실습 2

내 주소 -->

The address of the input array : 0xffffd164

The value of the frame pointer : 0xffffd138

The value of the return address : 0x56556345

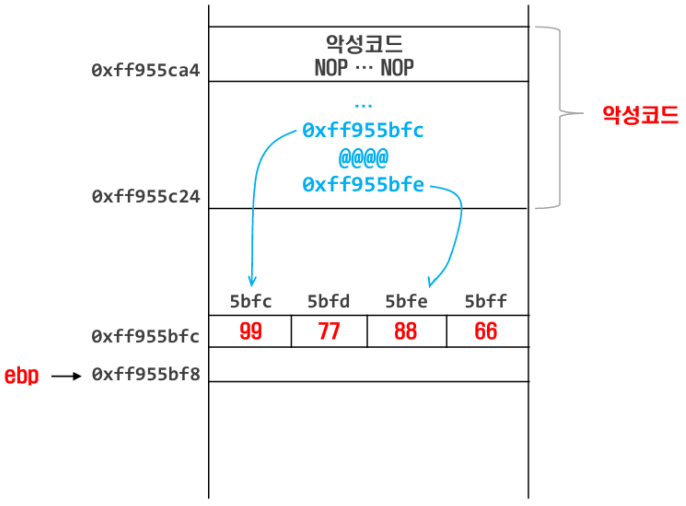
addr1, addr2 -> ret 주소(리턴주소)를 넣어서 쉘코드로 분기시키는 것이 목적

각각 ret의 2바이트 공간씩 할당하고, 중간에 구분자로 @@@@를 인자 데이터로 구분

addr1 = 리턴주소 + 2 (hn 기법) 내 주소 기준 : 0xffffd13e

addr2 = 리턴주소 내 주소 기준 : 0xffffd13c

리턴주소 : frame pointer (ebp) + 4 내 주소 기준 : 0xffffd138 + 4 = 0xffffd13c




```
   0x5bfc      0x5bfc      0x5bfc
+    0x01   +    0x02   +    0x03
----------  ----------  ----------
   0x5bfd      0x5bfe      0x5bff
```

hn 기법

4바이트의 %n 으로 특정 데이터를 넣는 것이 너무 오래 걸리기 때문에, %hn 으로 상위와 하위 2바이트로 나눠서 형식 지정자 인자를 넣어주기 위함

small, large -> 악성코드 주소 내 주소 기준 : 0xffffd164

small = 악성코드 주소 (2byte 기준 앞) - 12 – 19 * 8 내 주소 기준 : 0xffff - 12 - 19 * 8

large = 악성코드 주소 (2byte 기준 뒤) + 0x90 내 주소 기준 : 0xd164 + 0x90

small

-12 : 메모리에 설정한 2개의 4바이트 주소 + @@@@ 문자 4바이트

19 * 8 : 참조할 메모리의 스택위치가 21번째이기 때문, %x의 인자를 19번 할당 하였기 때문에 그만큼 문자열 길이를 빼준 것

나머지 하나%x는 문자열 길이(주소값) 맞춰주는 용도로 사용

large

0x90 : NOP