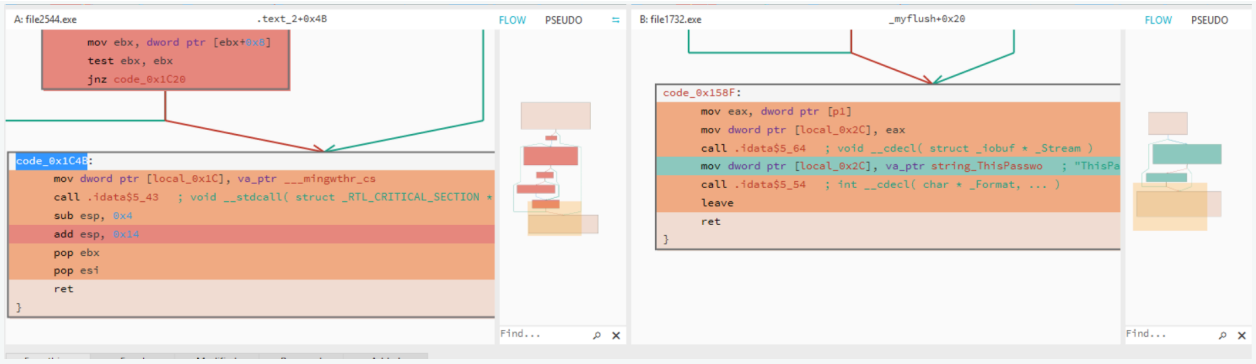
Deliverable #4: Report on analysis of the program

After analyzing the file2544.exe program, there were some similarities to file1732.exe found. The functionality seems to closely resemble program file1732.exe in that there is a login (“Enter password: “) and that after logging in there is a verbatim display string regarding IRC info (“This week’s IRC info: “). There is also a string (“Press [Enter] to continue: “) that is found in file1732’s program as well. This analysis has led me to believe that this program does have some similar functionality, with the possibility that this program could be doing more than file1732.

[Submission 1]

Below is a screenshot from the side-by-side analysis of the two programs. I believe that in file2544.exe, you can see the variable in which the password is stored and obfuscated (___minwthr_cs) as it aligns with file1732.exe's structure.



The call to _checkString below is where the entered password is verified (I believe).

```
and esp, 0xFFFFFFF0
sub esp, 0x20
call ___main   ; void __cdecl( void )
mov dword ptr [local_0x30], va_ptr string_Enterpassw   ; "Enter password: "
call .idata$5_57   ; int __cdecl( char * _Format, ... )
mov eax, dword ptr [.idata$5]   ; void *
mov dword ptr [local_0x28], eax
mov dword ptr [local_0x2C], 0x11
lea eax, [local_0x20]
mov dword ptr [local_0x30], eax
call .idata$5_51   ; char * __cdecl( char * _Buffer, int _MaxCount, struct _iobuf * _Stream )
call .idata$5_55   ; int __cdecl( void )
lea eax, [local_0x20]
mov dword ptr [local_0x30], eax
call _checkString   ; void __cdecl( int32_t p1 )
call _mypause   ; void __cdecl( void )
mov eax, 0x0
```

[Submission 2]

Deliverable #5: Decrypted password report

I was not entirely sure if we were supposed to use IDA or Relyze, but I used the Relyze code below from _checkString and decrypted the values that were being initialized here (with hopes they are the password). I got the following: .A. 226.3%.5(--.490

```
.text   :0x00001394        55                  push ebp
.text   :0x00001395        89E5                mov ebp, esp
.text   :0x00001397        83EC38              sub esp, 0x38
.text   :0x0000139A        C745F010000000      mov dword ptr [ebp-0x10], 0x10
.text   :0x000013A1        C645EB41            mov byte ptr [ebp-0x15], 0x41
.text   :0x000013A5        C645DB11            mov byte ptr [ebp-0x25], 0x11
.text   :0x000013A9        C645DC20            mov byte ptr [ebp-0x24], 0x20
.text   :0x000013AD        C645DD32            mov byte ptr [ebp-0x23], 0x32
.text   :0x000013B1        C645DE32            mov byte ptr [ebp-0x22], 0x32
.text   :0x000013B5        C645DF36            mov byte ptr [ebp-0x21], 0x36
.text   :0x000013B9        C645E02E            mov byte ptr [ebp-0x20], 0x2E
.text   :0x000013BD        C645E133            mov byte ptr [ebp-0x1F], 0x33
.text   :0x000013C1        C645E225            mov byte ptr [ebp-0x1E], 0x25
.text   :0x000013C5        C645E312            mov byte ptr [ebp-0x1D], 0x12
.text   :0x000013C9        C645E435            mov byte ptr [ebp-0x1C], 0x35
.text   :0x000013CD        C645E528            mov byte ptr [ebp-0x1B], 0x28
.text   :0x000013D1        C645E62D            mov byte ptr [ebp-0x1A], 0x2D
.text   :0x000013D5        C645E72D            mov byte ptr [ebp-0x19], 0x2D
.text   :0x000013D9        C645E812            mov byte ptr [ebp-0x18], 0x12
.text   :0x000013DD        C645E934            mov byte ptr [ebp-0x17], 0x34
.text   :0x000013E1        C645EA39            mov byte ptr [ebp-0x16], 0x39
.text   :0x000013E5        C745F400000000      mov dword ptr [ebp-0xC], 0x0
.text   :0x000013EC        EB23                jmp code_0x1411
```

[Submission 1]

So I'm guessing under '_releaseInfo' is the XOR key:

Hex: 0x28, 0x33, 0x22, 0x6F, 0x32, 0x2E, 0x2C, 0x23, 0x24, 0x33, 0x6F, 0x2F, 0x24, 0x35, 0x61, 0x62, 0x2F, 0x38, 0x2C, 0x24, 0x33, 0x28, 0x20, 0x17

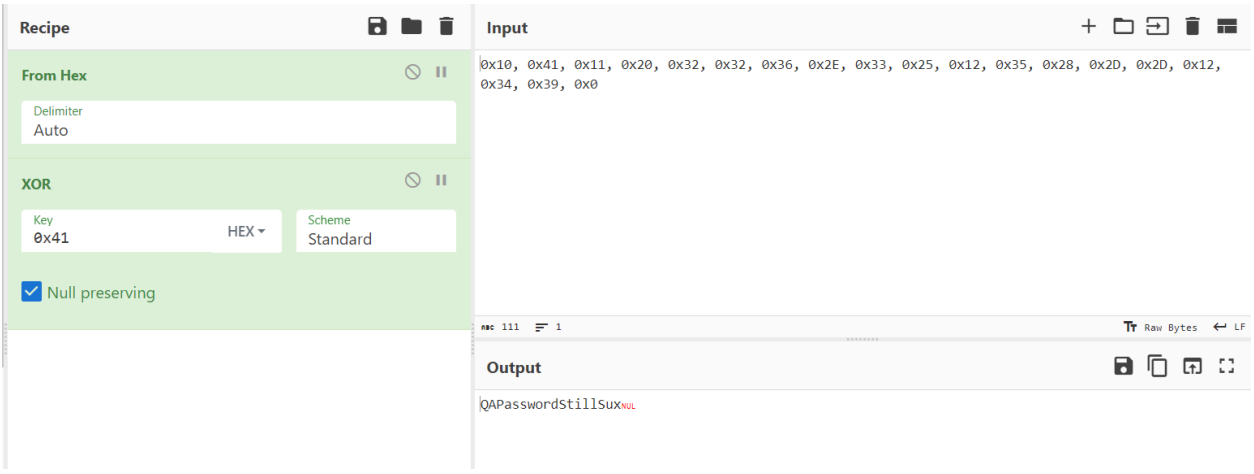
Equates to this: (3"o2.,#$3o/$5ab/8,$3(.

[Submission 2]

Hex: 0x11, 0x20, 0x32, 0x32, 0x36, 0x2E, 0x33, 0x25, 0x12, 0x35, 0x28, 0x2D, 0x2D, 0x12, 0x34, 0x39

XOR key: 0x41

Password: PasswordStillSux



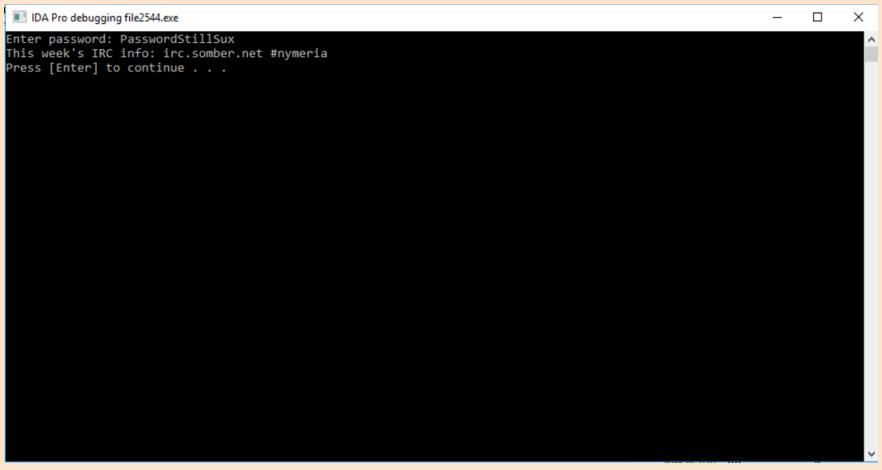
^remove 0x10 and 0x41 from the beginning of the input

Deliverable #6: Program Execution Report #2

After running the program and entering the password (PasswordStillSux) the program outputted the following:

This week's IRC info: irc.somber.net #nymeria
Press [Enter] to continue:

Afterward the process is then terminated.



Deliverable #7: IRC Channel Report #2

After joining the IRC server '*irc.somber.net*' and the channel *'#nymeria'* under the nick 'red_cloud', I observed an interesting and seemingly illicit ongoing conversation. Below is every message I encountered after joining (with usernames):

<@Alexi> Are you done testing exploit - we r doing it for real soon. It has to work. no second chance.
< VladTheDestroyer> right, I think it is working - I did test and uploadd it. You can get it here http://somber.net/uploads/file3666.exe
<@Alexi> Good
<@Alexi> Wait, is someone else here? Who are you?
< VladTheDestroyer> Вот дерьмо

I ran the commands /WHO and /WHOIS but nothing displayed (not sure if this was

internally figured or if I did this incorrectly), but I did notice at the top the only users were myself (red_cloud), @Alexi, and VladTheDestroyer. The top area also displayed a section that said 'Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2 normal] - denoting Vlad or Alexei were in charge of the channel having OP status.

As for the conversation, the messages definitely seemed to point toward some sort of potential exploit attack. A link to what I believe is the malicious program was sent as well. The two others realized I was in the chat at the end.

Further recommendations would be to look into the link provided. This seems to contain the EK or related information the two are looking to use. As for further OSINT on VladTheDestroyer and Alexi, possibly engaging in undercover conversation via the irc chat room could reveal more information if I can successfully gain their trust.

Regarding the Project Roadmap part 5 of this task: Add to your strategies log, as needed, based on what you find in the IP address research 0xCC has forwarded.

I did not see any additional IP info and was also not able to successfully run the /WHO or /WHOIS command when I was in the #nymeria channel.