

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

EXP.NO: 3

AIM:

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

ALGORITHM:

1. Access the Passive reconnaissance 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:





```

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

```

CS19642 Cryptography and Network Security

```
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)"

Answer the questions below

I agree not to complain too much about how theory heavy this room is.

No answer needed

✓ Correct Answer

Are SSH keys protected with a passphrase or a password?

passphrase

✓ Correct Answer

🔑 Hint

What does SSH stand for?

Secure Shell

✓ Correct Answer

How do web servers prove their identity?

certificates

✓ Correct Answer

🔑 Hint

What is the main set of standards you need to comply with if you store or process payment card details?

PCI-DSS

✓ Correct Answer

CS19642 Cryptography and Network Security

What's 30 % 5?

0

✓ Correct Answer

What's 25 % 7

4

✓ Correct Answer

What's 118613842 % 9091

3565

✓ Correct Answer

🔍 Hint

Should you trust DES? Yea/Nay

Nay

✓ Correct Answer

🔍 Hint

What was the result of the attempt to make DES more secure so that it could be used for longer?

Triple DES

✓ Correct Answer

🔍 Hint

Is it ok to share your public key? Yea/Nay

Yea

✓ Correct Answer

220701229

$p = 4391$, $q = 6659$. What is n ?

29239669

✓ Correct Answer

🔍 Hint

I understand enough about RSA to move on, and I know where to look to learn more if I want to.

No answer needed

✓ Correct Answer

What can you use to verify that a file has not been modified and is the authentic file as the author intended?

Digital Signature

✓ Correct Answer

CS19642

Cryptography

and

Network

Security

I recommend giving this a go yourself. Deploy a VM, like [Linux Fundamentals 2](#) and try to add an SSH key and log in with the private key.

No answer needed

✓ Correct Answer

🔍 Hint

Download the SSH Private Key attached to this room.

No answer needed

✓ Correct Answer

What algorithm does the key use?

RSA

✓ Correct Answer

🔍 Hint

Crack the password with [John The Ripper](#) and rockyou, what's the passphrase for the key?

delicious

✓ Correct Answer

🔍 Hint

Time to try some GPG. Download the archive attached and extract it somewhere sensible.

No answer needed

✓ Correct Answer

You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?

Pineapple

✓ Correct Answer

🔍 Hint

220701229

RESULT:

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