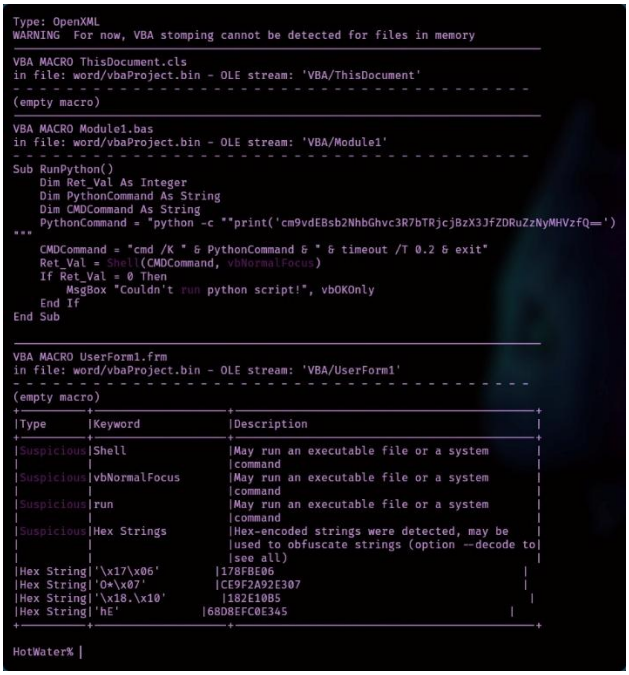
FORENSIC

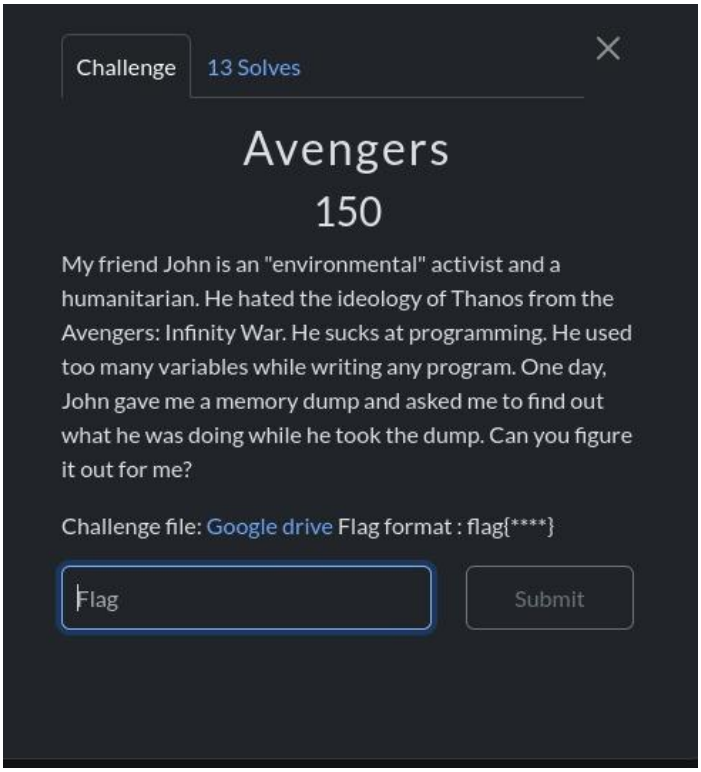
1. Decrypting the ransom : Malicious DOCM Analysis

- Download the file.docm
- Goto linux terminal and type following command.
  $olevba file.docm –decode



Flag is encoded in print statement, decoded using base64.
Flag : root@localhost{m4cr0s_r_d4ng3r0us}

2. Avengers



- Download challenge.raw
- Install volatility package for reading memory dump file.
- Get profile info from volatility command
  $ volatility -f challenge.raw –profile=Win7SP1x86 cmdscan
  (it will display command execution demon.py.txt)

- Check console for python output.
- $ volatility -f challenge.raw –profile=Win7SP1x86 consoles

- Output of demon.py.txt displayed in hexa encoded string

  $ volatility -f challenge.raw --profile=Win7SP1x86 Envars

  Capture the xor and password.
- Check the output of hashdump

  $volatility -f challenge.raw --profile=Win7SP1x86 Hashdump.

  We got a hash password, decrypting the other part of the flag

  Flag : flag{you_are_good_but1_4m_b3tt3r}