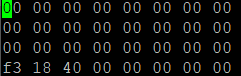
**AttackLAb**

Phase1

Touch1을 호출만 하면 되므로, Buffer overflow를 이용하여서 stack의 return address에 touch1의 주소가 들어가게 하면 된다. ctarget을 objdump로 조사한 결과 버퍼의 크기는 0x18즉 24바이트 였고, touch1함수는 4018f3이므로 버퍼의 크기만큼 입력하고 끝에 little endian에 주의하여서 touch1의 주소를 작성하면 된다.



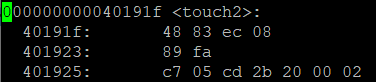
 24바이트만큼 채운다

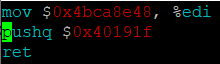
Touch1의 주소 입력(return address)

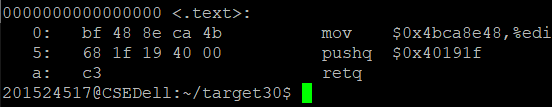
Phase2

주어진 쿠키값을 매개변수 레지스터 rdi에 넣어주고 touch2를 실행시키면 된다. 따라서 버퍼에 mov명령(쿠키값->rdi) 을 넣고 스택에 넣어준 다음 touch2에서 스택을 쓰게끔 실행시키면 된다. mov명령은 따로 간단히 만든다음 gcc로 어셈블해주고 objcump를 사용하면 직접만든 명령의 값을 볼 수 있다.

 cookie값

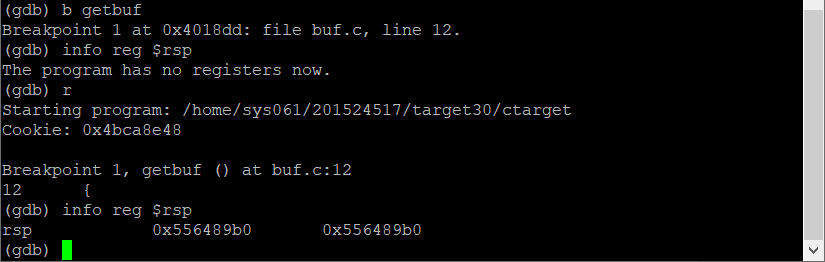
touch2의 주소는 0x40191f

 명령 만들기

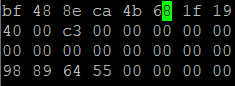


실행주소

버퍼의 주소는 gdb를 이용하여서 getbuf에 breakpoint를 넣고 실행하면 나오는 rsp의 주소에서 버퍼 크기만큼 뺀 주소이다.



저 주소에서 0x18을 빼면 된다. (0x556489b0 - 0x18 = 0x55648998)

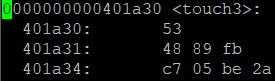
 mov하고 stack에 넣어주는 명령(mov, pushq, ret)을 포함해서 24바이트를 채운다.

버퍼(실행할 명령이 있는)의 주소(return address)

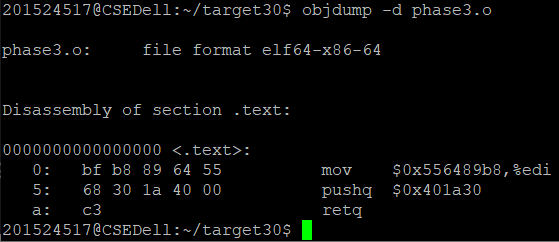
Phase3

Phase2와 비슷하지만 값이아닌 문자열로 주어야 한다. 문자열을 준뒤에 그 문자열이 있는 주소를 rdi에 주고 touch3을 실행되게 하면 된다. 그렇게 위해서는 touch2와 비슷하게 하되, 버퍼의 주소를 이용하여 버퍼안에 문자열을 넣고 그 위치의 주소를 rdi에 mov하고 스택에 넣어주고 스택에서 쓰게 실행시켜 주면 된다.

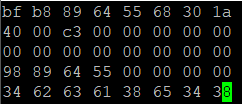
Rsp의 주소에서 첫명령의 주소가 return address로 위치하게 될것이므로 그 위에 문자열이 위치하게 된다. 따라서 문자열의 위치는 rsp주소 + 8바이트 이다. (0x556489b0 + 0x8 = 0x556489b8)

 touch3주소

 명령 만들기



실행주소

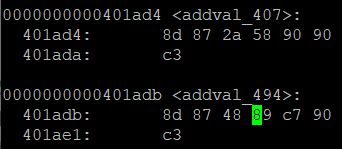
 mov하고 stack에 넣어주는 명령(mov, pushq, ret)을 포함해서 24바이트를 채운다.

버퍼(실행할 명령이 있는)의 주소(return address)

문자열(이곳의 주소를 쓰게 된다.)

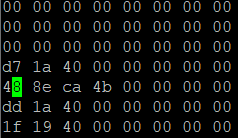
Phase4

여기서부터는 명령을 만들 수 없고, 있는 명령 중에서 골라서 써야한다. farm내부에 있는 함수들을 썼다. 사이에 90(nop)이 들어가도 되고, 주의해야 하는 점은 c3로 끝나야하는 것이다. return을 해야 다음 return address의 주소를 쓸 수 있기 때문이다. 하는 일은 touch2와 같다. 찾아보니 rax로 pop하는 함수와 rax에서 rdi로 mov하는 명령이 있었다. 따라서 버퍼에 쿠키값을 직접 넣고 그걸 rax로 pop해서 rax에서 rdi로 mov해주는 방법을 썼다.



Popq 명령: 0x401ad4 + 0x3 = 0x401ad7

Mov rax, rdi 명령: 0x401adb + 0x2 = 0x401add

버퍼를 채운다.

Popq rax

쿠키 값

Rax->rdi

Touch2의 주소

Phase5

여기서도 있는 명령들을 써서 문자열의 주소를 pop하여 rdi에 넣어주면 된다. add\_xy를 이용하여서 rsp의 주소를 rdi에 주고, offset을 rsi에 주어서 add\_xy를 실행시키면 문자열의 주소를 찾을 수 있고, 그 값은 rax에 저장되므로 rax에서 rdi로 mov하고 touch3을 실행 시키면 된다.

하지만, farm에서 적절한 명령을 찾지 못 하였다. 사이에 90이 있어도 되고, c3로 끝나는 명령들을 찾았는데, 적절하게 다 찾지를 못 하였다.