**Capture the Flag (CTF)**

Challenge on IoT Forensics • Challenge 1

**Index**

**Assumptions/Needs** 3

**Objective** 3

**Problem** 3

**Task 1** 4

**Task 2** 5

**Task 3** 6

**Task 4** 7

**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**

The first task is to create 3 files and collect baseline timestamps. You can assume that these timestamps were taken before the breach. Identify the **inode** of each file and upload screenshots of both the **inode** number and the metadata viewer.

**Evidence**

A screenshot of the debugfs stat readout of the viewed file and a few accompanying sentences explaining its content.

**Task 2**

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 a new file and moved it into your folder under the original name. Find out which file has been deleted and replaced.

**Evidence**

A screenshot of the debugfs stat readout of the viewed file and a few accompanying sentences explaining its content.

**Task 3**

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. Find out which file has been viewed, but not modified. Provide screenshots for evidence.

**Evidence**

A screenshot of the debugfs stat readout of the viewed file and a few accompanying sentences explaining its content.

**Task 4**

A different file within this folder has been modified without your permission. Determine which file was modified, and when the breach occurred.

**Evidence**

A screenshot of the debugfs stat readout of the viewed file and a few accompanying sentences explaining its content.