Lab #2 - Assessment Worksheet

Applying Encryption and Hashing Algorithms for Secure Communications

Course Name and Number: IT 280 - Ethical Hacking

Student Name: Connor Morrissy

Instructor Name: Darnell Payne

Lab Due Date: 10/13/22

Lab Assessment Questions & Answers

1. Compare the hash values calculated for *Example.txt* that you documented during this lab. Explain in your own words why the hash values will change when the data is modified.

   The md5 algorithm creates a hash number based on the characters in a file. When the hash is created on a file, it is unique to the data on the file. If the data is changed (removed or added), then that means there are different characters in the file, and therefore the hash number will change.

2. If you were to create a new MD5sum or SHA1sum hash value for the modified *Example.txt* file, would the value be the same or different from the hash value created in Part 3 of the lab?

   They would be different.

3. If you want secure email communications without encrypting an email message, what other security countermeasure can you deploy to ensure message integrity?

   You can use digital signatures to make sure there is authentication and verification for opening the message, however it does not encrypt the actual message.

4. When running the GnuPG command, what does the -e switch do?

   a. Extract
   b. Encrypt
   c. Export

   B. Encrypt

5. What is the difference between MD5sum and SHA1sum hashing calculations?

   MD5sum creates a 128 bit-long hash and SHA1sum creates a 160 bit-long hash

Which is better and why?

MD5sum is faster because it generates less bits, but that means it is less secure than SHA1sum. SHA1sum's 160 bit hash is more secure than MD5sum's 128 bit hash. SHA1sum is more secure, so I would rather use SHA1sum. However, both MD5 and SHA1 are outdated and there are better options now.

6. Name the cryptographic algorithms used in this lab.

   MD5sum and SHA1sum hash algorithms

7. What do you need if you want to decrypt encrypted messages and files from a trusted sender?

   You would need the private key that was used to encrypt the message in order to decrypt it.

8. When running the GnuPG command, what does the -d switch do?

   - a. Detach
   - b. Destroy
   - c. Decrypt

   C. Decrypt

9. When creating a GnuPG encryption key, what are ways to create entropy?

   Entropy is essentially random data that can be used by the encryption algorithm to encrypt data. Random data can be created on a computer by doing any tasks or giving input to the system. Moving your mouse, typing on a keyboard, and performing operations on the computer such as searching a file can be ways to create the needed entropy. In this lab we used a script that kept performing search operations in order to generate the entropy.