

LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN

RE CHALLENGES 2: WARGAMES

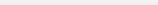
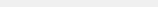

Giảng viên hướng dẫn	Phạm Văn Hậu		ĐIỂM
Sinh viên thực hiện 1	Trần Đức Lương	19521815	

Đây là file thực thi ELF 64-bit. Thực hiện chạy thử chương trình với không tham số đầu vào thì thấy chương trình báo cần thêm pass. Sau đó thử chạy với pass = **“test”** thì chương trình báo **“Wrong Password !!!”**. Ý tưởng của bài này chỉ là tìm password thích hợp.

```
(janlele91@kali)-[~/Documents/RE Challenges]
└─$ ./WarGames
Use ./WarGames pass

(janlele91@kali)-[~/Documents/RE Challenges]
└─$ ./WarGames test
Wrong Password !!!
```

Mở file **Wargames** bằng IDA Pro để thực hiện quá trình dịch ngược. Xem subview strings thì thấy có dòng “**Congratulation !!!**” chính là mục tiêu chúng ta cần hướng đến.

	.rodata:00000014	00000014	C	Use ./WarGames pass
	.rodata:00000013	00000013	C	Wrong Password !!!
	.rodata:00000013	00000013	C	Congratulation !!!

Truy vết string trên thì thấy nó nằm trong hàm **main**.

```
.rodata:0000000000495018 aWrongPassword db 'Wrong Password !!!',0  
; DATA XREF: main+57f0  
.rodata:0000000000495018 ; main+141f0  
.rodata:000000000049502B aCongratulation db 'Congratulation !!!',0  
; DATA XREF: main:loc_401E84f0
```

Mở hàm **main**, bắt đầu phân tích:

```
if ( j_strlen_ifunc(argv[1]) == 9 )
{
    memcpy(v6, "gssw#tpcz", sizeof(v6));
    v4 = 0;
    srand(1983LL);
    for ( i = 0LL; i <= 8; ++i )
    {
        v6[i] -= (int)rand() % 5 + 1;
        if ( v6[i] != argv[1][i] )
        {
            v4 = 1;
            break;
        }
    }
    if ( v4 )
        puts("Wrong Password !!!");
    else
        puts("Congratulation !!!");
    result = 0;
}
else
{
    puts("Wrong Password !!!");
    result = 0;
}
```

Ở đây **argv[1]** chính là **pass chúng ta nhập**, dựa vào dòng if đầu tiên ta thấy pass nhập vào phải là một chuỗi có **9 ký tự**. Để đi đến “**Congratulation !!!**”, chúng ta phải so sánh **argv[1]** với **v6**, nếu bằng nhau thì thành công. Tuy nhiên, với giá trị ban đầu là “**gssw#tpcz**”, qua vòng for thì từng ký tự của **v6** bị biến đổi bởi hàm **rand()**. Vì là random nên chúng ta phải đi debug chương trình 9 lần tương ứng với 9 ký tự để xem giá trị của từng ký tự sau khi rand() là bao nhiêu. Thực hiện debug với **Remote Linux Debugger** lần 1 với pass là “**abcd12345**” như hình dưới.

- [stack]:00007FFD3A4AC25F db 64h ; d
- [stack]:00007FFD3A4AC260 db 73h ; s
- [stack]:00007FFD3A4AC261 db 73h ; s
- [stack]:00007FFD3A4AC262 db 77h ; w
- [stack]:00007FFD3A4AC263 db 23h ; #
- [stack]:00007FFD3A4AC264 db 74h ; t
- [stack]:00007FFD3A4AC265 db 70h ; p
- [stack]:00007FFD3A4AC266 db 63h ; c
- [stack]:00007FFD3A4AC267 db 7Ah ; z

Quan sát ta thấy sau lần **rand()** đầu tiên thì **v6[0] = 'd' (0x64)** mà **argv[1][0] = 'a'** (pass là "abcd12345") nên chương trình in ra "**Wrong Password !!!**". Vậy để tiếp tục debug lần 2 thì **argv[1][0]** lúc này phải bằng **'d'**, ta sẽ debug với pass "**dbcd12345**". Quá trình diễn ra tương tự cho từng kí tự, kết quả cuối cùng ta nhận được là "**dont play**". Vậy đây chính là password chúng ta cần tìm.

```
(janlele91@kali)-[~/Documents/RE Challenges]
$ ./WarGames 'dont play'
Congratulation !!!
```