

# Gre Hack CTF 2012(root-me\_ch4)

## PE\_0\_protect

Author : hideroot(M.O.K)

Data : 11/4 2017

```
C:\Users\shin>C:\Users\shin\Desktop\system_hacking\system_hacking\rootme\ch15.exe abcd
Wrong password
```

문제를 받아서 실행 시켜 보았다. Cmd 에서 실행 시켰다. 실행 시켜보니 인자를 받으라고 해서 인자를 아무거나 넣어주었고(abcd) 출력을 보니 Wrong Password를 뱉었다.

자 이제 분석을 들어가보자. 올디버거로 분석 해보았다. 일단 열어보니 main 이 아닌듯 하다 뭐 상관은 없다. 나는 저 Wrong Password 주변에서 분석해보기로 했다.

004012C4	MOV DWORD PTR SS:[ESP+4],ch15.00404000	ASCII "_set_invalid_parameter_handler"
00401460	SUB ESP,0C	(Initial CPU selection)
004016AF	MOV DWORD PTR SS:[ESP],ch15.00404020	ASCII "libgcj.s.dll"
004016CA	MOV DWORD PTR SS:[ESP+4],ch15.0040402D	ASCII "Jv_RegisterClasses"
00401705	MOV EAX,ch15.00404044	ASCII "Usage: %s pass"
00401791	MOV EAX,ch15.00404053	ASCII "Gratz man :)"
004017AA	MOV DWORD PTR SS:[ESP],ch15.00404060	ASCII "Wrong password"
00401A03	MOV EDX,ch15.00404074	ASCII "Unknown error"
00401A39	MOV DWORD PTR SS:[ESP+4],ch15.00404084	ASCII "matherr(): %s in %s(%g, %g) (retval=%g)"
00401A80	MOV DWORD PTR SS:[ESP],ch15.004041A8	ASCII "mingw-w64 runtime failure:"
00401BF6	MOV DWORD PTR SS:[ESP],ch15.004041E4	ASCII "VirtualQuery failed for %d bytes at address %p"
00401C0A	MOV DWORD PTR SS:[ESP],ch15.004041C4	ASCII "Address %p has no image-section"
00401D14	MOV DWORD PTR SS:[ESP],ch15.0040424C	ASCII "Unknown pseudo relocation bit size %d."
00401E73	MOV DWORD PTR SS:[ESP],ch15.004041E4	ASCII "VirtualQuery failed for %d bytes at address %p"
00401E87	MOV DWORD PTR SS:[ESP],ch15.00404218	ASCII "Unknown pseudo relocation protocol version %d."
00402275	MOV DWORD PTR SS:[ESP],ch15.00404278	UNICODE "msvcrt.dll"
0040239C	ASCII "B@",0	

Search for 에서 refer to string 을 펼치면 현재 프로그램 내에서 사용하는 문자 시퀀스를 보여준다. 여기서 Wrong password나 Gratz man :) 에 브포를 걸고 가면 되겠다는 느낌이 났을 것이다. 0x401791에 Gratz Man :) 문자열이 있는 것으로 보아 이주변을 분석하면 패스워드를 알아 낼수 있을 것 같다.

00401726	55	PUSH EBP	
00401727	89E5	MOV EBP,ESP	
00401729	83EC 28	SUB ESP,28	
0040172C	C745 F4 000000	MOV DWORD PTR SS:[EBP-C],0	
00401733	837D 0C 07	CMP DWORD PTR SS:[EBP+C],7	
00401737	75 71	JNZ SHORT ch15.004017AA	
00401739	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
0040173C	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
0040173F	3C 53	CMP AL,53	
00401741	75 67	JNZ SHORT ch15.004017AA	
00401743	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401746	83C0 01	ADD EAX,1	
00401749	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
0040174C	3C 50	CMP AL,50	
0040174E	75 5A	JNZ SHORT ch15.004017AA	
00401750	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401753	83C0 02	ADD EAX,2	
00401756	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
00401759	3C 61	CMP AL,61	
0040175B	75 40	JNZ SHORT ch15.004017AA	
0040175D	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401760	83C0 03	ADD EAX,3	
00401763	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
00401766	3C 43	CMP AL,43	
00401768	75 40	JNZ SHORT ch15.004017AA	
0040176A	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
0040176D	83C0 04	ADD EAX,4	
00401770	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
00401773	3C 49	CMP AL,49	
00401775	75 33	JNZ SHORT ch15.004017AA	
00401777	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
0040177A	83C0 05	ADD EAX,5	
0040177D	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
00401780	3C 6F	CMP AL,6F	
00401782	75 26	JNZ SHORT ch15.004017AA	
00401784	8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401787	83C0 06	ADD EAX,6	
0040178A	0FB600	MOVZX EAX,BYTE PTR DS:[EAX]	
0040178D	3C 53	CMP AL,53	
0040178F	75 19	JNZ SHORT ch15.004017AA	
00401791	B8 53404000	MOV EAX,ch15.00404053	ASCII "Gratz man :)"
00401796	890424	MOV DWORD PTR SS:[ESP],EAX	
00401799	E8 12110000	CALL <JMP.&msvcrt.printf>	printf
0040179E	C70424 00000000	MOV DWORD PTR SS:[ESP],0	
004017A5	E8 F6100000	CALL <JMP.&msvcrt.exit>	exit
004017AA	> C70424 60404000	MOV DWORD PTR SS:[ESP],ch15.00404060	ASCII "Wrong password"
004017B1	E8 02110000	CALL <JMP.&msvcrt.puts>	puts

가서 보니 Push EBP로 Function Prologue 가 시작 되고 CMP로 ax, eax, al 에 있는 값들을 비교하기 시작한다. 이것들이 비교되었을 때 맞지 않다면 0x4017AA로 점프하는데 이 주소는 Wrong Password 출력하고 프로그램을 끝내버린다. 비교 되고 있는 문자들은 ASCII Code문자열로 보인다.

```
>>> chr(0x53)
'S'
>>> chr(0x50)
'p'
>>> chr(0x61)
'a'
>>> chr(0x43)
'C'
>>> chr(0x49)
'I'
>>> chr(0x6F)
'o'
>>> chr(0x53)
'S'
```

Python을 열고 스크립트는 귀찮아서 그냥 하나씩 쳐봤다. 쳐본후 문자열의 조합을 보면

### **SPaCloS**

라는 문자열을 얻게 된다. 그대로 입력해보니 성공

Ps1. 이게 대체 무슨말인가 싶어서 찾아 봤다. Gre Hack 이라고 하길래 왠지 느낌이 딱 그리스 같은 느낌이 오지 않는가? 그래서 그리스어로 넣고 번역기 돌려봤는데 "스포츠"라고 뜨더라. 근데 스펠링 하나 틀림 ㅋㅋ(답은 맞는듯)