WriteUP Reverse 300. KrasCTF 2017

Выражение: “Поступи с ней, как другие поступают с подобными фразами.” говорит о том, что нужно посмотреть, как работают фейковые файлы. Вывод сообщения в фейковом файле происходит посимвольно. К каждому символу предварительно применяется исключающее ИЛИ с константой, она нам и нужна.

```
 ,=< 0x00000977      eb1b            jmp 0x994                       ;[1]
 |       ; JMP XREF from 0x000009a9 (sub.strlen_8d0)
.--> 0x00000979      8b45bc          mov eax, dword [rbp - local_44h]
||   0x0000097c      4898            cdqe
||   0x0000097e      0fb64405c0      movzx eax, byte [rbp + rax - 0x40]
||   0x00000983      3245bb          xor al, byte [rbp - local_45h]
||   0x00000986      0fbec0          movsx eax, al
||   0x00000989      89c7            mov edi, eax
||   0x0000098b      e870fcffff      call sym.imp.putchar            ;[2]
||   0x00000990      8345bc01        add dword [rbp - local_44h], 1
!|       ; JMP XREF from 0x00000977 (sub.strlen_8d0)
|`-> 0x00000994      8b45bc          mov eax, dword [rbp - local_44h]
|    0x00000997      4863d8          movsxd rbx, eax
|    0x0000099a      488d45c0        lea rax, [rbp - local_40h]
|    0x0000099e      4889c7          mov rdi, rax
|    0x000009a1      e86afcffff      call sym.imp.strlen             ;[3]
|    0x000009a6      4839c3          cmp rbx, rax
`==< 0x000009a9      72ce            jb 0x979                        ;[4]
```

```
xor eax, eax
mov byte [rbp - local_45h], 0x72 ; 'r'
mov byte [rbp - local_40h], 0x26 ; '&'
mov byte [rbp - local_3fh], 0x1a
```

Применяем исключающее ИЛИ к HEX-строке, которая дана в формулировке задания, с константой 0x72. Получим строку “0F B6 85 9B FE FF FF 0F”. Это сигнатура искомого файла. Найдем этот файл с помощью YARA. Напишем следующее правило.

```
rule search
{
        strings:
                $sign = { 0F B6 85 9B FE FF FF 0F }

        condition:
                $sign
}
```

Номер искомого файла равен 679. Он принимает на вход файл длиной 32 байта. Также внутри программы инициализируются три массива:

1. Массив вычетов. Из считанного значения из файла вычитается очередной элемент данного массива. Элементы массива – старшие и младшие половины значений из файла.

```
mov byte [rbp - local_140h], 0xc
mov byte [rbp - local_13fh], 0x10
mov byte [rbp - local_13eh], 1
mov byte [rbp - local_13dh], 0x30 ; '0'
mov byte [rbp - local_13ch], 0xa
mov byte [rbp - local_13bh], 0x30 ; '0'
mov byte [rbp - local_13ah], 0
mov byte [rbp - local_139h], 0x30 ; '0'
mov byte [rbp - local_138h], 0xd
mov byte [rbp - local_137h], 0x20
mov byte [rbp - local_136h], 6
mov byte [rbp - local_135h], 0x20
mov byte [rbp - local_134h], 0xe
mov byte [rbp - local_133h], 0x30 ; '0'
mov byte [rbp - local_132h], 9
mov byte [rbp - local_131h], 0x20
```

2. Массив с сообщением. После всех преобразований данные из файла сравниваются с элементами данного массива.

```
mov byte [rbp - local_149h], 0x4a ; 'J'
mov byte [rbp - local_148h], 0x55 ; 'U'
mov byte [rbp - local_147h], 0x53 ; 'S'
mov byte [rbp - local_146h], 0x54 ; 'T'
mov byte [rbp - local_145h], 0x5f ; '_'
mov byte [rbp - local_144h], 0x41 ; 'A'
mov byte [rbp - local_143h], 0x44 ; 'D'
mov byte [rbp - local_142h], 0x44 ; 'D'
mov byte [rbp - local_141h], 0
```

3. Массив с масками. К преобразованным данным из файла применяется исключающее ИЛИ с элементами из данного массива.

```
mov byte [rbp - local_151h], 0x67 ; 'g'
mov byte [rbp - local_150h], 0x49 ; 'I'
mov byte [rbp - local_14fh], 0x5d ; ']'
mov byte [rbp - local_14eh], 0x4b ; 'K'
mov byte [rbp - local_14dh], 0x78 ; 'x'
mov byte [rbp - local_14ch], 0x5e ; '^'
mov byte [rbp - local_14bh], 0x56 ; 'V'
mov byte [rbp - local_14ah], 0x5b ; '['
```

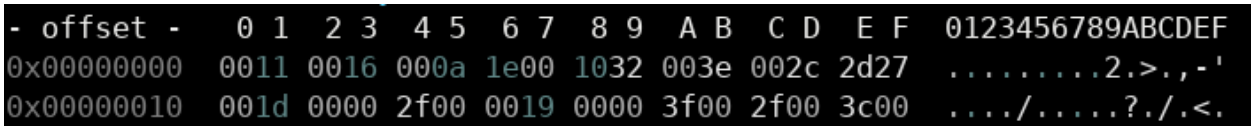
4. Массив со смещениями относительно конца файла.

```
mov byte [rbp - local_130h], 0x13
mov byte [rbp - local_12fh], 0xf
mov byte [rbp - local_12eh], 0x1f
mov byte [rbp - local_12dh], 2
mov byte [rbp - local_12ch], 0x1b
mov byte [rbp - local_12bh], 0x15
mov byte [rbp - local_12ah], 0x18
mov byte [rbp - local_129h], 6
mov byte [rbp - local_128h], 0x12
mov byte [rbp - local_127h], 0x11
mov byte [rbp - local_126h], 0x1d
mov byte [rbp - local_125h], 0xc
mov byte [rbp - local_124h], 0x1a
mov byte [rbp - local_123h], 0x17
mov byte [rbp - local_122h], 9
mov byte [rbp - local_121h], 4
```

Программа осуществляет следующий алгоритм проверки корректности файла:

1. Обнуление суммы;
2. Считывание первого значения;
3. Вычитание младшей части значения;
4. Добавление к сумме;
5. Считывание второго значения;
6. Вычитание старшей части значения;
7. Добавление к сумме;
8. Исключающее ИЛИ суммы и маски;
9. Сравнение полученного значения с соответствующим элементом сообщения;

Производя все действия в обратном порядке, получаем следующий файл.



Складывая по два значения из файла, используя таблицу смещений, получаем флаг - **IMHOTEPH**