

Технический Университет Молдовы
Факультет Вычислительной Техники, Информатики и Микроэлектроники

Tehnici de inginerie inversa

Отчёт

По лабораторной работе №3

Проверил:
Выполнил:
Группа:

Catanoi M.
Абабий Э.
SI-202

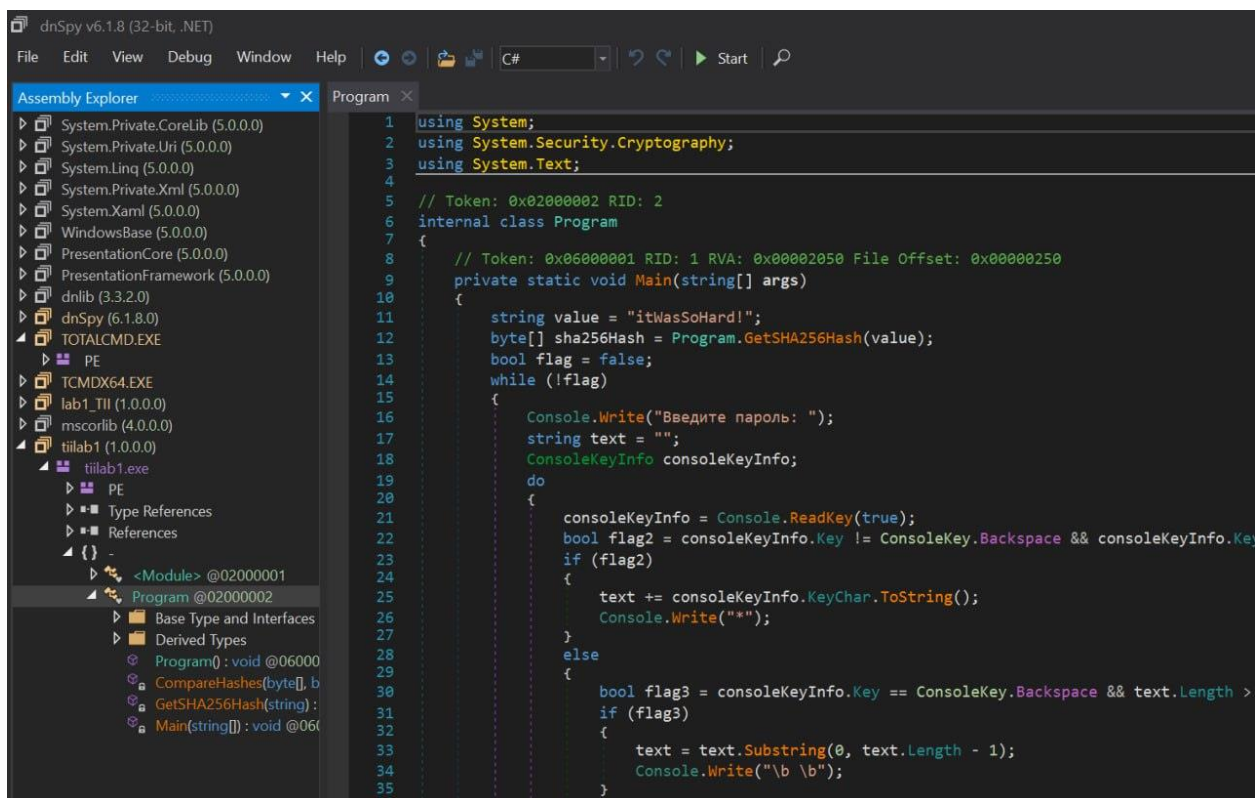
Кишинёв 2023

Задание: Нужно взломать программу таким образом, чтобы, не изменяя основной код и не вводя правильный пароль, программа на любой ввод должна вас пропускать

Шаг 1 Открываю уже нам знакомую программу dnSpy



Шаг 2 Загружаем файл в программу



Шаг 3 ищем возможность изменения кода так, чтобы он пропустил любое наше значение

```
Edit Class - Program @02000002
66
67 // Token: 0x06000003 RID: 3 RVA: 0x00021D0 File Offset: 0x00003D0
68 private static bool CompareHashes(byte[] hash1, byte[] hash2)
69 {
70     bool flag = hash1.Length != hash2.Length;
71     bool result;
72     if (flag)
73     {
74         result = false;
75     }
76     else
77     {
78         for (int i = 0; i < hash1.Length; i++)
79         {
80             bool flag2 = hash1[i] != hash2[i];
81             if (flag2)
82             {
83                 return false;
84             }
85             result = true;
86         }
87         return result;
88     }
89 }
90
91 // Token: 0x06000004 RID: 4 RVA: 0x0002221 File Offset: 0x0000421
92 public Program()
93 {
94 }
95 }
96
```

Такое место было найдено, когда hash1 не равняется hash2, возвращается false, что означает – программа не пропускает далее. Поменяем false на true и тогда чтобы мы не ввели flag2 всегда будет true

```
Edit Class - Program @02000002
66
67 // Token: 0x06000003 RID: 3 RVA: 0x00021D0 File Offset: 0x00003D0
68 private static bool CompareHashes(byte[] hash1, byte[] hash2)
69 {
70     bool flag = hash1.Length != hash2.Length;
71     bool result;
72     if (flag)
73     {
74         result = false;
75     }
76     else
77     {
78         for (int i = 0; i < hash1.Length; i++)
79         {
80             bool flag2 = hash1[i] != hash2[i];
81             if (flag2)
82             {
83                 return true;
84             }
85         }
86         result = true;
87     }
88     return result;
89 }
90
91 // Token: 0x06000004 RID: 4 RVA: 0x0002221 File Offset: 0x0000421
92 public Program()
93 {
94 }
95 }
96
```

Как и ожидалось, программа принимает любые значения. Скриношта нет, так как консоль мгновенно закрывается.

Программа принимает любые значения.

Вывод: в результате лабораторной я научился внимательно анализировать код программы, чтобы найти лазейку. Изменять исходный код программы таким образом открываю недоступное.