**Faculty of Computing and Information Technology (FCIT)**

**INDUS UNIVERSITY**


# Information Security

# Assignment 4

## Spring 2021

**Student Name: Syed Daniyal Ali**
**Student ID: 1163-2018**
**Program: BSCS**

**Submitted to: Sir Shad Muhammad**

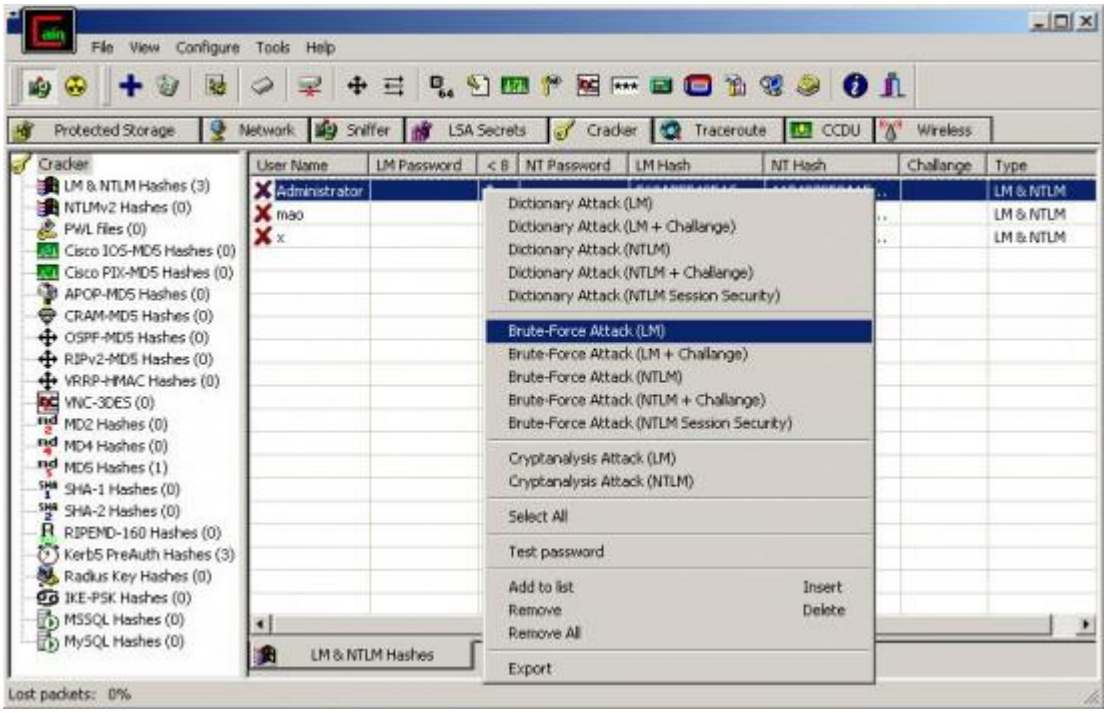
# Assignment 4

**Q1:** Explore Cain and Abel.

**Answer:**

Cain and Abel ( often abbreviated to Cain ) is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks are done via rainbow tables which can be generated with the winrtgen.exe program provided with Cain and Abel.

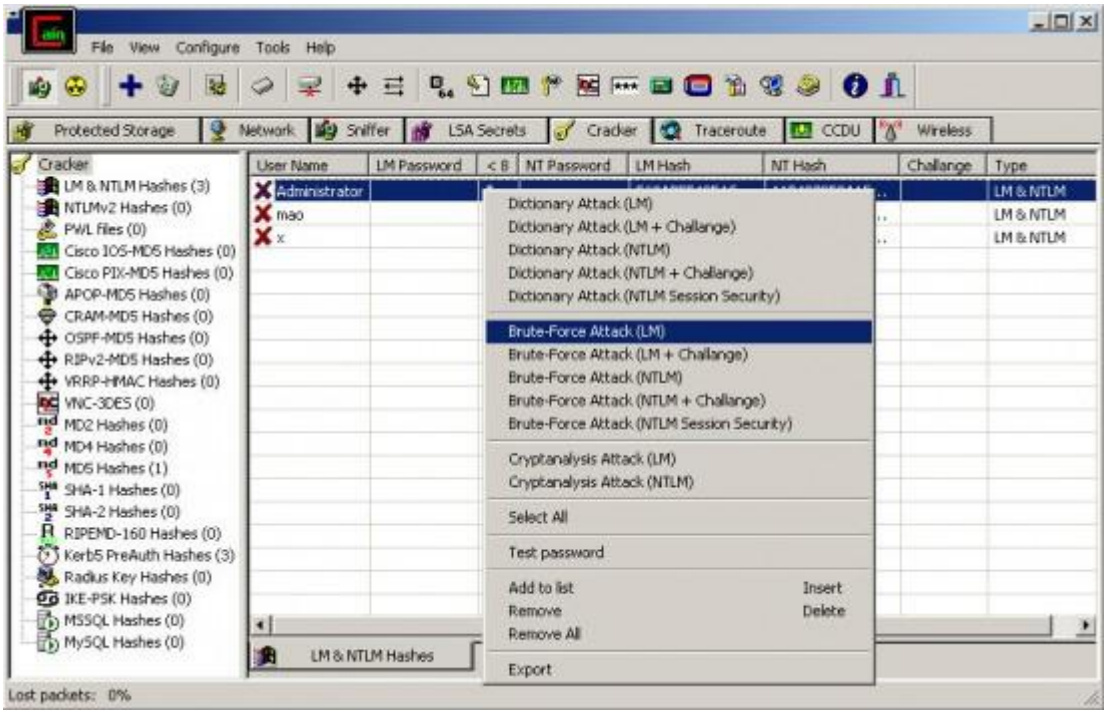
Cain & Abel uses dictionary lists as a basis for cracking passwords, brute-force attacks by trying different passwords many times every second and decoding information stored on the hard drives, the package attempts to determine the correct password. The software also removes the hidden passwords by showing passwords in certain software packages. Learns wireless network keys for forgotten Wi-Fi login information. The software has some security benefits too by indicating where passwords are insecure in an active system.




Cain & Abel is a very useful security tool used for decryption and decoding of passwords for a wide array of offline programs and network services. Built from the ground up to be extremely helpful to users who have forgotten passwords for some of their most-used apps on their home PC, Cain and Abel feature powerful decoding algorithms, extensive decrypting tools, and other.

⚠ Note: This software is no longer available for the download. This could be due to the program being discontinued, having a security issue or for other reasons.

To achieve this feat, the app relies on advanced algorithms and reliance on WinPcap to monitor network activity in the search for transmission of passwords and providing additional security for your own passwords.




Studies have shown that most home users don't have the practice to properly manage and store their passwords, leading them often to forget their own important passwords such as those in Outlook Express. Cain & Abel can not only extract saved passwords from such widely available apps, but it can also decipher any password that is showcased to you masked with asterisks.

Cain & Abel Key Features:
• Locate Wi-Fi password information
• Discover likely passwords for Windows operating system
• Dictionary-based words, brute-force password checking and other methods are used
• Reveal hidden password fields
• Sniff out data stored on drives to discover where passwords may be located
• Can be used for security to verify what can be easily discovered on your own system

**Q2:** What is Rainbow Table.
**Answer:**

## Rainbow Table:

The passwords in a computer system are not stored directly as plain texts but are hashed using encryption. A hash function is a 1-way function, which means that it can't be decrypted. Whenever a user enters a password, it is converted into a hash value and is compared with the already stored hash value. If the values match, the user is authenticated.

A rainbow table is a database that is used to gain authentication by cracking the password hash. It is a precomputed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash. Since more than one text can produce the same hash, it's not important to know what the original password really was, as long as it produces the same hash.

**How the Rainbow Table Attack work:**

A rainbow table works by doing a cryptanalysis very quickly and effectively. Unlike bruteforce attack, which works by calculating the hash function of every string present with them, calculating their hash value and then compare it with the one in the computer, at every step. A rainbow table attack eliminates this need by already computing hashes of the large set of available strings.

There are two main steps in this:
1. Creating a Table
2. Cracking the Password

**1. Creating a Table :**

Here, the hash of a string is taken and then reduced to create a new string, which is reduced again, repeatedly. For example, let's create a table of the most common password, 12345678, using MD5 hash function on first 8 characters:

- ✓ First we take the string and pass it through md5 hash function.
  hashMD5(12345678) = 25d55ad283aa400af464c76d713c07ad
- ✓ We reduce the hash by taking only the first 8 characters. Then, we re-hash it.
  hashMD5(25d55ad2) = 5c41c6b3958e798662d8853ece970f70
- ✓ This is repeated until enough hashes in output chain. This represents one chain, which starts from the first plain text and ends at the last hash.
- ✓ After obtaining enough chains, we store them in a table.

**2. Cracking the Password**

Starting off with the hashed text (the password) its checked if it exists in the database. If so, go to the start of the chain and start hashing until there is a match. As soon as the match is obtained, the process ceases and the authentication is cracked.

# Advantages and Disadvantages of Rainbow Table Attack

## Advantages:

1. Unlike brute-forcing, performing the hash function isn't the problem here (since everything is precomputed). With all of the values already computed, it's simplified to just a simple search-and-compare operation on the table.
2. The exact password string isn't needed to be known. If the hash is matched, it doesn't matter if the string isn't the password itself. It will be authenticated.

## Disadvantages:

1. A large amount of storage is required for store tables.
2. With all of the values already computed, it's simplified to just a simple search-and-compare operation on the table.

## Defense against Rainbow Table Attacks

Rainbow table attacks can easily be prevented by using salt techniques, which is a random data that is passed into the hash function along with the plain text. This ensures that every password has a unique generated hash and hence, rainbow table attack, which works on the principle that more than one text can have the same hash value, is prevented.

Another technique that helps prevent precomputation attacks is key stretching. Using this, the salt, the password, and some intermediate hash values are run through the hash function multiple times to increase the computation time required to hash each password. An alternative approach, called key strengthening, extends the key with a random salt, but then (unlike in key stretching) securely deletes the salt. This forces both the attacker and legitimate users to perform a brute-force search for the salt value. Therefore, there is no point of bypassing salting.