Hash Verification

Introduction and/or Background

You've just downloaded a new version of Linux. Unfortunately, due to the program's popularity, a group of cyber criminals has repackaged the ISO with malware. They've even replaced the legitimate ISO with their malware-infested version on several popular download sites.

In order to combat this, the group managing the Linux distro has released the hash value of the legitimate updater. This allows anyone that downloads the updater to discover if they've obtained its legitimate or malware-infested version. Needless to say, running the malware-infested updater on company computers is generally considered a bad thing.

Objectives

In this project/lab the student will:

- Check a file's hash value and how it changes if the file is modified.

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

1. Download gtkhash.
2. Create a test file using the touch command.
3. Use the md5sum command to generate its hash value.
4. Use gtkhash to generate its hash value.
5. Take a screenshot showing the output of both the md5sum command and gtkhash.
6. Open the test file and change its contents.
7. Use the md5sum command and gtkhash to obtain the file's new hash value.
8. Take a screenshot showing md5sum's and gtkhash's new values.

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Moodle for grading.

Reflection

1. Are the hash values in the two screenshots different? Why or why not?
2. What does it mean if you download a file and its hash value is the same as the value listed on the website you downloaded it from?
3. What does it mean if it's different?

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot of GTKHash for first file (42.5 points)	
	Criteria #2: Screenshots of GTKHash for second file (42.5 points)	
	Criteria #3: Answer to reflection question 1 (5 points)	
	Criteria #4: Answer to reflection question 2 (5 points)	
	Criteria #5: Answer to reflection question 3 (5 points)	