

Ex. No.: 1

Date: 01.08.2025

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

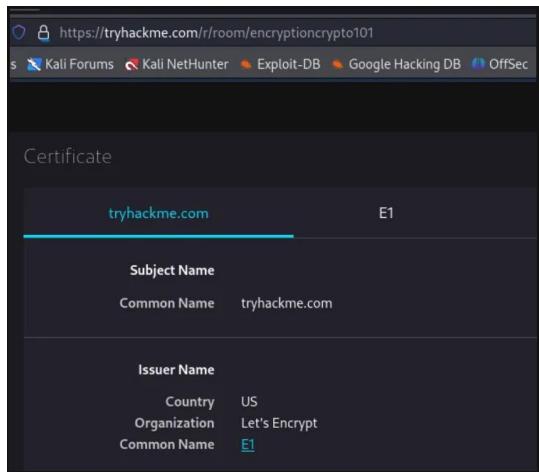
Aim:

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.
Find out who issued the HTTPS Certificate to tryhackme.com 4.
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.

The screenshot shows the TryHackMe platform interface. At the top, there are several tabs: 'try hack me - Yahoo India Search', 'TryHackMe | Dashboard', 'CAPTURE FLAGS-ENCRYPTION', and 'TryHackMe | Encryption - Crypto 101'. The main content area displays the 'Encryption - Crypto 101' room details. It includes a lock icon, a brief description ('An introduction to encryption, as part of a series on crypto'), a duration of '45 min', and a count of '132,141' users. Below this are buttons for 'Share your achievement', 'Start AttackBox', 'Save Room', '3887 Recommend', and 'Options'. A message at the top of the room says, 'Our beta VM region in Asia now supports public rooms via AttackBox and OpenVPN. Click for more information.' The room completion status is shown as 'Room completed (100%)'. Below the completion message, there are three tasks listed: 'Task 1' (What will this room cover?), 'Task 2' (Key terms), and 'Task 3' (Why is Encryption important?). The bottom half of the screenshot shows a terminal window titled '(kali㉿kali)-[~/Downloads]'. The terminal output shows a password cracking session using John the Ripper (john) against an SSH private key password. The command used was '\$ john ssh.txt --wordlist=/usr/share/wordlists/rockyou.txt'. The session output includes messages about loading hashes, cost factors, and iteration counts, followed by the successful cracking of the password 'delicious' (id_rsa_1593558668558.id_rsa). The session concludes with 'Session completed.'



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