Ex. No. 5

Implement Hacking windows - Windows login password

Aim:

To login to windows 7 by hacking the administrator account password.

Procedure:

● Turn on the UPS and the CPU, tap F8 continuously on the boot screen to get some windows start-up options.

● Choose "Start windows normally" option and turn the UPS off immediately.

● Then turn on the PC again, let it load.

● After that you will be prompted with two options in the boot screen (again), select the first option - "Launch Start-up Repair(recommended)"

● Let it load and Scan for issues.

● After few min, It will ask to restore defaults, select "Cancel" option.

● After few minutes, an error report screen will pop-up, asking to send information or not.

● Click on "View Problem Details" arrow, scroll down to the end of the report, then click a link stating X:\windows\something\something (the link starts with an"X")

● Another Window will pop-up, and will look like a notepad

● Click File on the Menu-Bar, then select Open, and another window will pop-up

● Navigate to C: drive (or the drive on which windows is installed), click Windows, then System32, after that click on the arrow beside the "File Type" option and select "all files"

● Then search for a file named "sethc"(this is the shortcut to sticky keys), rename it to something else (Eg: sethc.bak)

● Search for cmd, create a copy and rename the copy as "sethc"

● Close everything, restart the PC, go to the log-in screen, press shift 5 times, until a cmd (command prompt) pops-up.

● Type in "net user administrator /active:yes", and this will activate the default administrator account of the PC.

● Change/delete/manage/reset passwords from there.

● We can directly change passwords from cmd by typing "net user (admin/any admin

account's name) \*”

● For Example: “net user student \*”

● Once the new password is set, login normally in the login screen using the new password

Result:

Hence, access to administrator account was hacked by setting a new password and we

can login to the system.

Ex. No. 6

Implement Hacking windows - Accessing Restricted drives

Aim:

To access drives that are restricted to standard users by the administrator

Procedure:

Step 1 - Creating Restricted Drives as Administrator:

● Log on to your computer with an account with Administrator rights. Click “Start,” type “user” (without quotes) in the automatically selected “Search programs and files” search

box and click “User Accounts.” Click “Manage another account.”

● Click “Create a new account,” if you need to create a user account for other people that will be using the computer. If you already have another account set up, go to the next step. You need to have at least your user account and another one set up to restrict access to a drive. Type a name for the user and click “Create Account.”

● Click “Start” and “Computer.” Right-click the name of the hard drive you want to restrict access to. Click “Properties.”

● Click the “Security tab” in the “Properties” window that opened. Click “Edit...” and “Add...” in the “Select Users or Groups” window that opened.

● Type the name of the other user account on your computer or you can click “Advanced” and then “Find Now”, then select your user account. Click “OK.”

● Uncheck the boxes to the left of any options that you do not want the user to have available. Check the “Deny” box for “Full control” to disable all control from the user for files on the hard drive.

● Click “OK,” “Yes” and “OK.” Close any open windows. Click “Start,” log off of your account and log on as the other user to test your settings.

● Click “Start,” “Computer” and double-click the name of the hard drive you restricted access to. A window indicating that “Access is denied” is shown. Close the window and

log off the computer.

Step 2 - Removing restrictions as a standard user:

● Find the Administrator password or set a new password using the method described in the previous experiment.

● Click “Start” and “Computer.” Right-click the name of the hard drive for which you want to remove access restrictions. Click “Properties”.

● Click the “Security tab” in the “Properties” window that opened. Enter the new administrator password when prompted.

● Check the boxes to the left of any options that you do not want the user to have available.

Check the “Allow” box for “Full control” to enable all control from the user for files on the hard drive.

● Click “OK,” “Yes” and “OK.”

● Click “Start,” “Computer” and double-click the name of the hard drive for which restrictions were removed.

● Now the contents of the drive will be displayed and the ‘Access is Denied’ window no longer occurs.

Result:

Hence, the restrictions on the hard drive were removed and the contents can be accessed.