[Rev] DetectIve (499 points)

By: FieryBanana101

Diberikan sebuah elf 64 bit executable yang bernama ‘dotnet.exe’. Binary tersebut sudah di strip simbolnya.

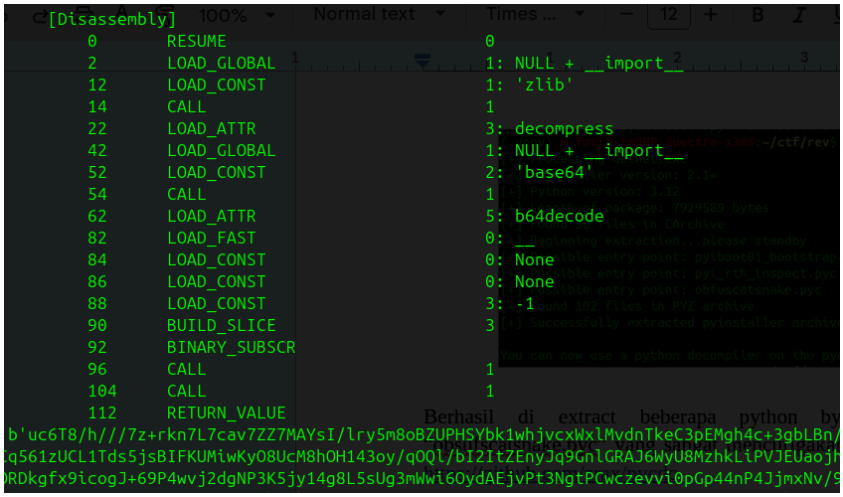
```
dotnet.exe: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
 for GNU/Linux 2.6.32, stripped
```

Ketika dijalankan, executable tersebut menjalankan permainan yang mirip seperti batu-gunting-kertas. Tentu kita memiliki asumsi bahwa diakhir permainan akan diberikan flag atau petunjuk selanjutnya. Namun mari kita lihat jalur lain, saya curiga program ini menggunakan bahasa python, maka mari kita coba extract dengan menggunakan:

https://github.com/extremecoders-re/pyinstxtractor

```
(.venv) m-fatih-im@HP-Spectre-x360:~/ctf/rev$ python3 ./arsenal/pyextractor.py dotnet.exe
[+] Processing dotnet.exe
[+] Pyinstaller version: 2.1+
[+] Python version: 3.12
[+] Length of package: 7929589 bytes
[+] Found 30 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: obfuscatsnake.pyc
[+] Found 102 files in PYZ archive
[+] Successfully extracted pyinstaller archive: dotnet.exe

You can now use a python decompiler on the pyc files within the extracted directory
```

Berhasil di extract beberapa python bytecode dari executable. Terlihat terdapat “obsufscatsnake.pyc” yang sangat mencurigakan. Mari kita analisis dengan menggunakan tools ‘pycdas’ dari https://github.com/zrax/pycdc.



Terlihat bahwa terdapat sebuah nilai berupa byte string yang sangat panjang. Jika kita coba translasikan secara kasar, maka file pyc tersebut akan setara dengan:

```
_ = lambda __ : __import__('zlib').decompress(__import__('base64').b64decode(__[::-1]));
exec((_)(b'uc6T8/h///7z+rkn7L7cav7ZZ7MAYsI/lry5m8oBZUPHSYbk1whjvcxWxlMvdnTkeC3pEMgh4c+3gbLB
```

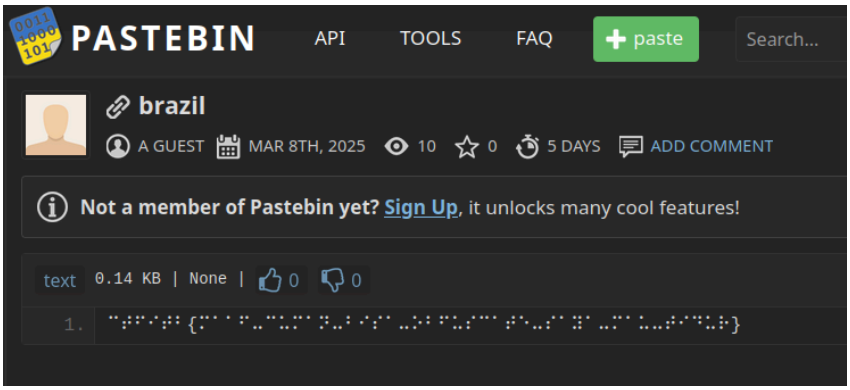
Sederhananya script tersebut akan mengambil nilai byte string, melakukan reverse pada string, dilakukan operasi base64 decoding, dilakukan zlib decompressing dan kemudian hasil akhirnya akan dijalankan sebagai kode. Tentu terlihat jelas bahwa ini adalah suatu source code yang di *obfuscate*. Kita dapat memulihkan source code aslinya dengan script seperti ini:

```
import zlib
import base64

enc = b"exec((_)(b'uc6T8/h///7z+rkn7L7cav7..."    # truncated for visual

with open("game.py", "w") as f:
   while True:
       try:
           enc = zlib.decompress(base64.b64decode(enc[11:-3][::-1]))
       except:      # Error means it is already plain
           f.write(enc.decode())
           break
import os
os.system("xdg-open game.py")
```

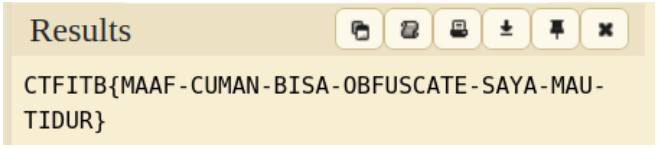
Akan kita dapatkan file ‘game.py’ yang berisi source code asli dari ‘dotnet.exe’. Dari source code terlihat bahwa jika kita memenangkan game yang ada, tetap saja kita tidak akan mendapat apapun. Namun clue selanjutnya terletak pada source code langsung, yaitu pada variabel ‘prize’.

```
if X:
    print(f"Final score: {J}. Processing result...")
    time.sleep(3)
    if J > 10:
        print(
            Z.D
            + Z.G
            + "Congratulations. You succeeded."
            + Z.F
        )
        prize = "104 116 116 112 115 58 47 47 112 97 115 116 101 98 105 110 46 99 111 109 47 90 76 51 70 69 49 83 53"
```

Setelah nilai-nilai desimal tersebut kita decode menjadi ascii, didapatkan link ‘https://pastebin.com/ZL3FE1S5’



Setelah melihat karakter ‘{‘ dan ‘}’, ini kemungkinan besar adalah flag akhir yang diubah menjadi braille. Dengan menggunakan tools braille decoder online (misalnya https://www.dcode.fr/braille-alphabet), kita dapat memulihkan flag aslinya (perlu hati-hati dengan kapitalisasi).



Note: Awalnya saya sempat salah kapitalisasi flag sehingga stuck di bagian braille, dan ditambah dengan deskripsi “I’m lying”, saya mengira bahwa ini adalah fake flag.

FLAG: CTFITB{MAAF-CUMAN-BISA-OBFUSCATE-SAYA-MAU-TIDUR}