

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

Share your achievement Start AttackBox Save Room Options 3890 Recommendation

Room completed (100%)

Our Asia Pacific VM region is now Fully available and should offer you better performance. More Info X

- 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

```
File Edit View Search Terminal Help
root@ip-10-10-18-189:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): myKey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in myKey.
Your public key has been saved in myKey.pub.
The key fingerprint is:
SHA256:mYLMN1vmJn1ZgFjuatvJ+ma0mK9HcIARIE//j0dXt9s root@ip-10-10-18-189
The key's randomart image is:
+---[RSA 2048]---+
|== . |
|o.. + . |
| ... o . |
| ..o.o + |
| .o+ = S . |
| ..o O o.. . |
| .+ + =. . . |
| +.0+=. . . |
| ++*OX. ...E |
+---[SHA256]---+
root@ip-10-10-18-189:~# ls
burp.json Downloads myKey.pub Rooms Tools
CTFBuilder Instructions Pictures Scripts welcome.txt
Desktop myKey Postman thinclient drives welcome.txt.gpg
```

```
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.