Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Duelist’s Crack me 4 |
| 파일명 | due-cm4.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/12/26 ~ 2017/01/01 |
| 문제 내용 | user name과 그에 맞는 register code를 구하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



user name과 code를 입력하는 2개의 칸이 있고 Check 버튼을 누르면 정답 여부를 체크하게 됩니다.



Check 버튼을 눌렀을 때의 루틴입니다. 2개의 SendDlgItemMessageA 메소드를 통해 username과 code 값을 가져옵니다. username을 읽어온 뒤 체크를 하는데 길이를 체크해 1~8자리의 길이가 아니면 invalid로 넘어가게 됩니다. 그 후, register code에선 ESI register에 저장한 username의 길이와 자신의 길이가 같은지를 비교해 다르면 invalid로 넘어갑니다. 즉, username과 register code의 길이는 같아야 합니다.



2개의 길이값 계산을 하고 난 후의 루틴입니다.

402160 주소에 저장된 username 값을 처음부터 읽어가는데 각 index의 값이 0x41 ~ 0x7A의 범위를 벗어나면 invalid로 넘어가게됩니다. 범위 내에 존재하면 0x5A 가 아닌 이상 0x20를 자신에서 뺍니다. 그 후, 402017 주소부터 시작되는 encode table 값을 차례대로 읽어 자신과 비교해 맞는 값이 나올때까지 찾습니다. 그 후, 찾은 index를 40203C 주소부터 시작되는 다른 encode table에 대입해 그 값을 encoded username 값으로서 저장합니다.



두 개의 encode table 주소값입니다. 이를 통해 username을 encode 하게 되는데 예를 들어 username "test"에서 t는 0x74이므로 0x20를 빼면 0x54이고 이를 첫 번째 encode table에서 찾으면 ESI는 0x17(=23)이고 두 번째 encode table에서 이 index에 해당하는 값은 R(0x52)가 됩니다.

이를 통해 "test"의 username에 맞는 register code는 "RFCR"임을 알 수 있습니다.



알아낸 register code를 입력해서 정답 확인을 받은 화면입니다.