task5

October 18, 2022

1 Task 5 - Core Dumped - (Reverse Engineering, Cryptography)Points: 500

1.1 Problem statement

The FBI knew who that was, and got a warrant to seize their laptop. It looks like they had an encrypted file, which may be of use to your investigation. We believe that the attacker may have been clever and used the same RSA key that they use for SSH to encrypt the file. We asked the FBI to take a core dump of ssh-agent that was running on the attacker's computer. Extract the attacker's private key from the core dump, and use it to decrypt the file. Hint: if you have the private key in PEM format, you should be able to decrypt the file with the command openssl pkeyutl -decrypt -inkey privatekey.pem -in data.enc Enter the token value extracted from the decrypted file.

[ ]: