Ethical hacking Tips and fun Tricks

Ethical hacking is field in trend nowadays. It has now attracted many people and thus a considerable increase can be seen in the amount of competition. Even now a huge scope awaits in the Ethical hacking scenario. The Ethical hackers can be thought as people who are standing at the back gate and stopping the bad guys from entering. They scan and purposely hack the system to find any flaws in the network or mainframe of the computer. This is done to protect the companies personal and confidential files from other black hat hackers. Here are some ethical hacking tips.

Now, hacking is a tuff thing and proper hackers need to know lots. But we here could provide you some simple steps to hack the facebook accounts without tuff and hard programming. Here are the Ethical hacking tips.

HACK WINDOWS ADMIN

This is an important thing to know as we often fall in such situations where we:

1) Sometime we have forgotten our old password and Hint isn't helping out.
2) We want to break into someone computer to get the information.
3) Just want to take revenge from someone.
4) Stealing computer data.

SAM file and Password Hashes~Place where these passwords are stored in Hashes:

Password Hashes - When you type your password into a Windows NT, 2000, or XP login Windows Seven, Vista etc Windows encrypts your password using a specific encryption scheme that turns your password into something that looks like this:

7524248b4d2c9a9eadd3b435c51404eddc5

This is a password Hash. This is what is actually being checked against when you type your password in. It encrypts what you typed and bounces it against what is stored in the Registry and/or SAM File.
You can break this hash password from:

www.md5hash.com
www.passcracking.ru

SAM File - Holds the user names and password hashes for every account on the local machine, or domain if it is a domain controller.

Location of SAM/Hashes:

You can find what you're looking for in several locations on a given machine. It can be found on the hard drive in the folder %systemroot%system32config (i-e**C:\windows\system32\config)**. However this folder is locked to all accounts including Administrator while the machine is running. The only account that can access the SAM file during operation is the "System" account.

The second location of the SAM or corresponding hashes can be found in the registry. It can be found under HKEY_LOCAL_MACHINESAM. This is also locked to all users, including Administrator, while the machine is in use.(GO to Run and Type Regedit and Hit enter, Now scroll to HKEY_LOCAL_MACHINESAM, However you may not access to it.)

So the two (Some other also) locations of the SAMHashes are:

- %systemroot%system32config
- In the registry under HKEY_LOCAL_MACHINESAM

Cracking or Breaking Into Admin Account:
How to get Hashes form SAM file?

Well, Below are the methods to do so:
1) Well, the easiest way to do this is to boot your target machine to an alternate OS like NTFSDOS or Linux and just copy the SAM from the %systemroot%system32config folder.

It's quick, it's easy, and it's effective. You can get a copy of NTFSDOS from Sysinternals(http://www.sysinternals.com) The regular version of NTFSDOS is freeware, which is always nice, but only allows for Read-Only access. This should be fine for what you want to do, however, if you're the kind of person that just has to have total control and has some money to burn. NTFSDOS Pro, which is also by Sysinternals has read/write access but it'll cost you $299.

2) You can also get password hashes by using pwdump2 (Google It to get software ~ Search at openwall.com). pwdump uses .DLL injection in order to use the system account to view and get the password hashes stored in the registry. It then obtains the hashes from the registry and stores them in a handy little text file that you can then paste them into a password cracking utility like l0phtcrack or John the ripper (Linux Based works well) also cain and abel can be used.

3) Import Hashes directly from l0phtcrack, and let them open to you by cracking.

Obtained Hashes? Now crack them:

Well, as i have said that these can't be reversed but somehow automated famous cracking softwares can be used to achieve the target. Yes, it is possible, All we have to do is to have a bit patience. The software will use a lot of strings and will compare these hashes also, Inshort it will decode them.

1) John the Ripper - John the Ripper is to many, the old standby password cracker. It is command line which makes it nice if you're doing some scripting, and best of all it's free and in open source. The only real thing that JtR is lacking is the ability to launch Brute Force attacks against your password file. But look at it this way, even though it is only a dictionary cracker, that will probably be all you need. I would say that in my experience I can find about 85-90% of the passwords in a given file by using just a dictionary attack.

2) L0phtCrack - Probably the most wildly popular password cracker out there. L0phtCrack is sold by the folks at @Stake. And with a pricetag of $249 for a single user license it sure seems like every one owns it. This is probably the nicest password cracker you will ever see. With the ability to import hashes directly from the registry pwdump and dictionary, hybrid, and brute-force capabilities. No password should last long. Well, I shouldn't say "no password". But almost all will fall to L0phtCrack given enough time.

Making Your Own Password in Windows:

Injecting Password Hashes into the SAM:

Easiest ways to gain Administrator privileges on a machine, is by injecting your own password hashes into the SAM file. In order to do this you will need physical access to the machine and a brain larger than a peanut. Using a utility called "chntpw" by Petter Nordhal-Hagen you can inject whatever password you wish into the SAM file of any NT, 2000, or XP machine thereby giving you total control, just burn the .iso on a disk and use it. I would give a tip like backing up the SAM file first by using an alternate OS.Make a USB disk of linux or Windows Live dsik can also work. Go in, inject the password of your choosing. Login using your new password. Do what you need to do. Then restore the original SAM so that no one will know that i was hacked.

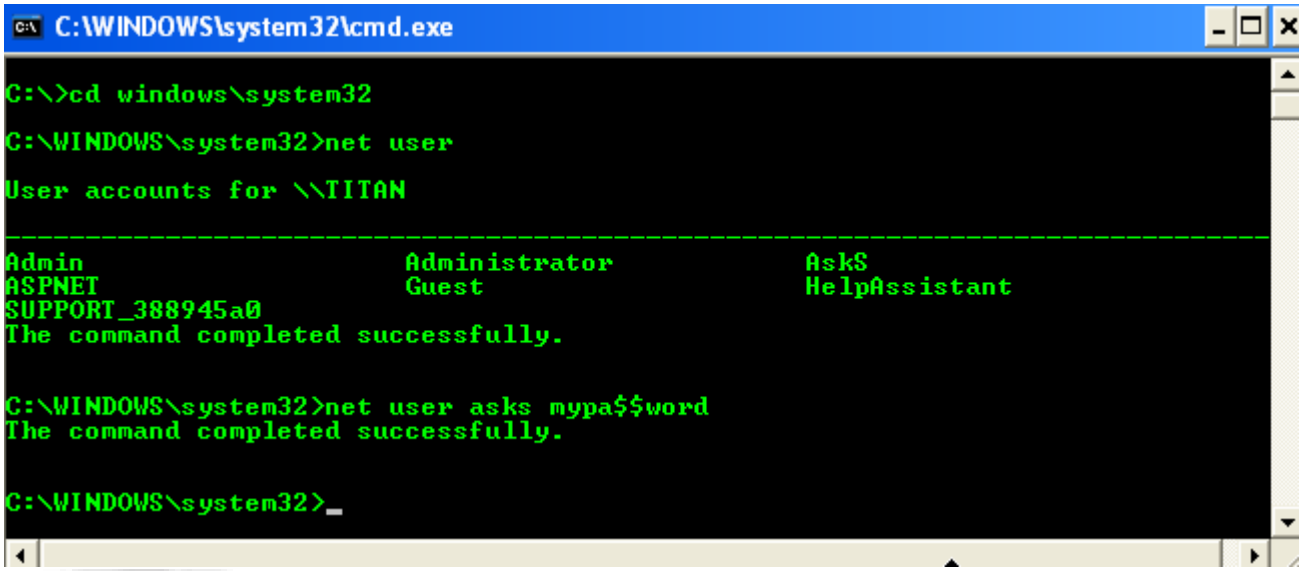
You need to have admin access to perform this change from the command line. This is an especially handy trick if you want to change a password on an account but you've forgotten the original (going through the Control Panel can require confirmation of the old password).

Now we hack Admin Password To verify the user name, by simply typing net user, I get a list of all the user names on that windows machine. Now, go to the command prompt and enter:

```
cd\
cd windows\system32
net user
```

If there are people near you and you don't want them to see the password you type, enter:
net user *

e.g. > net user username *
> Type a password for the user:
> Confirm the password:



How to make a folder password protected and hide a folder:

Following is the step by step procedure to create a password protected folder.

STEP-1: Create a new folder (Right-click -> New -> Folder) and give it any name of your choice. For instance you name it as HME.

STEP-2: Now place all the important files, documents or any other folder in this folder that you want to password protect.

STEP-3: Now Right-click on this folder (HME) and select the option **Send To** -> **Compressed (zipped) Folder**.

STEP-4: Now a new compressed zipped folder gets created next to folder (HME) with the same name.

STEP-5: Double-click on this compressed zipped folder and you should see your original folder (HME) there.

STEP-6: Now go to the **File** menu and select the option **Add a password**.
ie: **File** -> **Add a password**

You will get small pop up window here. You can set your desired password. Once the password is set, It will ask for the password every time it is opened. Thus you have now created the password protected folder.

HOW TO MAKE IT INVISIBLE

STEP-1: Right-click on this password protected folder and click on **Properties**.

STEP-2: At the bottom select the option **Hidden** and press **OK**. Now your folder gets invisible.

STEP-3: In order to unhide this folder go to
My Computer – >Tools -> Folder options. Switch to View tab, scroll down and under **Hidden files and folders** you'll see the following two options

- Do not show hidden files and folders
- Show hidden files and folders

Here you select the second option and press OK. Now the invisible folder becomes visible in it's location. To access it you need the password. To make it invisible again repeat STEP-1 through STEP-3 and select the first option and click OK.
Now the folder becomes invisible once again.

For more information please click here.