them. mode crack password.

It should be noted that the techniques introduced here are purely for research purposes, not for systems where you do not have the right to authenticate.

Collect password hashes

To crack the password you must obtain the hash stored inside the operating system. These hashes are stored in the SAM file of the Windows operating system. This SAM file is located on the system at *C: WindowsSystem32config* , but you cannot access it when the operating system is working. These values ??are also stored in the registry in *HKEY_LOCAL_MACHINESAM* , but this registry area is also not accessible when the operating system is launched.

There are a number of other options here depending on the level of access you have to the computer that is conducting the authentication.

Physical access

If you have physical access, one of the most effective methods is to boot your computer with another operating system. If you are comfortable using Linux, you can boot from a Linux live CD that can read NTFS drives, mount the Windows partition, and copy the SAM file to an external drive.

If you are not familiar with this method, you can use P. Nordahl's Offline NT Password Editor, which can be downloaded here. This is a bootable Linux distribution that is designed to help users forget their passwords by allowing them to reset them. The software will receive input from the user, create a valid hash and replace the old hash in the SAM file with the new hash. This is quite useful because we can also use this distribution to read the SAM file and retrieve the hash data.

To do so, boot from the CD image and select your system partition, the SAM file location and the registry structure, select the password reset option **[1]** , launch the registry editor **[9].** included, browse to **SAMDomainAccountUsers** , browse to the directory of the user you want to access, use the *cat* command to view the hash contained in the file. The output will be in hex format, but it is possible to convert this format.

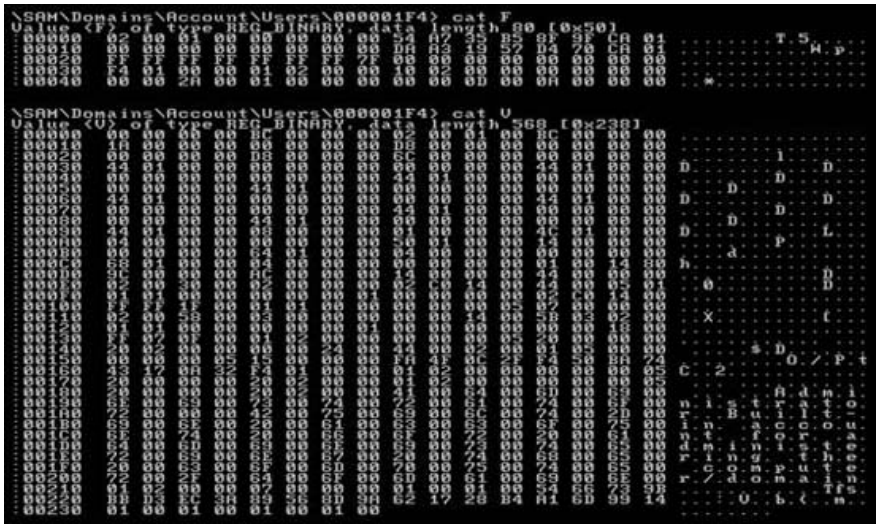


Figure 1: Hex output of SAM hash

Before using Offline NT Password Editor to reset the password, make sure that you are not using the Encrypted File System (EFS) on any version released after Windows XP / 2003. If you do that, the operating system loses its EFS keys and causes other problems, not just a forgotten password.

Access via software interface

If you are performing password validation actions without physical access to the device in question, it can still be accessed via the software interface via the remote desktop or VNC mechanism, then You can obtain password hashes using Fizzgig's **fgdump** utility, which can be downloaded here.

Once you have downloaded fgdump to use, you can run it simply.

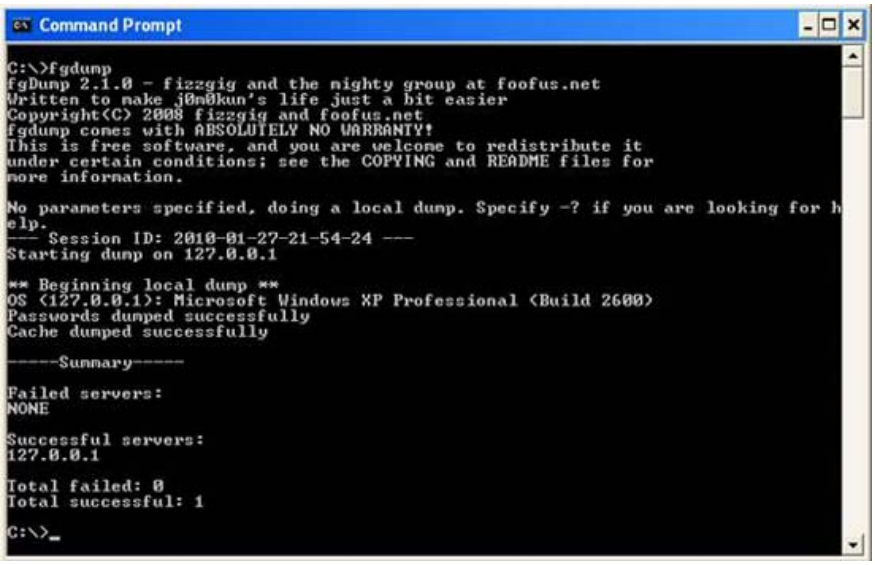


Figure 2: Configuring the Fgdump utility to run

When completed, a file will be created in the same directory that the utility launches, including a list of all user accounts, their LM hash, and also NTLMv2 hashes.

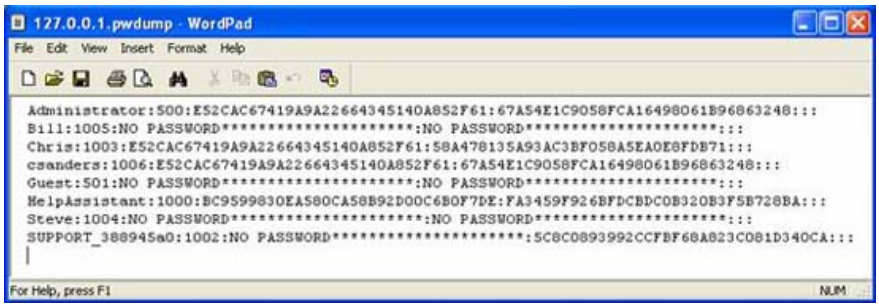


Figure 3: Output of password hashes obtained by Fgdump

Network Access

Finally, if there is no interactive access to the computer with the hash you want, the best solution is to try *sniffing* (sniff) the hash when they are transmitted over the network during the authentication process. Of course this will only work if the client is authenticating to the domain controller or accessing resources on another client.

If you are in the same network segment as the target client, you can use the **Cain & Abel** program to block password hashes when they are transmitted between devices. Cain & Abel is a free utility that can be downloaded here. Using Cain & Abel, you can initiate a process called 'ARP cache poisoning', which is likened to a middle person taking advantage of the ARP protocol to route traffic between two hosts through the machine. your calculator. ARP cache spoofing is a positive measure, but you can use *the* network *sniffer* that comes with Cain & Abel; It can allow you to block NTLM password hashes when communicating between fake hosts.

Page 3: Crack the password with Cain & Abel

Crack password with Cain & Abel

Now that we actually have password hashes, the next task to do this is to crack them. If you have downloaded and installed Cain & Abel, you are already a step ahead because we will use it to crack LM passwords for example.

If you have not installed Cain & Abel, you can download it here. The installation process is very simple. You will also be prompted to install the WinPCap data capture kit used for Cain & Abel's *sniffing* features. Once the program is installed, you can launch it and click the **Cracker** tab near the top of the screen. After doing this, click on the **LM & NTLM Hashes** header in the left pane, right-click an empty area in the center of the screen and select **Add to List** .

Cain will not accept a simple copy and paste of password hash, so you will have to put the hash into a formatted text file in a special way. If you extract your hashes with fgdump, you will have your necessary text file, this text file contains hashes on each line format.

Figure 4: Acceptable format of Hash Passwords

If you have extracted your Hash Passwords manually, you need to create a file with one entry for each user account. Each line contains the username, relational identifier (RID) of the user SID and the hash. The format of these components will be:

Username: RID: LMHash: NTLMHash :::

Browse to this file, select it and click **next** to *import* the hash into Cain & Abel. When done, you can right-click the account where you want to crack its password, select the **Brute Force Attack** option, select **LM hashes** . The *brute force* attack method is a method of trying to combine passwords with a hash value until a match is

found. On the following screen, you can select the characters you want to use for *brute force attacks* , minimum and maximum password lengths. Note that the character set will automatically be configured to use only letters in numbers and numbers with a maximum length of 7, due to the characteristics of the LM hash.

In the example scenario, with *PassWord123* password, we will see immediate results when the program returns ' *Plaintext of 664345140A852F61 is D123* '. The results also show that we cracked the second half of the password hash. On a modern computer, trying to find a unique password combination can take about 2.5 to 3 hours to ensure a real success.

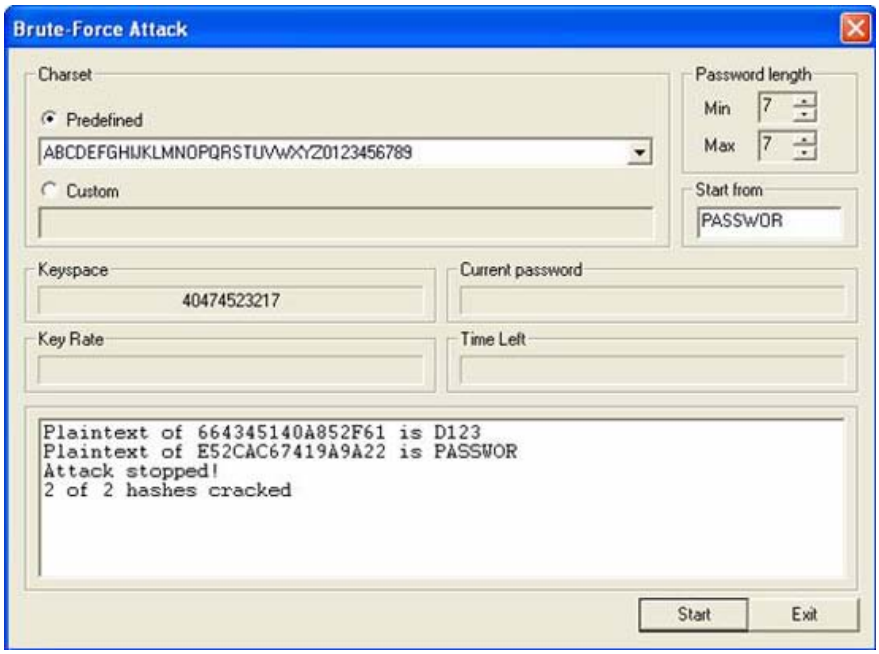


Figure 5: Cain successfully crack LM Password Hash

Crack the password with John the Ripper

Cain & Abel does a pretty good job of cracking LM passwords but it's quite slow and when doing crack NTLMv2 hash, its process is even much slower. If you don't have much experience or don't like the command line for password cracking actions, **John the Ripper** is one of the most popular and fast-paced crack machines we've ever seen.

You can download John the Ripper from here . Once you have extracted the contents of the file, you will find the john-386.exe executable file in the subdirectory / run. John can run in several other modes, but to run it in default mode, all you need to do is provide the file containing the hash password as an argument (argument) when running john-386 .exe from the command prompt.

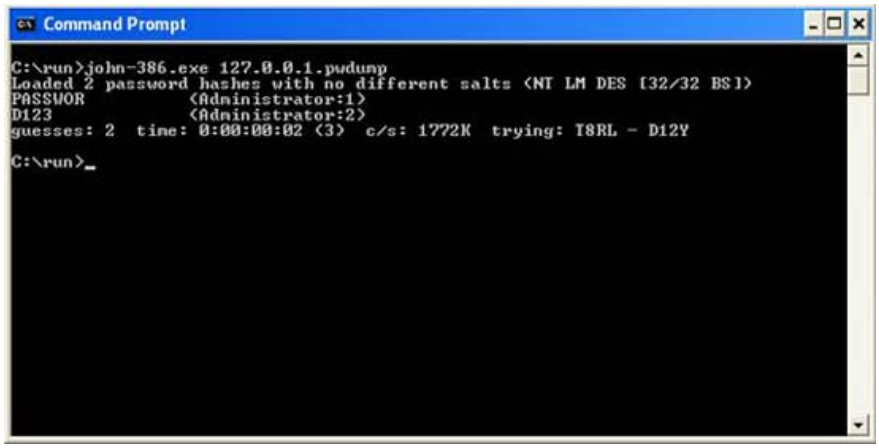


Figure 6: John the Ripper is trying to crack the password

When finished, John the Ripper will display the cracked passwords and save the results to its john.pot file. In most cases, the default crack mode is quite good, but John the Ripper also has other crack modes such as:

- Single Crack Mode - Use account name variables
- Wordlist Mode - Based on a dictionary to guess the password
- Incremental Mode - Based on *brute-force* attack
- External Mode - Based on another application (provided by the user) to guess the password.

John is very effective in all crack modes and is a program that I choose for cracking passwords.

Crack passwords with rainbow tables (Rainbow Table)

When you suspect complexity and spend a lot of time cracking an NTLMv2 password, the only logical decision is to use rainbow tables. A rainbow table is a lookup table containing password hash for each password combination that can be given to the encryption algorithm to use. As you can imagine, rainbow tables can consume quite a bit of storage space. Previously, these tables exceeded the processor's processing power and intensive storage space for creating and saving, but with the development of modern computers, hackers and malicious hackers It is easy to use external hard drives to store a series of rainbow tables.

Finding a place to create or download a collection of rainbow tables is Google search, but there are better methods for a password cracker. One such method is to use web services that contain its own set of rainbow tables. Such web services can be found here. This website maintains a lot of rainbow tables that you can submit password hash for crack, along with a list of recently hacked passwords.

To submit hashes to plain-text.info, you can click the **Add Hashes** link to specify the hash and encryption mode. If this hash has been cracked, you will see the result displayed, otherwise it will submit the hash to the queue. You can check the queue status by going to the **Search** link and searching for the hash, then it will tell you the location in your queue. Complex passwords can take quite a long time through this method, but it also shows faster than allowing execution on your own hardware.

Page 4 : **Protection against password crack actions**

Protection against password cracking actions

People often think that the goal of coding is to make encrypted text become something that no one can decipher, but this is just a little concept. That thought is based on the belief that computers have the ability to generate random numbers for coding purposes, but in all honest computers there is no such "random" that good, because 'random' is a programming logic based entirely on trust. Therefore, the real goal of encryption is to make encrypted text difficult to crack so much of the time it takes to crack heavier than the benefit of doing that crack.

With that in mind, there are a few things that can be done on an operating system to avoid cracking passwords.

Use complex passwords and keep changing

The most logical way to avoid password cracking is to make your password so complex ' *unexpected* '. If your password consists of lowercase characters, uppercase letters, numbers, special symbols and is relatively long, it will not be cracked with a short amount of time. To further increase complexity, change your password on a regular basis. There is no more precautionary measure than using a strong password and changing it often.

Disable LM Hash

You now know the weaknesses of LM hash. One good thing is that we don't have to use them anymore. Modern Windows operating systems can be configured to use *NTLMv2* exclusively with a few registry changes.

You can disable the LM hash repository by browsing to HKLMSystemCurrentControlSetControlLSA in the registry. Once in it, create a DWORD key named NoLMHash, with a value of 1.

Another step is to disable LM appraisal throughout the network. Again, you browse to *HKLMCurrentControlSetControlLSA.* When in there, find the key named *LMCompatibiltyLevel* . Its value can be set to 3 for the purpose of sending *NTLMv2* authentication, which is a great way for domain clients. In addition, its value can be changed to 5, which is the value used to configure the device to accept authentication requests, great for servers.

There is only one case where these settings can cause problems in which you have Windows NT 4 and lower-level computers on your network. Therefore, if you still have those systems online, remove them as the best security advice we give you.

Use SYSKEY

SYSKEY is a Windows feature that can be used to *add* 128 bits of encryption to the SAM file extension. SYSKEY works by using a user key that is used to encrypt the SAM file. When enabled, SYSKEY cannot be disabled.

Note that SYSKEY only protects the SAM file itself, protecting it from copying. SYSKEY does not protect against tools that extract hashes from running memory, such as Cain and fgdump.

You can find out more information about SYSKEY at http://support.microsoft.com/kb/143475.

Conclude

Password cracking is a skill for those who want to try to break into a system, because of that every system administrator needs to understand how passwords are saved, they can be stolen. and how to be unlocked. When

an intruder has breached the system, their goal will be more than half accomplished if your users are using simple passwords. Remember, what you know is half the battle, so if you get this information and do nothing with it, you only get half the victory. Using the prevention techniques provided in this article, you will prevent attackers from compromising passwords in your system.