МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

кафедра «Информационные системы»

Отчёт

по лабораторной работе №7

по дисциплине «Технические средства информационных систем»

Выполнил:

ст.гр. ИС/б-20-2-о

Филозоп А.Н.

Принял:

Минкин С.И.

Севастополь

2022 г.

7 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

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.

7.3. Ход выполнения работы

Программа отладчика была запущена. Для исследований была выбрана первая предложенная программа — CRACKME1.exe. После загрузки программы в отладчике сразу была установлена точка остановы на строке, осуществляющей проверку введённой пользователем строки с строкой-паролем. Исследуемая програм-

ма 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).

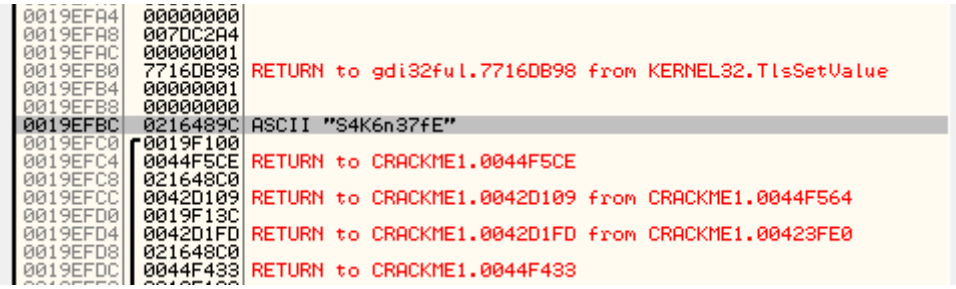

Рисунок 1 — Предположительное значение пароля в первой программе

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).

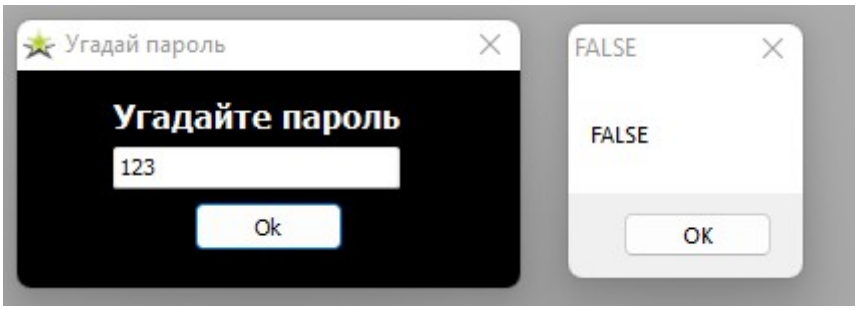

Рисунок 2 — Ввод неверного пароля в приложении №2

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

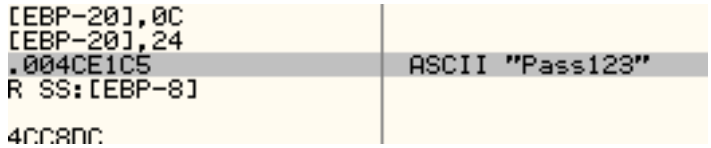

Рисунок 3 — Нахождение верного пароля в приложении №2

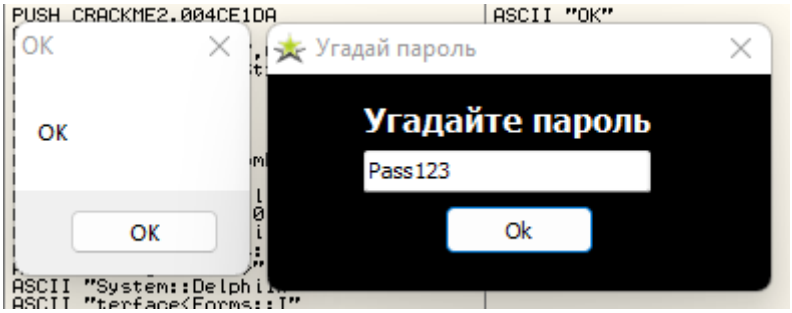

Рисунок 4 — Ввод верного пароля в программе №2

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

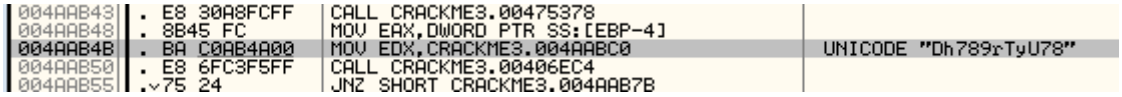

Рисунок 5 — Нахождение верного пароля в программе №3

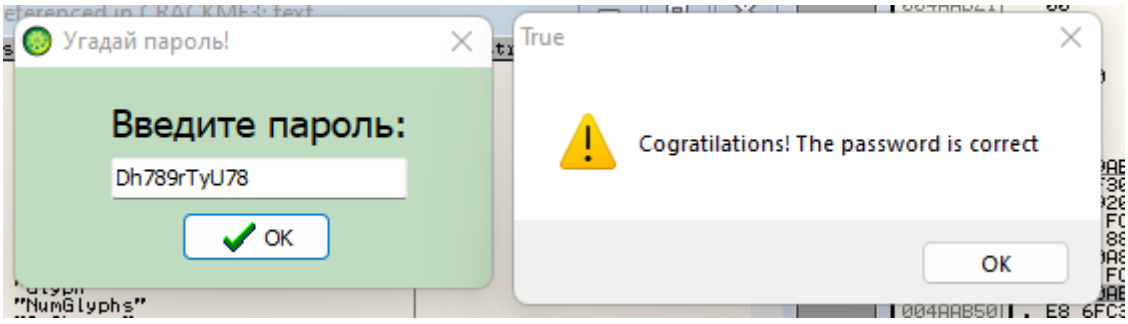

Рисунок 6 — Ввод верного пароля в программе №3

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.

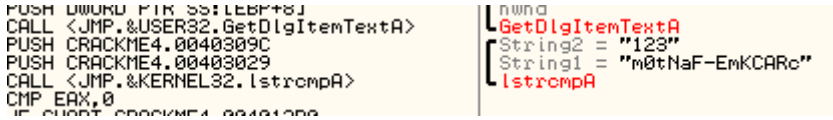

Рисунок 7 — Нахождение верного пароля в программе №4

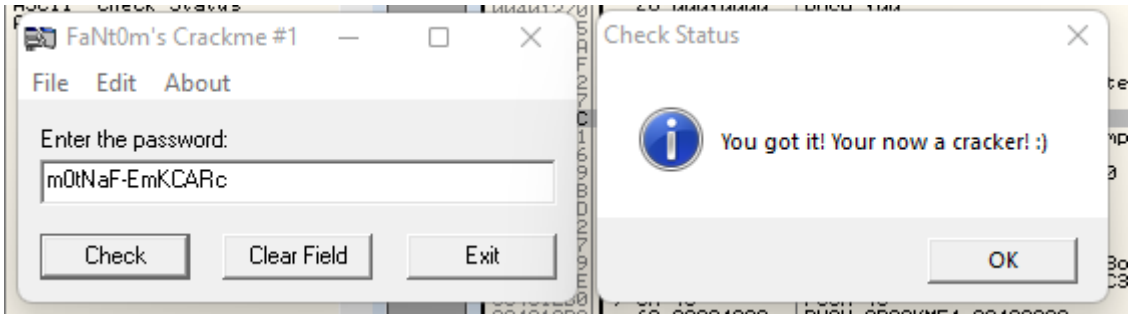

Рисунок 8 — Ввод найденной строки в программе №4

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).

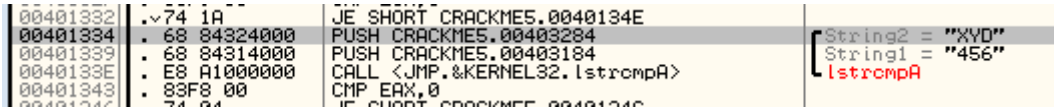

Рисунок 9 — Нахождение верного серийного номера для указанного имени в программе №5

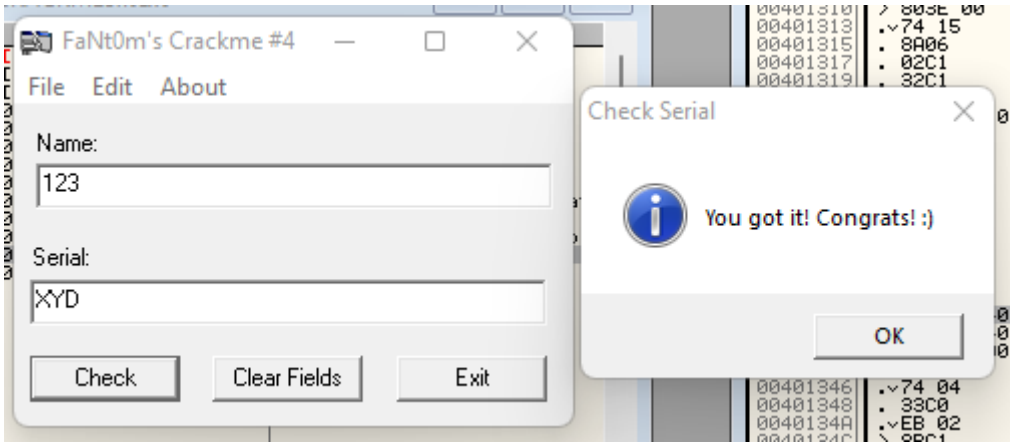

Рисунок 10 — Ввод определённых имени и с/н в программе №5

Вывод

При выполнении 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.

Приложение А

Ответы на контрольные вопросы

1. Суперскалярным называется центральный процессор (ЦП), который одновременно выполняет более чем одну скалярную команду. Это достигается за счет включения в состав ЦП нескольких самостоятельных исполнительных блоков, каждый из которых отвечает за свой класс операций и может присутствовать в процессоре в нескольких экземплярах. Так, в микропроцессоре Pentium III блоки целочисленной арифметики и операций с плавающей точкой дублированы, а в микропроцессорах Pentium 4 и Athlon — троированы. Процессор включает в себя шесть блоков: выборки команд, декодирования команд, диспетчеризации команд, распределения команд по функциональным блокам, блок исполнения и блок обновления состояния.

2. Для уменьшения потерь процессорных циклов, связанных с промахами при обращении к кэш-памяти в случае выполнения команд ветвления, в состав системы кэширования введены средства предсказания переходов, основное назначение которых - повысить вероятность наличия в кэш-памяти требуемой команды. Исполнение условных ветвлений состоит из следующих этапов: распознание команды условного ветвления; проверка выполнения условия перехода; вычисление адреса перехода; передача управления, в случае перехода.

3. Необходимость в преобразовании CISC команд в RISC появиллась ввиду того, что начиная с Pentium III ядро процессора состоит из двух частей: декодера и RISC-ядра. Соответственно задачей декодера является преобразование комплексных операций в микрооперации сокращенного набора команд.

4. …

5. …

6. …

7. Трассировка программы — процесс пошагового выполнения программы.

8. Содержимое регистров общего назначения тестируется с помощью команд CMP и TEST.

9. При выполнении команды PUSH содержимое регистра заносится в стек. При выполнении команды POP процессор записывает в указанный регистр считанное из стека машинное слово.

10. Для защиты программы от вскрытия паролей необходимо: следует как можно меньше применять стандартные функции; применять нестандартный способ ввода пароля; не следует анализировать введенный пароль сразу после его ввода.

11. …

12. Процедуру сравнения пароля можно локализовать по признаку сравнения двух строк — введённой пользователем и паролем.