

# PWN r3ktMeNu WriteUP

## Решение 1

Запускаем наш бинарник и видим, что нужно ввести пароль.

```
madwayz@life-lab: ~/Desktop
File Edit View Search Terminal Help
madwayz@life-lab:~/Desktop$ ./binary

#
# # ##### # # # # # # # #
# # # # ## ## # # # # # # #
# # # # # ## # # # # # # #
##### # # # # # # # # # #
# # # # # # # # # # # # #
# # ##### # # # # # # #

Input password:
```

Если пароль неверный, то выкидывает такую ошибку.

```
madwayz@life-lab: ~/Desktop
File Edit View Search Terminal Help
ERROR! Wrong password! Try again...

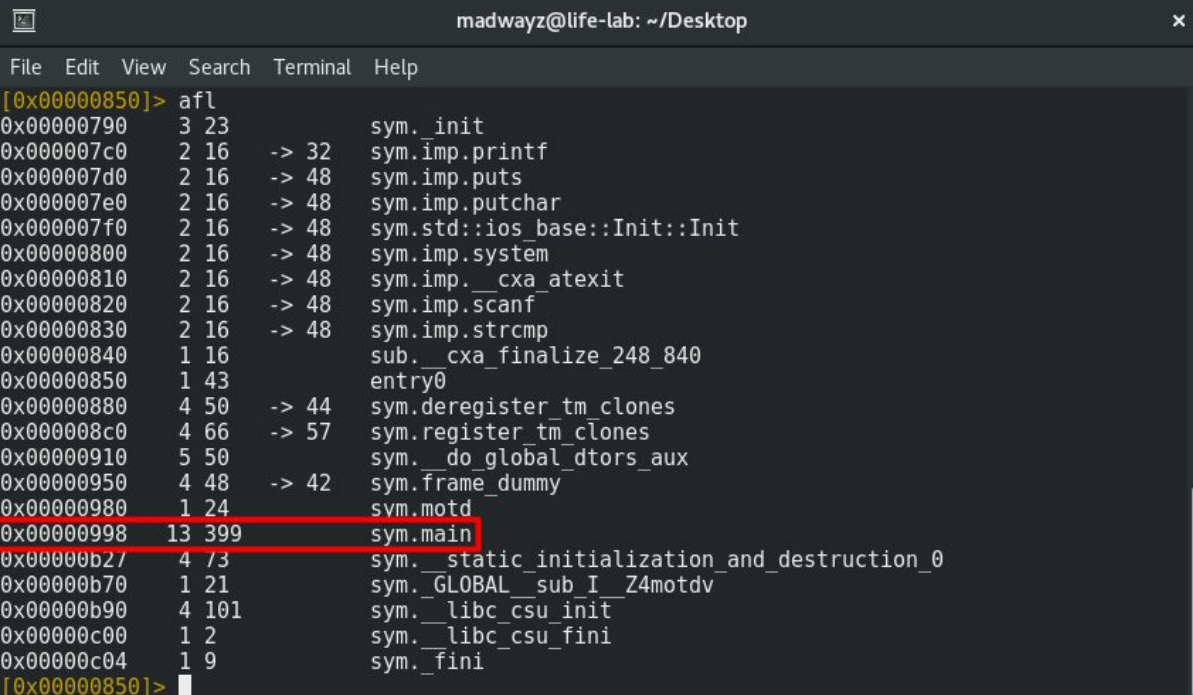
#
# # ##### # # # # # # # #
# # # # ## ## # # # # # # #
# # # # # ## # # # # # # #
##### # # # # # # # # # #
# # # # # # # # # # # # #
# # ##### # # # # # # #

Input password:
```

Запускаем этот бинарник в **radare2** с ключём **-A**

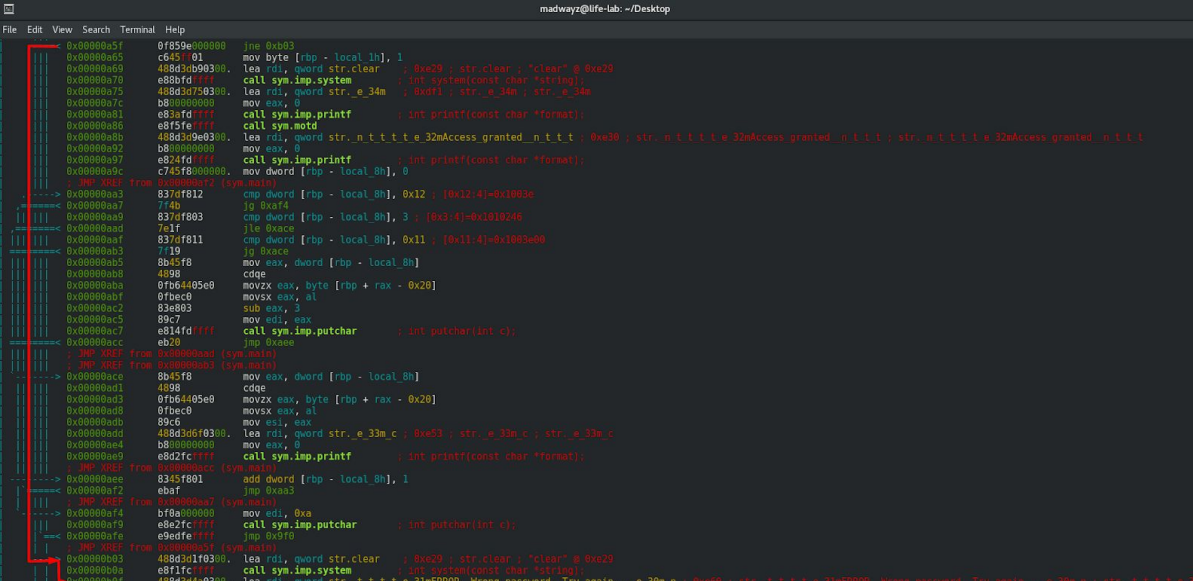
```
madwayz@life-lab:~/Desktop$ r2 -A binary
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze len bytes of instructions for references (aar)
[x] Analyze function calls (aac)
[ ] [*] Use -AA or aaaa to perform additional experimental analysis.
[x] Constructing a function name for fc.* and sym.func.* functions (aan)
[0x00000850]>
```

Выводим весь список функций, командой **afl** и находим там **main**



```
madwayz@life-lab: ~/Desktop
File Edit View Search Terminal Help
[0x00000850]> afl
0x00000790 3 23 sym._init
0x000007c0 2 16 -> 32 sym.imp.printf
0x000007d0 2 16 -> 48 sym.imp.puts
0x000007e0 2 16 -> 48 sym.imp.putchar
0x000007f0 2 16 -> 48 sym.std::ios_base::Init::Init
0x00000800 2 16 -> 48 sym.imp.system
0x00000810 2 16 -> 48 sym.imp._cxa_atexit
0x00000820 2 16 -> 48 sym.imp.scanf
0x00000830 2 16 -> 48 sym.imp.strcmp
0x00000840 1 16 sub._cxa_finalize_248_840
0x00000850 1 43 entry0
0x00000880 4 50 -> 44 sym.deregister_tm_clones
0x000008c0 4 66 -> 57 sym.register_tm_clones
0x00000910 5 50 sym._do_global_dtors_aux
0x00000950 4 48 -> 42 sym.frame_dummy
0x00000980 1 24 sym.motd
0x00000998 13 399 sym.main
0x00000b27 4 73 sym._static_initialization_and_destruction_0
0x00000b70 1 21 sym.GLOBAL_sub_I_Z4motdv
0x00000b90 4 101 sym._libc_csu_init
0x00000c00 1 2 sym._libc_csu_fini
0x00000c04 1 9 sym._fini
[0x00000850]>
```

Анализируем функцию **main** командой **pdf @ main** и сразу же видим, что есть переход в ветку **false**, если пароль неверный. Отлично. Избавимся от этого перехода.



```
madwayz@life-lab: ~/Desktop
File Edit View Search Terminal Help
0x00000a5f 0f85e00000 jne 0xb03
0x00000a65 c64501 mov byte [rbp - local_1h], 1
0x00000a69 488d3db90300 lea rdi, qword str.clear ; 0xb29 : str.clear : "clear" @ 0xb29
0x00000a70 e88b0000 call sym.imp.system ; int system(const char *string);
0x00000a75 488d3d7f0300 lea rsi, qword str_e_34m ; 0xb01 : str_e_34m : str_e_34m
0x00000a7c b800000000 mov eax, 0
0x00000a81 e83e000000 call sym.imp.printf ; int printf(const char *format);
0x00000a86 e93fe00000 call sym.motd
0x00000a8b 488d3d9e0300 lea rdi, qword str_n_t_t_t_t_e_32mAccess_granted_n_t_t_t_0 ; 0xb30 : str_n_t_t_t_t_e_32mAccess_granted_n_t_t_t_0 : str_n_t_t_t_t_e_32mAccess_granted_n_t_t_t_0
0x00000a92 b800000000 mov eax, 0
0x00000a97 e824000000 call sym.imp.printf ; int printf(const char *format);
0x00000a9c c745f8000000 mov dword [rbp - local_8h], 0
; JMP XREF from 0x00000a92 (sym.main)
0x00000aa3 837df812 cmp dword [rbp - local_8h], 0x12 ; 0x12(4)=0x1093e
0x00000aa7 740b jg 0xb44
0x00000aa9 837df803 cmp dword [rbp - local_8h], 3 ; 0x3(4)=0x1018246
0x00000aad 7e1f jle 0xb4e
0x00000aef 837df811 cmp dword [rbp - local_8h], 0x11 ; 0x11(4)=0x1003e00
0x00000ab3 7419 jg 0xb4e
0x00000ab5 b845f8 mov eax, dword [rbp - local_8h]
0x00000ab8 4d08 cdqe
0x00000aba 0f644405e0 movzx eax, byte [rbp + rax - 0x20]
0x00000abf 0fbec0 movsx eax, al
0x00000ac2 83e803 sub eax, 3
0x00000ac5 89c7 mov edi, eax
0x00000ac7 e814000000 call sym.imp.putchar ; int putchar(int c);
0x00000acc eb20 jmp 0xb4e
; JMP XREF from 0x00000aa3 (sym.main)
; JMP XREF from 0x00000abf (sym.main)
0x00000ace b845f8 mov eax, dword [rbp - local_8h]
0x00000ad1 4d08 cdqe
0x00000ad3 0f644405e0 movzx eax, byte [rbp + rax - 0x20]
0x00000ad8 0fbec0 movsx eax, al
0x00000adb 89c5 mov esi, eax
0x00000add 488d3d9e0300 lea rdi, qword str_e_33m_c ; 0xb31 : str_e_33m_c : str_e_33m_c
0x00000ade b800000000 mov eax, 0
0x00000ae9 e8d2000000 call sym.imp.printf ; int printf(const char *format);
; JMP XREF from 0x00000ace (sym.main)
0x00000af3 8345f801 add dword [rbp - local_8h], 1
0x00000af7 ebaf jmp 0xb4a
; JMP XREF from 0x00000ae7 (sym.main)
0x00000af9 b70a000000 mov edi, 0xa
0x00000afb e8e2000000 call sym.imp.putchar ; int putchar(int c);
0x00000afe e9edfe0000 jmp 0xb40
; JMP XREF from 0x00000af3 (sym.main)
0x00000b02 488d3d1f0300 lea rdi, qword str.clear ; 0xb29 : str.clear : "clear" @ 0xb29
0x00000b05 e81fc00000 call sym.imp.system ; int system(const char *string);
0x00000b08 488d3d4e0300 lea rdi, qword str_t_t_t_t_e_31mERROR_Wrong_password_Try_again..._e_30m_n_0 ; 0xb00 : str_t_t_t_t_e_31mERROR_Wrong_password_Try_again..._e_30m_n_0 : str_t_t_t_t_e_31mERROR_Wrong_password_Try_again..._e_30m_n_0
```

Перезапустим программу в режиме *read-write* командой **oo+**. Введем адрес перехода **jne 0xb03 - 0x0000a5f**  
 Заменяем на **pop** командой **wao pop**. Пишем **q**, чтобы выйти из тулзы и запускаем бинарник **./binary** и видим флаг.

```

# # ##### # # # # # # # #
# # # # # # # # # # # # #
# # # # # # # # # # # # #
##### # # # # # # # # #
# # # # # # # # # # #
# # ##### # # # # #
# # # # # # # # # # #
# # # # # # # # # # #

Access granted!
CTF{rEvErSwaSOWned}
madwayz@life-lab:~/Desktop$

```

## Решение 2

Откроем в том же радаре наш бинарник и видим здесь строку. Функция **strcmp()** должна с чем-то сравниваться. Рядом больше строк нет, значит можно сделать вывод, что строка **[0x3:4]=0x1010243** - пароль.

```

0x00000a45 e8d6fdfff call sym.imp.scanf ; int scanf(const char *format);
0x00000a4a 488d45c0 lea rax, qword [rbp - local_40h]
0x00000a4e 488d35c20300 lea rsi, qword str_0x3:4_0x1010243 ; 0xe17 ; str_0x3:4_0x1010243 ; "[0x3:4]=0x1010243" @ 0xe17
0x00000a55 4889c7 mov rdi, rax
0x00000a58 e8d3fdfff call sym.imp.strcmp ; int strcmp(const char *s1, const char *s2);

```

Вводим и получаем флаг. Фиаско!

```

# # ##### # # # # # # # #
# # # # # # # # # # # # #
# # # # # # # # # # # # #
##### # # # # # # # # #
# # # # # # # # # # #
# # ##### # # # # #
# # # # # # # # # # #
# # # # # # # # # # #

Access granted!
CTF{rEvErSwaSOWned}
madwayz@life-lab:~/Desktop$

```

Флаг: CTF{rEvErSwaSOWned}