CPRE 431

Module 2 Lab

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!

1. You are the security administrator in the XYZ company, and you noticed some strange traffic on the network of one of the employees sending an encrypted file to someone outside of the company. You want to check if the content doesn't have any confidential data. The encrypted file is attached with the homework (dont_smoke_hash_it_can_md5_you.zip). From the file name, you guessed that the password could be the md5 hash of the file name with the extension.

   a. Explain with screenshots how to use OpenSSL tool to determine the md5 hash, then use any file decompression tool (WinRAR, Winzip, etc.) to decrypt contents of the attached file. Hint: write the file name in a text file then get the hash for this text file. Note that hash is space sensitive.

   b. After decryption, you noticed that the content of the attached file was an excel sheet "my_funny_expenses.csv", an image "funny_image.png" and a text file "funny_jokes.txt". This could look normal, however there is a lot of secrets and hidden messages in the content. Depending on your cryptanalysis skills, you started with the text file and you noticed that it only contained random characters but it started with the word "Salted__". From your experience with OpenSSL tool, this means that this text file is encrypted using Symmetric Cipher (des, des3, aes128, aes192, aes256, etc.). Also, you noticed that all the three files have the word "funny" in their name, maybe this could be the encryption key. Explain with screenshots how to use OpenSSL tool to decrypt the original message in the text file.

   c. The decrypted message of part (a) will contain the instructions for this question. Explain with screenshots how did you solve this secret and get the new key.

   d. The decrypted message of part (b) will contain the instructions for this question. Explain with screenshots how did you solve this secret and get the final leaked confidential information.