Computer Security HW0x1

R08946007 資科所 蔡昀達

Nickname : r08946007

1. 使用 ida pro & hex ray decompiler 先 decompile KeyChecker.exe 可以得到原始碼大概理解這隻程式的功能

```
8  size_t i; // [esp+2Ch] [ebp-Ch]
9
10 sub_4019E0();
11 v3 = GetModuleHandleA(0);
12 v6 = (_DWORD *)((char *)v3 + *((_DWORD *)v3 + 15));
13 v5 = __readfsdword(0x30u);
14 if ( *(_WORD *)v3 == 23117 && *v6 == 17744 )
15 {
16   sub_407CA0(
17     " -------------------------- \n"
18     " | B@ck t0 7he Fu7ur3...  \n"
19     " | en.wikipedia.org/wiki/Back_to_the_Future\n"
20     "  -------------------------- \n");
21   dword_40C040 = sub_401600(v6[2]);
22   sub_407CA0("[+] It's a time machine built in 1985, \n\tand you're in %i year now.\n");
23   if ( dword_40C040 != 1985 )
24     puts("[!] WARNING: \n\tit might be some trouble if you're not in 1985 year.");
25   *(_BYTE *)(v5 + 2);
26   sub_407CA0("[!] Time Machine Guarder: %s\n");
27   sub_407CA0("[+] input password to launch time machine: ");
28   gets(byte_40C060);
29   for ( i = 0; strlen(byte_40C060) > i; ++i )
30     byte_40C060[i] |= 0x20u;
31   sub_407CA0("[!] reading ... the.... passw0r..d.....\n");
32   for ( j = 0; j <= 18; ++j )
33   {
34     byte_40C060[j] ^= 2 * (dword_40C040 + 63) + *(_BYTE *)(v5 + 2) + 127;
35     if ( byte_40C060[j] != byte_408008[j] )
36     {
```

2. 擬定策略如下
   i. 在 line23 將 year 的變數改成 1985
   ii. 在 line26 使用 debugger 修改值繞過 time machine guarder
   iii. 在 line35 觀察正確的 input password 並使用 debugger 修改值
3. 最終得到 flag : FLAG{PE_!S_EASY}