

Лабораторная работа №11

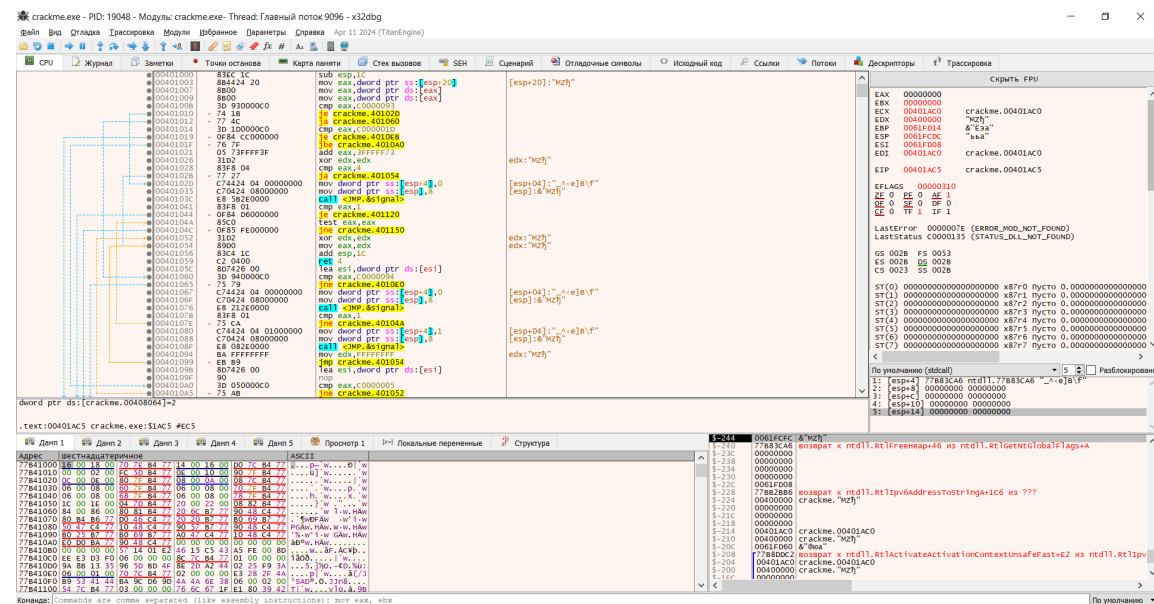
Практическое задание

С помощью x64dbg, IDA Freeware или других дизассемблеров/отладчиков определить пароль, необходимый для получения сообщения "congrats you cracked the password" в прикрепленной программе

(<https://crackmes.one/crackme/5fe8258333c5d4264e590114>).

Ход решения

Для начала загрузим программу в отладчик x32dbg



Листая дизассемблированный код программы, я обнаружил следующий интересный блок

0040142E	C74244 04 31323300	mov dword ptr ss:[esp+40],333231	[esp]:&"MZh", 406044:"welcome to my crack me"
00401436	C74244 44604000	mov dword ptr ss:[esp],crackme.406044	
0040143D	E8 722A0000	call <JMP.&puts>	
00401442	C74244 4C 01000000	mov dword ptr ss:[esp+4C],1	
0040144A	E9 9E000000	jmp crackme.4014E0	
0040144F	C74244 5C604000	mov dword ptr ss:[esp],crackme.40605C	[esp]:&"MZh", 40605C:"-----"
00401456	E8 592A0000	call <JMP.&puts>	
0040145B	C74244 97604000	mov dword ptr ss:[esp],crackme.406097	[esp]:&"MZh", 406097:"enter the password:"
00401462	E8 552A0000	call <JMP.&printf>	
00401467	804424 1A	lea eax,dword ptr ss:[esp+1A]	
0040146B	894424 04	mov dword ptr ss:[esp+4],eax	[esp+04]:&"^<e\b\f"
0040146F	C74244 AB604000	mov dword ptr ss:[esp],crackme.4060AB	[esp]:&"MZh", 4060AB:"&"s"
00401476	E8 312A0000	call <JMP.&scanf>	
0040147B	804424 1A	lea eax,dword ptr ss:[esp+1A]	
0040147F	894424 04	mov dword ptr ss:[esp+4],eax	
00401483	804424 38	lea eax,dword ptr ss:[esp+38]	[esp+04]:&"^<e\b\f"
00401487	890424 00	mov dword ptr ss:[esp],eax	[esp+38]:&"^&"oa"
0040148A	E8 052A0000	call <JMP.&strcmp>	[esp]:&"MZh"
0040148F	894424 48	lea eax,dword ptr ss:[esp+48],eax	
00401493	837C24 48 00	cmp dword ptr ss:[esp+48],0	
00401498	75 0E	jne crackme.4014A8	
0040149A	C74244 B0604000	mov dword ptr ss:[esp],crackme.4060B0	[esp]:&"MZh", 4060B0:"congrats you cracked the password"
004014A1	E8 0E2A0000	call <JMP.&puts>	
004014A6	EB 50	jmp crackme.4014F8	
004014AB	C74244 D2604000	mov dword ptr ss:[esp],crackme.4060D2	[esp]:&"MZh", 4060D2:"wrong pass!!"
004014B0	E8 002A0000	call <JMP.&puts>	
004014B4	B8 05000000	mov eax,5	
004014B8	284424 4C	sub eax,dword ptr ss:[esp+4C]	[esp+44]:&"MZh"
004014BD	894424 44	mov dword ptr ss:[esp+44],eax	[esp+44]:&"MZh"
004014C1	884424 44	mov eax,dword ptr ss:[esp+44]	
004014C5	894424 04	mov dword ptr ss:[esp+4],eax	[esp+04]:&"^<e\b\f"
004014C9	C74244 D6504000	mov dword ptr ss:[esp],crackme.4060D6	[esp]:&"MZh", 4060D6:"you got %d left\n"
004014D0	E8 72900000	call <JMP.&printf>	
004014D5	837C24 44 00	cmp dword ptr ss:[esp+44],0	[esp+44]:&"MZh"
004014DA	75 0C	jne crackme.4014E8	
004014DC	C74244 F0604000	mov dword ptr ss:[esp],crackme.4060F0	[esp]:&"MZh", 4060F0:"you are out of guesses"
004014E3	E8 04290000	call <JMP.&printf>	
004014E8	834424 4C 01	add dword ptr ss:[esp+4C],1	
004014ED	837C24 4C 05	cmp dword ptr ss:[esp+4C],5	
004014F2	0F8E 57FFFFFF	jle crackme.40144F	
004014F8	B8 00000000	mov eax,0	
004014FD	C9	leave	

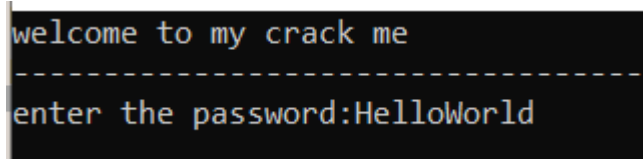
На этом скриншите видно, что программа дает 5 попыток ввода пароля. Сравнивает пароли через strcmp

00401493	837C24 48 00	cmp dword ptr ss:[esp+48],0	
00401498	75 0E	jne crackme.4014A8	
0040149A	C70424 B0604000	mov dword ptr ss:[esp],crackme.4060B0	[esp]:&"Mzh", 4060B0:"congrats you cracked the passw
004014A1	E8 0E2A0000	call <JMP.&puts>	
004014A6	EB 50	jmp crackme.4014F8	
004014A8	C70424 D2604000	mov dword ptr ss:[esp],crackme.4060D2	[esp]:&"Mzh", 4060D2:"wrong pass!!"
004014AF	E8 002A0000	call <JMP.&puts>	
004014B4	B8 05000000	mov eax,5	
004014B9	2B4424 4C	sub eax,dword ptr ss:[esp+4C]	
004014BD	894424 44	mov dword ptr ss:[esp+44],eax	[esp+44]:&"Mzh"
004014C1	8B4424 44	mov eax,dword ptr ss:[esp+44]	[esp+44]:&"Mzh"
004014C5	894424 04	mov dword ptr ss:[esp+4],eax	[esp+04]:&"^e]B\f"
004014C9	C70424 DF604000	mov dword ptr ss:[esp],crackme.4060DF	[esp]:&"Mzh", 4060DF:"you got %d left\n"
004014D0	E8 E7290000	call <JMP.&printf>	
004014D5	837C24 44 00	cmp dword ptr ss:[esp+44],0	[esp+44]:&"Mzh"
004014DA	75 0C	jne crackme.4014E8	
004014DC	C70424 F0604000	mov dword ptr ss:[esp],crackme.4060F0	[esp]:&"Mzh", 4060F0:"you are out of guesses"
004014E3	E8 D4290000	call <JMP.&printf>	
004014E8	834424 4C 01	add dword ptr ss:[esp+4C],1	
004014ED	837C24 4C 05	cmp dword ptr ss:[esp+4C],5	
004014F2	0F8E 57FFFFFF	jle crackme.40144F	
004014F8	B8 00000000	mov eax,0	
004014FD	C9	leave	

Поставим точку останова на строчку со сравнением паролей

0040144F	C70424 5C604000	mov dword ptr ss:[esp],crackme.40605C	
00401456	E8 592A0000	call <JMP.&puts>	
0040145B	C70424 97604000	mov dword ptr ss:[esp],crackme.406097	
00401462	E8 552A0000	call <JMP.&printf>	
00401467	8D4424 1A	lea eax,dword ptr ss:[esp+1A]	
0040146B	894424 04	mov dword ptr ss:[esp+4],eax	
0040146F	C70424 AB604000	mov dword ptr ss:[esp],crackme.4060AB	
00401476	E8 312A0000	call <JMP.&scanf>	
0040147B	8D4424 1A	lea eax,dword ptr ss:[esp+1A]	
0040147F	894424 04	mov dword ptr ss:[esp+4],eax	
00401483	8D4424 38	lea eax,dword ptr ss:[esp+38]	
00401487	890424	mov dword ptr ss:[esp],eax	
0040148A	E8 052A0000	call <JMP.&strcmp>	
0040148F	894424 48	mov dword ptr ss:[esp+48],eax	
00401493	837C24 48 00	cmp dword ptr ss:[esp+48],0	
00401498	75 0E	jne crackme.4014A8	
0040149A	C70424 B0604000	mov dword ptr ss:[esp],crackme.4060B0	
004014A1	E8 0E2A0000	call <JMP.&puts>	
004014A6	EB 50	jmp crackme.4014F8	
004014A8	C70424 D2604000	mov dword ptr ss:[esp],crackme.4060D2	
004014AF	E8 002A0000	call <JMP.&puts>	
004014B4	B8 05000000	mov eax,5	
004014B9	2B4424 4C	sub eax,dword ptr ss:[esp+4C]	
004014BD	894424 44	mov dword ptr ss:[esp+44],eax	
004014C1	8B4424 44	mov eax,dword ptr ss:[esp+44]	
004014C5	894424 04	mov dword ptr ss:[esp+4],eax	
004014C9	C70424 DF604000	mov dword ptr ss:[esp],crackme.4060DF	

Запустим программу и введем случайный пароль



Сработала точка останова

0040146F	C70424 AB604000	mov dword ptr ss:[esp],crackme.4060AB	[esp]:&"password123", 4060AB:"%s"
00401476	E8 312A0000	call <JMP.&scanf>	
0040147B	8D4424 1A	lea eax,dword ptr ss:[esp+1A]	
0040147F	894424 04	mov dword ptr ss:[esp+4],eax	[esp+04]:&"HelloWorld"
00401483	8D4424 38	lea eax,dword ptr ss:[esp+38]	
00401487	890424	mov dword ptr ss:[esp],eax	[esp]:&"password123"
0040148A	E8 052A0000	call <JMP.&strcmp>	
0040148F	894424 48	mov dword ptr ss:[esp+48],eax	
00401493	837C24 48 00	cmp dword ptr ss:[esp+48],0	
00401498	75 0E	jne crackme.4014A8	
0040149A	C70424 B0604000	mov dword ptr ss:[esp],crackme.4060B0	[esp]:&"password123", 4060B0:"congrats you cracked the password"
004014A1	E8 0E2A0000	call <JMP.&puts>	
004014A6	EB 50	jmp crackme.4014F8	
004014A8	C70424 D2604000	mov dword ptr ss:[esp],crackme.4060D2	[esp]:&"password123", 4060D2:"wrong pass!!"
004014AF	E8 002A0000	call <JMP.&puts>	
004014B4	B8 05000000	mov eax,5	eax:&"password123"
004014B9	2B4424 4C	sub eax,dword ptr ss:[esp+4C]	
004014BD	894424 44	mov dword ptr ss:[esp+44],eax	
004014C1	8B4424 44	mov eax,dword ptr ss:[esp+44]	
004014C5	894424 04	mov dword ptr ss:[esp+4],eax	[esp+04]:&"HelloWorld"
004014C9	C70424 DF604000	mov dword ptr ss:[esp],crackme.4060DF	[esp]:&"password123", 4060DF:"you got %d left\n"
004014D0	E8 E7290000	call <JMP.&printf>	
004014D5	837C24 44 00	cmp dword ptr ss:[esp+44],0	
004014DA	75 0C	jne crackme.4014E8	
004014DC	C70424 F0604000	mov dword ptr ss:[esp],crackme.4060F0	[esp]:&"password123", 4060F0:"you are out of guesses"
004014E3	E8 D4290000	call <JMP.&printf>	

Отсюда получаем искомый пароль: password123

Осталось его проверить

```
welcome to my crack me
-----
enter the password:HelloWorld
wrong pass!!
you got 4 left
-----
enter the password:password123
congrats you cracked the password
```