Create hash values

Description

As a security analyst, one of the security controls we can implement is hashing. It produces a code that cannot be decrypted. It works by uniquely identifying the contents of a file, later known as a unique identifier (hash value or digest). For example, a malicious program may mimic an original program. If one code line is different from the original program, it produces a different hash value. Security teams can then identify the malicious program and work to mitigate the risk.

Generate Hashes

First, ls command shows the files within the directory. We have two files and we would like to show the contents of them (cat). We could see from the picture below that the contents of both files appear to be identical.

```
analyst@f62f0dd57549:~$ ls
file1.txt  file2.txt
analyst@f62f0dd57549:~$ cat file1.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
analyst@f62f0dd57549:~$ cat file2.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

We can find if the files are different or not by using the sha256 command. From the picture below we can see both files have different hash values.

```
9sxa5Yq20Ranalyst@f62f0dd57549:~$ sha256sum file1.txt
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267  file1.txt
analyst@f62f0dd57549:~$ sha256sum file2.txt
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
```

Compare Hashes Files

Let's generate the hash of the file1.txt and file2.txt to a new file for file1hash and file2hash respectively.

```
9sxa5Yq20Ranalyst@f62f0dd57549:~$ sha256sum file1.txt
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267  file1.txt
analyst@f62f0dd57549:~$ sha256sum file2.txt
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
```

Inspect the contents of them by using cat commands. Finally, compare both files by using cmp command.

```
analyst@f62f0dd57549:~$ sha256sum file1.txt >> file1hash
analyst@f62f0dd57549:~$ sha256sum fil21.txt >> file2hash
sha256sum: fil21.txt: No such file or directory
analyst@f62f0dd57549:~$ sha256sum file2.txt >> file2hash
```

```
analyst@f62f0dd57549:~$ cat file1hash
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267  file1.txt
analyst@f62f0dd57549:~$ cat file2hash
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
analyst@f62f0dd57549:~$ cmp file1hash file2hash
file1hash file2hash differ: char 1, line 1
```

Summary

Though the contents of both files appear to be identical, only hash values of each file that can determine if they are the same or not.