NeverLAN CTF

Forensics : Look into the past

Value : 250 pts

Difficulty : Unknown

Description : We've captured a snapshot of a computer, but it seems the user was able to encrypt a file before we got to it. Can you figure out wha they encrypted ?

Attachment : look_into_the_past.tar.gz

Solution :

First, download the attachment «look_into_the_past.tar.gz» and extract his content. As said the description we get a snapshot of a computer and we realize it was running linux.

Into the directory, i used the tree command for see all files on the box and found some interesting one.

Inside the home user directory, we found the encrypted flag. And there is a picture inside his «Pictures» directory.

There is a database inside «/opt» directory, and also passwd and shadow file inside «/etc» directory.

Looking for a potential .bash_history inside the user directory and ifound one with interesting informations.

```
root@kali:~/Téléchargements/look_into_the_past/home/User# cat .bash_history
cd Documents
openssl enc -aes-256-cbc -salt -in flag.txt -out flag.txt.enc -k $(cat $pass1)$pass2$pass3
steghide embed -cf doggo.jpeg -ef $pass1
mv doggo.jpeg ~/Pictures
useradd -p '$pass2'  user
sqlite3 /opt/table.db "INSERT INTO passwords values ('1', $pass3)"
tar -zcf /opt/table.db.tar.gz /opt/table.db
rm $pass1
unset $pass2
unset $pass3
exit
```

So here we get the command used with openssl for encrypt the flag, we can see it use a key using three different password (pass1 pass2 and pass3).

We can se the user hidded the pass1 inside the picture present into the «Pictures» directory.

We can see the pass2 is the user password.

And the pass3 is present inside the database.

Let’s recolt those password.

Pass1 :

Extracting the password form the picture with steghide using no password (just hit enter) worked and extracted a text file called «steganopayload213658.txt».

```
root@kali:~/Téléchargements/look_into_the_past/home/User/Pictures# steghide extract -sf doggo.jpeg
Entrez la passphrase:
écriture des données extraites dans "steganopayload213658.txt".
root@kali:~/Téléchargements/look_into_the_past/home/User/Pictures# cat steganopayload213658.txt
JXrTLzijLb
```

Here we got the first password.

Pass1 is JXrTLzijLb

Pass2 :

Reading the shadow file give us the user password.

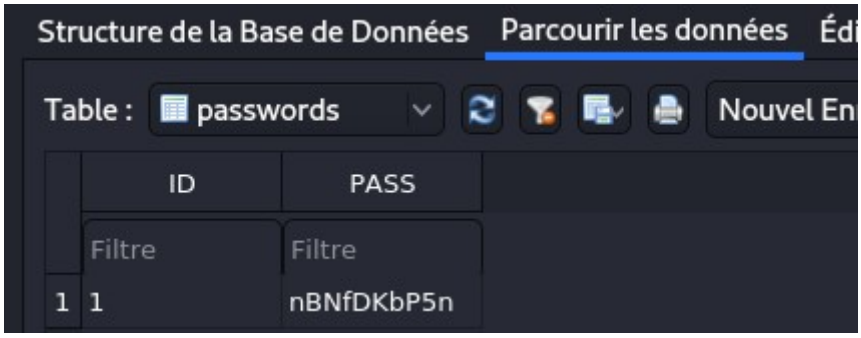
```
root@kali:~/Téléchargements/look_into_the_past/etc# cat shadow | grep "user"
user:KI6VWx09JJ:18011:0:99999:7:::
```

Here we got the second password.

Pass2 is KI6VWx09JJ

Pass3 :

Extracting the table.db.tar.gz and opening it with «DB Browser for SQLite» give us the last password.



Pass3 is nBNfDKbP5n

Decrypt the flag :

Now we get the full password for decrypt who is the one bellow, we can decrypt the flag.

Full Password : JxrTLzijLbKI6VWx09JJnBNfDKbP5n

```
root@kali:~/Téléchargements/look_into_the_past/home/User/Documents# openssl enc -aes-256-cbc -d -in flag.txt.enc
-out flag.txt -k 'JXrTLzijLbKI6VWx09JJnBNfDKbP5n'
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
root@kali:~/Téléchargements/look_into_the_past/home/User/Documents# cat flag.txt
flag{h1st0ry_1n_th3_m4k1ng}
```

Flag : flag{h1st0ry_1n_th3_m4k1ng}