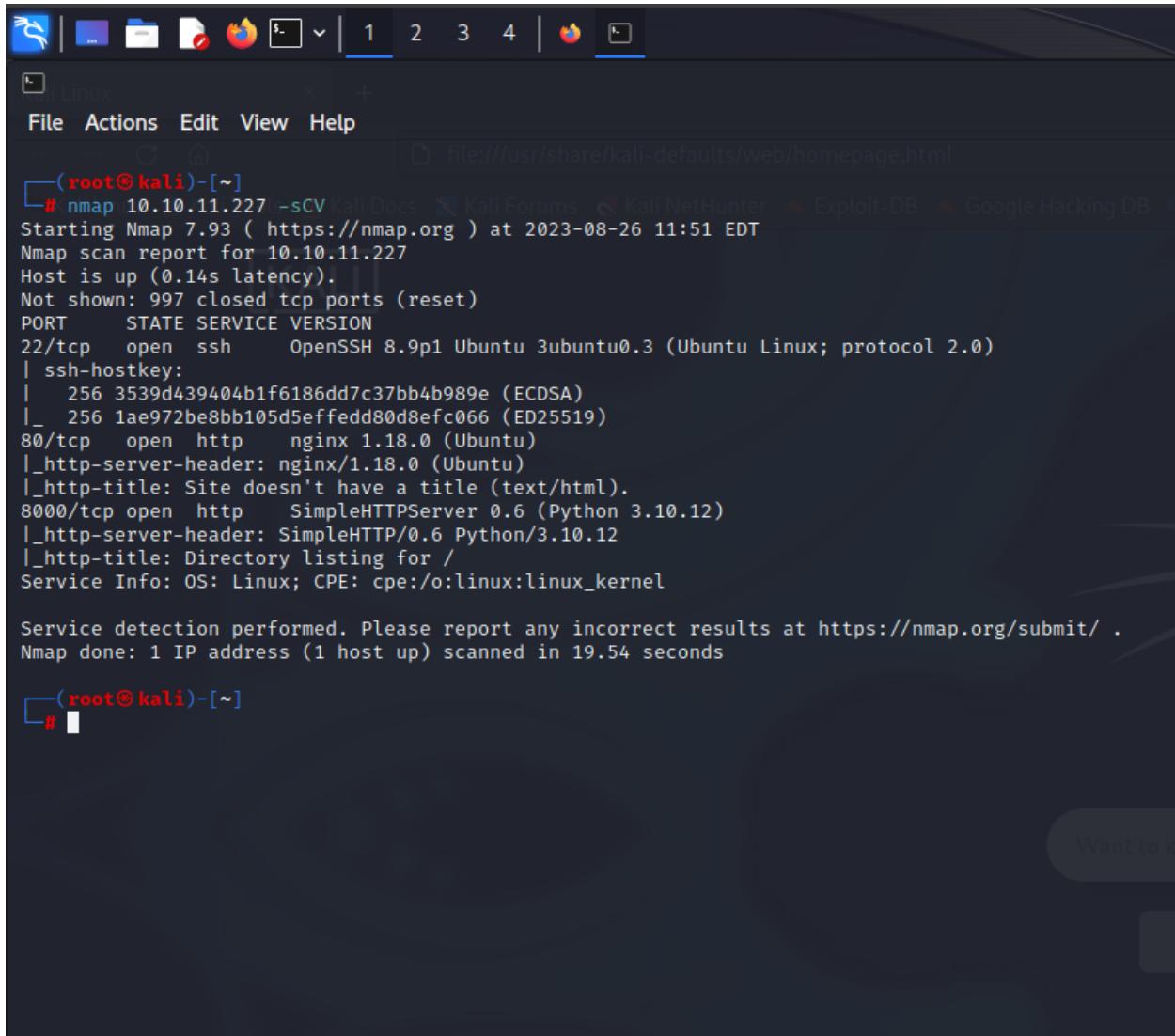


Keeper

Start with nmap :-

nmap [IP] -sCV



The screenshot shows a terminal window titled 'Linux' with several tabs open at the top. The active tab displays the output of an nmap scan. The command used was '# nmap 10.10.11.227 -sCV'. The output shows the host is up with 0.14s latency. It lists three open ports: 22/tcp (ssh), 80/tcp (http), and 8000/tcp (SimpleHTTPServer). The ssh service is identified as OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0) with an ECDSA key. The http service is nginx 1.18.0 (Ubuntu) running on ECDSA key 256. The SimpleHTTPServer service is Python 3.10.12. Service detection also found a directory listing for the root directory. The entire session is run as root ('root@kali:[~]').

```
(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).

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

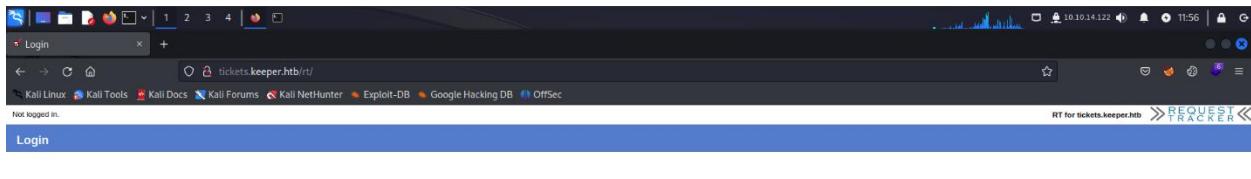
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds


```

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 >>



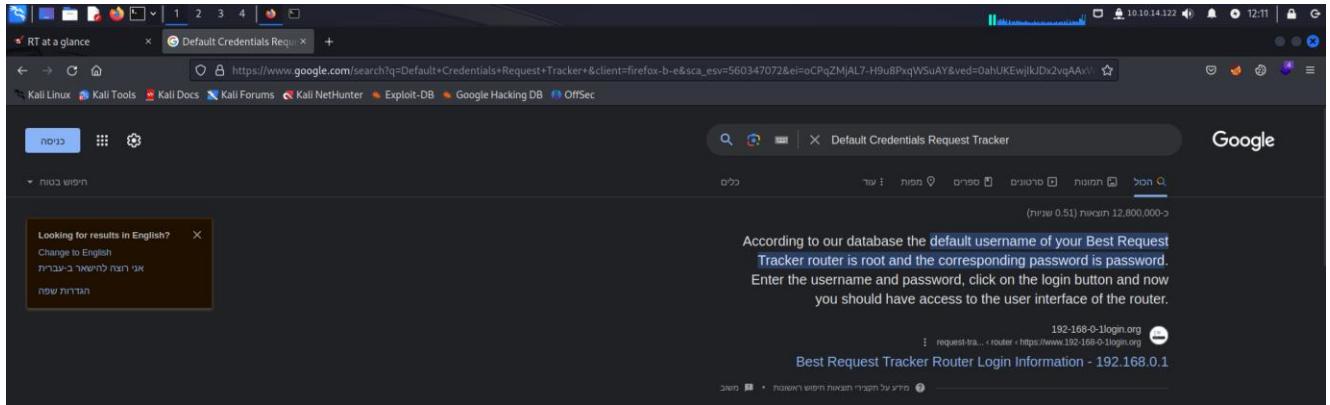
Login

Username:

Password:

RT 4.4.4-dtsq-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.

search for Default Credentials for the login page.



The Credential for the login page is >>

Username = root

Password = password

The screenshot shows the RT at a glance page. It displays several sections:

- 10 highest priority tickets I own**
- 10 newest unowned tickets**
- Bookmarked Tickets**
- Quick ticket creation**: A form with fields for Subject, Queue (General), Owner (Me), Requestors (root@localhost), and Content, with a "Create" button.
- My reminders**
- Queue list**: A table showing a single item in the General queue under the new column.
- Dashboards**
- Refresh**: A section with a dropdown menu and a "Go!" button.

At the bottom right, there is a "BEST PRACTICAL" logo.

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:

The screenshot shows the "Modify the user Lnorgaard" page. The user details are as follows:

Username: lnorgaard	(required)
Email: lnorgaard@keeper.hbt	
Real Name: Lise Norgaard	
Nickname: Lise	
Unix login: lnorgaard	<input type="text"/>
Language: Danish	
Timezone: System Default (Europe/Berlin)	
Extra info: Helpdesk Agent from Korsbæk	

Access control settings:

- Let this user access RT
- Let this user be granted rights (Privileged)

Root's current password: (redacted)

New password:

Retype Password:

Comments about this user:

New user. Initial password set to Welcome2023!

Location fields (empty):

Organization: <input type="text"/>
Address1: <input type="text"/>
Address2: <input type="text"/>
City: <input type="text"/>
State: <input type="text"/>
Zip: <input type="text"/>
Country: <input type="text"/>

Phone numbers (empty):

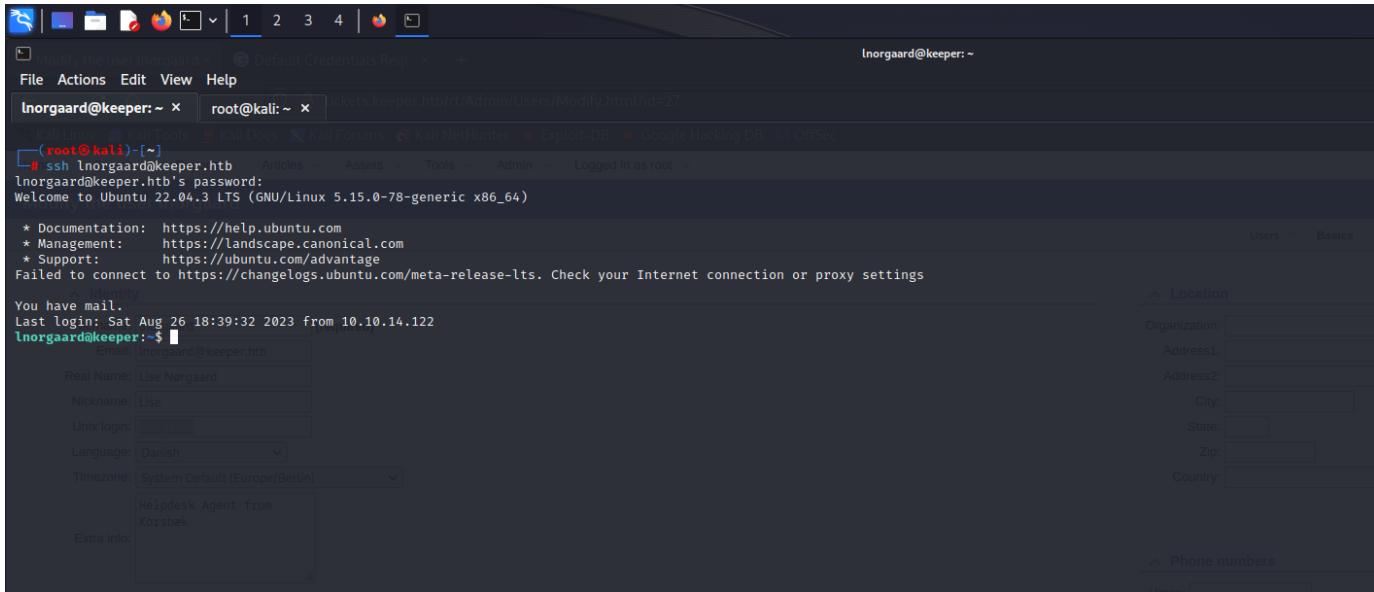
Home: <input type="text"/>
Work: <input type="text"/>
Mobile: <input type="text"/>
Pager: <input type="text"/>

Manage user data:

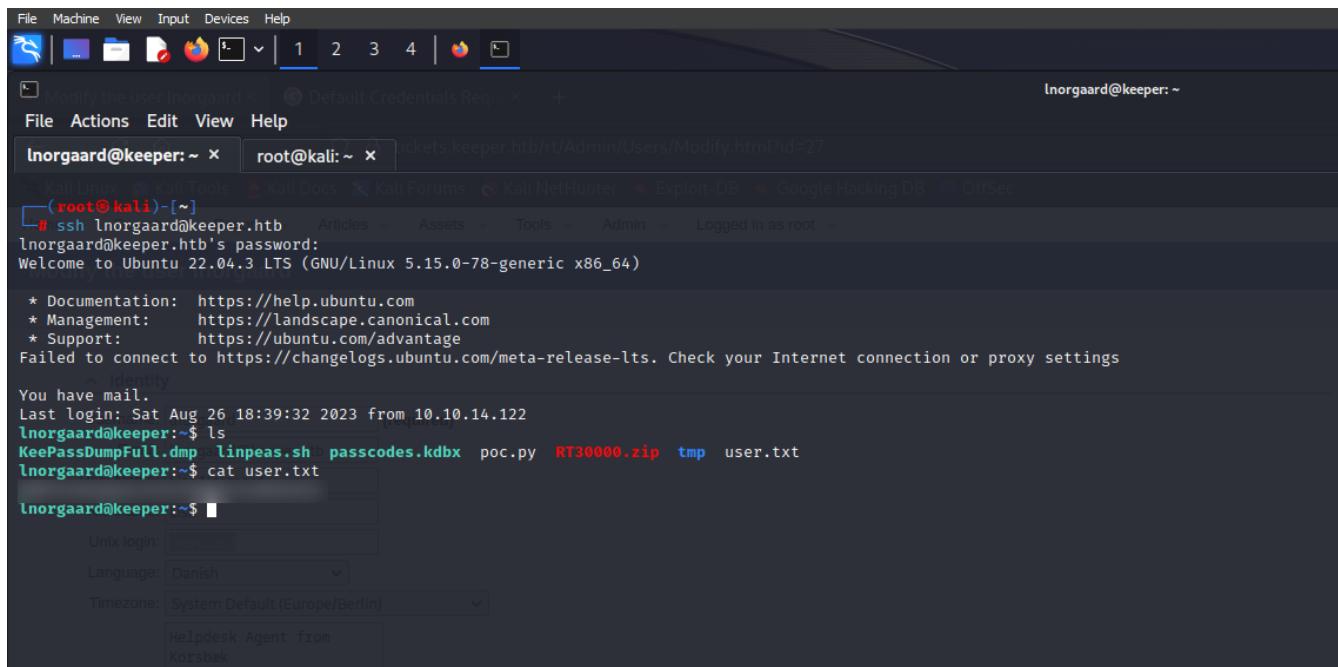
- Download User Information: User Data, User Tickets, User Transactions
- Core user data: Tickets with this user as a requester
- Ticket Transactions this user created
- Remove User Information: Anonymize User, Replace User, Delete User
- Clear core user data, set anonymous username: Replace this user's activity records with "Nobody" user
- Delete this user, tickets associated with this user must

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

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



User Flag →



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>

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

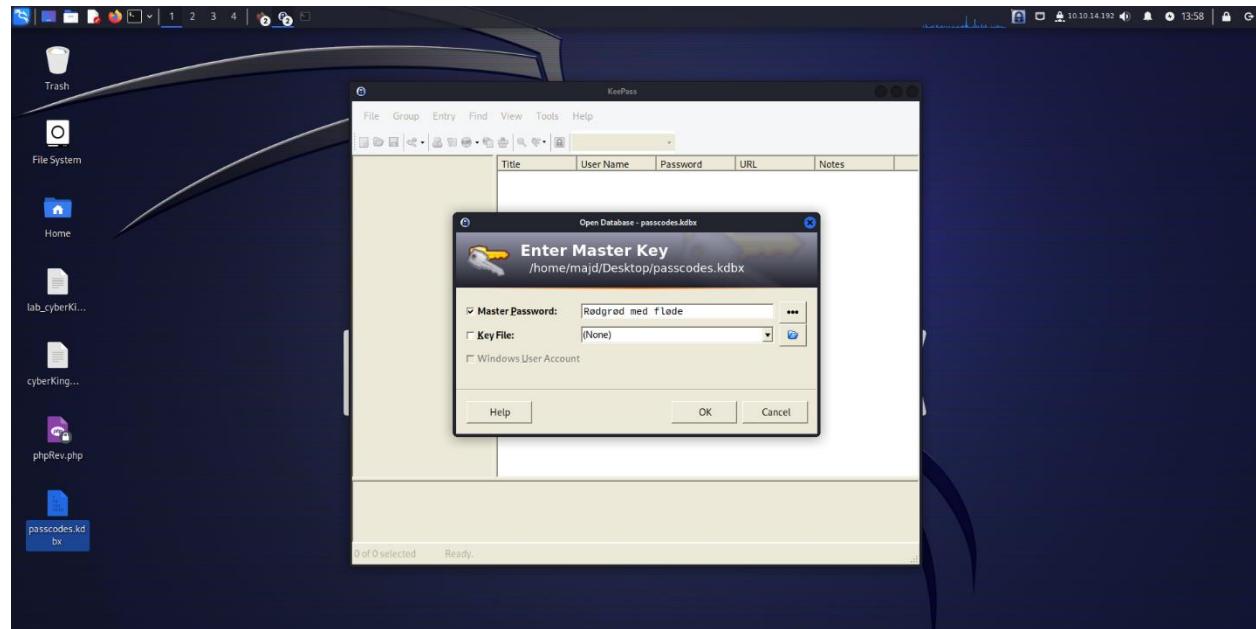
Now I need to read the kdbx file, so I install the KeePass tool:

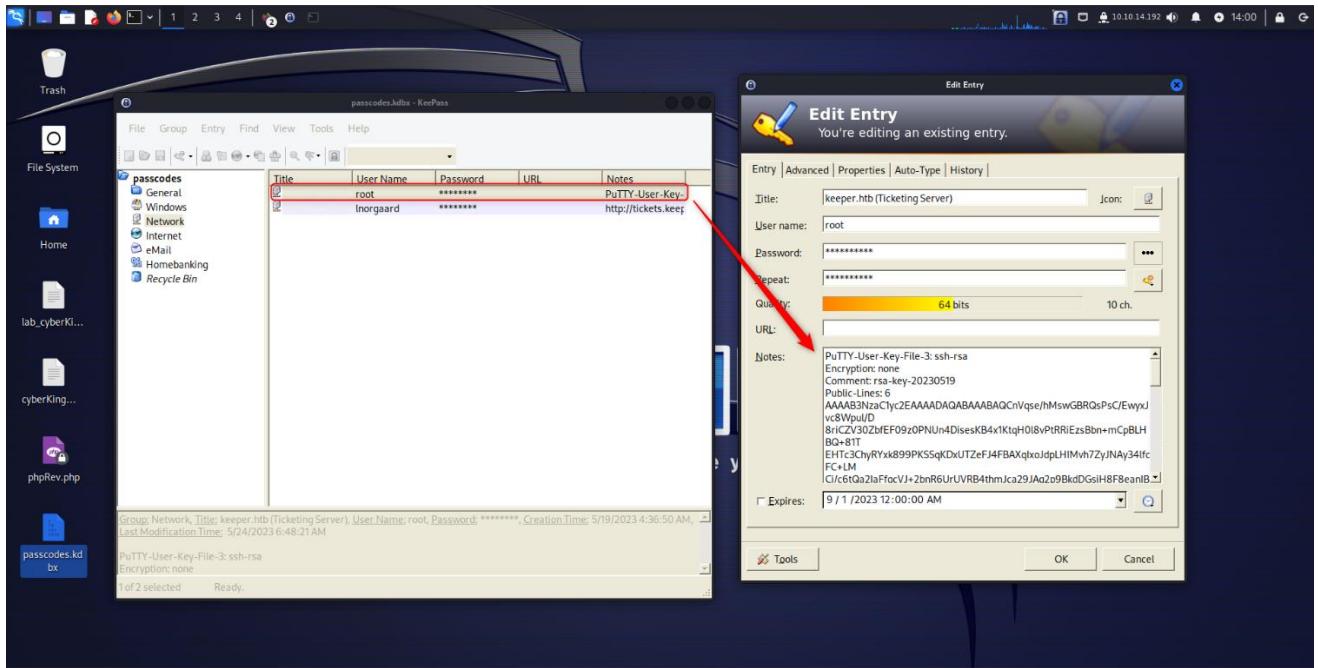
Sudo apt install keepass2

```
root@kali:~# 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 liblzo2-dev liblzo2
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  binfmt-support ca-certificates-mono cli-common libgdplus 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-xm4.0-cil libmono-system4.0-cil
Suggested packages:
  keepass2-doc mono-dmcslibmono-i18n4.0-all libgmenui-1 libgmenu0
Recommended packages:
  libbluez
The following NEW packages will be installed:
  binfmt-support ca-certificates-mono cli-common keepass2 libgdplus 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-xm4.0-cil libmono-system4.0-cil libmono-webbrowser4.0-cil mono-4.0-gac mono-gac mono-runtime mono-runtime-common mono-runtime-sgen xsel
0 upgraded, 0 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+1 [64.0 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libmono-accessibility4.0-cil 6.8.0.105+dfsg-3.3 [1,171 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libmono-btls-interface4.0-cil 6.8.0.105+dfsg-3.3 [1,253 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libmono-corlib4.5-cil 6.8.0.105+dfsg-3.3 [305 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-configuration4.0-cil 6.8.0.105+dfsg-3.3 [51.0 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-core4.0-cil 6.8.0.105+dfsg-3.3 [818 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-data4.0-cil 6.8.0.105+dfsg-3.3 [116 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-drawing4.0-cil 6.8.0.105+dfsg-3.3 [57.2 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-enterpriseservices4.0-cil 6.8.0.105+dfsg-3.3 [895 kB]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-numerics4.0-cil 6.8.0.105+dfsg-3.3 [97.5 kB]
Get:11 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-security4.0-cil 6.8.0.105+dfsg-3.3 [156 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-transactions4.0-cil 6.8.0.105+dfsg-3.3 [1,031 kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 libmono-webbrowser4.0-cil 6.8.0.105+dfsg-3.3 [1,703 kB]
Get:14 http://http.kali.org/kali kali-rolling/main amd64 libmono-accessibility4.0-cil 6.8.0.105+dfsg-3.3 [17.0 kB]
Get:15 http://http.kali.org/kali kali-rolling/main amd64 libmono-btls-interface4.0-cil 6.8.0.105+dfsg-3.3 [15.3 kB]
Get:16 http://http.kali.org/kali kali-rolling/main amd64 libmono-corlib4.5-cil 6.8.0.105+dfsg-3.3 [20.3 kB]
Get:17 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-configuration4.0-cil 6.8.0.105+dfsg-3.3 [14.3 kB]
Get:18 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-core4.0-cil 6.8.0.105+dfsg-3.3 [162 kB]
Get:19 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-data4.0-cil 6.8.0.105+dfsg-3.3 [152 kB]
Get:20 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-drawing4.0-cil 6.8.0.105+dfsg-3.3 [18.1 kB]
Get:21 http://http.kali.org/kali kali-rolling/main amd64 libmono-posix4.0-cil 6.8.0.105+dfsg-3.3 [1,031 kB]
Get:22 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-enterpriseservices4.0-cil 6.8.0.105+dfsg-3.3 [26.1 kB]
Get:23 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-numerics4.0-cil 6.8.0.105+dfsg-3.3 [29.3 kB]
Get:24 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-runtime-serialization-formatters-soap4.0-cil 6.8.0.105+dfsg-3.3 [581 kB]
Get:25 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-windows-forms4.0-cil 6.8.0.105+dfsg-3.3 [29.3 kB]
Get:26 http://http.kali.org/kali kali-rolling/main amd64 libmono-webbrowser4.0-cil 6.8.0.105+dfsg-3.3 [68.7 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 privateOpenssh -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
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~# cat root.txt
root@keeper:~#
```

Majd Abuleil

