



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

Лабораторная работа № 9

Дисциплина: Машинно-зависимые языки программирования

Тема: Дизассемблирование

Студент: Платонова О. С.

Группа: ИУ7-45Б

Оценка (баллы) _____

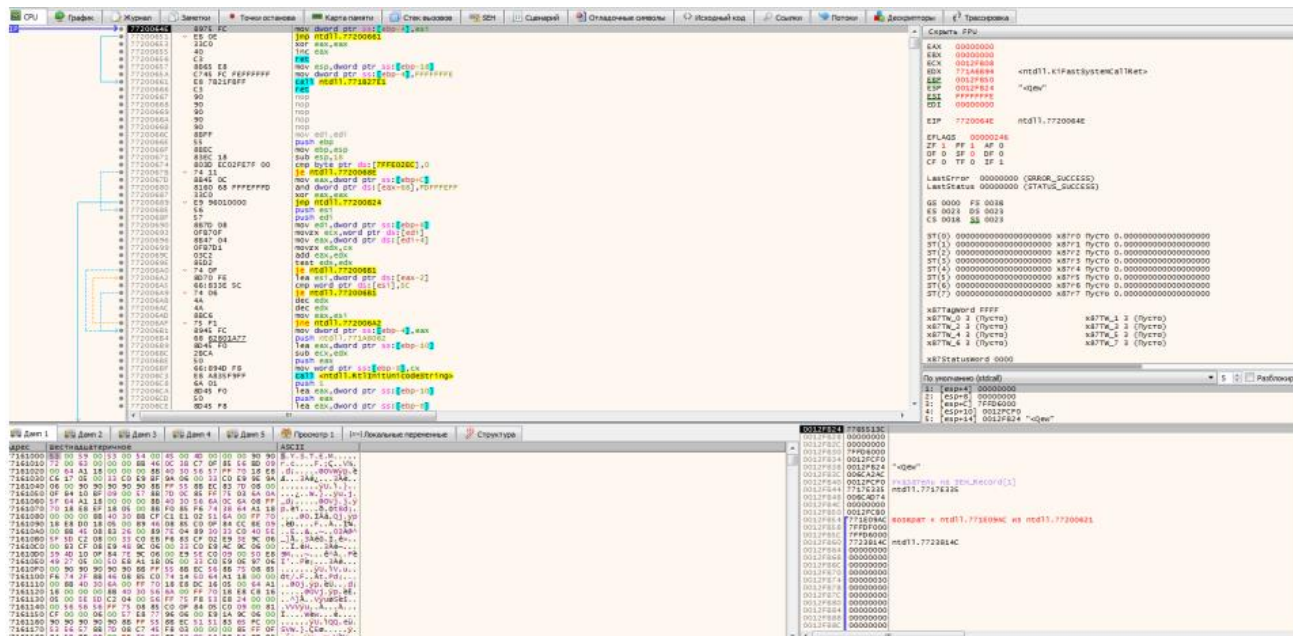
Преподаватель: Кузнецов Д. А.

Москва.
2020 г.

Выполним дизассемблирование файла BankCode.exe.

При запуске этого файла от пользователя требуется ввод кодового слова для восстановления пароля.

Откроем .exe файл в нашем отладчике. Вот так выглядит его интерфейс.



На данный момент мы оказались в точке входа.

EIP	7720064E	8975 FC	mov dword ptr ss:[ebp-4],esi
	77200651	EB 0E	jmp ntdll.77200661
	77200653	33C0	xor eax,eax
	77200655	40	inc eax
	77200656	C3	ret
	77200657	8B65 E8	mov esp,dword ptr ss:[ebp-18]
	7720065A	C745 FC FFFFFFFF	mov dword ptr ss:[ebp-4],FFFFFFF
	77200661	E8 7B21FBFF	call ntdll.771B27E1
	77200666	C3	ret

Выполним трассировку «Анимация с обходом» и перейдем к дизассемблированному коду выделенной строки, – исследуемой процедуры.

0040128D	E8 96610000	call <JMP.&_GetMainArgs>
00401292	B9 58804000	mov ecx,bankcode.408058
00401297	8B11	mov edx,dword ptr ds:[ecx]
00401299	09D2	or edx,edx
0040129B	74 02	je bankcode.40129F
0040129D	FFD1	call ecx
0040129F	FF35 30A04000	push dword ptr ds:[40A030]
004012A5	FF35 2CA04000	push dword ptr ds:[40A02C]
004012AB	FF35 28A04000	push dword ptr ds:[40A028]
004012B1	8925 14A04000	mov dword ptr ds:[40A014],esp
004012B7	E8 18000000	call bankcode.4012D4
004012BC	83C4 18	add esp,18
004012BF	31C9	xor ecx,ecx
004012C1	894D FC	mov dword ptr ss:[ebp-4],ecx
004012C4	50	push eax
004012C5	E8 82610000	call <JMP.&exit>
004012CA	C9	leave
004012CB	C3	ret
004012CC	64:A3 00000000	mov dword ptr [0],eax
004012D2	C3	ret

Отметим, что перед вызовом процедуры в стеке размещается три указателя.

0040129F	FF35 30A04000	push dword ptr ds:[40A030]
004012A5	FF35 2CA04000	push dword ptr ds:[40A02C]
004012AB	FF35 28A04000	push dword ptr ds:[40A028]
004012B1	8925 14A04000	mov dword ptr ds:[40A014],esp
004012B7	E8 18000000	call bankcode.4012D4

Перейдя к дампу, легко увидеть, что это сообщения, предназначенные для пользователя.

0040A0A0	4B 65 79 20	77 6F 72 64	20 69 73 20	69 6E 63 6F	Key word is inco
0040A0B0	72 72 65 63	74 0A 00 57	65 20 73 65	6E 74 20 6E	rrect..We sent n
0040A0C0	65 77 20 70	61 73 73 77	6F 72 64 20	6F 6E 20 6D	ew password on m
0040A0D0	61 69 6C 0A	00 09 49 6E	70 75 74 20	79 6F 75 72	ail...Input your
0040A0E0	20 63 6F 64	65 20 77 6F	72 64 0A 00	54 6F 20 72	code word..To r
0040A0F0	65 73 74 6F	72 65 20 70	61 73 73 77	6F 72 64 0A	estore password.

Это означает, что исследуемая функция ответственна за вызов функций ввода-вывода.

Рассмотрим процедуру.

Вот так, начиная с выделенной строки, выглядит наша процедура.

004012D4	55	push ebp
004012D5	89E5	mov ebp,esp
004012D7	83EC 34	sub esp,34
004012DA	B9 0D000000	mov ecx,D
004012DF	49	dec ecx
004012E0	C7048C 5A5AFAFF	mov dword ptr ss:[esp+ecx*4],FFFA5A5A
004012E7	75 F6	jne bankcode.4012DF
004012E9	57	push edi
004012EA	8D3D 1EA14000	lea edi,dword ptr ds:[40A11E]
004012F0	897D E8	mov dword ptr ss:[ebp-18],edi
004012F3	8D3D 19A14000	lea edi,dword ptr ds:[40A119]
004012F9	897D EC	mov dword ptr ss:[ebp-14],edi
004012FC	8D3D 14A14000	lea edi,dword ptr ds:[40A114]
00401302	897D F0	mov dword ptr ss:[ebp-10],edi
00401305	8D3D 0AA14000	lea edi,dword ptr ds:[40A10A]
00401308	897D F4	mov dword ptr ss:[ebp-C],edi
0040130E	8D3D 01A14000	lea edi,dword ptr ds:[40A101]
00401314	897D F8	mov dword ptr ss:[ebp-8],edi
00401317	68 ECA04000	push bankcode.40A0EC
0040131C	E8 FB5E0000	call bankcode.40721C
00401321	83C4 04	add esp,4
00401324	68 D5A04000	push bankcode.40A0D5
00401329	E8 EE5E0000	call bankcode.40721C
0040132E	83C4 04	add esp,4
00401331	8D7D CF	lea edi,dword ptr ss:[ebp-31]
00401334	57	push edi
00401335	E8 36610000	call <JMP.&gets>
0040133A	83C4 04	add esp,4
0040133D	C745 FC 00000000	mov dword ptr ss:[ebp-4],0
00401344	C745 FC 00000000	mov dword ptr ss:[ebp-4],0
0040134B	8B7D FC	mov edi,dword ptr ss:[ebp-4]
0040134E	FF74BD E8	push dword ptr ss:[ebp+edi*4-18]
00401352	8D7D CF	lea edi,dword ptr ss:[ebp-31]
00401355	57	push edi
00401356	E8 8D610000	call <JMP.&strcmp>
0040135B	83C4 08	add esp,8
0040135E	83F8 00	cmp eax,0
00401361	75 0F	jne bankcode.401372
00401363	68 B7A04000	push bankcode.40A0B7
00401368	E8 AF5E0000	call bankcode.40721C
0040136D	83C4 04	add esp,4
00401370	EB 09	jmp bankcode.401378
00401372	FF45 FC	inc dword ptr ss:[ebp-4]
00401375	837D FC 05	cmp dword ptr ss:[ebp-4],5
00401379	7C D0	j1 bankcode.40134B
0040137B	837D FC 05	cmp dword ptr ss:[ebp-4],5
0040137F	75 0D	jne bankcode.40138E
00401381	68 A0A04000	push bankcode.40A0A0
00401386	E8 915E0000	call bankcode.40721C
0040138B	83C4 04	add esp,4

Заметим, что внутри процедуры выполняется сравнение строк в цикле (счетчик [ebp-4] увеличивается на 1).

00401348	887D FC	mov edi,dword ptr ss:[ebp-4]
0040134E	FF74BD E8	push dword ptr ss:[ebp+edi*4-18]
00401352	8D7D CF	lea edi,dword ptr ss:[ebp-31]
00401355	57	push edi
00401356	E8 8D610000	call <JMP.&strcmp>
00401358	83C4 08	add esp,8
0040135E	83F8 00	cmp eax,0
00401361	75 0F	jne bankcode.401372
00401363	68 B7A04000	push bankcode.40A0B7
00401368	E8 AF5E0000	call bankcode.40721C
0040136D	83C4 04	add esp,4
00401370	EB 09	jmp bankcode.401378
00401372	FF45 FC	inc dword ptr ss:[ebp-4]
00401375	837D FC 05	cmp dword ptr ss:[ebp-4],5
00401379	7C D0	jl bankcode.401348

В случае равенства строк (eax = 0) происходит ввод/вывод сообщения на экран.

```
call <JMP.&strcmp>
add esp,8
cmp eax,0
jne bankcode.401372
push bankcode.40A0B7
call bankcode.40721C
```

Перейдя к дампу, увидим, что это сообщение о корректном вводе.

0040A0B7	57 65 20 73	65 6E 74 20	6E 65 77 20	70 61 73 73	We sent new pass
0040A0C7	77 6F 72 64	20 6F 6E 20	6D 61 69 6C	0A 00 09 49	word on mail...I

Значит, вся информация о доступе располагается в сегменте данных по адресу, начиная с [ebp - 8].

Действительно,

lea edi,dword ptr ds:[40A11E]	0040A11E: "Ivanov"
mov dword ptr ss:[ebp-18],edi	
lea edi,dword ptr ds:[40A119]	0040A119: "1405"
mov dword ptr ss:[ebp-14],edi	
lea edi,dword ptr ds:[40A114]	0040A114: "Mary"
mov dword ptr ss:[ebp-10],edi	
lea edi,dword ptr ds:[40A10A]	0040A10A: "Childhood"
mov dword ptr ss:[ebp-C],edi	
lea edi,dword ptr ds:[40A101]	0040A101: "Business"
mov dword ptr ss:[ebp-8],edi	

В случае окончания цикла и неравенства введенной строки ни одной строке из базы данных, происходит вывод сообщения на экран и завершение процедуры.

00401370	EB 09	jmp bankcode.401378
00401372	FF45 FC	inc dword ptr ss:[ebp-4]
00401375	837D FC 05	cmp dword ptr ss:[ebp-4],5
00401379	7C D0	jl bankcode.401348
0040137B	837D FC 05	cmp dword ptr ss:[ebp-4],5
0040137F	75 0D	jne bankcode.40138E
00401381	68 A0A04000	push bankcode.40A0A0
00401386	E8 915E0000	call bankcode.40721C
0040138B	83C4 04	add esp,4
0040138E	B8 00000000	mov eax,0

Также рассмотрим функции считывания строки из консоли и сравнения строк.

```
push edi
call <JMP.&gets>

push edi
call <JMP.&strcmp>
```

Функция сравнения строк

004074E8	FF25 7CB14000	jmp dword ptr ds:[<&strcmp>]	6C24E6C4 <crtdll strcmp>
004074EE	90	nop	push ebp
004074EF	90	nop	mov ebp,esp
004074F0	0000	add byte ptr ds:[eax],al	push edi
004074F2	0000	add byte ptr ds:[eax],al	push esi
			mov esi,dword ptr ss:[ebp+8]
			xor eax,eax
			mov edi,dword ptr ss:[ebp+C]
			or ecx,FFFFFFFF
			repne scasb
			not ecx
			sub edi,ecx
			repe cmpsb
			je crtdll.6C24E6E3
			sbb eax,eax
			sbb eax,FFFFFFFF
			pop esi
			pop edi
			leave
			ret

Функция использует команды обработки строк с префиксом повторения. И выполняет побитовое сравнение двух строк (ebp + 8; ebp + C) командой `repne scasb`. Предварительно вычисляется длина максимальной строки (командой `repne scasb`) и записывается в регистр `ecx`.

Функция считывания строки

00407470	FF25 54814000	jmp dword ptr ds:[<&gets>]	JMP.&gets
00407476	90	nop	6C24CA44 <crtdll gets>
00407477	90	nop	push esi
00407478	0000	add byte ptr ds:[eax],al	push edi
0040747A	0000	add byte ptr ds:[eax],al	mov edi,dword ptr ss:[esp+C]
			push 19
			mov esi,edi
			call crtdll.6C2515BE
			add esp,4
			dec dword ptr ds:[6C25E774]
			js crtdll.6C24CA6F
			mov ecx,dword ptr ds:[<_iob>]
			movzx eax,byte ptr ds:[ecx]
			inc dword ptr ds:[<_iob>]
			jmp crtdll.6C24CA7C
			push <crtdll._iob>
			call <crtdll._filbuf>
			add esp,4
			cmp eax,A
			je crtdll.6C24CA93
			cmp eax,FFFFFFFF
			je crtdll.6C24CA8B

Вывод

Мы научились проводить дизассемблирование exe файлов.