level14

태그	Assembly Shell
상태	완료

풀이과정

겪었던 어려움

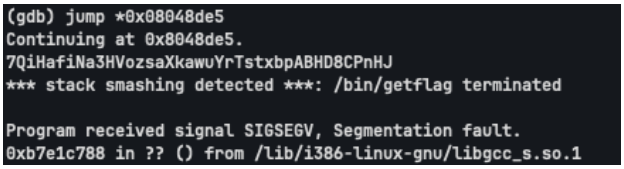
어셈블리어는 오지게 차갑다;

풀이과정

들어가면 아무 파일도 존재 하지않는다.

gdb를 이용해서 `gdb /bin/getflag` 명령어를 이용해서 디버깅 모드를 켜고 `disas main` 를 써서 확인해보면 `<ft_des>` 를 함수가 `0x08048bf3 <+685>: mov 0x804b060,%eax` 부분에 의거해서 이 값을 인자로 받아서 사용한다는 것을 알 수있다.

`b *main+1` 를 통해서 종단점을 잡고 `r` 을 통해서 실행시킨 후 ju(jump)를 통해서 첫번째 `<ft_des>`를 호출하기 전 인자를 입력하는 부분으로 강제 호출 시키는 `ju *0x08048bf3` 를 입력하면 flag00에 대한 flag값을 얻을 수 있고 이러한 원리로 마지막 `<ft_des>` 부분 앞에 있는 `0x08048de5 <+1183>: mov 0x804b060,%eax` 으로 이동하는 명령어 `ju *0x08048de5` 를 입력하면 flag값을 얻을 수 있다.



풀이과정(2)

우회해야 하는 함수는 ptrace와 getuid이다. gdb를 이용해서 해당 함수들의 리턴값을 조작하면 내가 원하는 권한을 탈취?가능하다

```
gdb /bin/getflag
//gdb를 이용해서 getflag 실행
```

```
break ptrace
run
return (int) 0
// ptrace까지 break를 걸어주고 실행한 다음 반환 값을 받아 0으로 조작
break getuid
continue
// 다시 getuid까지 break를 걸고 실행
return (int) 3014
// getuid 반환값을 3014(flag14)의 권한으로 변경
continue
```

실행하면 끝남

정답

```
level14@SnowCrash:~$ su flag14
Password:
Congratulation. Type getflag to get the key and send it to me the owner of this
livecd :)
flag14@SnowCrash:~$ getflag
Check flag.Here is your token : 7QiHafiNa3HVozsaXkawuYrTstxbpABHD8CPnHJ
```

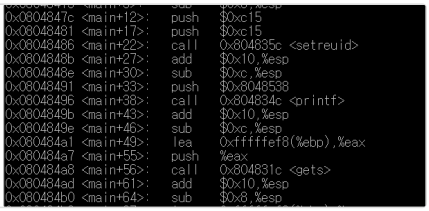
`“7QiHafiNa3HVozsaXkawuYrTstxbpABHD8CPnHJ”`

출처

gdb 명령어 모음

gdb 명령어 모음 시작과 종료 gdb (프로그램명): 시작 q(quit) / ctrl+d: 종료 file 프로그램명: 디버깅할 프로그램으로서 파일을 사용한다. disas 함수명: 특정 함수의 어셈블리 코드 출력 disas [주소] [주소]: 주소 사이의 어셈블리 코드 출력 jump *[주소]: 주소로 강제적 분기 (주소 외에 행번

https://yehey-study.tistory.com/entry/gdb-명령어-모음



[어셈블리] 범용 레지스터 EAX, EBX, ECX, EDX, ESI, EDI, EBP, ESP

1. EAX (Extended Accumulator Register)   EAX 레지스터는 산술(덧셈, 곱셈, 나...

https://m.blog.naver.com/PostView.naver?blogId=cung91&logNo=220196144355&fromRecommendationType=category&targetRecommendationDetailCode=1000