Keeper

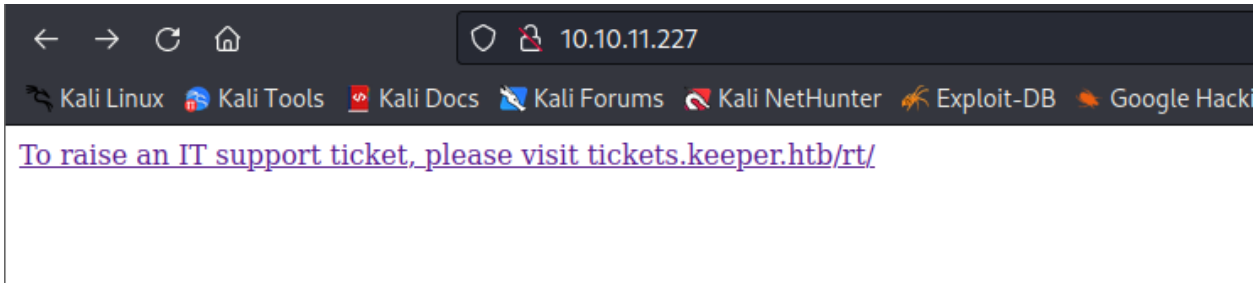
User Flag

Ater adding the target machine in /etc/hosts we conducted a NMAP scan.

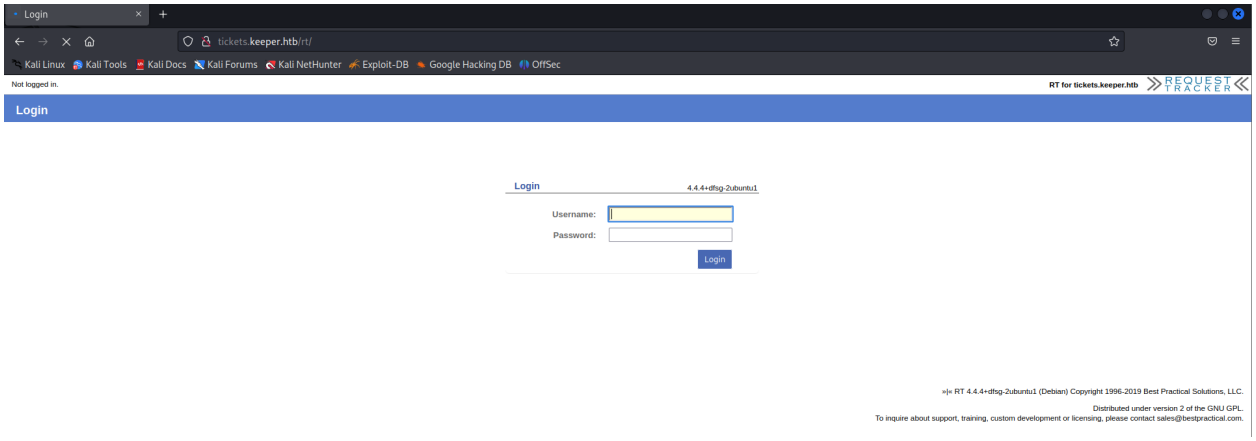
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.227 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-20 06:33 EDT
Stats: 0:02:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.67% done; ETC: 06:36 (0:00:31 remaining)
Stats: 0:04:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 94.28% done; ETC: 06:38 (0:00:17 remaining)
Nmap scan report for keeper.htb (10.10.11.227)
Host is up (0.28s latency).
Not shown: 997 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
9001/tcp open  http    SimpleHTTPServer 0.6 (Python 3.10.12)
|_http-title: Directory listing for /
|_http-server-header: SimpleHTTP/0.6 Python/3.10.12
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 394.47 seconds
```

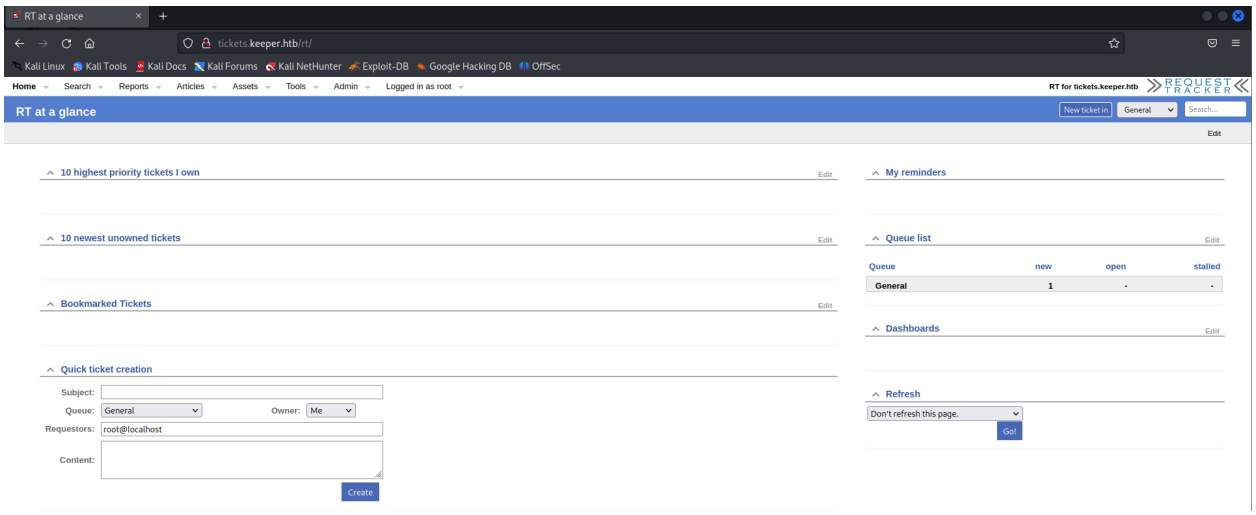
While accessing the IP over browser we got the following URL.



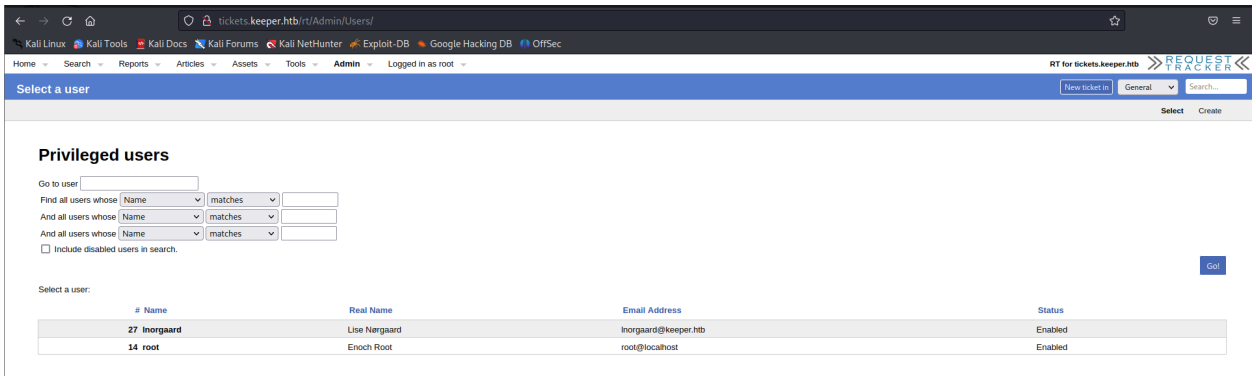
After adding this URL in the /etc/hosts file we tried to access the URL.



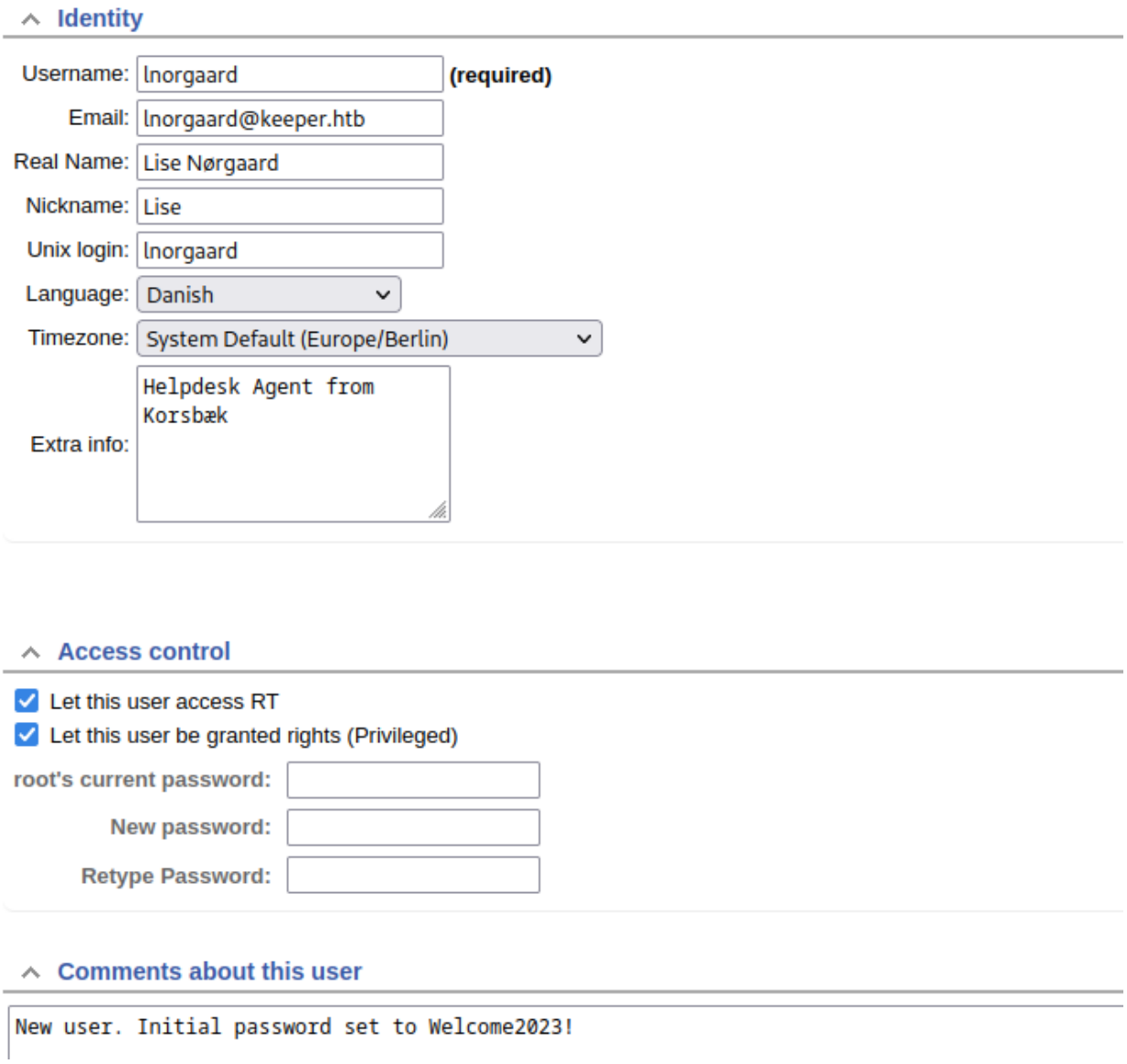
We tried to brute force the credentials manually and the following credential set worked.
root:password



Upon enumeration we found 2 users



While checking details for user lnorgaard we found an interesting comment.

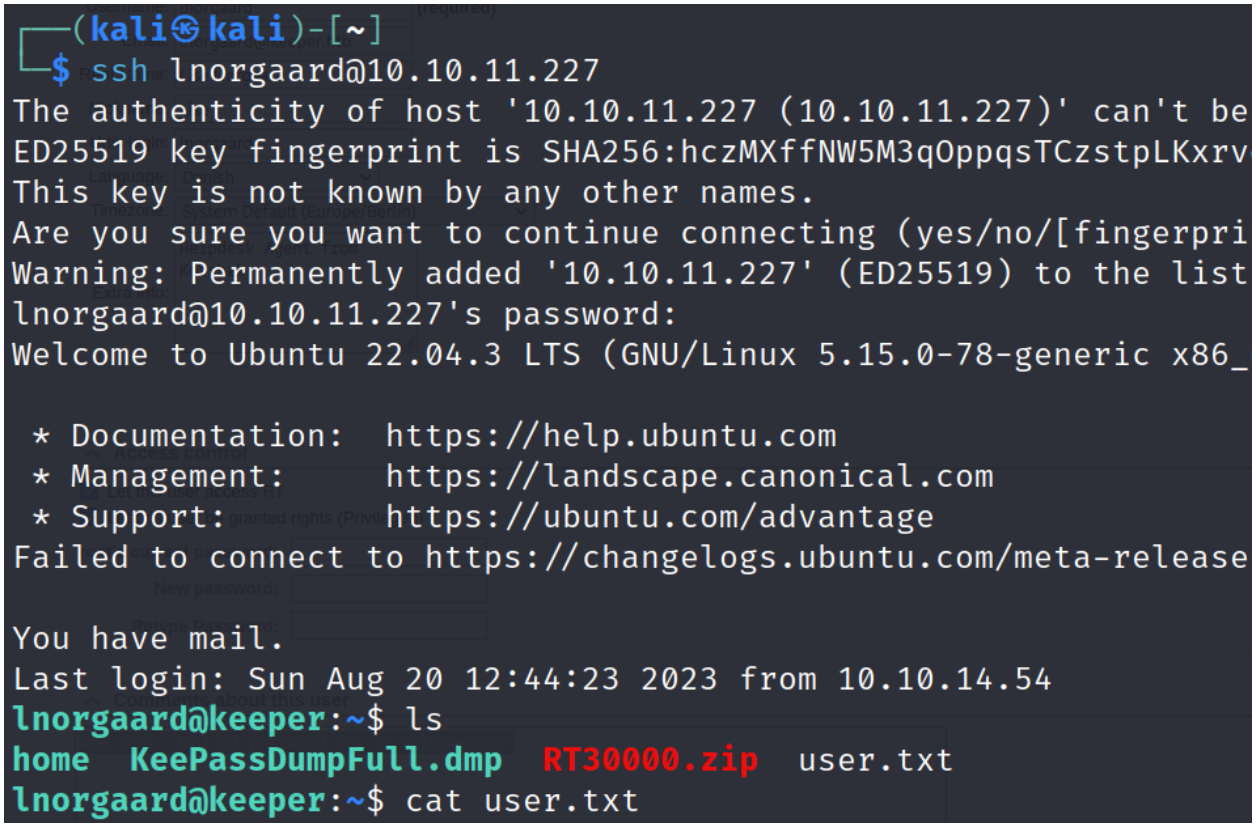


New user. Initial password set to Welcome2023!
So we have the username,password and the IP address.
Username: lnorgaard
Password: Welcome2023!
IP: 10.10.11.227

As per the nmap scan we say that ssh port is enabled.

So we have all the required information to connect the machine via ssh.

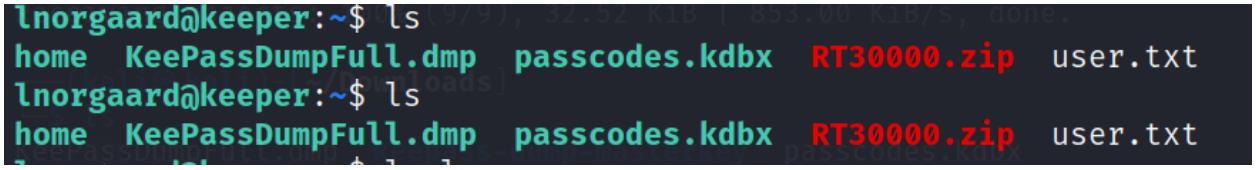
After connecting via ssh we got the user flag,



Root Flag

Here we have a RT30000.zip file. Let's unzip it.
To copy the files from remote to local machine we are using a web server.

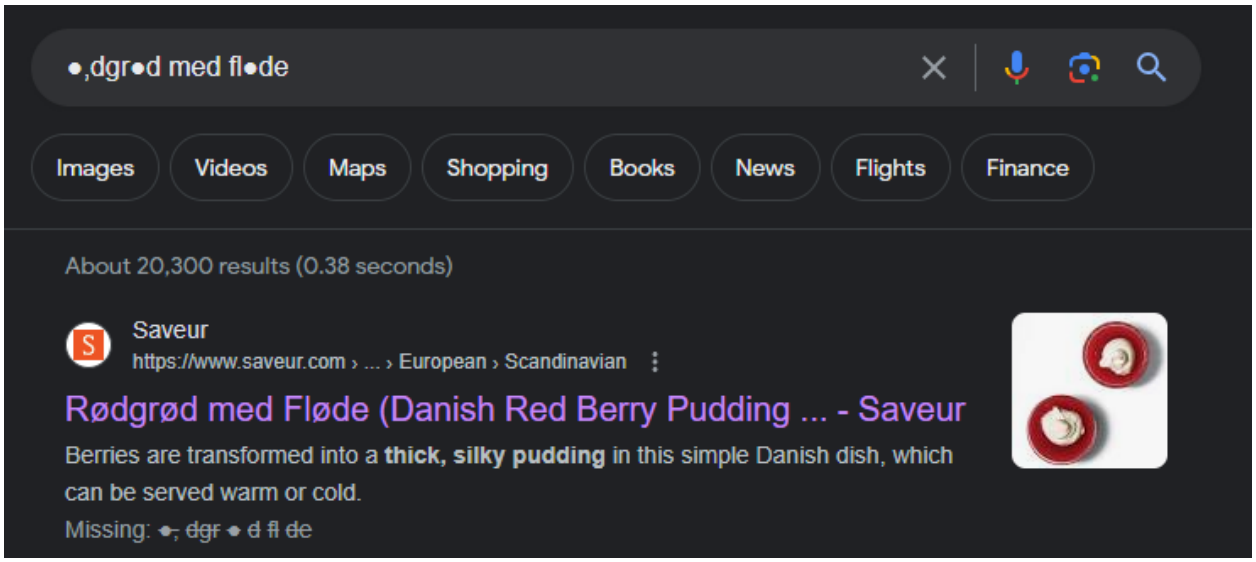
Looking at those files we found 2 interesting files.



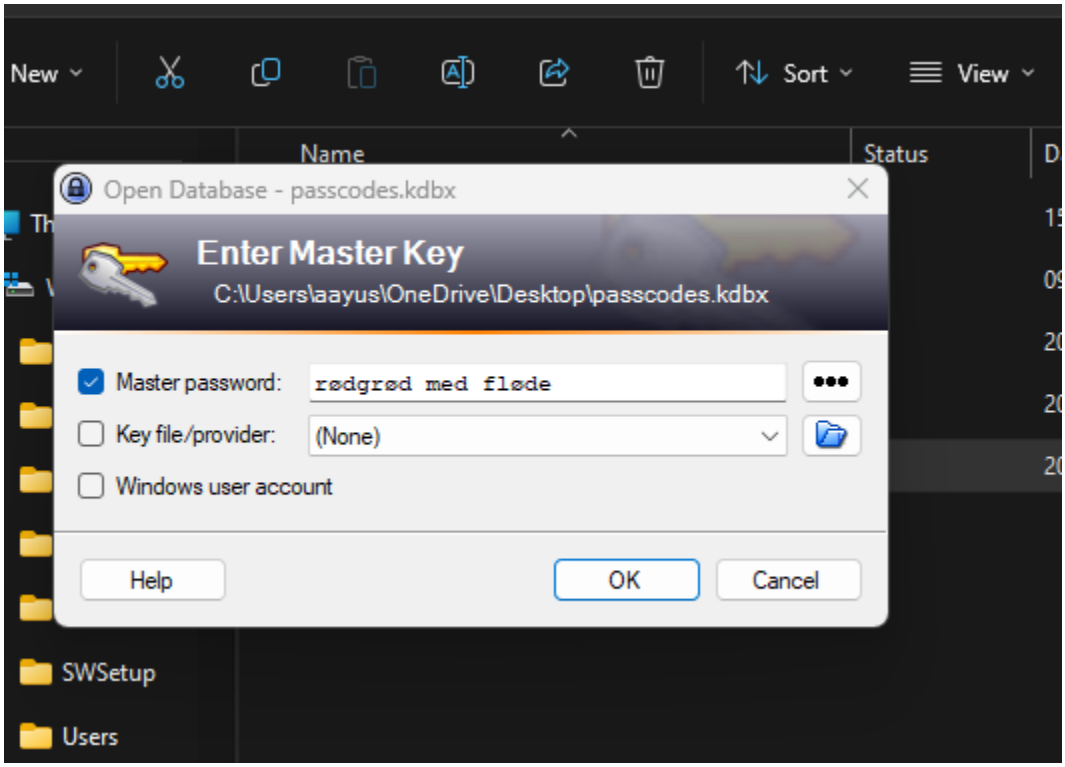
KeePassDumpFull.dmp
Passcodes.kdbx

Upon googling, I found these 2 URLs useful.

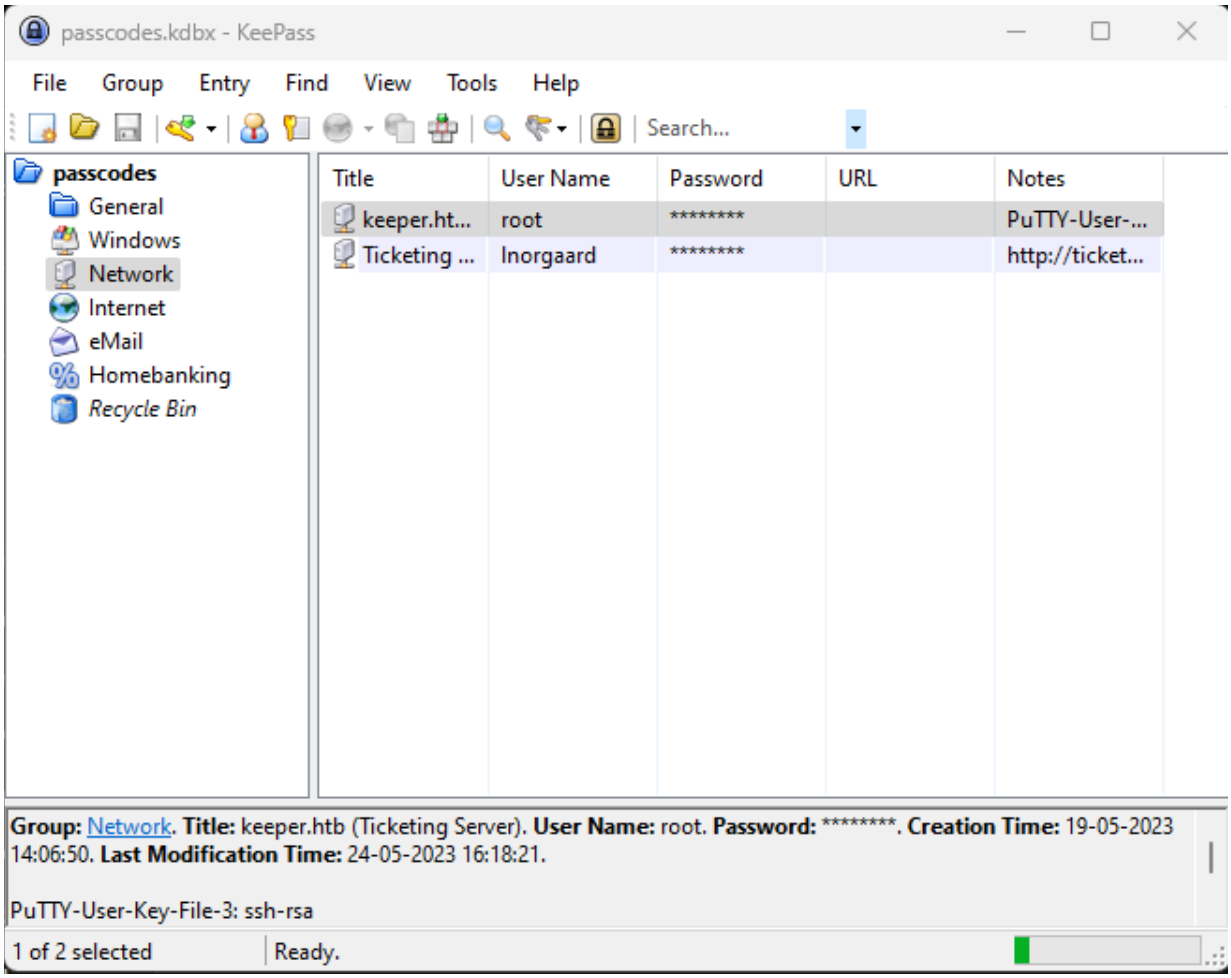
https://github.com/CMEPW/keepass-dump-masterkey
https://github.com/vdohney/keepass-password-dumper



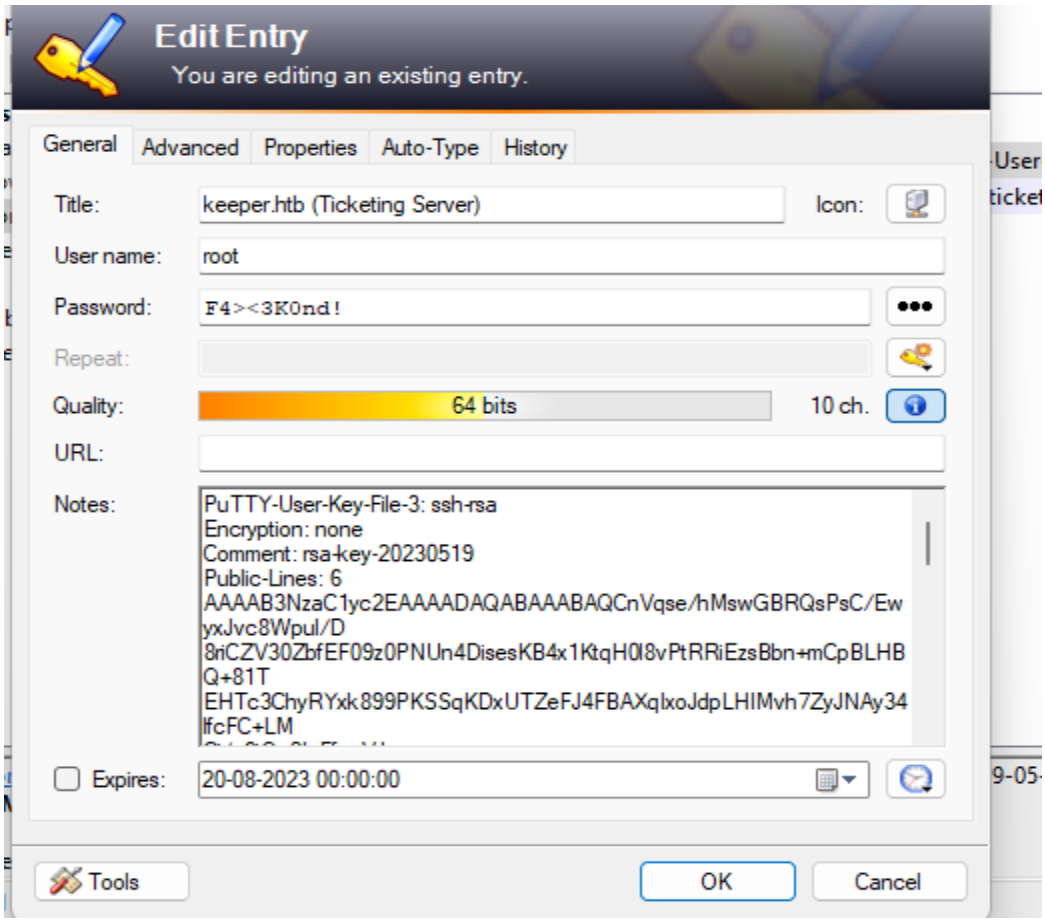
Master password: rødgrød med fløde



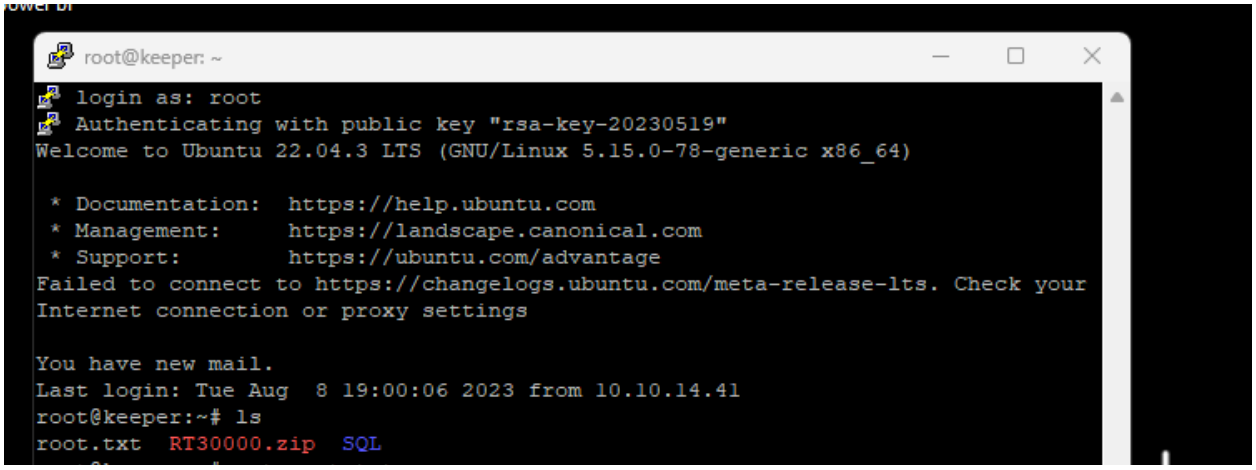
Using the master password we opened passcodes.kdbx in keepass application.



Below are the details for root.



Using putty we accessed the root over ssh and got the root flag.



Security Measures

1. Using secure credentials.
2. Set rate limit to reduce brute force.
3. Information Disclosure - Critical information like passwords should not be disclosed.
4. Critical files should not be accessed by normal users unless required.