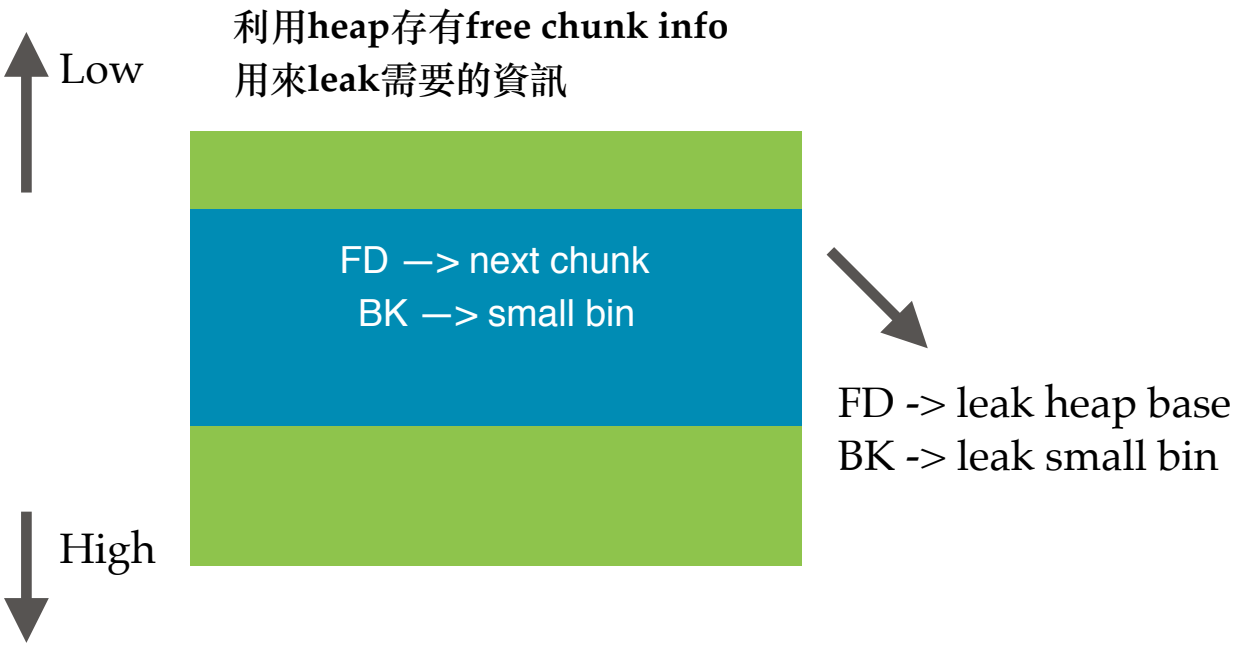
House of Force

HW5 Write up

r06922115 鄭皓謙 - 2017年12月6日




```
gdb-peda$ x/20gx $heap
0xacc000:       0x0000000000000000      0x0000000000000021
0xacc010:       0x6262626262626262      0x6262626262626262
0xacc020:       0x0000000000000000      0x000000000000fa1
0xacc030:       0x6161616161616161      0x00007f503a785188
0xacc040:       0x0000000000acc020      0x0000000000acc020
0xacc050:       0x0000000000000000      0x0000000000000031
0xacc060:       0x6262626262626262      0x6262626262626262
0xacc070:       0x6262626262626262      0x6262626262626262
0xacc080:       0x0000000000000000      0x000000000000f81
0xacc090:       0x0000000000000000      0x0000000000000000
gdb-peda$ heapinfo
(0x20)     fastbin[0]: 0x0
(0x30)     fastbin[1]: 0x0
(0x40)     fastbin[2]: 0x0
(0x50)     fastbin[3]: 0x0
(0x60)     fastbin[4]: 0x0
(0x70)     fastbin[5]: 0x0
(0x80)     fastbin[6]: 0x0
                  top: 0xacc080 (size : 0xf80)
       last_remainder: 0x0 (size : 0x0)
            unsortbin: 0x0
(0x020)  smallbin[ 0]: 0xaccfc0
gdb-peda$
```

詳細作法

首先利用boundary check有問題 read_input可以很輕易地做到house of force

```
44 void allocate_heap(){
45     size_t size ;
46     printf("Size :") ;
47     size = read_long();
48     heap = malloc(size);
49     if(heap){
50         printf("Data :");
51         //maybe leak spot, why size + 8?
52         read_input(heap,size+8);
53         puts("Done !");
54     }else{
55         puts("Error !");
56         _exit(0);
57     }
```

可是沒有heap的base只能做到將new top移到heap上的相對位置
所以必須將要leak的資訊放到heap上

透過malloc 超過top size,
grow top時會將舊的top 給free掉(注意有關的檢查,pagesize, in use flag)
於是做假的top配合house of force, free掉三個chunk
(兩個會被移到small bin ，另一個在unsorted bin)
就可以得到 有關libc base以及heap base
接著修改malloc_hook，就可以hijack control flow
直接跳去system
這時allocate_heap時 size填字串 /bin//sh的位置就可以成功拿到shell