ITIS 6200/8200 Principles of Information Security and Privacy

Project 1: Password Cracking of Windows XP

In this project, you will use a software tool to try to crack Windows XP password. It will use virtual machines. The detailed instruction is as follows.

Description

In the following exercise, we will be using **Cain & Abel**, a password recovery tool for Microsoft Operating systems, to crack and retrieve Windows XP system user passwords from their hashes.

Password Cracking (Part 1):

Follow the steps below you will get a Virtual Machine with Windows XP for this exercise.

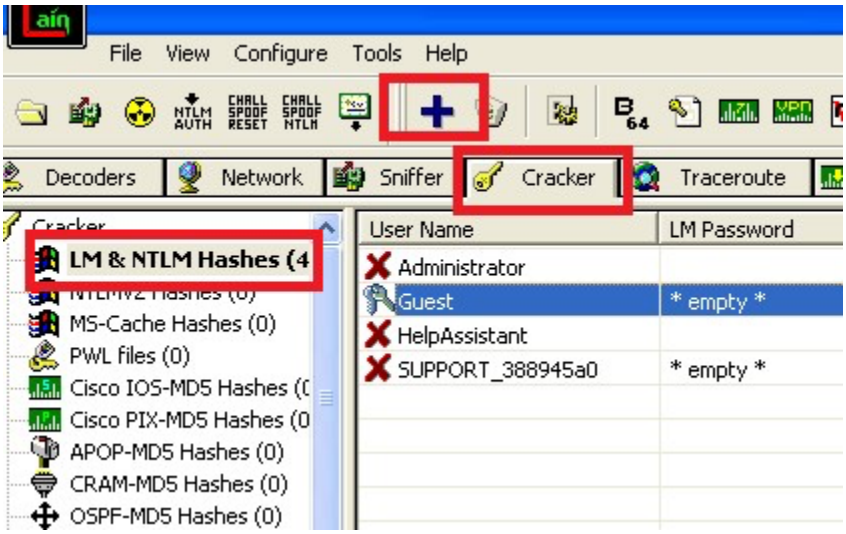
- Download and install **VirtualBox**
    - Virtual 7 may have issues. Using the old version is suggested: **VirtualBox 6.1**
    - At the moment, VirtualBox doesn't support ARM based MacBook. So, if your personal laptop is a MacBook with M1 or M2 processors, you may need to find a temporary replacement, e.g., get a loan from library, or borrow one from your friends
- Download a copy of Windows XP from **here**. In this step, you need to log into your UNCC email account in the browser; we have given read permission to all with UNCC email account.
- Open VirtualBox
- Select File -> Import Appliances
- Navigate to the location of the downloaded content
- Select the 'WindowsXP.ova' file
- Click "Import" and continue
- When the importing is finished, choose "WindowsXP" from your list of virtual machines, click "Settings" -> Network -> Adapter 2 -> uncheck "Enable Network Adapter", then click "OK"
- Start the new virtual machine
- Next, install **Cain & Abel** in the new virtual machine. You should find a file named ca_setup.exe on the desktop. Double click it and follow the instructions.
- Next confirm that a small password dictionary (500-worst-passwords.txt) exists on the desktop

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.** 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.**
- 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 Desktop and select 500-worst-passwords.txt.
- 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.

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.
- 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

	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.

Make sure you **include screenshots** of the steps you applied in your report.