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:

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:
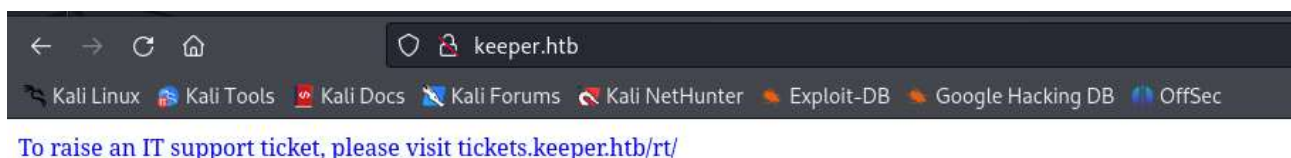

Picture 2 - Web application main page

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 Internet and I found the default credentials. I tried to use them in my target application and they worked.
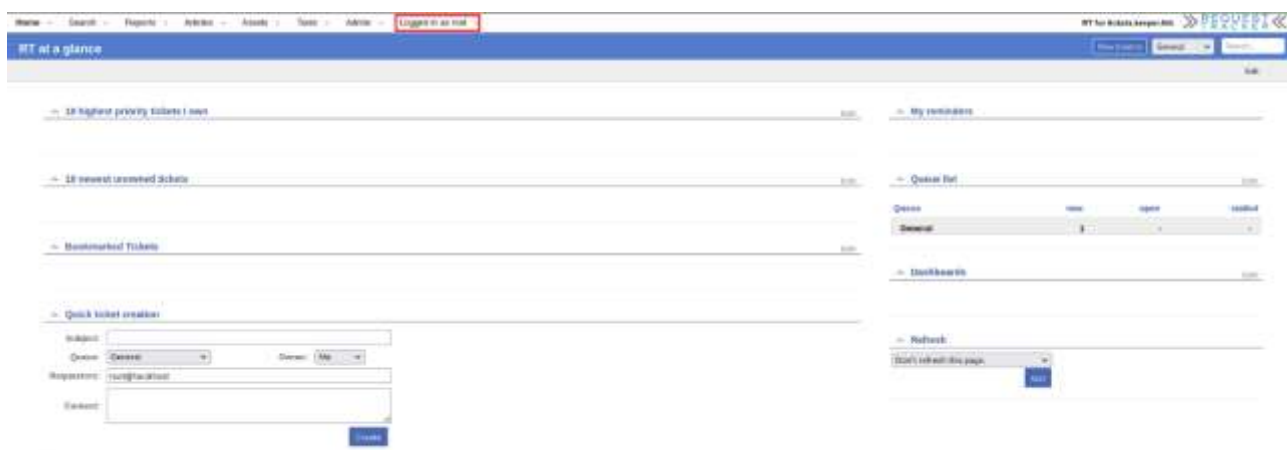
Picture 4 - Login successful

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

Picture 5 - User found

Specifically, when I found *lnorgaard* 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:

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 in 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:

Picture 9 - Exploiting KeePass

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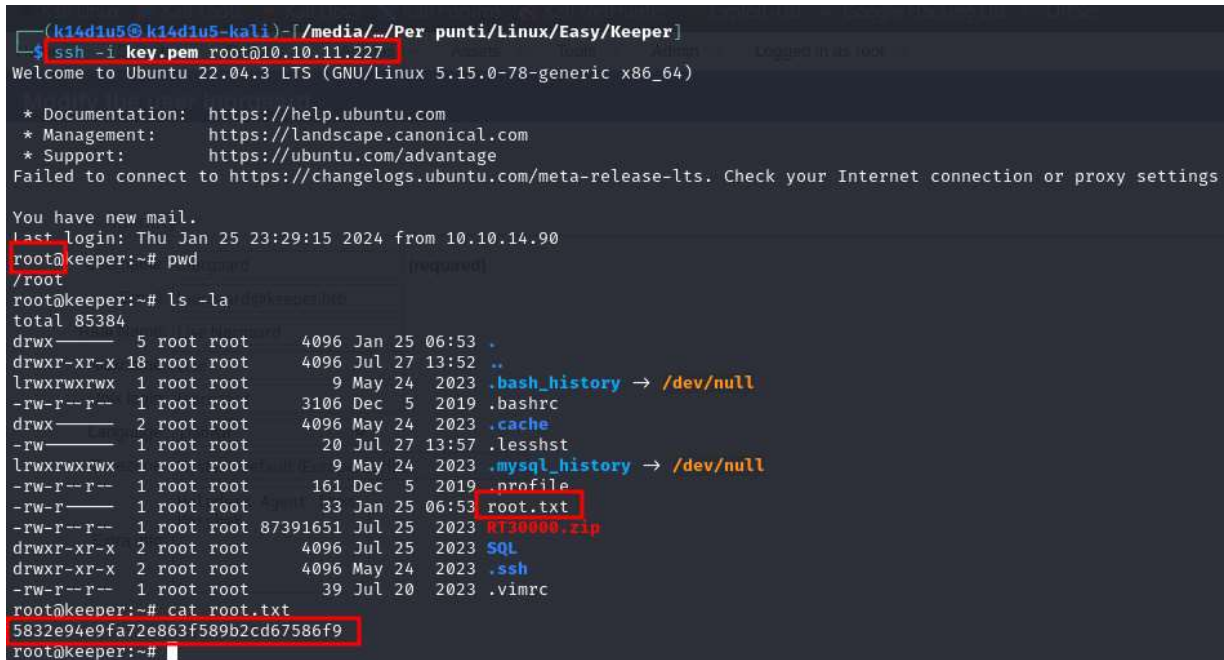

Picture 10 - Meaning of partial password

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:

Picture 11 - Privilege escalation and root flag