NAME: THULASI.S

ROLL NO:241901118

EXPERIMENT 1

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

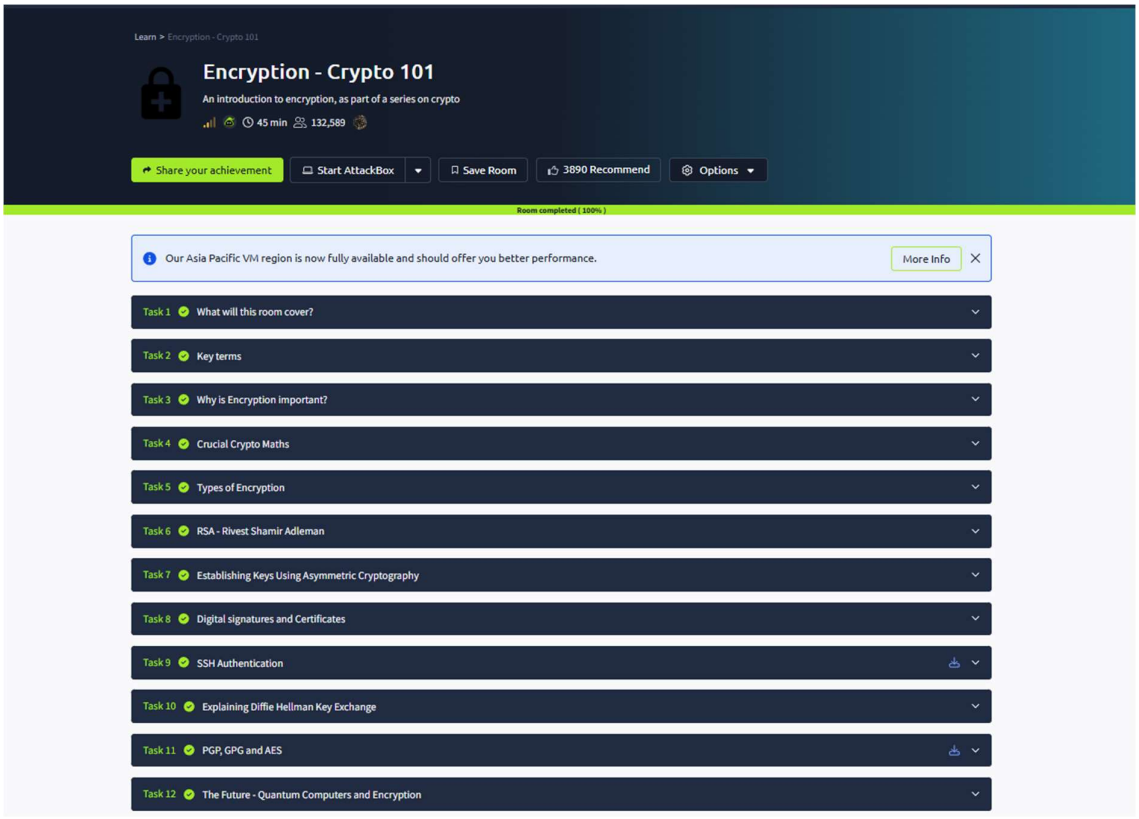
AIM:

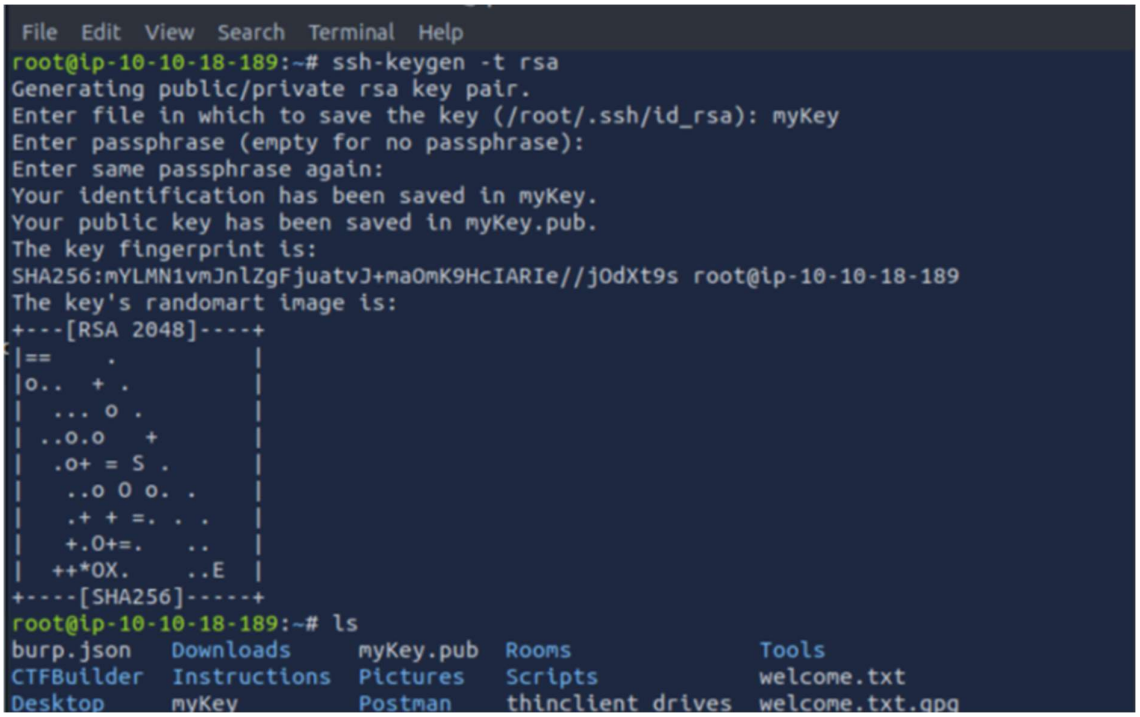
To capture the various flags in Encryption Crypto 101 in TryHackMe platform.

ALGORITHM:

1. Access the Passive reconnaissance lab in TryHackMe platform
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 jpg encrypted file and find out the secret word.

OUTPUT:


Learn > Encryption - Crypto 101
Encryption - Crypto 101
An introduction to encryption, as part of a series on crypto
45 min
132,589
Share your achievement
Start AttackBox
Save Room
3890 Recommend
Options
Room completed (100%)
Our Asia Pacific VM region is now fully available and should offer you better performance.
More Info
Task 1 What will this room cover?
Task 2 Key terms
Task 3 Why is Encryption important?
Task 4 Crucial Crypto Maths
Task 5 Types of Encryption
Task 6 RSA - Rivest Shamir Adleman
Task 7 Establishing Keys Using Asymmetric Cryptography
Task 8 Digital signatures and Certificates
Task 9 SSH Authentication
Task 10 Explaining Diffie Hellman Key Exchange
Task 11 PGP, GPG and AES
Task 12 The Future - Quantum Computers and Encryption




```
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.