МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федерально автономное бюджетное образовательное учреждение высшего образования

«Севастопольский государственный университет»

кафедра Информационных систем

Куркчи Ариф Эрнестович

Институт информационных технологий и управления в технических системах

курс 3 группа ИС/б-31-о

09.03.02 Информационные системы и технологии (уровень бакалавриата)

ОТЧЕТ

по лабораторной работе №5

по дисциплине «Информационные средства ИС»

на тему «Исследование безопасности программного обеспечения в среде отладчика OllyDbg»

Отметка о зачете \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

(дата)

Руководитель практикума

доцент   В. Ю. Карлусов

(должность) (подпись) (инициалы, фамилия)

Севастополь 2016

1.Цель работы

Исследование степени защиты программного обеспечение с помощью отладчика OllyDbg.

2.Порядок выполнения работы

1. Необходимо запустить утилиту PEiD и открыть файл CRACKME1.EXE. В появившимся окне видно, что программа создана с помощью Borland C++ 1999. Следовательно, исследуемая программа написана на языке программирования C++. В OllyDbg изменим программу таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.



Рисунок 1 – Измененная первая программа

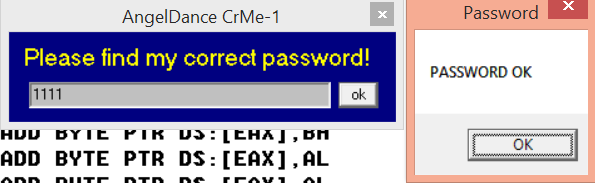


Рисунок 2 – Программа принимает любой пароль

1. Необходимо запустить утилиту PEiD и открыть файл CRACKME2.EXE. В появившимся окне видно, что программа создана с помощью Borland C++ 1999. Следовательно, исследуемая программа написана на языке программирования C++. В OllyDbg найдем верный пароль программы и изменим ее таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.



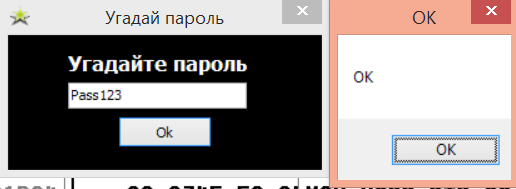


Рисунок 3 – Найден правильный пароль

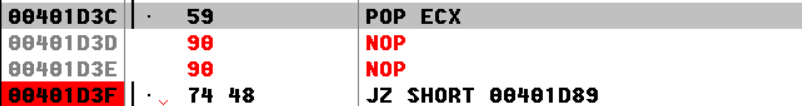


Рисунок 4 – Программа принимает любой пароль

1. Необходимо запустить утилиту PEiD и открыть файл CRACKME3.EXE. В появившимся окне видно, что программа создана с помощью Borland Delphi 3.0. Следовательно, исследуемая программа написана на языке программирования Delphi. В OllyDbg найдем верный пароль программы и изменим ее таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.

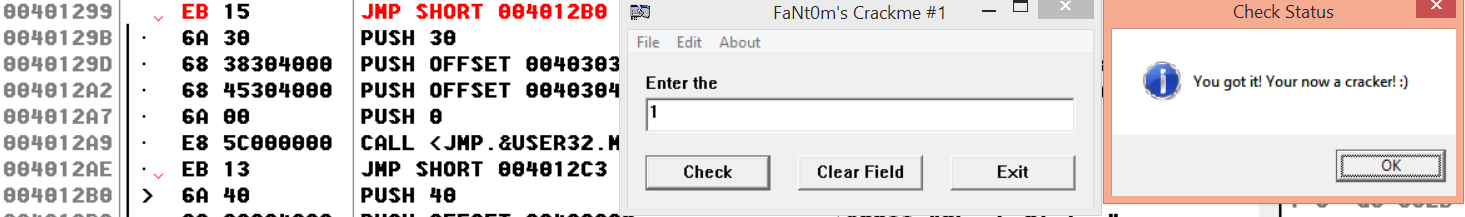


Рисунок 5 – Найден правильный пароль

http://pastexen.com/i/bUaof8InK9.png

Рисунок 6 – Программа принимает любой пароль

1. Необходимо запустить утилиту PEiD и открыть файл CRACKME4.EXE. В появившимся окне видно, что программа создана с помощью MASM32 / TASM32. Следовательно, исследуемая программа написана на языке программирования ассемблер. В OllyDbg найдем верный пароль программы и изменим ее таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.

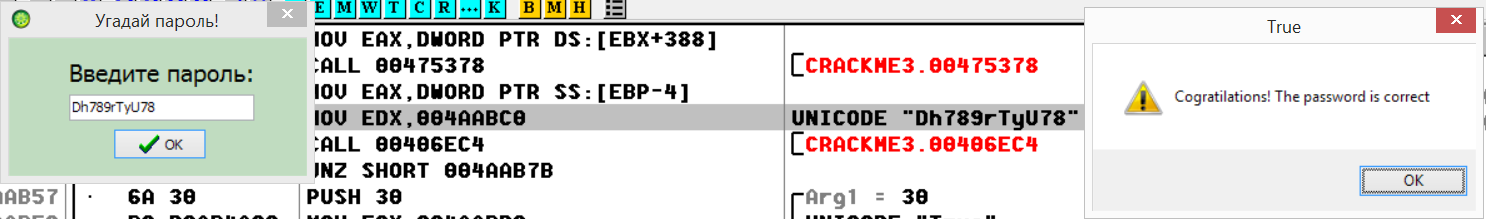


Рисунок 7 – Найден правильный пароль

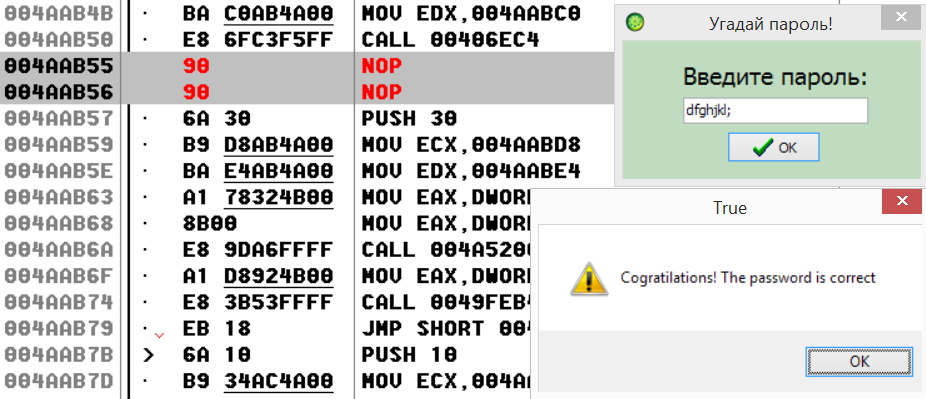


Рисунок 8 – Программа принимает любой пароль

1. Необходимо запустить утилиту PEiD и открыть файл CRACKME5.EXE. В появившимся окне видно, что программа создана с помощью MASM32 / TASM32. Следовательно, исследуемая программа написана на языке программирования ассемблер. В OllyDbg найдем верный пароль программы. Особенность заключается в том, что в данной программе ключ генерируется по введенному в первом поле имени. По формуле

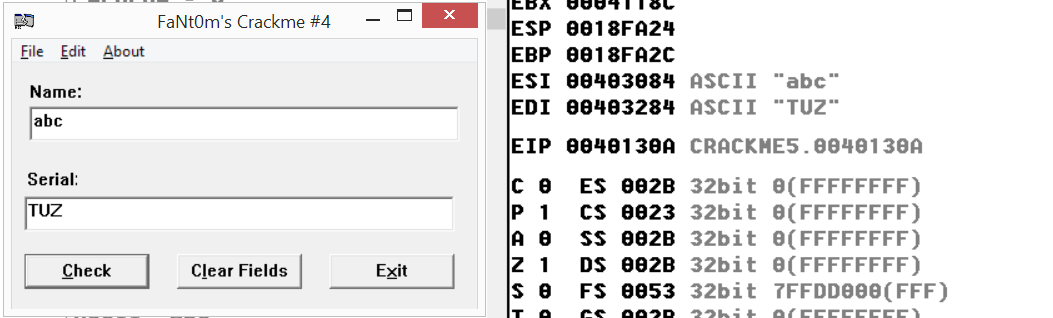


Рисунок 9 – Найден правильный пароль

Вывод

В ходе данной лабораторной работы были исследованы степени защиты программного обеспечения с помощью отладчика OllyDbg. В каждой исследованной программе степень защиты находится на низком уровне.