BÀI LÀM

1. re1.bin:

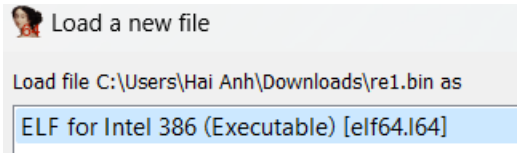
Chạy thử re1.bin trên Kali:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ./re1.bin
############################################################
##        Bienvennue dans ce challenge de cracking        ##
############################################################

Veuillez entrer le mot de passe :
```

Chương trình yêu cầu password nhập từ bàn phím. Chuỗi "Veui… : " tương đương "Nhập pass: "

Sử dụng IDP Pro 6.6 để mở file re1.bin, thấy file này có dạng ELF x64



Có thể hiểu những dòng đầu chỉ để khởi tạo chương trình:

```
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
```

Chú ý dòng mov [ebp+s2], offset a123456789, với biến a123456789 được ghi dưới đây:

```
.rodata:0804882D aReallocatingMe db 'Reallocating memory',0 ; DATA XREF: getString+6
.rodata:08048841 a123456789      db '123456789',0          ; DATA XREF: main+11↑o
.rodata:0804884B                 align 4
```

có ý nghĩa là đưa giá trị "123456789" vào ebp+s2.

```
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
mov     [ebp+s2], offset a123456789 ; "123456789"
mov     dword ptr [esp], offset s ; "##########################################"...
call    _puts
mov     dword ptr [esp], offset aBienvennueDans ; "##        Bienvennue dans ce challenge "...
call    _puts
```

Dòng mov dword ptr cùng với call _puts có mục đích xuất chuỗi ra màn hình

```
push    ecx
sub     esp, 24h
mov     [ebp+s2], offset a123456789 ; "123456789"
mov     dword ptr [esp], offset s ; "##########################################"...
call    _puts
mov     dword ptr [esp], offset aBienvennueDans ; "##        Bienvennue dans ce challenge "...
call    _puts
```

Với mốc “aVen” là dòng “Nhập pass”, đoạn dưới có chức năng lưu lại kí tự nhập vào ebp+s1

```
mov     dword ptr [esp], offset aVeuillezEntrer ; "Veuillez entrer le mot de passe : "
call    _printf
mov     eax, [ebp+s1]
mov     [esp], eax      ; ptr
call    getString
mov     [ebp+s1], eax
```

Sau đó chuyển giá trị từ s1, s2 sang esp và esp+4 rồi so sánh 2 chuỗi đó.

```
mov     eax, [ebp+s2]
mov     [esp+4], eax    ; s2
mov     eax, [ebp+s1]
mov     [esp], eax      ; s1
call    _strcmp
```

Rồi trả về kết quả “nhập đúng pass” hoặc “sai”

Từ đó đúc kết rằng, chuỗi “123456789” là password.

Nhập thử “123456789” vào chương trình. Chương trình in ra đoạn có ý nghĩa “nhập đúng pass”.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ./re1.bin
##########################################################
##        Bienvennue dans ce challenge de cracking      ##
##########################################################

Veuillez entrer le mot de passe : 123456789
Bien joue, vous pouvez valider l'epreuve avec le pass : 123456789!
```

2. Re2.exe:

Sử dụng IDA Pro, xem sub_401726

```
int __cdecl sub_401726(int a1, int a2)
{
  if ( a2 == 7
    && *(_BYTE *)a1 == 83
    && *(_BYTE *)(a1 + 1) == 80
    && *(_BYTE *)(a1 + 2) == 97
    && *(_BYTE *)(a1 + 3) == 67
    && *(_BYTE *)(a1 + 4) == 73
    && *(_BYTE *)(a1 + 5) == 111
    && *(_BYTE *)(a1 + 6) == 83 )
  {
    printf("Gratz man :)");
    exit(0);
  }
  return puts("Wrong password");
}
```

Ta thấy có 1 password giả, là số 7. Password đúng sẽ là giá trị nằm trong các biến còn lại. So sánh từng kí tự nhập vào với kí tự tương ứng (ASCII) trong Password:

a1 >< 83

a1+1 >< 80

a1+2 >< 97

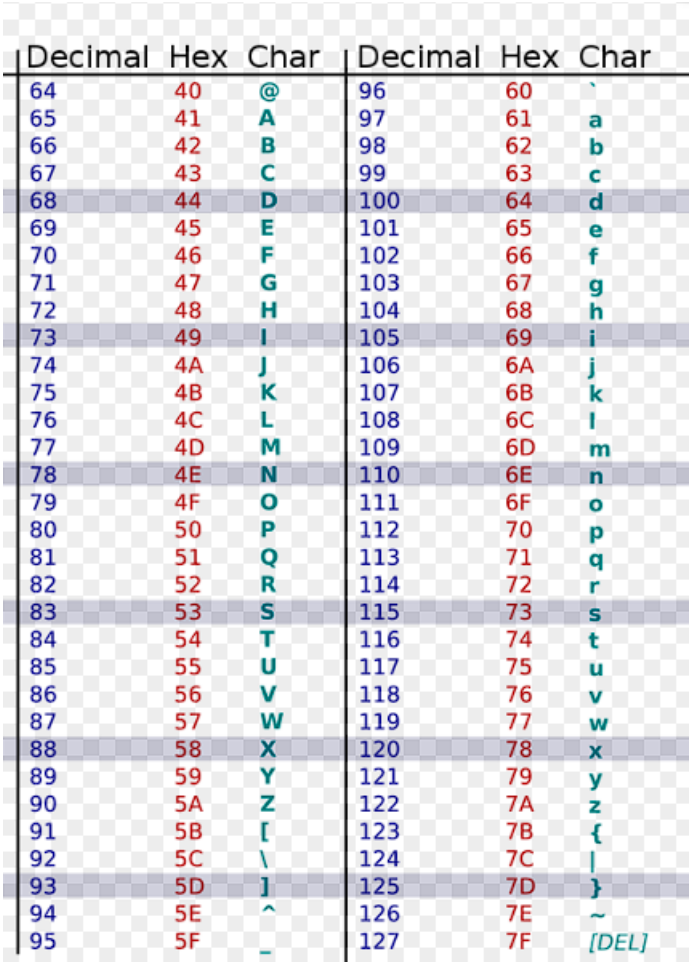
a1+3 >< 67

a1+4 >< 73

a1+5 >< 111

a1+6 >< 83

tương ứng với bảng ASCII:



Decimal	Hex	Char	Decimal	Hex	Char
64	40	@	96	60	`
65	41	A	97	61	a
66	42	B	98	62	b
67	43	C	99	63	c
68	44	D	100	64	d
69	45	E	101	65	e
70	46	F	102	66	f
71	47	G	103	67	g
72	48	H	104	68	h
73	49	I	105	69	i
74	4A	J	106	6A	j
75	4B	K	107	6B	k
76	4C	L	108	6C	l
77	4D	M	109	6D	m
78	4E	N	110	6E	n
79	4F	O	111	6F	o
80	50	P	112	70	p
81	51	Q	113	71	q
82	52	R	114	72	r
83	53	S	115	73	s
84	54	T	116	74	t
85	55	U	117	75	u
86	56	V	118	76	v
87	57	W	119	77	w
88	58	X	120	78	x
89	59	Y	121	79	y
90	5A	Z	122	7A	z
91	5B	[	123	7B	{
92	5C	\	124	7C	|
93	5D	]	125	7D	}
94	5E	^	126	7E	~
95	5F	_	127	7F	*[DEL]*

Vậy pass đúng là: SpaCIoS

Chạy thử với password vừa tìm:

```
C:\Users\Hai Anh\Downloads>re2.exe SPaCIoS
Gratz man :)
```

Vậy password của chương trình là SpaCIoS