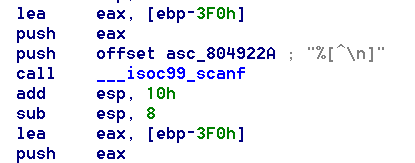
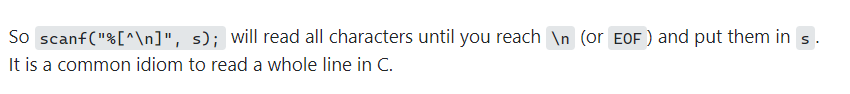
Bài 1:

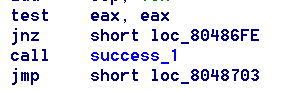




Hàm scanf sẽ được nhận 2 tham số, vị trí để lưu giá trị và kiểu định dạng. Sau khi bấm enter để hoàn thành nhập chuỗi, chương trình sẽ lấy địa chỉ lưu chuỗi và push vào stack

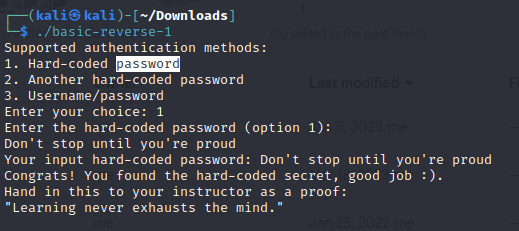


Sau đó hàm strcmp nhận 2 tham số lần lượt là địa chỉ chuỗi s1 và địa chỉ chuỗi s2, và thực hiện so sánh



Kết quả trả về sẽ lưu vào thanh ghi eax. Nếu giống nhau sẽ eax = 0, sau đó test thực hiện phép AND, 0&0 = 0 => thanh ghi ZF = 1 => jnz không thực hiện nhảy => gọi hàm success. Hoặc thất bại nếu ngược lại.

Graphical user interface, text, application

Description automatically generated

A picture containing text

Description automatically generated

Lấy chuỗi từ [ebp+s1] lưu vào eax, rồi push eax. Trước đó: push chuỗi từ s2



rồi gọi \_strcmp để so sánh



Nếu s1 = s2, nhảy tới success\_1

Bài 2:

28h: là 0x28 = 40 (10)

**Text

Description automatically generated with medium confidence**

**Table

Description automatically generated**

eax chứa 28h = 40 (10), vậy WHAT\_THAT[40\*4] tương ứng phần tử WHAT\_THAT[40] (vì mỗi phần tử 4 bytes) => Pass ở phần tử WHAT\_THAT[40]

3.

Graphical user interface, text, application

Description automatically generated

A picture containing icon

Description automatically generated

“byte ptr indicates that the memory operand refers to a byte in memory as opposed to a word or dword”

username: ebp + s

password: ebp + var\_25

Text

Description automatically generated with medium confidence

Text

Description automatically generated

Chạy code:

Text

Description automatically generated

Mã nguồn:

#include <stdio.h>

#include <string.h>

void check (char \*s, char \* v4){

for (int i = 0; i <= 8; i++){

char k = (v4[i] + s[i])/2;

printf ("%c", k);

}

}

int userpass()

{

size\_t v0; // ebx@2

int result; // eax@3

int v2; // eax@15

int v3; // edx@16

char v4[9]; // [sp+Ah] [bp-2Eh]@6

char v5[10]; // [sp+13h] [bp-25h]@1

char s[10]; // [sp+1Dh] [bp-1Bh]@1

char v7[5]; // [sp+27h] [bp-11h]@1

unsigned int i; // [sp+2Ch] [bp-Ch]@4

v7[0] = 85;

v7[1] = 71;

v7[2] = 37;

v7[3] = 56;

v7[4] = 111;

//getchar();

puts("Enter your username:");

scanf("%s", s);

getchar();

puts("Enter your password:");

scanf("%s", v5);

printf("Your input username: %s and password: %s\n", s, v5);

printf ("v7: %s \n", v7);

if ( strlen(s) == 9 && (v0 = strlen(s), v0 == strlen(v5)) )

{

for ( i = 0; (signed int)i <= 8; ++i )

{

printf ("i: %d \n", i);

if ( (signed int)i > 1 )

{

if ( (signed int)i > 3 )

v4[i] = v7[i - 4];

else

v4[i] = s[i + 5];

}

else

{

v4[i] = s[i + 2];

}

}

printf ("Chuoi~ v4: %s\n", v4);

check(s, v4);

for ( i = 0; ; ++i )

{

v2 = strlen(s);

if ( v2 <= i || (s[i] + v4[i]) / 2 != v5[i] ){

printf ("ki tu db s, v, /2: %c %c %c \n", s[i], v4[i], ((s[i] + v4[i]) / 2));

break;

}

}

v3 = strlen(s);

printf ("v3: %d \n", v3);

if ( v3 == i )

result = 1;

else

result = 0;

}

else

{

result = 0;

}

return result;

}

int main()

{

printf("Ket qua la`: %d",userpass());

return 0;

}