Отчет к л/р №11

По дисциплине: Машинно-зависимые языки программирования

Ivan Smirnov

ИУ7-42Б 2024г.

Оглавление

[Использованное ПО 2](#_Toc167038432)

[Задание 2](#_Toc167038433)

[Пошаговое объяснение решения 2](#_Toc167038434)

# Использованное ПО

[x32dbg](https://x64dbg.com/)

# 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

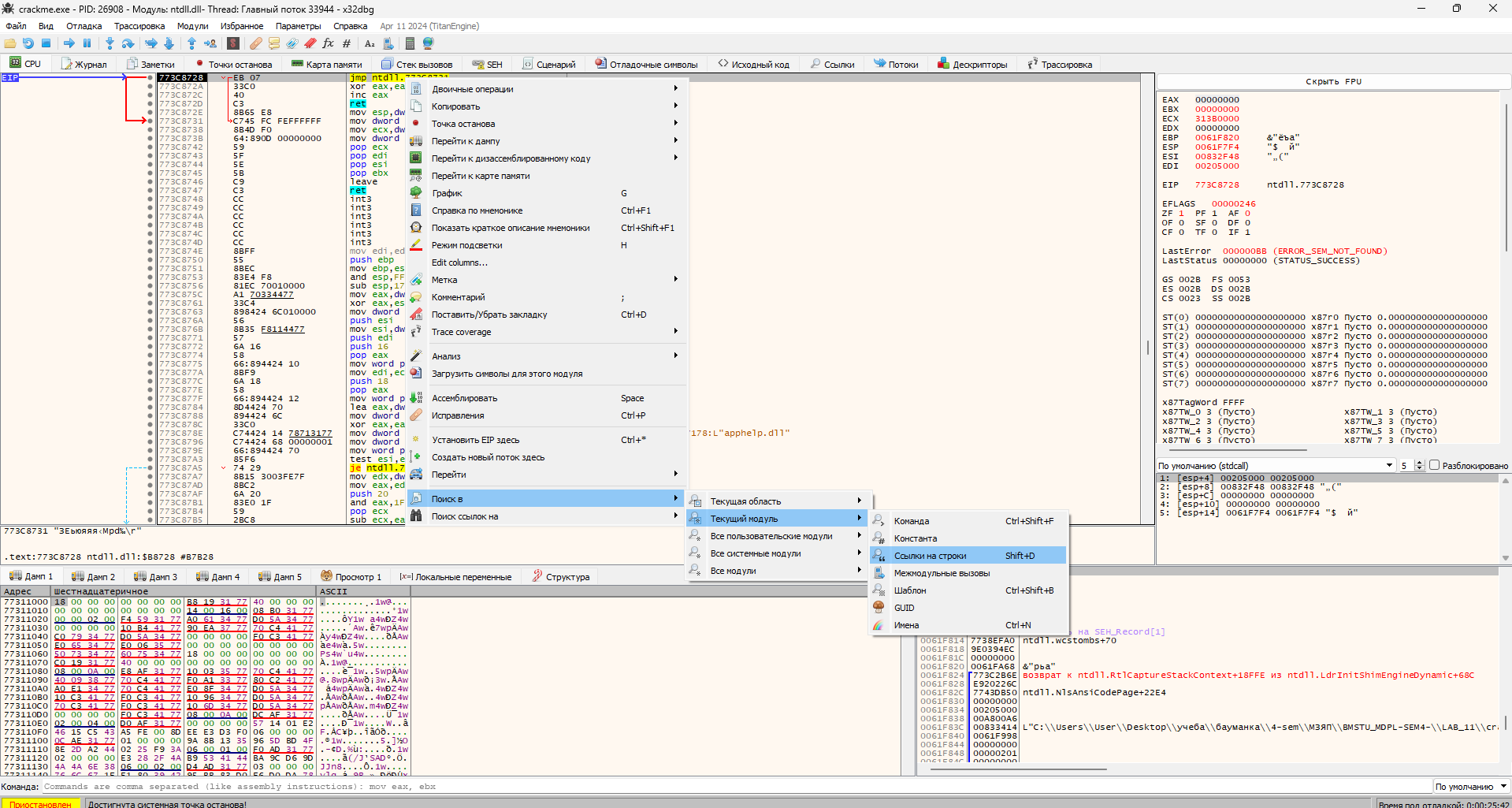
Сначала была протестирована сама программа, чтобы понять, какие сообщения можно получить на входе перед тем как ввести пароль.

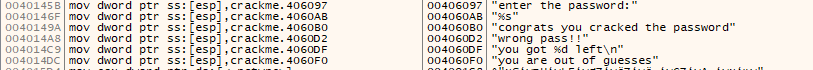


Как видно, перед вводом пароля выводится сообщение “enter the password:”. Его и попробуем найти с помощью отладчика.

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

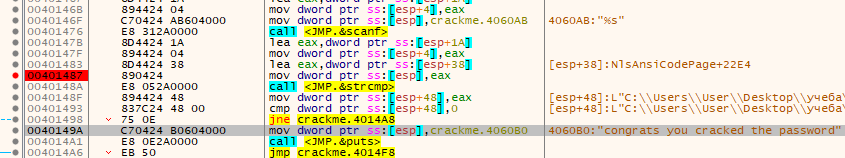
* Нажимаем на стрелочку “Выполнить”
* Правый клик по команде
* Поиск в
* Текущий модуль
* Ссылки на строки



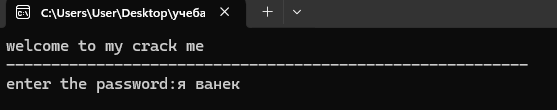


Повезло, в том смысле, что мы смогли найти не только строку “enter the password:”, но и строку “congrats you cracked the password”, которая скорее всего выводится, когда ввели правильный пароль.

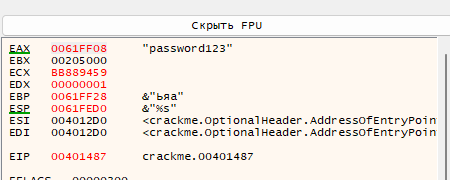
* Правый клик по строке
* Перейти к дизассемблерному коду



В этом блоке кода можно увидеть команду scanf, которая скорее всего считывает слово (введенный пользователем пароль) и после команду strcmp, которая скорее всего сравнивает введенный пароль и пароль, который считается программой правильным. Поставим точку останова прямо перед командой сравнения и в самой программе попробуем ввести случайный пароль.



В окошке FPU в EAX появился предположительно правильный пароль.



Перезапускаем программу, вводим этот пароль и он оказывается правильным.