

Challenge: Wide

Challenge Description :

We've received reports that Draeger has stashed a huge arsenal in the pocket dimension Flaggie Alpha. You've managed to smuggle a discarded access terminal to the Widely Inflated Dimension Editor from his headquarters, but the entry for the dimension has been encrypted. Can you make it inside and take control?

Context :

- We are given a compiled file, when we run the file it pops up with a weird TUI interface . Going on one of the options by inputting the names in as a numeric list, e.g Primus = 1 and Cheagaz = 2. . Selecting the Option six asks for a password as it is shown as "Encrypted".

Notes :

- Tools:
 - Text editor - To open the bash script / downloaded files.
 - You can choose your way to decoding the base64 string for simplicity im going to use a website, "www.base64decode.org"

Flag :

- Download the file and run it. I started doing some basic static analysis on the file using Strace , Ltrace, objdump and some other tools. I couldn't find anything interesting or anything linking to a password.

```
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Wide/rev_wide$ ./wide db.ex
[*] Welcome user: kr4eq4L2$12xb, to the Widely Inflated Dimension Editor [*]
[*] Serving your pocket dimension storage needs since 14,012.5 B [*]
[*] Displaying Dimensions.... [*]
[*]      Name      |      Code      |      Encrypted      [*]
[X] Primus        | people breathe variety practice | [*]
[X] Cheagaz       | scene control river importance   | [*]
[X] Byenoovia     | fighting cast it parallel        | [*]
[X] Cloteprea     | facing motor unusual heavy       | [*]
[X] Maraqa        | stomach motion sale valuable    | [*]
[X] Aidor         | feathers stream sides gate       | [*]
[X] Flaggie Alpha | admin secret power hidden       | * [*]
which dimension would you like to examine?
```

- When that fails, when I did some dynamic analysis on the file starting with IDA freeware, I got nothing from extracting strings or from just reading the binary.
- Instead I went to run it against another tool called Radare2, using this I got a better analysis and found something interesting. Using Radare2 was weird to start off with but finally got a slight handle.
- Opening it, i ran a command, [[AFL](#)] to show a bunch of Entries to enter as well as how the file was structured, i can enter the entries and print the binary of them entering the command : [[pdf@\(data_entry_name\)](#)]

E.g [[pdf@sym.imp.fread](#)]

```
[0x000008e0]> afl
0x00000800 1 6 sym.imp.wcscmp
0x00000810 1 6 sym.imp.puts
0x00000820 1 6 sym.imp.fread
0x00000830 1 6 sym.imp.mbstowcs
0x00000840 1 6 sym.imp.fclose
0x00000850 1 6 sym.imp.printf
0x00000860 1 6 sym.imp.fgets
0x00000870 1 6 sym.imp.calloc
0x00000880 1 6 sym.imp.ftell
0x00000890 1 6 sym.imp.strtol
0x000008a0 1 6 sym.imp.fseek
0x000008b0 1 6 sym.imp.fopen
0x000008c0 1 6 sym.imp.exit
0x000008d0 1 6 sym.imp.__cxa_finalize
0x000008e0 1 42 sub.entry0_8e0
0x00000910 4 40 sub.deregister_tm_clones
0x00000950 4 57 sub.register_tm_clones_9
0x000009a0 5 51 sub.__do_global_dtors_aux
0x000009e0 1 10 sub.frame_dummy_9e0
0x00001070 1 2 sub.__libc_csu_fini_1070
0x000009ea 15 1016 sub.menu_9ea
0x00001074 1 9 sym._fini
0x00001000 4 101 sub.__libc_csu_init_1000
0x00000de2 11 536 sub.main_de2
0x000007d0 3 23 sub._init_7d0
0x000001e0 1 89 sub.interp_1e0
```

- Using this i opened the main entry, got nothing, same with some sub files, i Finally opened a entries that gave me the password for the application :
[[pdf@sym.menu](#)]
- Either short for system menu or something else It should have been one of the first things to check based on what we are checking out.

- The Password is placed at the bottom of the result of the [[sym.menu](#)] Command i gave, the password in question being : sup3rs3cr3tw1d3

```

488d302004.. lea rdi, str._x__mat_entry_is_encrypted__please_enter_your_wide_decryption_key. ; 0x
key: " ; const char *format
b800000000 mov eax, 0
e89cfbffff call sym.imp.printf ; int printf(const char *format)
488b155513.. mov rdx, qword [obj.stdin] ; obj.__TMC_END__
; [0x202010:8]=0 ; FILE *stream

488d8540ff.. lea rax, [s]
be10000000 mov esi, 0x10 ; fcn.00000010 ; int size
4889c7 mov rdi, rax ; char *s
e891fbffff call sym.imp.fgets ; char *fgets(char *s, int size, FILE *stream)
488d8d40ff.. lea rcx, [s]
488d8540fe.. lea rax, [pwcs]
ba10000000 mov edx, 0x10 ; fcn.00000010 ; size_t n
4889ce mov rsi, rcx ; const char *s
4889c7 mov rdi, rax ; wchar_t *pwcs
e843fbffff call sym.imp.mbstowcs ; size_t mbstowcs(wchar_t *pwcs, const char *s, size_t n)
488d8540fe.. lea rax, [pwcs]
488d351d04.. lea rsi, str.sup3rs3cr3tw1d3 ; 0x1118 ; U"sup3rs3cr3tw1d3" ; const wchar_t *s2
4889c7 mov rdi, rax ; const wchar_t *s1
e8fdafaaff call sym.imp.wcsncmp ; int wcsncmp(const wchar_t *s1, const wchar_t *s2)
85c0 test eax, eax
0f85ae000000 jne 0xdb9
c78534feff.. mov dword [var_1cch], 0
eb7c jmp 0xd93
sub menu.0ea.0.0xd9c(x)

```

- Running the file again and going to the six option to prompt in the password gave us the flag : HTB{som3_string5_4r3_w1d3}

```

birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Wide/rev_wide$ ./wide db.ex
[*] Welcome user: kr4eq4L2$12xb, to the Widely Inflated Dimension Editor [*]
[*] Serving your pocket dimension storage needs since 14,012.5 B [*]
[*] Displaying Dimensions.... [*]
[*] Name | Code | Encrypted [*]
[X] Primus | people breathe variety practice | [*]
[X] Cheagaz | scene control river importance | [*]
[X] Byenoovia | fighting cast it parallel | [*]
[X] Cloteprea | facing motor unusual heavy | [*]
[X] Maraqa | stomach motion sale valuable | [*]
[X] Aidor | feathers stream sides gate | [*]
[X] Flaggle Alpha | admin secret power hidden | * [*]
Which dimension would you like to examine? 6
[X] That entry is encrypted - please enter your WIDE decryption key: sup3rs3cr3tw1d3
HTB{som3_string5_4r3_w1d3}
Which dimension would you like to examine? Our home dimension
Which dimension would you like to examine?

```