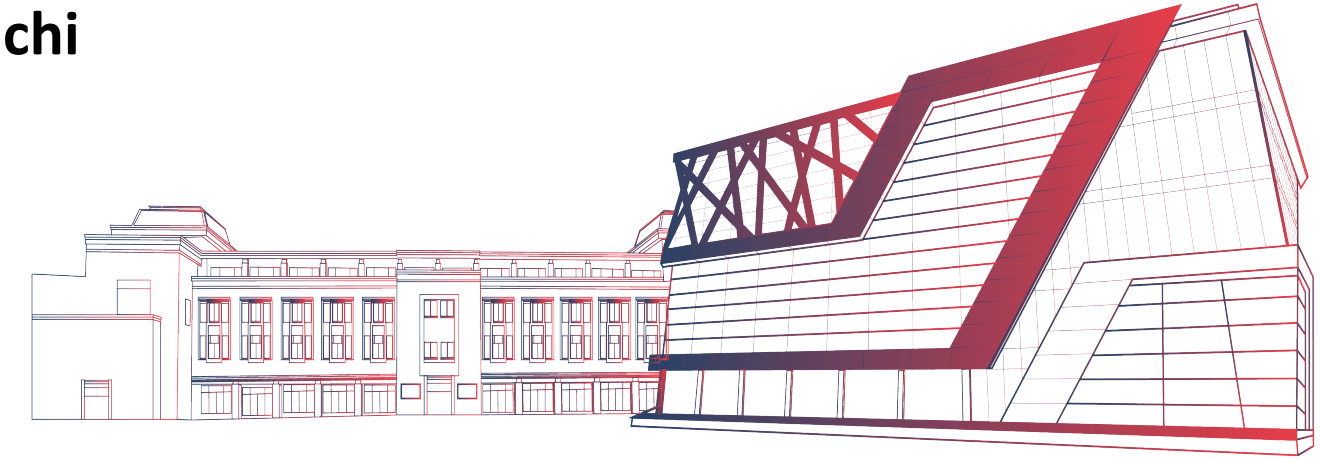
THE NORTHCAP UNIVERSITY

Login Bypass

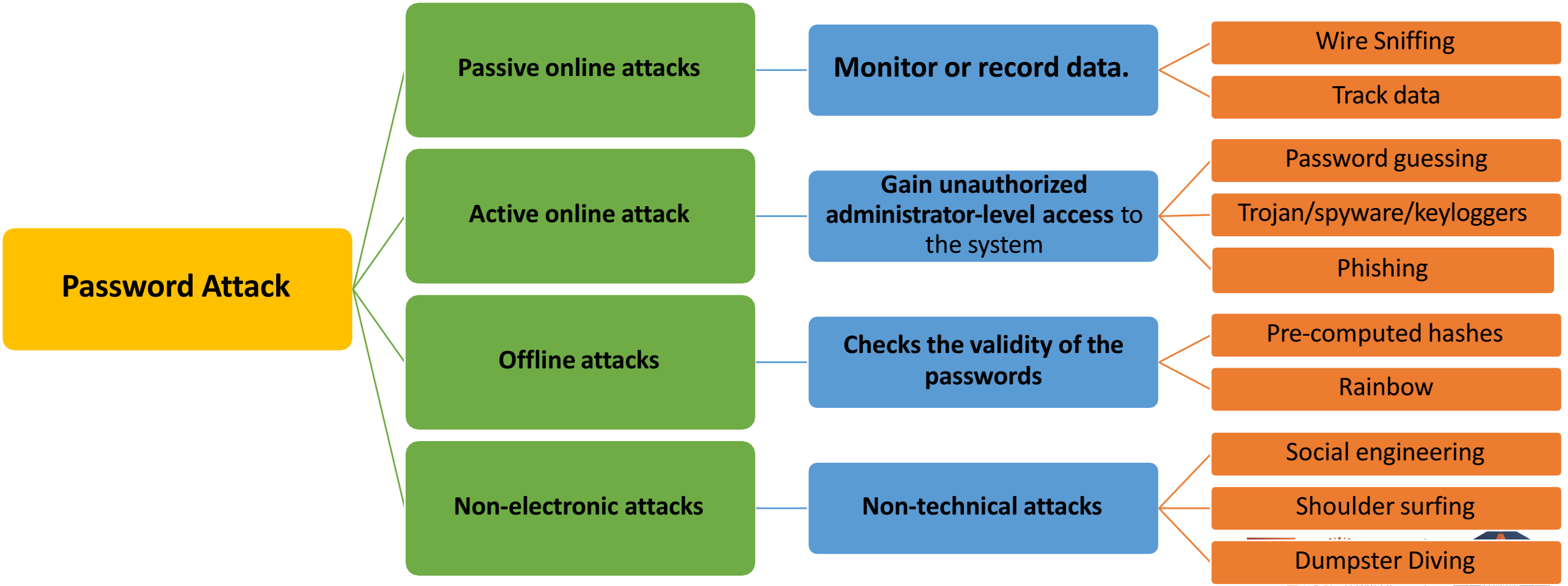
Dr. Prachi



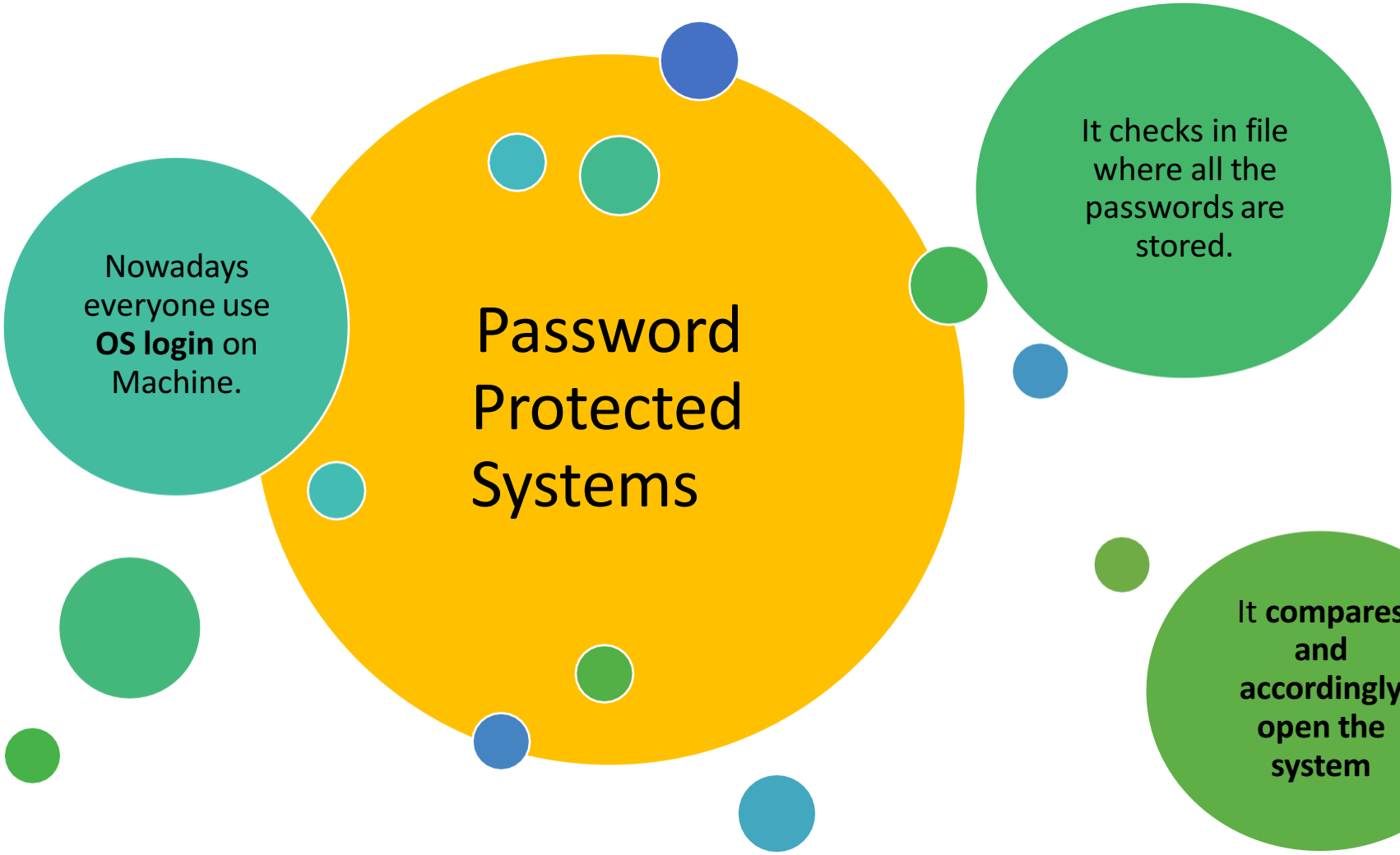
30 YEARS OF EXCELLENCE

NAAC Accredited

Types of Password Attacks



OS Login Bypass



THE NORTHCAP UNIVERSITY
POWERED BY Arizona State University

Which file in Windows stores the password of all the users??

SAM

THE NORTHCAP UNIVERSITY

In windows, **SAM (Security Account Manager)** file **stores passwords** of all the users

SAM is **part of the registry** and can be **found on the hard disk.**

C:\Windows\System32\config\SAM (contains password)

SAM file is part of the **Microsoft Windows Operating System**

THE NORTHCAP UNIVERSITY
POWERED BY Arizona State University

Which file in Linux/MAC is used for storing passwords?

etc

THE NORTHCAP UNIVERSITY

/etc/ is where **configuration files and directories** are located.

/etc/passwd-

- The user database includes **username, real name, home directory, and other information** about **each user**.
- The format is documented in the **passwd** manual page.

/etc/shadow-

- **It is an encrypted file that holds user passwords.**

Linus/Window/MAC

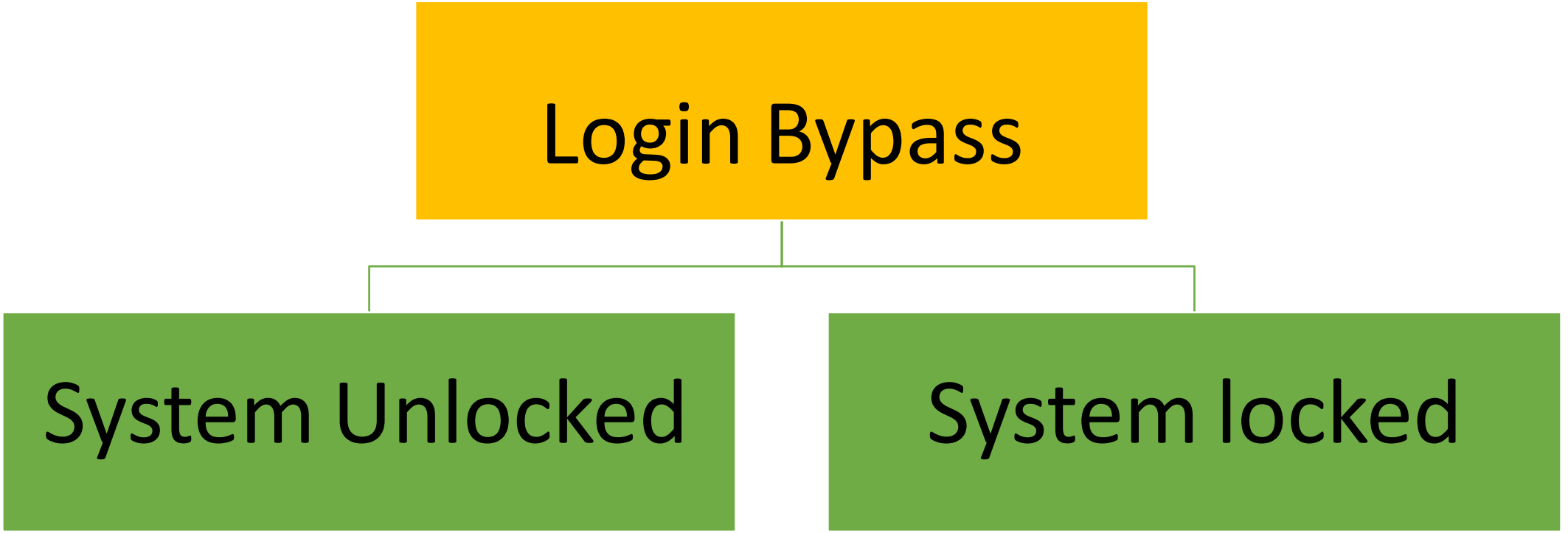
In windows-

Passwords can break

In Linux and MAC- passwords can be bypassed.

Then, we can enter the system and can change the password.

OS Login BYPASS



1. System unlocked: Change Password

If I get a call, or I go to washroom, or I go to take coffee-I keep my system unlocked

These steps will tell you on the basis of scenario's that how to enter and crack into a particular operating system.

1. Password change-Steps

(Good Method) using CMD

1. Open CMD (run as administrator)

2. CMD > net user (Net user is a tool which shows all the users)
   - Eg cmd> net user Mehak *

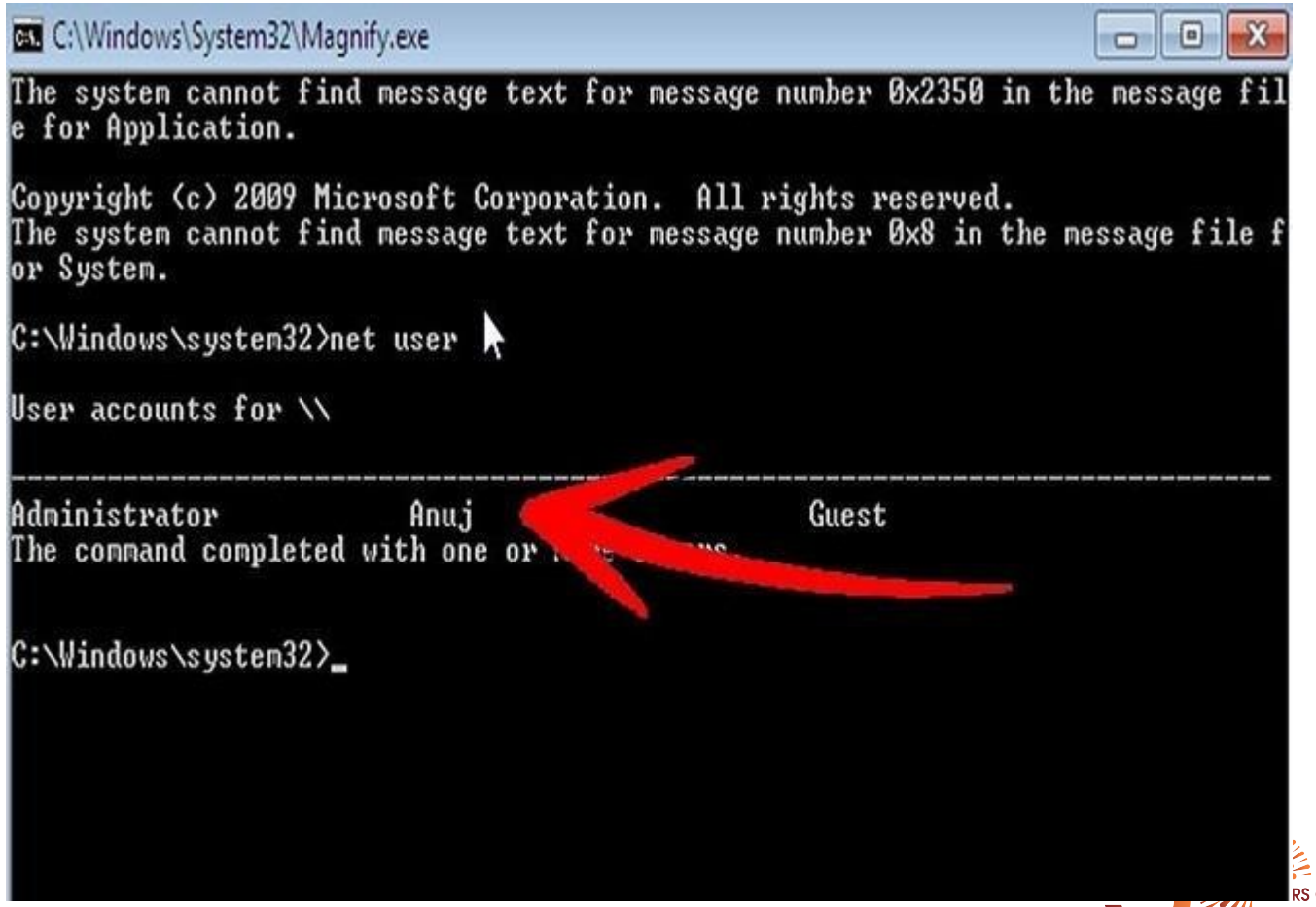
3. CMD > net user username *
   - Is used to change password
   - It will ask to enter and retype password.

4. Restart

Now do anything, you have your account in someone else system

Write command net user

- Open cmd
- Command : Net user



Change Password:

- Write command : net user username *

```
C:\Users\JKonquezt>net user username *
```

- It will ask you enter new password: net user Administrator *

```
C:\Users\prach>net user Administrator *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.
```

Password change-Steps (add user)

Other commands

https://www.lifewire.com/net-user-command-2618097

You can also add user using /add

1. Open CMD (run as administrator)

   2.CMD > net user username * /add

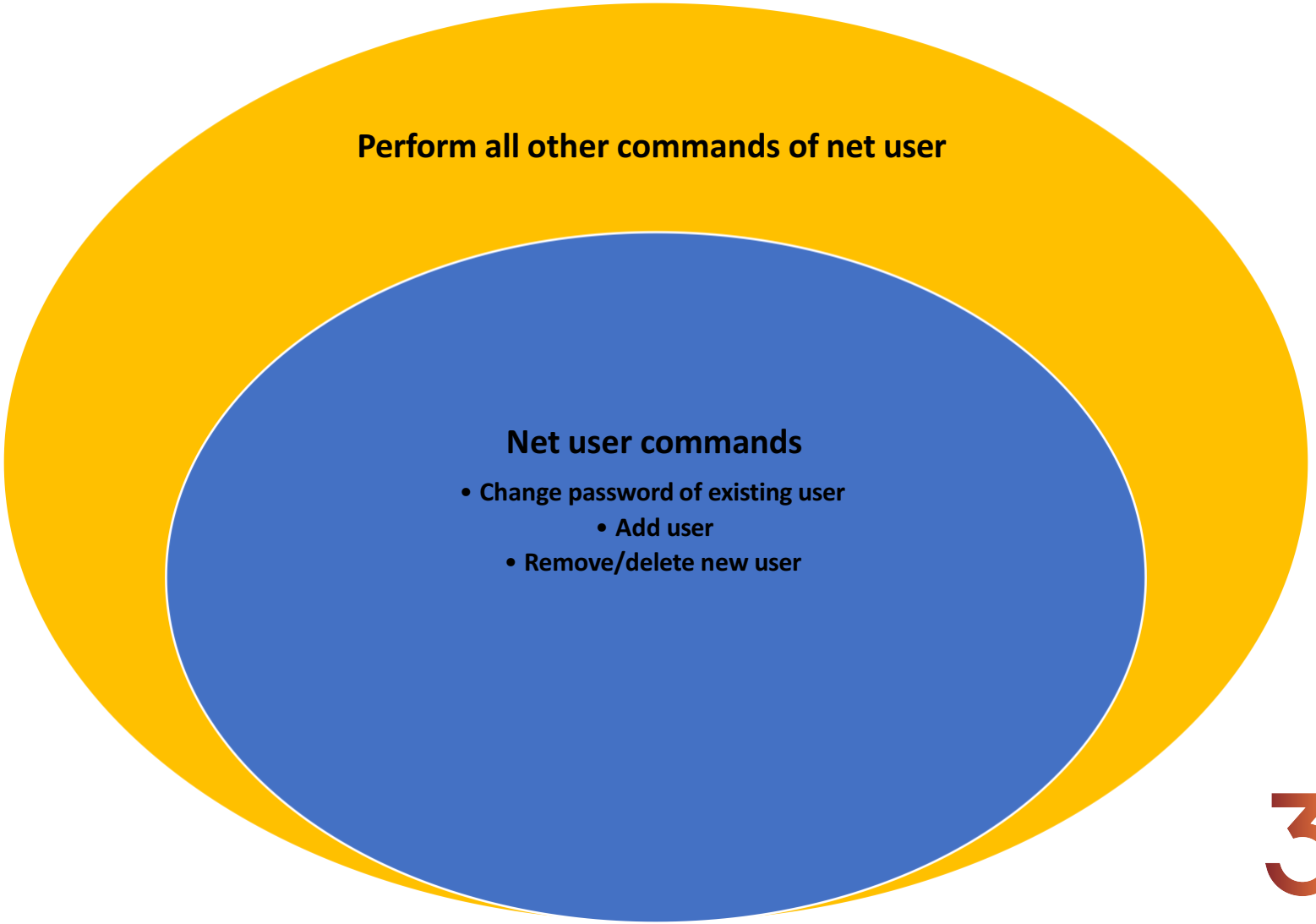
Eg cmd> net user Laxya * /add

It will ask to enter and retype password.

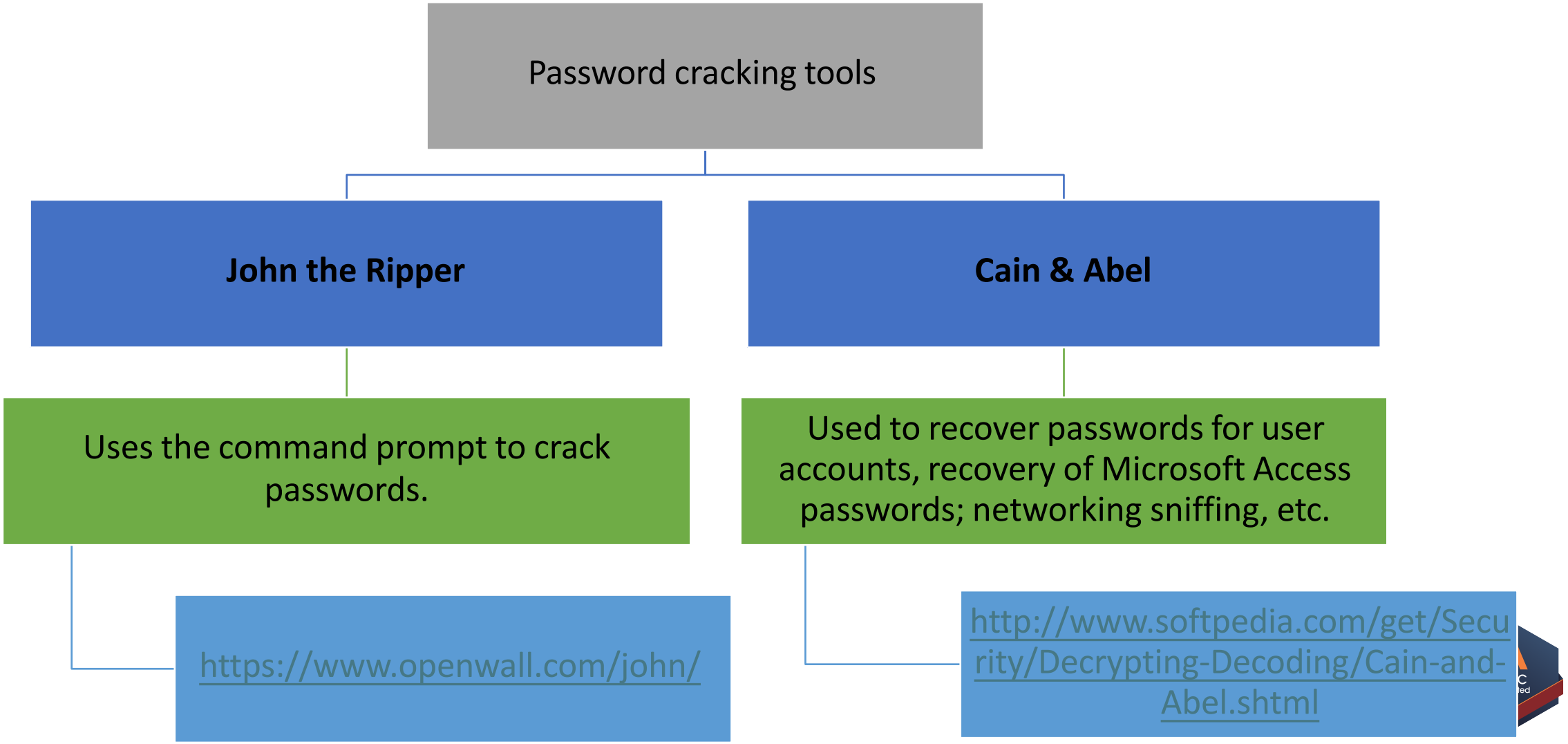
Password Change-Steps (add user)

```
C:\Users\prach>net user Laxya * /add
Type a password for the user:
Retype the password to confirm:
The command completed successfully.


C:\Users\prach>net user

User accounts for \\LAPTOP-REJCUKM6

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Laxya                    prach                    WDAGUtilityAccount
The command completed successfully.
```

In class Exercise



Password cracking tools



Password cracking tool: Cain and Abel

Use NTLM in Cain and Abel

Cain and Abel cracker can be used to crack passwords using;

- **Dictionary attack**
- **Brute force**
- **Cryptanalysis**

Use the dictionary attack in this example.

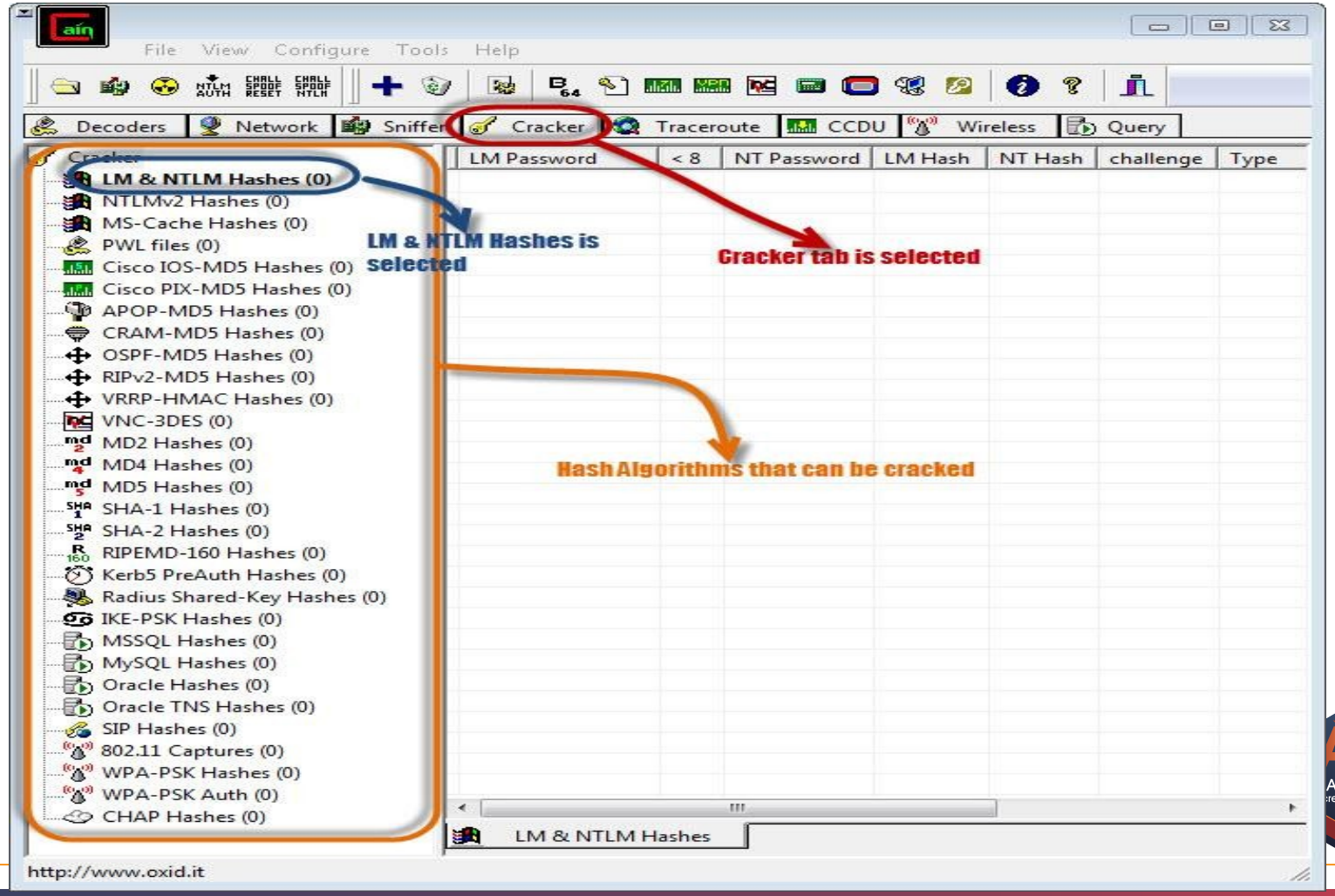
Download the dictionary attack wordlist from google

Password cracking tool: Cain and Abel

- Create an account called Accounts with the password qwerty on Windows 7

Password cracking steps

- Open **Cain and Abel**, you will get the following main screen



Password cracking steps

- Make sure the cracker tab is selected as shown above
- Click on Add button on the toolbar.

Password cracking steps

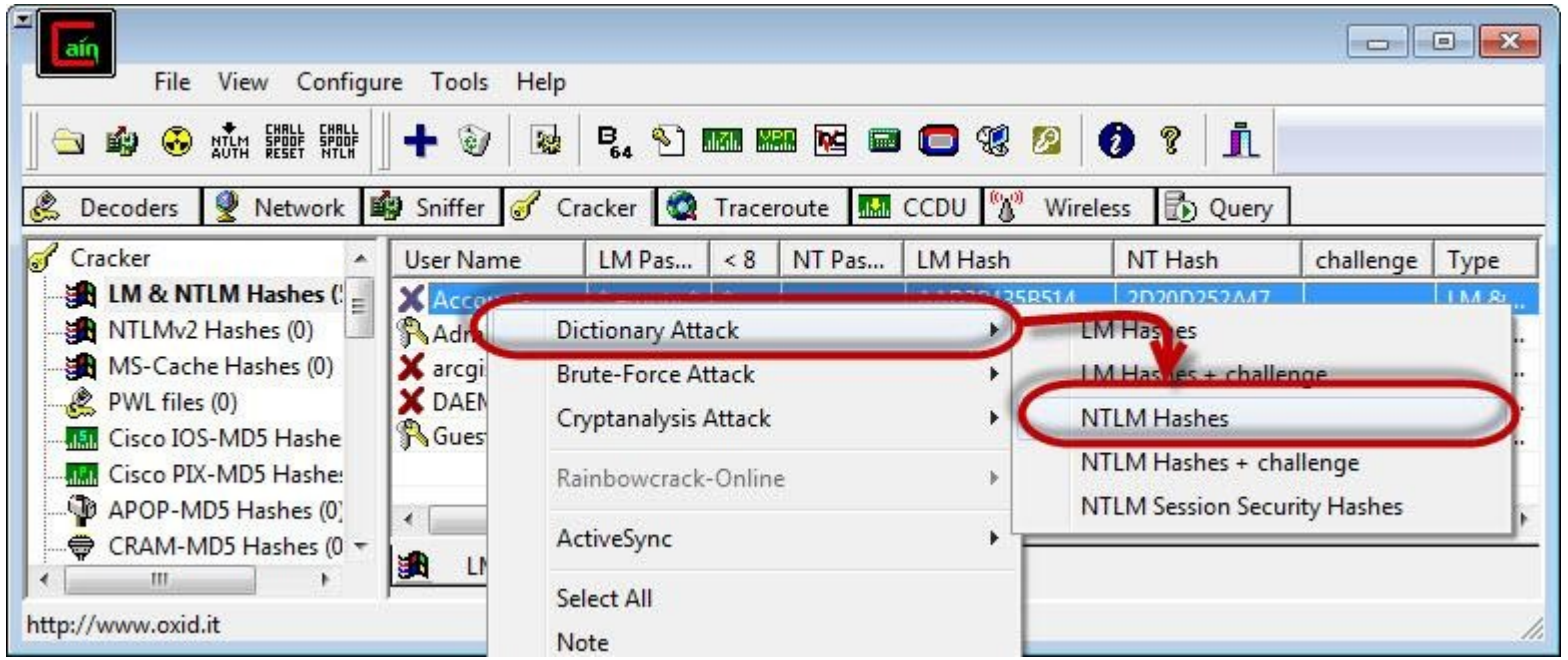
- The following dialog window will appear

Password cracking steps

- The local user accounts will be displayed as follows.
- Note the results shown will be of the **user accounts** on your local machine

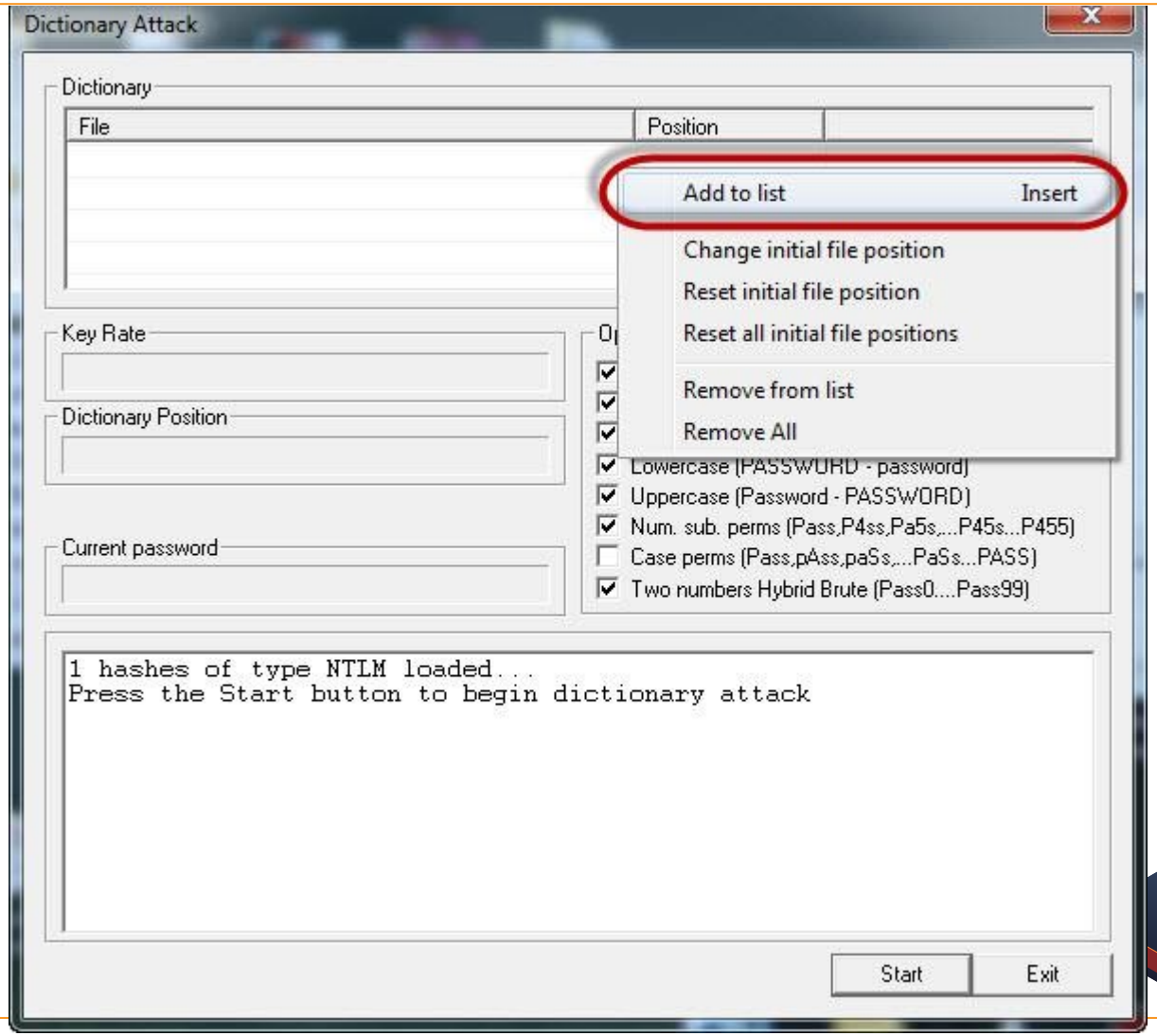
Password cracking steps

- Right click on the **account you want to crack.**
- Here We will use Accounts as the user account.



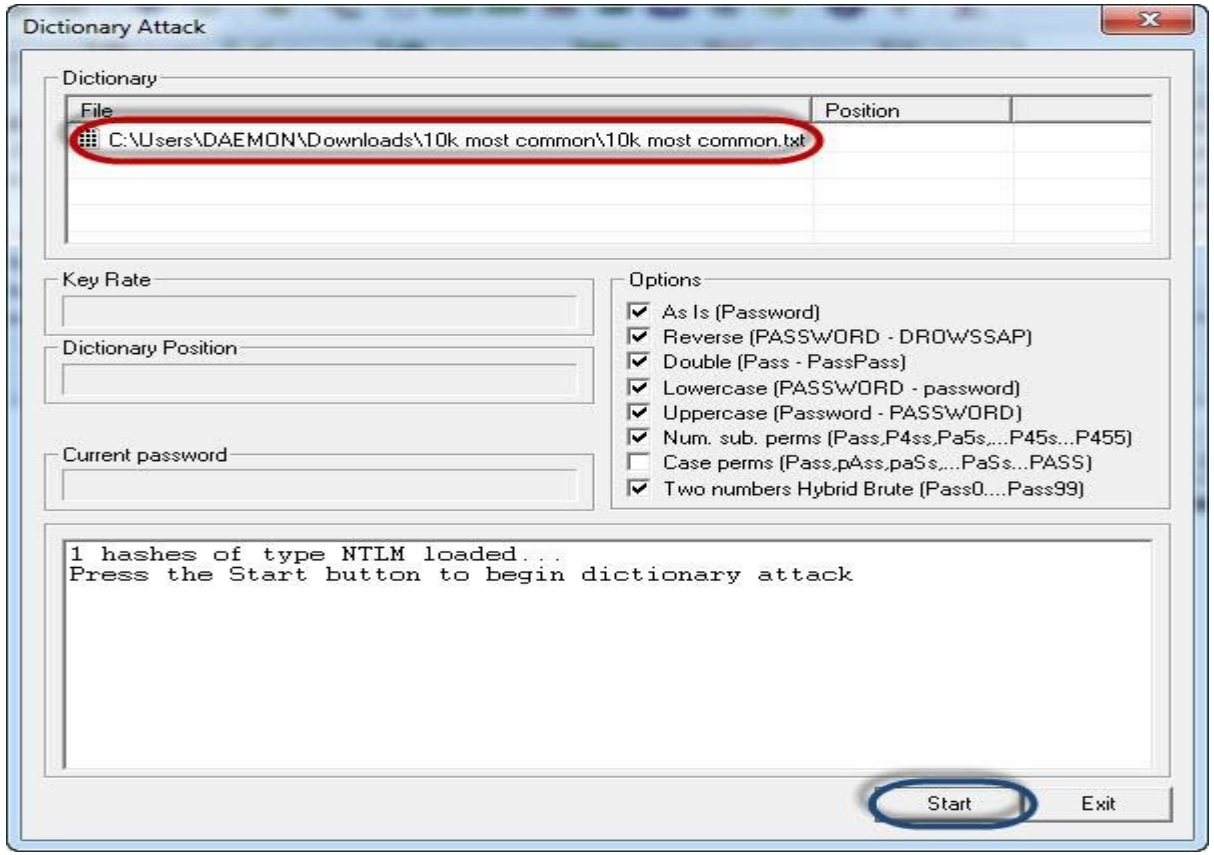
Password cracking steps

- The following screen will appear



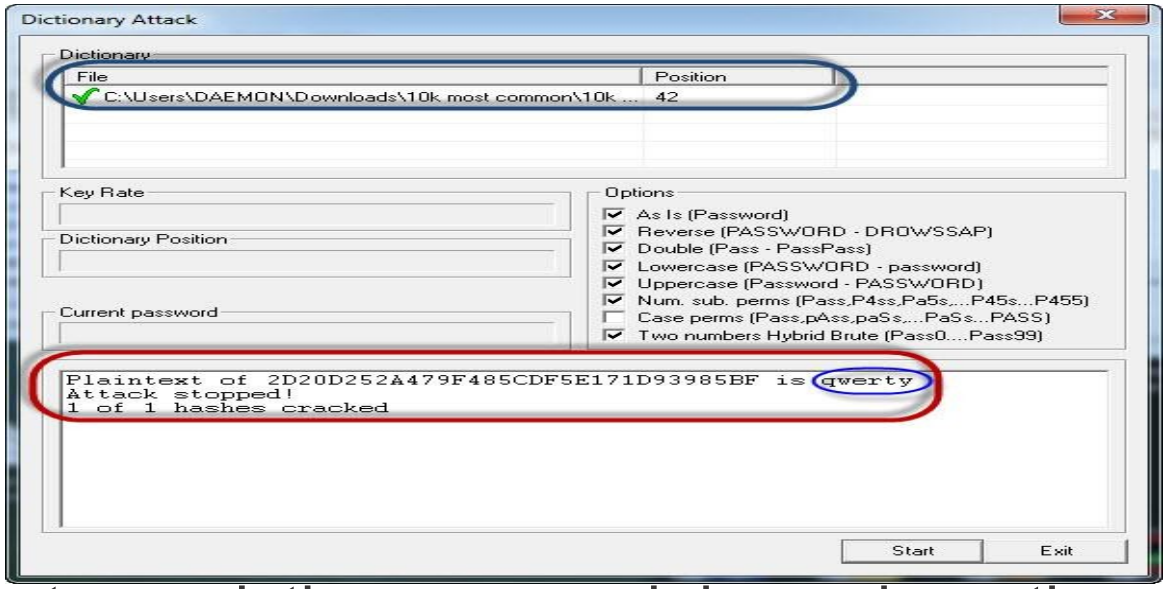
Password cracking steps

- Right click on the dictionary section and select Add to list menu as shown above
- Browse to the 10k most common.txt file that you just downloaded



Password cracking steps

- Click on start button
- If the user used a simple password like qwerty, then you should be able to get the following results



- ***Note***: the time taken to crack the password depends on the password strength, complexity and processing power of your machine.
- If the password is not cracked using a dictionary attack, you can try brute force or cryptanalysis attacks

John the Ripper-Linux

- Tool to recover the password of a compressed zip file called "**John the Ripper**".
- John the Ripper is a free password cracking software tool.
- Originally developed for the Unix operating system, it can run on 15 different platforms.

```
apt install zip apt install unzip apt
install john

```

- **I**

John the Ripper-Linux

•We can use the “John the Ripper” tool simply by entering “john” on our terminal. #john

•We can also use this tool by entering the following command on the terminal. #zip2john

Create Password Protected ZIP File

cat > file1.txt

Add text in file 1
Press CRTL+D

cat > file2.txt

Add text in file 2 Press CRTL+D

zip --password prachi@# myzipfile.zip file1.txt file2.txt

John the Ripper-Linux

- Try to unzip this file using unzip software:
  - unzip myzipfile.zip
  - Try different passwords

- **Suppose you forgot the password that you set during file creation ?**

Get a hashes of the zip file using the zip2john tool.

  - zip2john myzipfile.zip > zip.hashes

- **Crack Password with John**
  - john zip.hashes

- **If not able to crack the password:**
  - john --wordlist=wordlist.txt zip.hashes