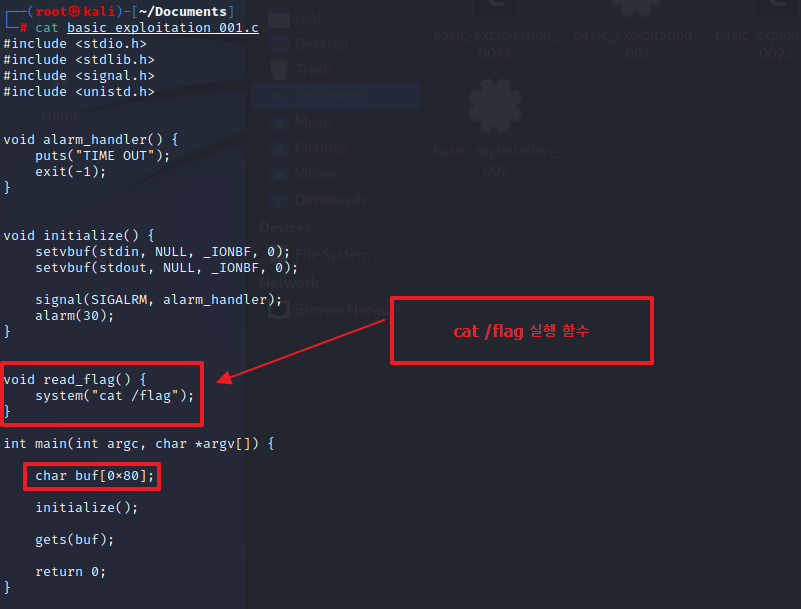
Dreamhack Systemhacking basic\_exploitation\_001 문제 풀이

Exploitation 문제는 칼리 리눅스가 되는 것이 있고, 안되는 것이 있어 우분투 리눅스와 병행 해서 썼습니다.

문제에 들어가면 다운로드 받을 수 있는 파일이 있습니다.

문제 파일을 다운로드 받은 후 문제 안을 들여다 보도록 하겠습니다.

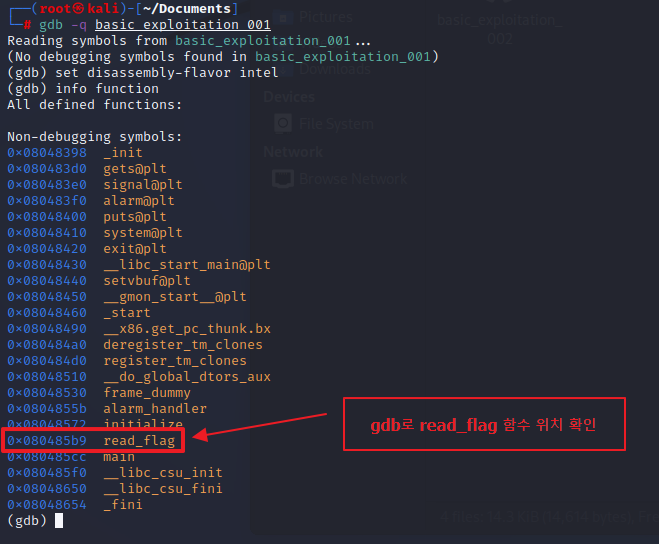


먼저 주어진 바이너리 코드를 cat 명령어로 확인했습니다.

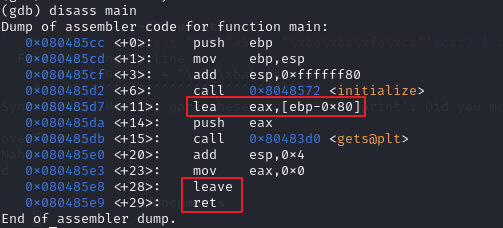
우선 main 함수에 buf 변수에 16진수 0x80값이 들어가 있다는 것을 알 수 있고,

main함수에는 없는 read\_flag 함수에 system(“cat /flag”) 명령이 들어있는 것을 확인했습니다.

Gdb로 바이너리 파일을 확인해보겠습니다.

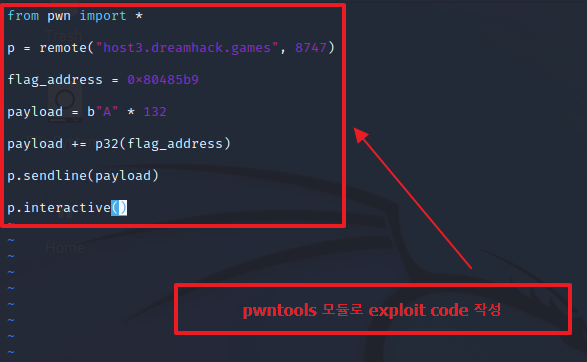


Gdb로 read\_flag 함수에 0x080485b9 주소 값이 있다는 것을 확인했습니다.



또한 0x80 크기만큼 입력을 할 수 있고, return 값까지 0x4 바이트가 남는 다는 것을 알 수 있습니다.

이제 exploit code를 짜보겠습니다.



Pwntools 라이브러리를 사용하였고 작성 언어는 python 입니다.

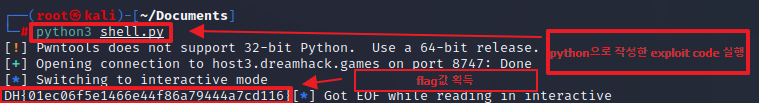
우선 remote 함수로 Host와 Port를 지정해줍니다. 로컬PC에 저장 되어있는 프로세스로 접속하려고 할 땐 process(“./파일이름”) 해주시면 됩니다.

아까 보았던 flag 함수의 주소 값을 flag\_address 변수에 넣어줍니다.

Payload 변수에는 0x84 크기 10진수로 변환했을 시 132byte가 나오기 때문에 문자열 “A”에 132를 곱해줍니다.

그리고 payload 변수에 p32 little endian으로 flag\_address 변수를 더해줍니다.

p.sendline 함수로 payload를 전송 해준 후 p.interactive 함수로 세션 유지 해줍니다.



exploit code 작성 후 python3으로 실행해 주면 이렇게 flag 값을 획득할 수 있습니다.