



Название:	Котик и фл@г
Категория:	Реверс-инжиниринг
Уровень:	Средний
Очки:	550
Описание:	Это AAA-котик?
Теги:	C, патчинг функций
Автор:	ROP

Прохождение:

Препятствие для решающих под номером 1.

Первое препятствие это то, что в ELF-файле есть проверка на имя программы. Оно должно быть "./kitten".

```
> ./kitten
```

Котик и флаг



Нажмите ENTER для запуска игры...



Если это не kitten или программа запущена под IDA, то происходит выход из приложения.

Ошибка!

~/CDB_CTF/reverse/april_ctf/Кот_да_еда > █

Препятствие для решающих под номером 2.

Файл статический, поэтому там находятся все библиотечный функции из заголовочных файлов, которые были использованы в программе. Из-за этого поиск немного усложнится.

The screenshot shows the IDA Pro interface. The assembly view displays the following code:

```
mov    [rbp-var_14], edi
mov    [rbp-var_20], rsi
mov    rax, fs:28h
mov    [rbp-var_8], rax
xor   eax, eax
mov    [rbp-var_10], 0
mov    [rbp-var_F], 0
mov    [rbp-var_E], 0
mov    [rbp-var_C], 0
mov    rax, [rbp+var_20]
mov    rax, [rax]
mov    edx, 8
lea    rcx, aKitten ; "./kitten"
mov    rsi, rcx
mov    rdi, rax
call   j_strcmp_ifunc
test  eax, eax
jz    short loc_402622
```

The debugger window shows the following assembly at address loc_402622:

```
loc_402622:
lea    rax, unk_48780B
mov    rsi, rax
mov    edi, 6
call   setlocale
lea    rax, unk_48780F
mov    rdi, rax
call   puts
```

The bottom pane shows the output of the program:

```
[1] Config file Ponce.cfg not found
[+] Ponce plugin running!
4BB320: name has been deleted: default_rwlockattr
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
```

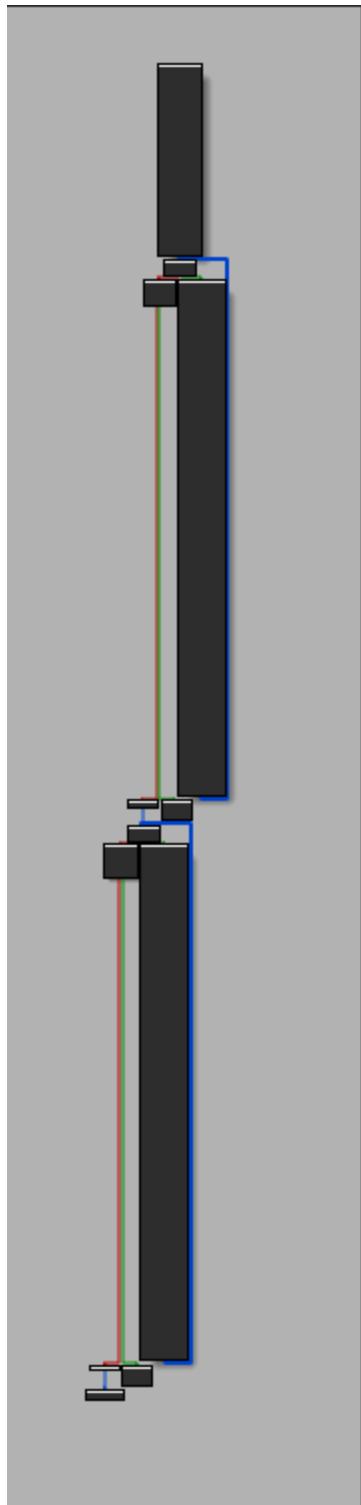
Препятствие для решающих под номером 3.

Файл упакован через UPX. И в нём изменён заголовок, чтобы нельзя было просто его распаковать.

Ложный вектор.

Самый главный ложный вектор - это пытаться выиграть в игре и изучать алгоритм для дешифровки в функции `give_flag`. Там ложный

флаг :)



Правильное решение.

Снимаем UPX, поменяв нужный заголовок через HEX-редактор.



Такой должен быть.

Потом используем `upx -d файл`.

```
› upx -d kitten
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2020
UPX 3.96          Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

      File size        Ratio        Format        Name
-----  -----  -----
     835288 <-    349244    41.81%    linux/amd64    kitten

Unpacked 1 file.
~/CDB_CTF/reverse/april_ctf/Кот_да_еда › █
```

Патчим проверку имени.

```

; _unwind {
endbr64
push    rbp
mov     rbp, rsp
sub    rsp, 20h
mov     [rbp+var_14], edi
mov     [rbp+var_20], rsi
mov     rax, fs:28h
mov     [rbp+var_8], rax
xor    eax, eax
mov     [rbp+var_10], 0
mov     [rbp+var_f], 0
mov     [rbp+var_e], 0
mov     [rbp+var_c], 0
mov     rax, [rbp+var_20]
mov     rax, [rax]
mov     edx, 8
lea     rcx, aKitten      ; "./kitten"
mov     rsi, rcx
mov     rdi, rax
call    j_strcmp_ifunc
test    eax, eax
Jmp    short loc_402622

```

```

loc_402622:
lea     rax, unk_48780B
mov     rsi, rax

```

48B320: name has been deleted: default_rwlockattr
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Applied 1/1 patch(es)
Applied 1/1 patch(es)

(вариант 1) Изучаем функции в `main` и понимаем, что функция `printf` была изменена автором этого таска.

```

; _ide_single_encoding_compare_cold
; _ide_mixed_encoding_compare_cold
; _add_ids_cold
; _linear_search_ids_cold
; _search_object_cold
; _Unwind_Find_FDE_cold
; _find_or_encode_value_cold
; _get_personality_id_cold
; _start_cold
; _di_relocate_static_pie
; _deregister_tm_clones
; _register_tm_clones
; _do_global_dtors_aux
; _frame_dummy
; _print_main
; _print_bar
; _print_menu
; _go_magazine1
; _get_water
; _go_sleep
; _correct_values
; _print_cat_with_params
; _check_params
; _give_flag
; _mail
; _print_flag
; _execute_code_end_section

Line 82 of 1085
Graph overview

```

```

short loc_410CAF:
nopabs [rsi+80h+var_80], xmm0
nopabs [rsi+80h+var_78], xmm1
nopabs [rsi+80h+var_60], xmm2
nopabs [rsi+80h+var_50], xmm3
nopabs [rsi+80h+var_40], xmm4
nopabs [rsi+80h+var_30], xmm5
nopabs [rsi+80h+var_20], xmm6
nopabs [rsi+80h+var_10], xmm7

```

```

loc_410CAF:
mov    rax, fs:28h
mov    [rsp+80h+var_C0], rax
xor    eax, eax
mov    rsi, rdi
lea    rax, [rsp+80h+arg_0]
mov    rdx, rax
mov    rdi, csstdout
mov    rax, [rsp+80h+var_D0], rax
xor    eax, eax
lea    rax, [rsp+80h+var_B8]
mov    [rsp+80h+var_08], 0
mov    [rsp+80h+var_D4], 30h ; 0
mov    rax, [rsp+80h+var_0C], rax
call    vfprintf_internal
mov    rdx, [rsp+80h+var_C0]
sub    rdx, rdx
leah   rdx, loc_410011
Jmp    short loc_410011

```

```

add    r15, 80h
loc_410011:
call    __stack_chk_fail_global
; // starts at 410C50
add    r15, 80h
ret
printf endp

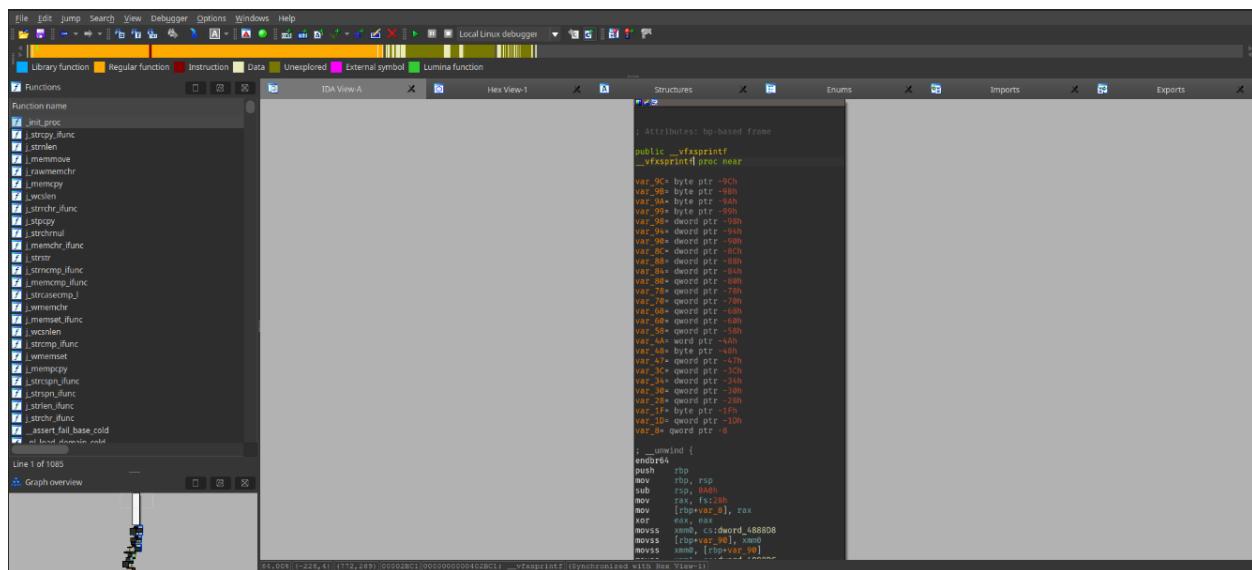
```

```

; Attributes: bp-based frame

public __stack_chk_fail_global
__stack_chk_fail_global proc near
; __ unwind {
endbr64
push    rbp
mov     rbp, rsp
mov     eax, 0
call    __vfxsprintf |
nop
pop    rbp
retn
; } // starts at 402BAC
__stack_chk_fail_global endp

```



В этой функции происходит вся магия. Просто её сложно найти.

Изучаем этот блок кода и понимаем, что программа хочет, чтобы у нас была системная переменная `cDb_rEv2rE` со значением флага. И ещё должна быть системная переменная `g00d_oR_bad` со значением 1.

Только в этом случае программа напечатает флаг.