LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN

RE CHALLENGES 3: crackme_by_chrisK_v02

Giảng viên hướng dẫn	Phạm Văn Hậu		ĐIỂM
Sinh viên thực hiện 1	Trần Đức Lương	19521815	

Đây là file exe PE 32-bit. Thử chạy chương trình với password nhập vào là "*test*" thì chương trình báo sai "*Wrong*". Ý tưởng của bài này cũng là đi tìm password đúng để chạy chương trình thành công.

```
PS E:\System Programming\RE Challenges\Release_3\crackme_by_chrisK_v02>
./crackme_by_chrisK_v02.exe
Enter Password: test
Wrong
```

Phân tích file bằng IDA Pro, mở Subview Strings thì thấy xuất hiện dòng '*Nice!!*' chính là mục tiêu chúng ta cần hướng tới. Thực truy xuất thì thấy nó nằm trong hàm ***main***.

.rdata:00405080	00000011	C	Enter Password:
.rdata:00405094	00000006	C	Wrong
.rdata:0040509A	00000015	C	Enter password key:
.rdata:004050AF	00000007	C	Nice!!

Thực hiện phân tích hàm ***main***, cụ thể password nhập vào sẽ được lưu vào chuỗi ***Str***, nó phải thỏa mãn có nhiều hơn 9 kí tự và kí tự thứ 6 phải là '.' (dấu chấm). Sau đó chương trình yêu cầu nhập password key được lưu vào chuỗi ***Str2***.

```
printf("Enter Password: ");
scanf("%s", Str);
if ( strlen(Str) > 9 && Str[5] == 46 )
{
  printf("Enter password key: ");
  scanf("%s", Str2);
```

Để chương trình in ra “Nice!!” , chúng ta cần nhập ***Str2*** đúng bằng ***mstring***. Ta sẽ đi tìm giá trị của chuỗi ***mstring***.

```
if ( !strcmp(mstring, Str2) )
{
  printf("Nice!!");
  result = 0;
}
else
{
  printf("Wrong");
  result = 1;
}
```

Ở block code này chương trình thực hiện tạo ra chuỗi v8, ta sẽ không cần quan tâm, chỉ cần debug để biết được giá trị v8. Sau đó ***v8*** và ***Str*** được đưa vào làm đối số cho hàm ***magic***.

```
while ( 1 )
{
  v4 = i++;
  if ( !Str[v4] )
    break;
  ++v9;
}
v8 = (char *)malloc(4 * v9);
srand(v9);
for ( i = 0; i < v9; ++i )
{
  v5 = &v8[4 * i];
  *(_DWORD *)v5 = rand() % v9 + v9 / -2;
}
magic(Str, v8);
```

Trong hàm ***magic***, chương trình thực hiện gán giá trị cho chuỗi ***mstring*** từ chuỗi ***Str*** và ***v8***.Ta chỉ cần đặt breakpoint như hình dưới rồi chạy debug với ***Str*** = ***“aaaaa.aaaa”*** để xem chuỗi ***mstring***.

```
v5 = 0;
for ( i = 0; ; ++i )
{
  v2 = v5++;
  if ( !*(_BYTE *)(v2 + a1) )
    break;
}
for ( j = 0; j < i; ++j )
  mstring[j] += *(_BYTE *)(4 * j + a2) + *(_BYTE *)(j + a1);
result = &mstring[j];
```

Sau khi debug thành công thì thấy giá trị của mảng ***mstring*** chính bằng chuỗi ***"]e^`c/^^be***".

```
public _mstring
; char mstring[52]
_mstring db 5Dh, 65h, 5Eh, 60h, 63h, 2Fh, 5Eh, 5Eh, 62h, 65h, 0, 0, 0, 0, 0, 0
                                        ; DATA XREF: _magic+3E↑o
                                        ; _magic+6F↑o ...
db 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
db 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

Như vậy ta chỉ cần nhập thêm password key ***Str2 = ""]e^`c/^^be"*** với password ***Str = "aaaaa.aaaa"*** thì chương trình sẽ thành công.

```
PS E:\System Programming\RE Challenges\Release_3\crackme_by_chrisK_v02>
./crackme_by_chrisK_v02.exe
Enter Password: aaaaa.aaaa
Enter password key: ]e^`c/^^be
Nice!!
```