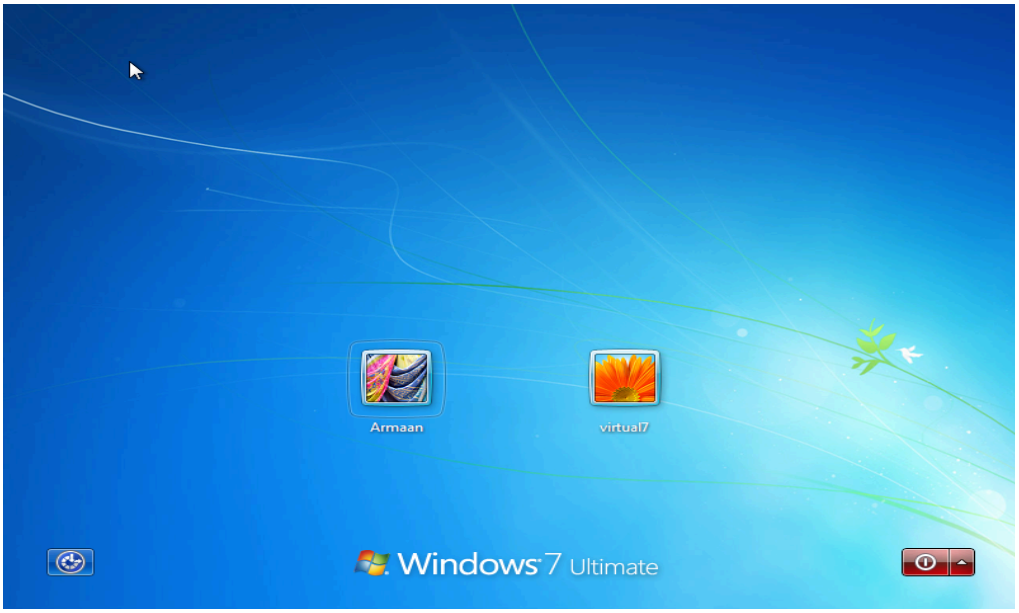
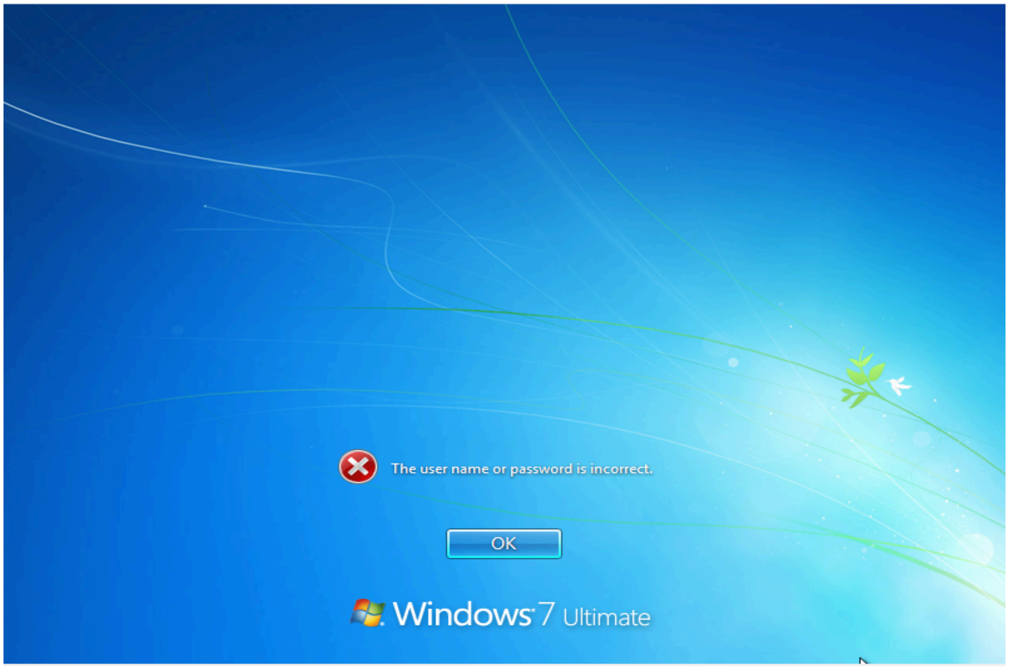
OPHCRACK TOOL

Crack the password of a windows machine by using the ophcrack tool in the virtual machine on windows 7 and try get the password, along with that mention the path of the SAM file in windows and explain about SAM file usage and how it can be cracked by tool.

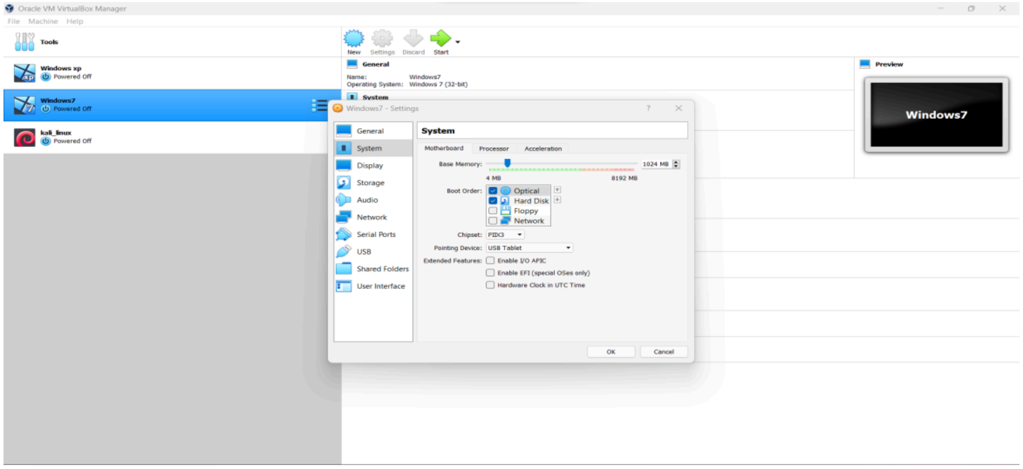
STEP 1: Start your Windows 7 on virtual box. You can see there are 2 accounts.



STEP 2: You do not have the password, due to which your access is denied.


The user name or password is incorrect.

STEP 3: Close your Windows 7 and open the settings for Windows 7. Click on system and select ‘Optical’ drive to be the first in boot order.



General

Name: Windows7
Operating System: Windows 7 (32-bit)

System

Base Memory: 1024 MB (4 MB – 8192 MB)

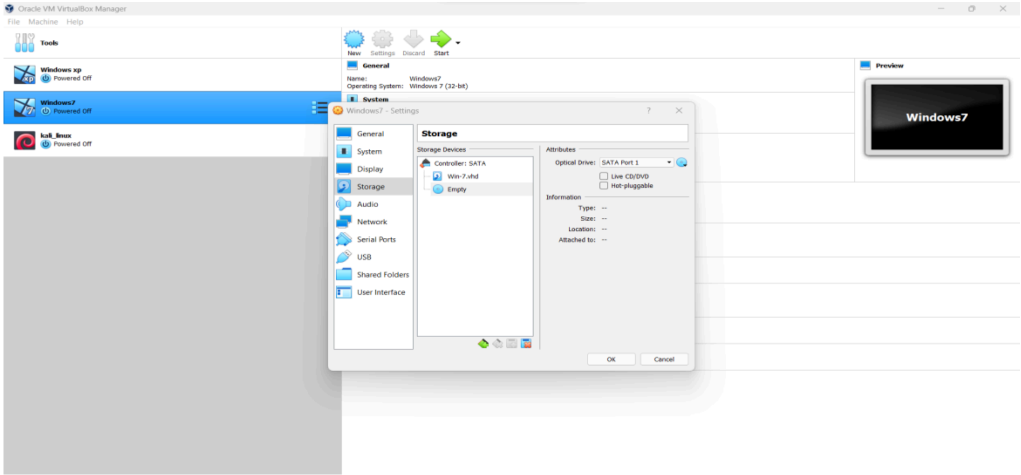
Boot Order:
☑ Optical
☑ Hard Disk
☐ Floppy
☐ Network

Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features:
☐ Enable I/O APIC
☐ Enable EFI (special OSes only)
☐ Hardware Clock in UTC Time

STEP 4: Click on storage and select the empty optical drive option.



General

Name: Windows7
Operating System: Windows 7 (32-bit)

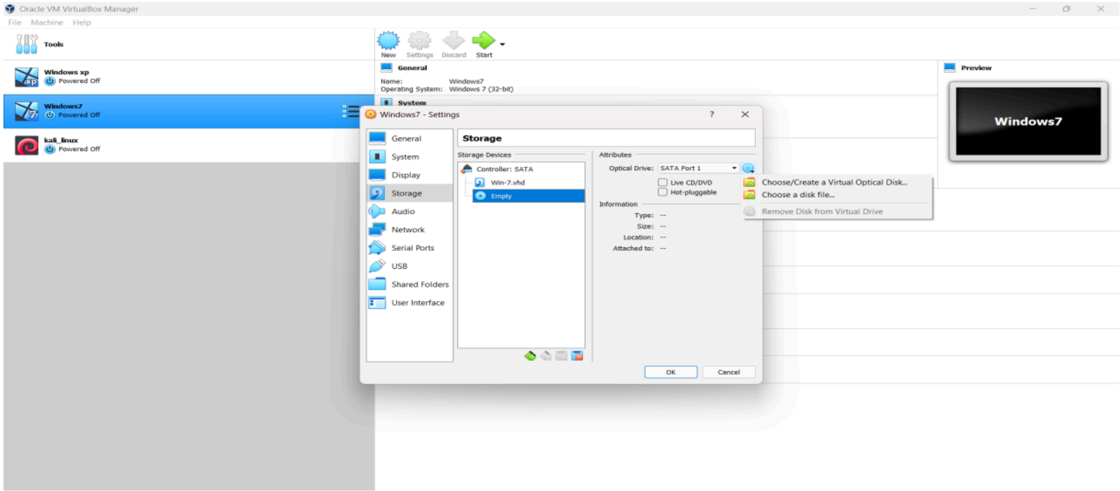
Storage

Storage Devices
Controller: SATA
Win-7.vhd
Empty

Attributes
Optical Drive: SATA Port 1
☐ Live CD/DVD
☐ Hot-pluggable

Information
Type: --
Size: --
Location: --
Attached to: --

STEP 5: Click on the Optical drive menu icon and select the ‘Choose a disk file’ option and upload the ophcrack file.



Name: Windows7
Operating System: Windows 7 (32-bit)

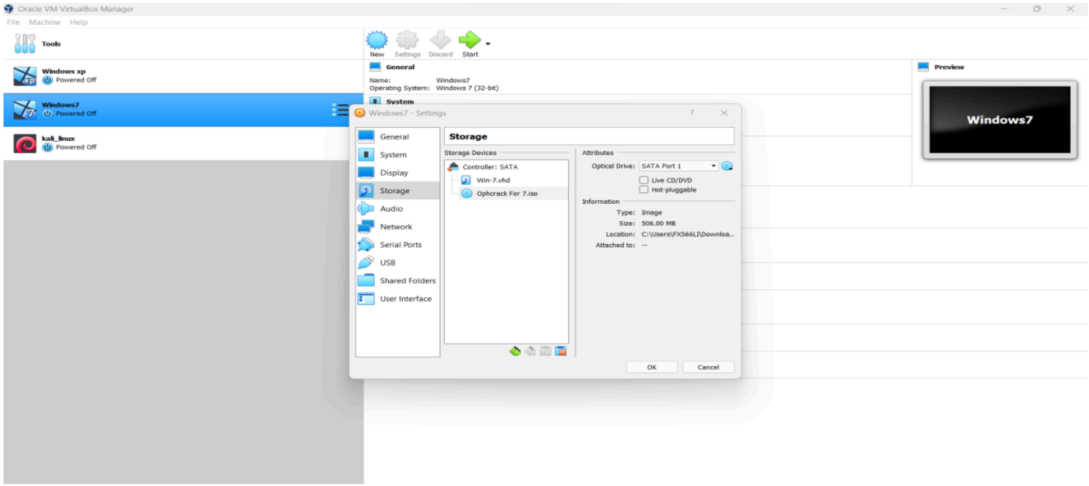
Storage

Storage Devices
Controller: SATA
Win-7.vhd
Empty

Attributes
Optical Drive: SATA Port 1
□ Live CD/DVD
□ Hot-pluggable

Information
Type: --
Size: --
Location: --
Attached to: --

STEP 6: The ophcrack file has been successfully uploaded. Start Windows 7 in your virtualbox.



Name: Windows7
Operating System: Windows 7 (32-bit)

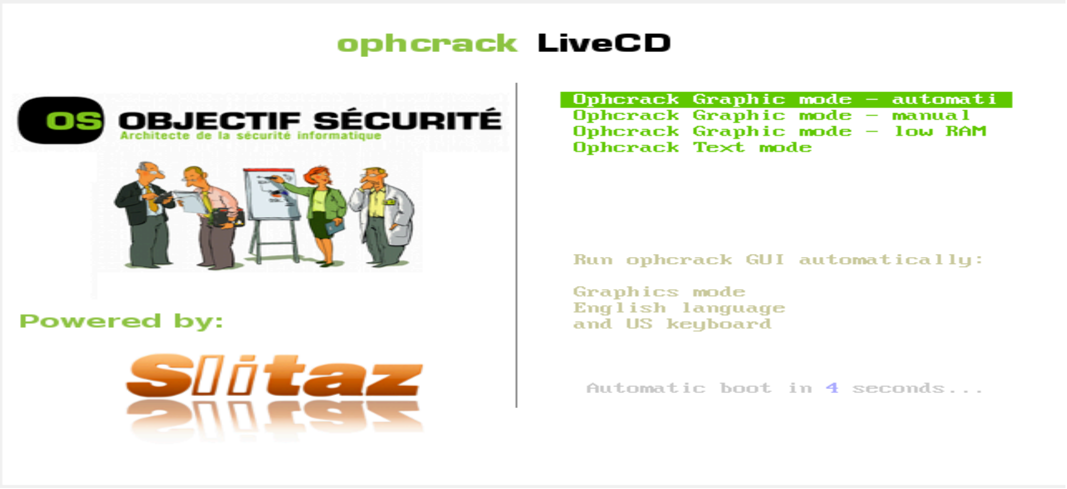
Storage

Storage Devices
Controller: SATA
Win-7.vhd
Ophcrack For 7.iso

Attributes
Optical Drive: SATA Port 1
□ Live CD/DVD
□ Hot-pluggable

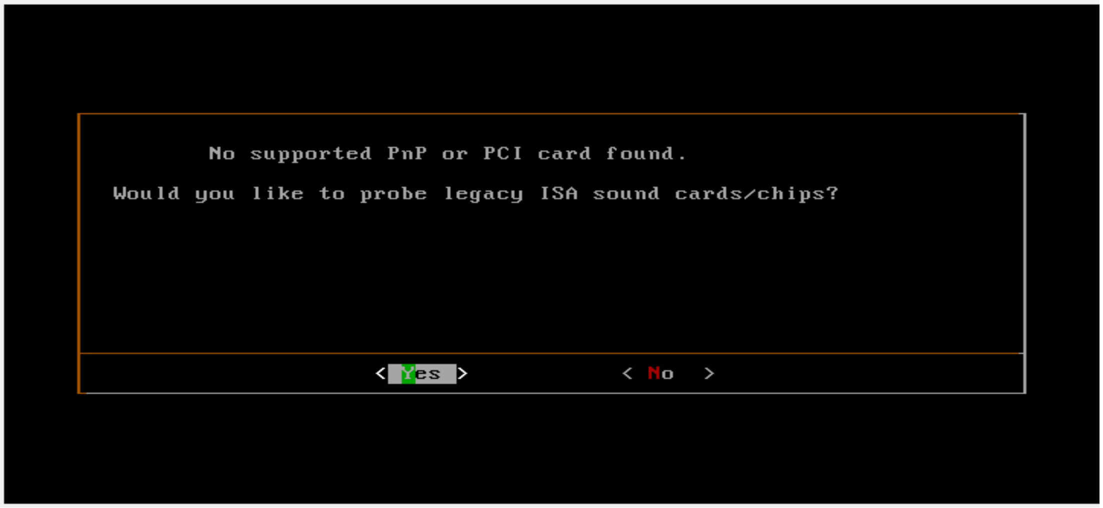
Information
Type: Image
Size: 506.00 MB
Location: C:\Users\FX566LI\Downloa...
Attached to: --

STEP 7: Due to its 1^{st} priority Ophcrack has been loaded.



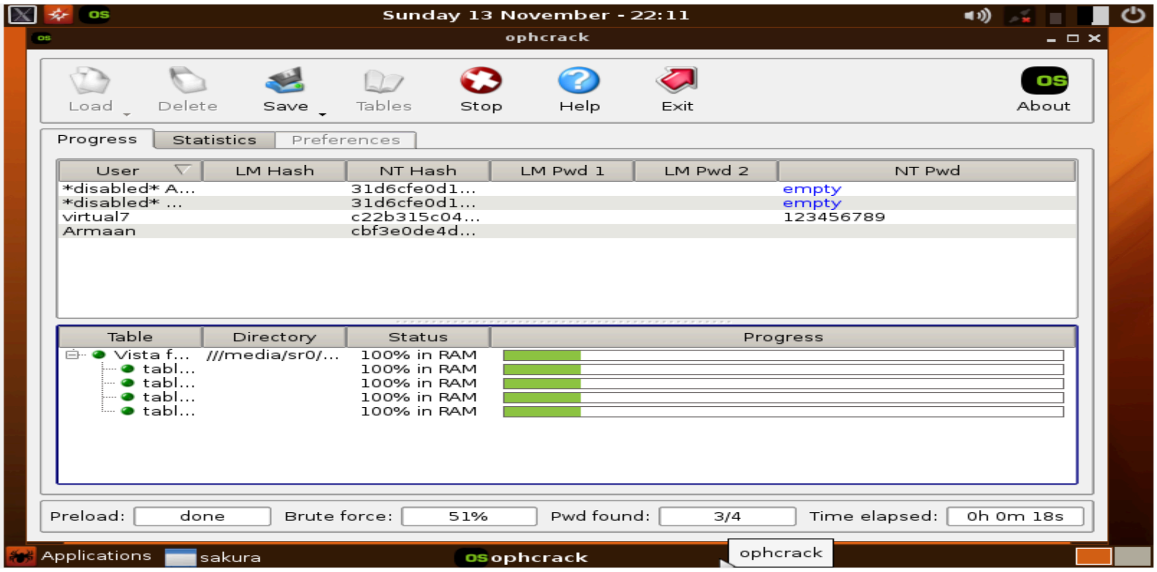
```
Ophcrack Graphic mode - automati
Ophcrack Graphic mode - manual
Ophcrack Graphic mode - low RAM
Ophcrack Text mode

Run ophcrack GUI automatically:

Graphics mode
English language
and US keyboard

Automatic boot in 4 seconds...
```

STEP 8: Click on ‘NO’ or else your system may be jeopardized.



```
      No supported PnP or PCI card found.

 Would you like to probe legacy ISA sound cards/chips?



              < Yes >            <  No  >
```

STEP 9: Ophcrack will start the process of cracking the password. If the password is simple then it will be cracked in seconds but if it has medium difficulty then it will take a while.

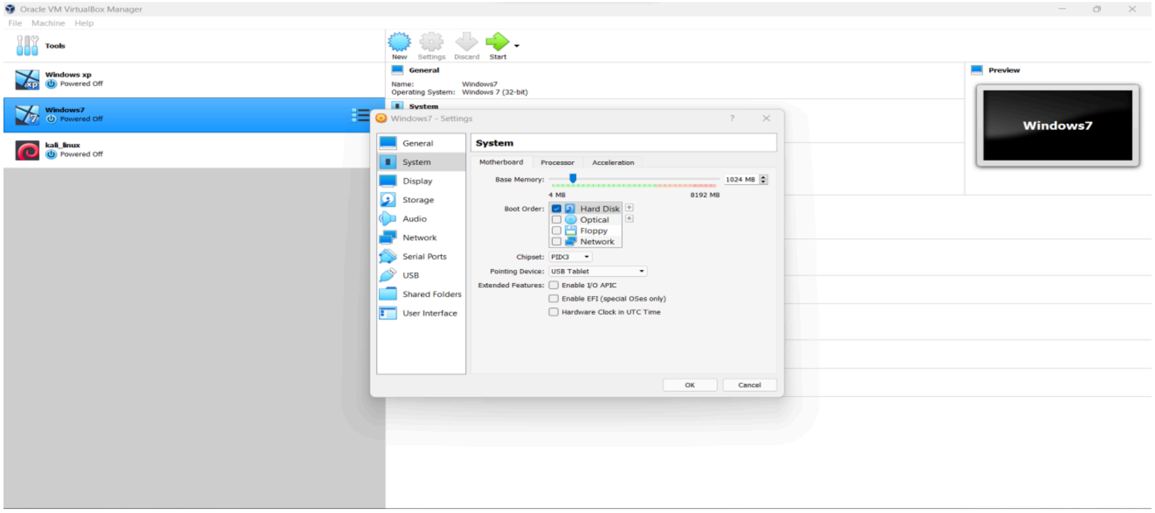


User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
disabled A…		31d6cfe0d1…			empty
disabled …		31d6cfe0d1…			empty
virtual7		c22b315c04…			123456789
Armaan		cbf3e0de4d…			

Table	Directory	Status	Progress
Vista f…	///media/sr0/…		
tabl…		100% in RAM	
tabl…		100% in RAM	
tabl…		100% in RAM	
tabl…		100% in RAM	
tabl…		100% in RAM	

Preload: done Brute force: 51% Pwd found: 3/4 Time elapsed: 0h 0m 18s

STEP 10: Once the password is cracked, close Windows 7 and reset the settings for the Windows 7 in virtual box.



Name: Windows7
Operating System: Windows 7 (32-bit)

System

Base Memory: 1024 MB (4 MB – 8192 MB)

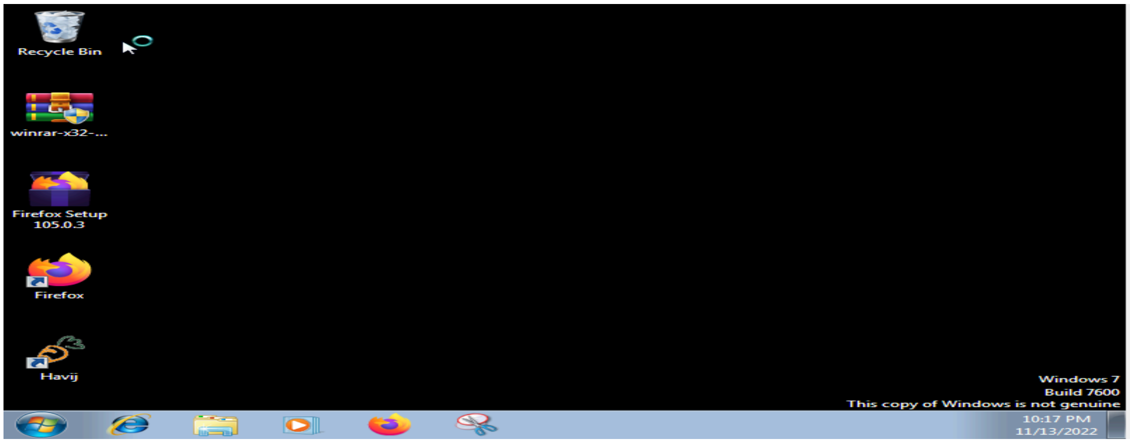
Boot Order:
☑ Hard Disk
☐ Optical
☐ Floppy
☐ Network

Chipset: PIIX3

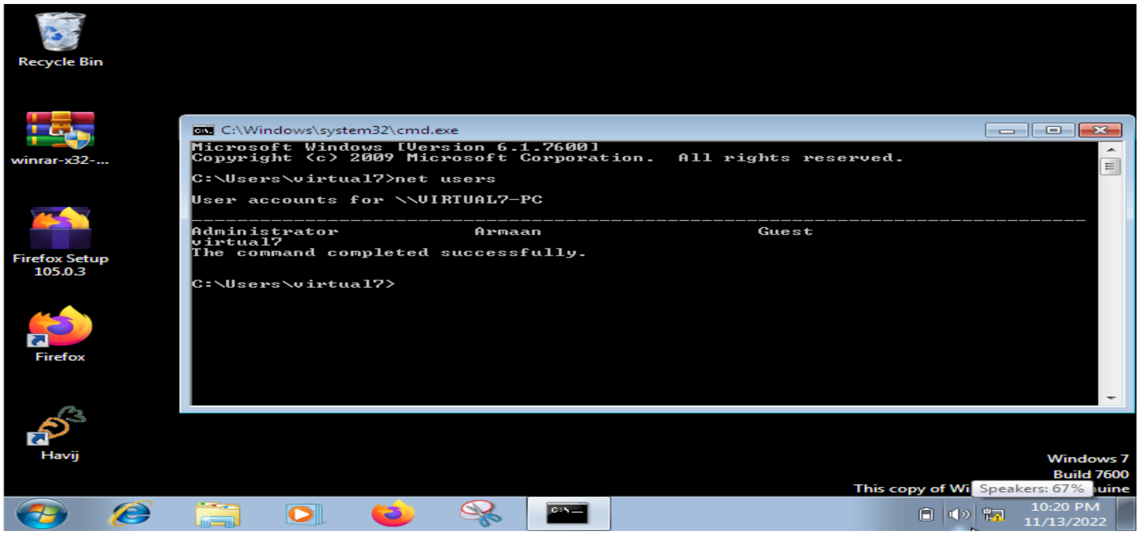
Pointing Device: USB Tablet

Extended Features:
☐ Enable I/O APIC
☐ Enable EFI (special OSes only)
☐ Hardware Clock in UTC Time

STEP 11: No with the passwords we can get access for the user accounts and use Windows normally

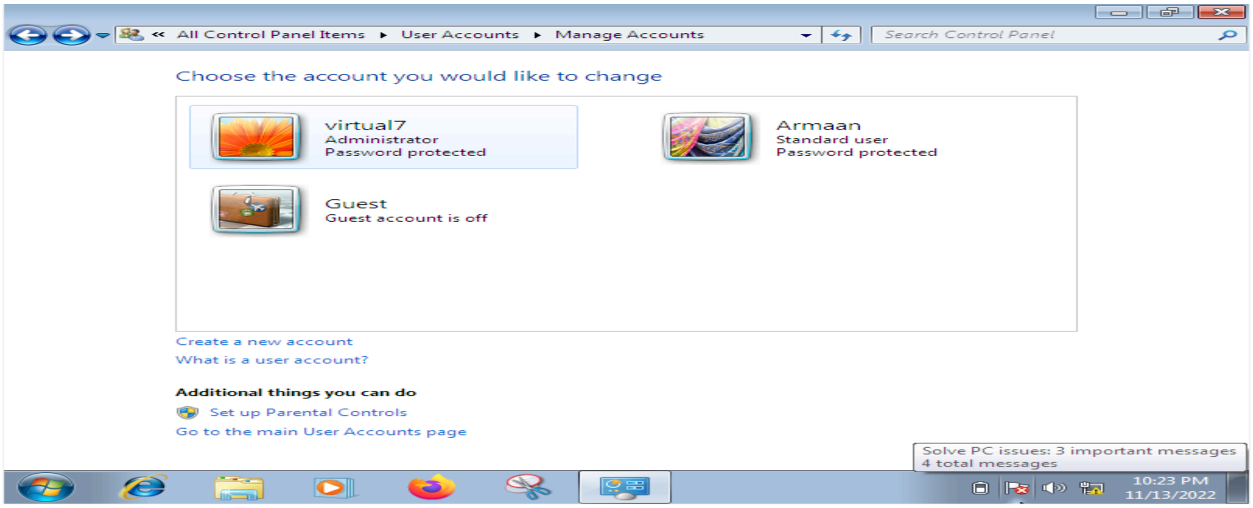


STEP 12: Open the command prompt and enter the command ‘net users’ to get the information about the user accounts.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7>net users

User accounts for \\VIRTUAL7-PC

-------------------------------------------------------------------------------
Administrator            Armaan                   Guest
virtual7
The command completed successfully.

C:\Users\virtual7>
```

STEP 13: Open the control panel. Go for ‘User accounts >> Manage different accounts >> Change passwords’.



Choose the account you would like to change

virtual7
Administrator
Password protected

Armaan
Standard user
Password protected

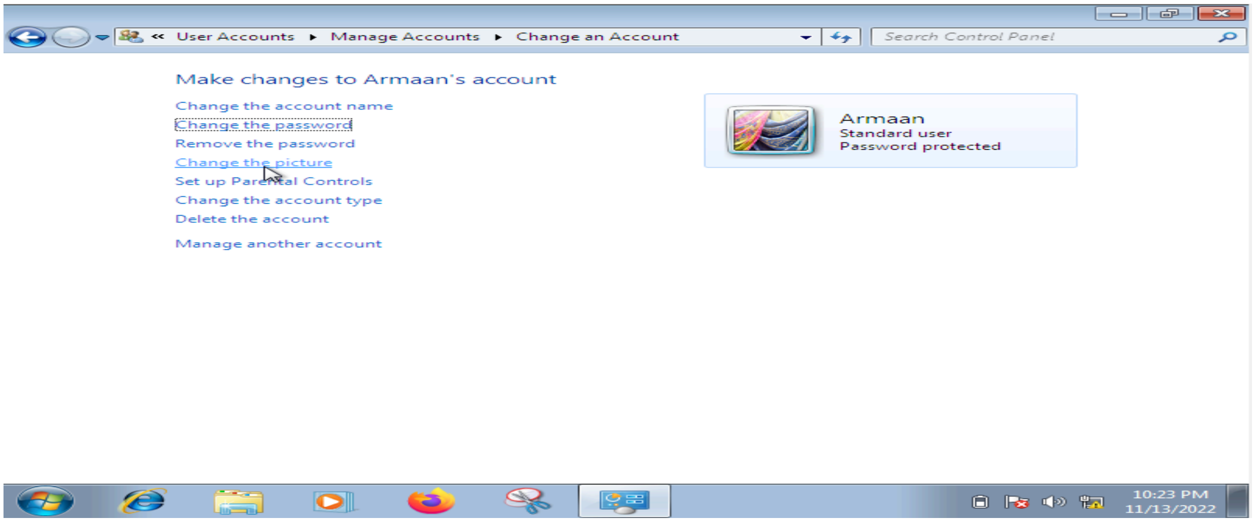
Guest
Guest account is off

Create a new account
What is a user account?

Additional things you can do

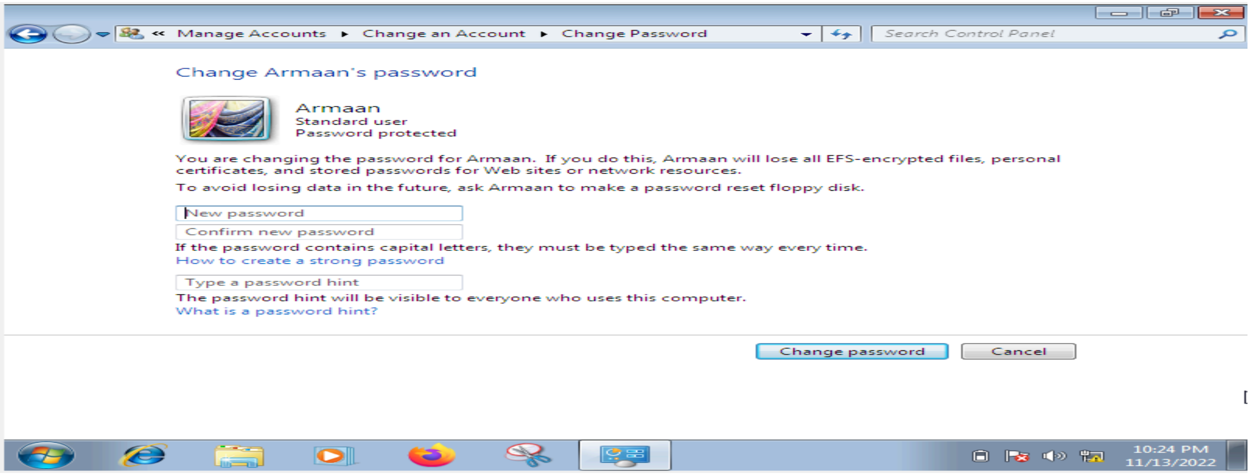
Set up Parental Controls
Go to the main User Accounts page

Solve PC issues: 3 important messages
4 total messages



Make changes to Armaan's account

Armaan
Standard user
Password protected


« Manage Accounts ▸ Change an Account ▸ Change Password
Search Control Panel
How to create a strong password
What is a password hint?
Change password
Cancel
10:24 PM
11/13/2022

Change Armaan's password

Armaan
Standard user
Password protected

You are changing the password for Armaan. If you do this, Armaan will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask Armaan to make a password reset floppy disk.

New password

Confirm new password

If the password contains capital letters, they must be typed the same way every time.

Type a password hint

The password hint will be visible to everyone who uses this computer.

In this way we can change the password for different accounts as well.

- **<u>SAM files</u>**:
  - □ The Security Account Manager (SAM) is a database that is present on computers running Windows operating systems that stores user accounts and security descriptors for users on the local computer.
  - □ If the SAM is somehow deleted in some way while Windows is running, the system loses all user account passwords, resulting in Windows throwing an error exception (Blue Screen) and shutting down.