

Name: JANANY M

Rollno:231901012

Ex. No.: 1

Date:30.08.2024

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:

tryhackme.com/r/room/encryptioncrypto101

TryHackMe Dashboard Learn Compete Other Access Machines 1

Complete Beginner > Cryptography > Encryption - Crypto 101

Encryption - Crypto 101

An introduction to encryption, as part of a series on crypto

Medium 45 min

Start AttackBox Help Save Room 3537 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

5 new notifications

tryhackme.com/r/room/encryptioncrypto101

10.10.18.189

Complete Beginner > Cryptography > Encryption - Crypto 101

Encryption - Crypto 101

An introduction to encryption, as part of a series on crypto

Medium 45 min

Help Save Room 3537 Options

Room completed (100%)

Task 1 What will this room cover?

Task 2 Key terms

Your machine is initializing...

Use the AttackBox to attack machines you start on tasks

Loading (18%)

```

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//jOdXt9s root@ip-10-10-18-189
The key's randomart image is:
+---[RSA 2048]---+
|==          .|
|o.. + .      |
|... o .      |
|..o.o +      |
|.o+ = S .    |
|..o O 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

```

```

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.