

Ex. No.: 1

Date:30/7/2024

NAME:P.SHAMRUDHA VARSHINI

ROLLNO:231901048

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:

The screenshot displays the TryHackMe interface for the 'Encryption - Crypto 101' room. The browser address bar shows the URL `tryhackme.com/r/room/encryptioncrypto101`. The TryHackMe logo and navigation links (Dashboard, Learn, Compete, Other) are visible at the top. The room title 'Encryption - Crypto 101' is prominently displayed, along with the subtitle 'An introduction to encryption, as part of a series on crypto'. The difficulty is 'Medium' and the estimated time is '45 min'. A green progress bar indicates 'Room completed (100%)'. Below the header, a list of six tasks is shown, each with a green checkmark indicating completion:

- 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

At the bottom right, there is a notification badge that says '5 new notifications'.

The screenshot shows the tryhackme website interface. The top navigation bar includes the URL `tryhackme.com/r/room/encryptioncrypto101`. The main content area displays the room title "Encryption - Crypto 101" with a sub-header "An introduction to encryption, as part of a series on crypto". It indicates a difficulty level of "Medium" and a duration of "45 min". Below this, there are buttons for "Help", "Save Room", a thumbs up icon with "3537", and an "Options" dropdown. A green progress bar at the bottom of the room page shows "Room completed (100%)". Below the room page, two tasks are listed: "Task 1: What will this room cover?" and "Task 2: Key terms". To the right of the room page, a separate window shows a machine initialization screen with the text "Your machine is initializing..." and "Use the AttackBox to attack machines you start on tasks". A progress bar for the machine loading is shown at 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//j0dXt9s 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
```

Department of Computer Science and Engineering (Cyber Security)/CR23331

```
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.

Department of Computer Science and Engineering (Cyber Security)/CR23331

