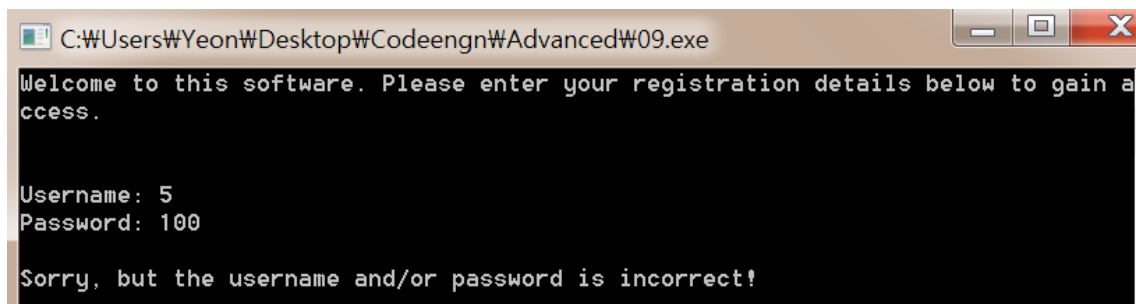


코드 엔진 Challenges: Advance 09

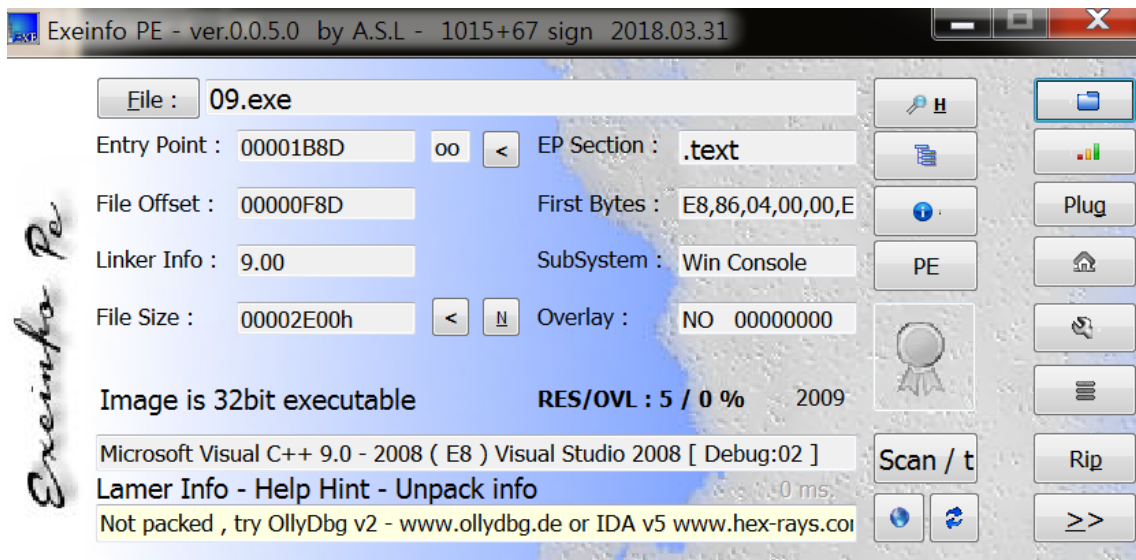
Author: MulleDK13

Korean: password는 무엇인가

파일을 실행하면 username과 password를 입력하는 화면이 나오는데 문제에서 어떠한 설명도 없으므로 username과 password 두 개 모두에 임의의 값을 넣는다.



PEID로 특이사항과 패킹여부를 확인한후 올리디버거로 분석해보자.



파일은 C++로 작성되어있고 패킹되어있지 않기 때문에 바로 올리디버거로 분석하면 될 것 같다.

Text strings referenced in 09:text		
Address	Disassembly	Text string
0027105F	MOV ECX, 09.00273218	ASCII "DonaldDuck"
002712C1	MOV ESI, 09.002731C8	ASCII "Welcome, TheRightName. You've gained access!"
002712FA	MOV ESI, 09.00273190	ASCII "Sorry, but the username and/or password is incorrect!"
00271367	MOV ESI, 09.00273138	ASCII "Welcome to this software. Please enter your registration details be
002713BE	PUSH 09.00273224	ASCII "Username: "
002713E0	PUSH 09.00273230	ASCII "Password: "
00271B80	CALL 09.00272018	(Initial CPU selection)
00271FED	PUSH 30000	ASCII "Actx "

문자열 찾기를 보면 Username과 ,Password가 보이고 성공문자열과 실패문자열이 보인다. 따라 들어가보자.

일단 어떤 아이디와 어떤 패스워드를 입력해야하는지 모르기 때문에 아이디부터 찾아보자.

002E13BE	68 24322E00	PUSH 09.002E3224	ASCII "Username: "
002E13C3	51	PUSH ECX	MSVCP90.7c0e3V7\$basic_ostream@DU?\$char_traits@Estd@
002E13C4	E8 57030000	CALL 09.002E1720	
002E13C9	8B15 58302E00	MOV EDI, DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@	MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@
002E13CF	68 0C442E00	PUSH 09.002E440C	
002E13D4	52	PUSH EDI	
002E13D5	FF15 54302E00	CALL DWORD PTR DS:[&MSVCP90.77575DU7\$char_traits@Estd@Estd@VAAV7\$basic_ist	MSVCP90.77575DU7\$char_traits@Estd@Estd@VAAV7\$basic_ist
002E13DB	A1 78302E00	MOV EAX, DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@	Arg2 = 002E3230 ASCII "Password: "
002E13E0	68 30322E00	PUSH 09.002E3230	Arg1 => 74E16BC8
002E13E5	50	PUSH EAX	09.00271720
002E13E6	E8 35030000	CALL 09.002E1720	
002E13EB	8B0D 58302E00	MOV ECX, DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@	MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@
002E13F1	83C4 18	ADD ESP, 18	
002E13F4	68 2C442E00	PUSH 09.002E442C	
002E13F9	FF15 3C302E00	CALL DWORD PTR DS:[&MSVCP90.77575DU7\$basic_istream@DU?\$char_traits@Estd@Estd@	MSVCP90.77575DU7\$basic_istream@DU?\$char_traits@Estd@Estd@
002E13FF	E8 FCFBFFFF	CALL 09.002E1000	
002E1404	A1 58302E00	MOV EAX, DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@	
002E1409	8B08	MOV ECX, DWORD PTR DS:[EAX]	
002E140B	8B49 04	MOV ECX, DWORD PTR DS:[ECX+4]	
002E140E	6A 00	PUSH 0	
002E1410	6A 00	PUSH 0	
002E1412	03C8	ADD ECX, EAX	
002E1414	FF15 4C302E00	CALL DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_ios@WU?\$char_traits@W@Estd@Estd@	MSVCP90.7c0e3V7\$basic_ios@WU?\$char_traits@W@Estd@Estd@
002E141A	8B0D 58302E00	MOV ECX, DWORD PTR DS:[&MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@	MSVCP90.7c0e3V7\$basic_istream@DU?\$char_traits@Estd@
002E1420	6A 00	PUSH 0	

002E113BE 로 이동하면 username 문구가 저장되어있다. 진행을 해보면 002E13D5부에서 username을 입력받는다. 간단하게 user라고 입력해보자. EAX에 74E16BC8이 저장되고 다음 명령어를 실행하면 passwd 출력 문자열이 스택에 첫 번째 인자로 저장 되고 EAX값이 스택에 두 번째 인자로 들어간다 그리고 함수 002E1720이 호출된다. 그리고 002E13F9에서 비밀번호를 100을 입력했다. 그리고 002EC1000이 출력되면서 실패 문자열이 출력되는 것을 확인하였다 .

이 함수를 따라 들어가보자.

001B1000	51	PUSH ECX	MSVCP90.74DBDD7F
001B1001	53	PUSH EBX	
001B1002	56	PUSH ESI	
001B1003	B9 F8311B00	MOV ECX, 09.001B31F8	
001B1008	B8 0C441B00	MOV EAX, 09.001B440C	ASCII "user"
001B100D	8D49 00	LEA ECX, DWORD PTR DS:[ECX]	
001B1010	> 8A10	MOV DL, BYTE PTR DS:[EAX]	
001B1012	3A11	CMP DL, BYTE PTR DS:[ECX]	
001B1014	75 1A	JNZ SHORT 09.001B1030	
001B1016	84D2	TEST DL, DL	
001B1018	74 12	JE SHORT 09.001B102C	
001B101A	8A50 01	MOV DL, BYTE PTR DS:[EAX+1]	
001B101D	3A51 01	CMP DL, BYTE PTR DS:[ECX+1]	
001B1020	75 0E	JNZ SHORT 09.001B1030	
001B1022	83C0 02	ADD EAX, 2	
001B1025	83C1 02	ADD ECX, 2	
001B1028	84D2	TEST DL, DL	
001B102A	75 F4	JNZ SHORT 09.001B1010	
001B102C	> 33C0	XOR EAX, EAX	
001B102E	EB 05	JMP SHORT 09.001B1035	
001B1030	> 1BC0	SBB EAX, EAX	
001B1032	83D8 FF	SBB EAX, -1	

우리가 입력한 user도 보이고 비교문,분기문 등이 보인다. 한줄씩 실행해보자.

우리가 입력한 001b440에 저장된 user가 eax에 저장된다. 그리고 001b31f8에 저장된 001b31f8이 ECX에도 저장되었다.

차례대로 실행해보자.

001B1010.MOV DL,BYTE PTR DS:[EAX]

DS:[001B440C]=75 ('u')
DL=0A (Line Feed)

```
DS:[001B31F8]=00
DL=75 ('u')
```

//비교한 값이 같지않으면 분기하는데 같지않아 분기하게된다.

001F1030	> 1BC0	SBB EAX,EAX	
001F1032	> 8D08 FF	SBB EAX,-1	09.001f440c
001F1035	> 8BDD 04441F00	MOV ECX,DWORD PTR DS:[1F4404]	
001F103B	> 8B15 50301F00	MOV EDI,DWORD PTR DS:[<&MSVCP90.?end!std@?basic_ostream@DU?\$char_traits@WU?>	MSVCP90.?end!std@?VAANAV?\$basic_ostream@DU?\$char_traits@WU?>
001F1041	> 85C0	TEST EAX,EAX	
001F1043	> A1 2C441F00	MOV EAX,DWORD PTR DS:[1F442C]	
001F1048	> 0F9AC3	SETBE BL	
001F104B	> 3B01	CMP EAX,DWORD PTR DS:[ECX]	
001F104D	> 8BD0 78301F00	MOV ECX,DWORD PTR DS:[<&MSVCP90.?cout@std@?basic_ostream@DU?\$char_traits@WU?>	MSVCP90.?cout@std@?3V?\$basic_ostream@DU?\$char_traits@WU?>.??6?>basic_ostream@WU?\$char_traits@WU?>
001F1053	> 52	PUSH EDX	
001F1054	> 0F944A24 0F	SETE BYTE PTR SS:[ESP+FI	
001F1059	> FF15 44301F00	JNZL DWORD PTR DS:[<&MSVCP90.??6?>basic_ostream@WU?\$char_traits@WU?>	MSVCP90.??6?>basic_ostream@WU?\$char_traits@WU?>
001F105F	> B9 18321F00	MOV ECX,09.001f3218	ASCII "Donald Duck"
001F1064	> B8 0C441F00	MOV EAX,09.001f440c	ASCII "user"
001F1069	> 8DA424 00000000	LEA ESP,DWORD PTR SS:[ESP]	
001F1070	> 8A10	MOV DL,BYTE PTR DS:[EAX]	
001F1072	> 3A11	CMP DL,BYTE PTR DS:[ECX]	
001F1074	> ~ 75 1A	JNZ SHORT 09.001F1090	
001F1076	> 84D2	TEST DL,DL	
001F1078	> ~ 74 12	JE SHORT 09.001F108C	
001F107A	> 8A50 01	MOV DL,BYTE PTR DS:[EAX+1]	
001F107D	> 3A51 01	CMP DL,BYTE PTR DS:[ECX+1]	
001F1080	> ~ 75 0F	JNZ SHORT 09.001F1090	

즉 DonaldDuck이 우리가 입력해야하는 name인 것을 알 수 있다.

```

01001021 > EB 05          SBB EBX,EBX
01001030 > 1BC0          SBB EAX,EAX
01001032 > 83D8 FF       SBB EAX,-1
01001035 > 8BD0 04440A01 MOV ECX,DWORD PTR DS:[100A4401]
0100103B > 8B15 50300A01 MOV EDX,DWORD PTR DS:[<&MSVC$P0.?end!@MSVC$P0.?end!@std::basic_ostream@DU?$char_traits@DU?@]
01001041 > 85C0          TEST EAX,EAX
01001043 > A1 2C440A01  MOV EAX,DWORD PTR DS:[100A442C]
01001048 > 0F94C9       SETE BL
0100104B > 3B01          CMP EAX,DWORD PTR DS:[ECX]
0100104D > 8BD0 78300A01 MOV ECX,DWORD PTR DS:[<&MSVC$P0.?cout@MSVC$P0.?cout@std::basic_ostream@DU?$char_traits@DU?@]
01001053 > 52           PUSH EDX
01001054 > 0F944424 0F SETE BYTE PTR SS:[ESP+4]

```

```
Welcome to this software. Please enter your registration details below to gain access.

Username: DonaldDuck
Password: 8921743

I can't believe you felt for that! xD

Sorry, but the username and/or password is incorrect!
_
```

여전히 틀렸다고 나온다.

0125120D	74 30	JF SHORT 09.0125120F	
0125120F	807C24 0B 00	CMP BYTE PTR SS:[ESP+0B],0	
012512B4	74 29	JF SHORT 09.0125120F	
012512B6	0FB605 C83125	MOVZX EAX, BYTE PTR DS:[12531C8]	
012512BD	84C0	TEST AL, AL	
012512BF	74 47	JF SHORT 09.01251308	
012512C1	BE C8312501	MOV ESI, 09.012531C8	ASCII "Welcome, TheRightName. You've gained access!"
012512C6	> 50	PUSH EAX	

성공문을 출력하는 부분으로 찾아가보니 맞아도 00a112ad부분에서 실패할 때 나오는 문자열을 출력한다. 패치를 해주도록 하자.

012512AD	75 30	JNZ SHORT 09.0125120F	
012512AF	807C24 0B 00	CMP BYTE PTR SS:[ESP+0B],0	
012512B4	74 29	JF SHORT 09.0125120F	
012512B6	0FB605 C83125	MOVZX EAX, BYTE PTR DS:[12531C8]	
012512BD	84C0	TEST AL, AL	
012512BF	74 47	JF SHORT 09.01251308	
012512C1	BE C8312501	MOV ESI, 09.012531C8	ASCII "Welcome, TheRightName. You've gained access!"

```
Welcome to this software. Please enter your registration details below to gain access.

Username: DonaldDuck
Password: 8921743

I can't believe you felt for that! xD

Welcome, TheRightName. You've gained access!
```

패치후 다시 입력해주니 제대로 돌아가는 것을 확인할 수 있다.