Lab #2 – Assessment Worksheet

Applying Encryption and Hashing Algorithms for Secure Communications

Course Name and Number: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you applied common cryptographic techniques to ensure confidentiality, integrity, and authentication. You created an MD5sum and SHA1 hash on a simple text file on a Linux virtual machine and compared the hash values of the original files with those generated after the file had been modified. Next, you used GnuPG to generate an encryption key pair and encrypted a message. Finally, you used the key pairs to send secure messages between two user accounts on the virtual machine and verified the integrity of the received files.

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.

2. Why are the MD5sum and SHA1sum hash values the same every time you calculate for the *example.txt* file? What if it were different when you recalculated the hash value at the other end?

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

4. What is the –e switch used for with running the GnuPG command?

○ A. Extract

○ B. Encrypt

○ C. Export

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

6. Name the cryptographic algorithms used in this lab.

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

8. What is the -d switch used for when running the GnuPG command?

   ○ A. Detach

   ○ B. Destroy

   ○ C. Decrypt

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