

EXP NO 1: CAPTURE ALL THE FLAGS IN ENCRYPTION 101 IN TRYHACKME PLATFORM

Rollno:241901058

AIM:

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

ALGORITHM:

1. Access the Encryption Crypto 101 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 gpg 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 👤 132,019 🏆

🔗 Share your achievement Start AttackBox Save Room 🏆 3886 Recommend ⚙️ Options

Room completed (100%)

- 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: ~  
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:MYLMN1vmJnLZgFjuatvJ+ma0mK9HcIARie//j0dXt9s root@ip-10-10-18-189  
The key's randomart image is:  
+----[RSA 2048]----+  
|== . |  
|o.. + . |  
| ... o . |  
|..o.o + |  
|.o+ = S . |  
| ..o 0 o. . |  
|. + + =. . . |  
|. +.o+=. . . |  
| ++*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
```

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