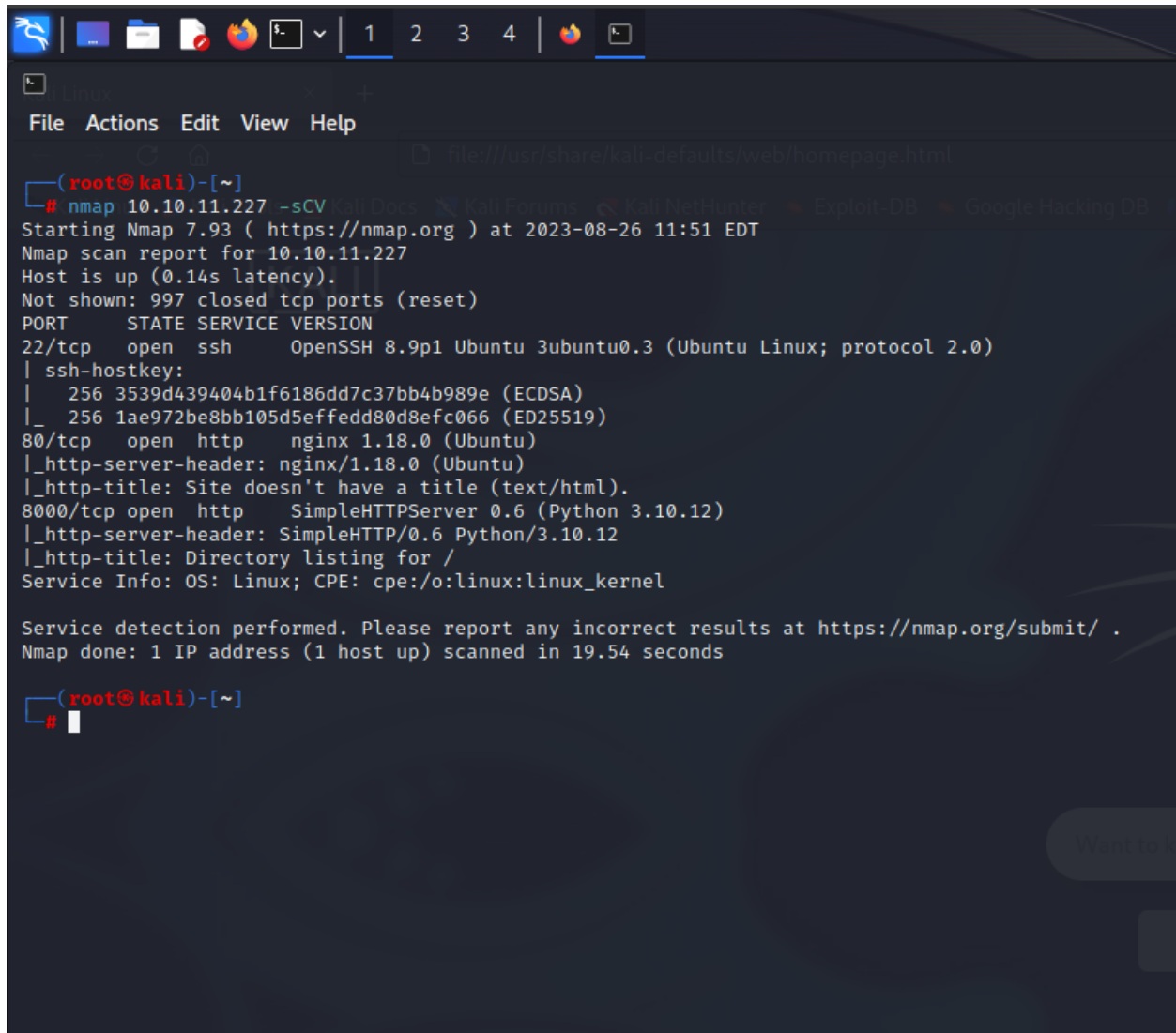


# Keeper

Start with nmap :-

**nmap [ IP ] -sCV**



```
(root@kali)-[~]
# nmap 10.10.11.227 -sCV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 11:51 EDT
Nmap scan report for 10.10.11.227
Host is up (0.14s latency).
Not shown: 997 closed tcp ports (reset)
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).
8000/tcp  open  http     SimpleHTTPServer 0.6 (Python 3.10.12)
|_ http-server-header: SimpleHTTP/0.6 Python/3.10.12
|_ http-title: Directory listing for /
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 19.54 seconds

(root@kali)-[~]
#
```

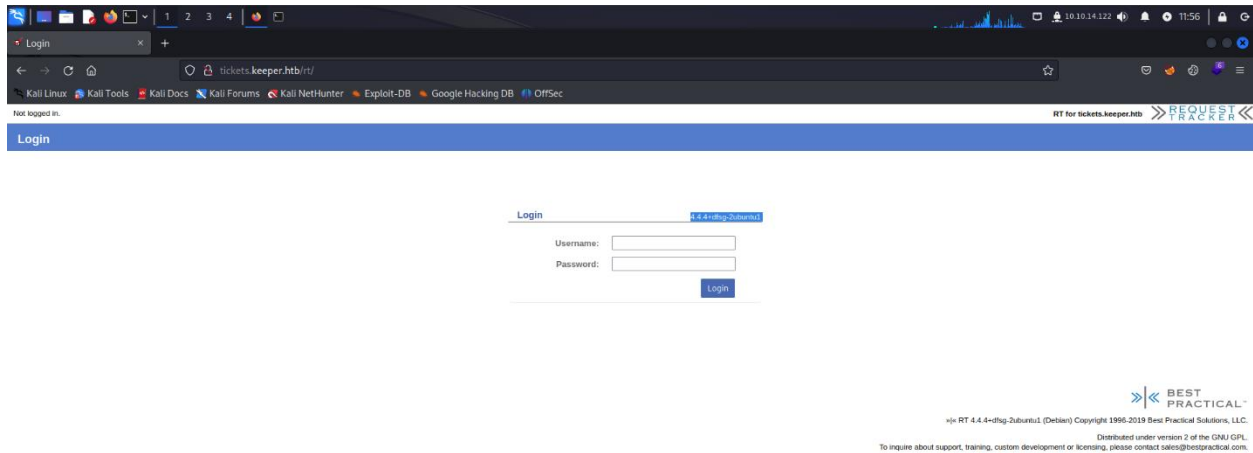
Found →

22/tcp open ssh

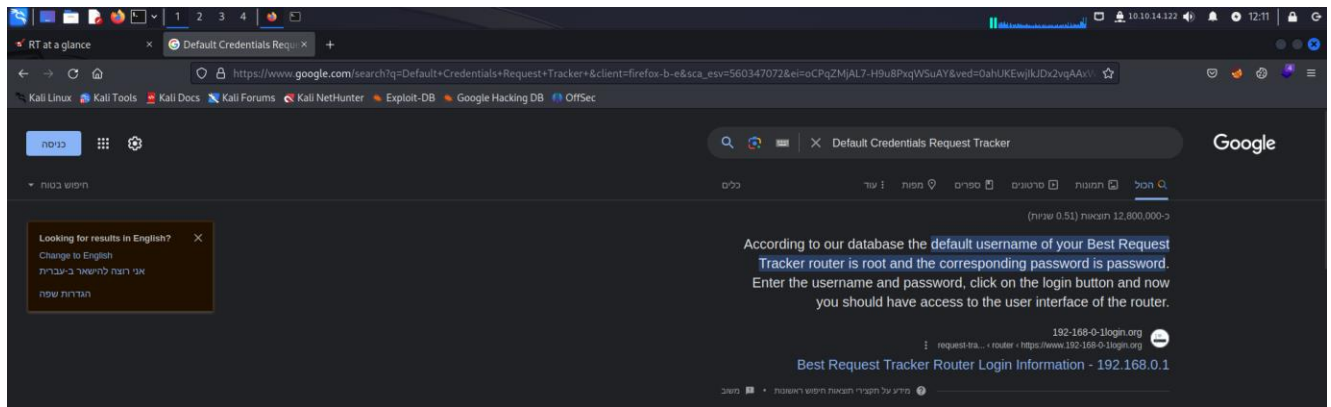
80/tcp open http nginx 1.18.0 (Ubuntu)

8000/tcp open http SimpleHTTPServer 0.6 (Python 3.10.12)

I don't find anything in port 8000 BUT in the port 80 I found this site >>



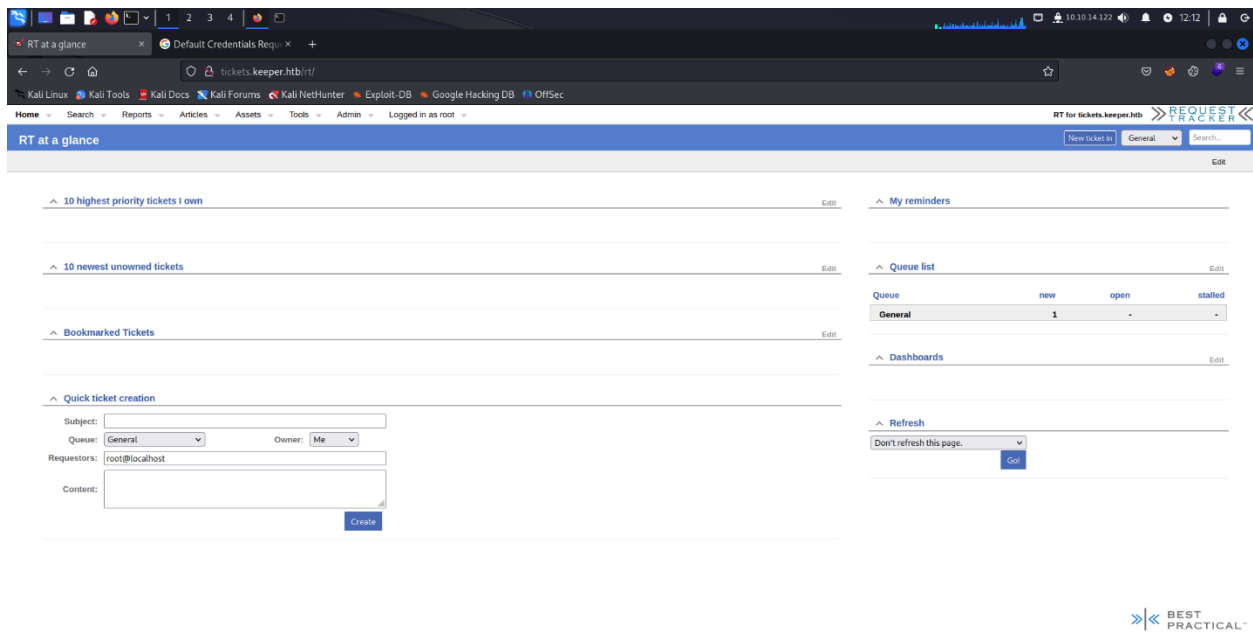
search for Default Credentials for the login page.



The Credential for the login page is >>

**Username** = root

**Password** = password

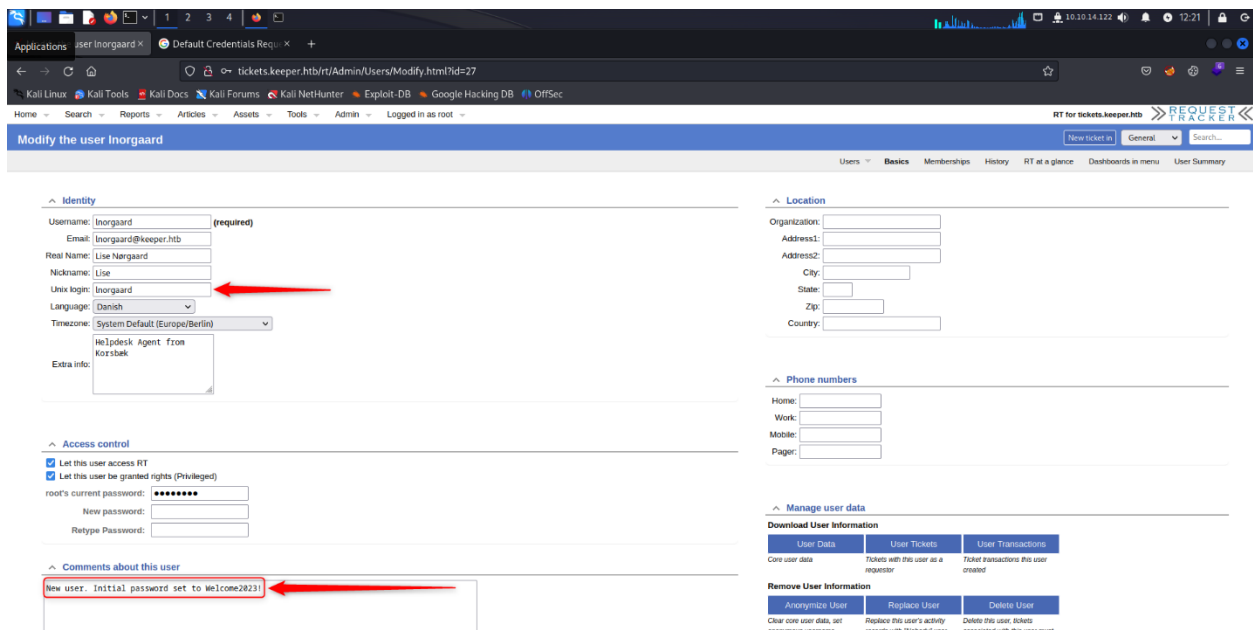


After I login to the site I saw an admin so I click on that and there is a user's page

There is 2 users there:

- 1- Lnorgaard
- 2- Root

Click in Lnorgaard and found this:



I have a comment telling me that the password is **Welcome2023!**

So, I used the name and this password to connect to the SSH.

```
lnorgaard@keeper: ~  
File Actions Edit View Help  
lnorgaard@keeper: ~ x root@kali: ~ x tickets.keeper.htb/r/Admin/Users/Modify.html?id=27  
[root@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: Sat Aug 26 18:39:32 2023 from 10.10.14.122  
lnorgaard@keeper:~$
```

User Flag →

```
lnorgaard@keeper: ~  
File Machine View Input Devices Help  
lnorgaard@keeper: ~ x root@kali: ~ x tickets.keeper.htb/r/Admin/Users/Modify.html?id=27  
[root@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: Sat Aug 26 18:39:32 2023 from 10.10.14.122  
lnorgaard@keeper:~$ ls  
KeePassDumpFull.dmp linpeas.sh passcodes.kdbx poc.py RT30000.zip tmp user.txt  
lnorgaard@keeper:~$ cat user.txt  
lnorgaard@keeper:~$
```

## Privilege to root:

Now we need the root flag.

we have a zip file we use unzip for the file and there is 2 files in the zip file

1 with **kdbx** format and the other **dmp** format.

After that I search for a KeePass vulnerability to read the KeePassDumpFull.dmp.

I found this **CVE-2023-32784**

And a tools to help us read the file.

<https://github.com/CMEPW/keepass-dump-masterkey>

A screenshot of a Kali Linux terminal window. The terminal shows the execution of the 'keePass-dump-masterkey' tool. The user 'lnorgaard@keeper:~' runs the command 'keePass-dump-masterkey poc.py RT10000.zip tmp user.txt'. The tool outputs its usage, positional arguments, and options. It then generates a list of possible passwords, all of which are 'ldgrd med fl0de'. The terminal window has a dark theme and a title bar indicating the user is 'lnorgaard@keeper: -'.

this tool give me a password.

After I search and try to know what the full password is because in the tool it is not complete and clear

In the end I found that the password is Rødgrød med fløde

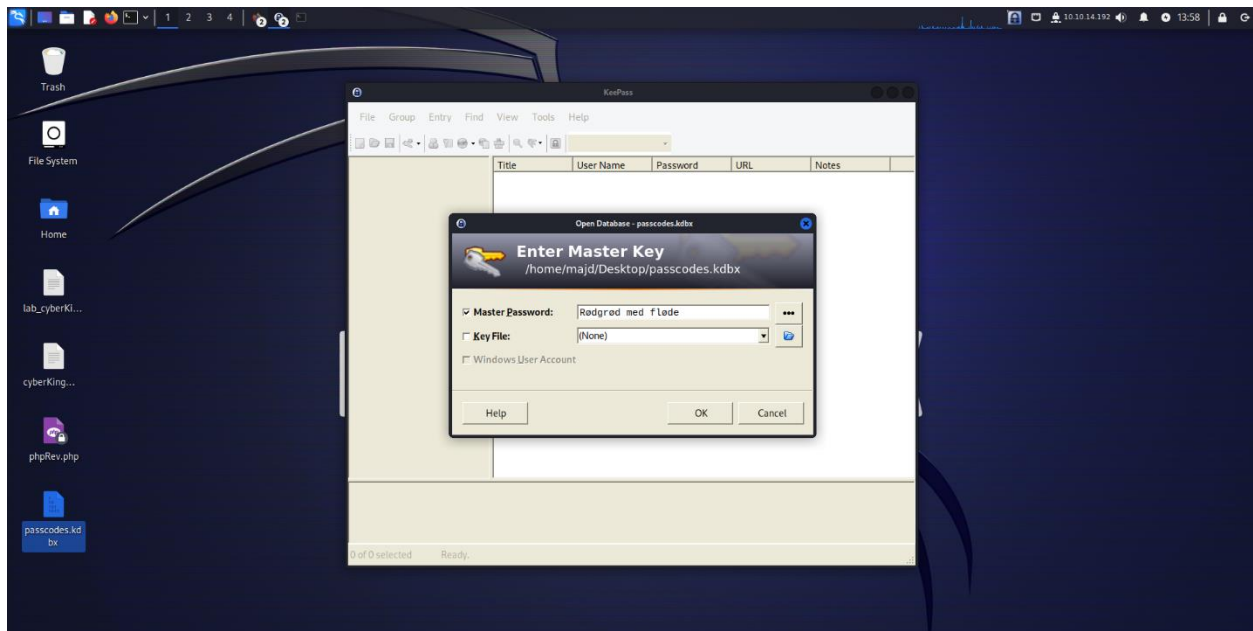
Now I need to read the kdbx file, so I install the KeePass tool:

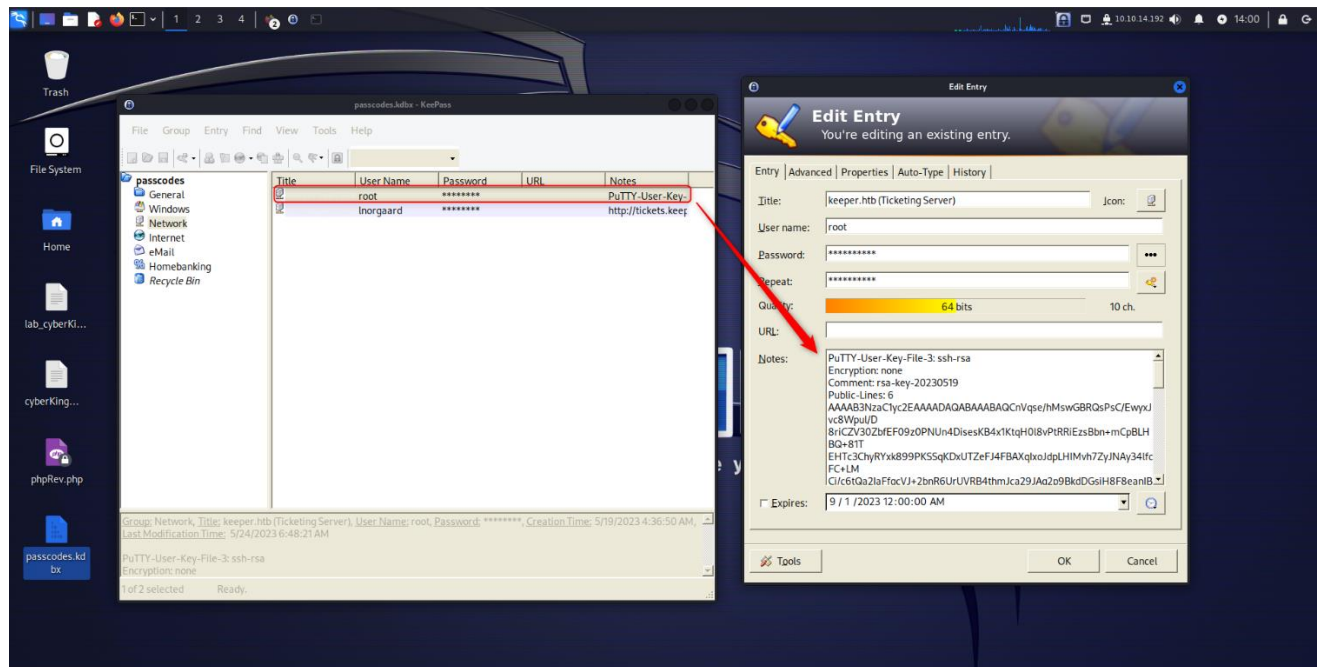
**Sudo apt install keepass2**

```
root@kali: ~  
File Actions Edit View Help  
[root@kali: ~]#  
# sudo apt install keepass2  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  gccgo-12 libgo-12-dev libgo21  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  binfmt-support ca-certificates-mono cli-common libgdiplus libmono-accessibility4.0-cil libmono-btls-interface4.0-cil libmono-corlib4.5-cil libmono-corlib4.5-dll libmono-i18n-west4.0-cil libmono-i18n4.0-cil libmono-posix4.0-cil  
  libmono-security4.0-cil libmono-system-configuration4.0-cil libmono-system-core4.0-cil libmono-system-data4.0-cil libmono-system-drawing4.0-cil libmono-system-enterpriseservices4.0-cil libmono-system-numerics4.0-cil  
  libmono-system-runtime-serialization-formatters-soap4.0-cil libmono-system-security4.0-cil libmono-system-transactions4.0-cil libmono-system-windows-forms4.0-cil libmono-system-xml4.0-cil libmono-system4.0-cil  
  libmono-webbrowser4.0-cil libmono-websockets4.0-cil mono-gac mono-gac-mono-runtime mono-runtime-common mono-runtime-sgen xsel  
Suggested packages:  
  keepass2-doc mono-mcs libmono-i18n4.0-all libnoneui-0 libgamin0  
Recommended packages:  
  libguezilla  
The following NEW packages will be installed:  
  binfmt-support ca-certificates-mono cli-common keepass2 libgdiplus libmono-accessibility4.0-cil libmono-btls-interface4.0-cil libmono-corlib4.5-cil libmono-corlib4.5-dll libmono-i18n-west4.0-cil libmono-i18n4.0-cil  
  libmono-posix4.0-cil libmono-security4.0-cil libmono-system-configuration4.0-cil libmono-system-core4.0-cil libmono-system-data4.0-cil libmono-system-drawing4.0-cil libmono-system-enterpriseservices4.0-cil  
  libmono-system-numerics4.0-cil libmono-system-runtime-serialization-formatters-soap4.0-cil libmono-system-security4.0-cil libmono-system-transactions4.0-cil libmono-system-windows-forms4.0-cil libmono-system-xml4.0-cil  
  libmono-system4.0-cil libmono-webbrowser4.0-cil libmono-websockets4.0-cil mono-gac mono-gac-mono-runtime mono-runtime-common mono-runtime-sgen xsel  
0 upgraded, 32 newly installed, 0 to remove and 730 not upgraded.  
Need to get 10.3 MB of archives.  
After this operation, 34.7 MB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://kali.download/kali kali-rolling/main amd64 binfmt-support amd64 2.2.2-2 [64.0 kB]  
Get:2 http://kali.org/kali kali-rolling/main amd64 mono-runtime-common amd64 6.8.0.105+dfsg-3.3 [1,171 kB]  
Get:3 http://kali.org/kali kali-rolling/main amd64 libmono-corlib4.5-dll all 6.8.0.105+dfsg-3.3 [1,253 kB]  
Get:4 http://kali.org/kali kali-rolling/main amd64 libmono-system-core4.0-cil all 6.8.0.105+dfsg-3.3 [305 kB]  
Get:5 http://kali.org/kali kali-rolling/main amd64 libmono-system-numerics4.0-cil all 6.8.0.105+dfsg-3.3 [51.0 kB]  
Get:6 http://kali.org/kali kali-rolling/main amd64 libmono-system-xml4.0-cil all 6.8.0.105+dfsg-3.3 [588 kB]  
Get:7 http://kali.org/kali kali-rolling/main amd64 libmono-system-security4.0-cil all 6.8.0.105+dfsg-3.3 [116 kB]  
Get:8 http://kali.org/kali kali-rolling/main amd64 libmono-system-configuration4.0-cil all 6.8.0.105+dfsg-3.3 [57.2 kB]  
Get:9 http://kali.org/kali kali-rolling/main amd64 libmono-system4.0-cil all 6.8.0.105+dfsg-3.3 [800 kB]  
Get:10 http://kali.org/kali kali-rolling/main amd64 libmono-security4.0-cil all 6.8.0.105+dfsg-3.3 [97.5 kB]  
Get:11 http://kali.org/kali kali-rolling/main amd64 mono-4.0-gac all 6.8.0.105+dfsg-3.3 [156 kB]  
Get:12 http://kali.org/kali kali-rolling/main amd64 mono-gac all 6.8.0.105+dfsg-3.3 [12.2 kB]  
Get:13 http://kali.org/kali kali-rolling/main amd64 mono-runtime-sgen amd64 6.8.0.105+dfsg-3.3 [1,703 kB]  
Get:14 http://kali.org/kali kali-rolling/main amd64 mono-runtime amd64 6.8.0.105+dfsg-3.3 [17.0 kB]  
Get:15 http://kali.org/kali kali-rolling/main amd64 libmono-corlib4.5-cil all 6.8.0.105+dfsg-3.3 [15.3 kB]  
Get:16 http://kali.org/kali kali-rolling/main amd64 ca-certificates-mono all 6.8.0.105+dfsg-3.3 [20.3 kB]  
Get:17 http://kali.org/kali kali-rolling/main amd64 cli-common all 0.10+mmul [180 kB]  
Get:18 http://kali.org/kali kali-rolling/main amd64 libgdiplus amd64 6.1+dfsg-1+b1 [162 kB]  
Get:19 http://kali.org/kali kali-rolling/main amd64 libmono-system-drawing4.0-cil all 6.8.0.105+dfsg-3.3 [152 kB]  
Get:20 http://kali.org/kali kali-rolling/main amd64 libmono-accessibility4.0-cil all 6.8.0.105+dfsg-3.3 [18.1 kB]  
Get:21 http://kali.org/kali kali-rolling/main amd64 libmono-posix4.0-cil all 6.8.0.105+dfsg-3.3 [84.6 kB]  
Get:22 http://kali.org/kali kali-rolling/main amd64 libmono-system-transactions4.0-cil all 6.8.0.105+dfsg-3.3 [26.1 kB]  
Get:23 http://kali.org/kali kali-rolling/main amd64 libmono-system-enterpriseservices4.0-cil all 6.8.0.105+dfsg-3.3 [29.3 kB]  
Get:24 http://kali.org/kali kali-rolling/main amd64 libmono-system-data4.0-cil all 6.8.0.105+dfsg-3.3 [581 kB]  
Get:25 http://kali.org/kali kali-rolling/main amd64 libmono-system-runtime-serialization-formatters-soap4.0-cil all 6.8.0.105+dfsg-3.3 [29.3 kB]  
Get:26 http://kali.org/kali kali-rolling/main amd64 libmono-webbrowser4.0-cil all 6.8.0.105+dfsg-3.3 [40.7 kB]
```

I open the tool and open the file but we need a password to open the file and we have the password.

I type **Rødgrød med fløde** did not work so I type **rødgrød med fløde**





Here we have a key.

I save this in a keeper.ppk [ ppk it is the format of the PuTTY ]

So if I need to use that in ssh I need to transfer the format to pem format.

Here I used the puttygen tool >>> **puttygen keeper.ppk -O private-openssh -o keeper1.pem**

After this I used the file to connect to the root user using SSH.

ROOT FLAG



## Root Flag →

```
(root@kali)~# ssh root@10.10.11.227 -i keeper1.pem
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: Fri Sep  1 20:11:14 2023 from 10.10.14.158
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~# cat root.txt
root@keeper:~#
```

Majd Abuleil

