Лабораторная работа №7

«Исследование безопасности программного обеспечения информационных систем в среде отладчика OllyDbg»

7.1 Цель работы:

Углубление знаний архитектуры 32-разрядных процессоров и системы команд языка ассемблера. Исследование методов защиты программного обеспечения информационных систем и ее нейтрализации, приобретение практических навыков исследования и отладки программ с помощью пакета OllyDbg.

7.2 Постановка задачи

Вариант – 8

Повторить теоретический материал, касающийся архитектуры 32-разрядных микропроцессоров, программно доступных регистров и системы команд языка ассемблера.

Исследовать способы парольной защиты в программе CRACKME1.EXE. Для этого выполнить последовательность действий, описных в разделе 4 настоящих методических указаний. Изменить программу таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.

С помощью отладчика OllyDbg исследовать способы парольной защиты программ CRACKME2.EXE, CRACKME3.EXE и CRACKME4.EXE, которые расположены в папке лабораторных работ. Определить на каких языках написаны программы. Изменить программы таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.

С помощью отладчика OllyDbg исследовать способ защиты программы CRACKME5.EXE. Определите на каком языке написана программа. В данной программе ключ генерируется по введенному в первом поле имени.

Разработать рекомендации по усилению защиты вскрытия пароля.

7.3 Ход работы

Были исследованы способы парольной защиты в программе CRACKME1.EXE.

Программа отладчика была запущена. Для исследований была выбрана первая предложенная программа – CRACKME1.exe. После загрузки программы в отладчике сразу была установлена точка остановки на строке, осуществляющей проверку введённой пользователем строки с строкой-паролем. Исследуемая программа была запущена на выполнение. В поле была введена случайная последовательность символов «123», затем нажата кнопка подтверждения ввода. Отладчик остановил выполнение исследуемой программы в установленной точке и показал, с какой именной строкой происходит сравнение (рисунок 1).


Рисунок 1 – Предположительное значение пароля в первой программе

Строка была введена. По нажатию кнопки программа показала сообщение о том, что был введён верный пароль.

Те же исследования были проведены со второй программой. Введена последовательность символов «123». Было выведено сообщение, согласно которому был введён неверный пароль (рисунок 2).

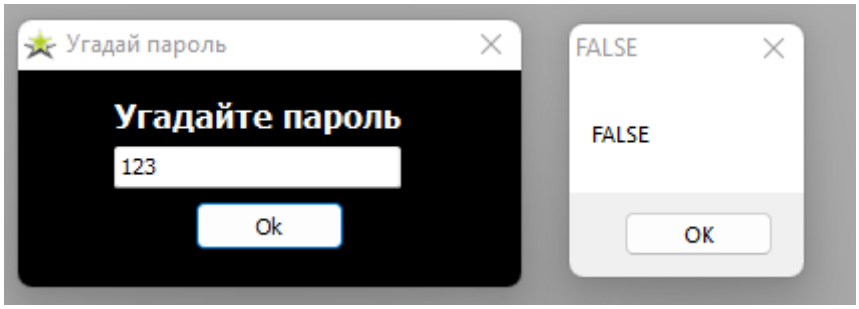


Рисунок 2 – Ввод неверного пароля в приложении №2

Затем были повторены действия из предыдущего исследования, и был получен пароль «Pass123» (рисунки 3 и 4).


Рисунок 3 – Нахождение верного пароля в приложении №2

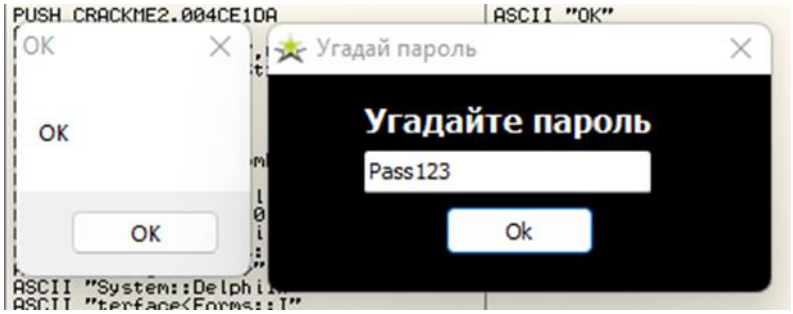


Рисунок 4 – Ввод верного пароля в программе №2

Во время исследования третьей программы все описанные выше действия были повторены. В результате получен пароль «Dh789rTyU78» (рисунки 5 и 6).

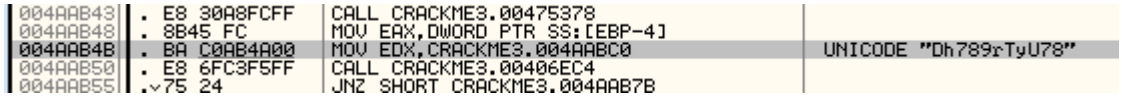


Рисунок 5 – Нахождение верного пароля в программе №3

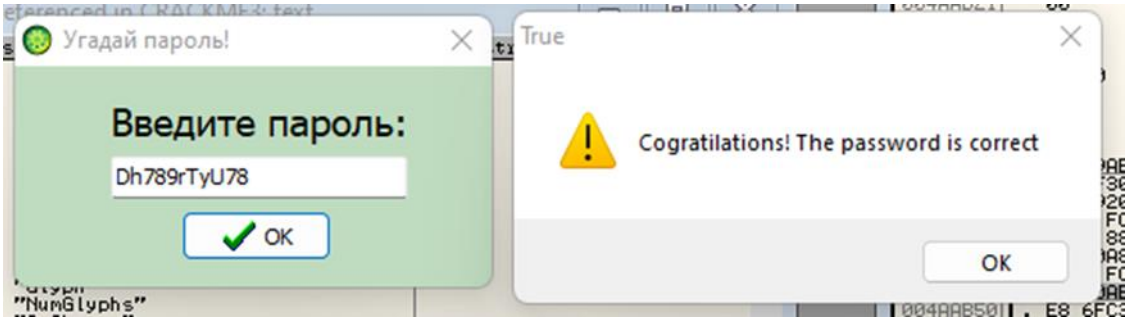


Рисунок 6 – Ввод верного пароля в программе №3

Во время исследования четвёртой программы все описанные выше действия были повторены. В результате получен пароль «m0tNaF-EmKCARc» (рисунки 7 и 8). Стоит отметить, что в этот раз подсказкой в поиске пароля послужило использование стандартной библиотечной функции «lstrcmpA», которая сравнивает две строки.


Рисунок 7 – Нахождение верного пароля в программе №4

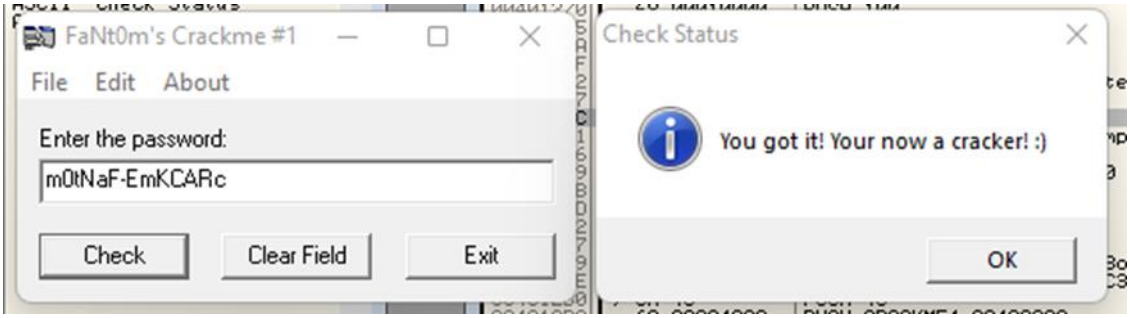


Рисунок 8 – Ввод найденной строки в программе №4

При отлаживании программы №5 выявлено, что для указанного в поле Name значения в соответствии с некоторым правилом вычисляется некоторое единственно верное значение пароля, в данном случае строки в поле Serial. Определено, что для Name=123 значением пароля будет являться «XYD» (рисунок 9). Таким образом было определено, что для Name=123 верным будет Serial=XYD (рисунок 10).

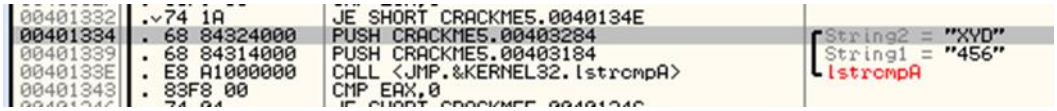


Рисунок 9 – Нахождение верного серийного номера для указанного имени в программе №5

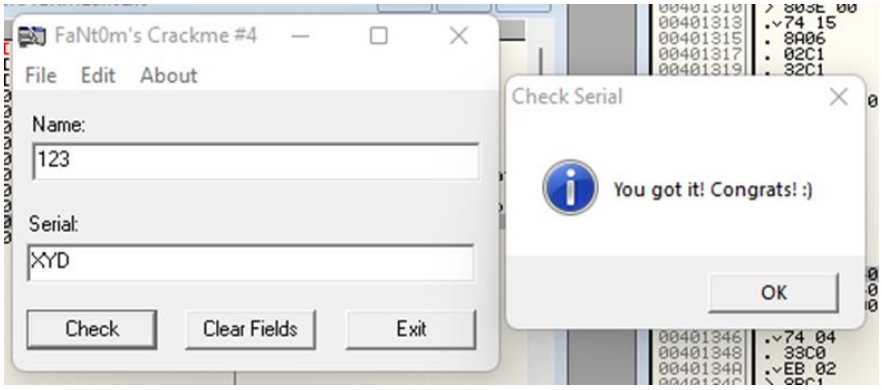


Рисунок 10 – Ввод определённых имени и с/н в программе №5

Были разработаны рекомендации по усилению защиты вскрытия пароля:

– Использовать сложные пароли: Пароль должен состоять из нескольких типов символов, таких как буквы, цифры и специальные символы.
– Шифрование паролей: Использование шифрования для хранения паролей может значительно усложнить попытки их взлома.

- Ограничение количества неудачных попыток входа: Можно установить ограничение на количество неудачных попыток входа, что поможет предотвратить попытки перебора пароля.
- Обновление ПО: Установка последних обновлений для ПО может помочь исправить уязвимости безопасности.
- Использовать хеширование паролей при хранении.
- Не хранить пароли в открытом виде.
- Ограничить доступ к системе только авторизованным пользователям.

## Выводы

В ходе выполнения данной лабораторной работы были получены навыки отлаживания программ с использованием отладчика OllyDB, защиты программного обеспечения от взлома. Также получены навыки работы с программами, написанными для 32-битной архитектуры.