ITIS-62000: Principles of Information Security & Privacy

Project 2: Packet Eavesdropping and Analysis

Name: Yaswitha Sai Atluri

Student ID: 801366057

Password Cracking (Part 1)

Step 1: Downloaded and installed Virtual Box

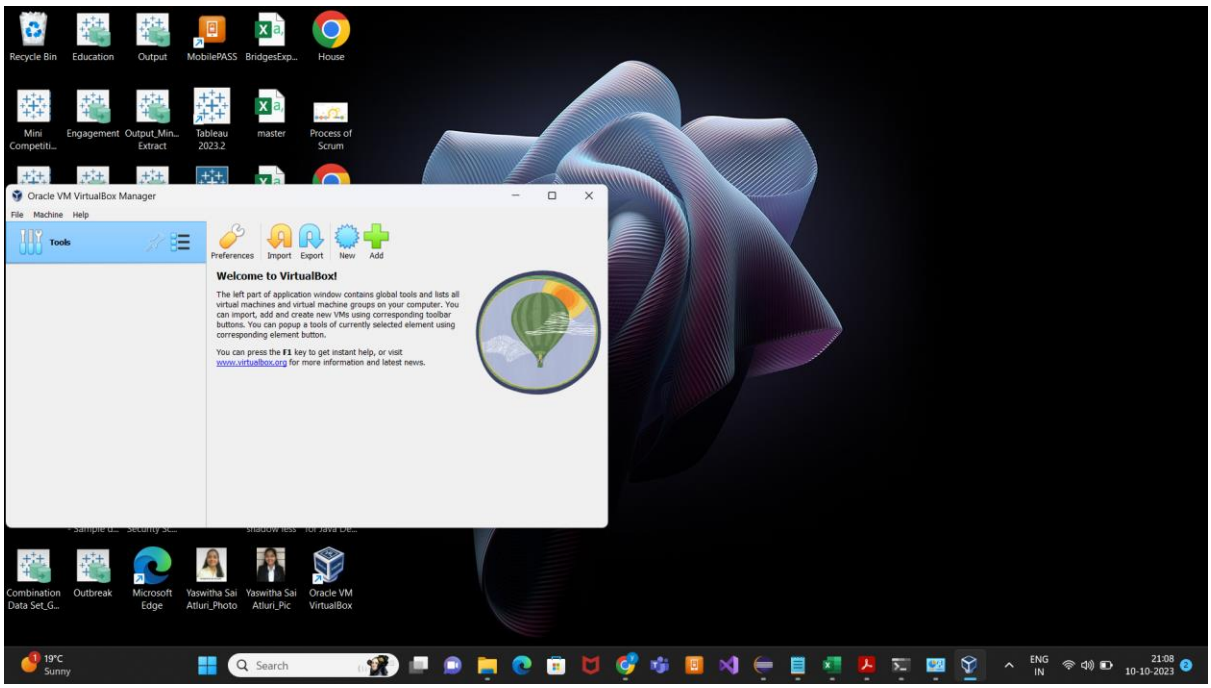

Figure 1: Installed Virtual Box

Step 2: Obtain a Windows XP copy by logging into your UNCC email account using a web browser. We already have permissions to users with UNCC email accounts.

- Open VirtualBox
- Select File -> Import Appliances
- Navigate to the location of the downloaded content.
- Select the ‘WindowsXP.ova’ file.
- Click "Import" and continue.

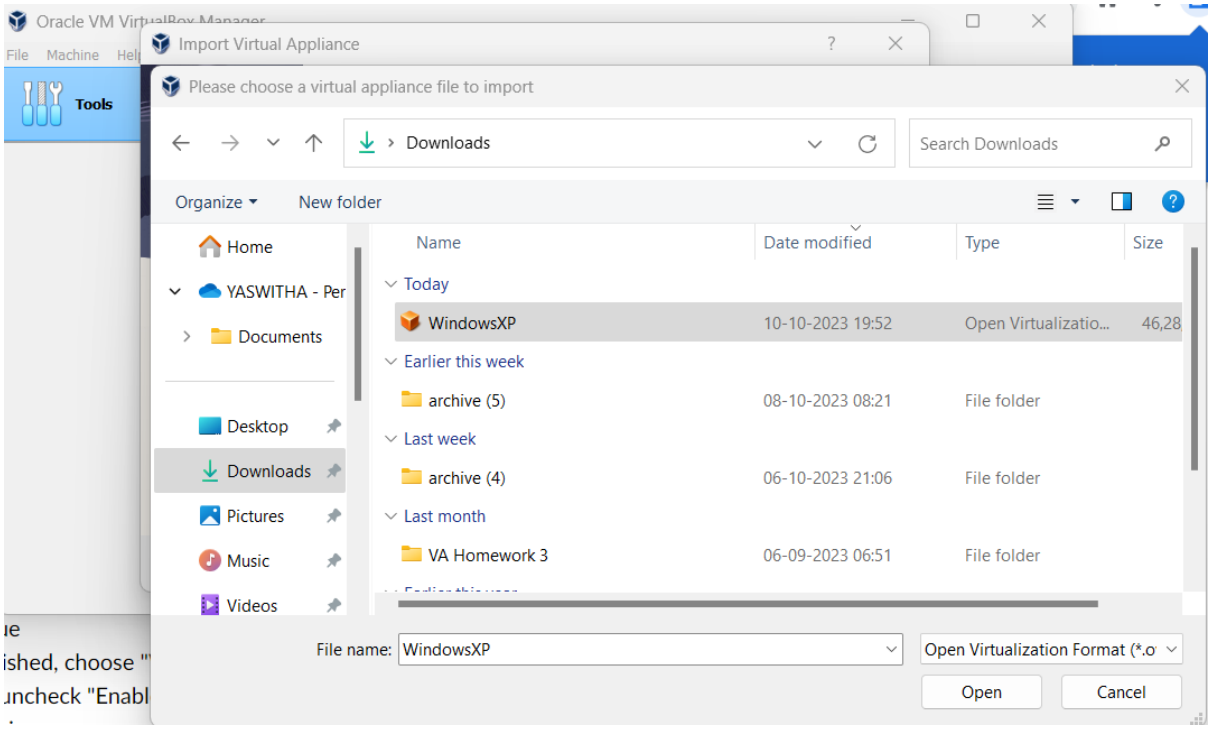

Figure 2: Selecting Downloaded WindowsXP file

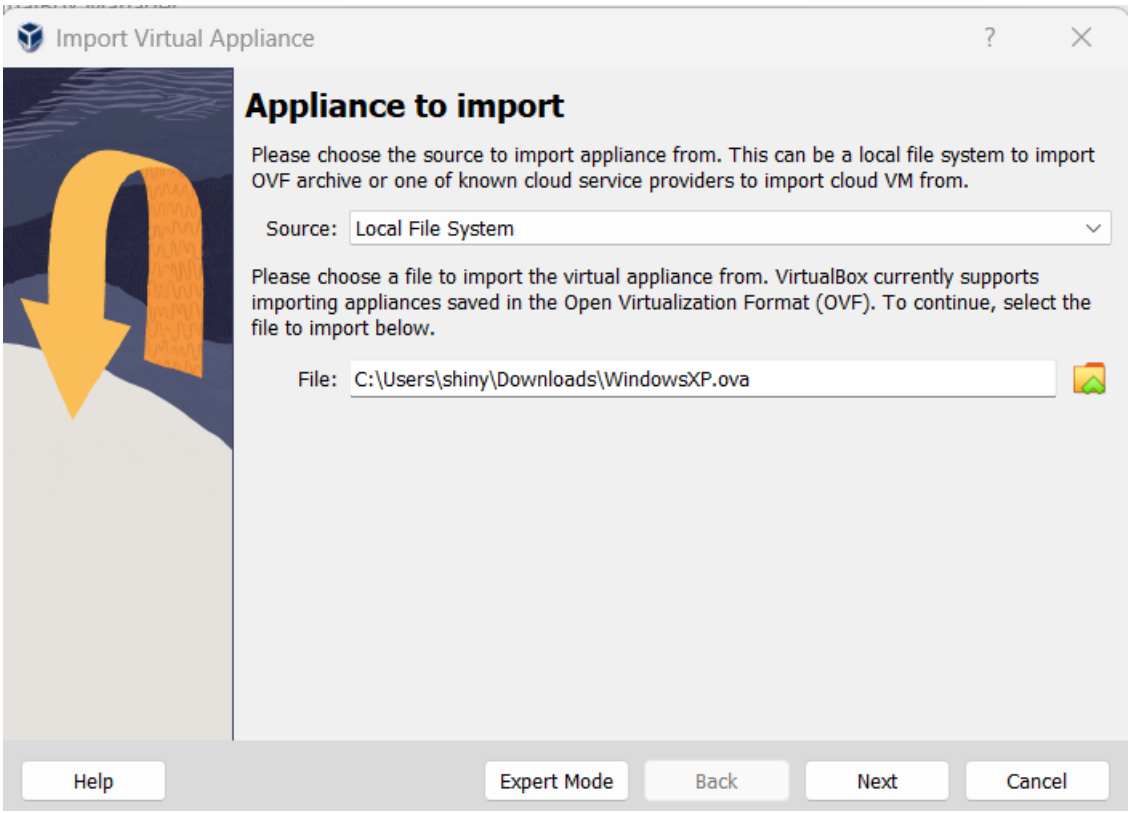

Figure 3: Importing the Appliance

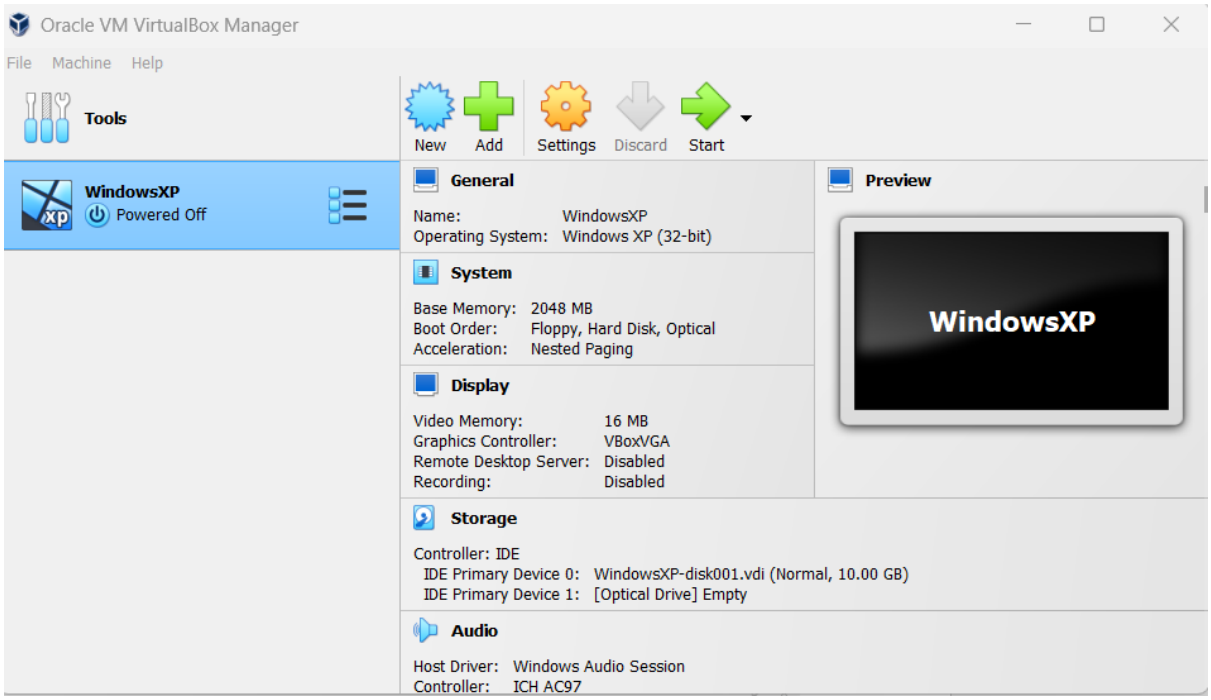

Figure 4: Successfully Imported the appliance WindowsXP

Step 3: After the import process is complete, select 'WindowsXP' from your virtual machine list. Then, navigate to 'Settings,' go to 'Network,' choose 'Adapter 2,' unmark the 'Enable Network Adapter' option, and finally, click 'OK'.

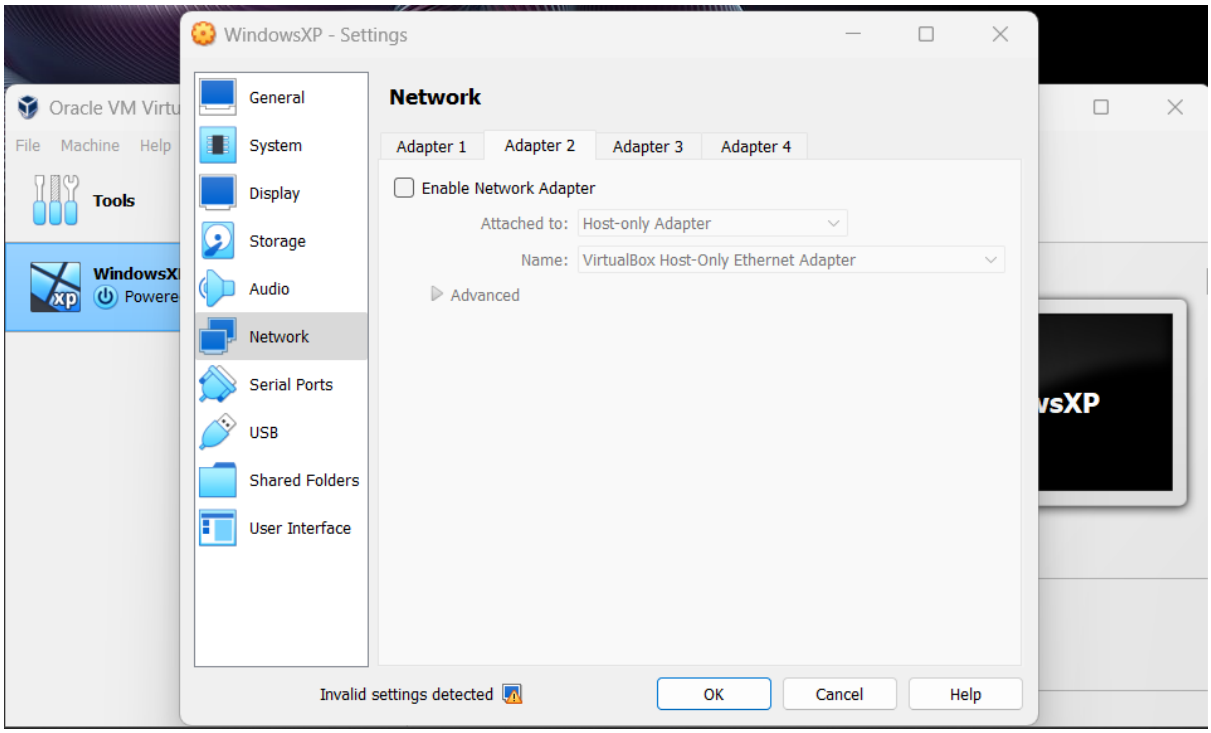

Figure 5: Changed the network settings

Step 4: Started the new virtual machine to perform the task

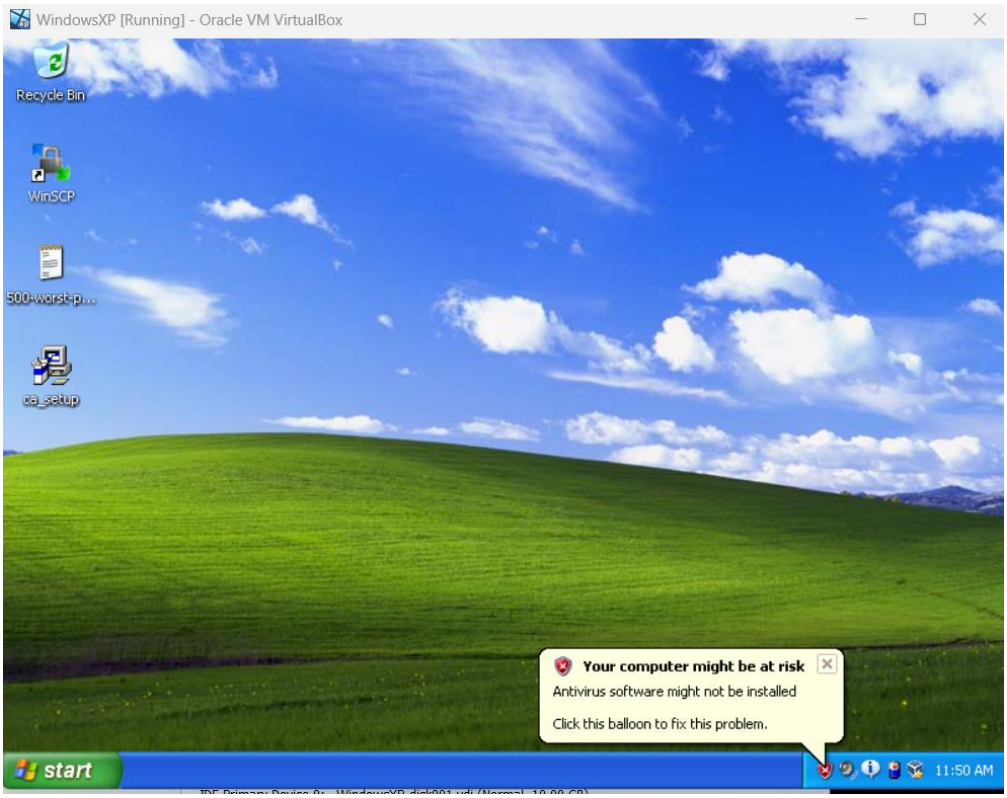

Figure 6: Started the new virtual machine

Step 5: Subsequently, proceed to install Cain & Abel on the freshly set up virtual machine. Locate the file labelled 'ca_setup.exe' on the desktop, double-click it, and adhere to the provided instructions.

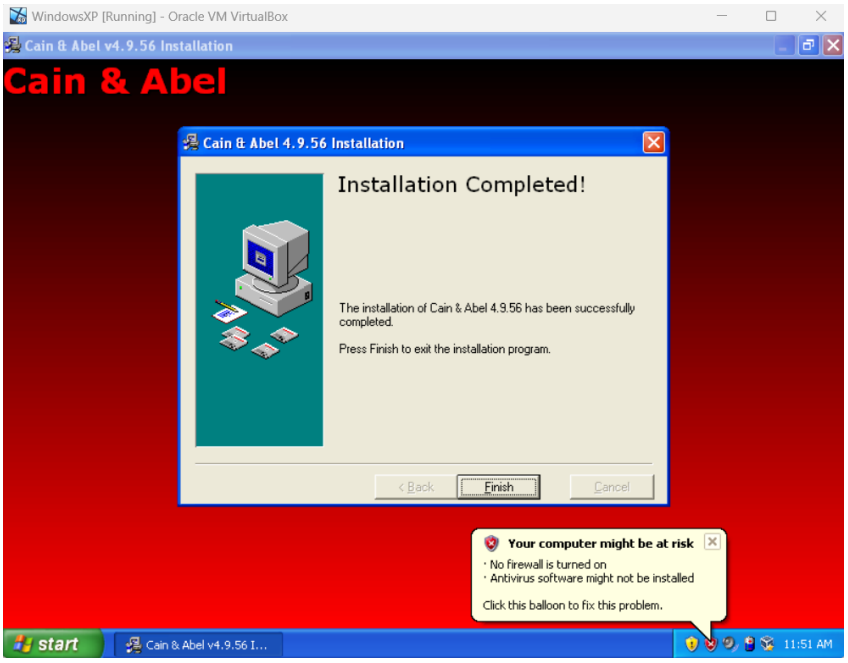

Figure 7: Installed Cain & Abel

Step 6: Next, verify the presence of a compact password dictionary (500-worst-passwords.txt) on the desktop.

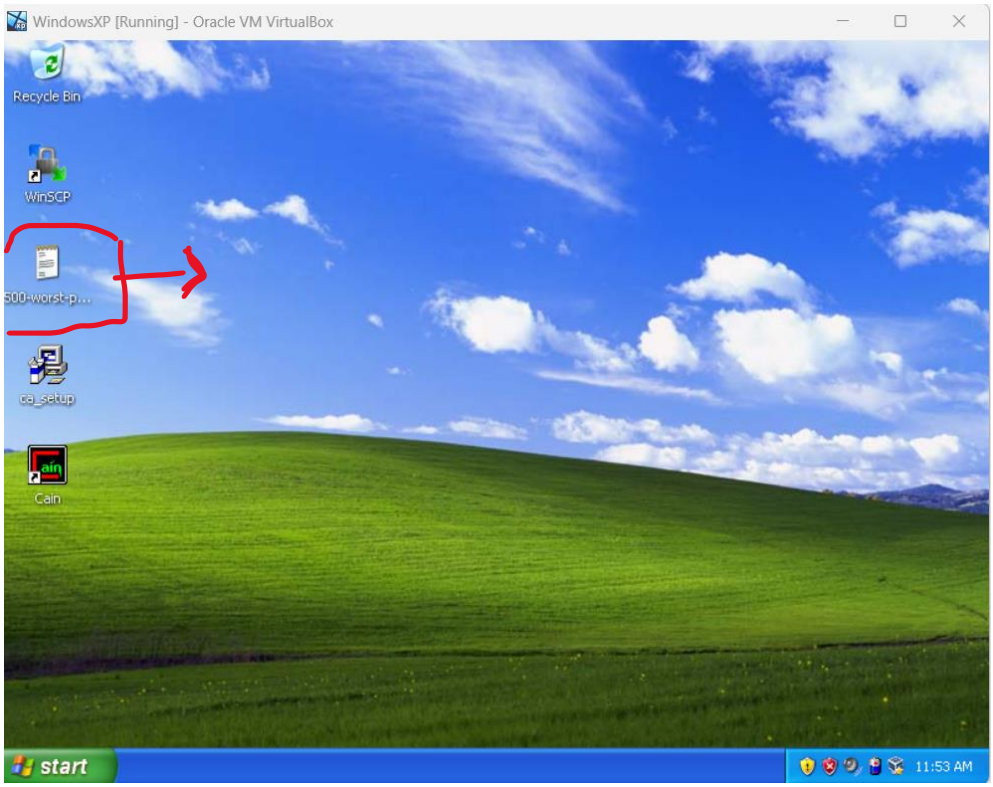

Figure 8: Located 500 worst passwords.txt

Password Cracking (Part 2):

Step 7: In your Virtual Machine, generate three user profiles named test1, test2, and test3. Avoid using personal passwords for any of these accounts. You can establish new profiles through the 'Control Panel.' After creating a user account, proceed to set up its password.

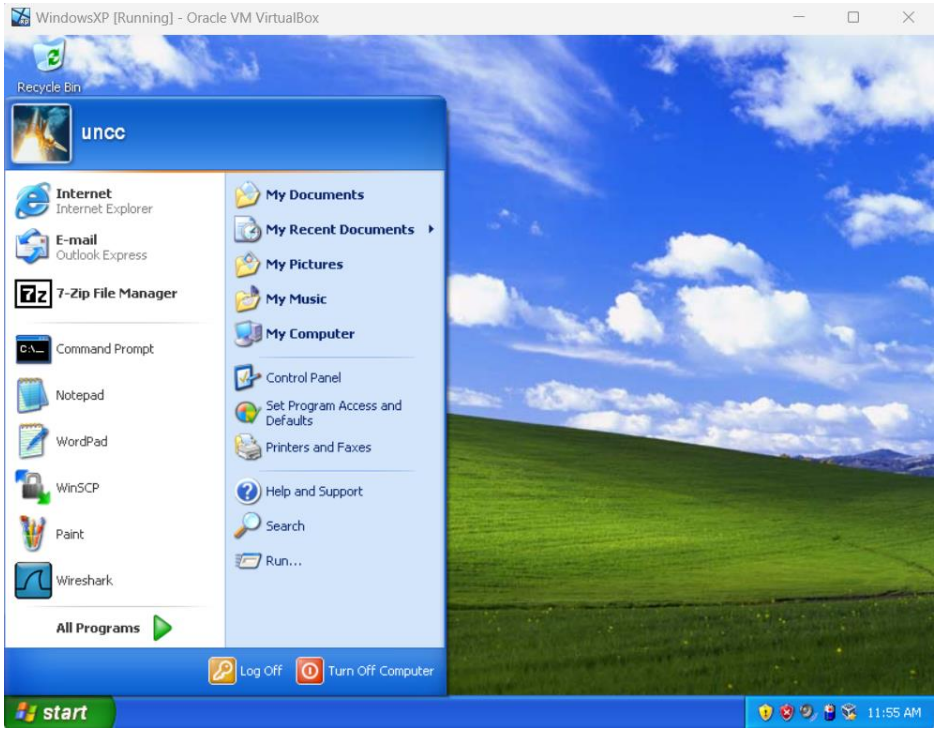

Figure 9: Navigating through control panel

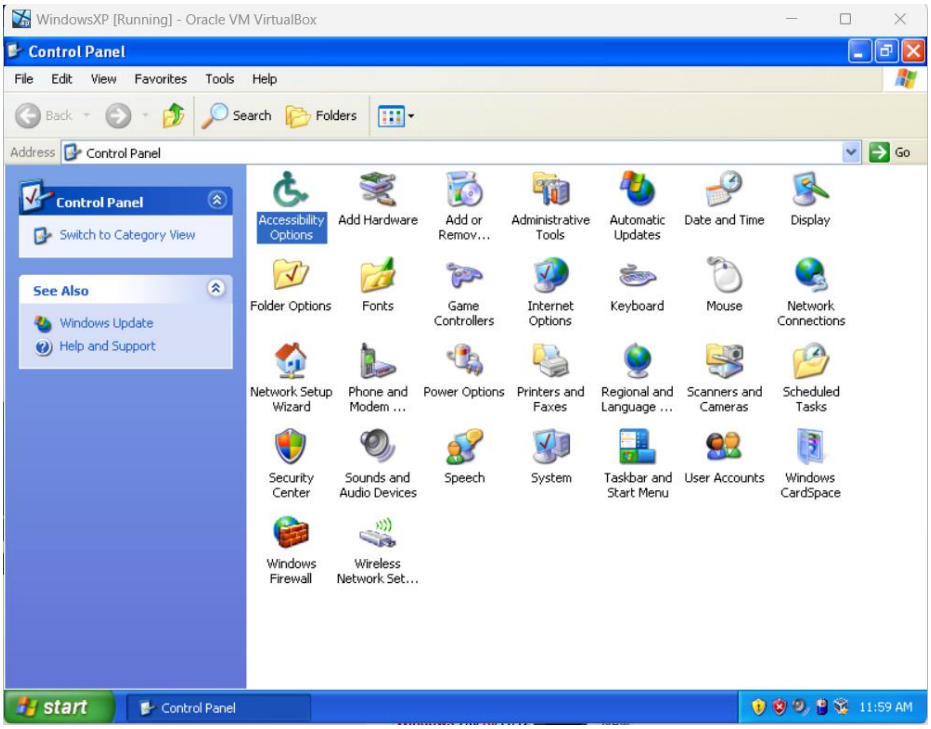

Figure 10: Selecting the user accounts

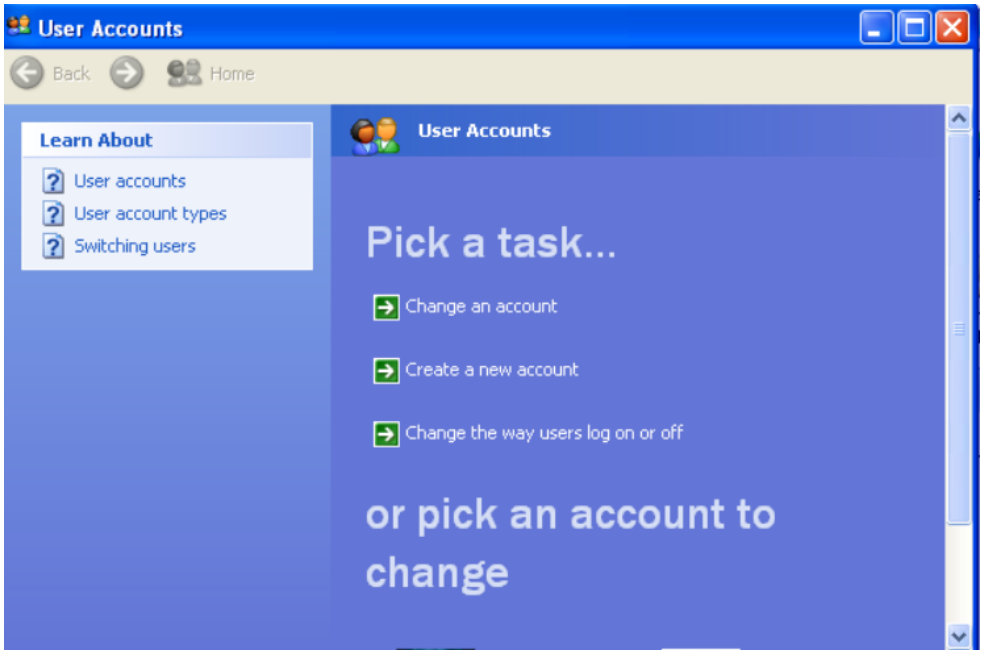

Figure 11: Start creating the user accounts

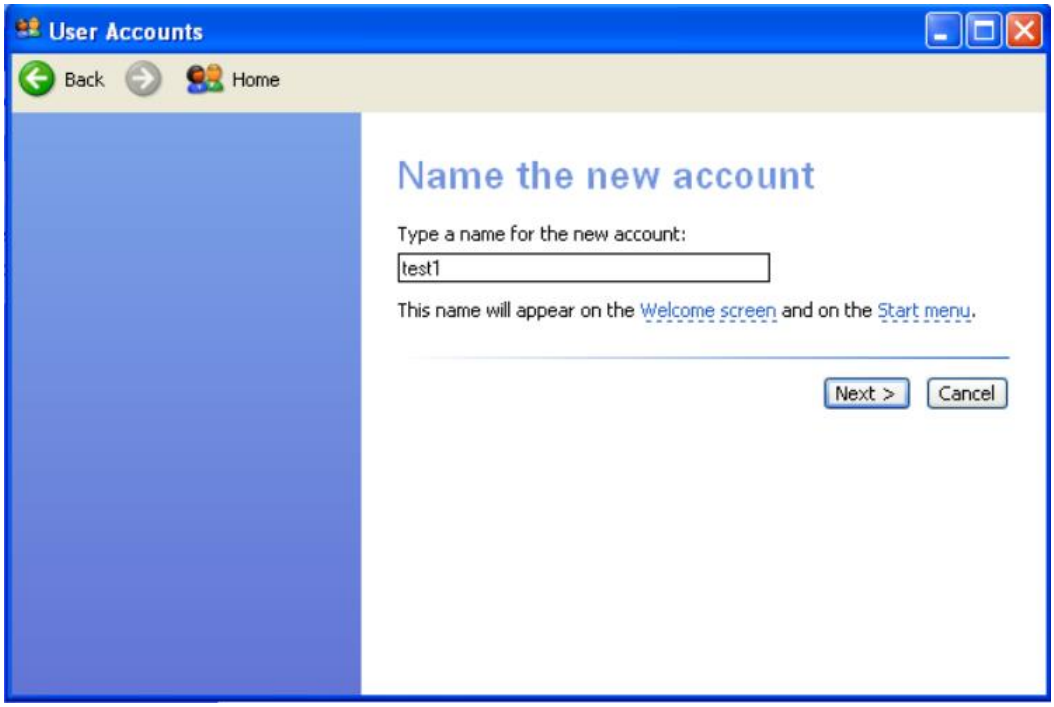

Figure 12: Creating the user account test1

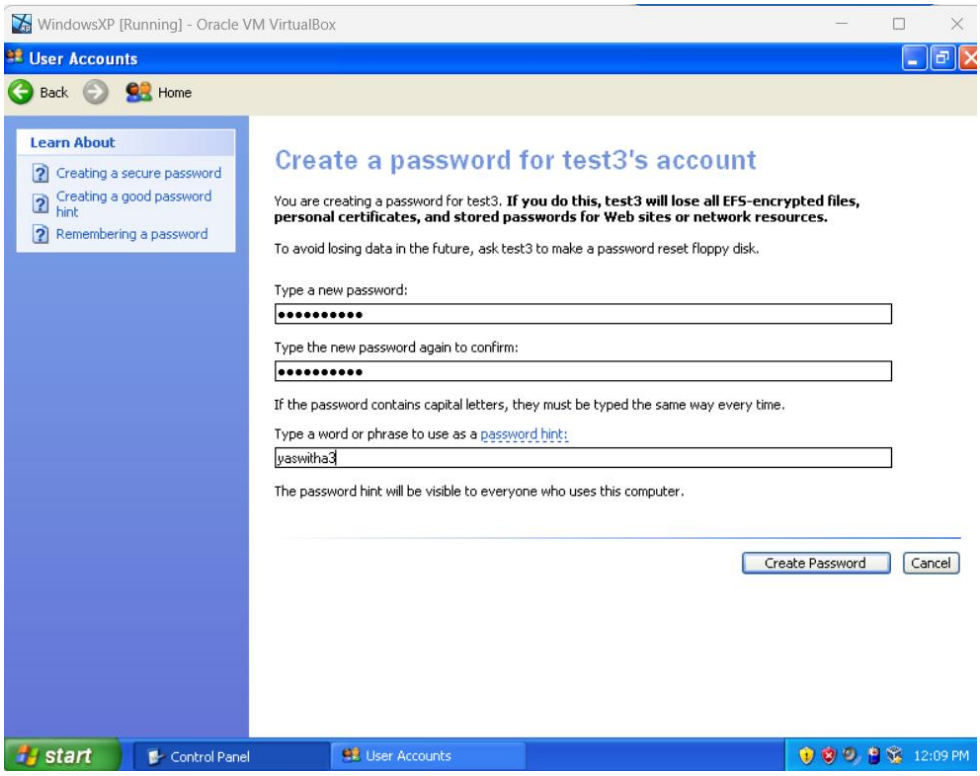

Figure 13: Creating the user account with password for test 3

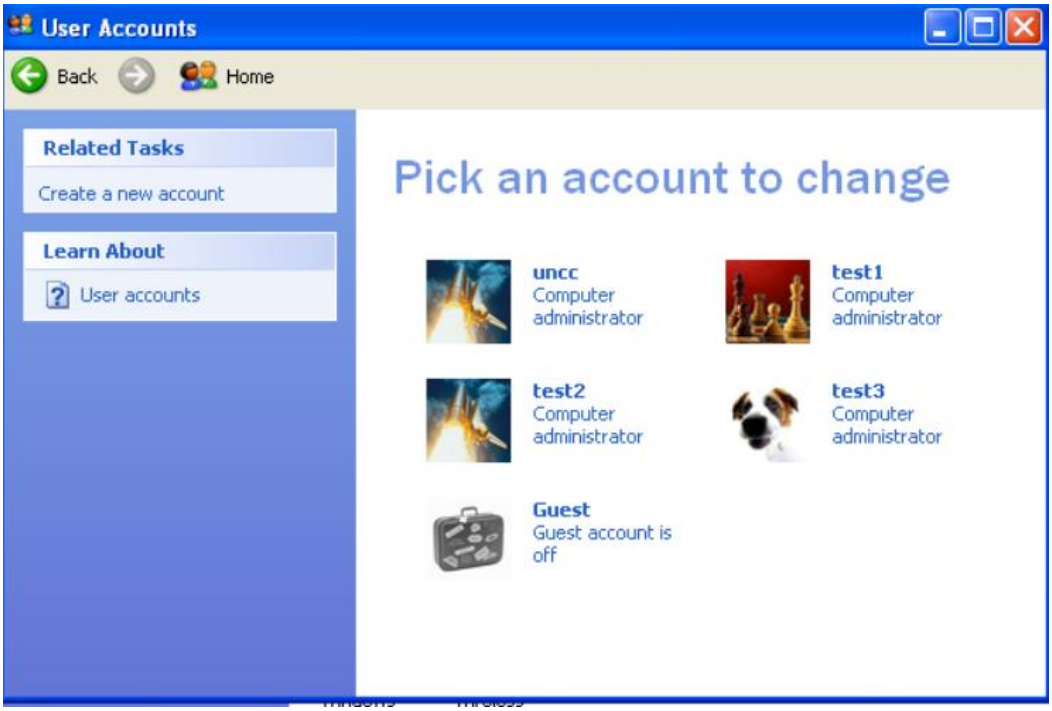

Figure 14: Created all the 3 user accounts

Task 1: Dictionary Attack

Step 8: For this task, you will only require the test1 account. Select a password for test1. Launch Cain & Abel, then access the 'Cracker' tab, and opt for 'LM & NTLM Hashes' from the left-hand column.

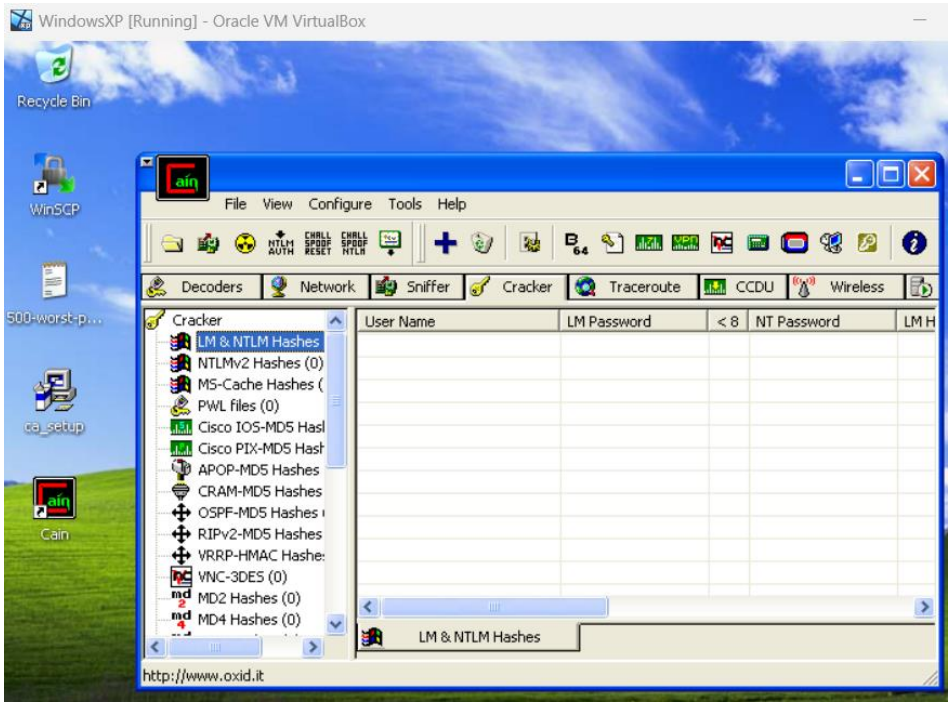

Figure 15: Opened and Selected the LM & NTLM Hashes

Step 9: Next, click on the plus symbol in the taskbar to incorporate NT hashes. Choose 'Import hashes from the local system' and proceed by clicking 'Next'.

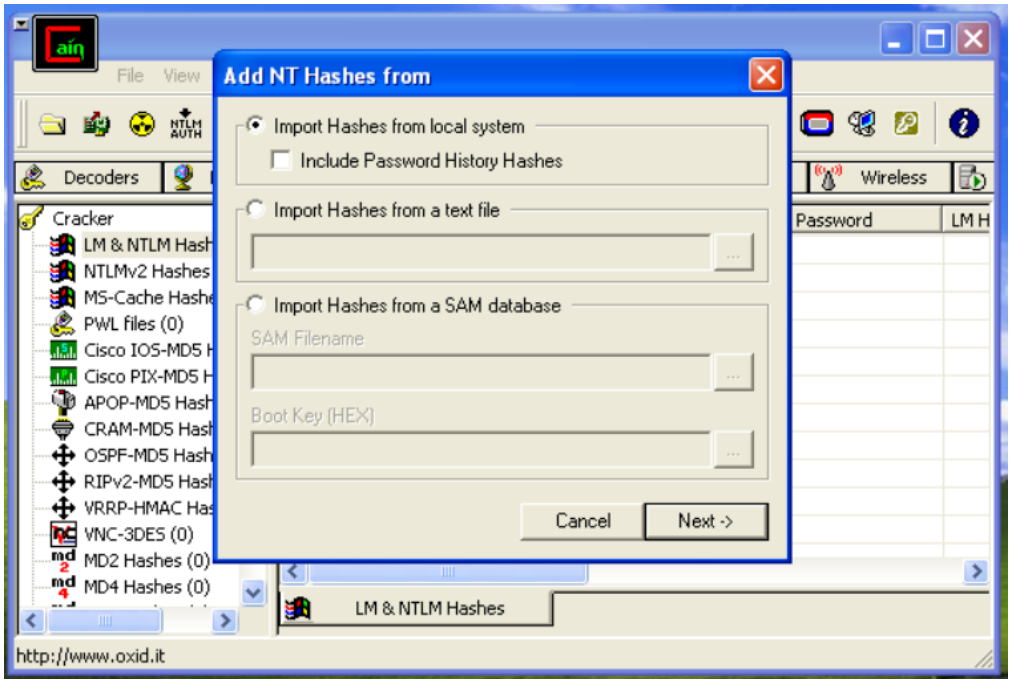

Figure 16: Importing the NT Hashes

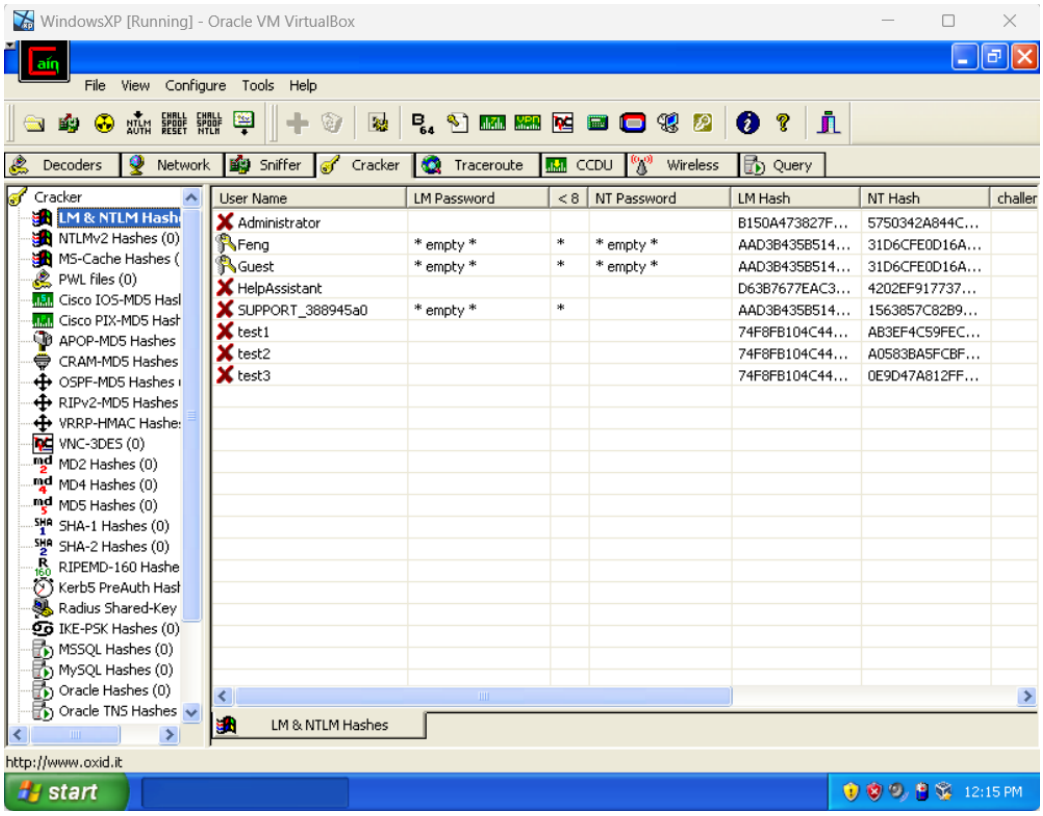

Figure 17: Imported all the NT Hashes

Step 10: Perform a right-click on the 'test1' account, then choose 'Dictionary Attack.' opt for 'NTLM hashes' from the submenu.

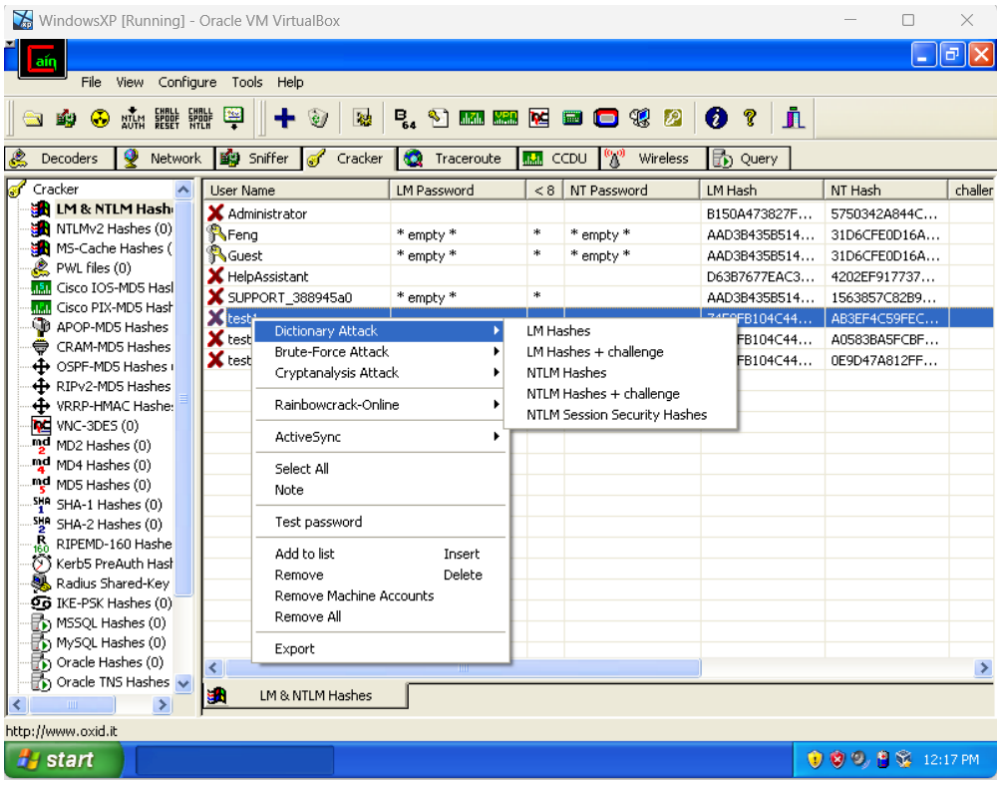

Figure 18: Selecting Dictionary attack using NTLM Hashes

Step 11: Subsequently, right-click within the dictionary section, and choose 'Add to list' to incorporate dictionaries. Go to the Desktop and pick '500-worst-passwords.txt'.

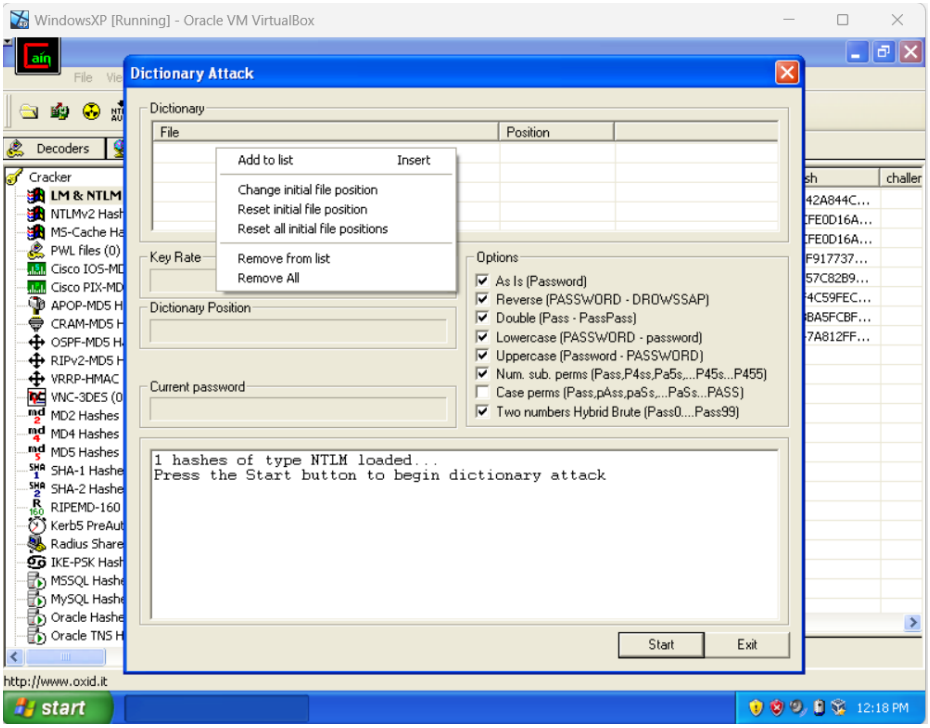

Figure 19: Adding 500 worst passwords to the list

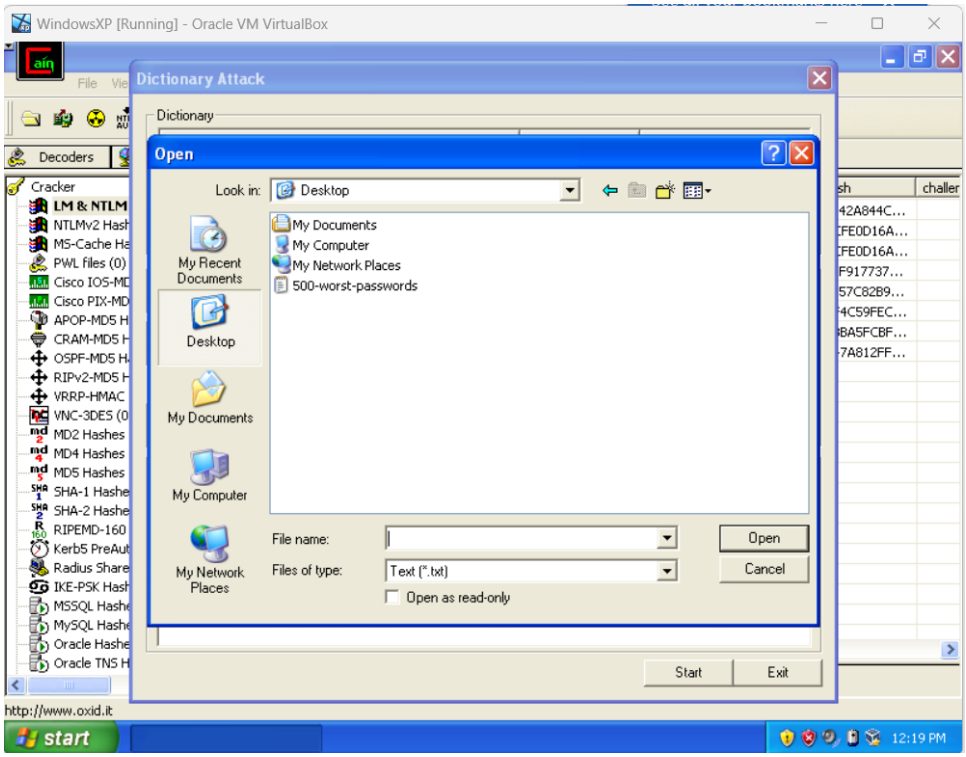

Figure 20: Selecting from the location

Step 12: Click on 'Start' to start the attack. Discover the password you entered.

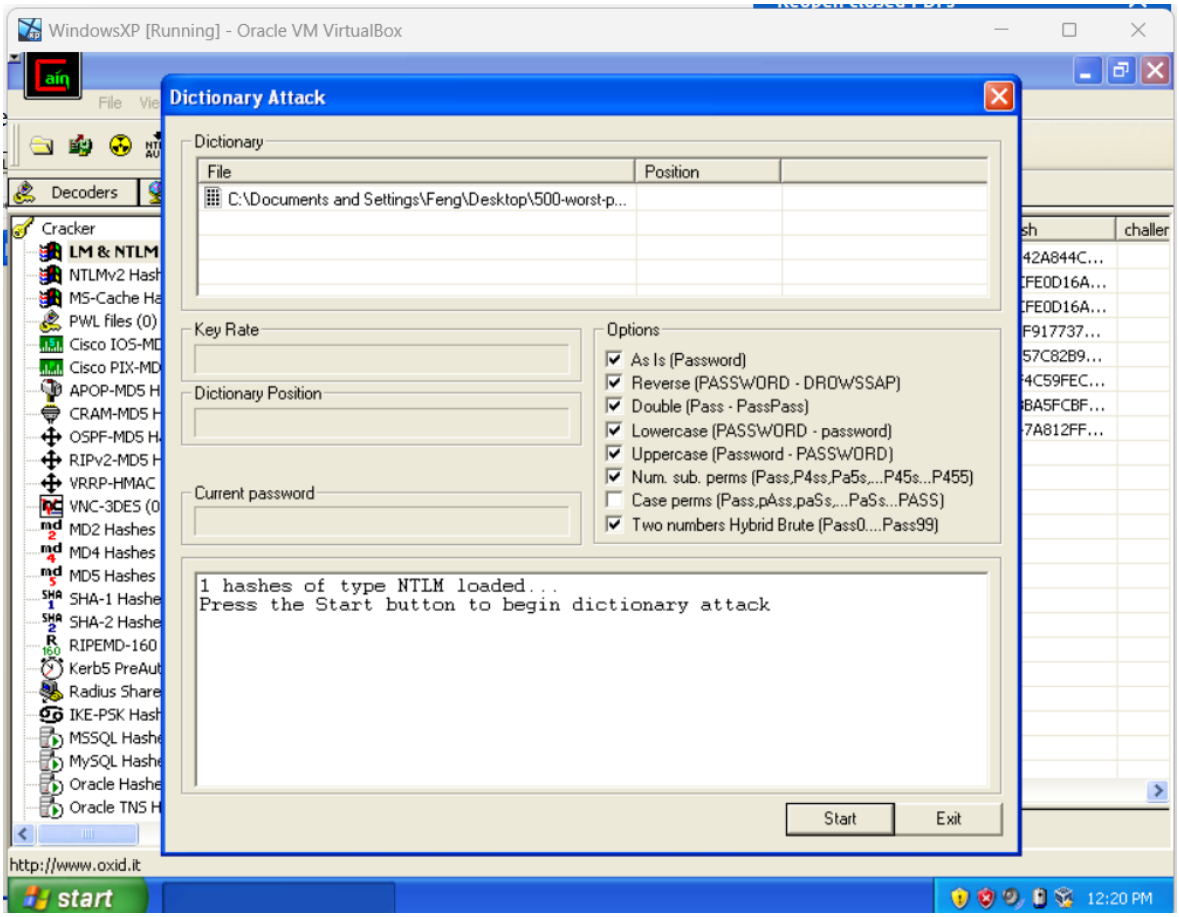

Figure 21: Starting the dictionary attack

Answer Task 1: Attempting to use a dictionary attack with the Cain application to break the password for "test1."

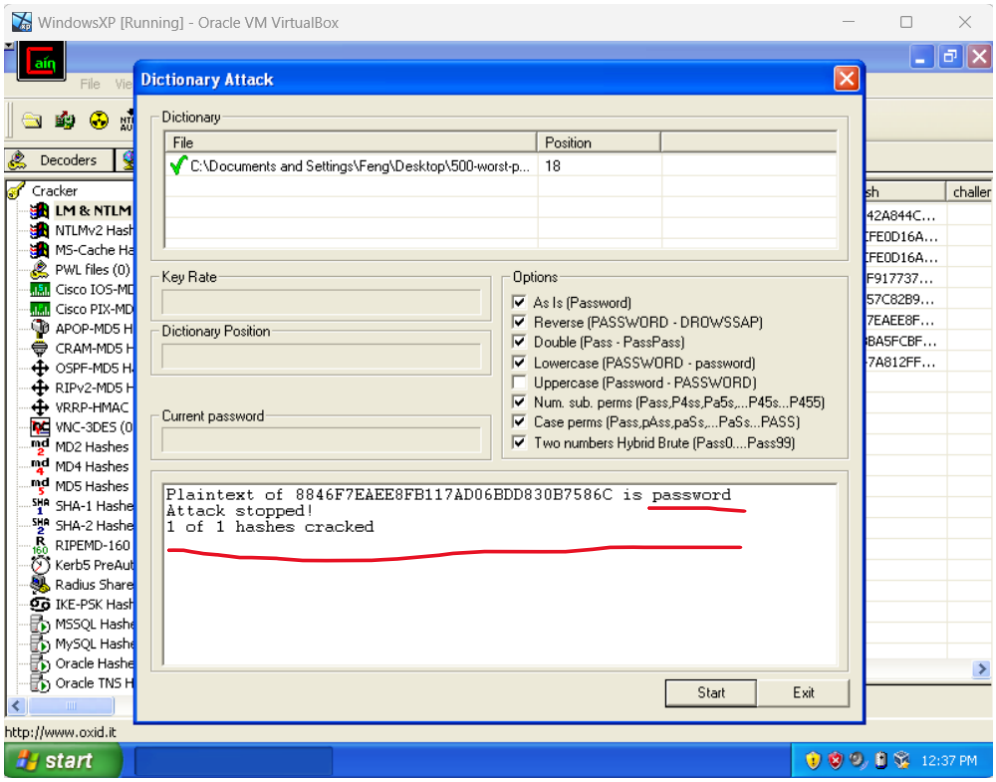

Figure 22: Cracking the user test 1 user's password using dictionary attack – with 500 worst password list.

***Step 13*:** In the window, you will notice that the password has been successfully deciphered through a dictionary attack. The password is 'password'.

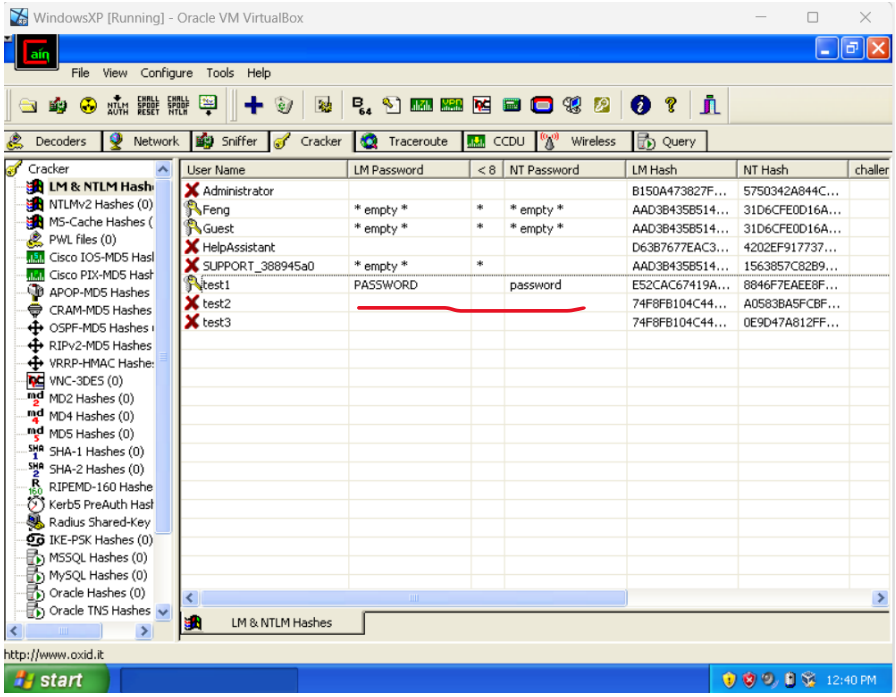

Figure 23: Obtained password through dictionary attack

Task 2: Brute-Force Attack

Step 14: For this task, you'll require all three accounts: test1, test2, and test3. Generate one password of each type listed in the table below for each respective account. Please adhere to the precise specifications for each password type as specified in the table.

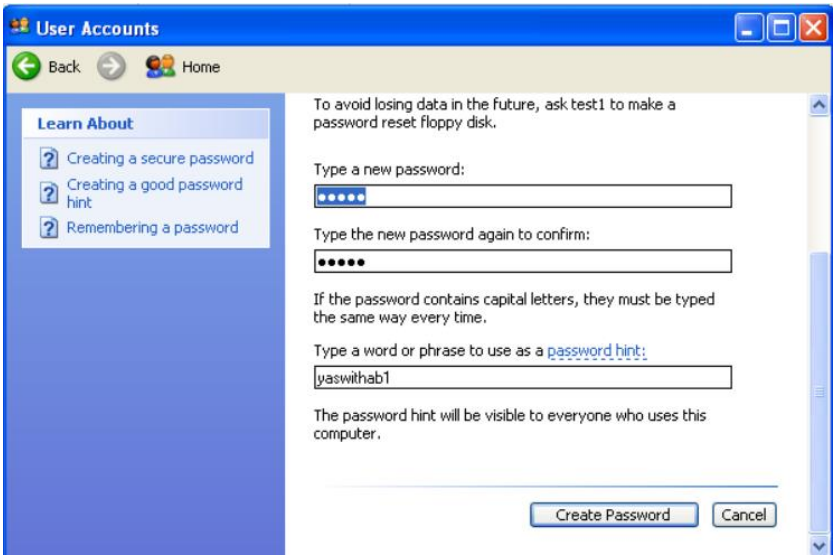

Figure 24: Setting the passwords according to the requirement

Step 15: Record the selected password for each type in the provided table. Right-click on the relevant account, for example, 'test1,' and opt for 'Brute-force Attack.' Select 'NTLM hashes' from the submenu. Ensure that you set the password length correctly. Failing to do so might prolong the process significantly. Adjust the password length as needed and choose the appropriate character set. Repeat this procedure for all three passwords.

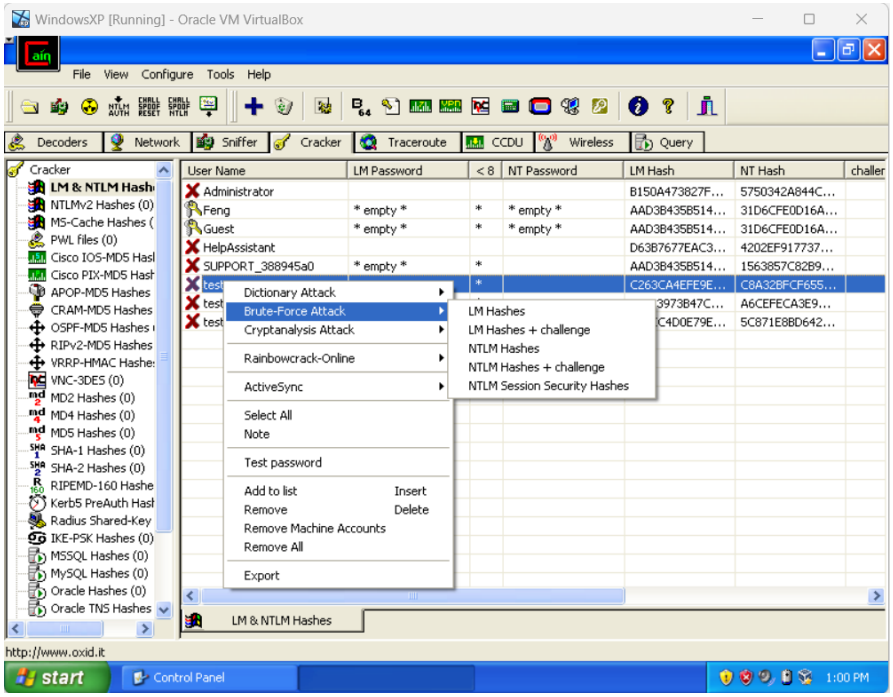

Figure 25: Selecting the Brute-force attack with NTLM Hashing

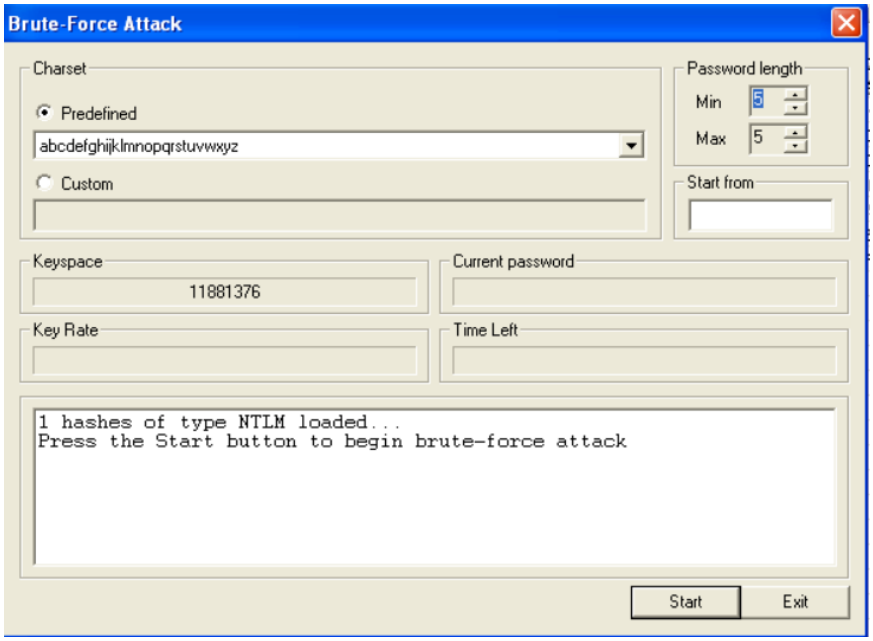

Figure 26: Selecting charset type for the attack

Step 16: Fill the following table with the details based on your activity.

	Password Description	Chosen Password	Charset	Time Taken
1	Lowercase letters only (Length 5)	Test1: **yashu** Test 2: **shiny** Test 3: **saiat**	abcdefghijklmnopqrstuvwxyz	Test 1: < 1 sec Test 2: < 1 sec Test 3: < 1sec
2	Lowercase, uppercase letters and numbers from 0 to 9 (length 5)	Test 1: **Y05hu** Test 2: **sH17y** Test 3: **S01AT**	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789	Test 1: **16.56 sec** Test 2: **21.81 sec** Test 3: **36.28 sec**
3	Lowercase, uppercase letters, numbers from 0 to 9 and symbols (length 5)	Test1:**Y@5hu** Test 2: **sH!7y** Test 3: **s*1A$**	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@($	Test 1: **41.35 sec** Test 2: **48.1 sec** Test 3: **2Min7sec**

Table 1: Table containing the details of chosen password, password type and charset with time taken to crack it

Case 1: Lower Letters only with Length 5

Test1: Successfully used brute force to discover the password for 'test1,' which is **'yashu'**.

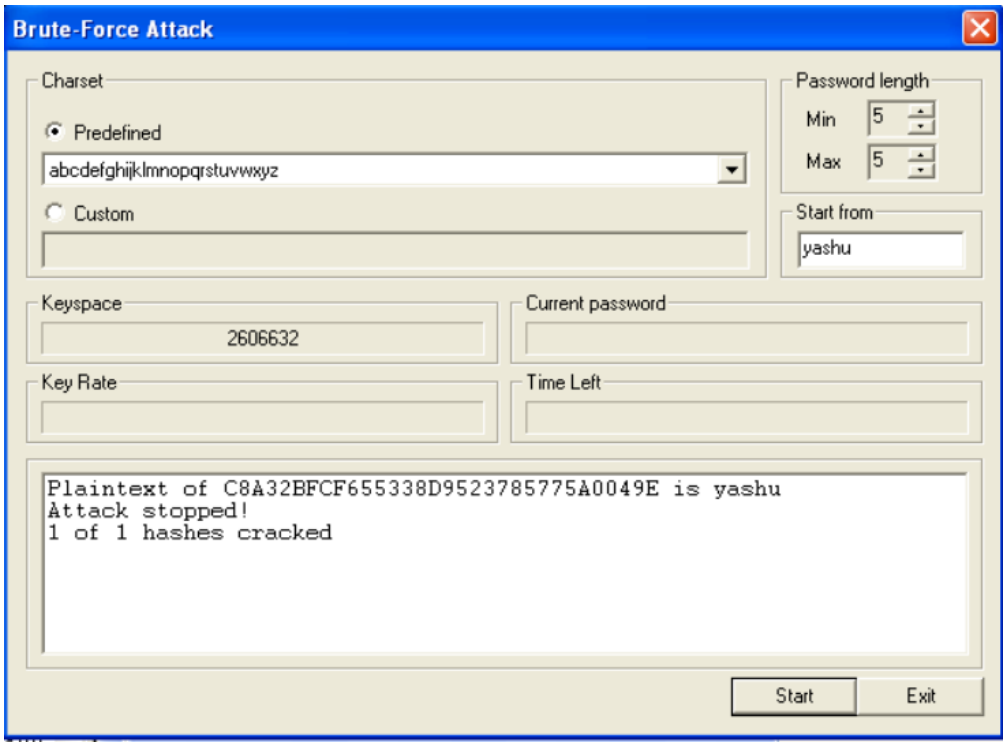

Figure 27: Password cracked for Lower case letters with length 5 for test 1-yashu

Test 2: Successfully used brute force to discover the password for 'test 2,' which is **'shiny'**.

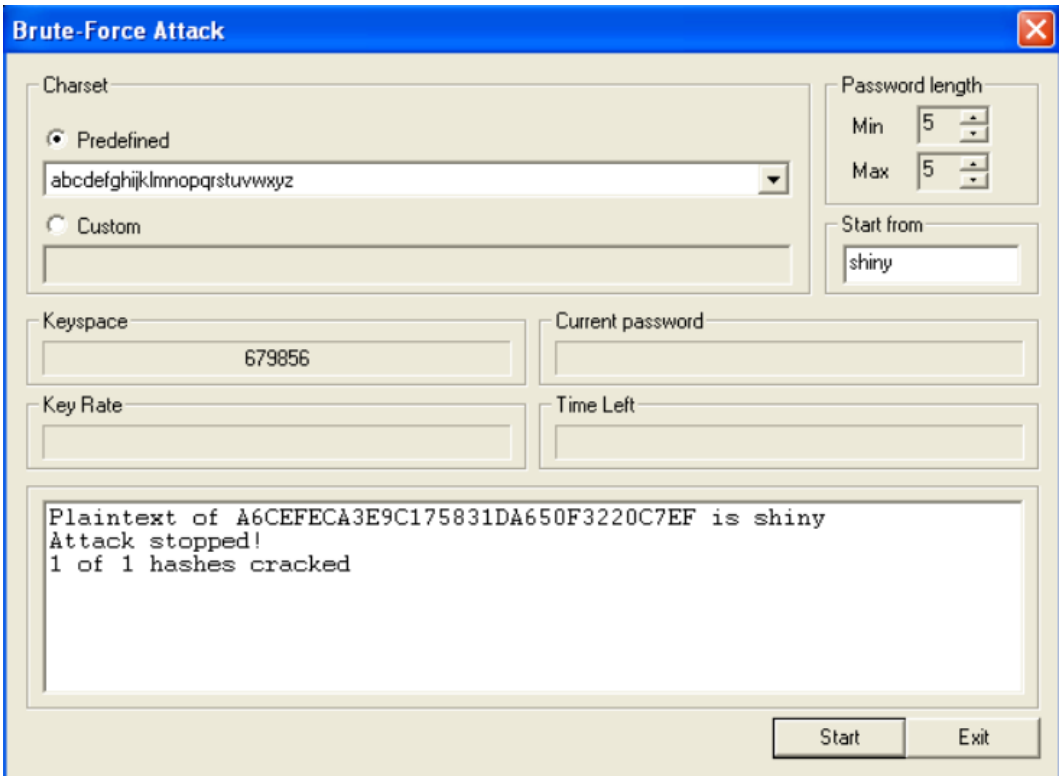

Figure 28: Password cracked for Lower case letters with length 5 for test 2-shiny

Test 3: Successfully used brute force to discover the password for 'test 3,' which is **'saiat'**.

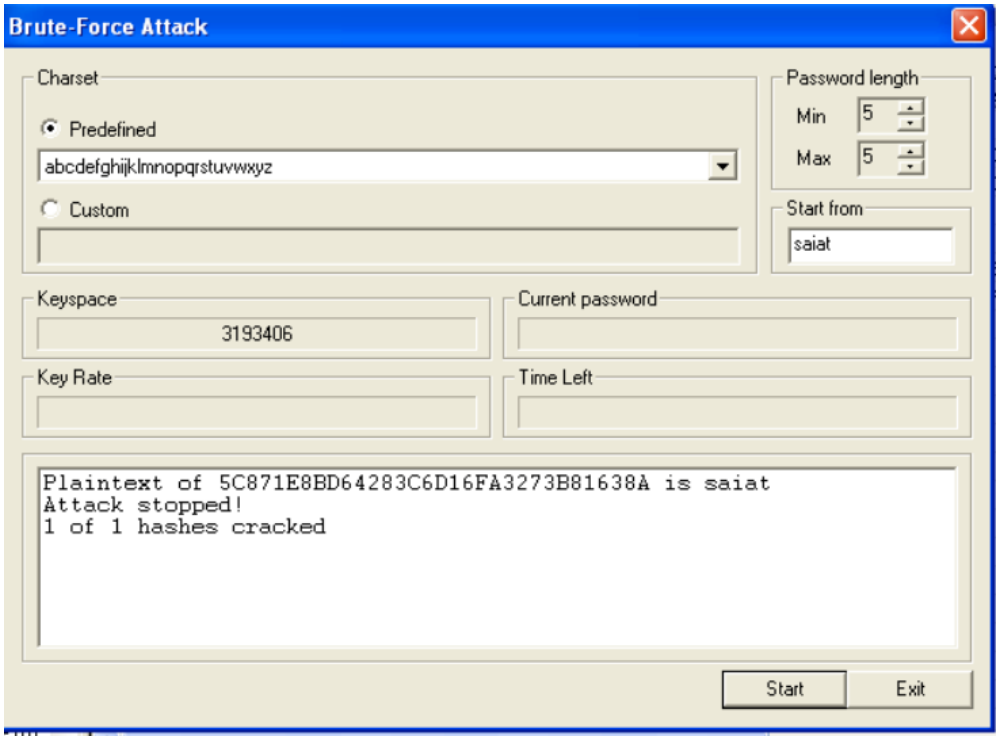

Figure 29: Password cracked for Lower case letters with length 5 for test 3-saiat

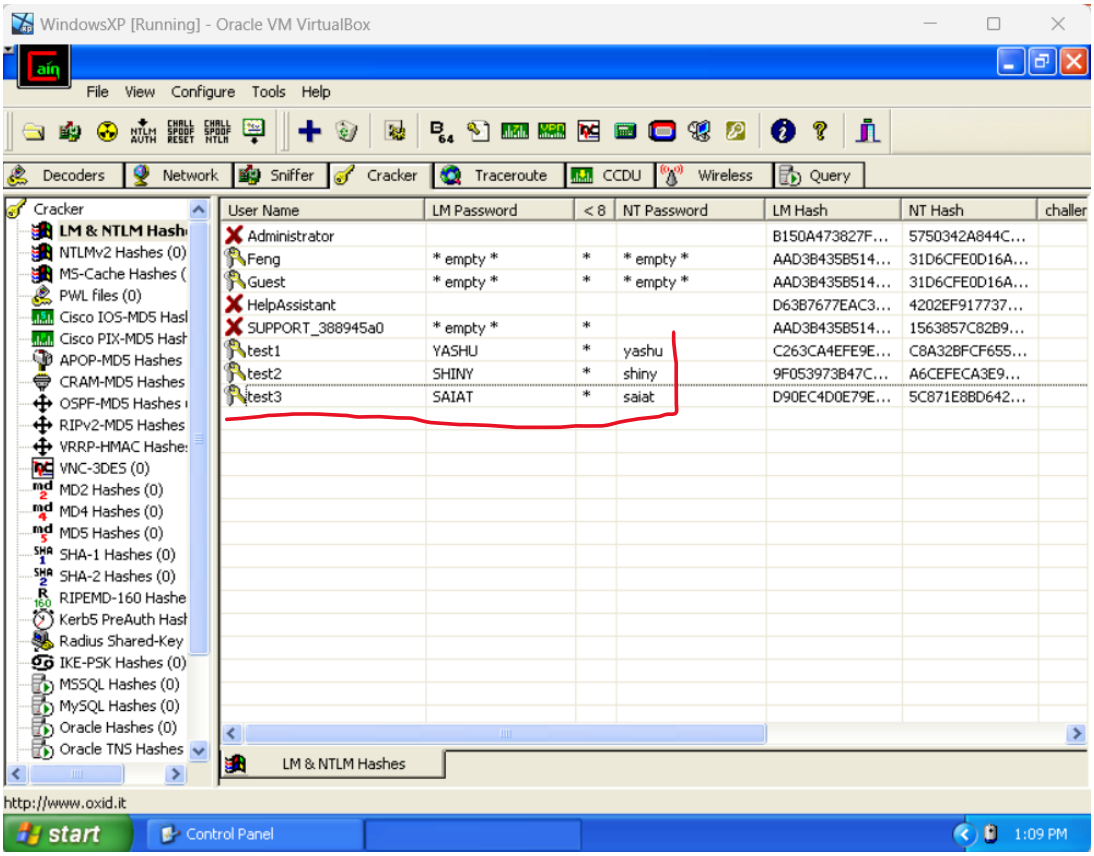

Figure 30: Cracked all the passwords of the test 1, test 2, test 3 using brute force attack

Case 2: Lowercase, uppercase letters & numbers from 0 to 9 with length 5

Test1: Successfully used brute force to discover password for 'test1, i.e.,**'Y05hu'** in **16.56 sec**

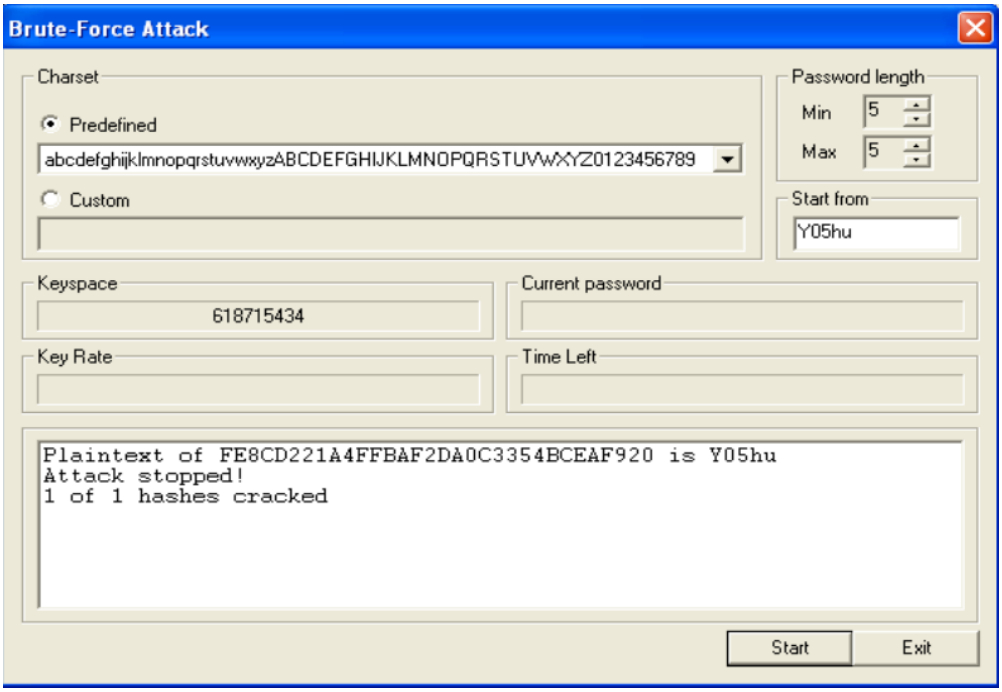

Figure 31: Password cracked for Lower, upper and numbers case with length 5 for test 1

Test2: Successfully used brute force to discover password for 'test 2, i.e., **'sH17y'** in **21.81sec**

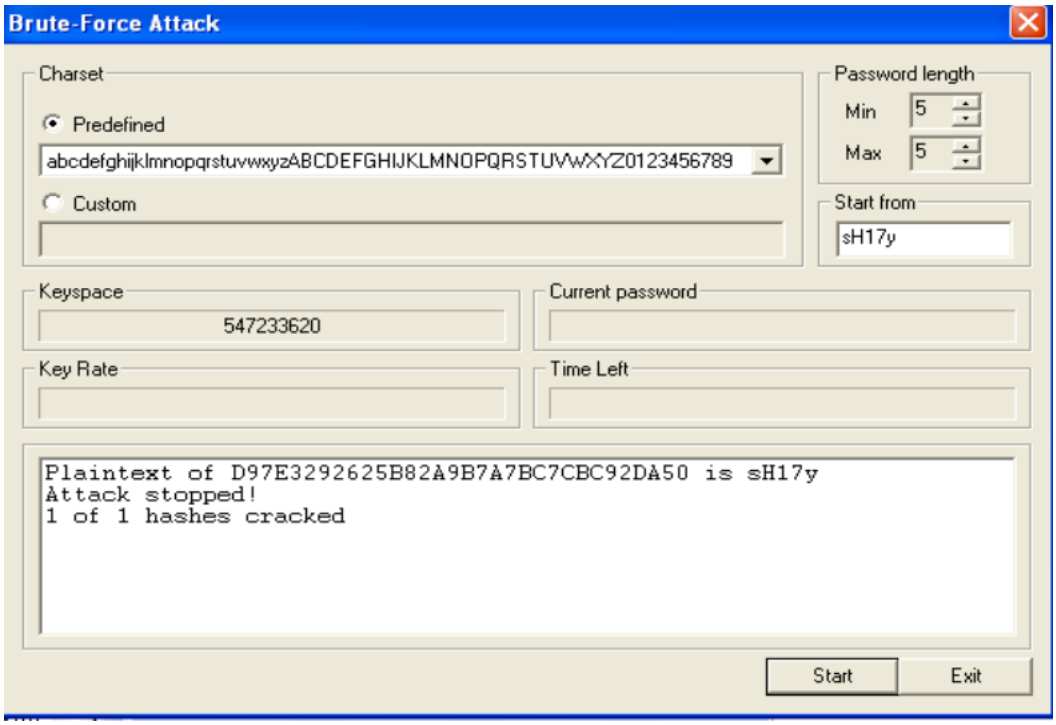

Figure 32: Password cracked for Lower, upper and numbers case with length 5 for test 2

Test 3: Successfully used brute force to discover password for 'test3, i.e.,**'s01AT'** in **36.28 sec**

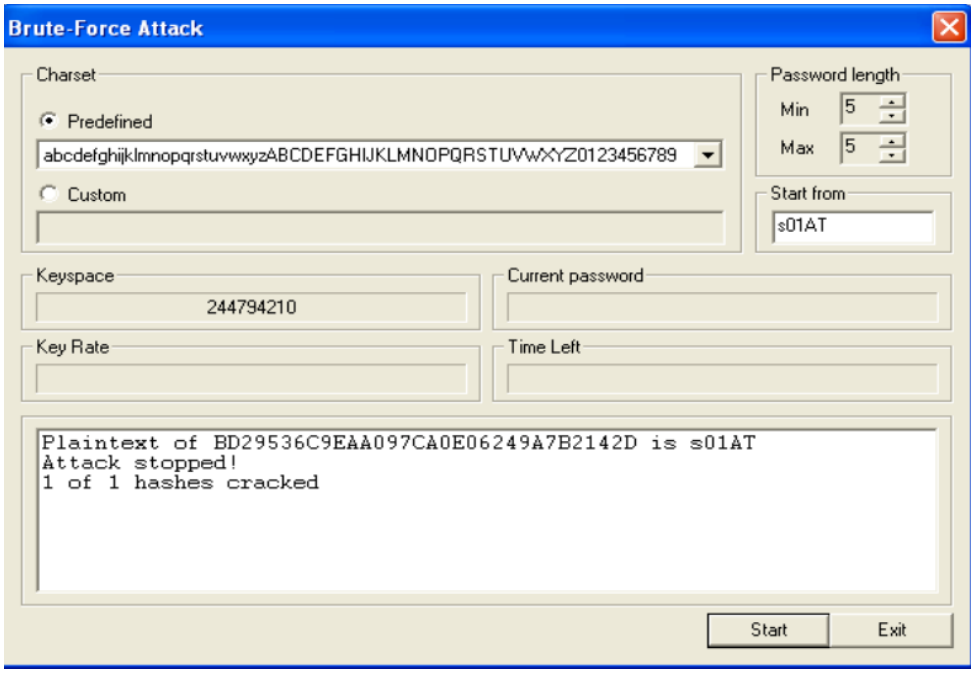

Figure 33: Password cracked for Lower, upper and numbers case with length 5 for test 3

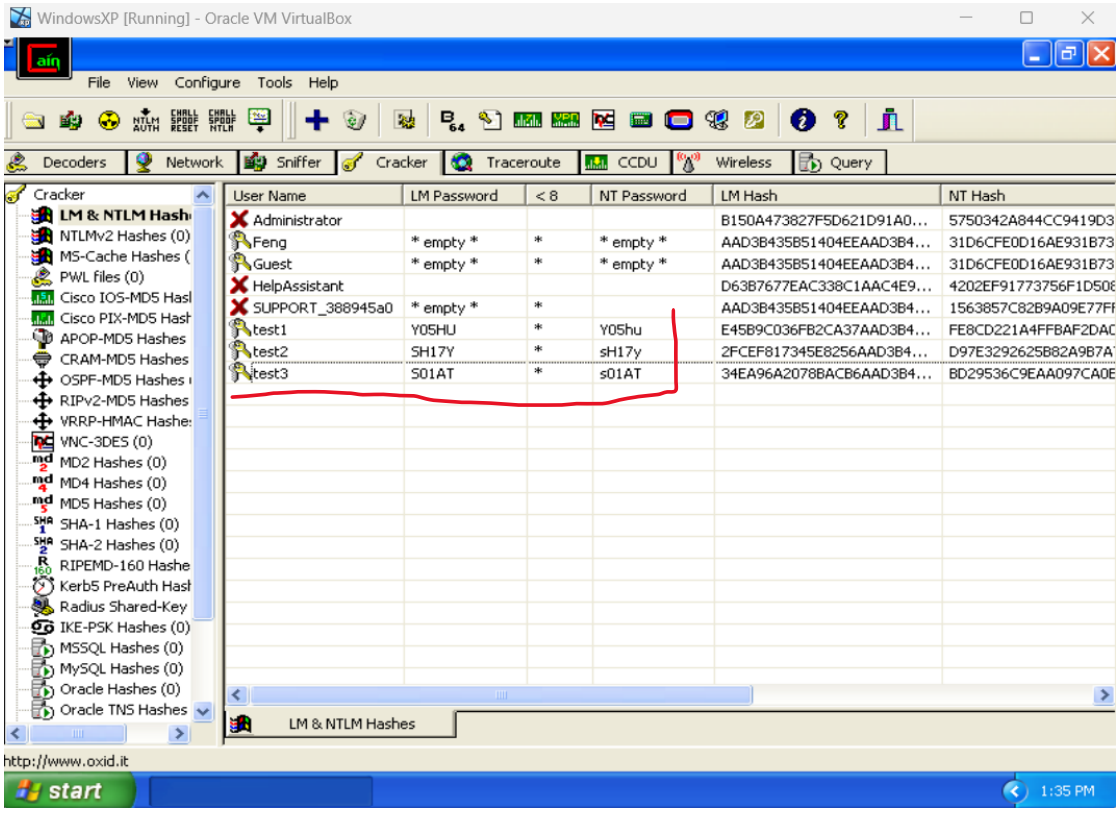

Figure 34: Cracked all the passwords of the test 1, test 2, test 3 using brute force attack

Case 3: Lowercase, uppercase letters & numbers from 0 to 9 and symbols with length 5

Test1: Successfully used brute force to discover password for test1 i.e.,**'Y@5hu'** in **41.35 sec**

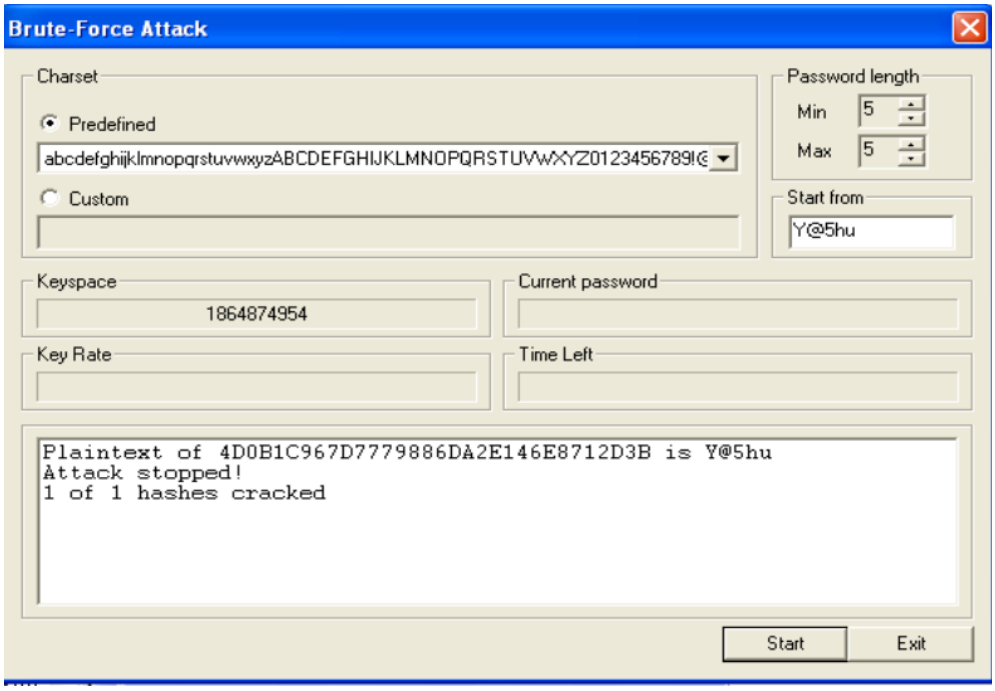

Figure 35: Password cracked for Lower, upper, numbers and symbol case for test 1

Test2: Successfully used brute force to discover password for test2 i.e.,**'sH!7y**in **48.1 sec**

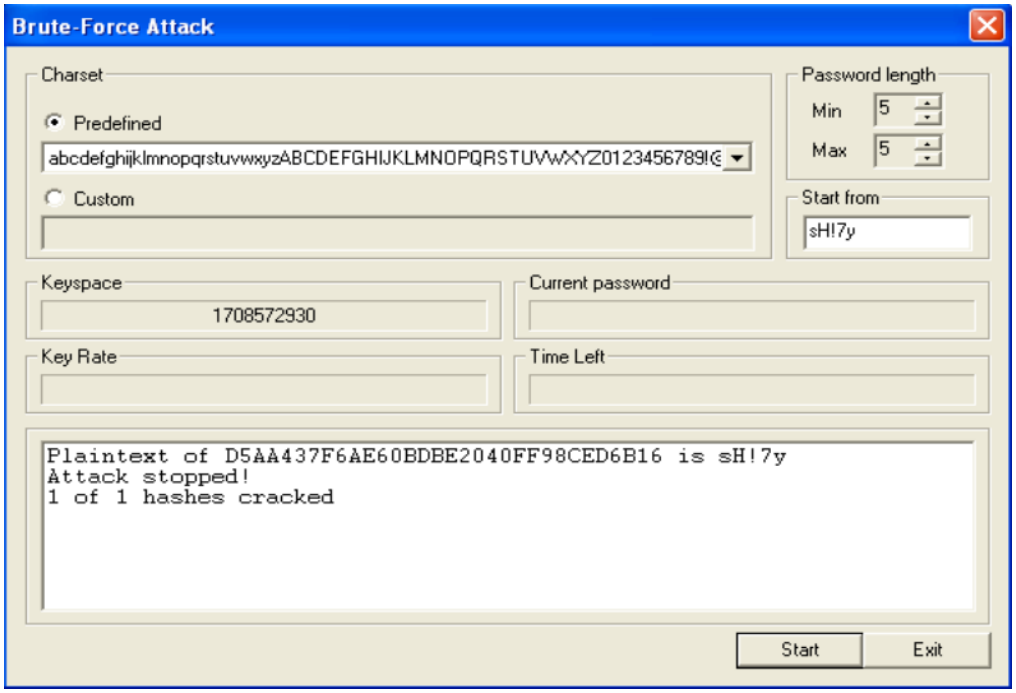

Figure 36: Password cracked for Lower, upper, numbers and symbol case for test 2

Test 3: Successfully used brute force to discover password for test3 i.e., **'s*1A$'** in **2Min7sec**

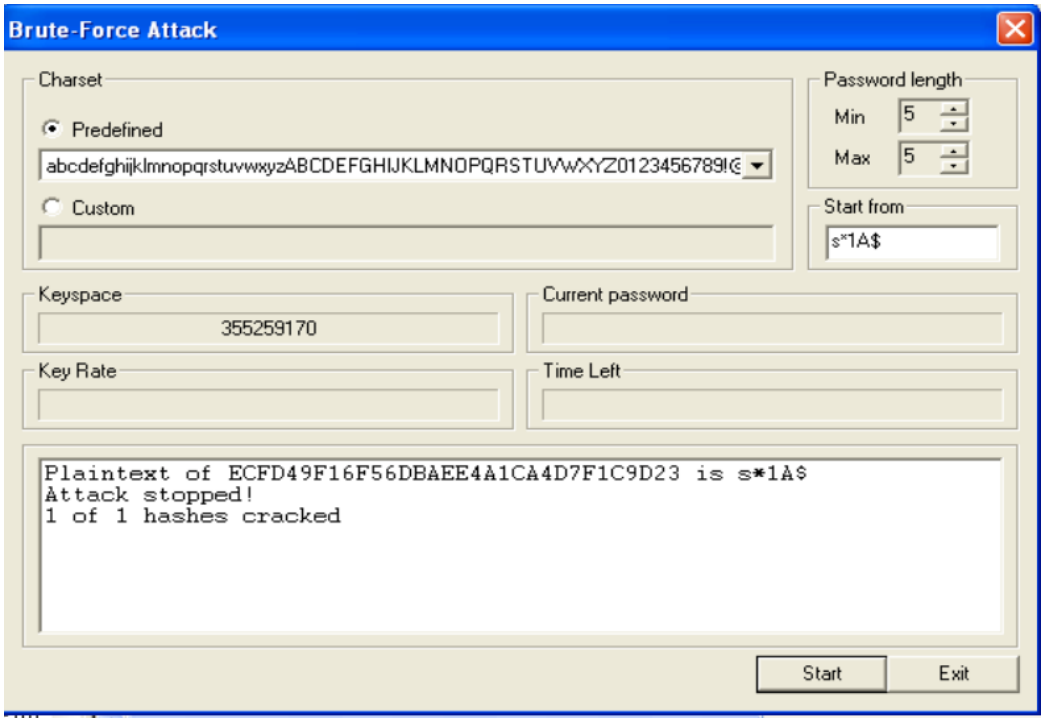

Figure 37: Password cracked for Lower, upper, numbers and symbol case for test 3

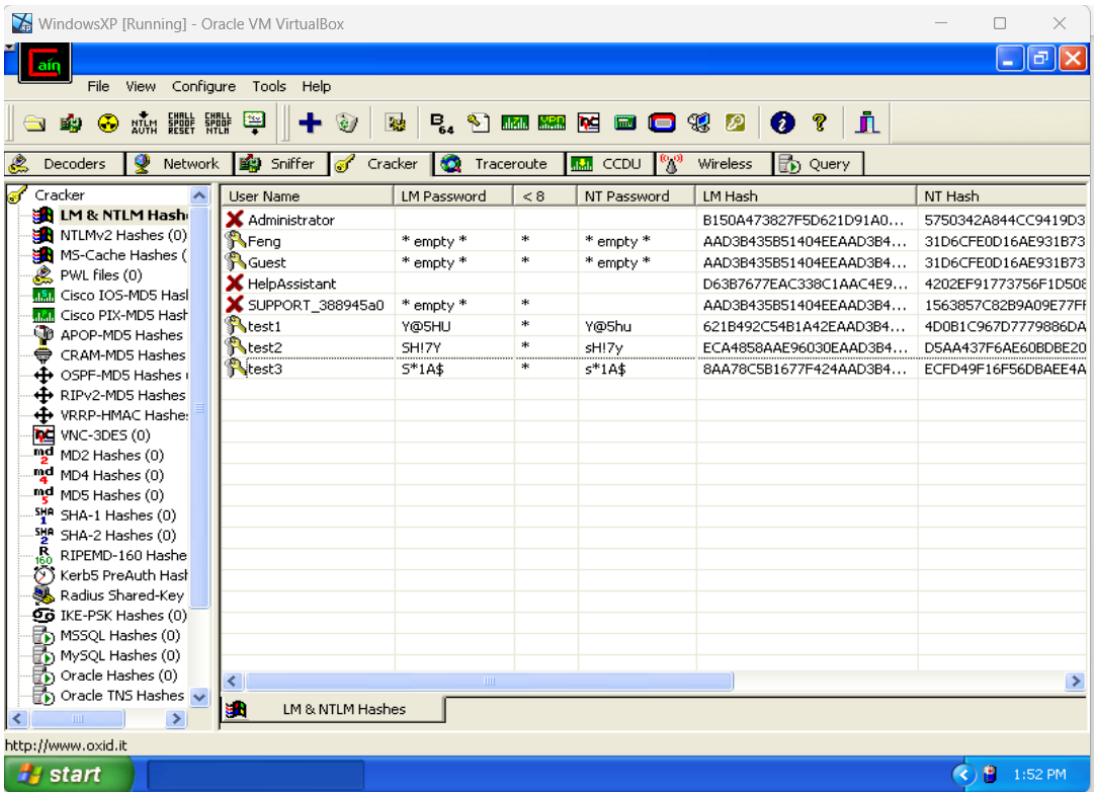

Figure 38: Cracked all the passwords of the test 1, test 2, test 3 using brute force attack

TASK 3: When you created passwords for the brute force attack, would Cain & Abel have finished faster if your password didn't include all the character types in the password description? So, for example if the description said, "lower and uppercase letters", and if your chosen password was "aaa", would Cain and Abel have discovered it faster than if you had chosen "aBC"? Remember that in real scenarios, if you were trying to recover a password using a tool like Cain & Abel, you would not know what the password was, only what the password space was!

Answer:

With my system configuration, the estimated cracking time considering case 1, as provided by the Cain & Abel application, is approximately 1 second for all three test accounts. Considering case 2, it takes around 1 minute on maximum for all three test accounts, and for scenario 3, it takes approximately 2 minutes on the maximum settings for all three test accounts. As observed in Table 1 on page 15, the time it takes to crack a password increases when the password contains a more complex character set. The application can attempt approximately 14,000,000 passwords per second, which is a significant computational capacity. However, the time it takes for a particular character set remains roughly the same, given that this is a brute-force algorithm. The application must test all possible combinations of characters within the specified constraints to find a hash value.

Considering the computational capabilities of modern computers and their ability to test a vast number of passwords per second, it takes less time to crack a shorter password compared to a longer one. For example, it can take roughly the same amount of time to crack a password like 'aaa' and 'aBC,' even if the character set is larger, such as abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ. In my testing, both 'aaa' and 'aBC' were cracked in less than a second.

When the password space is known but not the length of the password, cracking becomes more challenging and time-consuming, as the length is unknown. Increasing the password length results in a higher number of possible character combinations in the character set, decreasing the likelihood of discovering the correct password early. Additionally, including symbols in passwords increases complexity and the time required for cracking.

Hence, it is advisable to use a wide range of characters and longer passwords. Many websites recommend passwords of at least 8 characters in length, including lowercase, uppercase, numbers, and symbols, to enhance security.