

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский университет ИТМО»**

Факультет безопасности информационных технологий

Дисциплина:

«Технологии и Методы программирования»

ОТЧЕТ

по

Лабораторной работе №3

Выполнил:

Студент гр. N33472

Шарифов Ф.Р.

Проверил:

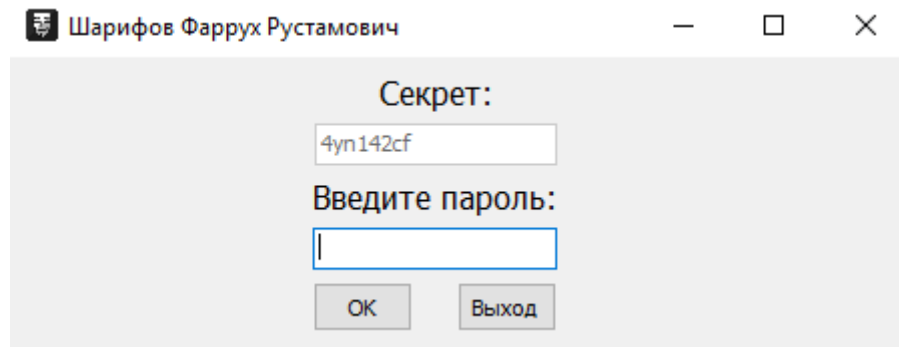
Ищенко А. П.

Санкт-Петербург

2020г

Задание

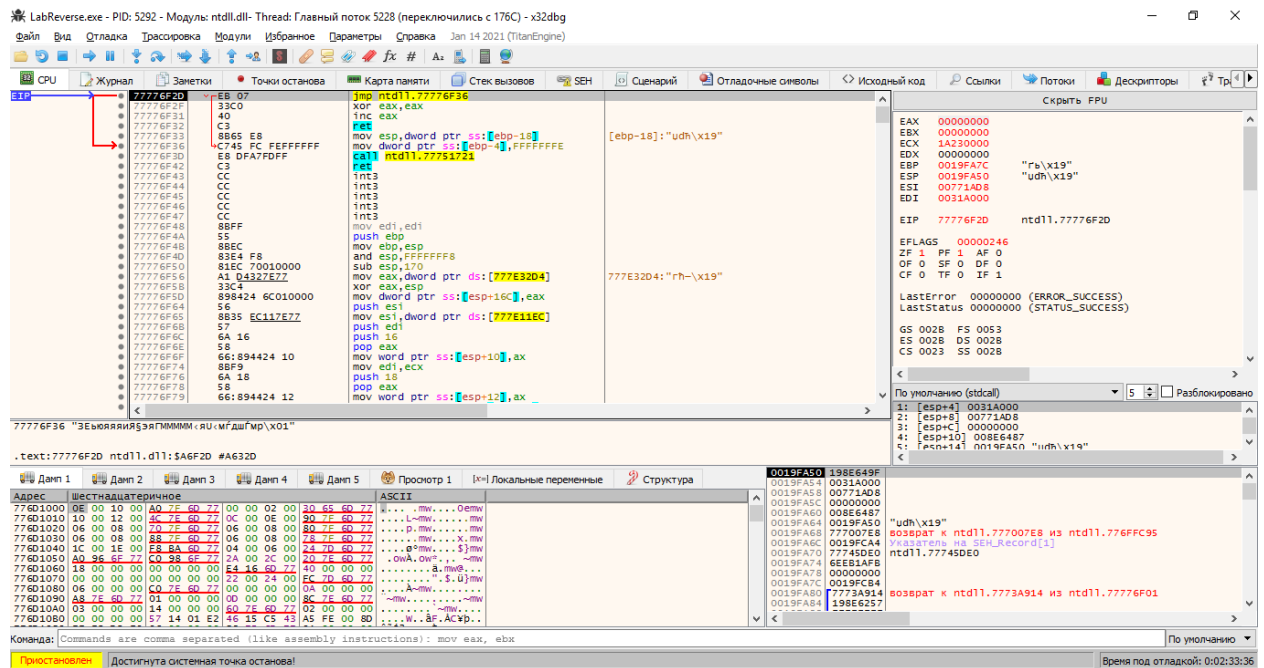
Найти верный пароль от программы LabReverse.



Ход работы

Для нахождения верного пароля используем программу “x32dbg”.

Запускаем нашу программу с помощью “x32dbg”.



Шарифов Фаррух Рустамович

Секрет:

4yn142cf

Введите пароль:

qwertyui

OK Выход

Labreverse

Неверный пароль!

OK

LabReverse.exe - PID: 7148 - Модуль: labreverse.exe - Thread: главный поток 5380 - x32dbg

Файл Вид Отладка Трасировка Модули Избранное Параметры Справка Jan 14 2021 (TitanEngine)

CPU Журнал Заметки Точки останова Карта памяти стек вызовов SEH Сценарий Отладочные символы Исходный код Ссылки Потоки Дескрипторы Tr

Адрес	Дисассемблированный код	Комментарии
0040403E	66C8 3BFFFFFF 300	mov word ptr [ebp-C8], 300
0040403F	FF85 14FFFFFF	inc dword ptr [ebp-E4]
00404040	83BD 14FFFFFF 09	cmp dword ptr [ebp-E4], 9
00404041	0FBC D0FFFFFF	jbe labreverse.658500
00404042	68 3C965600	push labreverse.658500
00404043	68 20D26500	push labreverse.650220
00404044	E8 737A2500	call labreverse.658500
00404045	83C4 08	add esp, 8
00404046	84C0	test al, al
00404047	F4 72	js labreverse.4040C6
00404048	66C785 3BFFFFFF 5C0	mov word ptr [ebp-C8], 15C
00404049	80BD SCFFFFFF	lea ecx, dword ptr [ebp-A4]
0040404A	59	push ecx
0040404B	E8 38020000	call labreverse.4042A4
0040404C	59	pop ecx
0040404D	8BDD	mov ebx, eax
0040404E	FF85 14FFFFFF	inc dword ptr [ebp-E4]
0040404F	8B85 24FFFFFF	mov esi, dword ptr [ebp-DC]
00404050	BB80 C4030000	mov esi, dword ptr [esi+eax*3CA]
00404051	E8 AD451200	call labreverse.652688
00404052	EBX SCFFFFFF	mov ebx, dword ptr [ebp-A4]
00404053	8B12	mov edx, dword ptr [edx]
00404054	A1 548E6600	mov ecx, dword ptr [esi+Form2]
00404055	8B08	mov ecx, dword ptr [esi]
00404056	BB81 C4030000	mov esi, dword ptr [esi+ecx*3CA]
00404057	E8 75451200	call labreverse.652688
00404058	FF80 14FFFFFF	dec dword ptr [ebp-BE]
00404059	6A 02	push r
0040405A	8095 SCFFFFFF	lea ecx, dword ptr [ebp-A4]
0040405B	52	push ecx
0040405C	E8 4F7A2500	call labreverse.658500
0040405D	83C4 08	add esp, 8
0040405E	8BDD 548E6600	mov ecx, dword ptr [esi+Form2]
0040405F	8B08	mov ecx, dword ptr [edx]
00404060	E8 7F692200	call labreverse.62AA40
00404061	E9 71010000	jmp labreverse.404237
00404062	66C785 3BFFFFFF 680	mov word ptr [ebp-C8], 168
00404063	68 03D53500	push labreverse.650303
00404064	8095 3BFFFFFF	lea ecx, dword ptr [ebp-A8]
00404065	52	push ecx
00404066	E8 7A732500	call labreverse.658A54
00404067	83C4 08	add esp, 8

0068E54: "P-f"

0068E54: "P-f"

65D303: "Неверный пароль!"

Скрыты FPU

```

EAX 398C4093
EBX 00023200 <labreverse.EntryPoint>
ECX 004020FA <labreverse.EntryPoint>
EDX 004020FA &"\x19"
ESP 0019FF94 &"\x19"
ESI 0019FF84 &"\x19"
EDI 004020FA <labreverse.EntryPoint>
ETP 004020FA <labreverse.EntryPoint>

EFLAGS 00000244
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

LastErrorf 00000008 (ERROR_ENVVAR_NOT_FOUND)
LastStatus 00000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B FS 002B
ES 002B DS 002B
CS 0023 SS 002B

ST(0) 00000000000000000000000000000000 x87r0 Пусто 0.00000000000000000000000000000000
ST(1) 00000000000000000000000000000000 x87r1 Пусто 0.00000000000000000000000000000000
ST(2) 00000000000000000000000000000000 x87r2 Пусто 0.00000000000000000000000000000000
ST(3) 00000000000000000000000000000000 x87r3 Пусто 0.00000000000000000000000000000000
ST(4) 00000000000000000000000000000000 x87r4 Пусто 0.00000000000000000000000000000000
ST(5) 00000000000000000000000000000000 x87r5 Пусто 0.00000000000000000000000000000000

```


По умолчанию (stdcl) 5 Разблокировано

0019FFBC 775862C4 воззрат к kernel32.775862C4 из ???
0019FFBC 775862A0 kernel32.775862A0
0019FF94 0019FFDC "\x19"
0019FF98 77730609 воззрат к ntdll.77730609 из ???

Команда: Commands are comma separated (like assembly instructions): mov ecx, ebx

Запушен Дата: 024E7AB4 -> 024E7AB4 (0x00000001 bytes)

Время от отладки: 0:02:51



Form2

Поздравляем, вы выбрали пароль!

be1alm10

Сообщите его преподавателю
и сдайте работу.

Вывод

В ходе лабораторной работы, была проведена работа с отладчиком, и найден правильный пароль от программы. Задание успешно выполнено.