Ethical Hacking Lab Series

Lab 7: Breaking Windows Passwords

Certified Ethical Hacking Domain:
System Hacking

Document Version: 2013-07-18 (Beta)

Organization: Moraine Valley Community College
Author: Jesse Varsalone

.

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

By the end of this lab, students will be able to crack the passwords of user accounts on Windows systems. A variety of techniques will be utilized to crack password hashes including Rainbow Tables, Brute Force, and dictionary attacks. Students will also utilize two tools, Windows Credentials Editor and Mimikatz, which may be used to dump the passwords in plain text from RAM.

This lab includes the following tasks:

- 1 - Creating Users in Windows
- 2 - Breaking Windows Passwords
- 3 - Dumping Windows Passwords in Clear Text

Domain: System Hacking

In many cases, the security of a device is tied to the user's password on the system the device resides. Many utilities can be used to break the passwords of accounts on a Microsoft Windows operating system. It is always best to use a password that contains a minimum of 8 characters and includes uppercase letters, lowercase letters and special characters. Even when a very strong password is utilized, if an attacker has physical access to the machine and is able to gain administrative rights to that machine, there are tools available that can be used to display the password in plain text.

For this lab on Windows Password Cracking, the following terms and concepts will be of use:

Cain – Cain is a password-cracking suite that will allow an attacker to crack passwords through a dictionary attack, the use of brute force, or a rainbow table. Cain, which is available from the website www.oxid.it, will not run on most computers that have anti-virus software installed. Cain does not run on Linux or Mac OS X systems.

LM HASH – The LAN Manager, or LM, hash dates back to the days of MSDOS. It is the default hash used for systems running DOS, Windows 3.11, Windows, 95, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows 2003. Some of the newer operating systems in the list can have their security settings adjusted so that the LM hash will not be used. However, their default setting is to use the LM hash, not NTLM.

NT HASH - The NTLM, or New Technology LAN Manager hash has been around for a while but it was not until the release of Windows Vista that it became the default hash used. Windows Vista, Server 2008, Windows 7, Server 2012, and Windows 8 all are set

to use the NTLM hash by default. However, their security settings can be scaled back to use the older, less secure, LM hash. It is more secure for the OS to use the NTLM hash.

WCE – Windows Credentials Editor will allow users to display hashes and the corresponding passwords in plain text. There is a 32 and 64-bit version. The tool is available via the following link: http://www.ampliasecurity.com/research/wcefaq.html

mimikatz – This tool will dump the stored logon hashes and provide the corresponding password that matched the hash in plain text. The tool, which is written in French, is available from the following link: http://blog.gentilkiwi.com/mimikatz

Pod Topology

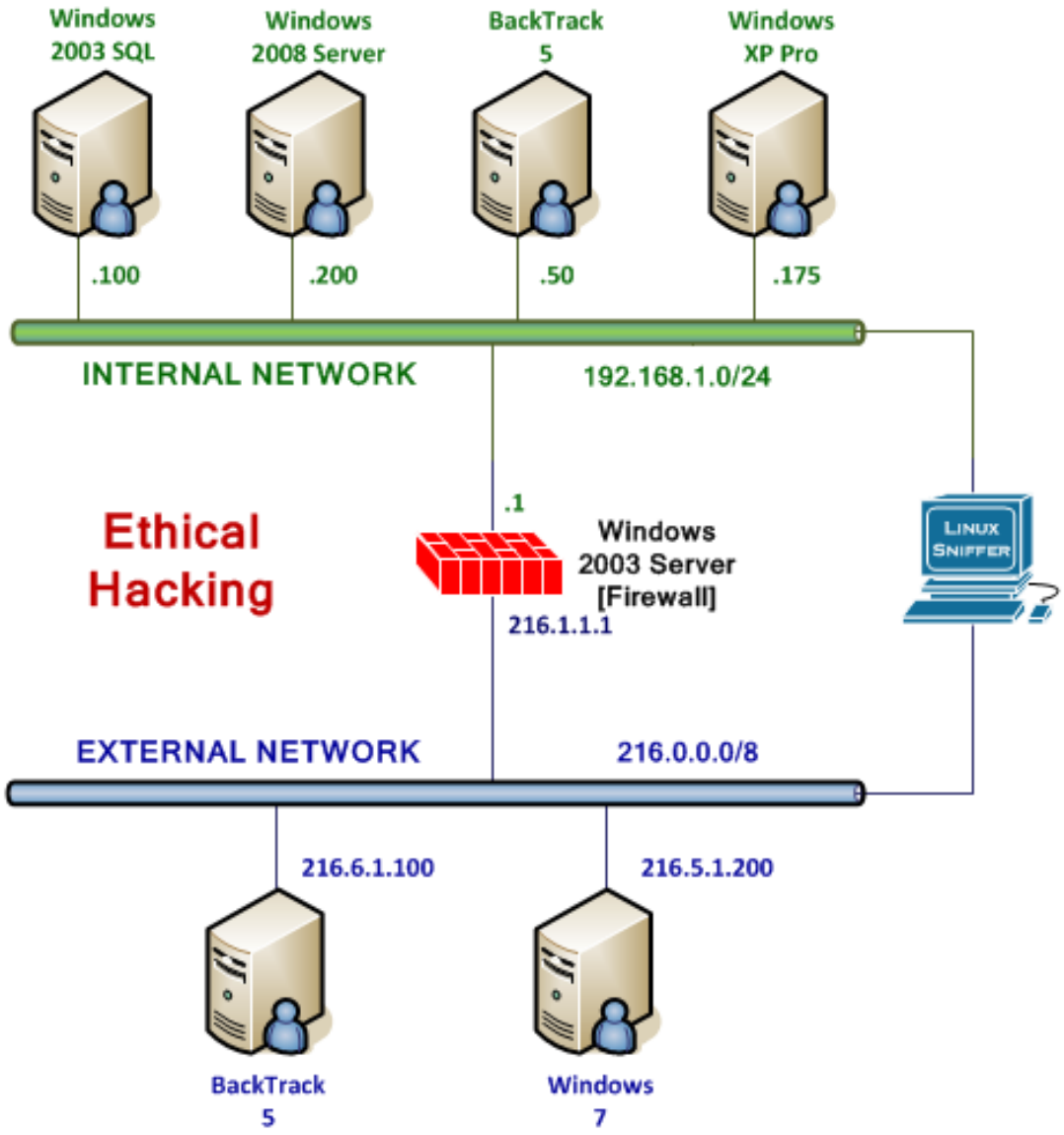

Figure 1: Lab Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

This lab requires the use of the **Windows XP Pro** machine.

Windows XP Pro	192.168.1.175
Windows XP Pro **hacker** password	toor

1 Creating Users in Windows

Managing users and resetting their Windows passwords is one of the main tasks performed by individuals in network administration or help desk positions.
In many situations, hackers will also often perform these tasks, including:

- Creating new accounts
- Enabling accounts
- Escalating User Privileges
- Dumping Hashes
- Dumping Passwords

This lab will provide you with an opportunity to create user accounts and assign passwords.

1.1 Creating Users on a Windows System

Open the Local User Manager

1. On the **Windows XP Pro** system, click on **Start**, go up to the run box, and type the following:
   lusrmgr.msc

Figure 2: The lusrmgr.msc command

The command, lusrmgr.msc, works on computers running Windows 2000, XP, Server 2003, Vista, Windows 7, Server 2008, Windows 8, and Server 2012. However, the command will not work on Windows 2000, 2003, 2008, or 2012 Servers that are Domain Controllers. The command will also not work on Home versions of the Microsoft client operating system. Any Microsoft Windows operating system that has Home, Home Basic, or Home Premium in its name will not have a local user manager.

2. After you type lusrmgr.msc, the **Local Users and Groups** management console will appear. Double-click on the **Users** folder to view the system's user accounts.

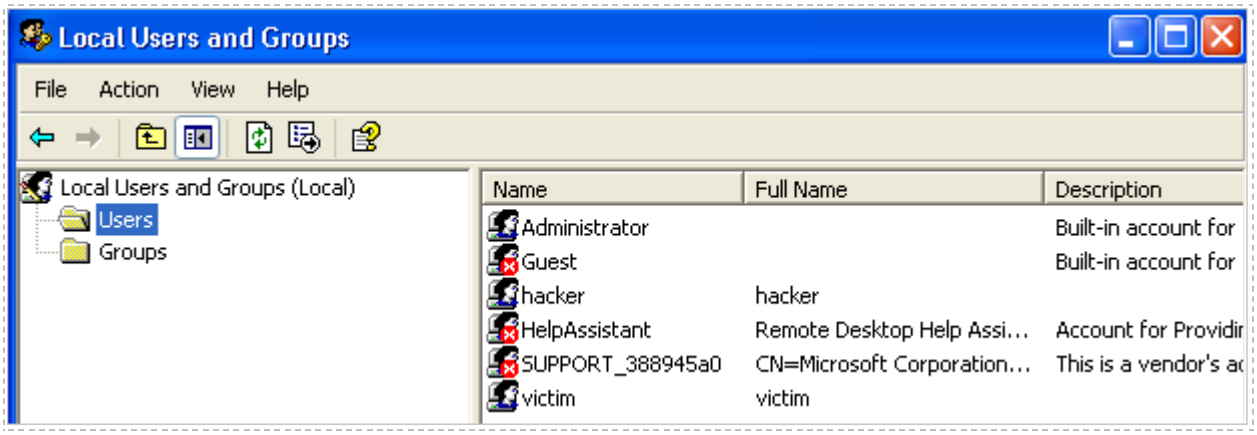

Figure 3: The Local Users and Groups Management Console

3. Users can be created from the Graphical User Interface (GUI) tool, Local Users and Groups, or from the command line. To use Local Users and Groups, right-click in the white space below the user list and select **New User…**

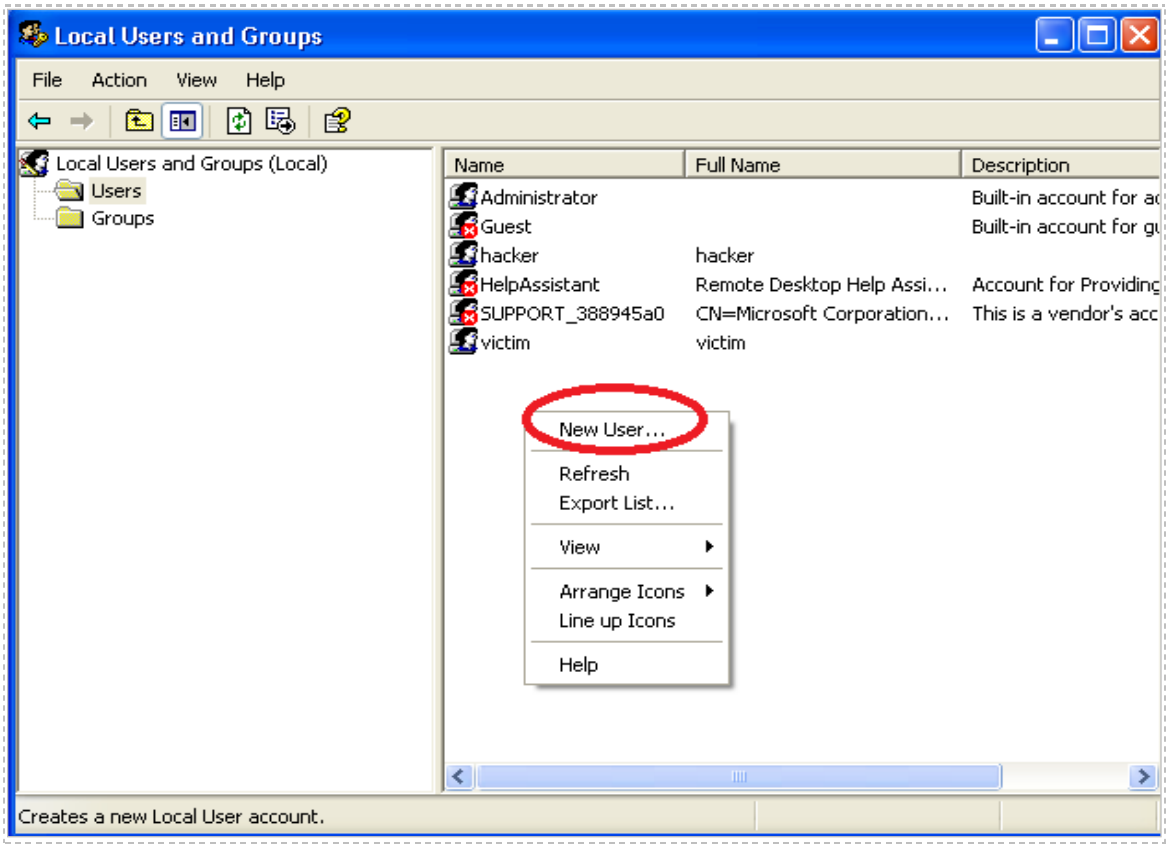

Figure 4: Creating a New User within the Local Users and Groups Management Console

4. At the New User screen:
    a. Type **bart** for the username.
    b. Type **simpsons** for the password.
    c. Type **simpsons** for the confirmation password.
    d. Uncheck User must change password at next logon.
    e. Check Password never expires.
    f. Click the Create button.
    g. Click Close.

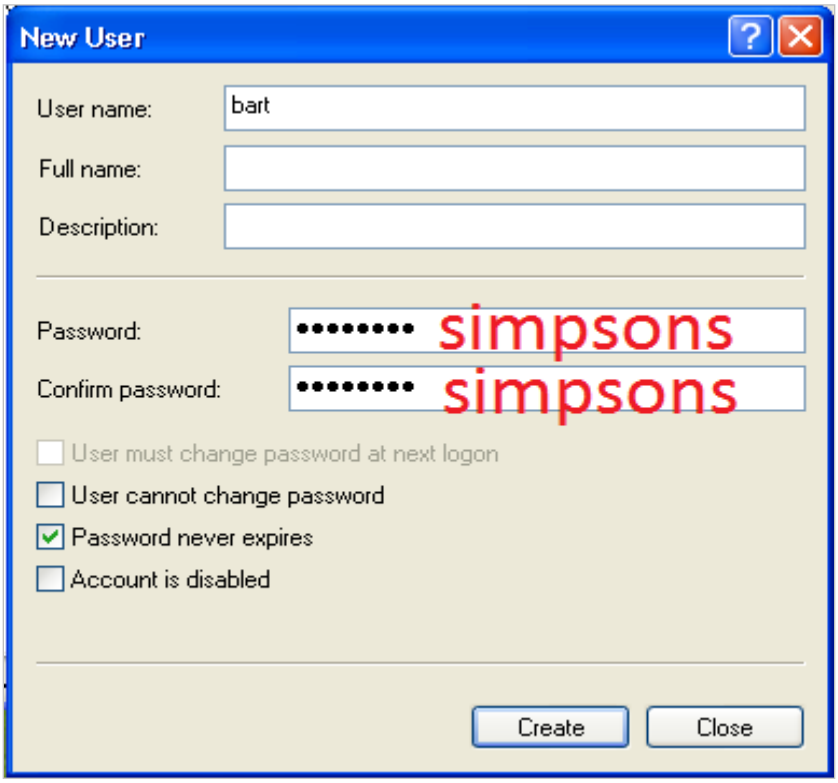

Figure 5: Creating the new user bart

5. View the user list. The user **bart** should be listed directly under **Administrator**.

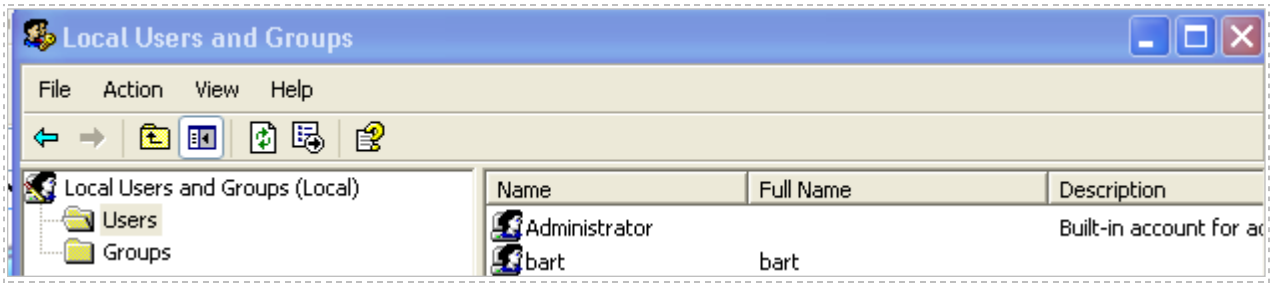

Figure 6: The User Bart has been Created

6. Right-click in the white space below the user list and select **New User…**

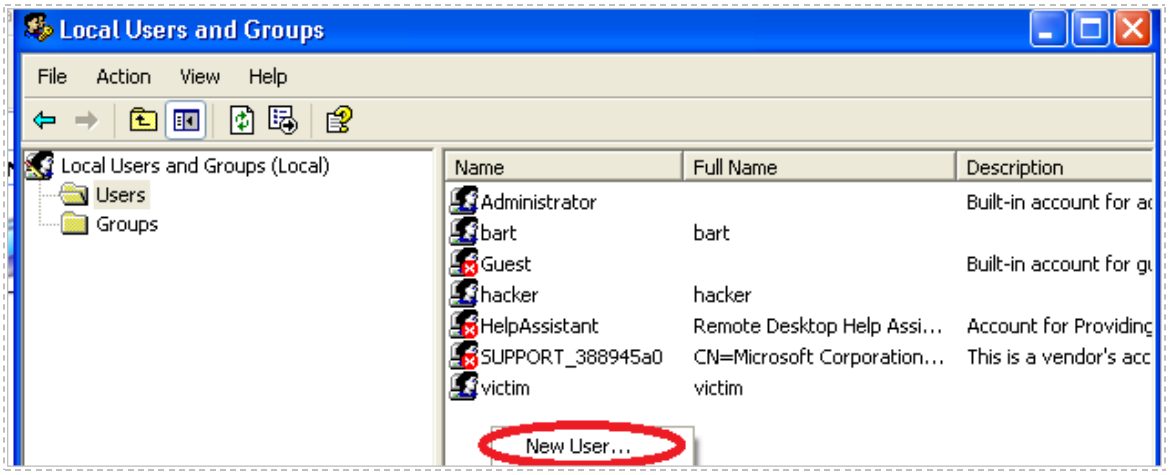

Figure 7: Windows Firewall is on

7. At the New User screen,
   a. Type **lisa** for the username.
   b. Type **mycat** for the password.
   c. Type **mycat** for the confirmation password.
   d. Uncheck User must change password at next logon.
   e. Check Password never expires.
   f. Click the Create button.
   g. Click Close.

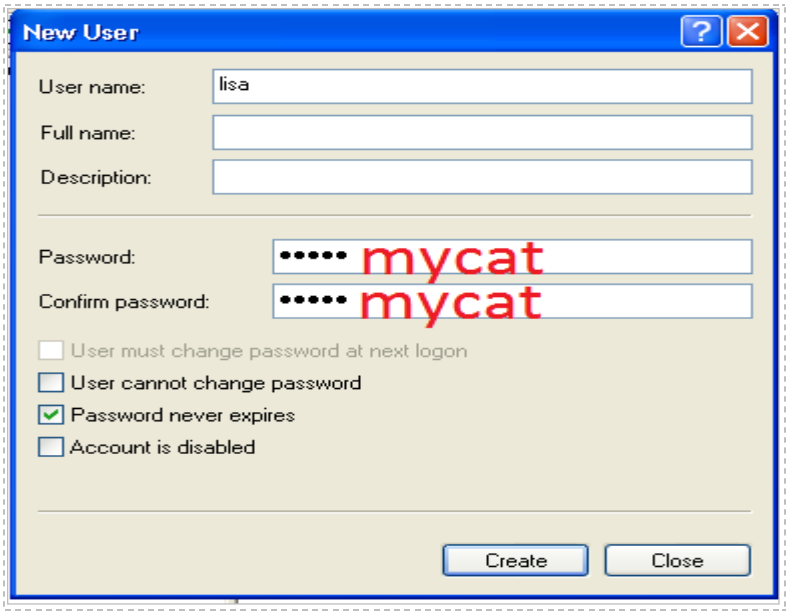

Figure 8: Creating the user list

8. View the user list. The user lisa should be listed directly under HelpAssistant. Click **File** from the Local Users and Groups menu bar and select **Exit**.

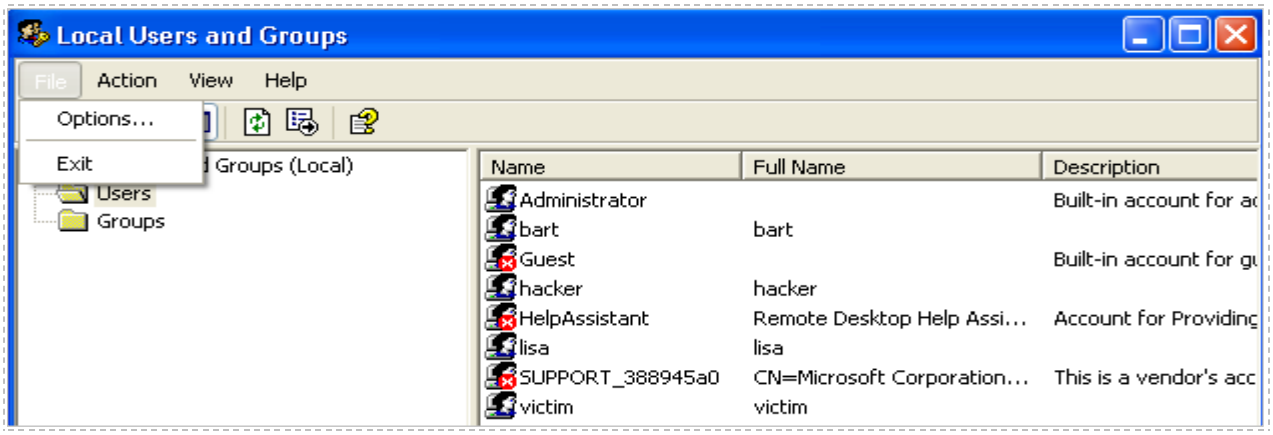

Figure 9: The user Lisa is Created

Users can also be created from the command line. Hackers tend to create their users from the command line because the tools they use to connect to their victims do not always have a GUI. Hackers tend to be proficient with commands.

9. Open the command prompt on the **Windows XP Pro** machine by clicking the desktop shortcut for the **Command Prompt**.

Figure 10: A Shortcut to the Command Prompt

10. To add the user homer with the password of funny, type the following:
C:\>**net user homer funny /add**

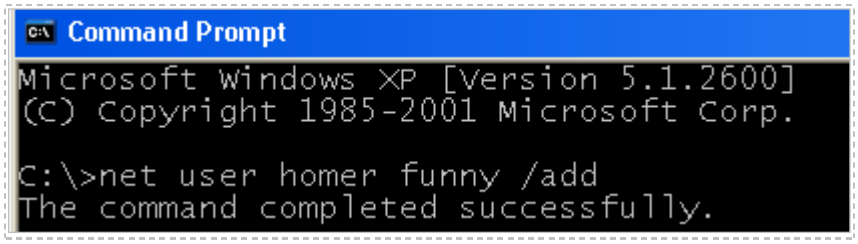

Figure 11: The User Homer is Successfully Added

You should receive the message that *the command completed successfully*.

11. To add the user **marge** with the password of **myblue**, type the following:
    C:\>**net user marge myblue /add**

Figure 12: The User Marge is Successfully Added

12. To add the user **maggie** with the password of **y!**, type the following:
    C:\>**net user maggie y! /add**

Figure 13: The show all command

13. To add the user **moe** with the password of **!a**, type the following:
    C:\>**net user moe !a /add**

Figure 14: Multiple OS Results

14. To display all of the users on the local system, type the following:
    C:\>**net user**

Figure 15: The Net User Command

1.2 Conclusion

User administration can be done through the command line or through the GUI. The net user command can be utilized to add users and view all the accounts on the system. Managing users and resetting their Windows passwords is one of the main tasks performed by individuals in network administration or help desk positions.

1.3 Discussion Questions

1. What is the command to create the user Selma with the password of hair?
2. What is the command to launch the Local User Manager from the run box?
3. Will the Local User Manager work on a server that is a Domain Controller?
4. Will the Local User Manager work on Windows 8 Home Premium?

2 Breaking Windows Passwords

Users' passwords are not stored in the Microsoft Windows registry. Instead, their password hashes are stored in the SAM file in C:\Windows\System32\Config. There are programs, such as Cain, pwdump, and fgdump, which can dump these hashes. Cain is a GUI based program while pwdump and fgdump are command line tools. Cain can be downloaded from the following link: http://www.oxid.it/downloads/ca_setup.exe

2.1 Breaking Windows Passwords with Cain

Launch Cain to Extract the Hashes from the Local Machine

1. Click the shortcut to **Cain** on the **Windows XP Pro** desktop.

Figure 16: The shortcut to Cain

2. Click the **Cracke**r tab (key icon) in the middle of the Cain program.

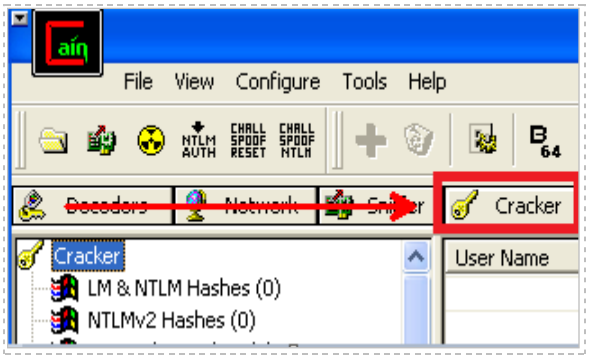

Figure 17: The Cracker Tab of Cain

3. Right-click in the white space and select **Add to list**.

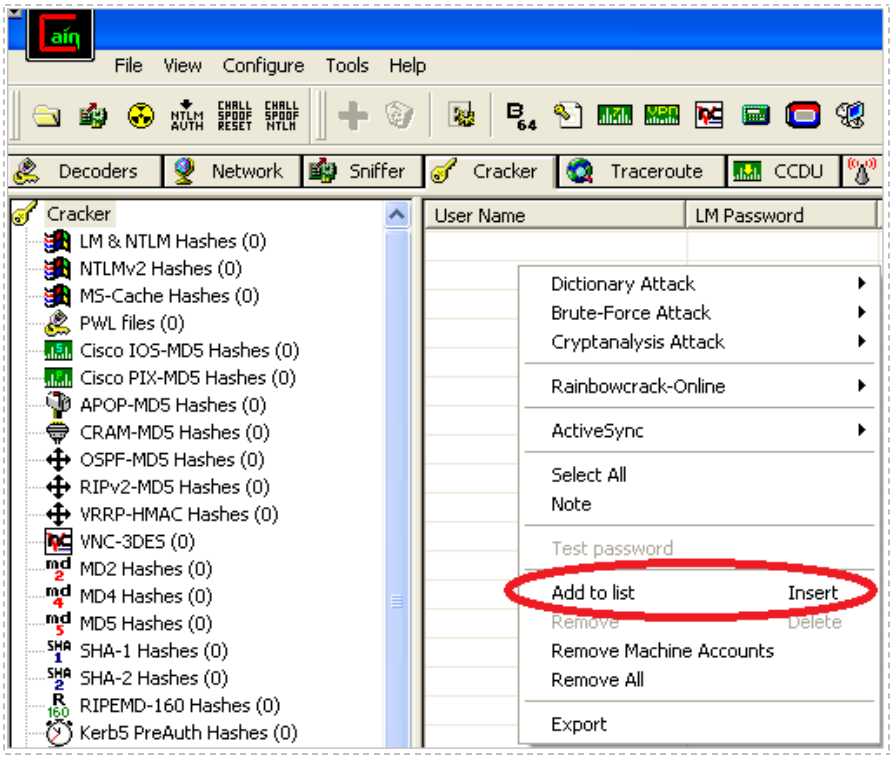

Figure 18: Adding to the List within Cain

4. Verify that **Import Hashes from local system** is selected and click Next**.**

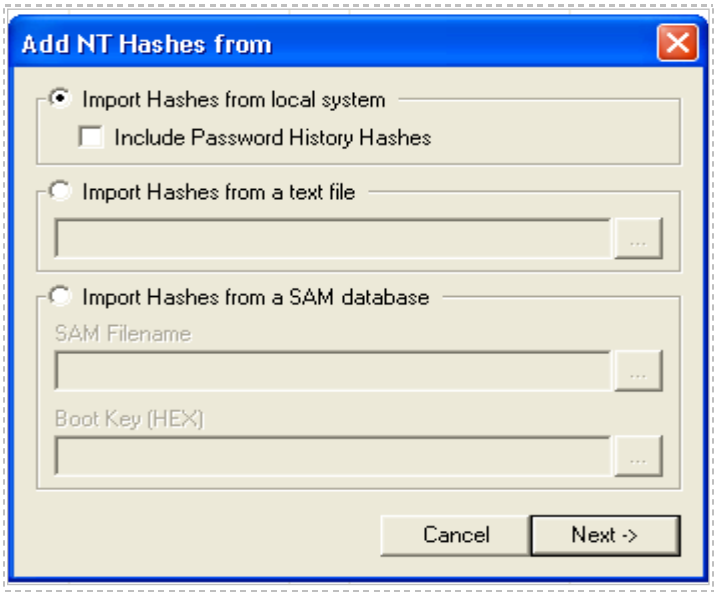

Figure 19: Import Hashes from a Local System

5. View the list of local Windows accounts and their corresponding hashes.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
Administrator				921AA366F261191078BE710E0E4AC29B	C8ACD9CDAD44F747E45D760F8C489DAB
bart				E6088F5EC227D7F393E28745B8BF4BA6	F8B551702EDE50782D95D6C83A2200A6
Guest	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C0
hacker		*		A9A1D510B01177D1AAD3B435B51404EE	AFC44EE7351D61D00698796DA06B1EBF
HelpAssistant				56991EC2DEBE0A22379753C3550506A8	535B8A5CB471C874715FA13259623614
homer		*		A24F150836EE9ABBAAD3B435B51404EE	C700FBDFC9007A715D8C0DC879DB6A9C
lisa		*		D8C770C7E94592D9AAD3B435B51404EE	EEC1E8A883208C9A53FD91821F0EAB68
maggie		*		C6EBE8776A153FEBAAD3B435B51404EE	BCDF115FD9BA99336C31E176EE34B304
marge		*		1C575548D2332D49AAD3B435B51404EE	D6FCE10188753E5950DF71A3596564A4
moe		*		A49DC3F590CCA23DAAD3B435B51404EE	632D38A11FA14E5D2610ADAC4202C7B4
SUPPORT_388945a0	* empty *	*		AAD3B435B51404EEAAD3B435B51404EE	9765E54143F42EE07EC69CEE5B4280C3
victim	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C0

Figure 20: The Windows Users Accounts

The two types of hashes extracted from the SAM file are the LM and NTLM hashes. The LAN Manager, or LM hash, dates back to the days of MSDOS. It is the default hash used for systems running DOS, Windows 3.11, Windows, 95, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows 2003. Some of the newer operating systems in the list can have their security settings adjusted so that the LM hash will not be used. However, their default operating system setting is to use the LM hash, not NTLM.

The NTLM, or New Technology LAN Manager hash, has been around for a while but it was not until the release of Windows Vista that it became the default hash used. Windows Vista, Server 2008, Windows 7, Server 2012, and Windows 8 all are set to use the NTLM hash by default. However, their security settings can be scaled back to use the older, less secure, LM hash. It is more secure for the OS to use the NTLM hash.

Three methods that can be used to crack passwords:

Method	Description
Dictionary Attack	In order for this method to be successful, the password must exist in the dictionary. If the dictionary does not contain the password, the password will not be cracked.
Cryptanalysis Attack (Rainbow Table)	In this case, a large list of hashes and their corresponding passwords are listed in the table. The time it takes to crack the password depends upon the amount of time it takes to search for the hash and corresponding password in the table.
Brute Force Attack	This method, which is the most time consuming, will try all possible combinations until the password is cracked.

6. Right-click in the white space and click on **Select All** to select all accounts.

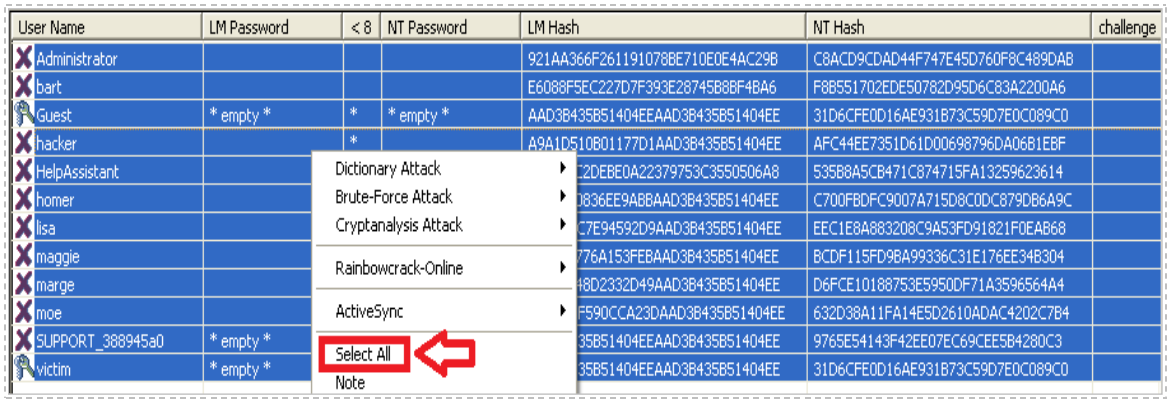

Figure 21: Selecting All Users

7. Right-click and then Select **Dictionary Attack,** and then select the **NTLM Hashes** choice from the list.

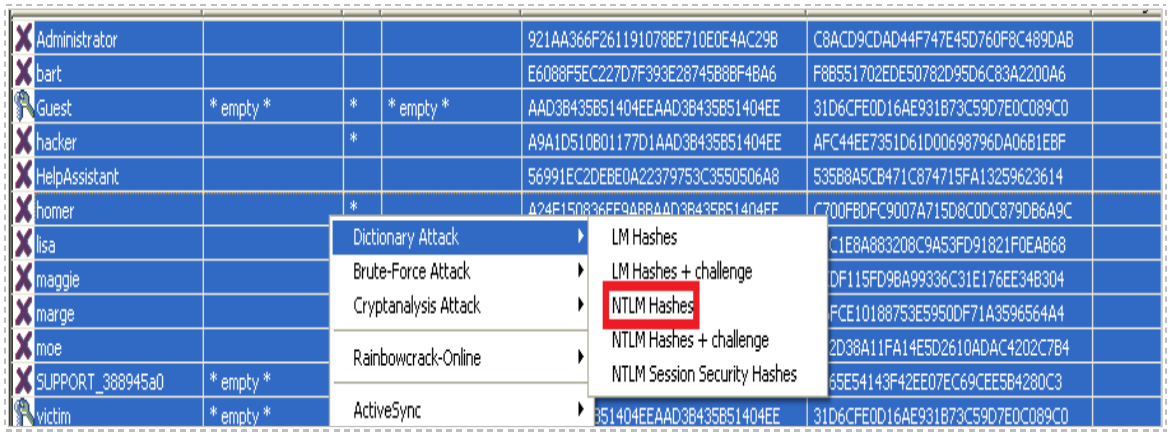

Figure 22: A Dictionary Attack on the NTLM Hashes

8. Right-click in the top pane under the word Dictionary and select **Add to list.**

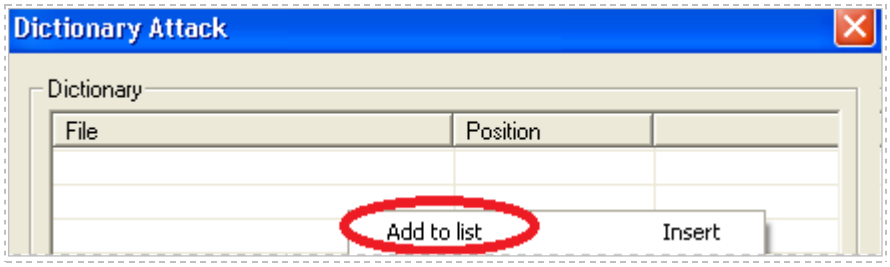

Figure 23: Adding a Dictionary File to the List

9. First, double-click on the **Wordlists** folder. Now, double-click on **Wordlist.txt.**

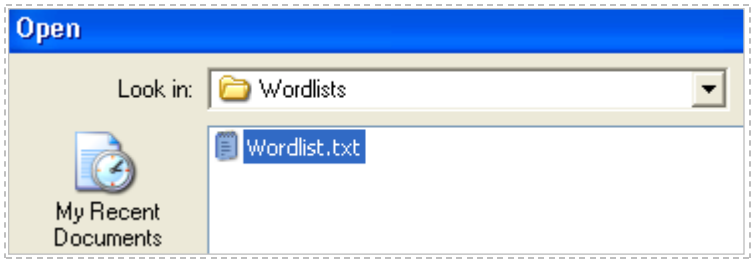

Figure 24: The Wordlist.txt Dictionary file

10. Click the **Start** button in the bottom right corner to start the dictionary attack.

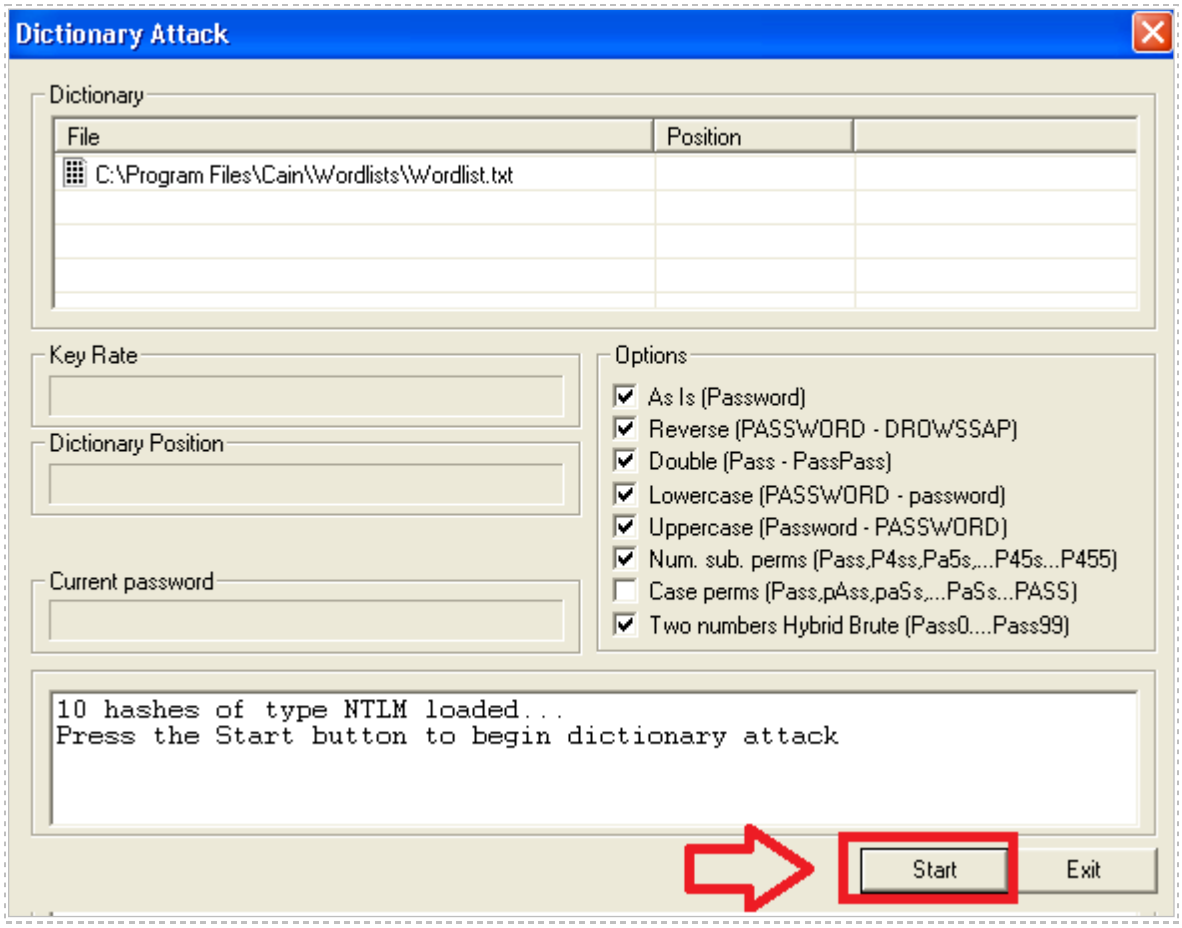

Figure 25: Starting the Dictionary Attack

11. The plaintext passwords for three password hashes are revealed. Click Exit.

```
Plaintext of C700FBDFC9007A715D8C0DC879DB6A9C is funny
Plaintext of AFC44EE7351D61D00698796DA06B1EBF is toor
Plaintext of F8B551702EDE50782D95D6C83A2200A6 is simpsons
Attack stopped!
3 of 10 hashes cracked
```

Figure 26: The Results of the Dictionary Attack

The wordlist.txt dictionary file that comes with Cain is located in the following directory: C:\Program Files\Cain\Wordlists. If the plain text passwords are not located within the dictionary file, the plaintext passwords will not be revealed. Another method, such as a brute force attack or Cryptanalysis Attack (Rainbow Table) will have to be utilized.

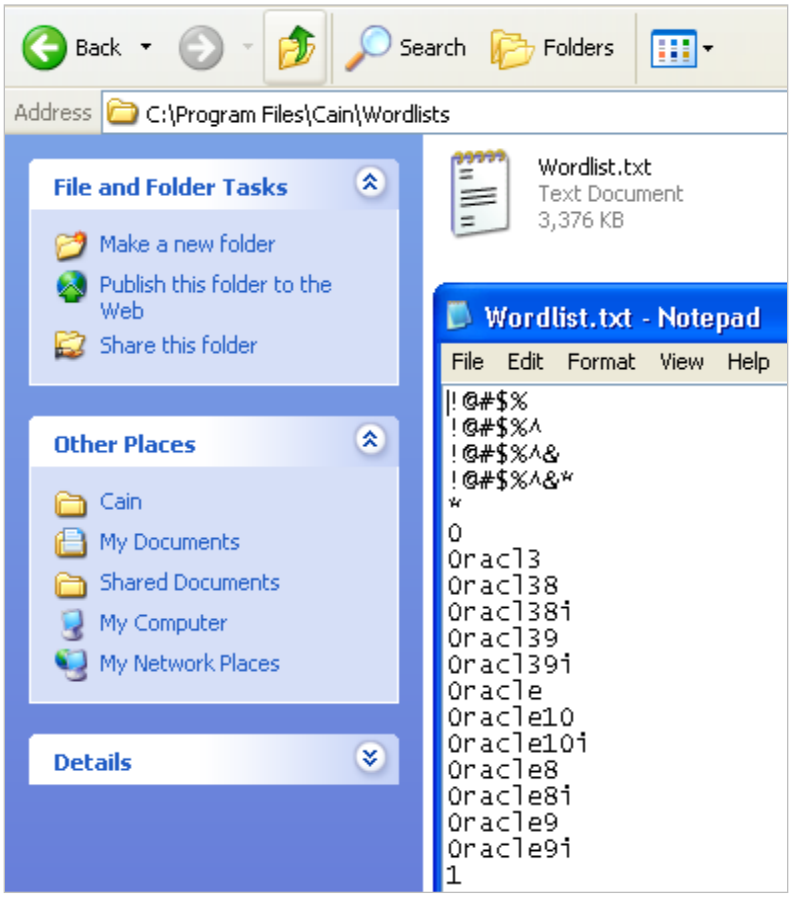

Figure 27: The Wordlist.txt Dictionary File

In order to perform a Cryptanalysis Attack with a Rainbow Table, you will need one or more Rainbow Tables. Rainbow Tables can be created with a program like Winrtgen, which is located in the C:\Program Files\Cain\Winrtgen folder. This program is placed in this folder when Cain is installed on the system. Double-clicking on the Winrtgen.exe file will open up a Rainbow Table generator for Windows. By clicking the add Table button, LM or NTLM rainbow tables can be generated. The time to generate the Rainbow Table will depend on the character set used and the maximum password length. Rainbow Tables can take a few hours or a number of years to generate, depending on the options selected.

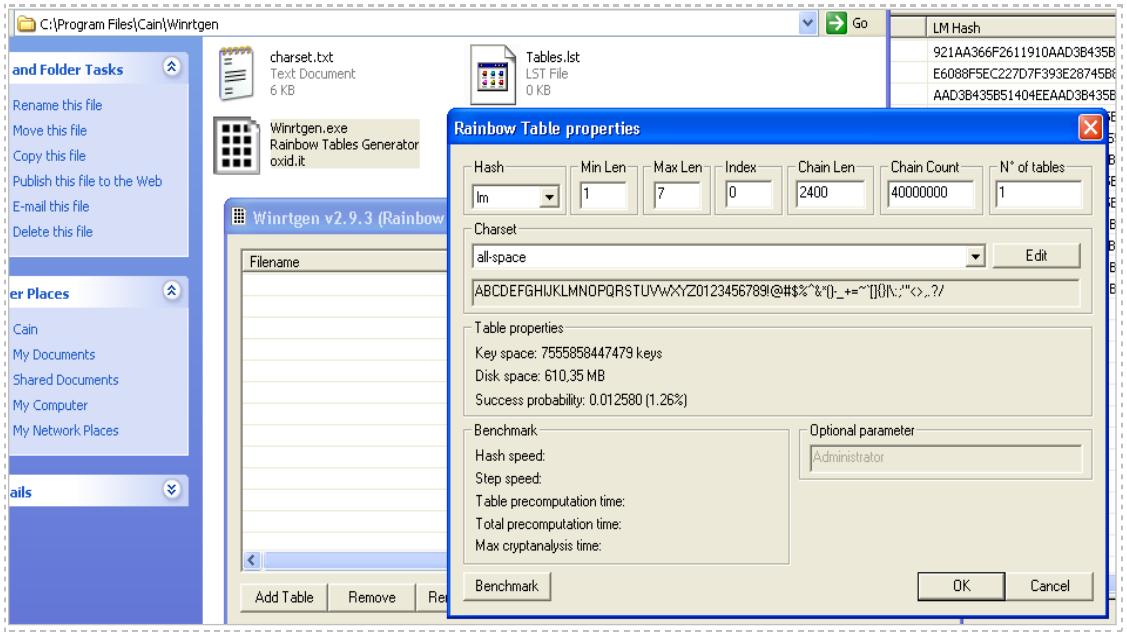

Figure 28: Generating Rainbow Tables with Winrtgen

12. Hold down the **CTRL** key and select the accounts without revealed passwords. Right-click, select **Cryptanalysis Attack > LM Hashes via RainbowTables (RainbowCrack)**

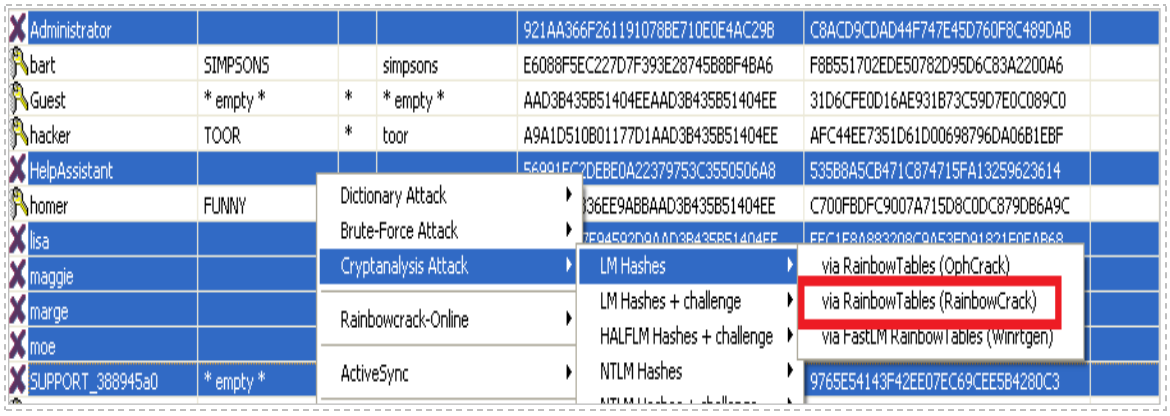

Figure 29: Cryptanalysis Attack

13. Click the **Add Table** button in the right hand pane of the LM Hashes cryptanalysis window.

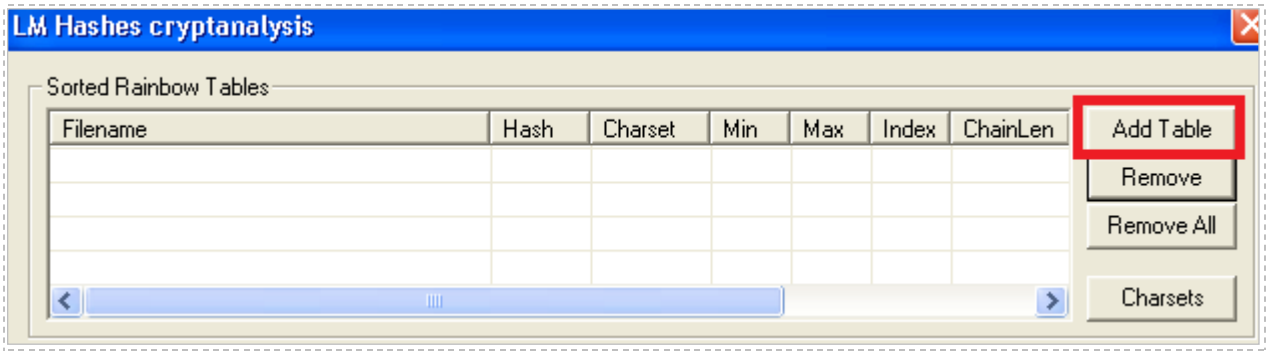

Figure 30: Adding a Rainbow Table

14. Browse to the desktop, and choose the LM rainbow table with the name **lm_alpha#1-7_0_2400x40000000_oxid#000.rt**. Double-click on it, then click **Start** to begin the Cryptanalysis Attack.

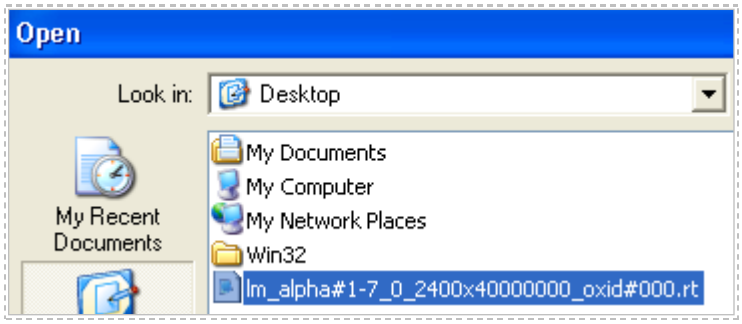

Figure 31: The LM Rainbow Table

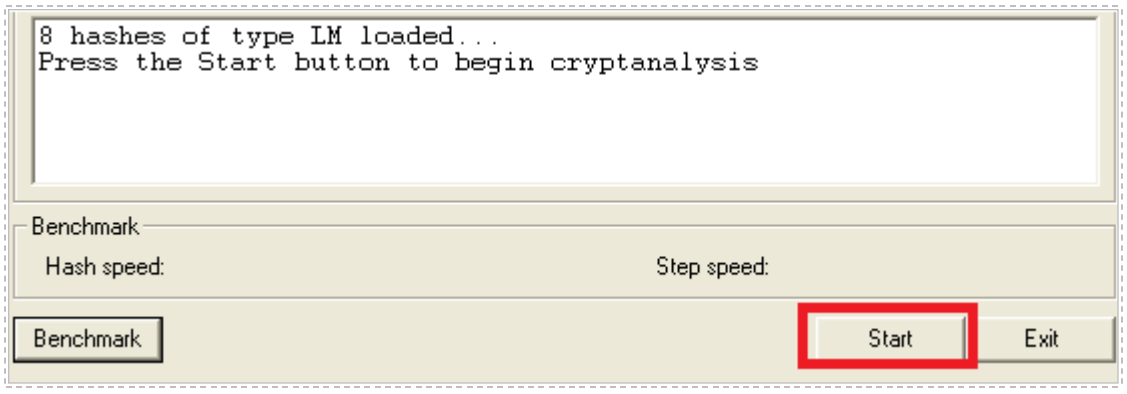

Figure 32: Starting the Cryptanalysis Attack

15. View the results. Three more passwords in the list are revealed. Click **Exit**.

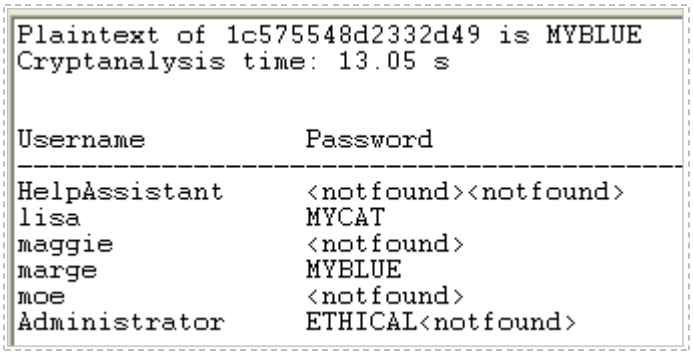

Figure 33: The Results of the Cryptanalysis Attack

16. Hold down **CTRL** and select **Maggie** and **Moe**. (Don't include Help Assistant or Support) Right-click, select **Brute Force Attack**, and then select **LM Hashes**.

Figure 34: A Brute Force Attack

17. Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length (Max) to 2 by using your mouse to reduce the max from the default. Click **Start**.

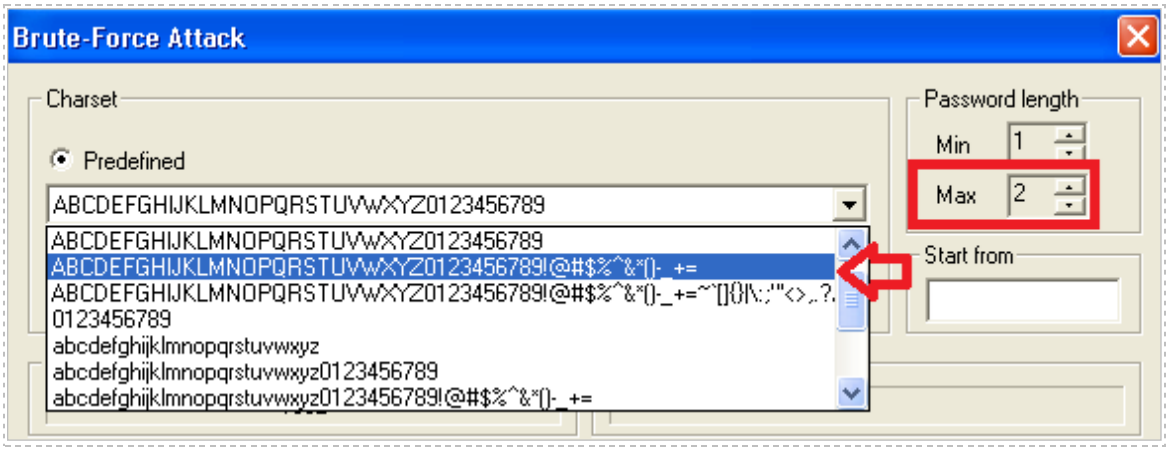

Figure 35: Options for a Brute Force Attack

18. View the revealed passwords. Click Exit to exit the Brute Force Attack.

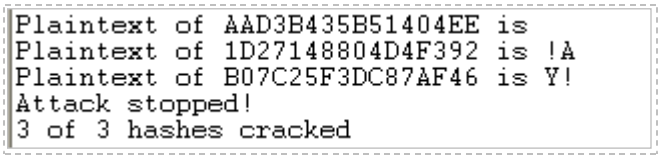

Figure 36: Passwords Cracked via Brute Force

All of the passwords you assigned to the users in this exercise were cracked. The HelpAssistant and Support Accounts were not cracked. These accounts are disabled on the system anyway by default, so it is not really necessary to crack their passwords. Although Brute Force could be used to crack these accounts, it is likely to take a long time. The administrator password will be attacked in Task 3 using a different technique.

Administrator	ETHICAL???????		
bart	SIMPSONS		simpsons
Guest	* empty *	*	* empty *
hacker	TOOR	*	toor
HelpAssistant			
homer	FUNNY	*	funny
lisa	MYCAT	*	mycat
maggie	Y!	*	y!
marge	MYBLUE	*	myblue
moe	!A	*	!a
SUPPORT_388945a0	* empty *	*	
victim	* empty *	*	* empty *

Figure 37: Passwords Cracked via 3 Methods

19. Right-click in the white space and select **Remove All** to remove the accounts.

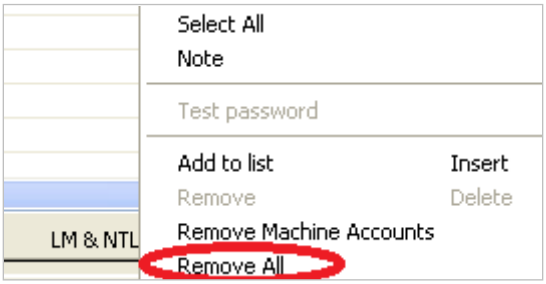

Figure 38: Removing the Accounts from Cain

We will now try the methods used in the previous examples to attempt to crack passwords.

20. Right-click in the white space of the Cracker tab and select **Add to list**.

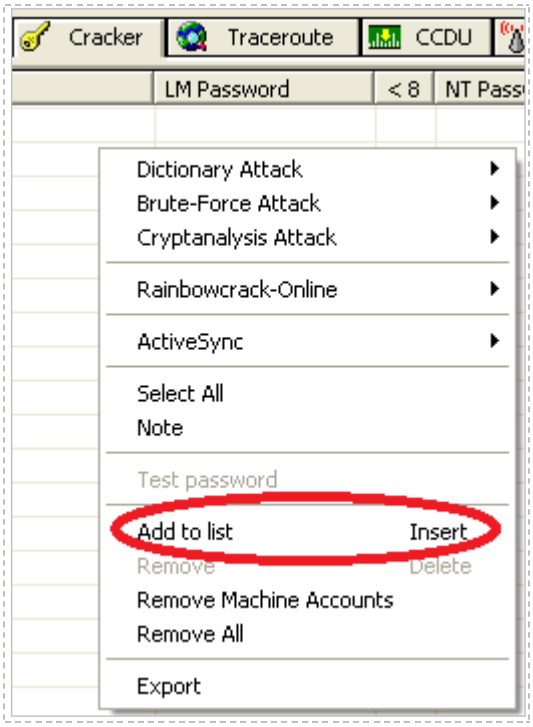

Figure 39: Select add to List within Cain

21. Click the radio button to **Import Hashes from a text file**.

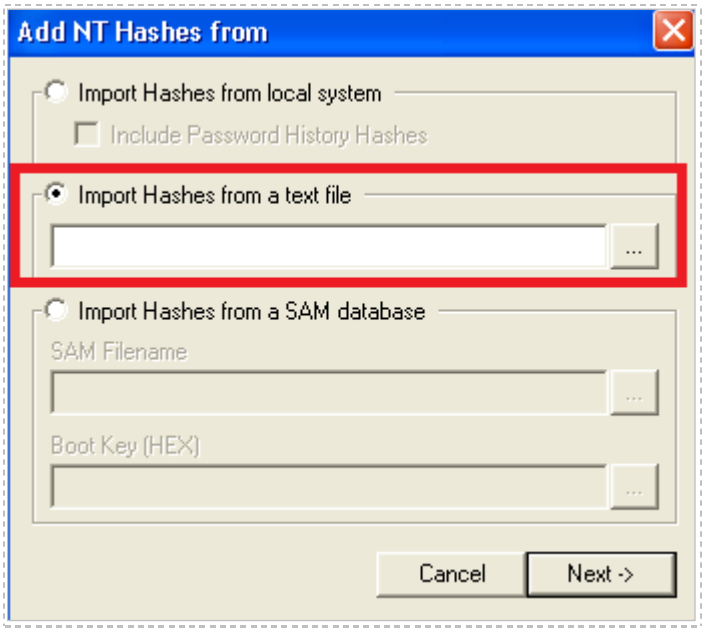

Figure 40: Select Import Hashes from a text file

22. Click the **Browse** square on the right. Click **Desktop** and click **accounts.txt**.

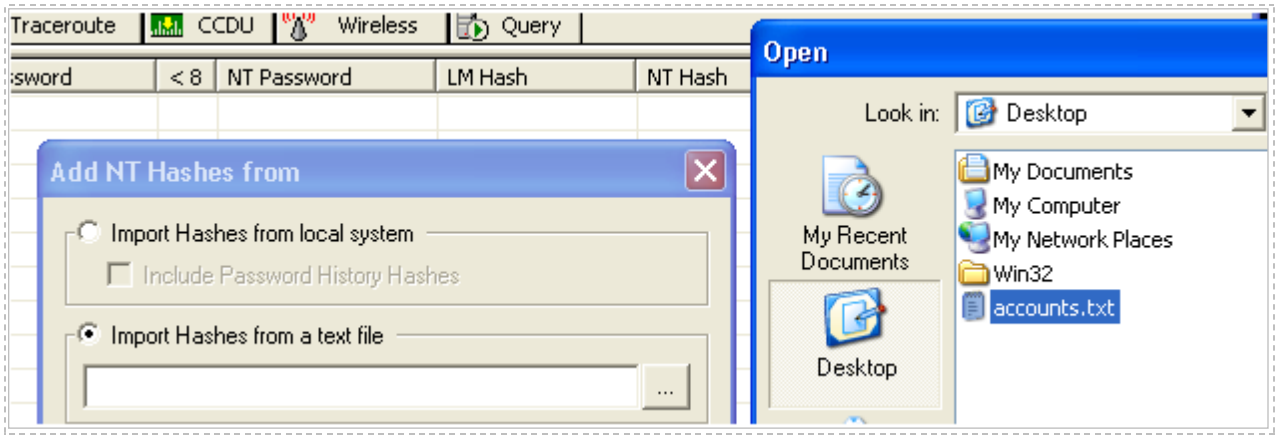

Figure 41: Select Import Hashes from a text file

23. Click **Next**. You should see a large list of users, starting with pmanning.

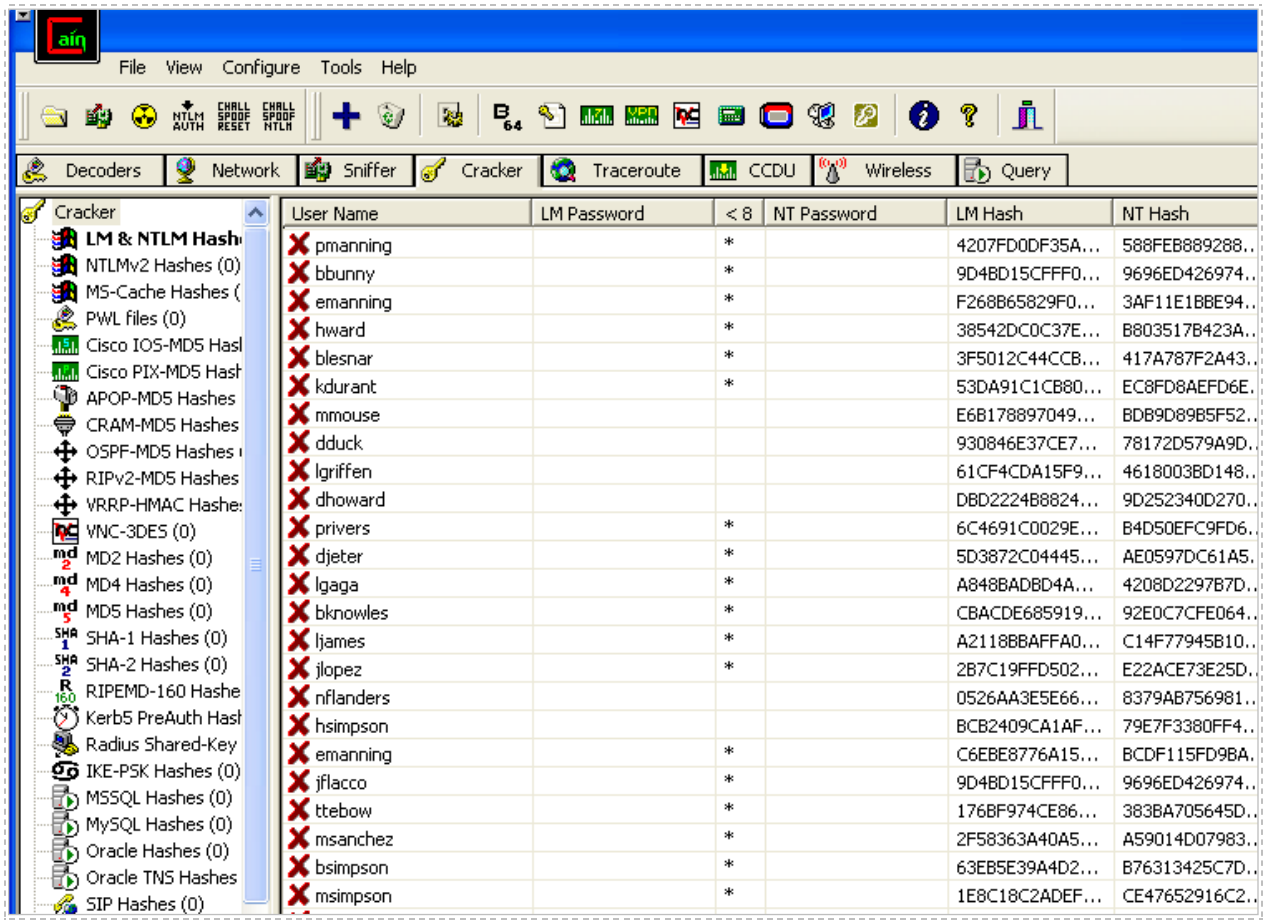

Figure 42: Select Import Hashes from a text file

In order to crack the passwords for all of the users, we can use one of three methods:

- Cryptanalysis Attack (Rainbow Table)
- Dictionary Attack
- Brute Force Attack

First, let's try to crack as many passwords from the list by using the Rainbow Table.

24. To crack the user's passwords listed, right-click and choose **Select All**.

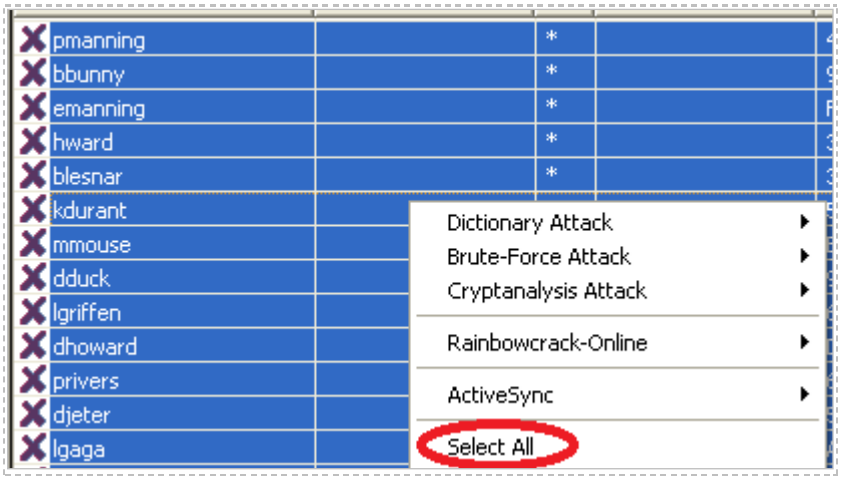

Figure 43: Select All

25. All the usernames in the list will be highlighted blue. To crack passwords, right-click and select **Cryptanalysis Attack LM Hashes via RainbowTables (RainbowCrack)**. You should receive the message that *37 hashes of type NTLM loaded…*

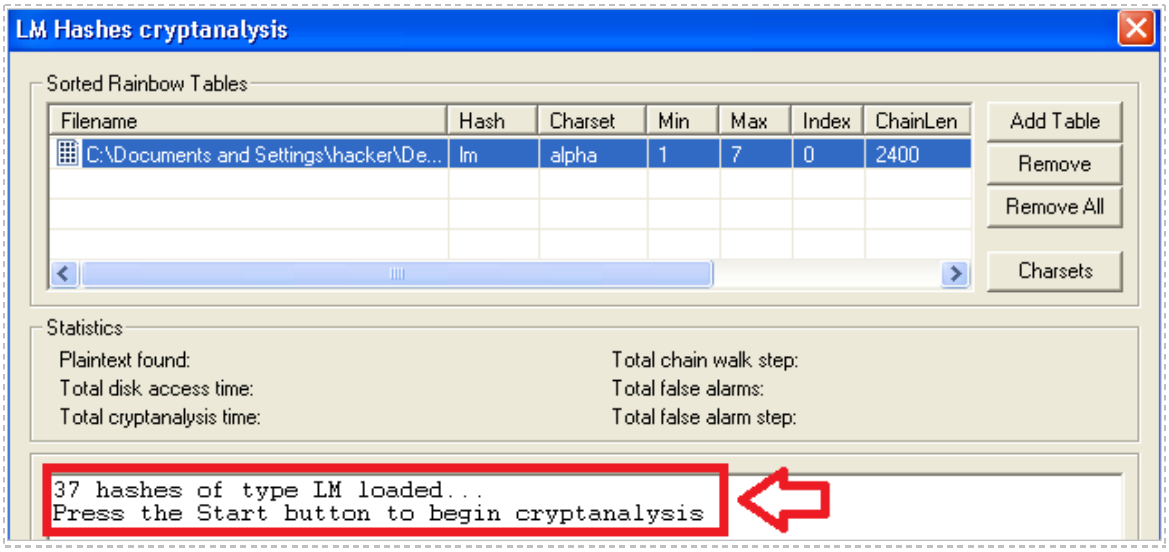

Figure 44: Cryptanalysis Attack

26. Click the **Start** button to begin the Cryptanalysis Attack on the hashes. After the Cryptanalysis Attack is over, 32 of 37 plaintext passwords will be revealed. Click **Exit** to leave the Cryptanalysis Attack screen to return to the user list.

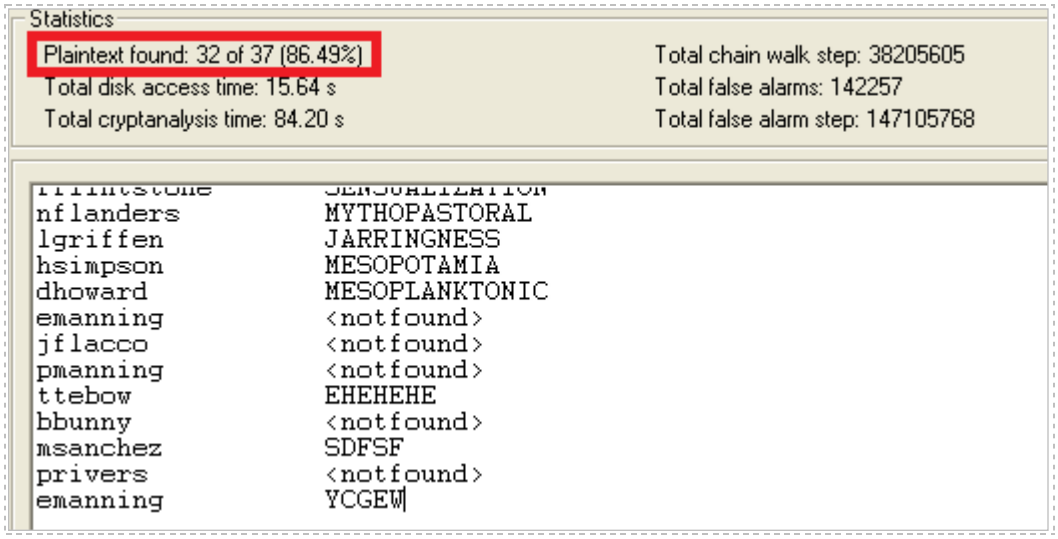

Figure 45: The Results of the Cryptanalysis Attack

27. Notice that all but six of the users' passwords have been cracked. Hold down **CTRL** and select the remaining six accounts without revealed passwords. Right-click, select **Dictionary Attack**, and then select the choice for **NTLM Hashes**.

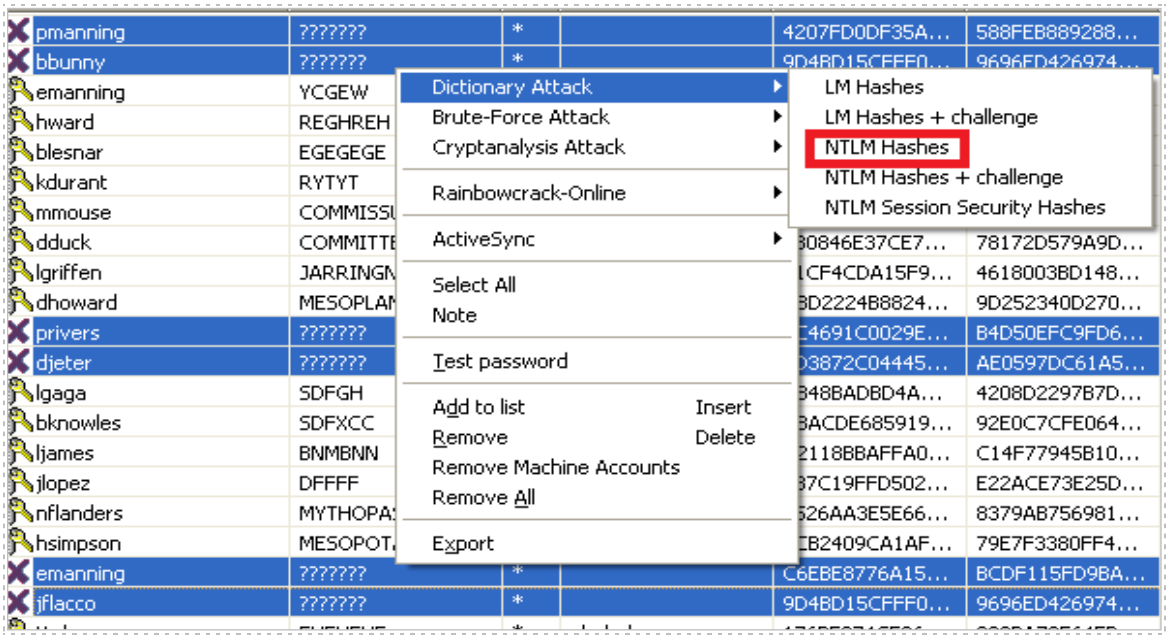

Figure 46: Selecting the Users with Unrevealed Passwords

Before starting the Dictionary Attack, we need to reset the initial file position of the dictionary. If this is not done, the dictionary attack will start from where the attack last left off. It is always a good idea to reset the initial file position of the Dictionary file.

28. Right-click on **Wordlist.txt** dictionary file and select **Reset initial File Position**.

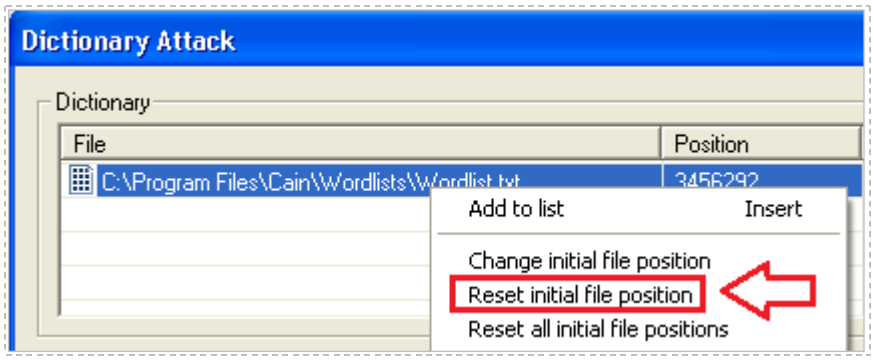

Figure 47: Reset initial File Position of the Dictionary File

29. Click the **Start** button to attack the 5 loaded hashes of type NTLM.

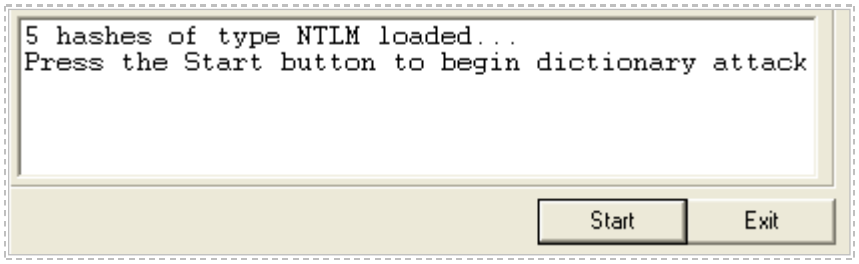

Figure 48: Starting the Dictionary Attack

30. You will receive the message that 3 of 5 hashes are cracked. Click **Exit**.

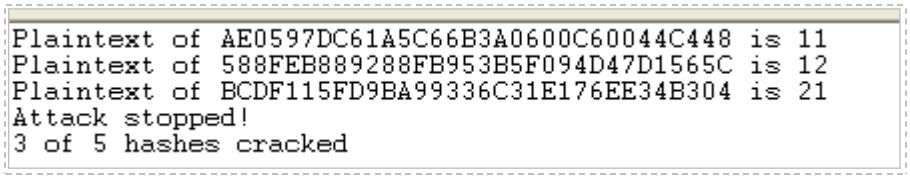

Figure 49: Three of Five Hashes were Cracked!

31. Notice that all of the users' passwords have been cracked except six of them. Hold down **CTRL** and select the accounts without revealed passwords. Right-click, select **Brute Force**, and then select the choice for **LM Hashes.**

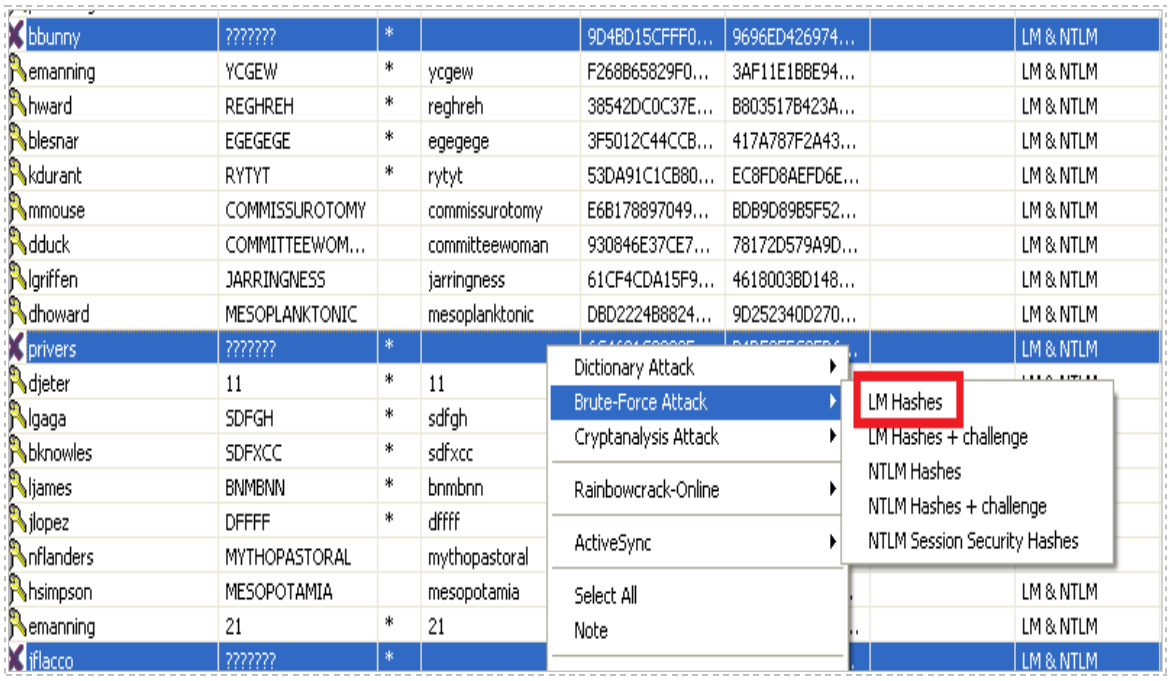

Figure 50: Brute Force Attack of LM hashes

32. Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length **(Max) to 2** by using your mouse to reduce the max from the default. Click **Start**.

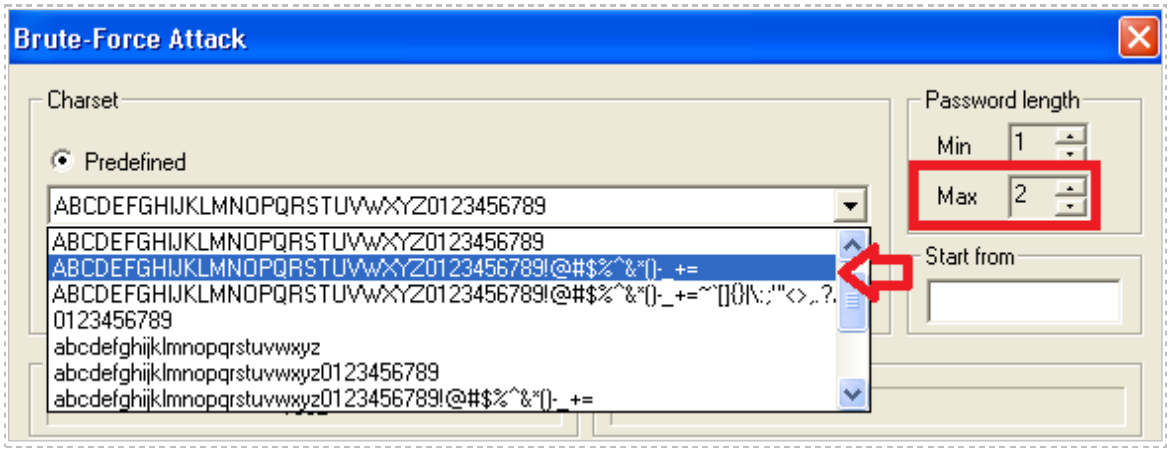

Figure 51: Options for a Brute Force Attack

33. You will receive the message, 3 *hashes of type LM loaded*. Click **Start**.

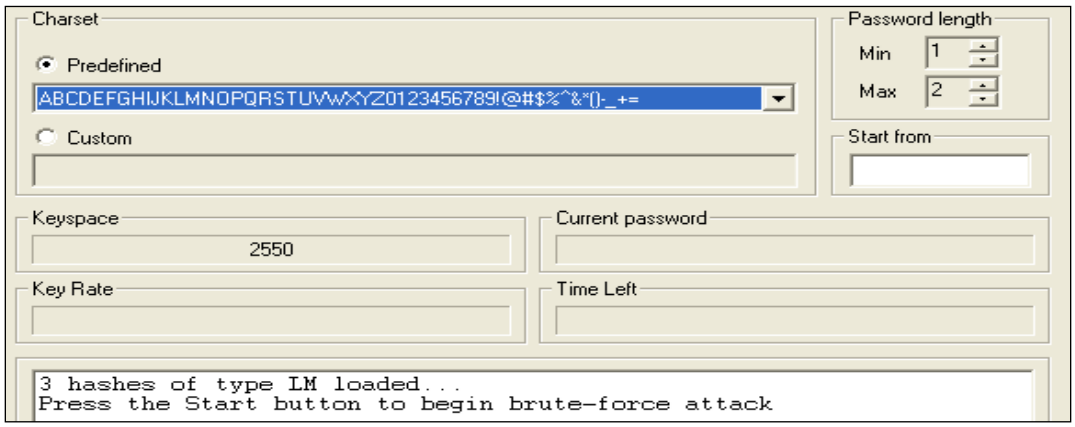

Figure 52: The Hashes are Loaded

34. The three hashes will be cracked. Click **Exit** to view the entire passwords list.

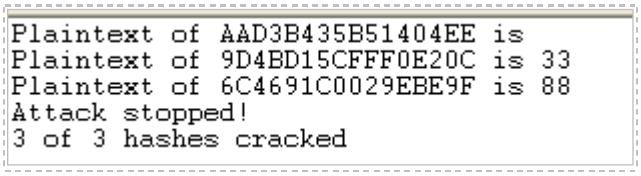

Figure 53: The Hashes are Cracked

35. Close Cain by selecting **File** from the menu bar and select **Exit**. Click **Yes** you are sure.

2.2 Conclusion

There are many techniques that can be used to crack passwords, including Dictionary Attack, Cryptanalysis Attack (Rainbow Table), and a Brute Force Attack. The dictionary attack only works if the password is contained within the dictionary. A Rainbow Table must first be generated in order to perform a Cryptanalysis Attack. The Brute Force Attack will take the longest of the three methods. Cain has support for all three attacks.

2.3 Discussion Questions

1. What file can be used to generate a Rainbow Table?
2. Why would you want to change the character set before you attempt a Brute Force Attack?
3. Where is the dictionary file located that comes with the Installation of Cain?
4. Which Microsoft operating systems are unlikely to have LM hashes present?

3 Dumping Windows Passwords in Clear Text

When we used Cain in Task 2, Cain dumped the hashes and we had to use a Cryptanalysis Attack, Dictionary Attack, or a Brute Force Attack to convert the hashes into plain text passwords. However, there are two tools, Windows Credentials Editor, or WCE, and Mimikatz that allow users to dump passwords in plain text.

3.1 Viewing Passwords in Clear Text

1. Open the shortcut to the command prompt on the **Windows XP Pro** desktop.

Figure 54: The Shortcut to the Command Prompt

2. Drag the **wce.exe** file into the Command Prompt window.

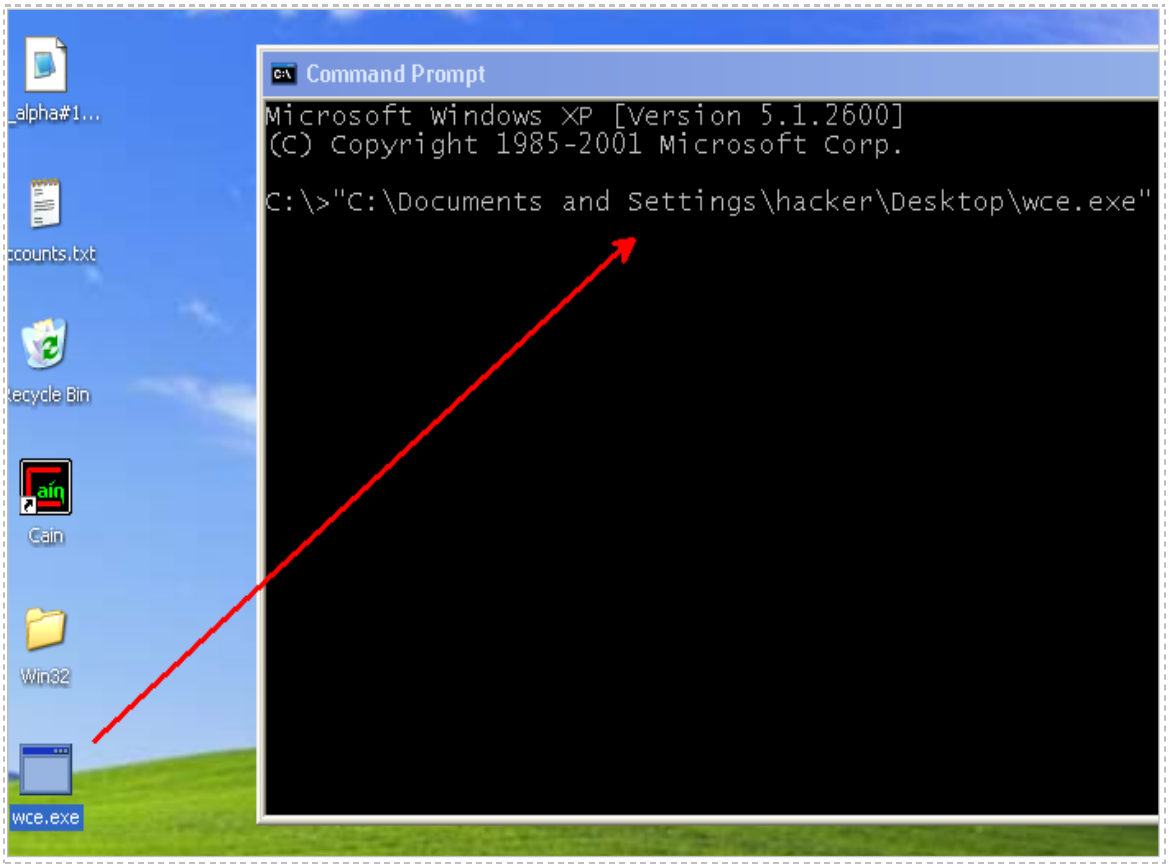

Figure 55: Drag wce.exe into the Command Prompt Window

3. Add a space and a question mark to the command to see the available switches:
   C:\>**"C:\Documents and Settings\hacker\Desktop\wce.exe" ?**

```
C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" ?
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security - by Hernan
 Ochoa (hernan@ampliasecurity.com)
Use -h for help.
Options:
        -l              List logon sessions and NTLM credentials (default).
        -s              Changes NTLM credentials of current logon session.
                        Parameters: <UserName>:<DomainName>:<LMHash>:<NTHash>.
        -r              Lists logon sessions and NTLM credentials indefinitely.
                        Refreshes every 5 seconds if new sessions are found.
                        Optional: -r<refresh interval>.
        -c              Run <cmd> in a new session with the specified NTLM credentials.
```

Figure 56: The Options for the Windows Credentials Editor

4. Add a space and a **-w** to the command to dump the cleartext passwords:
   C:\>**"C:\Documents and Settings\hacker\Desktop\wce.exe" -w**

```
C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" -w
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security - by Hernan
 Ochoa (hernan@ampliasecurity.com)
Use -h for help.


hacker\WINXP:toor
NETWORK SERVICE\WORKGROUP:toor
```

Figure 57: Dumping the Password in Clear Text

The mimikatz tool can also dump the passwords of other users that have logged on.

5. Log off as hacker by clicking on the **Start button** and selecting **Log Off**.
   Then, click **Log off** a second time when an additional log off box appears.

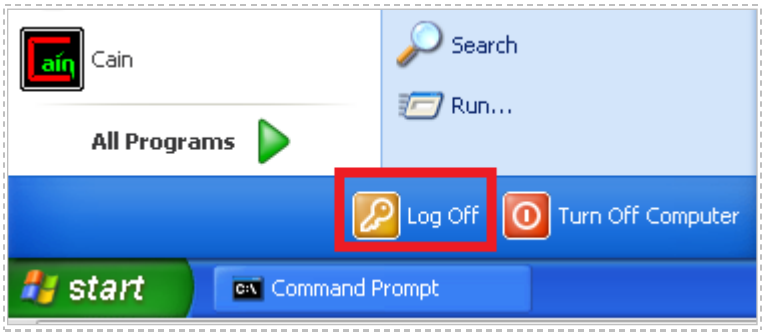

Figure 58: Logging off as Hacker

6. Log on as **Administrator** with the password of Ethicalhackin&.

Figure 59; Logging in as Administrator

7. Log off as administrator by clicking on the Start button and selecting **Log Off**. **Do NOT LOG OFF**, Select **Switch Users** instead, which will leave Administrator logged into the system.

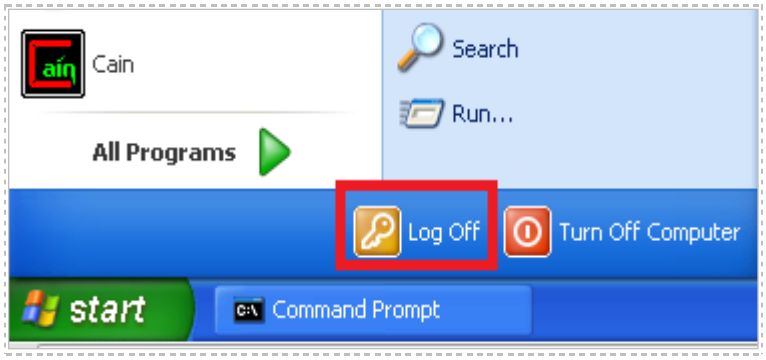

Figure 60: Logging off as Administrator

8. Log back into the XP system using the **hacker** account with the password of **toor**.

Figure 61: Logging in as hacker

9. Open the shortcut to the command prompt on the **Windows XP Pro** desktop.

Figure 62: The Shortcut to the Command Prompt

10. Double-click on the **Win32** folder on the Desktop of the hacker account. Drag the mimikatz file from the Win32 folder into the command prompt Window.
C:\>**"C:\Documents and Settings\hacker\Desktop\Win32\mimikatz.exe"**

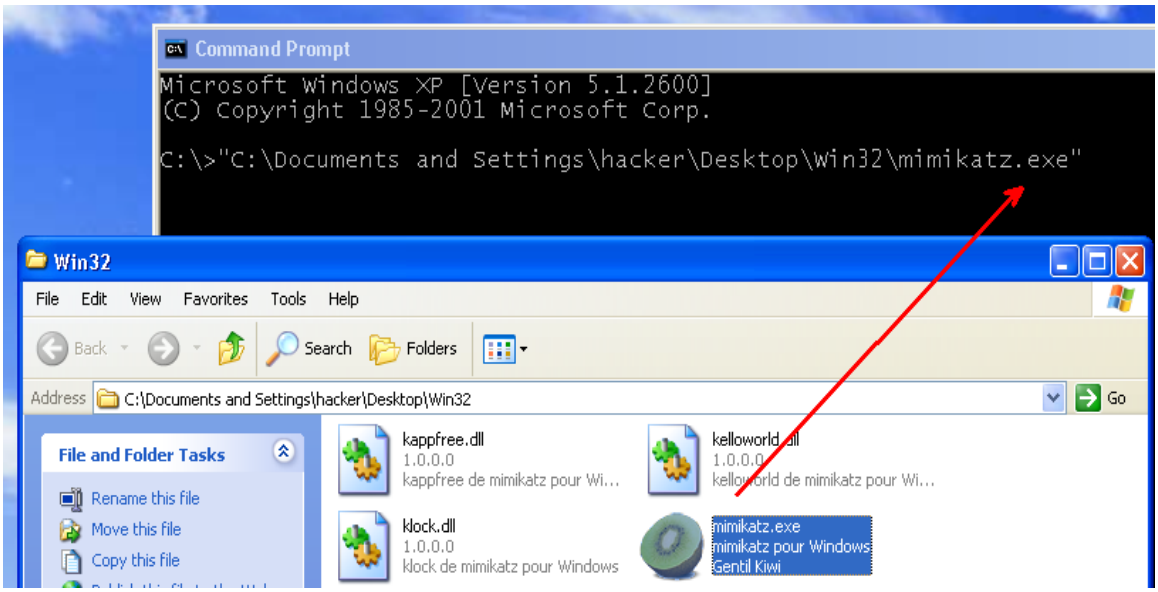

Figure 63: Dragging the Mimikatz file into the Command Prompt Window

11. Double-click on the **pass.txt** file in the Win32 folder. Copy the first line, **privilege::debug** and paste it into the mimikatz terminal:
mimikatz # **privilege::debug**

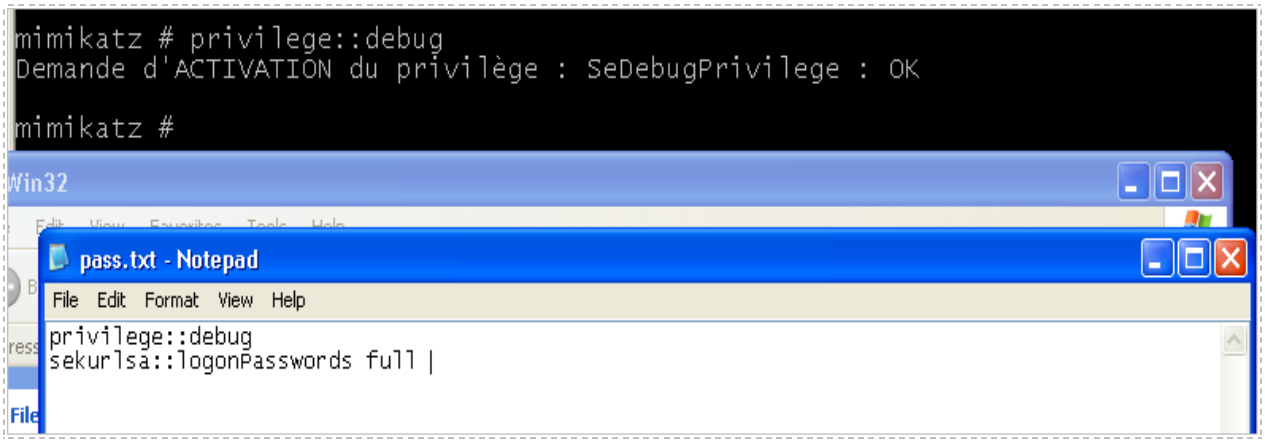

Figure 64: Listing the Files in the C Directory

If successful, you will receive the following message back from the mimikatz prompt:

Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK

12. Paste the second line from the pass.txt file into the mimikatz terminal:
    mimikatz # **sekurlsa::logonPasswords full**

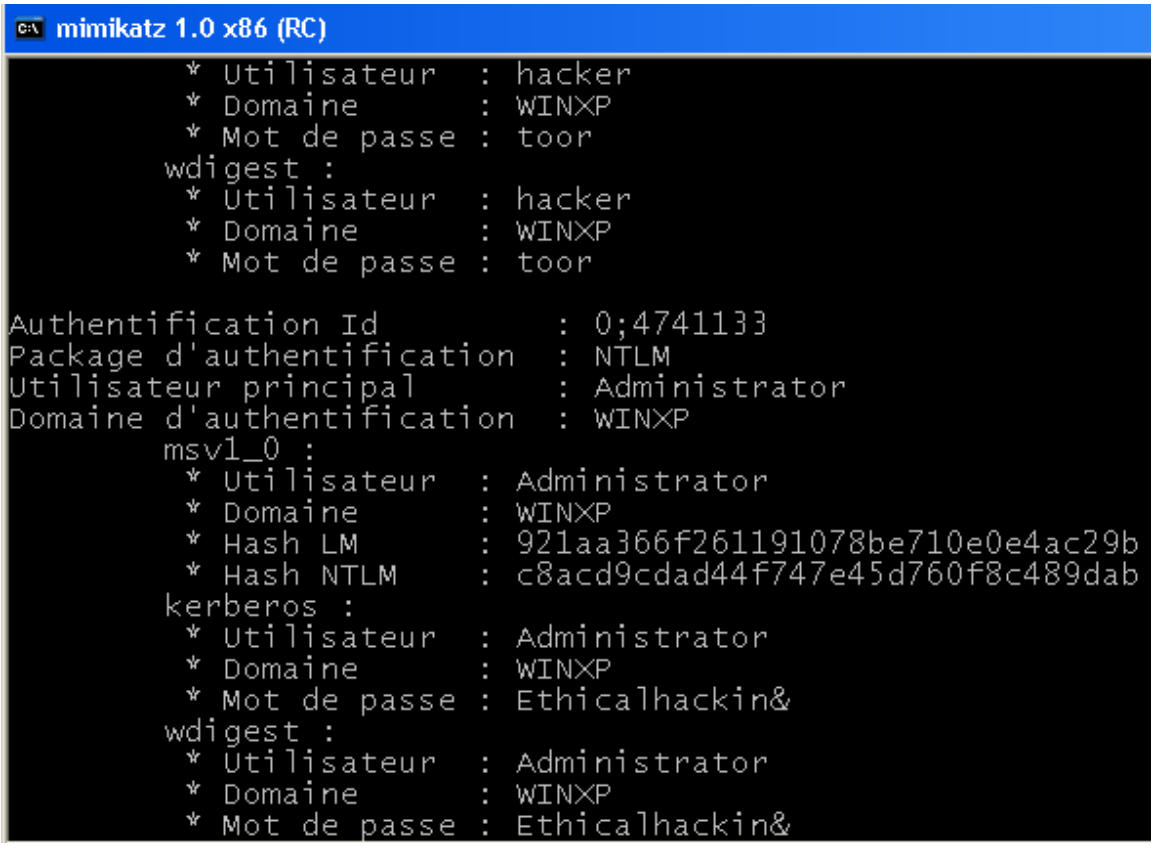

Figure 65: The Plain Text passwords for the administrator and hacker accounts are dumped

You may need to go back and redo steps 5-12 if you do not see the administrator's password dumped in clear text. These steps should be done in a timely fashion.

3.2 Conclusion

Windows Credentials Editor (WCE) and Mimikatz allow users to dump passwords in plain text. These tools pull the passwords from memory in plain text. Even if a user has a very complex password, the use of these tools will reveal their password easily.

3.3 Discussion Questions

1. What switch allows you to dump plain text passwords with WCE?
2. How does the WCE tool differ from the mimikatz tools?
3. What must a user do in order for mimikatz to retrieve a password from RAM?

References

1. Cain:
   http://www.oxid.it/cain.html

2. Windows Credentials Editor:
   http://www.ampliasecurity.com/research/wcefaq.html

3. Mimikatz:
   http://blog.gentilkiwi.com/mimikatz

4. Net User Command:
   http://retrohack.com/net-user-command-reference-and-examples/

5. Rainbow Table:
   http://en.wikipedia.org/wiki/Rainbow_table

