Return to shellcode

1.CALL & RET instruction

Call은 현재주소를 스택에 저장하고 다른 주소로 이동하고, RET은 스택에 저장한 주소로 다시 되돌아가는 것인데, 스택의 주소를 변경한다면 프로그램의 흐름을 바꿀 수 있다. -> stack overflow를 이용해 return adress를 바꿔 원하는 주소로 이동할 수 있다.

Ex) return address: 0x7fffffffe448 변수의 주소:0x7fffffffe400 => return adress가 72byte만큼 떨어져 있으므로 변수에 72byte를 입력하고 그 이상 입력하게 되면 return adress를 덮어쓸 수 있게 된다.

2.Permissions in memory

메모리영역에는 3가지 권한이 있는데 read(r), write(r), excute(x)는 각각 읽고, 쓰고, 실행을 할 수 있다는 것을 의미합니다. Shellcode를 실행하기 위해 이것이 저장된 영역은 실행 권한이 설정되어야 한다. GCC는 코드가 저장된 영역에 실행권한이 있고, 데이터 저장영역은 실행권한이 없습니다.