

Timelapse

In this tutorial, you will explore side-channels, metadata and steganography. Question 1 uses the `timelapse.out` executable provided.

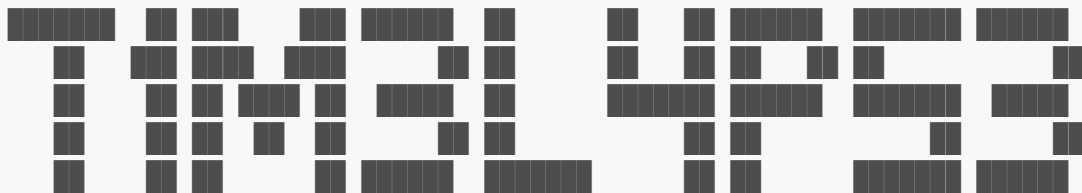
Question 1

- What is a vulnerability where an attacker can gain information about a system's secret or private data by measuring the time it takes for certain operations to complete?
- What is the flag obtained from the `timelapse` program?

Hint

- The `timelapse` program takes in a 4 digit password. There also seems to be a delay when processing the password. Find out if the delay varies with the digits entered.

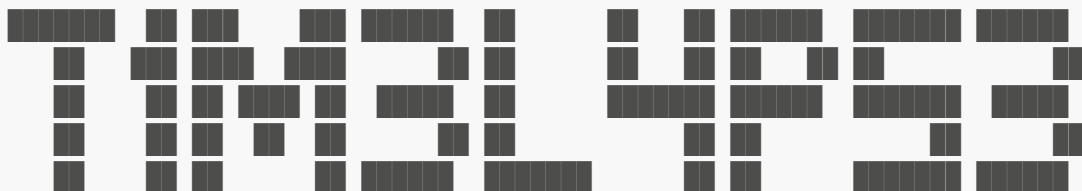
```
$ ./timelapse
```



```
Usage: ./timelapse <password>
```

```
Please enter the 4 digit numerical password...
```

```
$ ./timelapse 0000
```



```
1.004884958267212
```

```
1.005920171737671
```

```
1.0057597160339355
```

```
1.0117690563201904
```

```
Access denied...
```

Question 2

- You have been tasked with investigating an image found at the following link:
<https://raw.githubusercontent.com/0x4067/KpMU010N/main/SCSE.png>. What is interesting about the metadata of the image?
- A QR code with a link to a text file is hidden somewhere within the image. What is the steganography technique used in the text file?
- The flag obtained contains a link to a research paper. What is the phone model discussed in the paper?

Hint

- Search online for EXIF viewers and steganography tools!