ITIS 6200: Principles of Information Security and Privacy

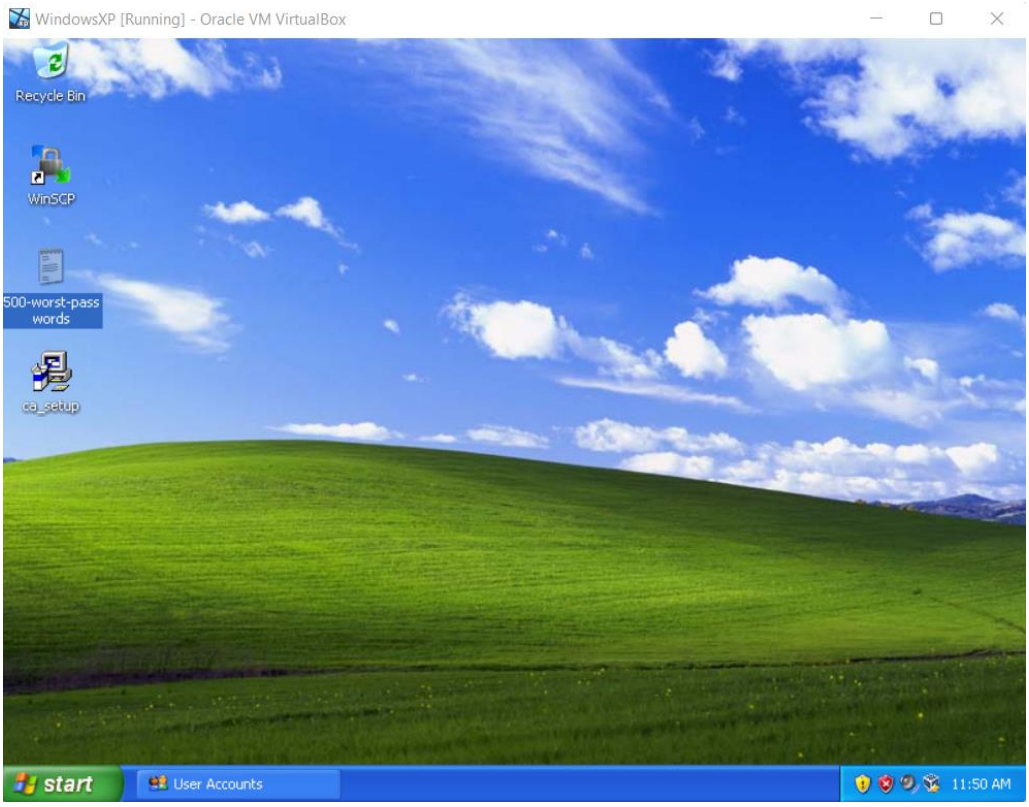
Project 2: Password Cracking for Windows XP

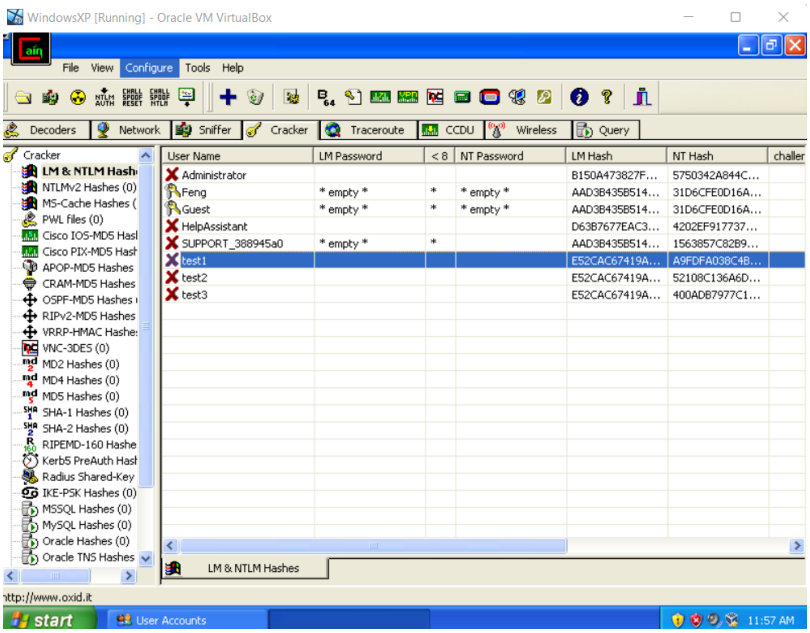
Done by:

Gautham Krishna Kumar (801242601)

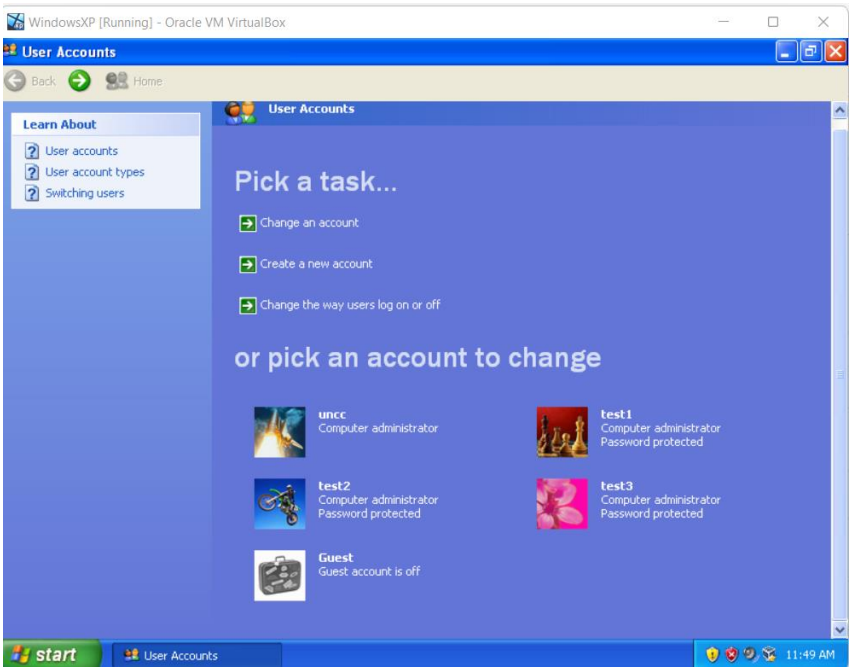
Task 1: Dictionary Attack on test1

First, we need to start the VM on VirtualBox. Once the machine is booted up, we can locate the ca_setup.exe file and the 500-worst-passwords.txt in the Desktop. Cain & Abel has been successfully installed in the VM.

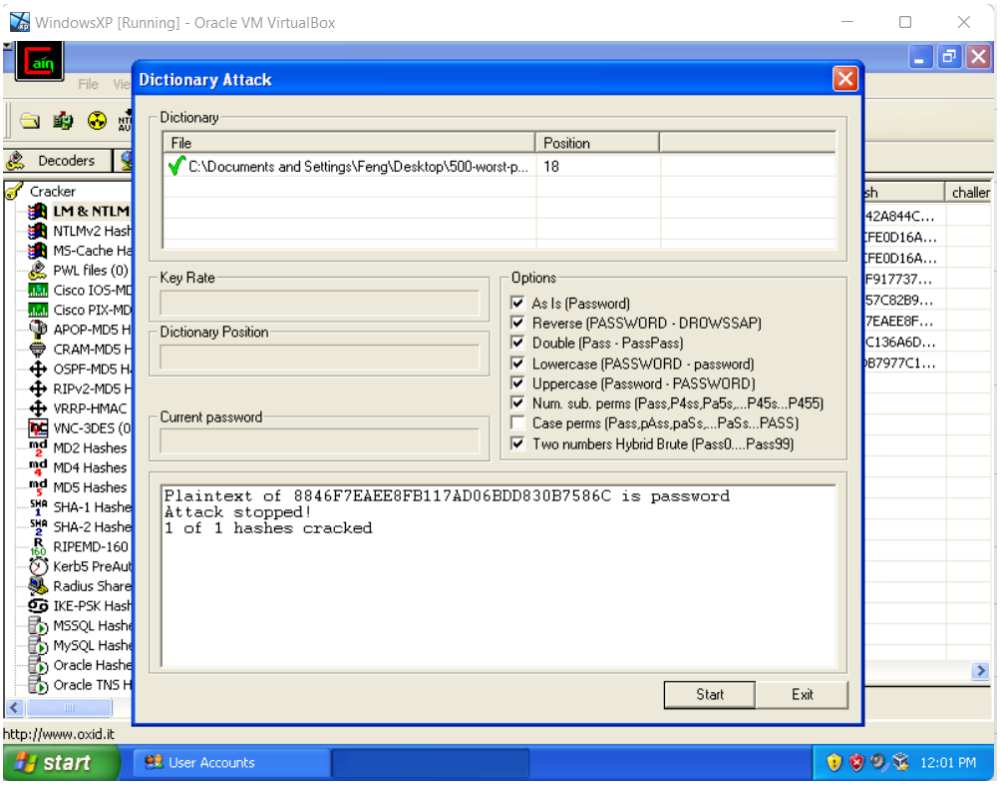




Three users test1, test2 and test3 have been successfully created.



Now, in Cain & Abel, we need to run a dictionary attack on test1 to find out the password. We load the 500-worst-passwords.txt and start the attack. Once the attack is finished, the password of test1 has been found. The password is “password”.



From this attack, we should suggest users not to create easy passwords like the one above since it is easy to perform a dictionary attack from a pre – defined list of common passwords.

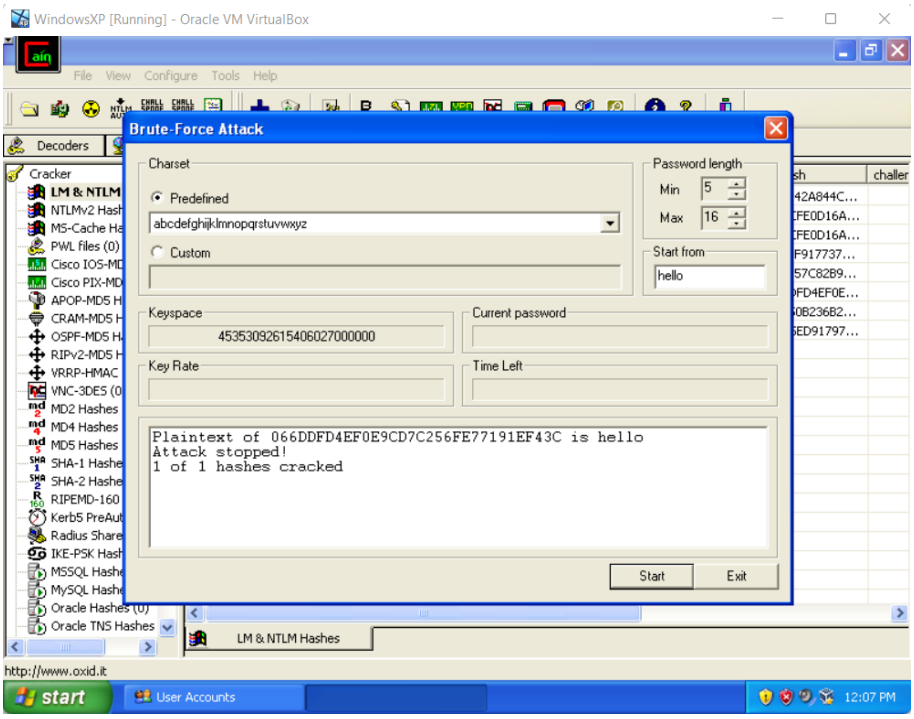
Task 2: Brute – Force Attack

We must now change the passwords of test1, test2 and tes3

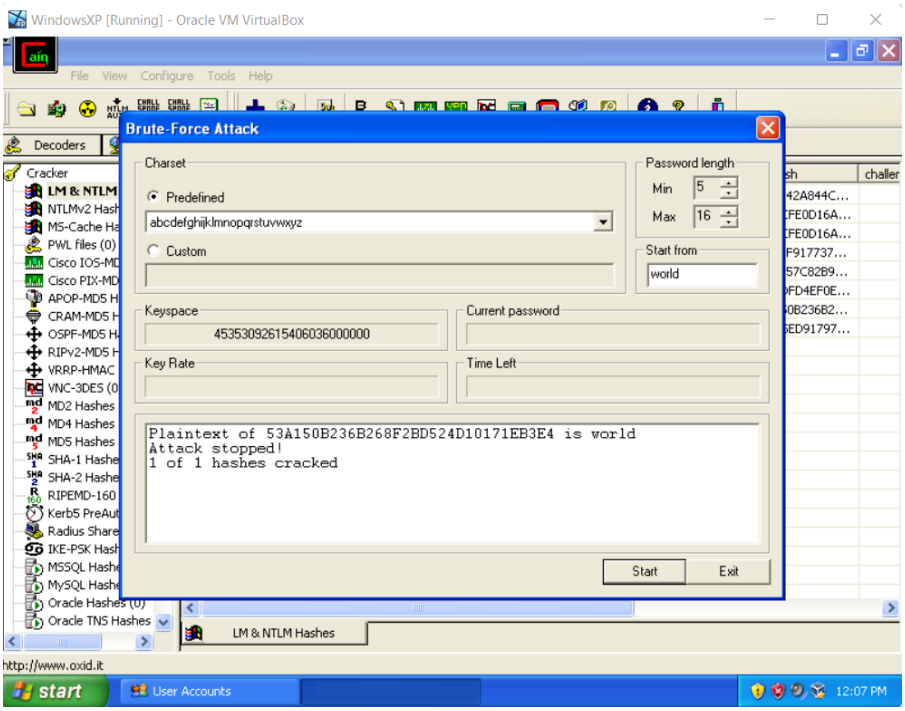
Case 1: Lowercase letters only (length 5)

We create passwords for the three accounts with the above rule mentioned. We perform a brute – force attack on these three accounts to obtain the passwords.

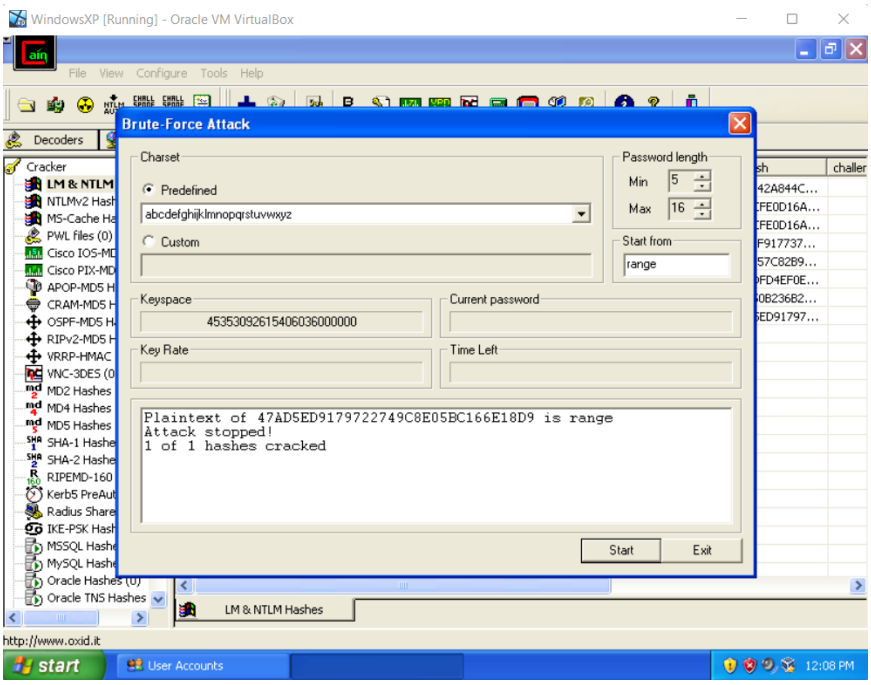
Password of test1: hello



Password of test2: world



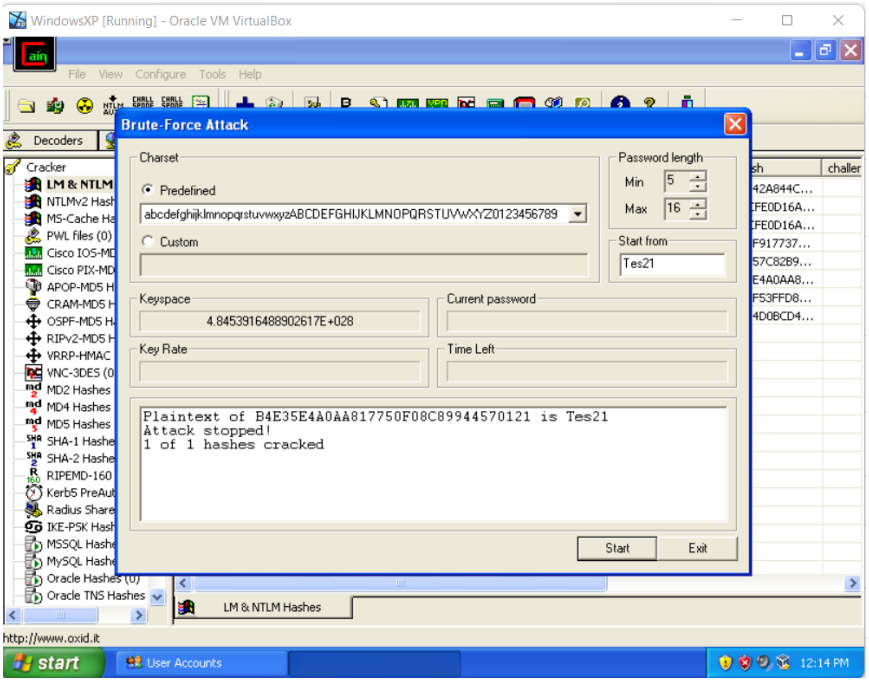
Password of test3: range



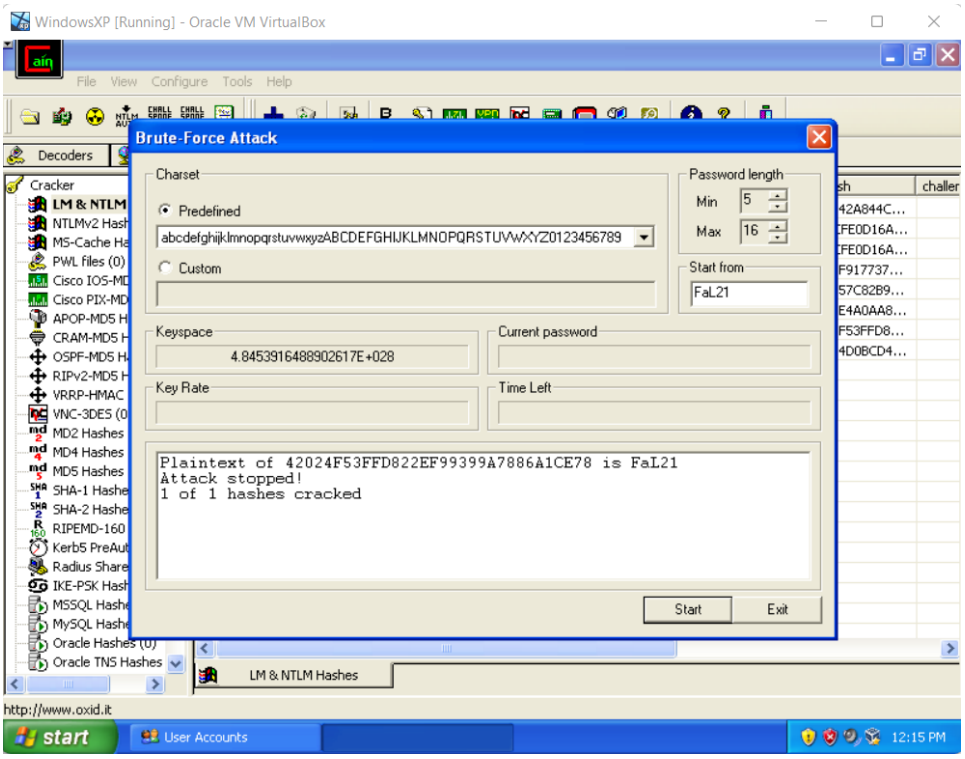
Case 2: Lowercase, uppercase and numbers from 0 – 9 (length 5)

Changed the passwords of the three accounts and performed a brute – force attack.

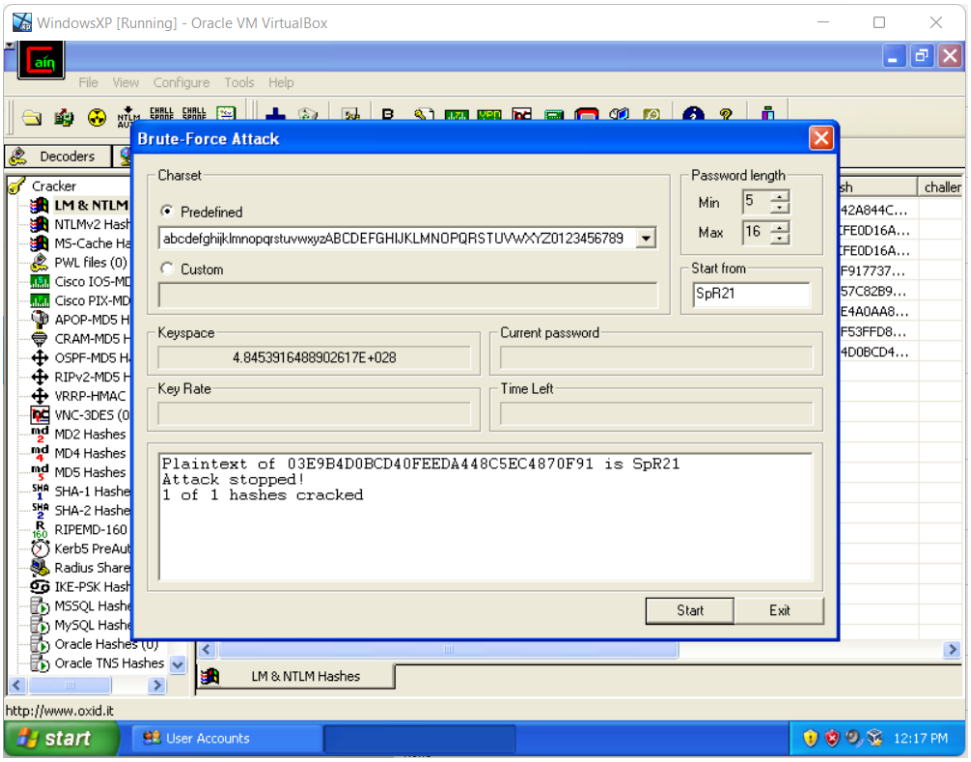
Password of test1: Tes21



Password of test2: FaL21



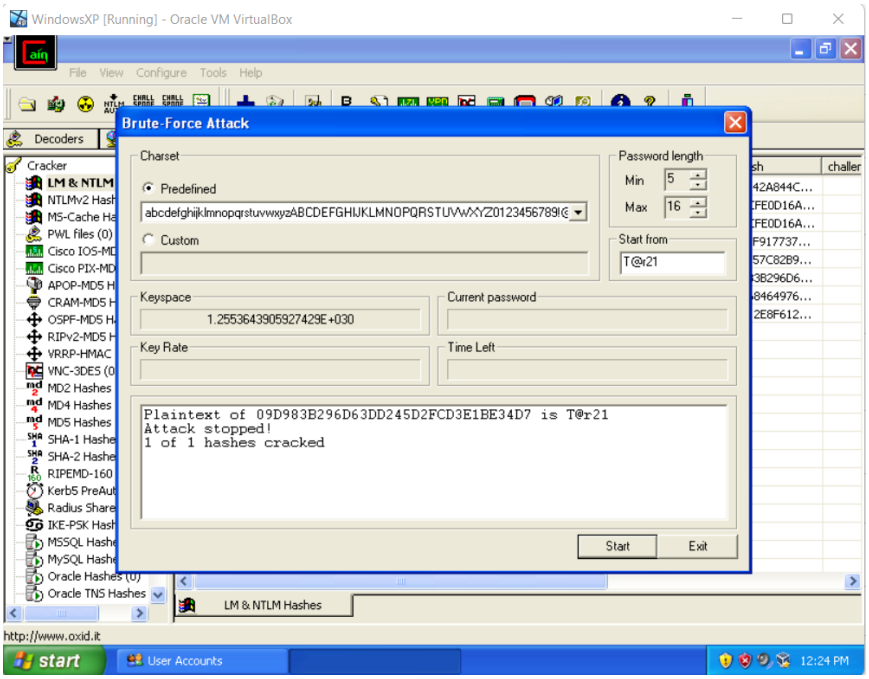
Password of test3: SpR21



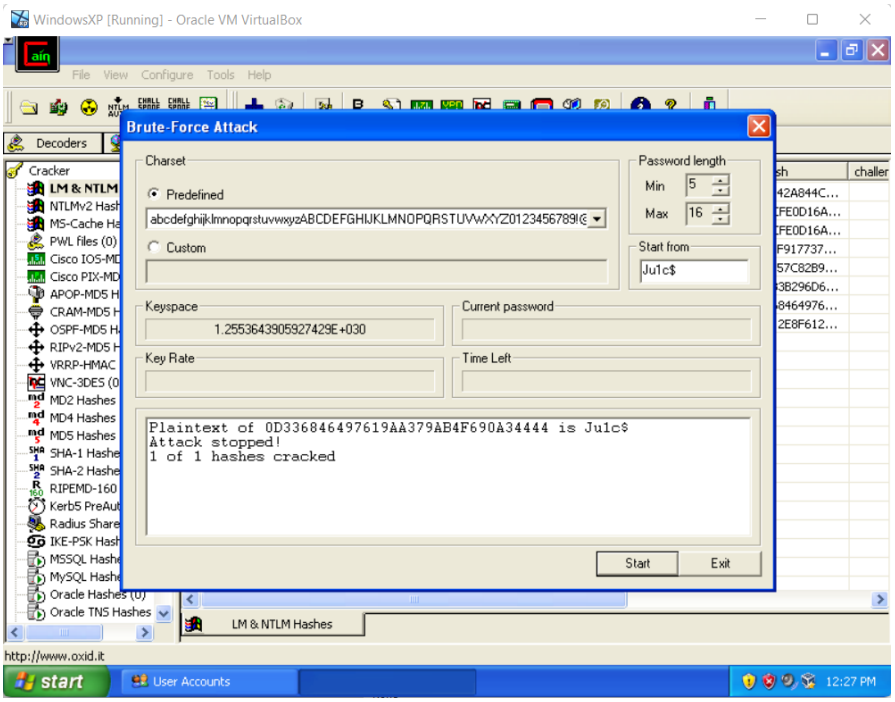
Case 3: Lowercase, uppercase letters, numbers from 0 – 9 and symbols (length 5)

Once again passwords have been changed and brute – force attack has been performed.

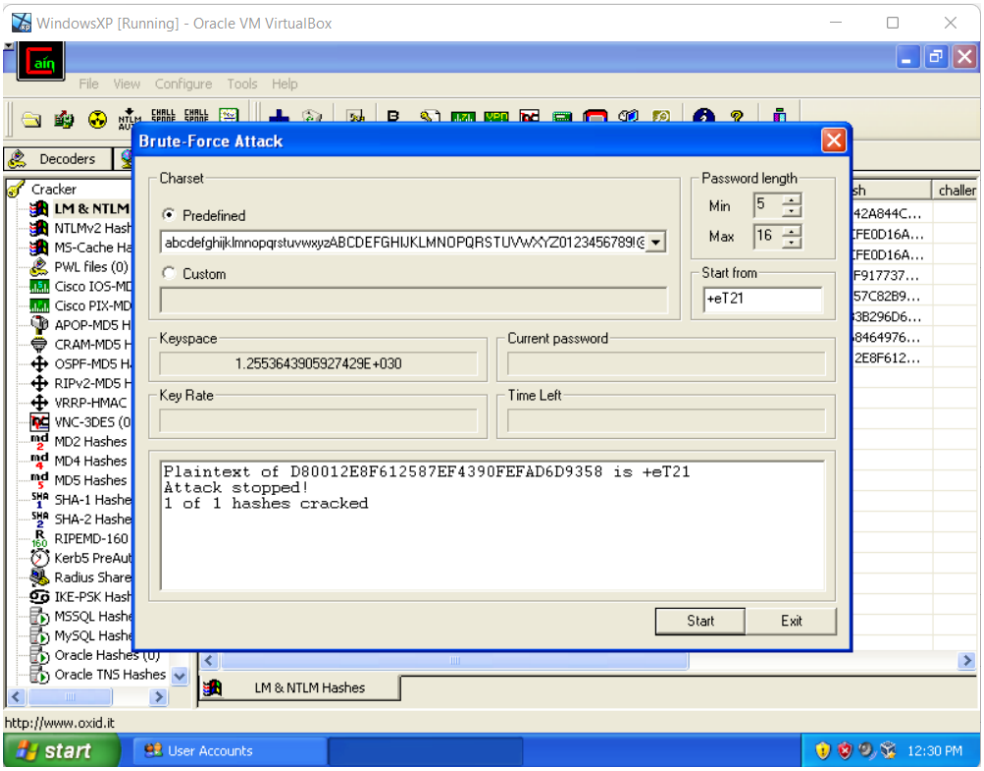
Password of test1: T@r21



Password of test2: Ju1c$



Password of test3: +eT21



Based on the above activity, a table has been made.

	Password Description	Chosen Password		Charset	Time Taken
1	Lowercase letters only (length 5)	test1	hello	abcdefghijklmnopqrstuvwxyz	Less than 1 second
		test2	world		
		test3	range		
2	Lowercase, uppercase letters and numbers from 0 – 9 (length 5)	test1	Tes21	abcdefghijklmnopqrstuvwxyzABCDEFGHIJ KLMNOPQRSTUVWXYZ0123456789	About 1 minute
		test2	FaL21		
		test3	SpR21		
3	Lowercase, uppercase letters, numbers from 0 – 9 and	test1	T@r21	abcdefghijklmnopqrstuvwxyzABCDEFGHIJ KLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=	About 2 minutes and 20 seconds
		test2	Ju1c$		
		test3	+eT21		

	symbols (length 5)			

Question:
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:

If the password chosen is "aBC", Cain & Abel would choose the lowercase and uppercase letters charset and crack the password. The password "aaa" can be cracked using the lowercase and uppercase letter charset as well. There is a small fraction of time difference between cracking these two passwords. Overall, it took Cain & Abel less than 1 second to crack both the passwords. Since "aaa" was cracked a few milliseconds before "aBC" was cracked, I would say that it would take the same time for Cain & Abel to crack both the passwords. Hence my answer is NO for the given question.

If you look at Task 2:

Lowercase letters only: Less than 1 second to crack passwords

Lowercase, uppercase letters and numbers from 0 – 9: Around 1 minute to crack the passwords.

Lowercase, uppercase letters, numbers from 0 – 9 and symbols: Approximately 2 minutes and 20 seconds to crack the passwords.

Hence, the time taken to crack the passwords vary based on password strength, charset, or combination instead of depending on the combination of the password from the same charset.