

# Отчет к л/р №11

По дисциплине: Машинно-зависимые языки программирования

Ivan Smirnov

ИУ7-42Б 2024Г.

## Оглавление

Использованное ПО .....	2
Задание .....	2
Пошаговое объяснение решения .....	2

## Использованное ПО

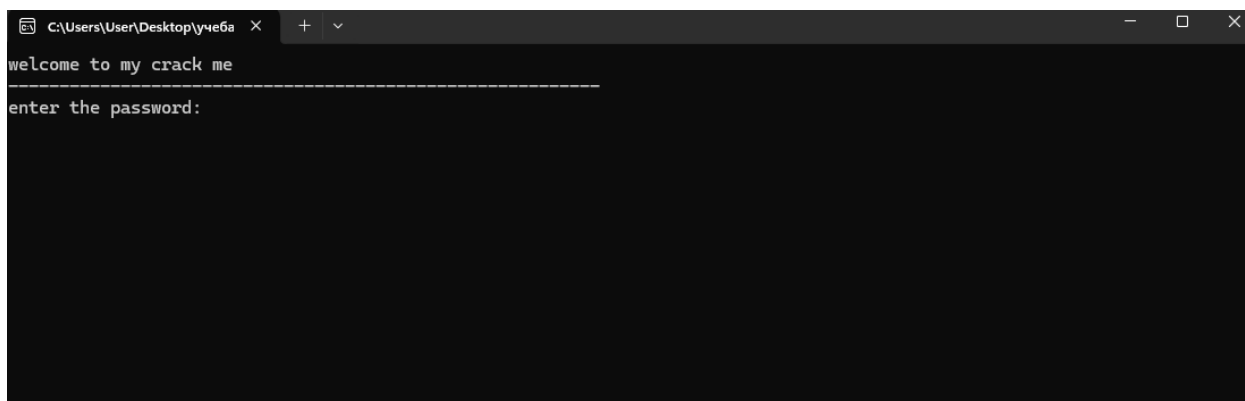
[x32dbg](#)

### Задание

С помощью x64dbg, IDA Freeware или других дизассемблеров/отладчиков определить пароль, необходимый для получения сообщения "congrats you cracked the password" в прикреплённой программе (<https://crackmes.one/crackme/5fe8258333c5d4264e590114>).

### Пошаговое объяснение решения

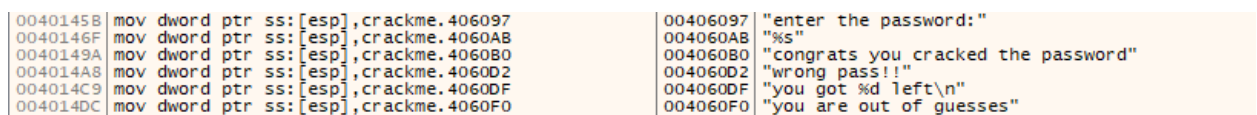
Сначала была протестирована сама программа, чтобы понять, какие сообщения можно получить на входе перед тем как ввести пароль.



Как видно, перед вводом пароля выводится сообщение “enter the password:”. Его и попробуем найти с помощью отладчика.


Запускаем отладчик, закидываем в него программу и попытаемся найти эту строку путем выполнения следующих действий.

- Нажимаем на стрелочку “Выполнить”
- Правый клик по команде
- Поиск в
- Текущий модуль
- Ссылки на строки



- Правый клик по строке
- Перейти к дизассемблерному коду

0040146B	89 4424 04	mov dword ptr ss:[esp+4],eax	
0040146F	C70424 AB604000	mov dword ptr ss:[esp],crackme.4060A8	4060A8:"%s"
00401476	E8 312A0000	call <JMP.&scantf>	
0040147B	8D 4424 1A	lea eax,dword ptr ss:[esp+1A]	
0040147F	89 4424 04	mov dword ptr ss:[esp+4],eax	
00401483	8D 4424 38	lea eax,dword ptr ss:[esp+38]	[esp+38]:NtAnsiCodePage+22E4
00401487	890424	mov dword ptr ss:[esp],eax	
0040148B	E8 052A0000	call <JMP.&strcmp>	
0040148F	8D 4424 48	mov dword ptr ss:[esp+48],eax	[esp+48]:L"C:\\Users\\User\\Desktop\\\\y4e6a\\
00401493	837C24 48 00	cmp dword ptr ss:[esp+48],0	[esp+48]:L"C:\\Users\\User\\Desktop\\\\y4e6a\\
00401498	75 0E	jne crackme.4014A8	
0040149A	C70424 80604000	mov dword ptr ss:[esp],crackme.4060B0	4060B0:"congrats you cracked the password"
004014A1	E8 0E2A0000	call <JMP.&puts>	
004014A6	EB 50	jmp crackme.4014F8	



```
C:\Users\User\Desktop\учеба >
welcome to my crack me
-----
enter the password:я ванек
```

В окошке FPU в EAX появился предположительно правильный пароль.

Скрыть FPU		
EAX	0061FF08	"password123"
EBX	00205000	
ECX	BB889459	
EDX	00000001	
EBP	0061FF28	&"бяа"
ESP	0061FED0	&"%s"
ESI	004012D0	<crackme.OptionalHeader.AddressOfEntryPoin
EDI	004012D0	<crackme.OptionalHeader.AddressOfEntryPoin
EIP	00401487	crackme.00401487
ESI	00000000	

Перезапускаем программу, вводим этот пароль и он оказывается правильным.