CIS 480 Project – Injection 5

Injection

• Well done, team! It has been reported that you discovered mysterious files on the e-commerce server and transferred these to Kali successfully.

• Using the information in the files, find a treasure in the image file.

• Ignore GoodData-e.txt file you transferred from the e-commerce server.

• Use the following file for the instructions for Injection 5: 0x8F6568A3-pub.asc.encrypted.txt. This file is posted on BB Injection 5. You need to download the private key as well from BB Injection 5.

Tutorials

• A private and public key pair was created using RSA algorithm on a site that offers generation of PGP keys (pgptool.org). The instruction for Injection 5 is encrypted with the public key and you need to use the private key to decrypt.

• What is Pretty Good Privacy (PGP)?

- https://en.wikipedia.org/wiki/Pretty\_Good\_Privacy

Steps

• Go to pgptool.org. You will see the webpage shown below.

• Import the private key.

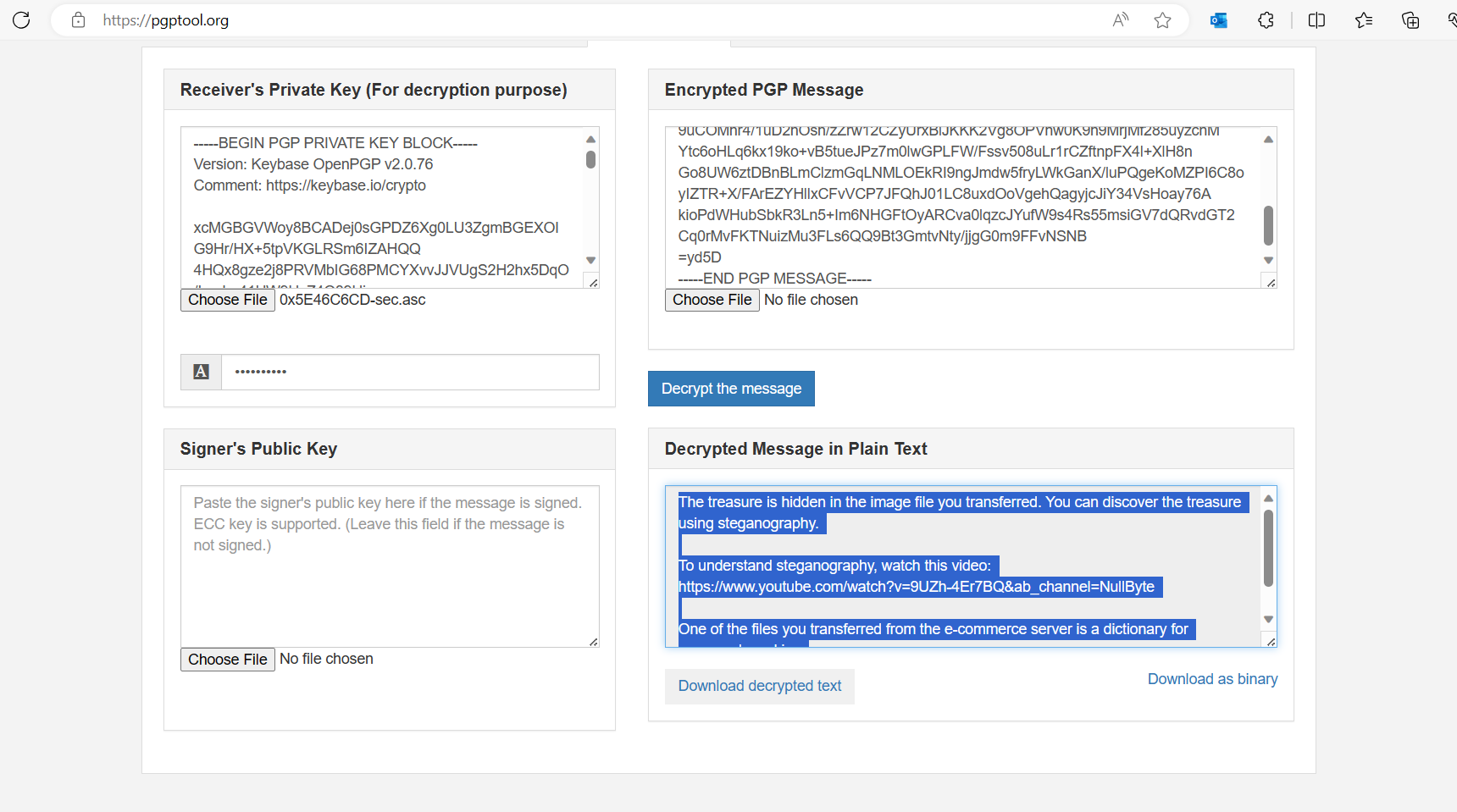
• Import the encrypted message.

• Enter the passphrase: louisville.

• Click on Decrypt the message.

• Use the decrypted message for the next steps.

1. Provide a screenshot of the decrypted message on pgptool.org.

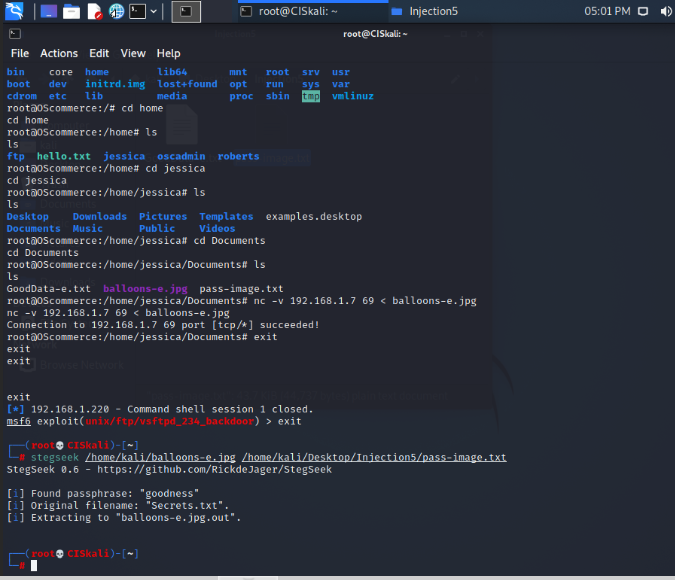


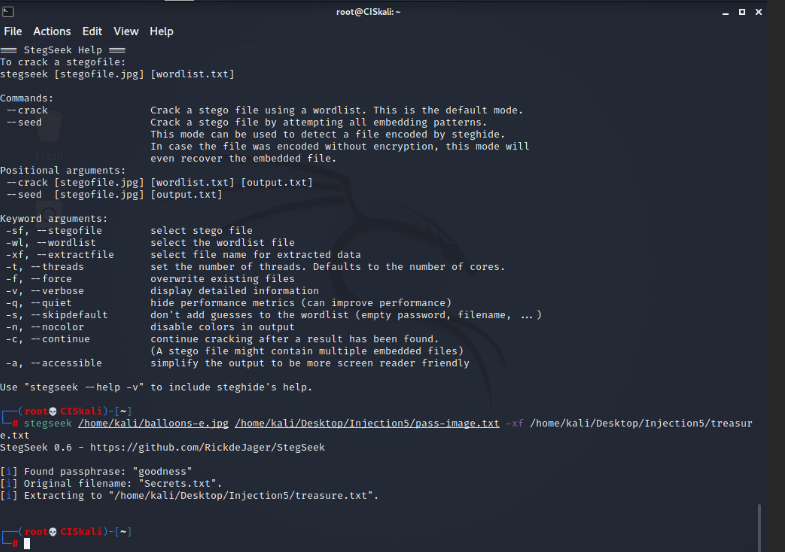
1. Explain the process of treasure discovery.

The process of treasure discovery went as follows. First, we decrypted the injection 5 instructions via pgptool. Once we received the decrypted message, we followed the instructions given. After reviewing video and researching how to use a list of passwords with steghide, we came to the conclusion that we would need to use a different tool. We found Stegseek and downloaded it from Github and installed it. Upon running the command on the balloons image and password list we kept receiving a “premature end of file” error on the balloons file. After some research we realized that the image file we transferred from the e-commerce server to the linux box via netcat had been corrupted somehow. We then got back into the e-commerce server via the FTP backdoor vulnerability we used in injection 4 to retrieve the balloons image once more with netcat. Once this was done, we ran the stegseek command once more and was given the hidden message which was a credit card number.

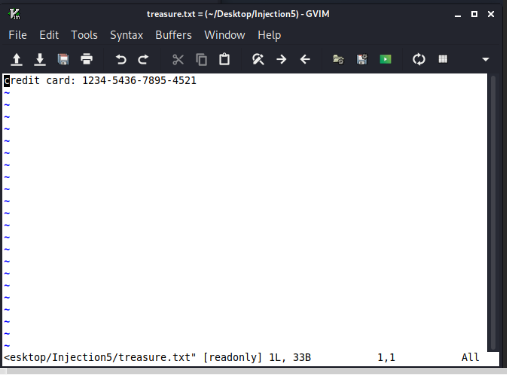
1. Provide screenshots of the commands you used along the way.







1. Show the treasure in a screenshot.



Response to Injection 5

1) Team members: Tristan Rogers, Chip Carter, Eric Lopez-Gutierrez

2) Address the above requirements.