sefi-roee / **CTFs-Writeups**

Branch: **master** ▾ **CTFs-Writeups** / picoCTF-2018 / Reversing / 11-radixs_terminal-400 / **solution.md** Find file Copy path

sefi-roee [picoCTF-2018] Fix radixs_terminal 06dbc5b on Oct 17

1 contributor

50 lines (31 sloc) 1.14 KB

Problem

Can you find the password to Radix's login? You can also find the executable in /problems/radix-s-terminal_1_35b3f86ea999e44d72e988ef4035e872?

Hints:

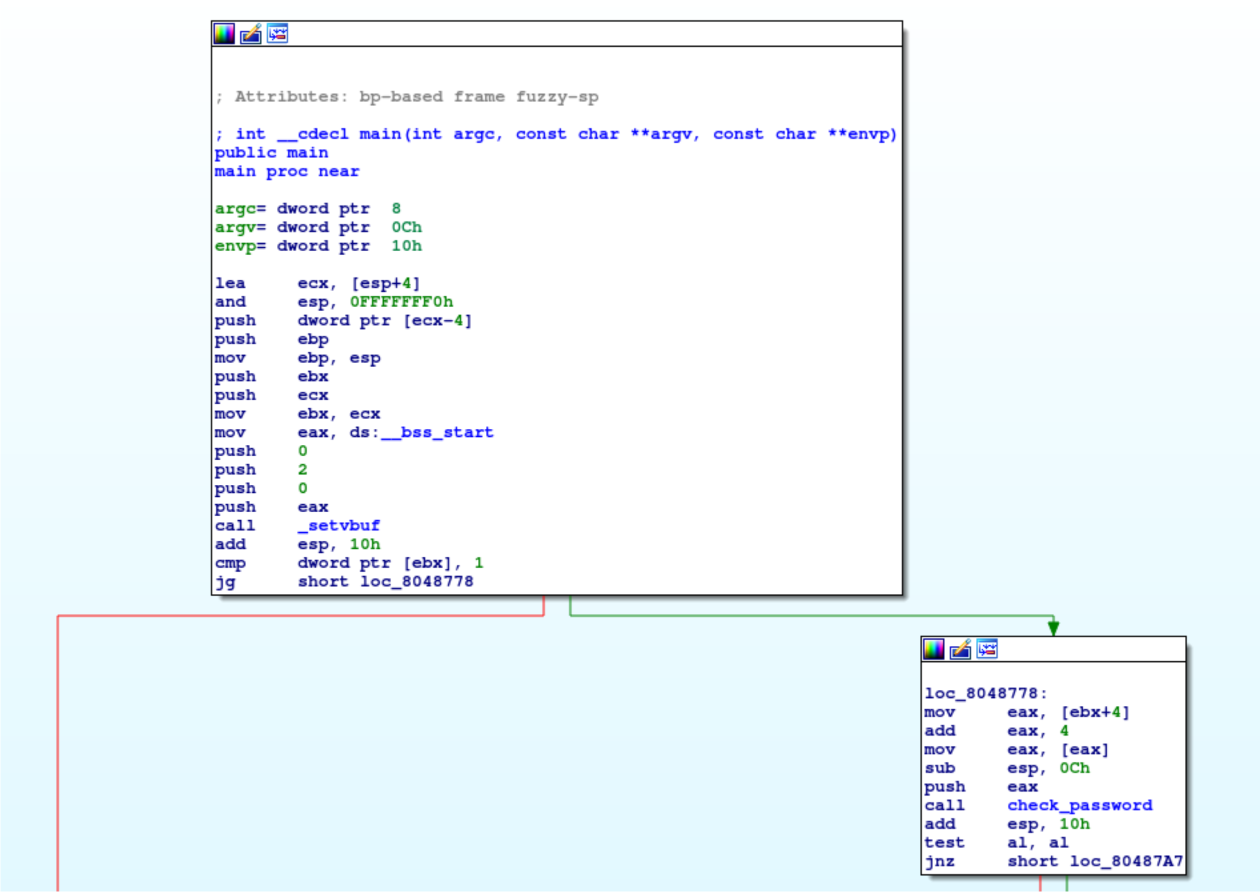
https://en.wikipedia.org/wiki/Base64

Solution:

First lets download the file and try to execute it

```
wget https://2018shell1.picoctf.com/static/2f848bb17aae35fb0fc703cbe15afbef/radix
chmod +x ./radix
./radix

Please provide a password!

./radix 1

Incorrect Password!
```

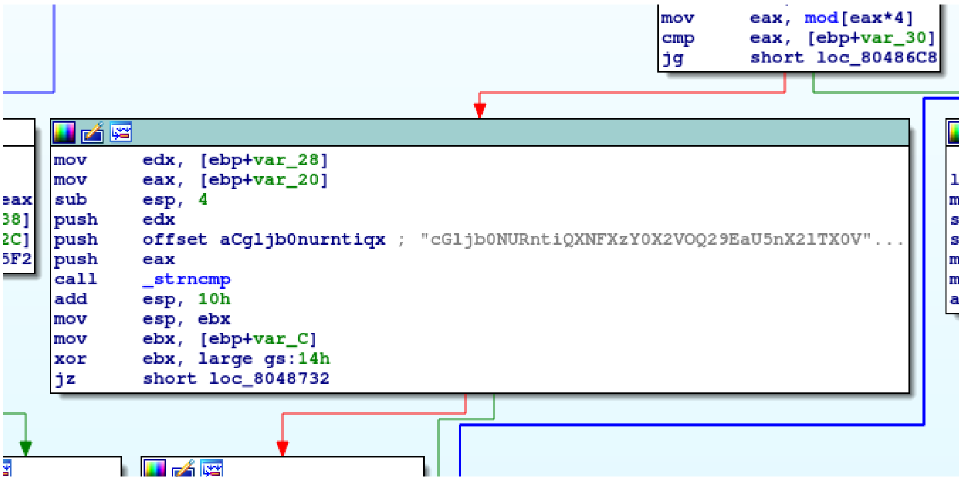
Lets look with IDA:



```
; Attributes: bp-based frame fuzzy-sp

; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ebx
push    ecx
mov     ebx, ecx
mov     eax, ds:__bss_start
push    0
push    2
push    0
push    eax
call    _setvbuf
add     esp, 10h
cmp     dword ptr [ebx], 1
jg      short loc_8048778
```

```
loc_8048778:
mov     eax, [ebx+4]
add     eax, 4
mov     eax, [eax]
sub     esp, 0Ch
push    eax
call    check_password
add     esp, 10h
test    al, al
jnz     short loc_80487A7
```

We can try to reverse the function, but there is a shortcut, there is a string inside (strings could find it as well):



```
mov     eax, mod[eax*4]
cmp     eax, [ebp+var_30]
jg      short loc_80486C8
```

```
mov     edx, [ebp+var_28]
mov     eax, [ebp+var_20]
sub     esp, 4
push    edx
push    offset aCgljb0nurntiqx ; "cGljb0NURntiQXNFXzY0X2VOQ29EaU5nX2lTX0V"...
push    eax
call    _strncmp
add     esp, 10h
mov     esp, ebx
mov     ebx, [ebp+var_C]
xor     ebx, large gs:14h
jz      short loc_8048732
```

```
cGljb0NURntiQXNFXzY0X2VOQ29EaU5nX2lTX0VBc1lfMTg3NTk3NDV9
```

Lets use the hint and try to decode it from base64.

```
echo "cGljb0NURntiQXNFXzY0X2VOQ29EaU5nX2lTX0VBc1lfMTg3NTk3NDV9" | base64 -d

picoCTF{bAsE_64_eNCoDiNg_iS_EAsY_18759745}
```

Just to make sure:

```
./radix picoCTF{bAsE_64_eNCoDiNg_iS_EAsY_18759745}

Congrats, now where's my flag?
```

Got lucky...

Flag: picoCTF{bAsE_64_eNCoDiNg_iS_EAsY_18759745}