Gre Hack CTF 2012(root-me_ch4)

PE_0_protect

Author : hideroot(M.O.K)

Data : 11/4 2017

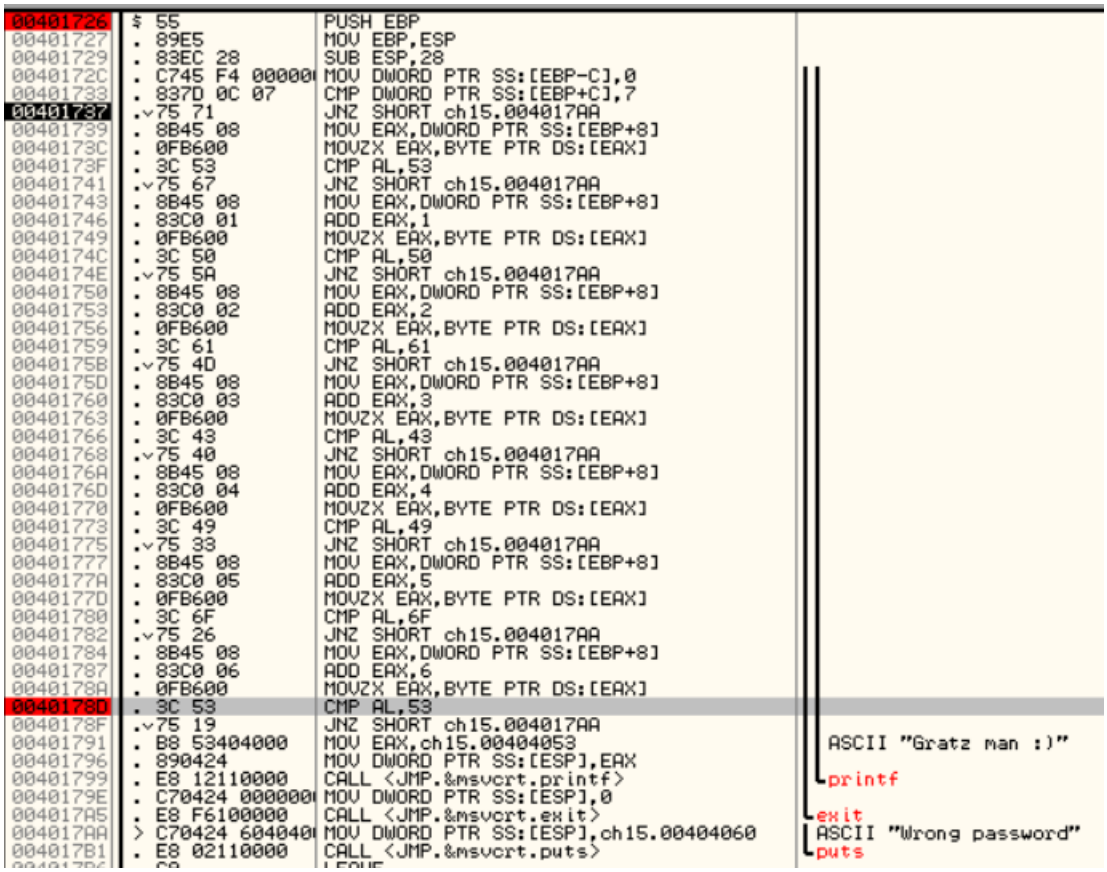
```
C:₩Users₩shin>C:₩Users₩shin₩Desktop₩system_hacking₩system_hacking₩rootme₩ch15.exe abcd
Wrong password
```

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. 올리디버거로 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"
004014E0 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"
00401706 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)□"
00401A8D 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 빡 올 것이다. 0x401791에 Gratz Man :) 문자열이 있는 것으로 보아 이주변을 분석하면 패스워드를 알아 낼수 있을 것 같다.



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

SPaCIoS

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)