A novel approach on Basic security hacks and Tips for Windows Users

[1]Mayank Kumar Prajapati, Mohammad Faiz, [3]Kaushal Kumar, [4]Mohammad Aalam, [5]Pramod Kumar
[1]Student, [2]Guest Faculty, [3]Professor, [4]Guest Faculty, [5]Guest Faculty
[1]Computer Science & Engg., [2]Information Technology, [3]Process &Food Engg., [4]Mechanical Engg.,[5]Mathematics
[1]G.L Bajaj Group of Institution, Mathura, [2,3,4,5] Mahamaya College of Agricultural Engineering and Technology, Ambedkarnagar (U.P.), India.

Abstract: This paper basically deals with the basic security issues of the operating system mainly in windows. What are the ways in which your system can be compromised and what are the ways to secure yourself from these kinds of attacks will be briefly covered in this paper . This paper is for beginners as well as advance users of computer system. We will cover only basic things in this paper. This will mainly focus on the things that we do unknowingly and get trapped. When you give physical access to someone to your system, you don't even know what that person can do with your system.

***IndexTerms* - Component,formatting,style,styling,insert.**

I. MOTIVATION: The motivation of this paper actually came from my friends and colleagues. They are not aware about their security and hand over their system to anyone. I think that this is the worst thing that we all are doing with our privacy. The consequences sometimes may be very serious and will place you in worst condition. You can have your saved passwords, online banking credentials, private photos, documents etc in your system. But if you give access to your system in absence of you because only you trust him/her may become the biggest mistake of you and they can blackmail you also for your private data. So I decided to write on this topic, how hackers or your friend able to compromise with your privacy and how you can secure yourself. Everyone in this modern should learn and implement these techniques to secure themselves. Nowadays there are many cybercrimes happening each and every day. If system user will not know how to prevent themselves from cyber- attacks and some basic security tips then how he or she can be able to protect their system. So I decided to write this paper. This will tell you about some basic security tips and also explain some methods by which the information of your system go into the hands of bad person[1][2][7].

II. INTRODUCTION: Windows Operating system is one of the popular operating system. This Operating system is commonly used across the world and it has more population of users than any of other operating system. The reasons are, it is very simple, easy to understand and user friendly. Many organizations have adopted Microsoft Windows as the standard operating system for their working environment. So this attracts evil and black hat hackers more to create malware for windows operating system. It is not the surprising thing that today most of the viruses and malware are created for windows operating system. Yet Microsoft is providing regular support, security updates etc to secure their users from being hacked or trapped but still most of the hacker prone system is windows operating system. Can you guess why this happens? It is not only the responsibility of the Microsoft, it sometimes or most of the times depends upon the user of the system. Most of the systems are hacked due to irresponsible behavior of the user towards their system. Microsoft has released several versions of windows

e.g. windows7, windows8.1, windows10 etc. Among these, windows10 and windows7 are most commonly used operating system. The differences between windows7 and windows10 are given below in the tabular format [3][4][5][6].

Table 1: Differences between windows7 and windows10

Windows7	**Windows10**
Start menu of windows7 is very simple and doesn't take much more ram.	Start menu of windows10 is attractive and takes ram more than windows7.
Syskey password support is available in windows7.	Syskey password support is removed from the windows10 latest update.
In overall performance windows7 is somewhere lags behind as compared to windows10.	Windows10 is the latest windows os launched by Microsoft and it is very fast as compared to windows7
Cortana(Virtual support) is not present in windows7.	Cortana support is available in windows10.

The features of windows10 are given below(currently updated O.S of Microsoft)

- It improved multitasking.
- Cortana is there for helping you.
- Xbox app is present here for game streaming.
- Performance and efficiency is increased.
- Microsoft Edge has finally replaced Internet Explorer.

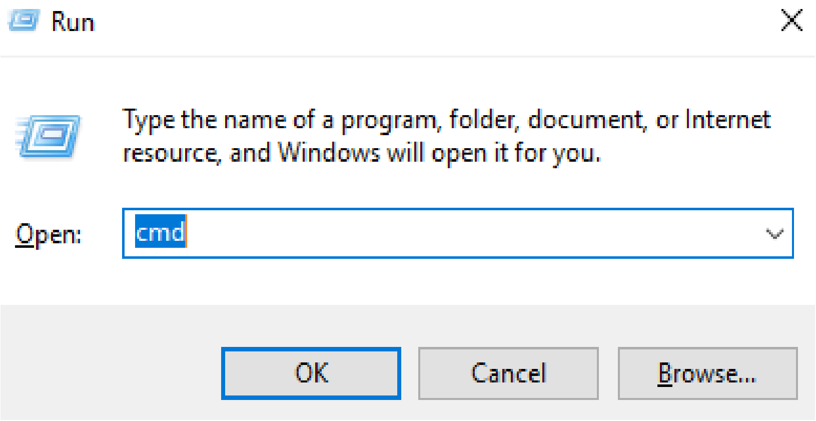
III. BASIC BUT DESTRUCTIVE HACKS AN EVIL HACKER CAN PERFORM ON WINDOWS OPERATING SYSTEM:

We will cover those techniques and tips that even a noob hacker can perform if he has your system in his hand. After reading these hacks I am assuring you that you will think twice before giving your system to anyone. Sometimes you save your passwords, even banking passwords, browsing history etc. what if I tell you that these credentials can be viewed without any difficulty. Yes this is much surprising but it very easy and this doesn't require any extra speciality to perform these kinds of attacks. But these are more vulnerable to you, your privacy and much more. These tricks and tips are explained below with pictures. You have to go through only step by step and at last you realise that these are very simple but destructive.

1. Viewing saved Wifi Passwords:

The steps for viewing saved wifi passwords the system are as follows.

- Open command prompt as administrator by simply pressing win+r keys together. A dialogue box will appear write "cmd" and hit enter as shown in the picture.



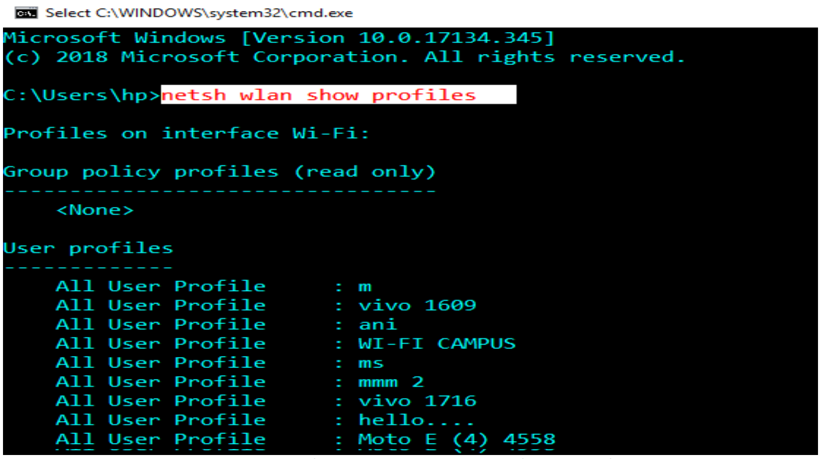
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Fig.1. Open cmd in windows

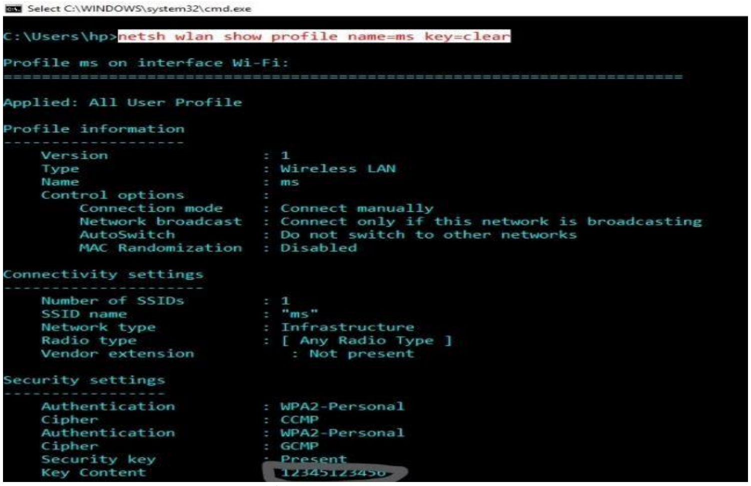
- Command prompt screen will appear on your screen. Now you have to view the name of the profiles (Wifi networks) whose passwords are saved on your computer. The command for viewing those profiles names is "netshwlan show profiles"



```
Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\hp>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : m
    All User Profile     : vivo 1609
    All User Profile     : ani
    All User Profile     : WI-FI CAMPUS
    All User Profile     : ms
    All User Profile     : mmm 2
    All User Profile     : vivo 1716
    All User Profile     : hello....
    All User Profile     : Moto E (4) 4558
```

Fig.2. Command for seeing essid(name) of saved wifi networks

- Suppose we want to view the password of the profile (Wi-Fi name) named “ms”. You have to execute this command in the command prompt.
  “netshwlan show profile name=ms key=clear”



Select C:\WINDOWS\system32\cmd.exe

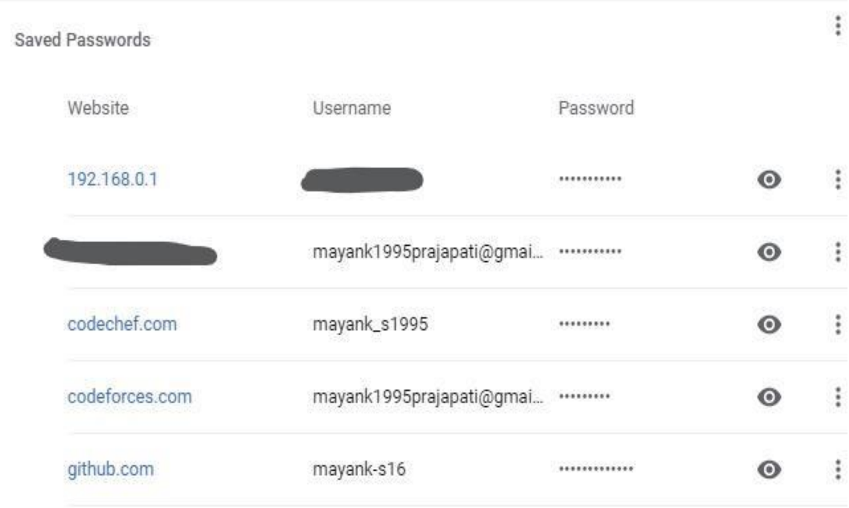
```
C:\Users\hp>netsh wlan show profile name=ms key=clear

Profile ms on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : ms
    Control options        :
        Connection mode    : Connect manually
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "ms"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 12345123456
```

Fig.3. Gaining wifi password using netsh command

- Well, you got what you want from the system. You will see the password of that access point in the Key Content.

2. **Viewing Google Chrome Saved passwords:**
   This is not a big deal I think, everyone should aware of it in this high modernized computer age. But anyhow we will cover this as short as possible. The steps are as

- Open your chrome browser and navigate to Settings>Passwords and here by clicking on the Eye icon you will be able to see the credentials.



Saved Passwords

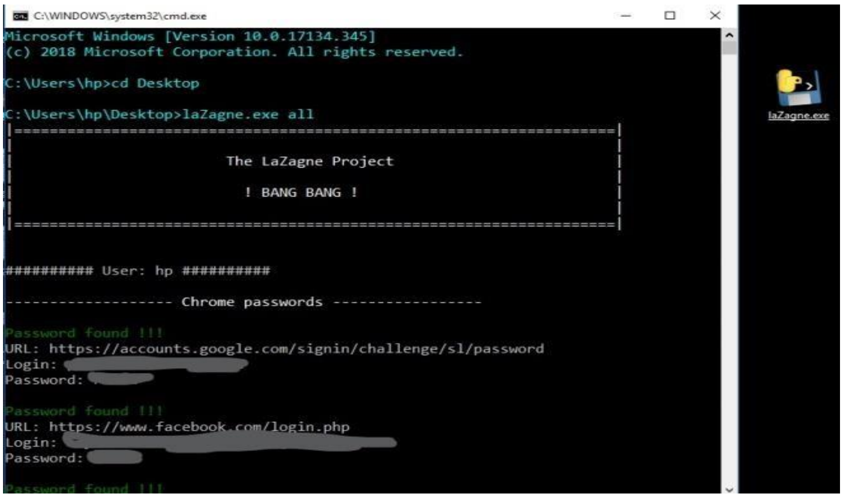
Website	Username	Password
192.168.0.1	[redacted]	•••••••••••
[redacted]	mayank1995prajapati@gmai...	•••••••••••
codechef.com	mayank_s1995	•••••••••
codeforces.com	mayank1995prajapati@gmai...	•••••••••
github.com	mayank-s16	•••••••••••••

Fig.4.. View saved passwords in Google chrome

3. **Gaining all the passwords in just one command:**
   This can be the most dangerous thing an evil mind person can do with your system and you. There is large number of software available on the internet today for windows which don’t even need installation and by only a single command someone will be able to access your all saved passwords. One of the most popular tool for achieving this goal is “Lazagne”. This is available for both windows and linux operating system.
   Firstly you have to download this software by going to the below link for windows.

   https://github.com/AlessandroZ/LaZagne/releases Download laZagne.exe file from the above link.

- Place it anywhere in the system either on the Desktop or some other directory.
- Open cmd and navigate to that directory where laZagne.exe file is present.
- Now just write “laZagne.exe all” in the command prompt and this will work amazingly and show you all the passwords as shown below. The person who is performing this attack on your personal computer can take the screenshot of this screen, cut and paste into his physical drive and even you will not be notified about it.

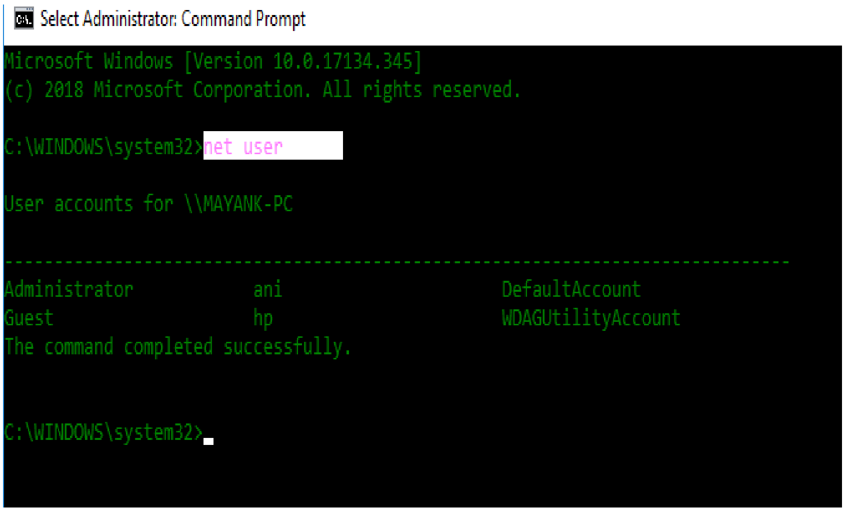


```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\hp>cd Desktop

C:\Users\hp\Desktop>laZagne.exe all
|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

########## User: hp ##########

------------------- Chrome passwords -----------------

Password found !!!
URL: https://accounts.google.com/signin/challenge/sl/password
Login: [redacted]
Password: [redacted]

Password found !!!
URL: https://www.facebook.com/login.php
Login: [redacted]
Password: [redacted]

Password found !!!
```

Fig.5. Lazagne command demonstration

4. **Change user password without knowing the old password:**
   This will ruin your comfort. You will be surprised to know that your system password can be changed without knowing your old password. Also this doesn't require much more time and even steps are not very complex.

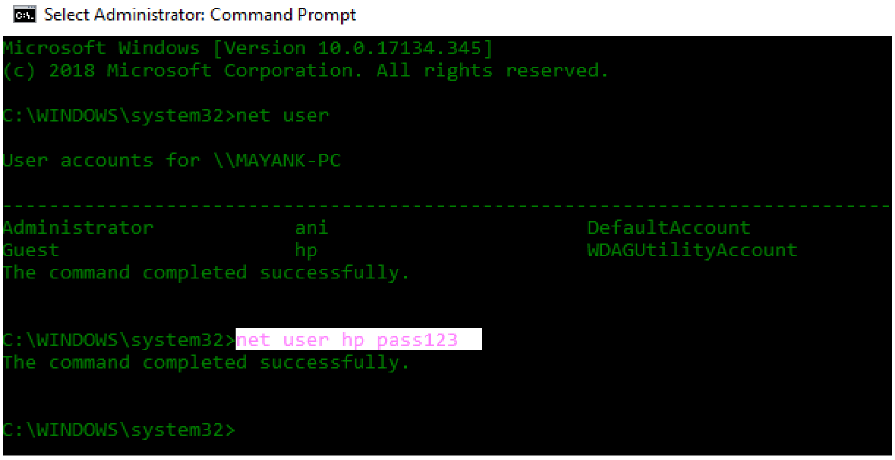
- Open cmd as admin(Without admin account this will not work)
- Type "net user" and hit enter to see the user list on the system.



```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net user

User accounts for \\MAYANK-PC

-------------------------------------------------------------------------------
Administrator            ani                      DefaultAccount
Guest                    hp                       WDAGUtilityAccount
The command completed successfully.


C:\WINDOWS\system32>
```

Fig.6. Detecting users on operating system

- Now select the user according to your choice and type the following command. I am selecting "hp". This may be different in your case.
  Command: "net user hp pass123"
  This command will remove the current password of the hp user and set the new password "pass123".



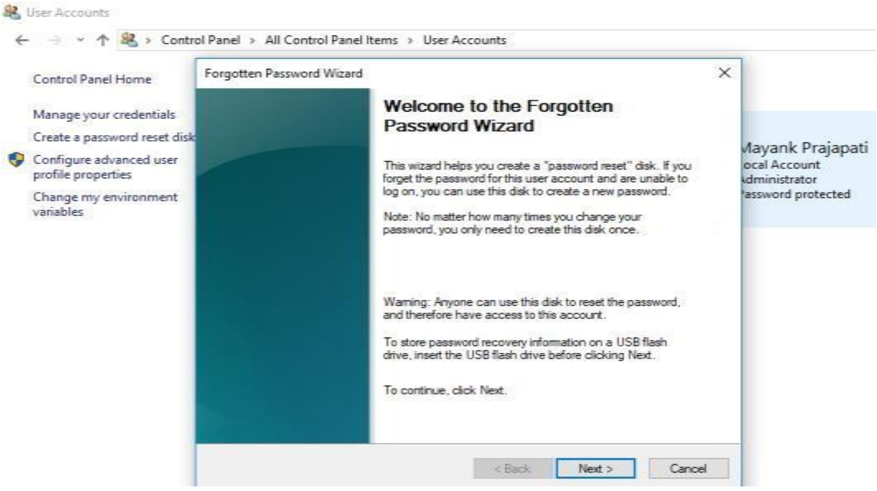
```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net user

User accounts for \\MAYANK-PC

-------------------------------------------------------------------------------
Administrator            ani                      DefaultAccount
Guest                    hp                       WDAGUtilityAccount
The command completed successfully.


C:\WINDOWS\system32>net user hp pass123
The command completed successfully.


C:\WINDOWS\system32>
```

Fig.7. Changing the password of user hp to pass123

5. **Creating password Reset Disk:**

Once you have given your system openly and you are away from your system for some time then that person will be able to make a disk which can crack your login password at any time. You think that you can also change your password, but this is the beauty of the password reset disk that once it is created on your system, it will be able to crack the login password even if later you changed that. So without much focusing on intro, I will create a password reset disk for you step by step. You will need a pendrive for creating password reset disk.

- Insert the pen drive into the victim's computer.
- Navigate to Control Panel>User Accounts
- You will be in front of a screen. In left corner click on the "Create a Password Reset Disk Option" as shown in the picture.



User Accounts
Control Panel > All Control Panel Items > User Accounts
Control Panel Home
Manage your credentials
Create a password reset disk
Configure advanced user profile properties
Change my environment variables
Mayank Prajapati
Local Account
Administrator
Password protected
Forgotten Password Wizard
< Back
Next >
Cancel

Welcome to the Forgotten Password Wizard

This wizard helps you create a "password reset" disk. If you forget the password for this user account and are unable to log on, you can use this disk to create a new password.

Note: No matter how many times you change your password, you only need to create this disk once.

Warning: Anyone can use this disk to reset the password, and therefore have access to this account.

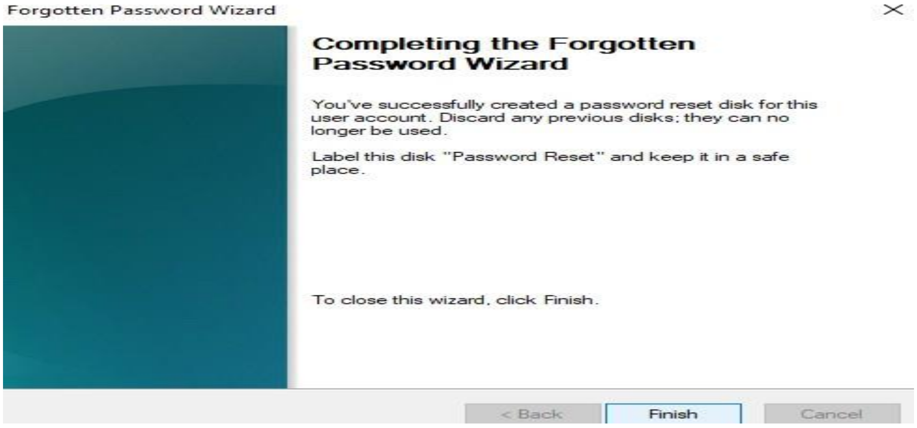
To store password recovery information on a USB flash drive, insert the USB flash drive before clicking Next.

To continue, click Next.

Fig.8. Password Reset Disk wizard

- After clicking on the Next and selecting the Pendrive you have to enter the current password of the system. You can use above method to change the user password.

  After that you will see the dialogue box as below and your pen drive is now converted to password reset disk for victim's system.



Completing the Forgotten Password Wizard

You've successfully created a password reset disk for this user account. Discard any previous disks; they can no longer be used.

Label this disk "Password Reset" and keep it in a safe place.

To close this wizard, click Finish.

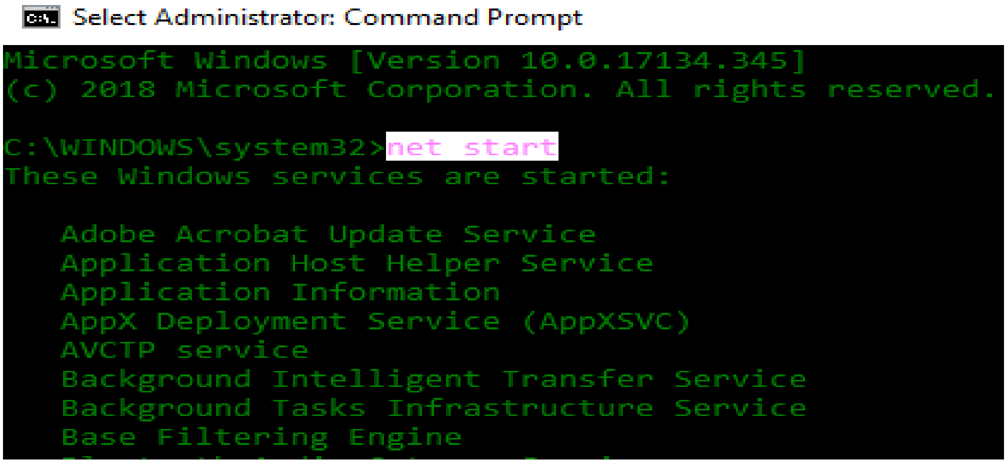
Fig.9. Last step of creating password reset disk

- Click on the Finish button and your pendrive (password cracking device) is ready now. You can reset the login password of the computer system on which this drive is created anytime you want.

6. **Corrupting any running service:**

This method is generally used for bothering the system owner. By using this method we can stop any important service of the system like Audio service etc. This can be done in the following manner.

- Open cmd as Adminstrator
- Type the command "net start" to see all the running services on the system.

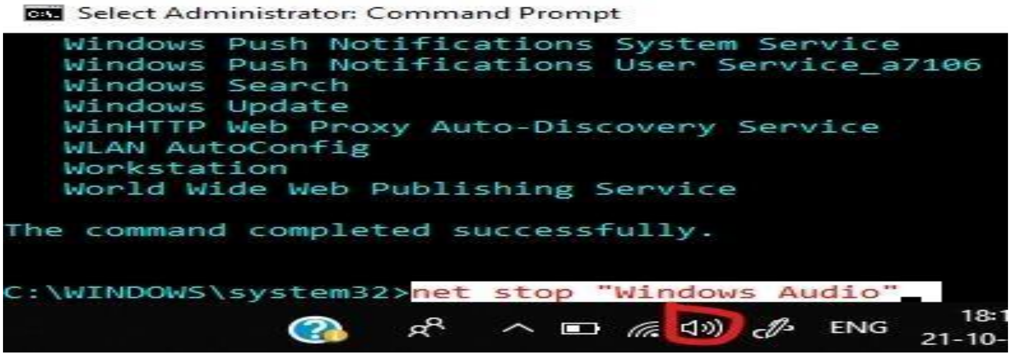


Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net start
These Windows services are started:

   Adobe Acrobat Update Service
   Application Host Helper Service
   Application Information
   AppX Deployment Service (AppXSVC)
   AVCTP service
   Background Intelligent Transfer Service
   Background Tasks Infrastructure Service
   Base Filtering Engine
```

Fig.10. Detecting all running services on windows operating system

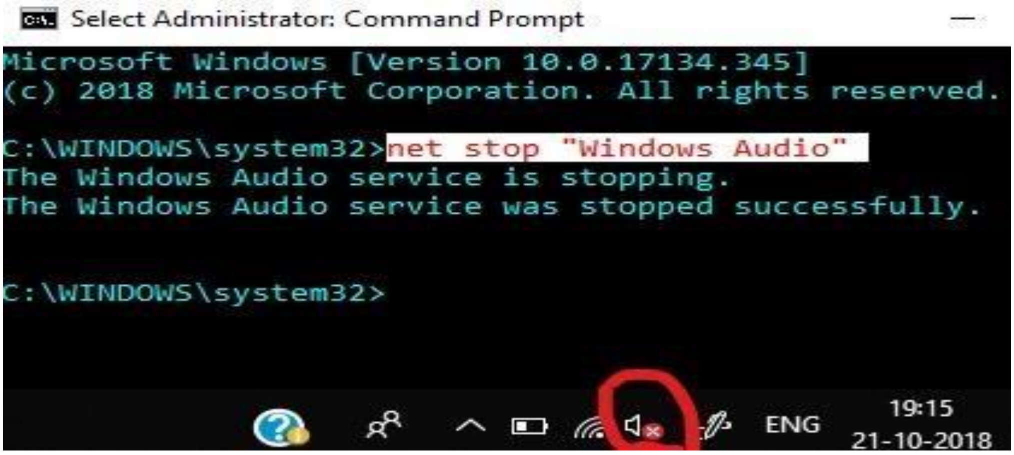
- Suppose we want to stop the audio service. The command that we have to type for stopping the Audio Service is as “net stop “Windows Audio””. You will notice the difference on the icon of Audio when we hit enter after typing this command. The audio option becomes unusable due to this command. This can be clearly shown in the pictures below.



Select Administrator: Command Prompt

```
   Windows Push Notifications System Service
   Windows Push Notifications User Service_a7106
   Windows Search
   Windows Update
   WinHTTP Web Proxy Auto-Discovery Service
   WLAN AutoConfig
   Workstation
   World Wide Web Publishing Service

The command completed successfully.

C:\WINDOWS\system32>net stop "Windows Audio"
```

Fig.11. Before stopping Audio Service



Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net stop "Windows Audio"
The Windows Audio service is stopping.
The Windows Audio service was stopped successfully.


C:\WINDOWS\system32>
```

Fig.12. After stopping Audio Service

- Now your goal is achieved and Windows Audio Services stopped successfully. No sound will came from the system even if the user try to increase the volume, nothing will going to be happen.

IV. PREVENTION METHODS OR TECHNIQUES:

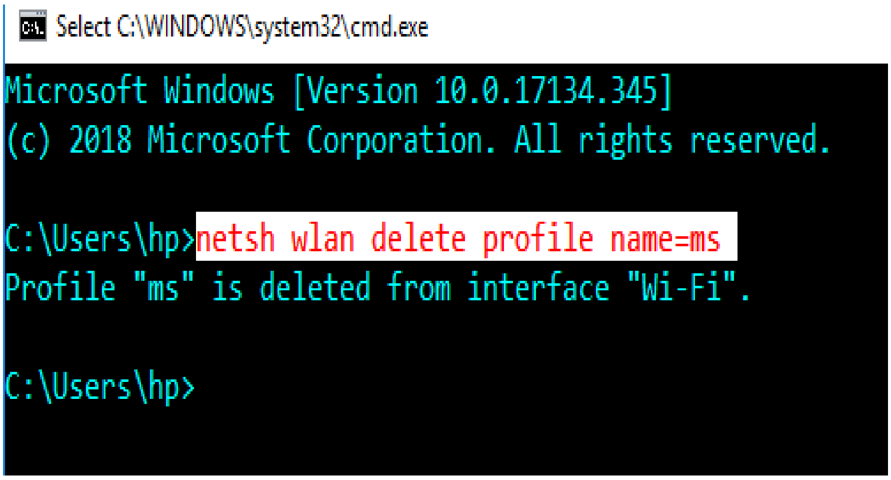
This is going to be the most important section for you, as I will try to secure our system even if there is such a condition arises, in which we have to handover our system to other untrusted person. So before giving your system to another person you can secure yourself to some extent. But I will advise you not to handover your system to untrusted person because with physical access anyone can do anything with your system. Some of the methods to secure your self are explained below:

1. **Deleting wifi password using netsh command:**

As I have explained earlier that even a noob hacker can view your wifi saved passwords using the netsh command, so here is the solution of that. You know which wifi you are using regularly and you don’t want to share or compromise the credentials to anyone then you can also delete that wifi name or password from the list of saved password. The steps are as follows.

- Open cmd as administrator.

- Type the following command to delete the profile from the saved list.
  “netshwlan delete profile name=ms”



```
Select C:\WINDOWS\system32\cmd.exe

Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\hp>netsh wlan delete profile name=ms
Profile "ms" is deleted from interface "Wi-Fi".

C:\Users\hp>
```

Fig.13. Deleting a wifiessid(wifi network) from your system

- Now your wifi network credentials are successfully removed from the saved list and another person will not be able to see your wifi password.

2. **Hiding your entire volume:**
   Suppose you have to give your pc to someone in absence of you. Then you can place all your important data into a volume. After that you can hide that volume in the following manner.

- I have 3 volumes on my PC as you can see named C, M and H.

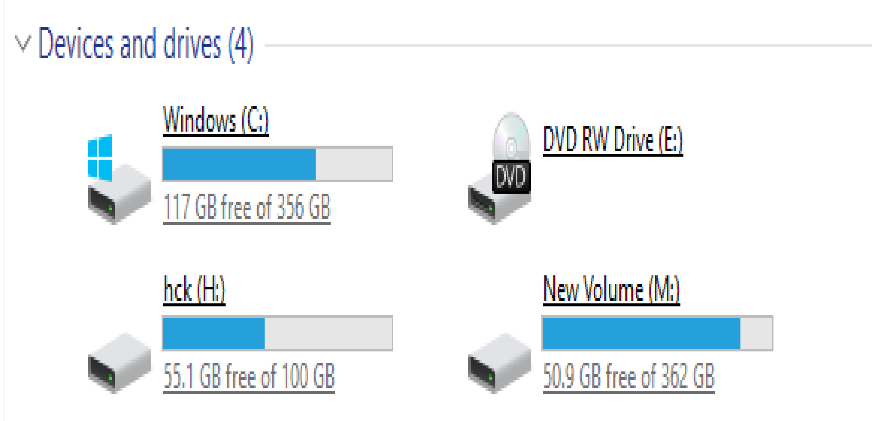
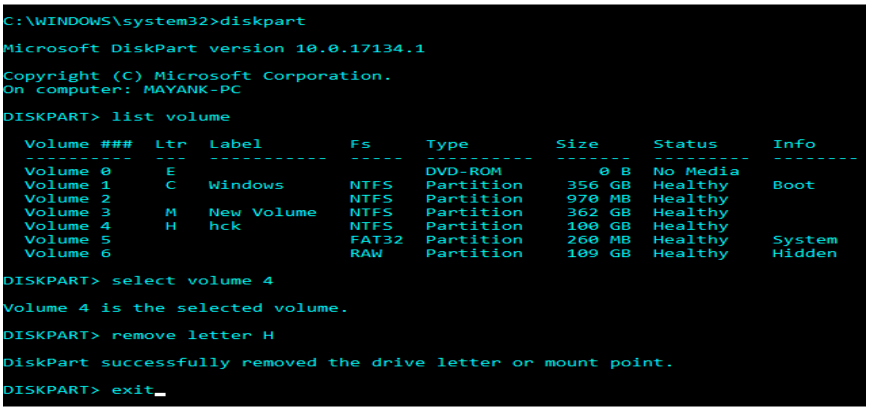


Fig.14. Volumes on our pc before hiding

- I have moved all my important data to H volume. Now we have to open the cmd as usual in administrator mode.
- Type these commands one by one.
- diskpart
- list volume
- select volume “VolumeNumber”
- remove letter “Letter”
- exit



```
C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: MAYANK-PC

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E                       DVD-ROM        0 B  No Media
  Volume 1     C   Windows      NTFS   Partition    356 GB  Healthy    Boot
  Volume 2                      NTFS   Partition    970 MB  Healthy
  Volume 3     M   New Volume   NTFS   Partition    362 GB  Healthy
  Volume 4     H   hck          NTFS   Partition    100 GB  Healthy
  Volume 5                      FAT32  Partition    260 MB  Healthy    System
  Volume 6                      RAW    Partition    109 GB  Healthy    Hidden

DISKPART> select volume 4

Volume 4 is the selected volume.

DISKPART> remove letter H

DiskPart successfully removed the drive letter or mount point.

DISKPART> exit_
```

Fig.15. Demonstration of hiding of volume on pc

- You will see now that volume labelled with H letter is removed and your private drive is not visible to anyone. Note that anyone can again be able to see your data in this volume but anything is better than nothing. So we can use this trick.

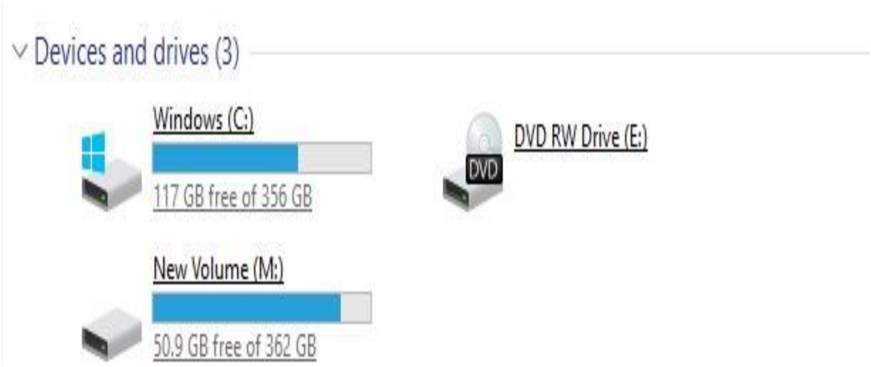
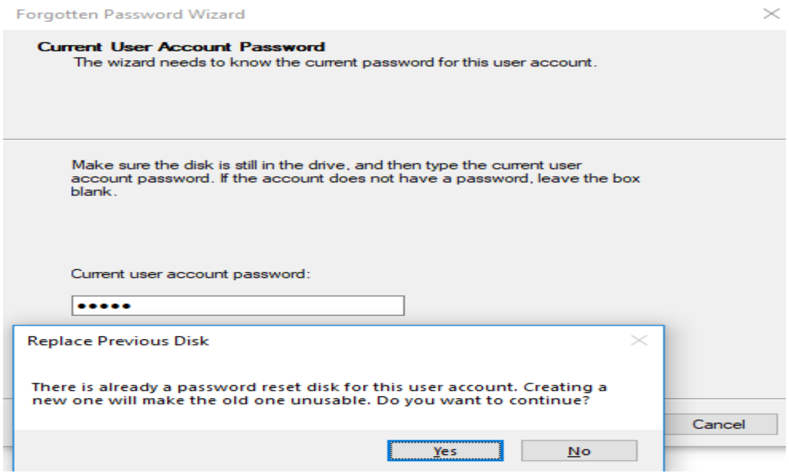


Fig.16. Volumes on pc after hiding

3. **Checking if someone has created password reset disk for your pc:**
   We can also check if someone has already created a password reset disk for our system or not. As explained earlier password reset disk is any physical drive created once on someone pc able to reset the login password of that system at any time. The steps are same as explained above in “Creating password Reset Disk” section.
   It will give you a warning at last step that password reset disk is already created for this pc. If you create new one then old disk will be unusable. In this way you can prevent your pc from serious trauma.


Forgotten Password Wizard

Current User Account Password

The wizard needs to know the current password for this user account.

Make sure the disk is still in the drive, and then type the current user account password. If the account does not have a password, leave the box blank.

Current user account password: •••••

Replace Previous Disk

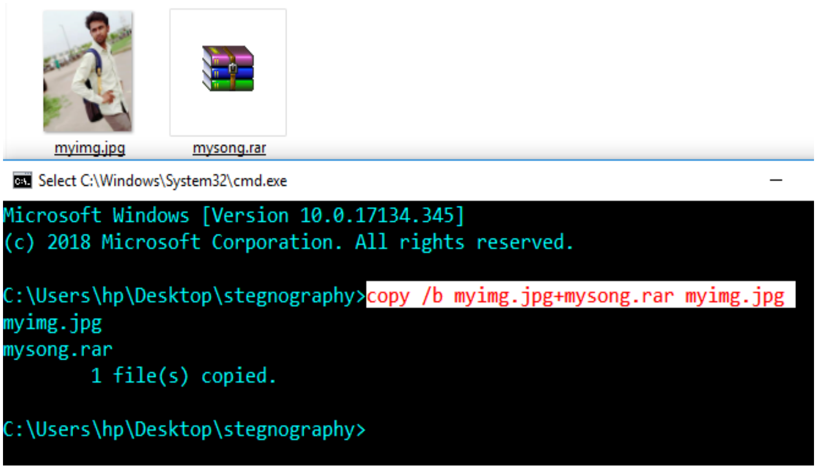
There is already a password reset disk for this user account. Creating a new one will make the old one unusable. Do you want to continue?

Fig.17. Detecting if someone already created password reset disk for your pc

Choose “Yes” and simply you have ruin the hacker’s evil thought and enjoy.

4. **Steganography:**
   Steganography means “covered writing”. Steganography is way of hiding data, video, audio files etc behind another file. It can be used with cryptography to provide more security to the data. In windows operating system we can achieve steganography by some methods with software and without software also. Now I am going to hide my audio file within an image file. The audio file name is “myaudio.mp3” and image file name is “myimg.jpg”.
   The steps to be followed are given below:

- Right click on the myaudiomp3 file and choose “Add to archive” option. Delete mysong.mp3 file. Now you have two files named as “mysong.mp3” and “myimg.jpg” files.
- Now open cmd as usual and navigate to the directory where you have placed these two files and execute the following command.
  copy/b myimg.jpg+mysong.rar myimg.jpg

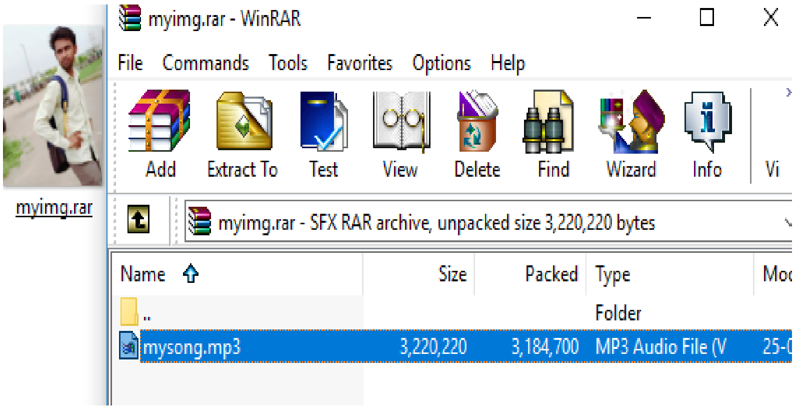


```
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\hp\Desktop\stegnography>copy /b myimg.jpg+mysong.rar myimg.jpg
myimg.jpg
mysong.rar
        1 file(s) copied.

C:\Users\hp\Desktop\stegnography>
```

Fig.18. Hiding command

Now delete mysong.rar file also. You will be amazed to know that your audio file is now behind the image file in rar format but you and anyone not able to see it directly.

You can view your file simply by changing the extension of the image file to rar and the myimg.rar file you can extract your audio file as well.



myimg.rar - SFX RAR archive, unpacked size 3,220,220 bytes

Name	Size	Packed	Type	Moc
..			Folder	
mysong.mp3	3,220,220	3,184,700	MP3 Audio File (V	25-(

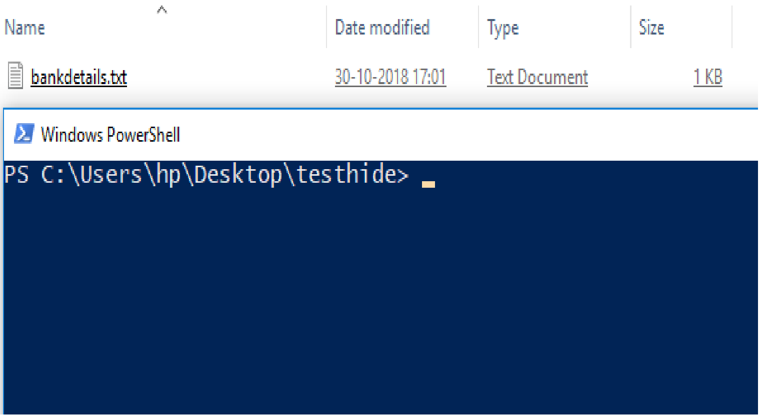
Fig.19. Audio file detection

This is the simple but effective method of hiding your personal files so that no one is able to access them even if they have physical access to your system.

5. **Hiding any file or folder as a system folder:** We can also hide our important file by converting these files into system file. Similar can be applied to folder also. The steps for hiding or converting any file into system file are given below. When a file becomes system file, it will not be visible.

- Open command prompt and navigate to that directory where your file is present (You can also open powershell in windows10 and do the same steps below)

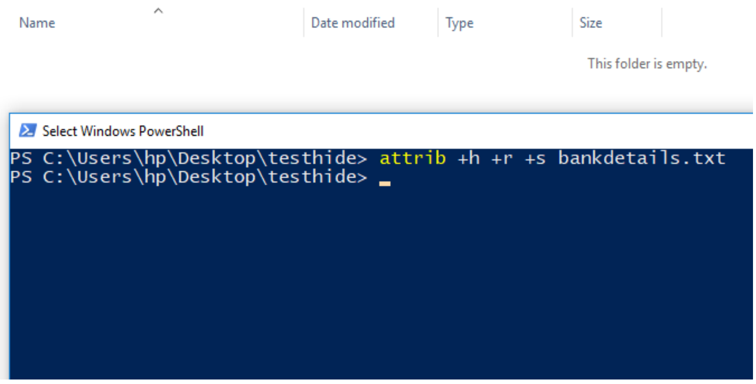
- Type the following command:
  "attrib +h +r +s filename.extension" Here file name is bankdetails.txt
  The pictures before and after executing this command are shown below.



Name	Date modified	Type	Size
bankdetails.txt	30-10-2018 17:01	Text Document	1 KB

```
PS C:\Users\hp\Desktop\testhide> _
```

Fig,.20. File is visible before executing the hiding command



Name	Date modified	Type	Size

This folder is empty.

```
PS C:\Users\hp\Desktop\testhide> attrib +h +r +s bankdetails.txt
PS C:\Users\hp\Desktop\testhide> _
```

Fig.21. File is not visible after executing the command

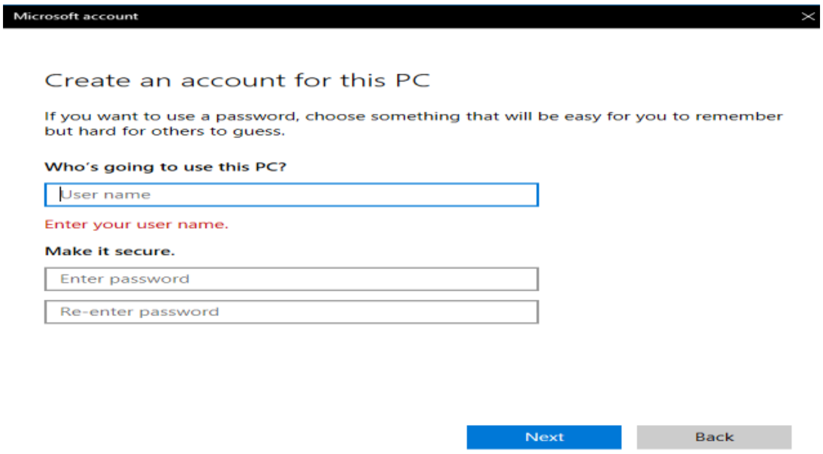
- Here in this command h stands for hidden, r for read only and s stands for system file. When you want to unhide the file simply type the command as:
  "attrib -h -r -s bankdetails.txt"
  In this way you can hide or unhide your important files and folders.

6. Creating a new user for your friends:

You can also create a new user for your friends, family and some other persons. This new user has not more privileges as compared to administrator user. So whenever there such condition arises in which you have to give physical access to your system to anyone. Then just login with new user and handover your system to that person. But we cannot say that your system is completely secure now, although it is secure to some extent now.

The steps for creating new or guest user in windows10 are much simpler.

- Type control panel in the search box and hit enter.
- Go to User Accounts> Manage Another Account>Add a new User in pc setting> Add someone to this pc
- Simply follow all the steps and fill required information and that's all about it.



Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

User name

Enter your user name.

Make it secure.

Enter password

Re-enter password

Fig.22. Creating a new user account in windows10

V. CONCLUSION AND TIPS OF SECURITY:

After reading and implementing all the methods of simple hacks and their prevention, we can conclude to the following points.

- Never ever give physical access to your system to anyone.
- Don't trust anyone in this computerized age as it may lead to privacy risk.
- Always create a guest user for family or friends so that they have limited access to your system and not able to do wrong things.
- You can secure your system with BIOS or power on password also.
- Don't use corrupted pendrive or any physical drive in your system.
- Always stay updated, some people think that windows updates are comes for data consume purpose only. But this is not true; they are working harder day by day for making our digital life more secure and better.
- Turn your windows defender and firewall always on.
- Purchase good antiviruses programs for more security.
- If you have any suspect then check your task manager if there are unknown process running stop them immediately using End Button.
- Use IDS(Intrusion Detection System) if you are the owner of the organisation to detect who is spying on you and for tracing them.

REFERENCES

[1] Daniel W. Dieterle "Basic security testing with kali linux

[2] Digital Cop Book "SahilBaghla"

[3]Er. **SahilBaghla** "EH1 infotech"

[4] Vinay Gupta "EC Council"

[5] Vivek Ramachandran "Backtrack5 Wireless Penetration Testing"

[6] Cyber Security Awareness Program "Innovative Ideas Infotech

[7]Workshop "Cyber Security awareness program" "SahilBaghla"