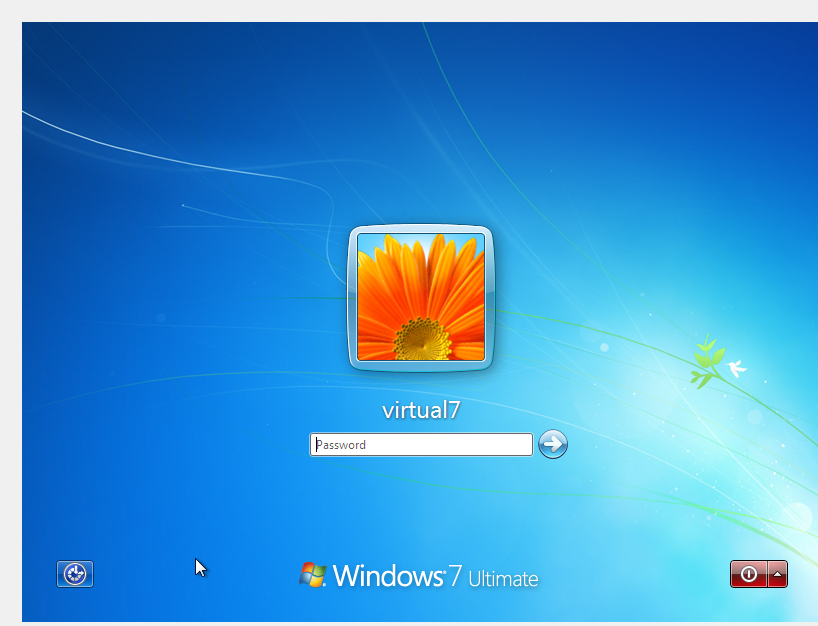
**System Hacking Using Ophcrack**

**Security Account Manager = is the file that stores passwords ,used to authenticate local and remote users**

**So with the the ophrack we can bypass the SAM and load the operating system**

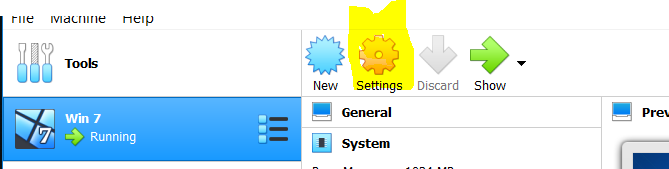
**Steps:**

1. **First step is to obviously install the .iso for ophrack windows 7**
2. **As you can see that my windows is protected by a password , so I turn the system of.**

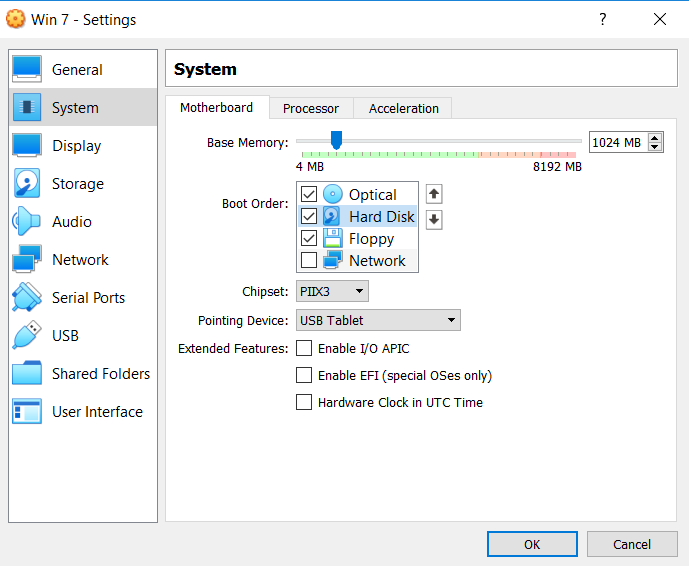


**3)So next we will take ophrack in pen drive or in my case since I am using a virtual machine a disk**

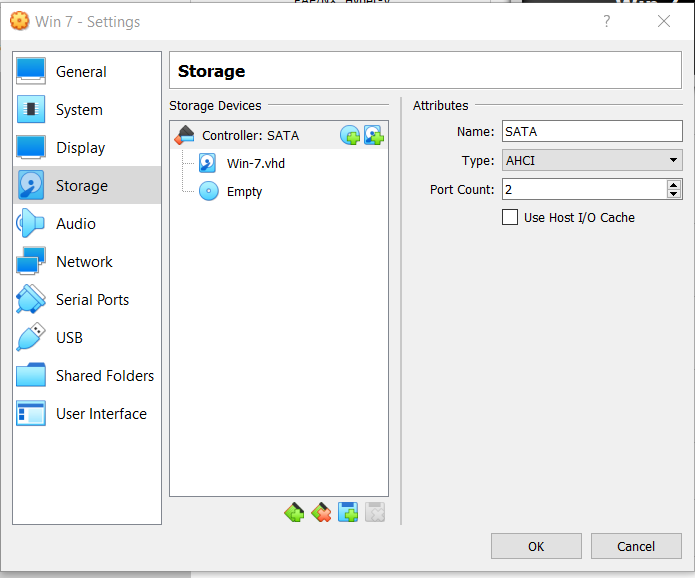
**4)So first I would go to my operating system in oracle and click on settings**



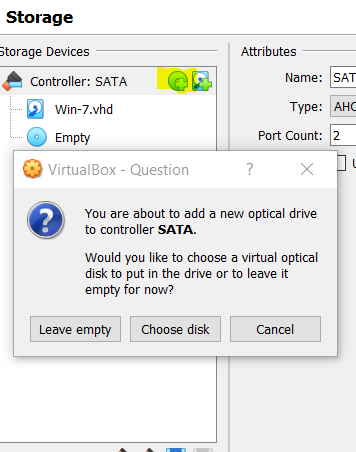
**5)Next in settings we go to systems-> motherboard, in Motherboard->Boot Order, we prioritise ‘Optical’ over ‘Hard Disk’.**



**6)After that we head to storage to add our .iso file**

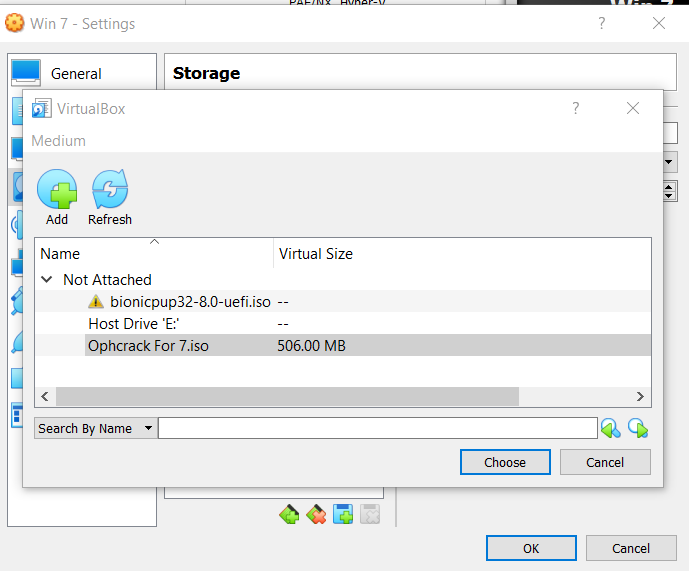


**7) Click on the icon with a disk symbol in it in storage devices and then proceed by clicking ‘Choose disk’**



**8) Click on Add and then locate the folder consisting of the iso file**

**9)Click on the iso file and then select the option Choose**



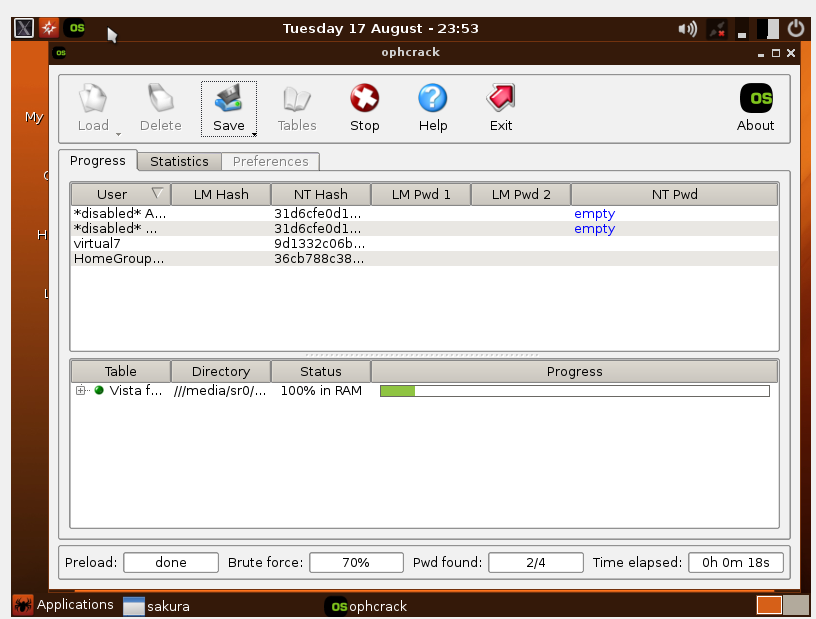
**10) Next click on the iso file and select ok**

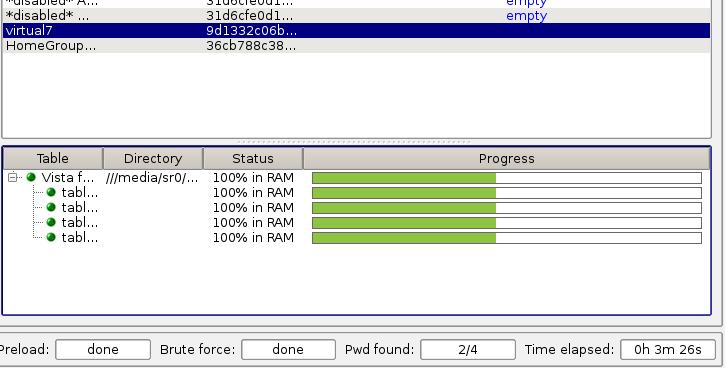
**11)Run our windows os**

**12)Click on ‘yes’ for all the pop ups that are coming and then click Ok**

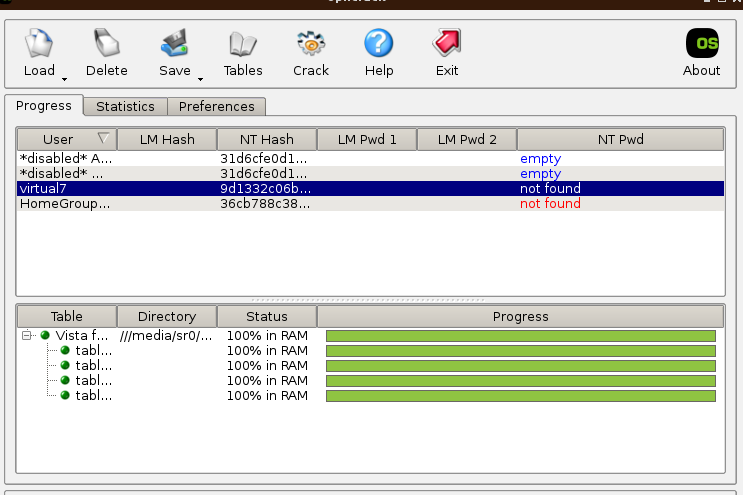


13) After booting is over we come to a screen having ophcrack loaded



**14) To retrieve the passwords wait for the ophcrack to crack the password** 

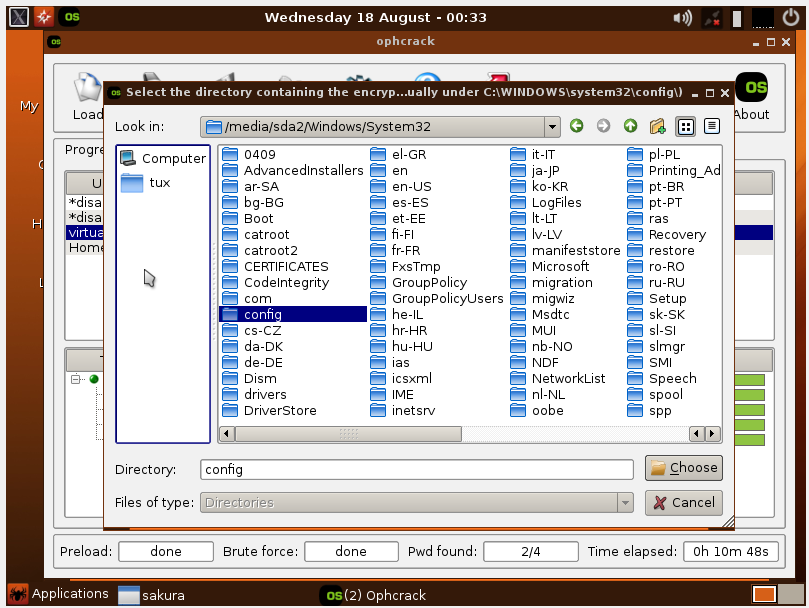
**15) As I don’t have the required rainbow tables my password couldn’t be found**



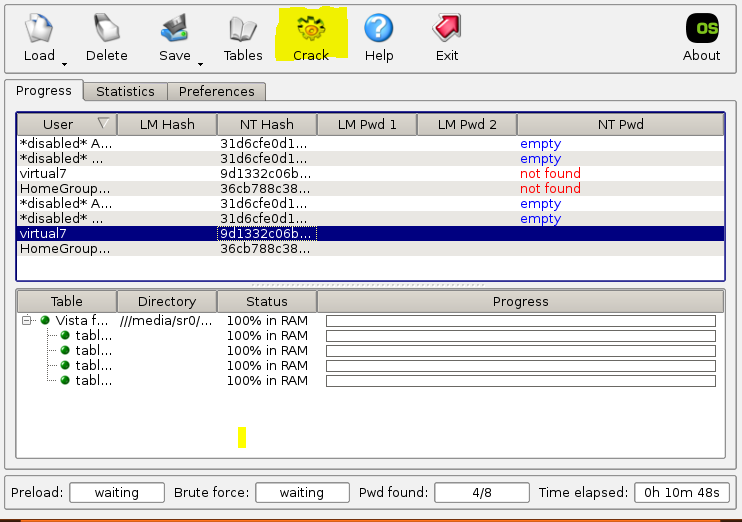
**16)So next click load-> Encrypted SAM, so now I will try to locate the SAM file,**

**File path= Computer->/->media->sd2->Windows->System32**

**After finding the config file , click choose**

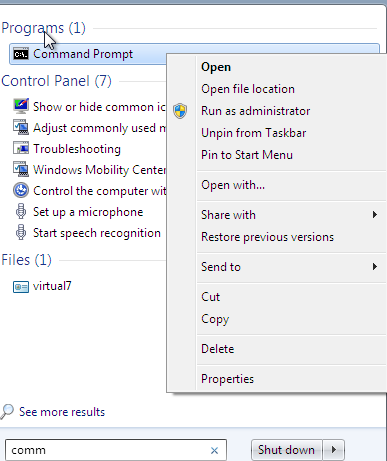


**17)Next click on Crack**



**RESETING PASSWORD WITHOUT KNOWING OLD WITH THE HELP OF COMMAND PROMPT**

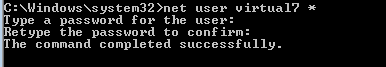
1. **Search for command prompt then right click and select Run as Administrator**



1. **In cmd prompt enter the command net user to view all the accounts**



1. **Next type net user ‘USERNAME ‘ \* and then change the password**

****