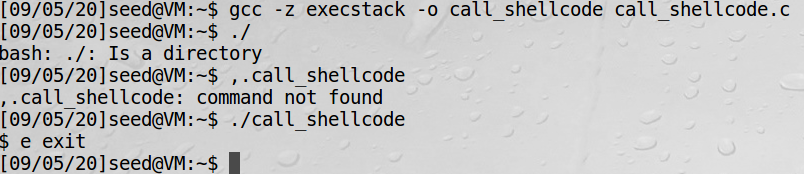
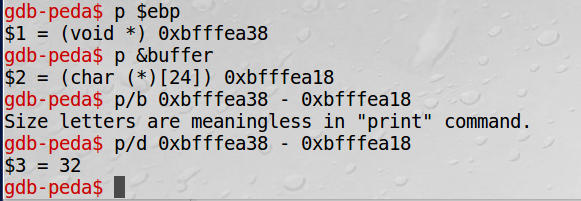
57118130 王嘉麟

Task1&2:



成功运行zsh,



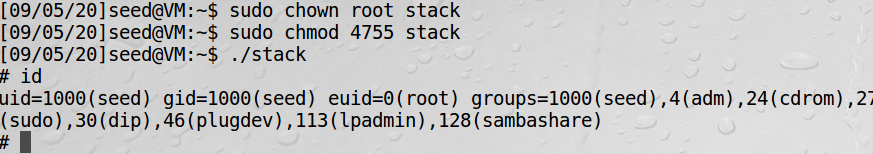
查看&ebp与buffer位置差值，得到return addresss位置 = 0xbfffea38 + 36 = 0xbfffea6e

将其赋值0xbfffea6e + 50 = 0xbfffeaa0

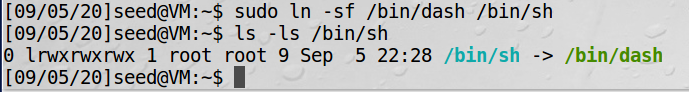
将值填入exploit.py中

ret = 0xbfffeaa0 # replace 0xAABBCCDD with the correct value

offset = 36 # replace 0 with the correct value

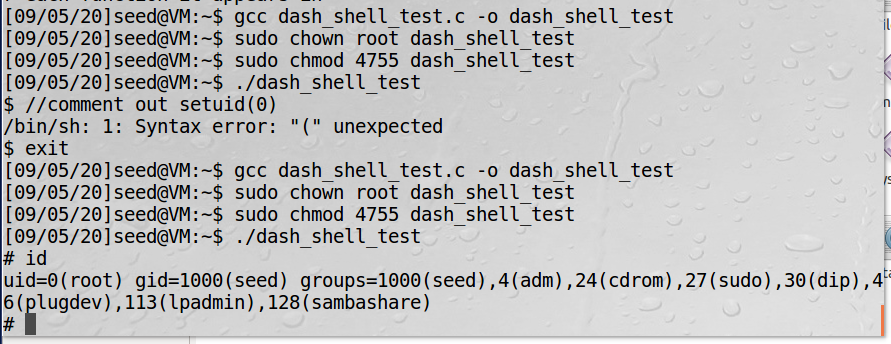


成功运行sh,得到root euid

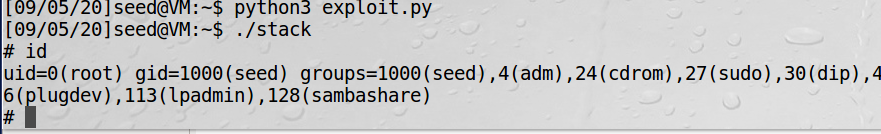


更改sh程序，使其指向之前的dash

Task3:

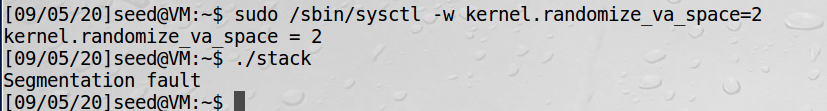


The second time gets the euid 0(root),The first time still 1000(seed),setuid(0) makes a difference.



Get root privilege in dash,obviously changed the ruid to 0

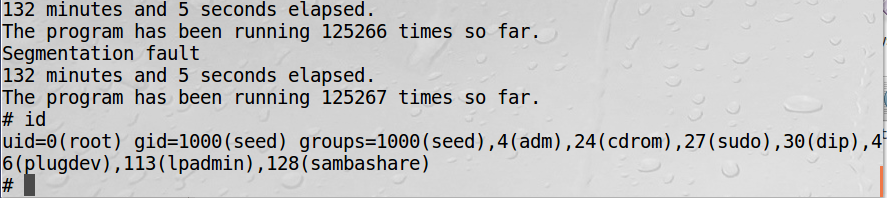
Task4:



Turn on address randomization and attack

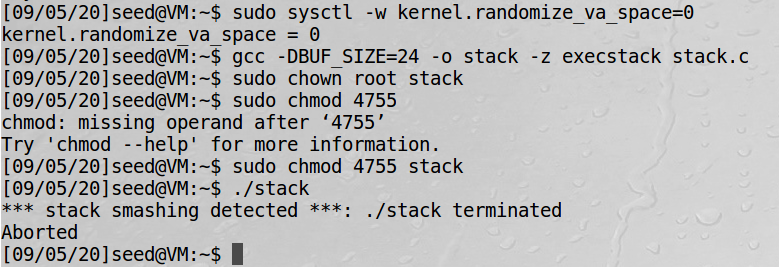
失败

执行手册上shell程序



125267times to get root

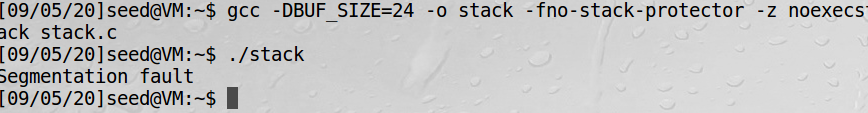
Task5:



检测到栈溢出，stack进程被终止

说明gcc的金丝雀机制有用

Task6:



明显不行，是因为虚拟硬件检测到stack中执行了shell命令，然后命令被制止，有机会我们可以去了解一下Return-to-lib攻击