Sleuthkit Intro

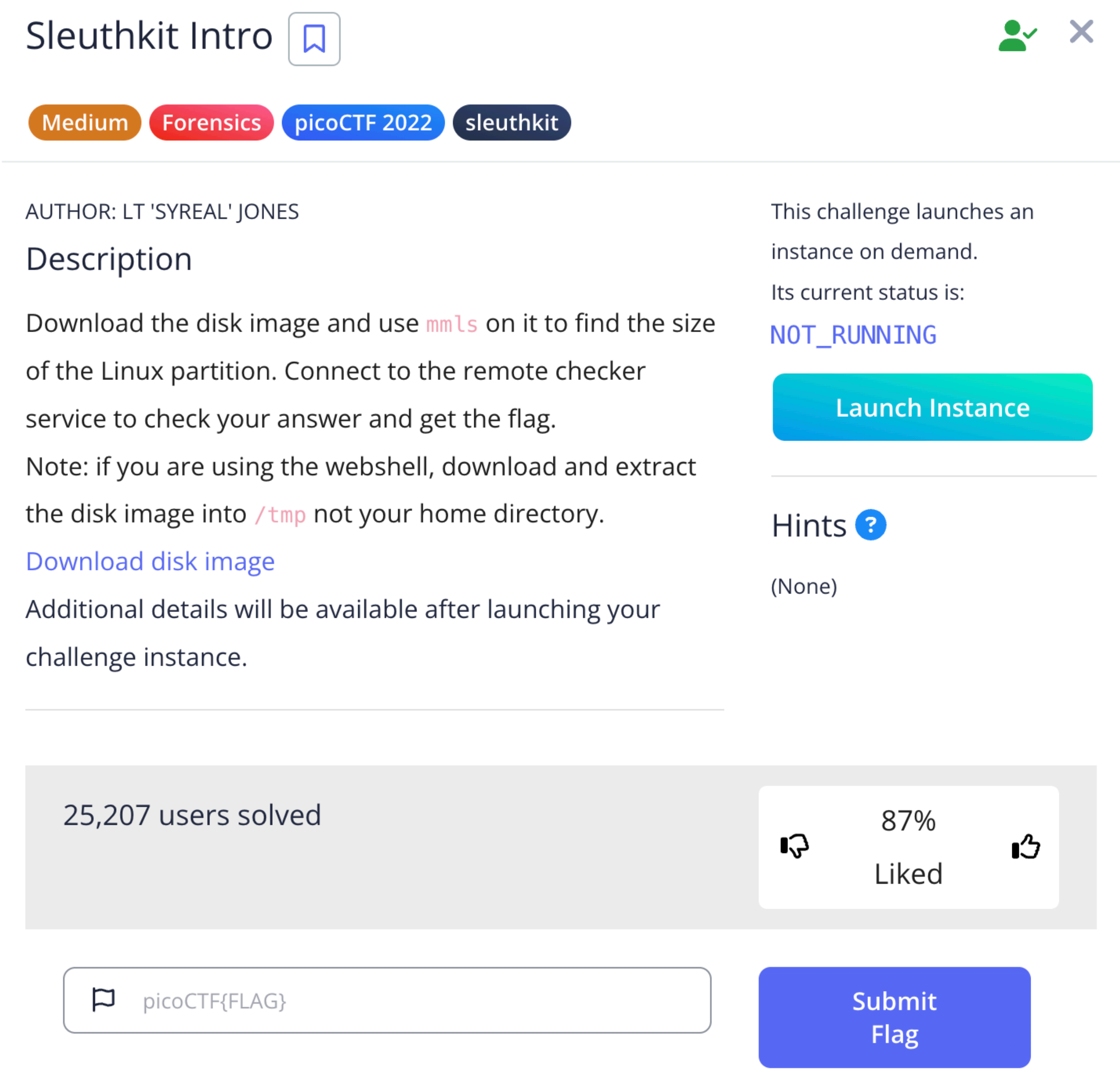
Challenge Information

- **CTF Name**: picoCTF
- **Challenge Name**: Sleuthkit Intro
- **Challenge link**: https://play.picoctf.org/practice/challenge/301?category=4&originalEvent=70&page=1
- **Category**:Forensics
- **Difficulty**:medium
- **Author** : Vishvambhar Ranoshe

Summary

The objective of this challenge is to explore a provided disk image to locate specific metadata about the partition table. [cite_start]By using command-line tools from **The Sleuth Kit**, you must identify the starting sector of a specific partition and then provide that information to a remote server to retrieve the final flag.

Challenge Description



Setup / Tools

`Tools:mmls,gunzip`

Exploitation Steps

Step 1:

Begin by downloading the disk image provided in the challenge description. This is typically a compressed file (e.g., `.gz`). You must extract it to access the raw disk image file .

```
┌──(kali㉿kali)-[~/Downloads/picoCTF]
└─$ ls
disk.img.gz

┌──(kali㉿kali)-[~/Downloads/picoCTF]
└─$ gunzip disk.img.gz

┌──(kali㉿kali)-[~/Downloads/picoCTF]
└─$ ls
disk.img
```

Step 2:

To view the layout of the disk image, use the `mmls` (Media Management List) tool. [cite_start]This command displays the partition table, including the starting and ending offsets of each partition.

Command: mmls disk.img

Look for the partition labeled as "Linux" or the primary data partition and note its **starting sector** (the value under the "Length" column).

```
┌──(kali㉿kali)-[~/Downloads/picoCTF]
└─$ mmls disk.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000204799   0000202752   Linux (0x83)
```

Step 3:

Once you have the starting sector, you must connect to the picoCTF challenge server.

When you launch the challenge, you are provided with a netcat command like `nc saturn.picoctf.net [port]`. Using `nc` (Netcat) allows you to interact with the challenge's remote backend script.

Run the provided `nc` command in your terminal. The server will prompt you for the starting offset of the partition you identified in Step 2. Input the numeric value of the starting sector you found.

```
vishvambharranoshe@Vishvambhars-MacBook-Air ~ % nc saturn.picoctf.net 59211
What is the size of the Linux partition in the given disk image?
Length in sectors: 202752
202752
Great work!
picoCTF{mm15_f7w!}
```

Flag

`picoCTF{mm15_f7w!}`