Windows Password Recovery|Crack Windows XP or Vista Password Using Ophcrack

Labels: How To, Password, Windows

What will you do if you forget your Windows XP or Vista Password? The very first thing you should try is to go to safe mode and check whether you have set your administrator password. But if the administrator password is also set then you may be thinking the only way is to format the computer and install fresh Windows XP or Vista. Well, here I am going to suggest a method here that will simply recover your lost passwords, both administrator and user in few seconds or at most some minutes without installing any software or without breaking your head. But if you are not interested in recovering the password or you simply want to **reset or delete** the password then there is much easier technique which requires only a 3 MB file instead of Ophcrack. Just see how to Reset windows Password Using a USB drive or a CD

Here, We will be using a software called Ophcrack which is an open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables. But you may be thinking whether it is a legal one. Yes it is completely legal according to Wikipedia. But you should not use this software for illegal purposes like unauthorized access to other’s system. I have tried this method in Windows XP, Windows Vista, and Windows 7 Beta and it works perfectly fine for an alphanumeric password length up to 14.

The method is a very simple one. You just need to download the software which is 452MB for XP and 532MB for Vista or Windows 7. Ophcrack comes in bootable Live CD 2.1.0 ISO and installation files. Here we will be using the Live CD method where no installation is required. Follow the steps below:

Step 1: Download the ISO File For Ophcrack Live CD 2.1.0 From the links below: (Choose according to your operating system)

Windows XP:

Size: 452 MB

http://downloads.sourceforge.net/ophcrack/ophcrack-xp-livecd-2.1.0.iso

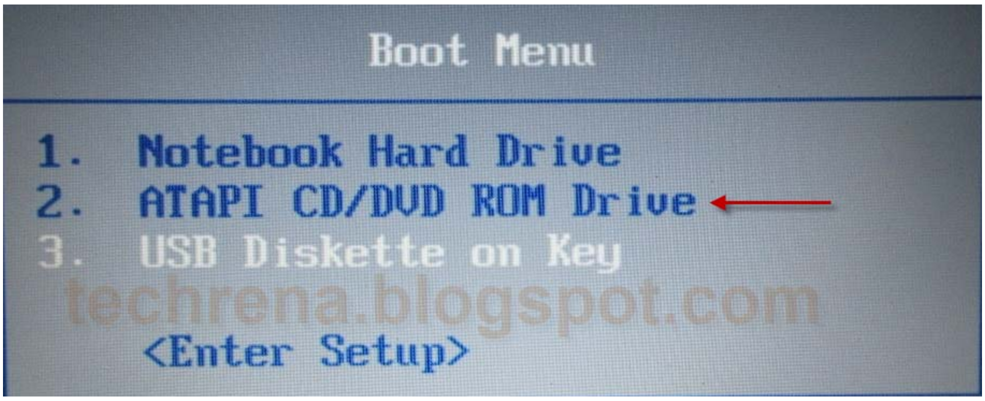
Windows Vista or 7:

Size: 532 MB

http://downloads.sourceforge.net/ophcrack/ophcrack-vista-livecd-2.1.0.iso

Step 2: After the download is completed successfully burn the ISO file to a CD using a burning software. ISO files can be directly burnt (Just open with burners like Nero etc.). You should not use data mode or any other mode to burn. The CD is a bootable one. But if you do not want to use a CD, you can very well use a USB Flash Drive to run the program. Click here To see the USB Boot Technique.

Step 3: Insert the CD to your CD/DVD drive. Restart the System. You need to set the boot order to Boot from CD as the first option if you have not set CD drive as the first option. To do this you need to go to bios setup and change the order. For most of the systems the keys like DELETE, F10, F2, F12 etc are used for going to the Bios setup. But here I have used the Boot Menu Key which will show the available boot options during start up. For my System(HP) the boot menu key is Esc. For Compaq Systems it is usually F9. So if you know the Boot menu key then no need to change the order. Just Select CD/DVD ROM from the menu.

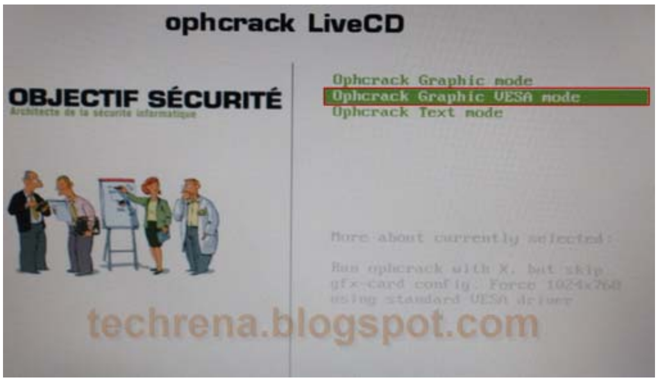


Boot Menu

1. Notebook Hard Drive
2. ATAPI CD/DVD ROM Drive
3. USB Diskette on Key

<Enter Setup>

Step 4: After booting from the Live CD, wait for it to load and select Ophcrack VESA mode(Recommended). If you have a graphics card you can try Graphics Mode.

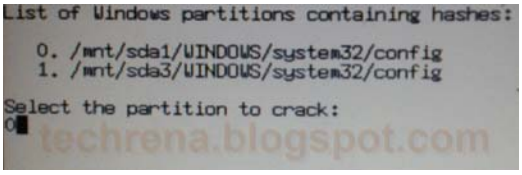


```
Ophcrack Graphic mode
Ophcrack Graphic VESA mode
Ophcrack Text mode

More about currently selected:

Run ophcrack with X, but skip
gfx-card config. Force 1024x768
using standard VESA driver
```

Step 5: If you have more than one partition containing the password hashes it will ask you to select one. But most of the computers will have only one hash partition, so you may not see this step. Select any partition and try if it asks you as shown below.

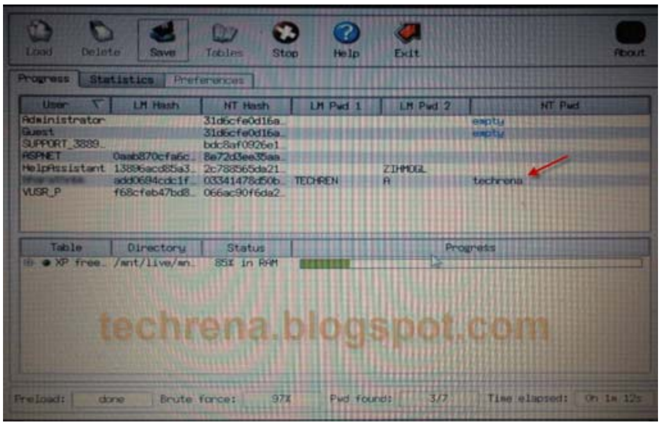


```
List of Windows partitions containing hashes:

  0. /mnt/sda1/WINDOWS/system32/config
  1. /mnt/sda3/WINDOWS/system32/config

Select the partition to crack:
0
```

Step 6: Wait for Ophcrack to run and find your password. After getting the password you need,you can simply click exit even if the progress is not 100%. No need to wait till end.



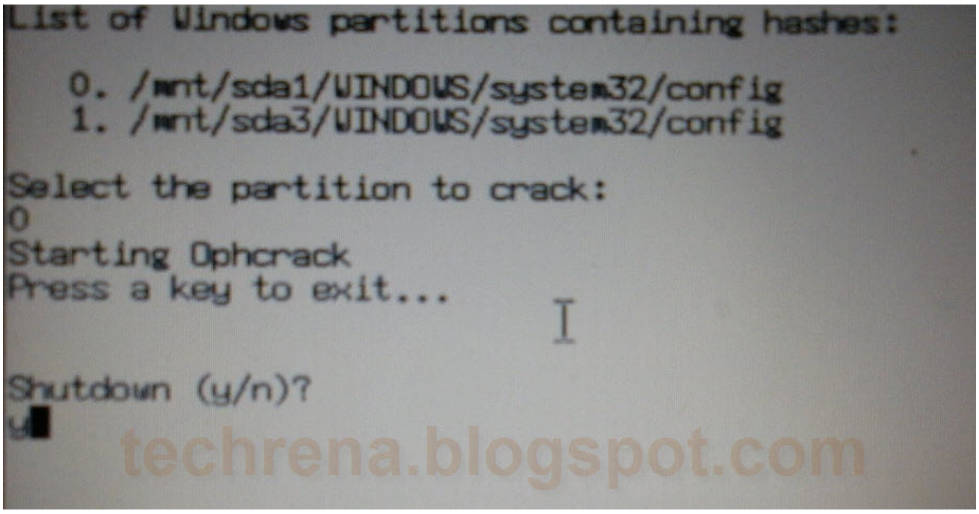
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		31d6cfe0d16a…			empty
Guest		31d6cfe0d16a…			empty
SUPPORT_3889…		bdc8af0926e1			
ASPNET	0aab870cfa6c…	8e72d3ee35aa…			
HelpAssistant	1389бacd85a3…	2c788565da21…		ZIHMOGL	
[redacted]	add0694cdc1f…	03341478d50b…	TECHREN	A	techrena
VUSR_P	f68cfeb47bd8…	066ac90f6da2…			

Table	Directory	Status	Progress
● XP free…	/mnt/live/mn…	85% in RAM	

Preload: done   Brute force: 97%   Pwd found: 3/7   Time elapsed: 0h 1m 12s

Here I had set the password as techrena. It took around 1 min 20 sec to find this password.

Step 7: After the process it will ask you to press any key to exit Ophcrack. Then Type ‘y’ to shutdown the System.



```
List of Windows partitions containing hashes:

   0. /mnt/sda1/WINDOWS/system32/config
   1. /mnt/sda3/WINDOWS/system32/config

Select the partition to crack:
0
Starting Ophcrack
Press a key to exit...

Shutdown (y/n)?
y
```

Now start your system. Enter the password you have found. And that’s it, see how simple it is!

Important:

1. You can use any USB Drive instead of the CD to run Ophcrack. To see this technique Visit: http://techrena.blogspot.com/2009/03/ophcrack-usb-booting-windows-password.html

2. If you are not interested in recovering the password or you simply want to **reset** the password then there is much easier technique which requires only a 3 MB file instead of Ophcrack. Just visit the link to see how it works:http://www.techrena.net/computers/reset-windows-xp-vista-7-password-usb-pen-drive-cd/

3. The windows vista live CD works for Windows 7 Beta Build 7000 also. There is no official release for Windows 7 yet.

4. This is for information purposes only. We are not responsible for any damages or illegal acts resulting from this information.

5. The information provided here should be used for legal purposes only.

6. Ophcrack is a legal open source program. Visit http://ophcrack.sourceforge.net/ for more details. Click Here to Read the Terms of Use.

Posted by Dennis on Thursday, March 19, 2009