ITIS 6200/8200 Principles of Information Security and Privacy

Lab: Password Cracking – Part 2

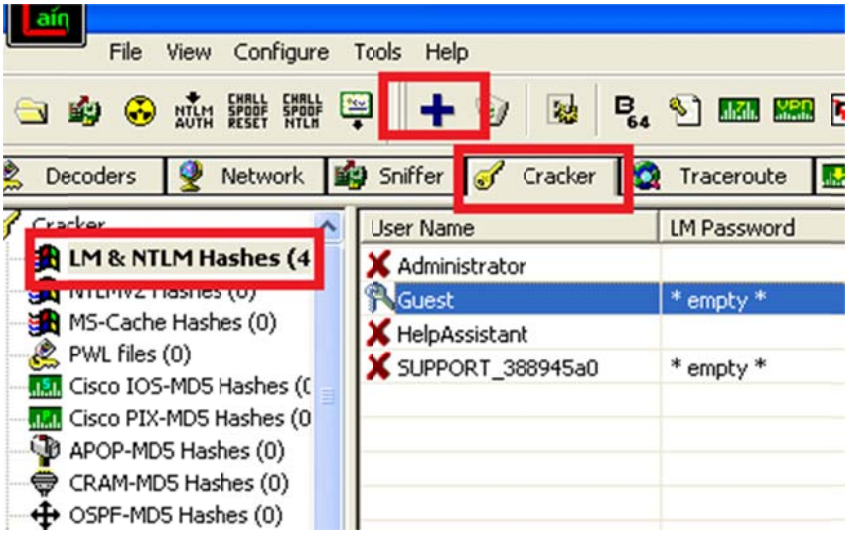
On your Virtual Machine, create three user accounts: **test1**, **test2**, **test3**. **DO NOT USE PERSONAL PASSWORDS ON ANY OF THESE ACCOUNTS since we try to crack the password.** You can create new accounts in the "control panel". Once a user account is created, you can add its password.

TASK 1: DICTIONARY ATTACK

- You only need **test1** for this. We will come around and enter a password for **test1. Do not enter a too long/complicated password since it will take forever to crack it. You can choose a password from the password dictionary that you download.**

- Open Cain & Abel and go under the "**Cracker**" tab and select ***'LM & NTLM Hashes'*** from the left column. (The two red squares in the figure below.)

- Now click on the plus ("+") sign from the taskbar to add NT hashes. Select ***'Import hashes from local system'*** and click next.



- Right click on **'test1'** account and select **'Dictionary Attack'.** Select **'NTLM hashes'** from the sub list.

- Now right click in the dictionary section and select **'Add to list'** to add dictionaries. Navigate to the dictionary file you downloaded and select it.

- Click on **'Start'** to start the attack.
- Discover the password we entered. Note it down, you will have to submit it at the end of the activity via email. Please see end of this document for submission instructions.

TASK 2: BRUTE-FORCE ATTACK

- You will need **test1**, **test2**, and **test3** for this. Create for each account, one password from each type below (in the table). Note: follow exact specifications for the password as specified in the table below.

- Note your chosen password for each type in the table below.

- Right click on the appropriate account, for e.g., **'test1'** and select **'Brute-force Attack'.** Select **'NTLM hashes'** from the sub list. Make sure that you adjust the password length correspondingly. Otherwise, it will take days to finish. My recommendation is to start with a small number. Then you will have a feeling of how long it will take.

- Adjust password length. Choose the appropriate charset.

- Perform the activity with the three passwords.

- Fill the following table with the details based on your activity

- See next page for submission instructions.

	Password Description	Chosen Password	Charset	Time Taken
1	Lowercase letters only (length 5)			
2	Lowercase, uppercase letters and numbers from 0 to 9 (length 5)			
3	Lowercase, uppercase letters, numbers from 0 to 9 and symbols (length 5)			

SUBMISSION INSTRUCTIONS

Your submission should constitute three parts:

1) Password discovered from Task 1
2) Filled table from Task 2
3) Answer the 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!

Submit your results in Canvas before the deadline.