HitCon Two

题目场景非常简单直接:

- 防护全开
- 给出Libc基址
- 栈全部用e填充
- 寄存器全部用随机值填充
- rip执行ret.

- 我们能做的:

- 输入16个Byte
- 16个Byte被放到rsp上
- 也就意味着可以执行两个gadget的rop

- 问题

跳去哪?。 只能控制两个gadget pop rsp可以将栈帧转移到libc上? 但是,也没办法有然后。

- 回忆Onegadget(MagicGadget)

libc里有一些地址可以直接跳过去拿shell。 One_gadget by david942j@217

```
int execve(const char *file, char *const argv[], char *const envp[])
ex: execve("/bin/sh", {"-c","ls","-l"},environ)
execve("/bin/sh", NULL, NULL)
```

```
eax, DWORD PTR [esi-0xb8]
mov
add
       esp,0xc
       DWORD PTR [esi+0x1620],0x0
mov
       DWORD PTR [esi+0x1624],0x0
mov
       DWORD PTR [eax]; environ
push
lea
       eax,[esp+0x2c]
push
       eax
       eax,[esi-0x567d5] ; "/bin/sh"
lea
push
call
       0xb0670 <execve>
```

```
add esp,0xc
->esp_1 = esp + 0xc
push environ (para_1)
->esp_2 = esp_1 - 4 = esp + 8
lea eax, [esp+0x2c]
->eax = esp_2 + 0x2c = esp + 34
--> execve("/bin/sh", esp + 0x34, environ)
--> constraint_1 : [esp+0x34] == NULL

从Libc任何一个位置去做符号执行,可以遍历one_gadget.
但是如何满足限制条件?
```

- find one gadget feeds all constraints

constraints found by one_gadget:

```
root@iZwz9gcvsrkr5nw9jw657bZ:~/TwoGadgets# one_gadget libc.so.6
0x4557a execve("/bin/sh", rsp+0x30, environ)
constraints:
  [rsp+0x30] == NULL
0xcde41 execve("/bin/sh", r15, r13)
constraints:
  [r15] == NULL || r15 == NULL
  [r13] == NULL || r13 == NULL
0xce0e1 execve("/bin/sh", [rbp-0x78], [rbp-0x50])
constraints:
  \lceil \lceil rbp - 0x78 \rceil \rceil == NULL \mid \lceil \lceil rbp - 0x78 \rceil == NULL
  [[rbp-0x50]] == NULL || [rbp-0x50] == NULL
0xf1651 execve("/bin/sh", rsp+0x40, environ)
constraints:
  [rsp+0x40] == NULL
0xf24cb execve("/bin/sh", rsp+0x60, environ)
constraints:
  \lceil r_{Sp} + 0x60 \rceil == NULL
root@iZwz9gcvsrkr5nw9jw657bZ:~/TwoGadgets# one_gadget libc.so.6
0x4557a execve("/bin/sh", rsp+0x30, environ)
constraints:
  [rsp+0x30] == NULL
```

- --> 观察libc里面的gadget,找不到可以set *(rsp+X) = NULL 这样的Gadget.
- --> 很难用一条Gadget设置两个寄存器恰好为需要的值.

怎么办? 观察一下这些one gadget.

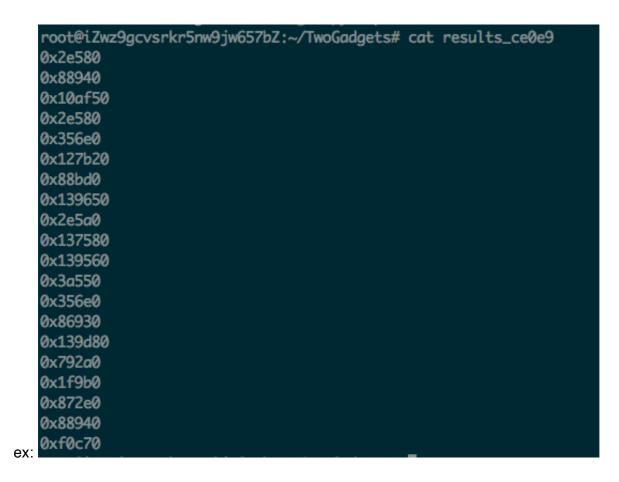
我们可以简单地选择从mov X,[rbp-Y]后面开始执行,把constraint作一个转换。

[[rbp-0x78]] == NULL && [[rbp-0x50]] == NULL --> r9 == 0 && rdx == 0.

利用第一个qadget满足这个限制.

怎样才可能用一个gadget满足多个限制?调用函数:

--> 写脚本暴力搜索libc库函数,可以得到每一个onegadget对应的twogadget可能的结果:



two-gadget真是非常多.

思考: 有没有更高级的方法去搜索two-gadget,three gadget, X-gadget以及其他constraint下的gadgets? 符号执行。

将gadget2要满足的constraint作为限制,搜索可能存在的gadget1.