**Capture the Flag (CTF)**

Challenge on IoT Forensics • Challenge 2

**Index**

**Assumptions/Needs** 3

**Objective** 3

**Problem** 3

**Task 1** 4

**Task 2** 5

**Task 3** 6

**Objective**

The user’s objective will be to use a filesystem debugger tool to read a baseline timestamp on a few files. After establishing the baseline timestamps, a malicious actor will make modifications to some of the files. The user will have to determine which files were affected, when the attack took place, and what was done.

**Problem**

You suspect that you have experienced a breach. Your job is to determine the extent of the breach and when the breach occurred.

**Assumptions/Needs**

* Hyper-V software for virtual Rasperry Pi
* Raspbian Stretch OS
* debugfs enabled in Linux.

**Task 1**

**Description**

The first task is to create 3 (three) files (eg.: **file1.txt**, **file2.txt**, and **file3.txt**).

2 (two) files with the ‘**nano’** and ‘**echo’** commands respectively, and 1 (one) file with the **‘cat’** command. Collect baseline timestamps. You can assume that these timestamps were taken before the breach. Identify the **inode** and **timestamps** of each file and upload screenshots of the **inode** number**, timestamps** and the metadata viewer. Include a brief analysis of your findings.

**Task 2**

**Description**

The baseline timestamps for a system you are in charge of are given. Since then, however, the system has been breached. In an effort to cover his tracks, the attacker made new files by **compressing** his files with the **‘tar’** and **‘gzip’** commands and by moving them into your folder under the same original names . Identify the **inode** and **timestamps** of each file and upload screenshots of the **inode** number**, timestamps** and the metadata viewer. Include a brief analysis of your findings.

**Task 3**

**Description**

You discovered which file the attacker deleted and replaced, but you still suspect that the attacker has seen a file that he shouldn’t have, even if no changes were made. For this scenario, let us assume you as the attacker. Open one of the files with the **‘cat’** commands, and close it without any modification. Now, as an analyst, provide screenshots for evidence of how you can conclude that a file has been viewed but not modified. Include a brief analysis of your findings.