CS471 Assignment 2

Abstract

Work with symmetric and asymmetric encryption using Kali Linux, gpg, md5sum, and steghide.

Assignment

Using your Kali Linux virtual machine, complete the following activity.

Provide a single document detailing the activity, including your process, methods, and results. All screenshots should be nicely resized and annotated. Your document should show what you did, how you did it, display the results, and explain what happened.

Include all of the files created during this activity with your submission. Additionally, include all of the commands used during your work in separate text file; this will also be included with your submission.

Activity

Create a plaintext file, named plaintext.txt, with the following text:
Your name
NetID
Some secret message of your choosing.

Use the GPG application to perform symmetric and asymmetric encryption tasks.

- Encrypt the plaintext file with symmetric encryption in ASCII armored format.
  Use password: letmein
- Import the provided public key, csmith.pub.key into your gpg keyring. This will be used for asymmetric encryption.
- List keys in GPG keyring. This will simply display the keys.
- Create a key public/private key pair. Save your password!
- List keys in GPG keyring. This will simply display the keys. There should be new keys now.
- Export your public key as ASCII armored file named YOURNETID.public.key. Include this file.
- Sign the plaintext.txt file with your private key. Do not share or submit your private key!
- Encrypt the signed file to Ascii output using provided key. Include this signed file.

Use Netcat to transmit ASCII formatted encrypted text.
This message must be captured using Wireshark. Include a packet capture file with only these captured packets. The Netcat listener must save the received data in a file on the receiver. Include this file.

Use Steganography tools, Steghide, to embed your plaintext.txt file in a jpeg image of your choosing.
For this step, you will need to install Steghide. Include this embedded image file and the original image file in your submission. You must use the password letmein for embedding the image.
Use the same Steganography tools to extract your plaintext from the previous embedding.

Use md5 tools to get the md5 hash of your original jpeg image and jpeg with an embedded file.
Compare these checksums. What does this result mean?
Rename the original file and get the md5 sum for the renamed file.
Compare these checksums. What does this result mean?

Conclusion

In addition to your conclusion, add the following:

- Discuss the limitations and use cases for the tools used in the activity. Be specific.
- For each of the tools used, describe how they do or do not provide:
    - Authentication
    - Access control
    - Data confidentiality
    - Data integrity
    - Non-repudiation

Deliverables

A document detailing the activity, including your process, methods, and results. This includes annotated screenshots. Clearly detail your work in a reproducible way following the provided sample format. Do not provide any image or text from another source without citation.

Additionally, submit all files created for this assignment. Attach these files to your submission. Do not zip, tar, or archive. The packet capture files should only include the requested files; these should be fairly small files.

Additionally, submit a single text file with all of the commands used for this assignment. One command per line. This should be complete and organized in order of use.

Upload these files to BlackBoard before the deadline.