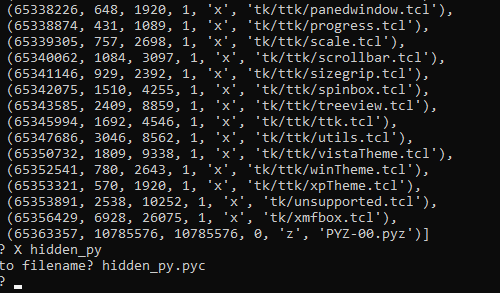
1. Смотрим строки в бинаре, понимаем, что питоновский скрипт был сконвертирован в .elf
2. Устанавливаем pyinstaller
3. Запускаем cmd из директории

…\Python\Python37-32\Lib\site-packages\PyInstaller\utils\cliutils

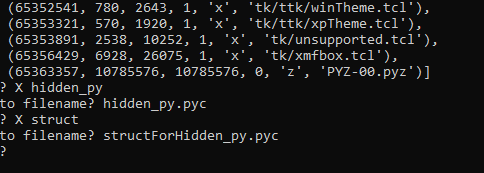
и вводим следующую команду:

…\Python\Python37-32\Lib\site-packages\PyInstaller\utils\cliutils>python archive\_viewer.py hidden\_py

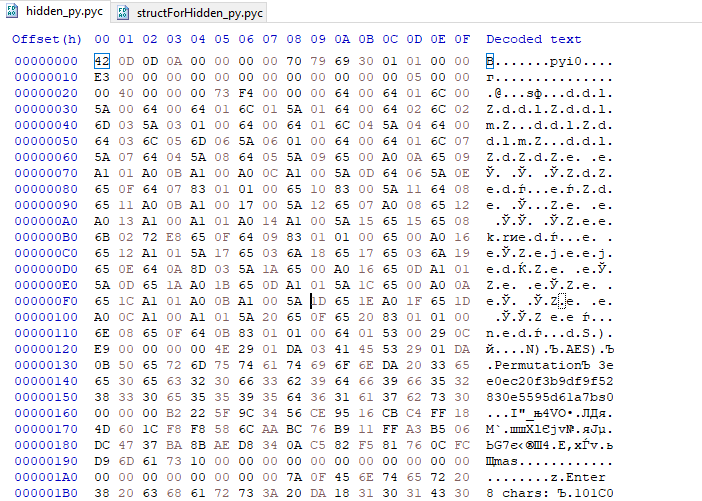
1. Далее экспортируем в .pyc файл:



1. Но он не запустится. Надо экспортировать структуру, введя следующую команду



1. Открыть два полученных файлы в hex-редакторе и дополнить файл hidden\_py.pyc необходимыми начальными байтами (в данном случае это 16 байт) из файла structForHidden\_py.pyc, чтобы получилось вот так:



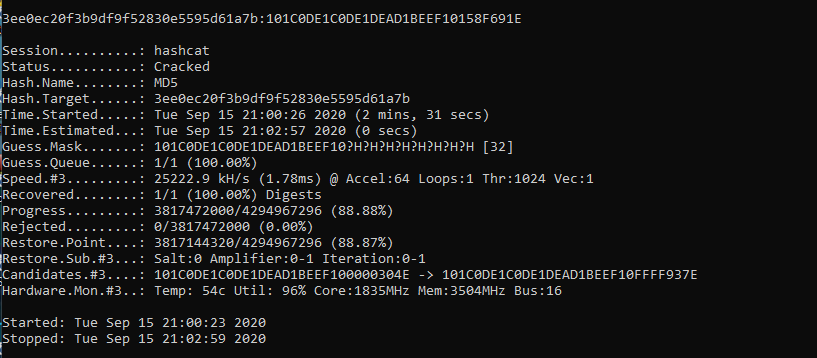
1. Далее декомпилируем полученный файл. Можно в онлайн декомпиляторах. Я сделал это с помощью uncompyle6:

>uncompyle6 -o hidden\_py\_unpack.py hidden\_py.pyc



1. Теперь файл откроется. Изучив код видно, что флаг расшифровывается, если ввели правильную часть ключа. Часть ключа проверяется так md5(«101C0DE1C0DE1DEAD1BEEF10» + «input») == '3ee0ec20f3b9df9f52830e5595d61a7b'
2. Сбрутить это можно с помощью hashcat:

>hashcat.exe -a 3 -m 0 3ee0ec20f3b9df9f52830e5595d61a7b 101C0DE1C0DE1DEAD1BEEF10?H?H?H?H?H?H?H?H



Недостающая часть ключа: 158F691E. Введем её или в .elf или .py и получим флаг.

