NAME:PRIYANKA E ROLLNO:231901038

Ex. No.: 1 **Date: 30.08.24**

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

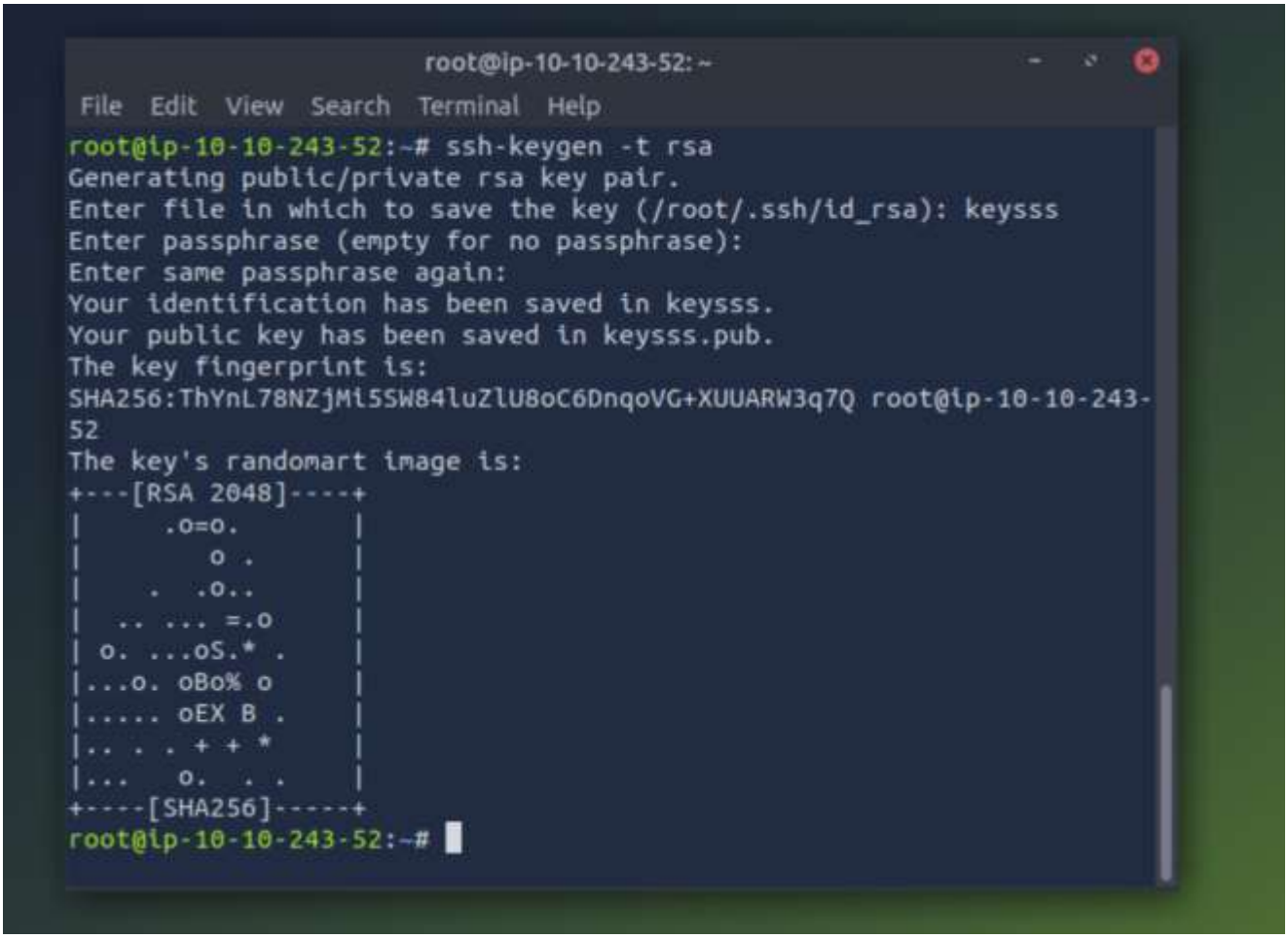
Aim:

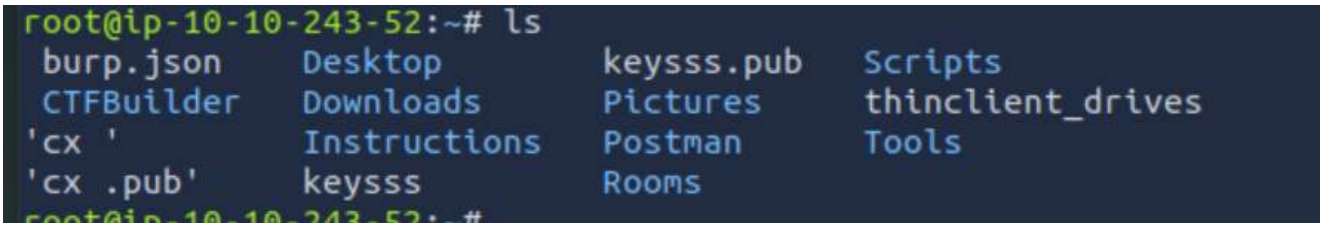
To capture the various flags in Encryption Crypto 101 in TryHackMe platform.

Algorithm:

1. Access the Encryption Crypto 101 lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/encryptioncrypto101
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Solve the crypto math used in RSA.
4. Find out who issued the HTTPS Certificate to tryhackme.com
5. Perform SSH Authentication by generating public and private key pair using ssh-keygen
6. Perform decryption of the gpg encrypted file and find out the secret word.

Output:


root@ip-10-10-243-52: ~
File Edit View Search Terminal Help
root@ip-10-10-243-52:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): keysss
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in keysss.
Your public key has been saved in keysss.pub.
The key fingerprint is:
SHA256:ThYnL78NZjMi5SW84luZlU8oC6DnqoVG+XUUARW3q7Q root@ip-10-10-243-52
The key's randomart image is:
+---[RSA 2048]----+
| .o=o. |
| o . |
| . .o.. |
| .. ... =.o |
| o. ...oS.* . |
|...o. oBo% o |
|..... oEX B . |
|.. . . + + * |
|...   o. . . |
+----[SHA256]-----+
root@ip-10-10-243-52:~#


root@ip-10-10-243-52:~# ls
burp.json Desktop keysss.pub Scripts
CTFBuilder Downloads Pictures thinclient_drives
'cx ' Instructions Postman Tools
'cx .pub' keysss Rooms

root@ip-10-10-18-189:~# gpg --import tryhackme.key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key FFA4B5252BAEB2E6: public key "TryHackMe (Example Key)" imported
gpg: key FFA4B5252BAEB2E6: secret key imported gpg: Total number processed:
1
gpg: imported: 1 gpg:
secret keys read: 1
gpg: secret keys imported: 1

root@ip-10-10-18-189:~# gpg message.gpg

gpg: WARNING: no command supplied. Trying to guess what you mean ... gpg:
encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
"TryHackMe (Example Key)"

gpg: WARNING: no command supplied. Trying to guess what you mean ... gpg:
encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
"TryHackMe (Example Key)"

Result:

Thus, the various flags have been captured in Encryption Crypto 101 in TryHackMe platform.