

Ex. No.: 1

Date:06/08/2024

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.

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 room title is 'Encryption - Crypto 101' with a 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 at the top indicates 'Room completed (100%)'. Below the progress bar, there is a list of 12 tasks, 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
- 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

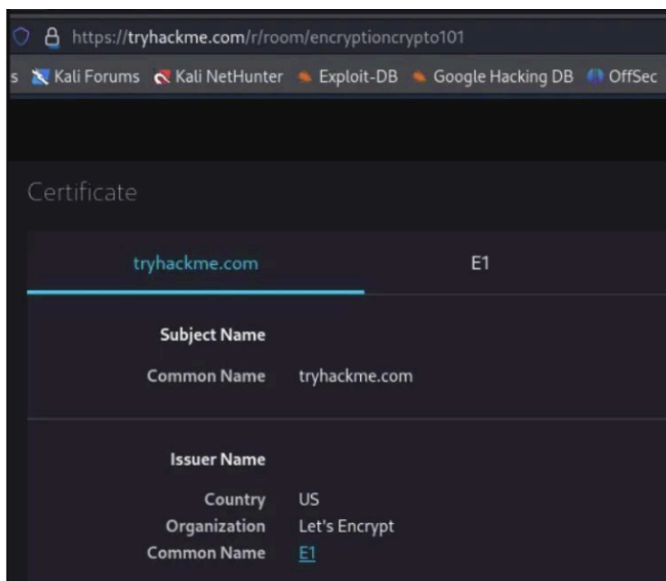
At the bottom of the page, there is a table with room statistics:

Created by	Room Type	Users in Room	Created
NinjaJc01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	118,963	1532 days ago

```

(kali㉿kali)-[~/Downloads]
$ john ssh.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
delicious (id_rsa_1593558668558.id_rsa)
1g 0:00:00:00 DONE (2024-06-06 18:57) 25.00g/s 98400p/s 98400c/s 98400C/s savannah1..delicious
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```



Result:

Thus, the various flags have been captured in Encryption crypto 101 in TryHackMe Platform.