

**Lab 6: *Accounts, Accounts Everywhere* (2%)**

**Overview:**

In this lab you’ll be checking and verifying the integrity of a down loaded file and doing two types of password cracking attacks.

**Objective:**

1. Checking the integrity of an data file/application
2. Creating accounts to be cracked
3. Cracking passwords

**Note:** Any file names given in the text with **MSU** in them, should have the MSU replaced by your MySeneca username e.g. MSU\_L6.docx would become alex\_L7.docx if “alex” was your MySeneca username.

**The Lab Activities**

**Part 1: Am I Cracked? (Optional)**

This part is purely for your interest and enlightenment.

Before looking at cracking passwords you may be wondering if anyone have possibly cracked your passwords, or at least, got a hold of your personal data in some fashion. Another way to ask that question is to ask yourself: “Have I been pwned?”

*If you do not know what ‘pwn’ means, have a look at the definition: https://en.wikipedia.org/wiki/Pwn*

If you really want to know, one way to check this is to go to the following website… you may be surprised:

<https://haveibeenpwned.com/>

**Part 2: Downloading and Verifying an Application (Integrity Checking)**

When you down load an application from the web you do not know if malicious code has been added to the application. To allow users to verify this is not the case, developers often provide a hash of the file to the user can verify that the file they have downloaded is the original file.

For this activity we will be using FastSum, which calculates hashes.

**Steps**

1. Go to the [www.fastsum.com](http://www.fastsum.com) downloads web page. Download and install the program **FastSum Standard + Command Line Edition** from the web site
2. Still on the downloads page, you will see MD5 hash given for the **FastSum Standard + Command Line Edition**. Copy into a text file called “MD5\_FS.txt”.
3. Use *FastSum* **command-line** (fsum) to calculate the hash of *for the FastSum* and compare it against MD5\_FS.txt.
4. Arrange the two windows (one showing the fsum command-line with the result and the other the open MD5\_FS.txt file) so that the two hash values can be seen and take a screen shot of the desktop. Save the file as **MSU\_MD5.jpeg**.

**Part 3: Creating User Accounts**

Before we can look at cracking passwords, first we need to create some user accounts. On your Ubuntu VM create the following accounts with the associated passwords:

|  |  |
| --- | --- |
| **Account** | **Password** |
| BTN710\_user1 | abc! |
| BTN710\_user2 | password |
| BTN710\_user3 | snow |
| BTN710\_user4 | qwas21 |

Copy the content of /etc/passwd and /etc/shadow to MSU\_passwd.txt, and MSU\_shadow.txt, remove your own username and password, and save the files.

**Part 4: Cracking Passwords**

In this part of the lab you will be using ***John*** (John the ripper) on the Kali VM to crack passwords. We are only using a very simple capability of this software. If you are interested, you can find tutorials for John the ripper online. To crack the passwords follow the instructions here:

john /etc/shadow

Keep track of the password cracking and for each password indicate if it took the program seconds, minutes, or hours to crack the password.

**Lab Assignment Report Write-up**

As there is not template, create your own report template using the previous templates as a basis.

Save the report as MSU\_L6.pdf

**Deliverable**

To submit your lab assignment report, MSU\_passwd.txt, and MSU\_shadow.txt to Blackboard.

Note:

* Submission deadline is on Sunday, June 12th.
* Late labs will be assigned a grade of ‘0’..
* Late labs still need to be satisfactorily completed and submitted by the end of Week 12 to meet BTN710’s Promotion Requirements.