Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Lập trình hệ thống

Kỳ báo cáo: Buổi 04

Tên chủ đề: Kỹ thuật dịch ngược cơ bản

GVHD: Đỗ Thị Hương Lan

Ngày báo cáo: 24/05/2022

1. THÔNG TIN CHUNG:

Lớp: NT209.M21.ATCL

STT	Họ và tên	MSSV	Email
1	Trương Đình Trọng Thanh	20520766	20520766@gm.uit.edu.vn
2	Trần Đức Minh	20521617	20521617@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài 1	100%
2	Bài 2	100%
3	Bài 3	100%

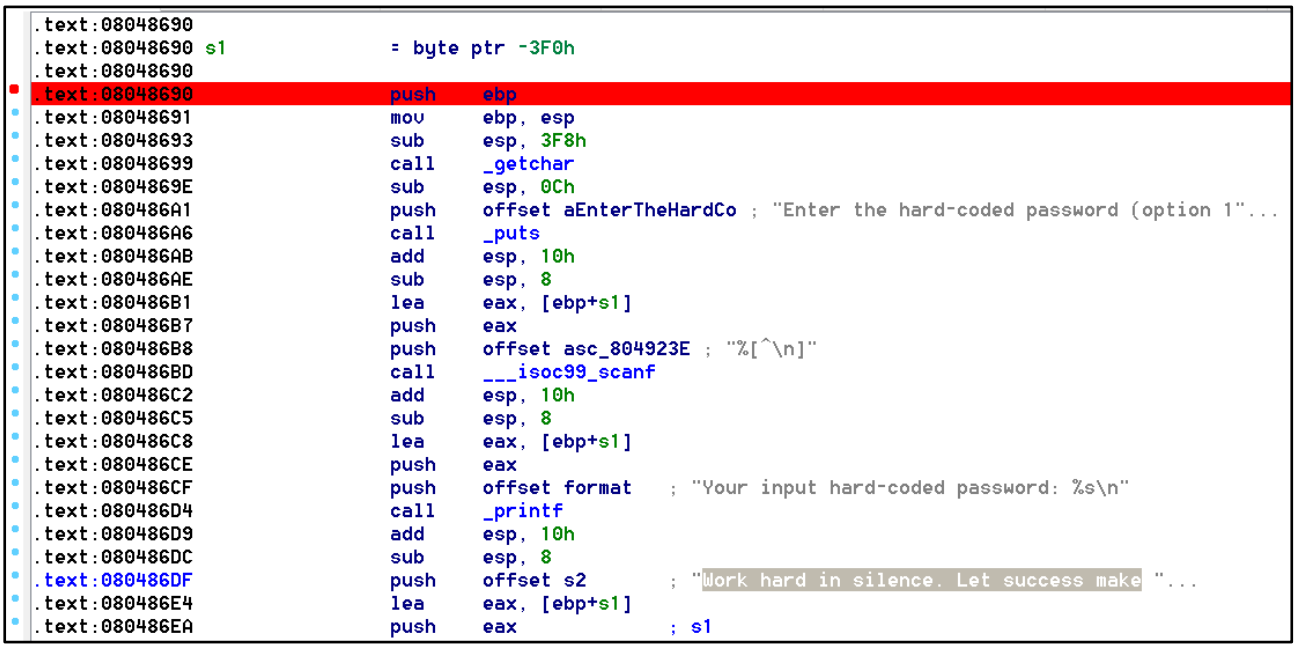
BÁO CÁO CHI TIẾT

1. Bài 1: Tìm passphase cố định (option 1)

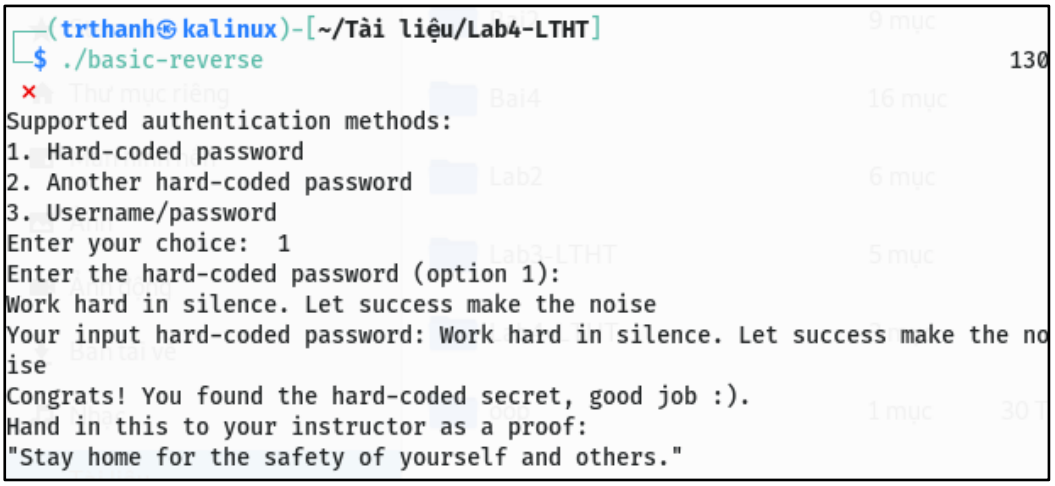
- Dò code ở mục HardCode

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành


Function name
_init_proc
_strcmp
_printf
_fflush
_getchar
_puts
_exit
_strlen
__libc_start_main
__isoc99_scanf
__gmon_start__
_start
__x86_get_pc_thunk_bx
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
is_equal
success_1
success_2
success_3
failed
hardCode
otherhardCode
userpass
int hardCode()
{
int result; // eax@2
char s1; // [sp+8h] [bp-3F0h]@1
getchar();
puts("Enter the hard-coded password (option 1):");
__isoc99_scanf("%[^\n]", &s1);
printf("Your input hard-coded password: %s\n", &s1);
if (!strcmp(&s1, "Work hard in silence. Let success make the noise"))
result = success_1();
else
result = failed();
return result;
}


.text:08048690
.text:08048690 s1 = byte ptr -3F0h
.text:08048690
.text:08048690 push ebp
.text:08048691 mov ebp, esp
.text:08048693 sub esp, 3F8h
.text:08048699 call _getchar
.text:0804869E sub esp, 0Ch
.text:080486A1 push offset aEnterTheHardCo ; "Enter the hard-coded password (option 1"...
.text:080486A6 call _puts
.text:080486AB add esp, 10h
.text:080486AE sub esp, 8
.text:080486B1 lea eax, [ebp+s1]
.text:080486B7 push eax
.text:080486B8 push offset asc_804923E ; "%[^\n]"
.text:080486BD call ___isoc99_scanf
.text:080486C2 add esp, 10h
.text:080486C5 sub esp, 8
.text:080486C8 lea eax, [ebp+s1]
.text:080486CE push eax
.text:080486CF push offset format ; "Your input hard-coded password: %s\n"
.text:080486D4 call _printf
.text:080486D9 add esp, 10h
.text:080486DC sub esp, 8
.text:080486DF push offset s2 ; "Work hard in silence. Let success make "...
.text:080486E4 lea eax, [ebp+s1]
.text:080486EA push eax ; s1

- Kết quả


(trthanh㉿kalinux)-[~/Tài liệu/Lab4-LTHT]
$ ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. Another hard-coded password
3. Username/password
Enter your choice: 1
Enter the hard-coded password (option 1):
Work hard in silence. Let success make the noise
Your input hard-coded password: Work hard in silence. Let success make the no
ise
Congrats! You found the hard-coded secret, good job :).
Hand in this to your instructor as a proof:
"Stay home for the safety of yourself and others."

2. Bài 2: Tìm passphase cố định (option 2)

- Kết nối giữa IDAPro và Linux để kiểm tra từng dòng code

```
.text:08048727                lea     eax, [ebp+s1]
.text:0804872D                push    eax
.text:0804872E                push    offset asc_804923E ; "%[^\n]"
.text:08048733                call    ___isoc99_scanf
.text:08048738                add     esp, 10h
.text:0804873B                sub     esp, 8
.text:0804873E                lea     eax, [ebp+s1]
.text:08048744                push    eax
.text:08048745                push    offset format   ; "Your input hard-coded password: %s\n"
.text:0804874A                call    _printf
.text:0804874F                add     esp, 10h
.text:08048752                mov     [ebp+var_C], 1
.text:08048759                mov     eax, [ebp+var_C]
.text:0804875C                mov     eax, WHAT_THAT[eax*4]
.text:08048763                mov     [ebp+s2], eax
.text:08048766                sub     esp, 8
.text:08048769                push    [ebp+s2]        ; s2
.text:0804876C                lea     eax, [ebp+s1]
.text:08048772                push    eax             ; s1
.text:08048773                call    _strcmp
.text:08048778                add     esp, 10h
.text:0804877B                test    eax, eax
.text:0804877D                jnz     short loc_8048786
.text:0804877F                call    success_2
.text:08048784                jmp     short loc_804878B
.text:08048786 ; ---------------------------------------------------------------------------
.text:08048786
.text:08048786 loc_8048786:                           ; CODE XREF: otherhardCode+77↑j
```

- Cho chương trình chạy đến dòng chứa thông tin của chuỗi dữ liệu WHAT_THAT vì WHAT_THAT là chuỗi dữ liệu chứa nhiều loại mật khẩu khác nhau nên phải truy theo dòng code cho đến khi chương trình chạy đúng dòng chứa dữ liệu WHAT_THAT ta sẽ tìm thấy được mật khẩu cần thiết.

- Kết quả:

```
└─$ ./basic-reverse
Supported authentication methods:
1. Hard-coded password
2. Another hard-coded password
3. Username/password
Enter your choice: 2
Enter the hard-coded password (option 2):
New one in, old one out
Your input hard-coded password: New one in, old one out
Congrats! You defeated a harder level of finding hard-coded secret :).
Hand in this to your instructor as a proof:
"Stay positive during the COVID-19 pandemic."
```

3. Bài 3: Tìm cặp username/password phù hợp

Code và giải thích chi tiết: