



COURSE: Computer Forensics & Investigation

MARKS:

CODE: BCN3193

ASSESSMENT: Lab 3

DURATION:

Password Cracking

Lab Objectives:

Through this lab sheet, student will have the ability to enumerate:

1. Use the pwdump7 tool.
2. Crack administrator password.
3. Window XP environment

Lab Environment:

To carry out the lab you need:

1. Download the latest version of pwdump7 from the link <http://www.tarasco.org/security/pwdump7/index.html>
(Note: Many antivirus programs will flag this tool as a malicious product. You will have to remove the virus control package or make other arrangements to work with this tool on most systems.)
2. Administrative privilege to run tools.

Task 1- Generating Hashes :

1. Using administrator account, create several test accounts with password to detect.
2. Click **Start**, click **Control Panel**, double-click **User Account**, then click **Create a new account** with administrator level and its password.
3. At command prompt, navigate to pwdump7 directory.
4. Type **pwdump** and press **Enter**, which will display all the password hashes.
5. Now type **pwdump7.exe > c:\hashes.txt** in the command prompt, and press **Enter**.
6. This command will copy all the data of pwdump.exe to the c:\hashes.txt file.
7. Open the file hashes.txt and observe the result.

Task 2- Hashes Cracking :

1. Open the hashes.txt file.
2. Analyze all the password hashes gathered during the lab and figure out what the password were.
3. Find the answer and submit your report.

End of Lab Sheet 3