**CIS 2640 – Lab 25**

**Securing Data with Encryption Software**

| **Your Name:** | Liliane Owens |
| --- | --- |
| **Date:** | 4/17/23 |

**Instructions**: Complete the tasks described in this worksheet. Read the instructions carefully and submit evidence of your completed tasks (a screen shot is your evidence). Answer the questions below in the space provided.

* **Showing Evidence of Completion:** Your evidence of completion is a screen shot, as described in each exercise. Use the tool of your choice to take a screen shot of the required content. ***Screen shots should be pasted at the end of this document.***
* **Answering Questions:** Your answers should be written in carefully edited college-level English, using complete sentences.

| **Lab – Securing Data with Encryption Software** | |
| --- | --- |
| **Instructions and Evidence of Completion** | **Answer a Question** |
| At the end of this document (not within this table) paste screen captures that show the following:   1. A successful creation of a TrueCrypt volume on your Kali system 2. The successful cracking of your TrueCrypt password using TrueCrack.   ***Be sure your screen shot(s) include any command executed and the resulting output in clear / cropped screenshots.*** | Answer each of the questions below; use the space to the right of each question for your answer. Make sure your answers are clear and complete. |
| **Question** | **Answer** |
| 1. What command was used to create the billing.txt file? | The command used to create billing.txt file was : **touch billing.txt** |
| 1. The TrueCrypt volume you created resides in a file; what is that file’s name? | **Billing.txt.** |
| 1. What FIPS-approved cipher was selected for your TrueCrypt volume? What hash algorithm was used? | The FIPS-approved was **AES** and hash algorithm was **RIPEMD-160.** |
| 1. What are the steps to open a TrueCrypt volume? | In the main TrueCrypt window, under Volume, click “Select File”, select the file you have created, and then click “Open”.  Highlight the driver number you want to map to your encrypted file and click “Mount”. Then you will be prompted for password, type it and click OK. Now you can use your TrueCrypt drive just like any other mapped drive. |
| 1. Section 3 of this lab refers to “Bruteforcing a TrueCrypt Container”. The truecrack command was executed using the “–w” option. What does this option do? What type of password attack was really used in this case? | The -w was for displays all wordlist passlist file. Brute force is the password attack was used in this scenario. |

Put screenshots here:

1. A successful creation of a TrueCrypt volume on your Kali system

![Graphical user interface, text, application

Description automatically generated]()

![Graphical user interface, application

Description automatically generated]()

1. The successful cracking of your TrueCrypt password using TrueCrack.

![Text

Description automatically generated]()