

**Summit**

Can you chase a simulated adversary up the Pyramid of Pain until they finally back down?

**Objective**

After participating in one too many incident response activities, PicoSecure has decided to conduct a threat simulation and detection engineering engagement to bolster its malware detection capabilities. You have been assigned to work with an external penetration tester in an iterative purple-team scenario. The tester will be attempting to execute malware samples on a simulated internal user workstation. At the same time, you will need to configure PicoSecure's security tools to detect and prevent the malware from executing.

Following the **Pyramid of Pain's** ascending priority of indicators, your objective is to increase the simulated adversaries' cost of operations and chase them away for good. Each level of the pyramid allows you to detect and prevent various indicators of attack.

**Room Prerequisites**

Completing the preceding rooms in the [Cyber Defence Frameworks module](https://tryhackme.com/module/cyber-defence-frameworks) will be beneficial before venturing into this challenge. Specifically, the following:

* [The Pyramid of Pain](https://tryhackme.com/room/pyramidofpainax)
* [MITRE](https://tryhackme.com/room/mitre)

Connection Details

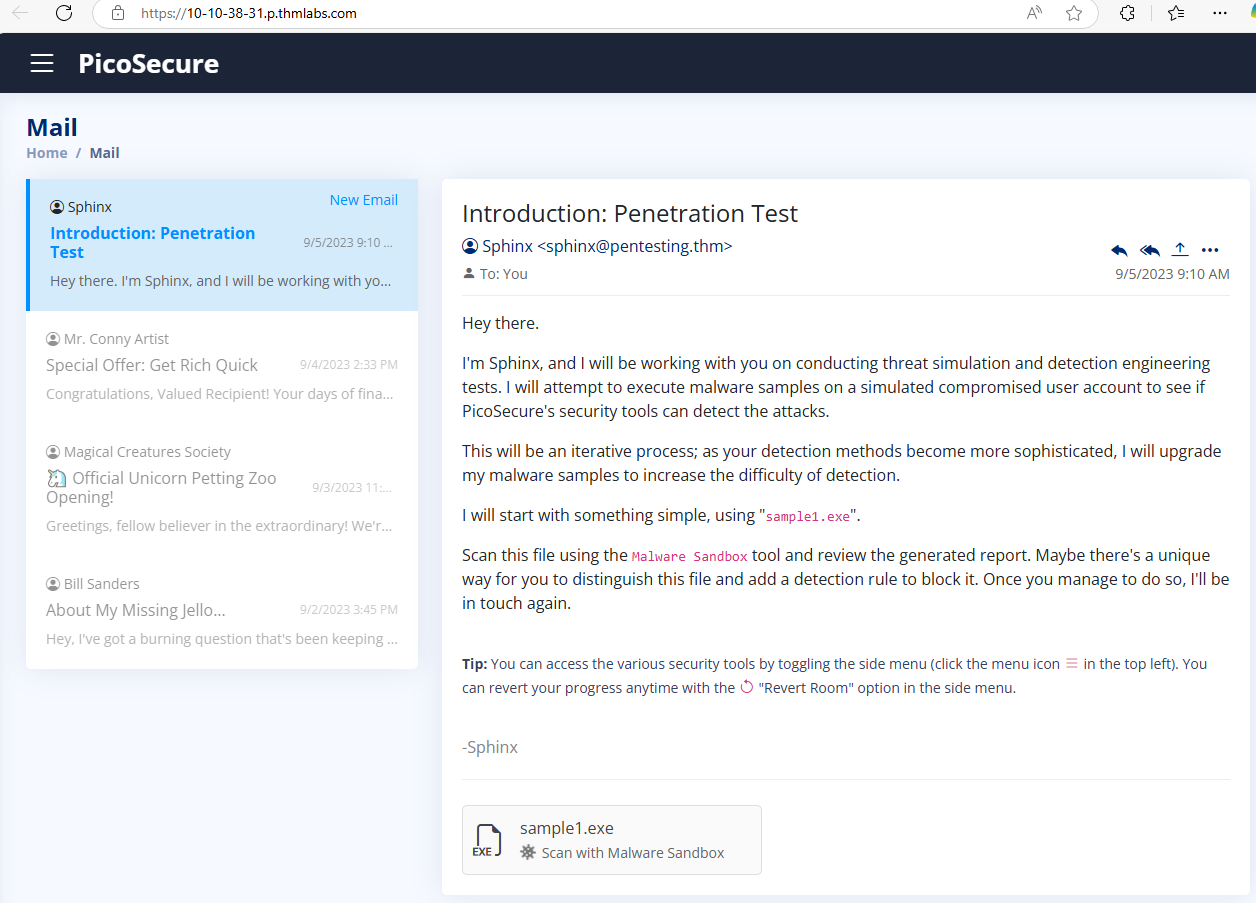
Please click **Start Machine** to deploy the application, and navigate to [https://10-10-38-31.p.thmlabs.com](https://10-10-38-31.p.thmlabs.com/) once the URL has been populated.

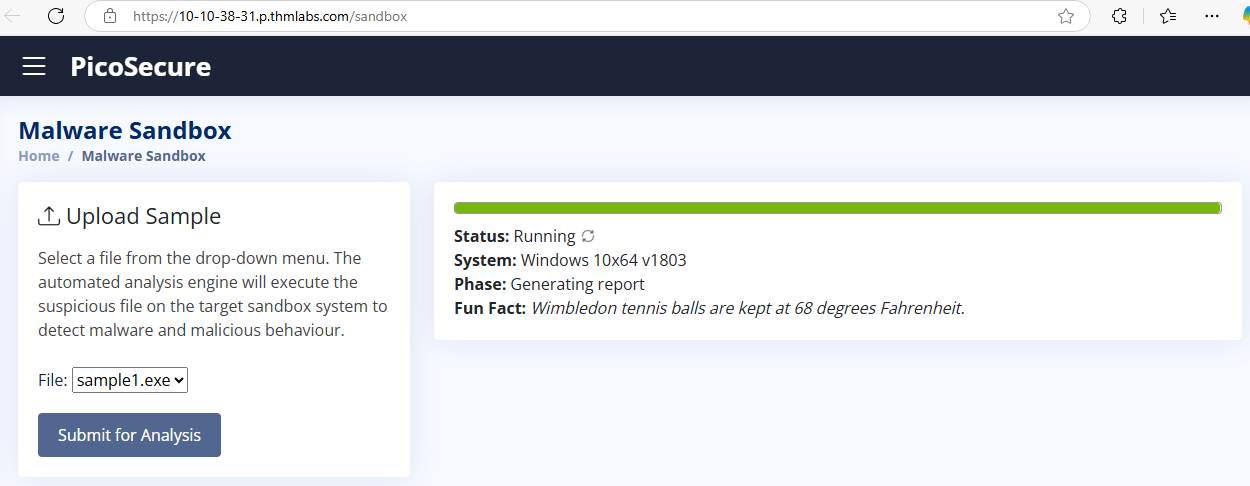
**Note:** It may take a few minutes to deploy the machine entirely. If you receive a "Bad Gateway" response, wait a few minutes and refresh the page.

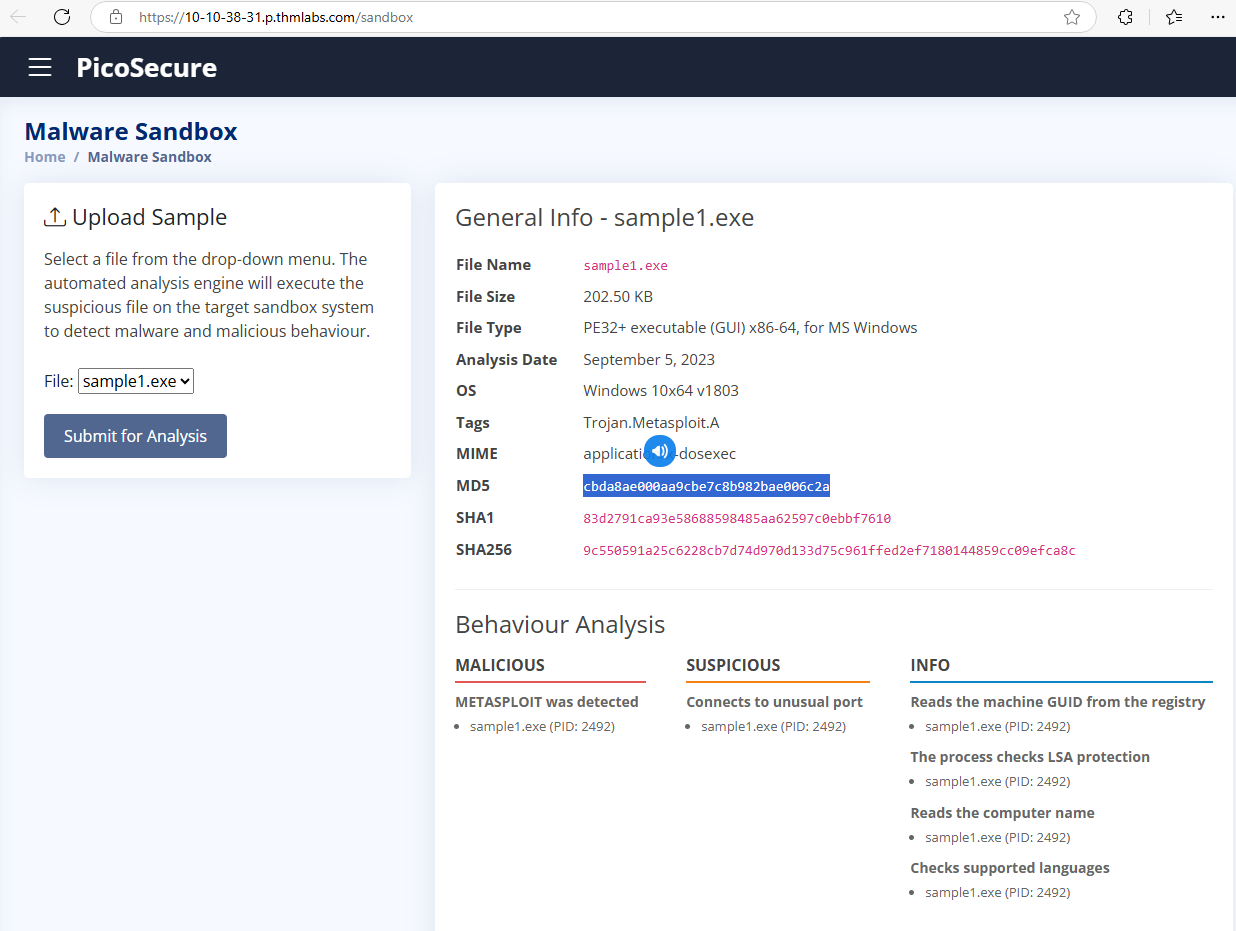
# Task 1: Challenge

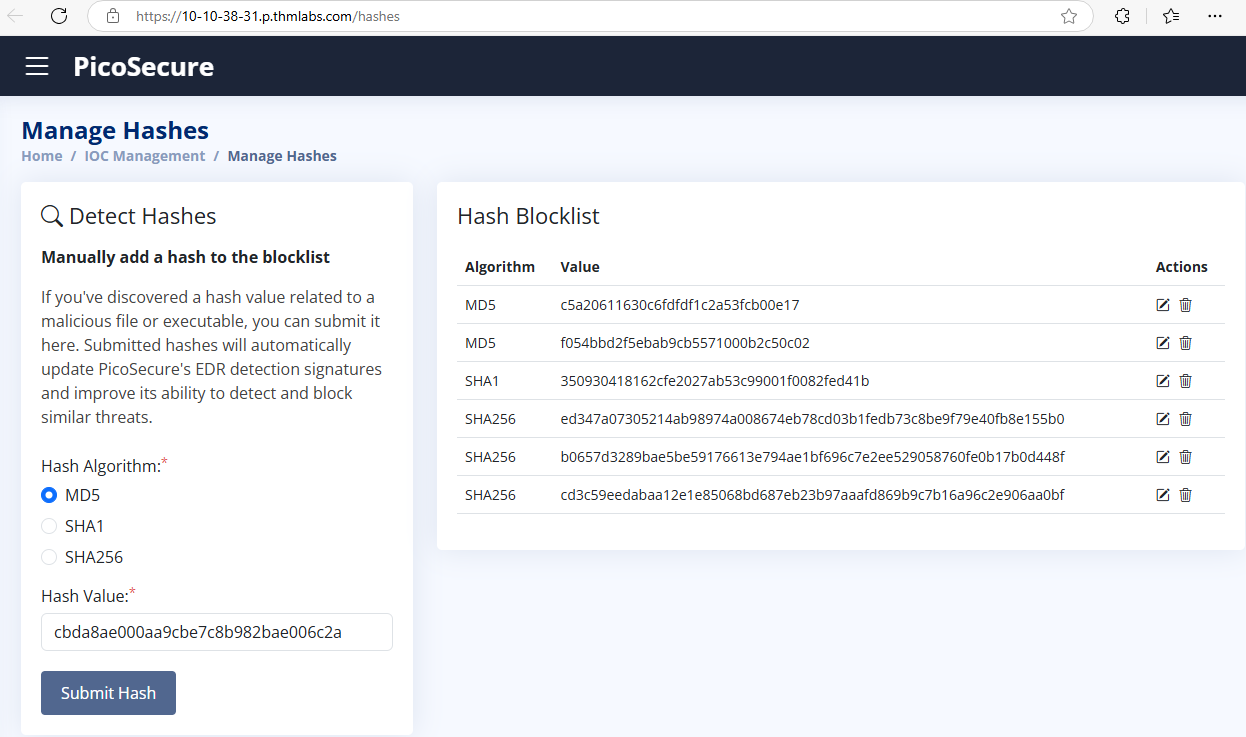
## 1. What is the first flag you receive after successfully detecting **sample1.exe**?

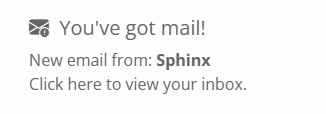
After starting the machine and navigating to the provided URL, we’re greeted with an introduction to the test.

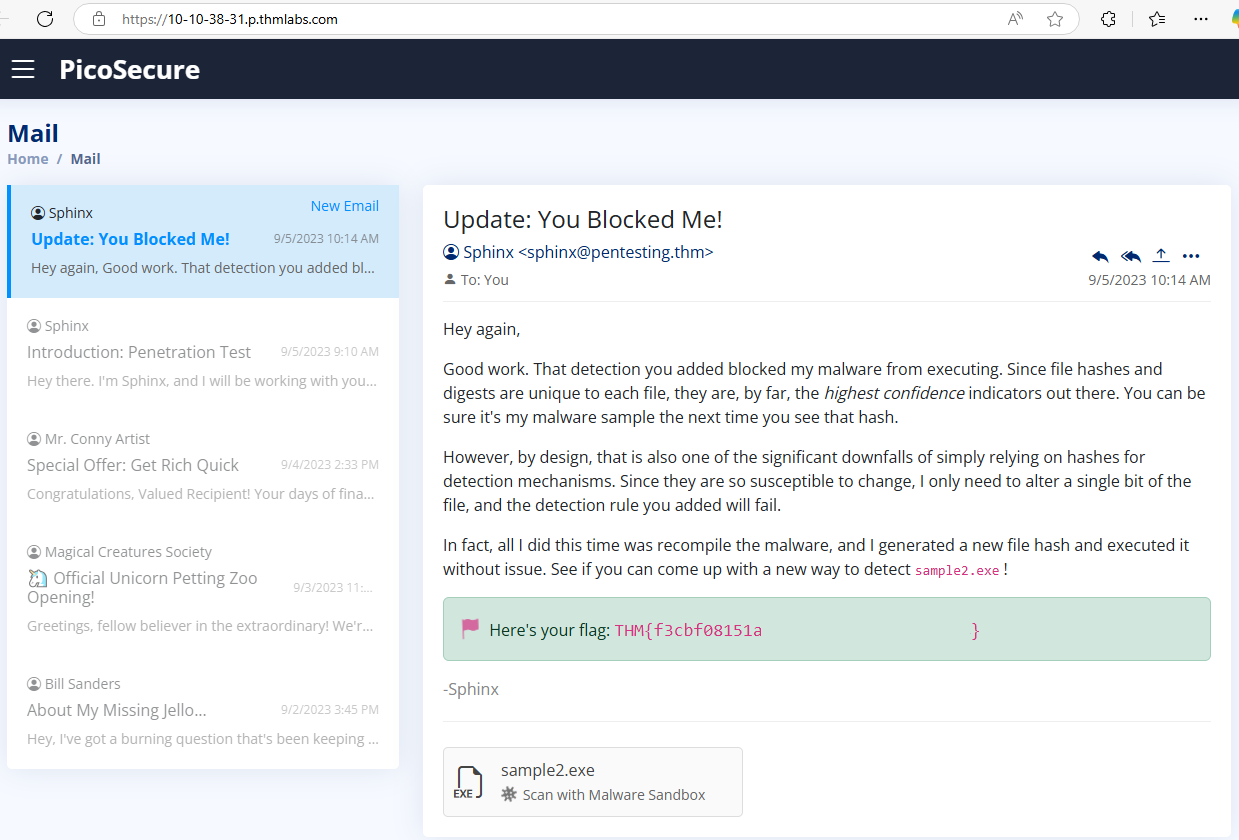




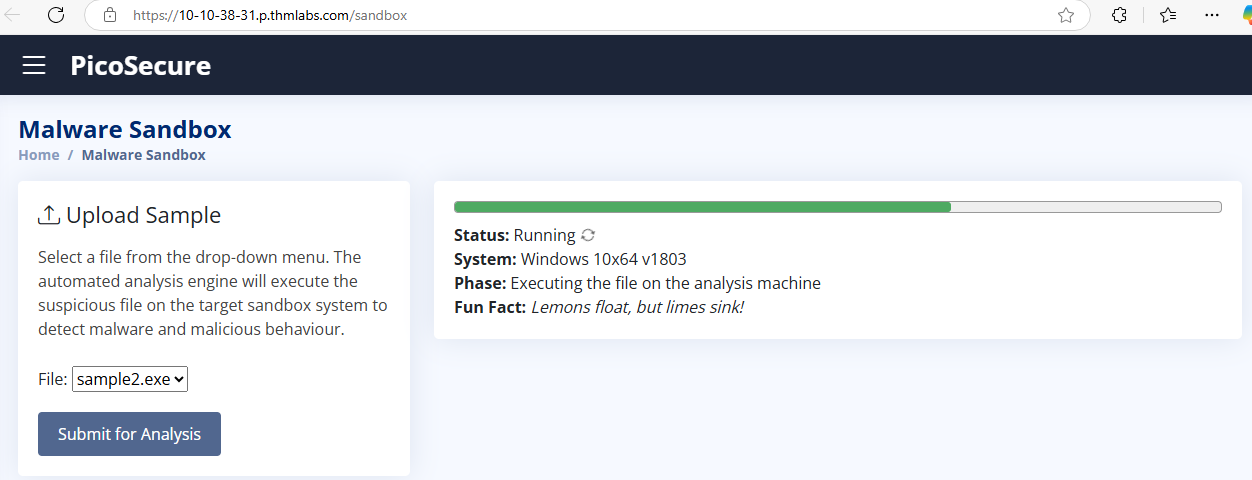


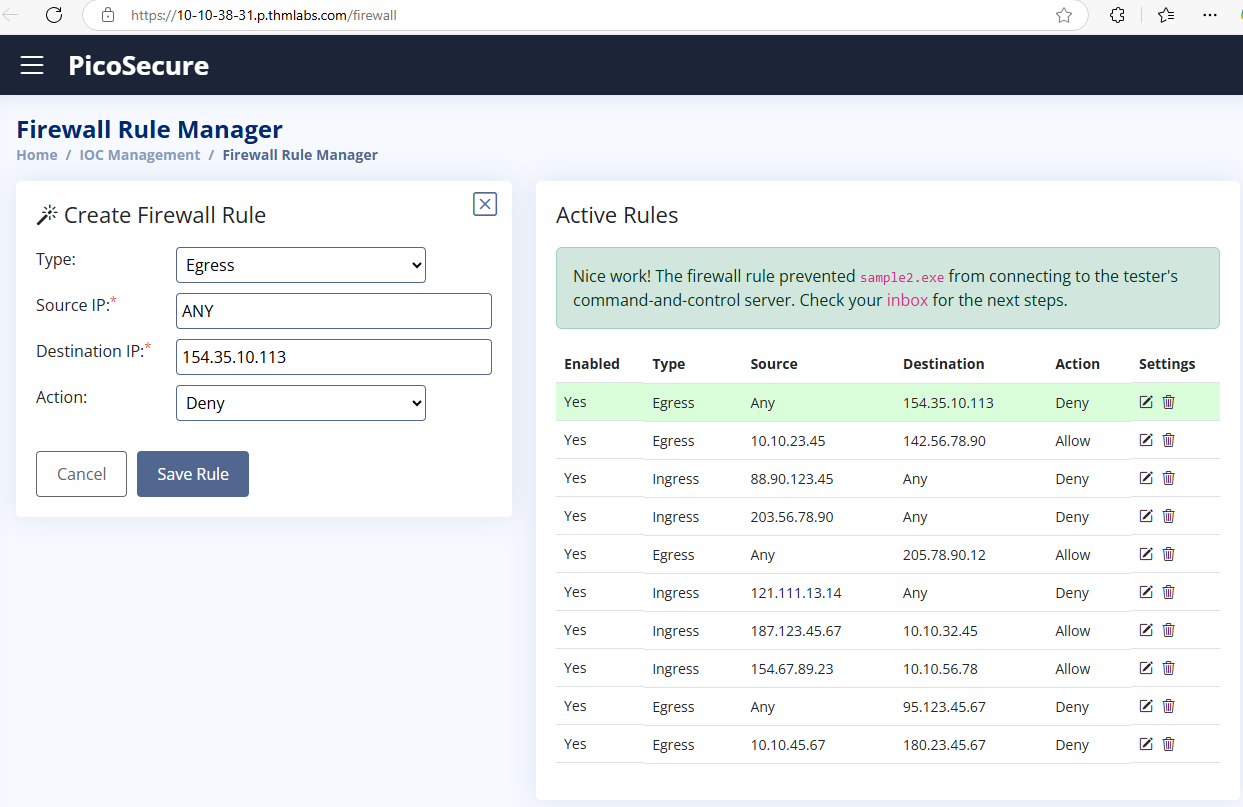


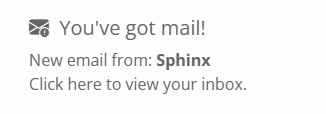


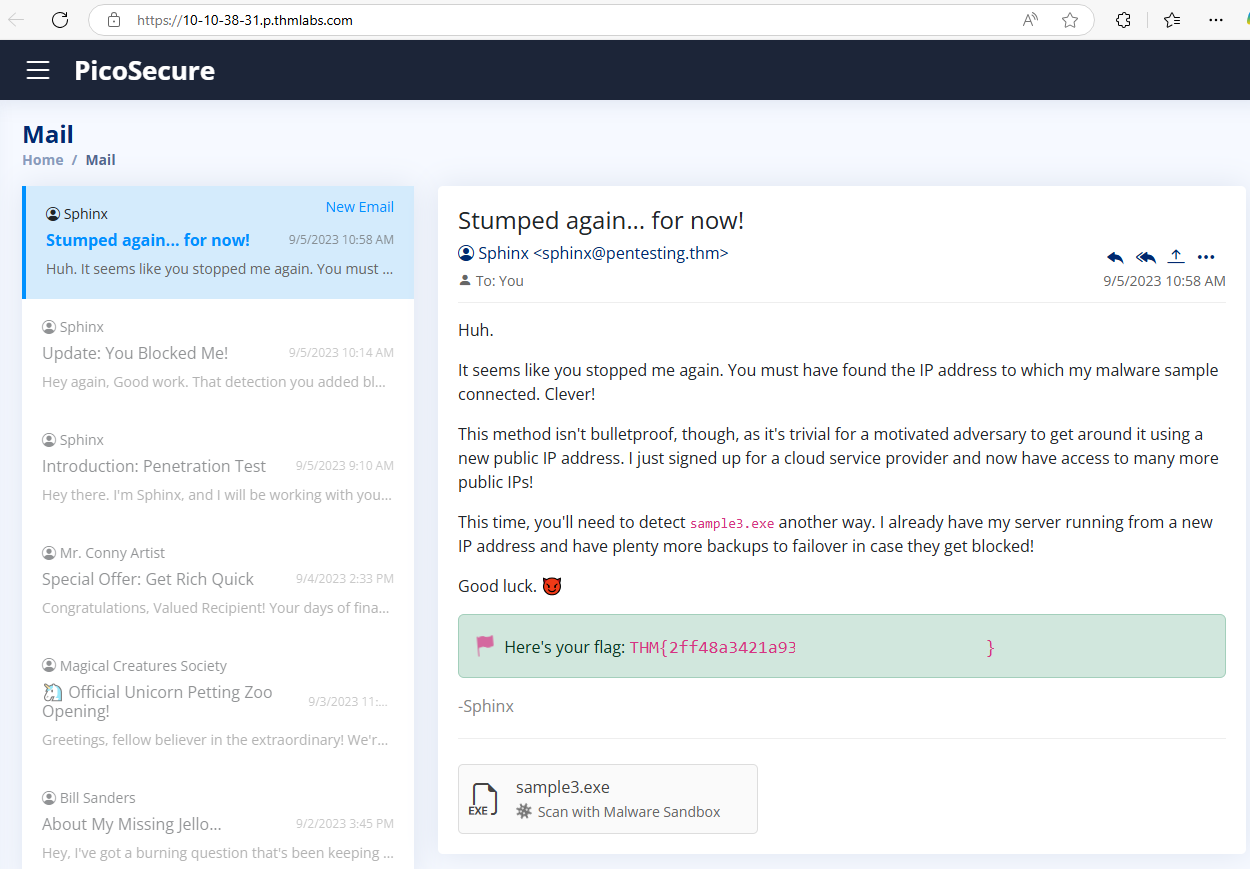


2. What is the second flag you receive after successfully detecting **sample2.exe**?

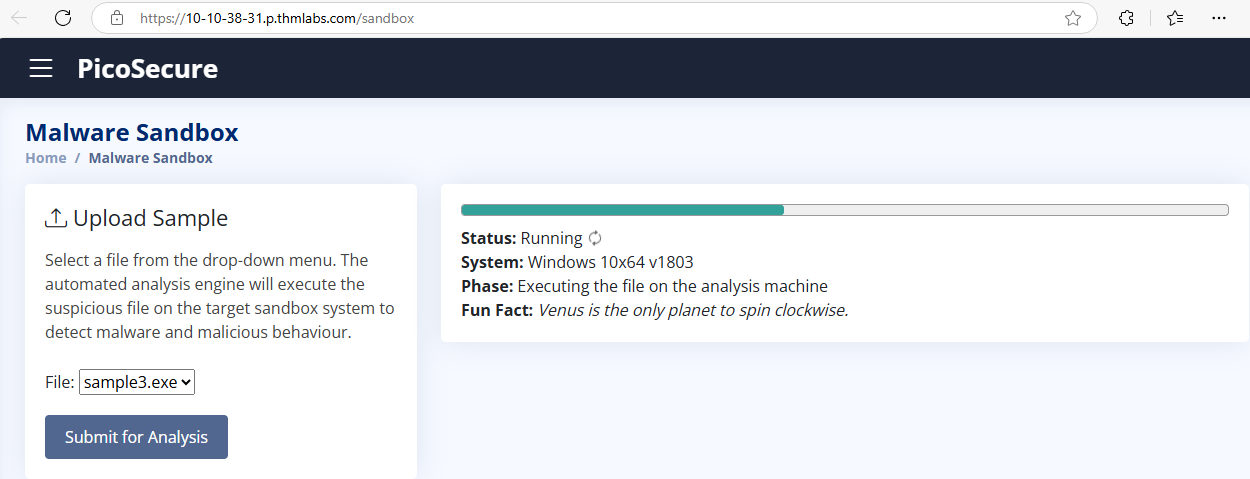


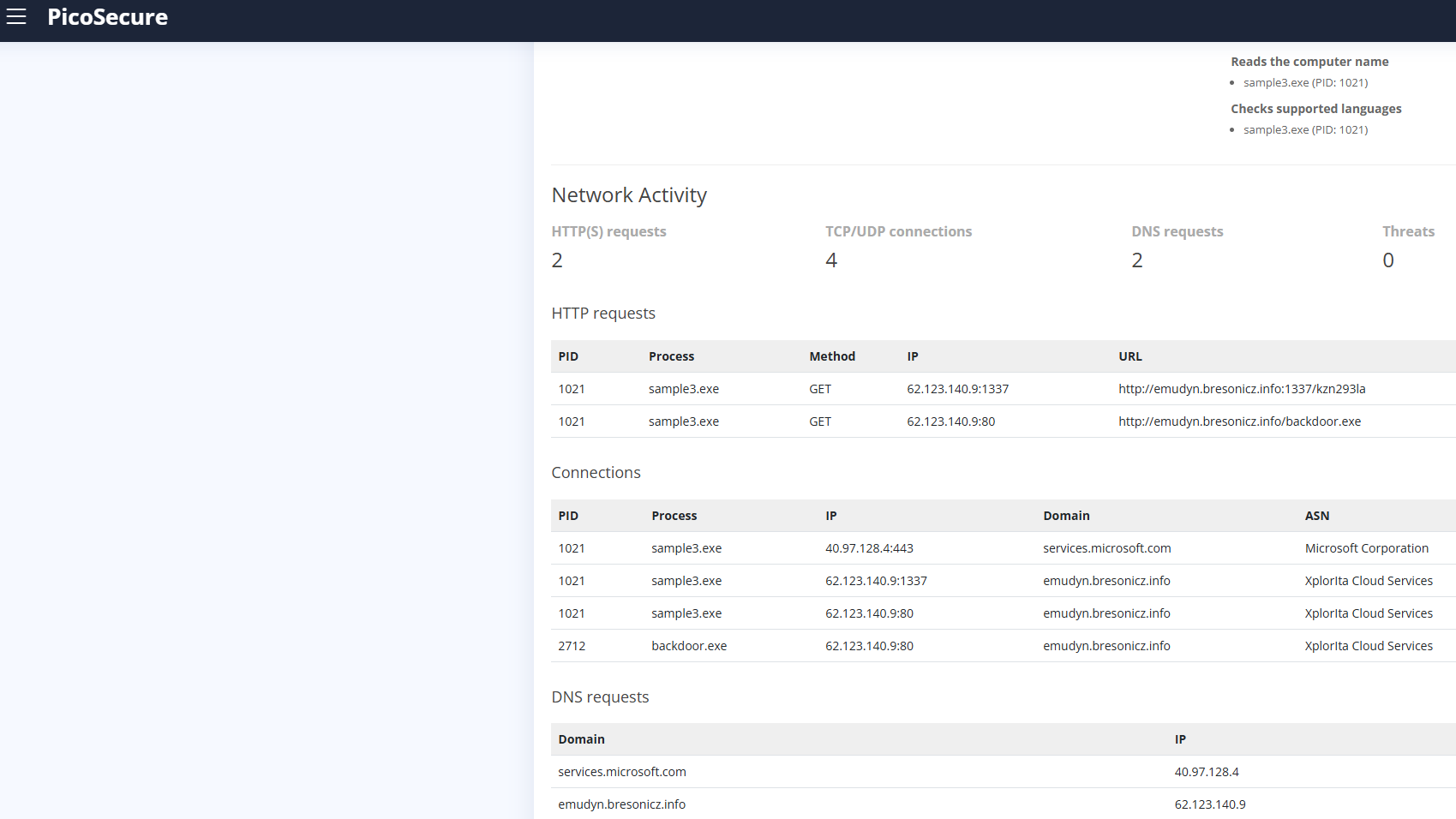


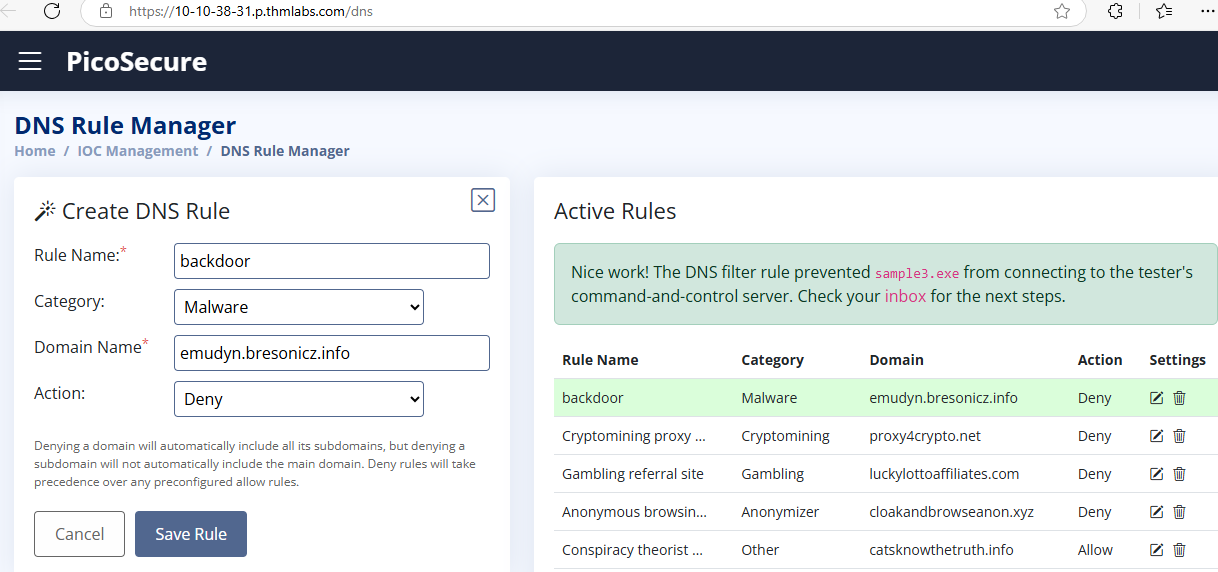


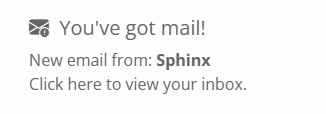


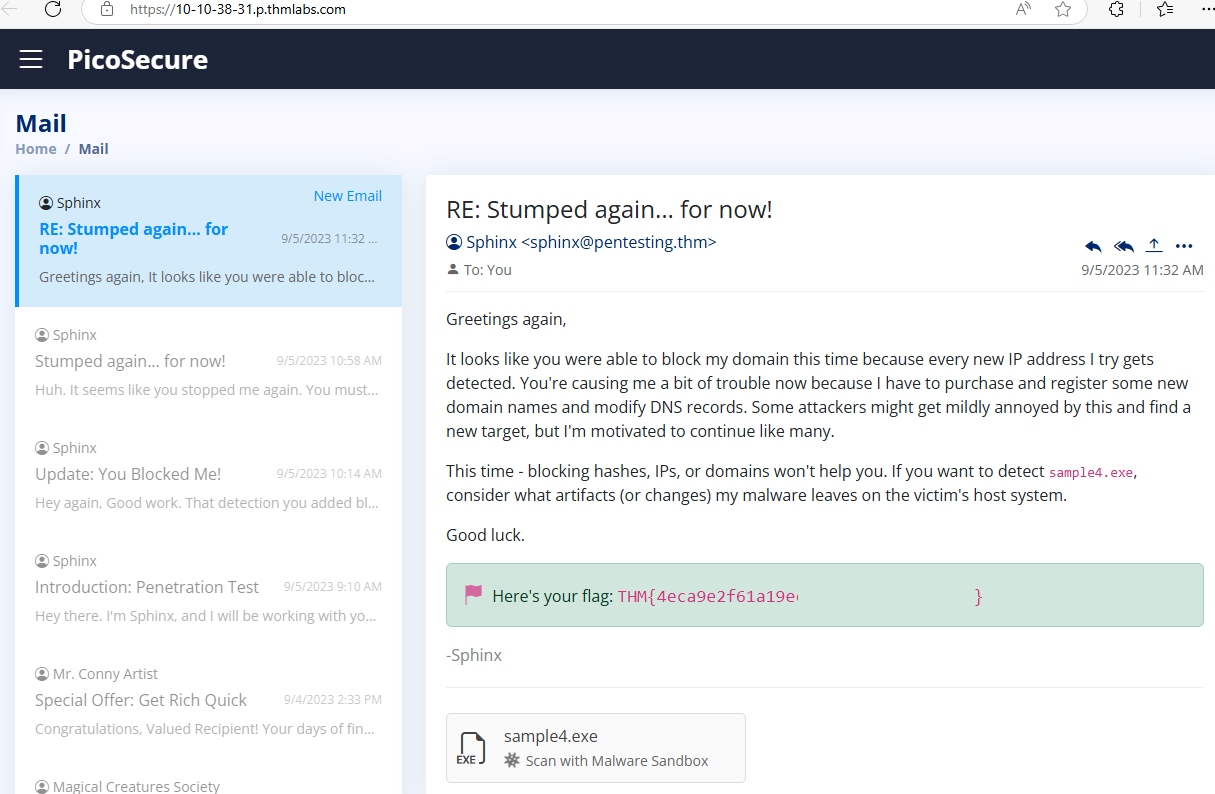
3 What is the third flag you receive after successfully detecting **sample3.exe**?



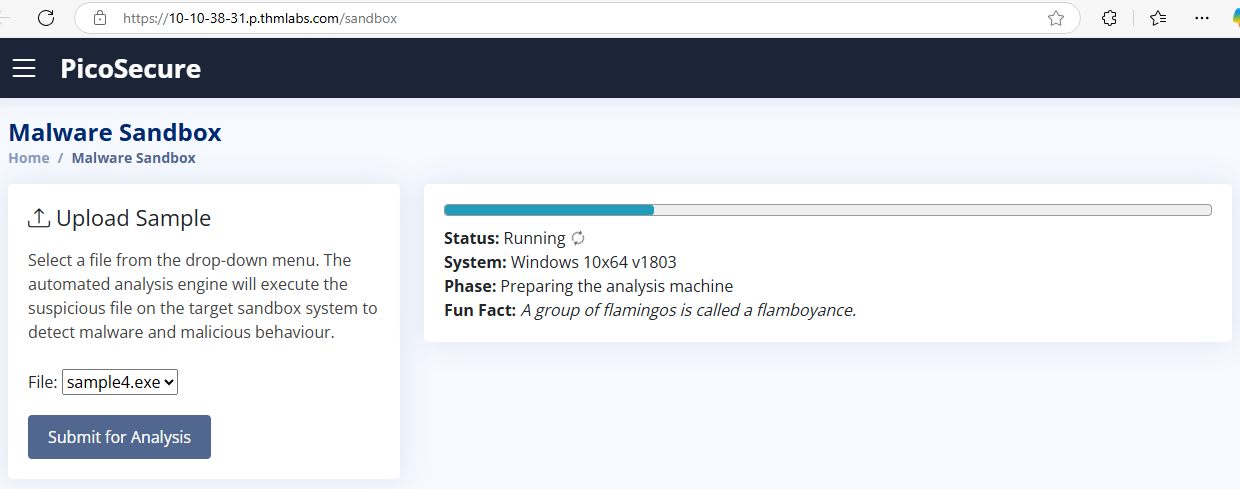


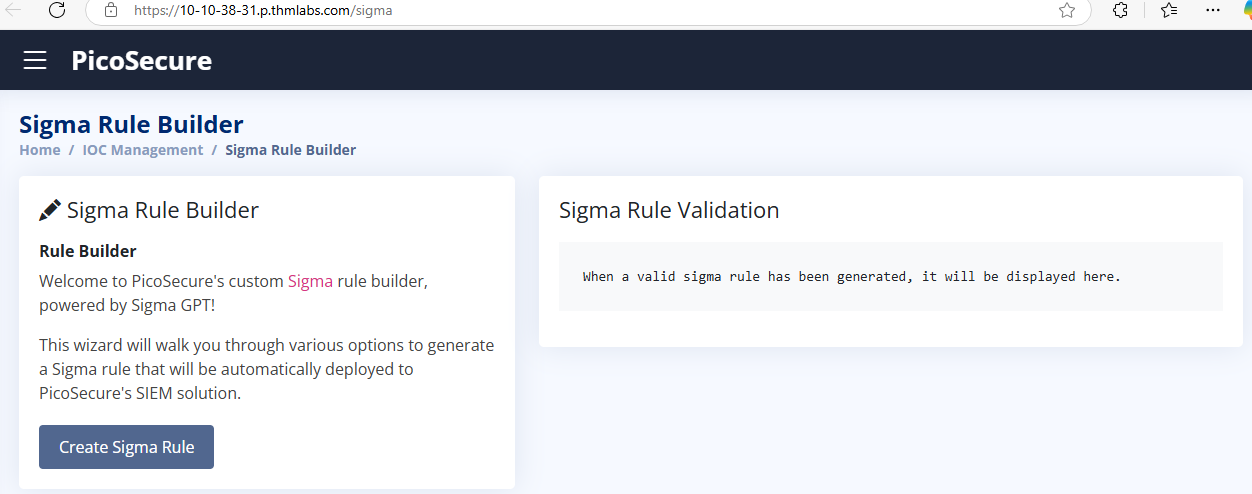


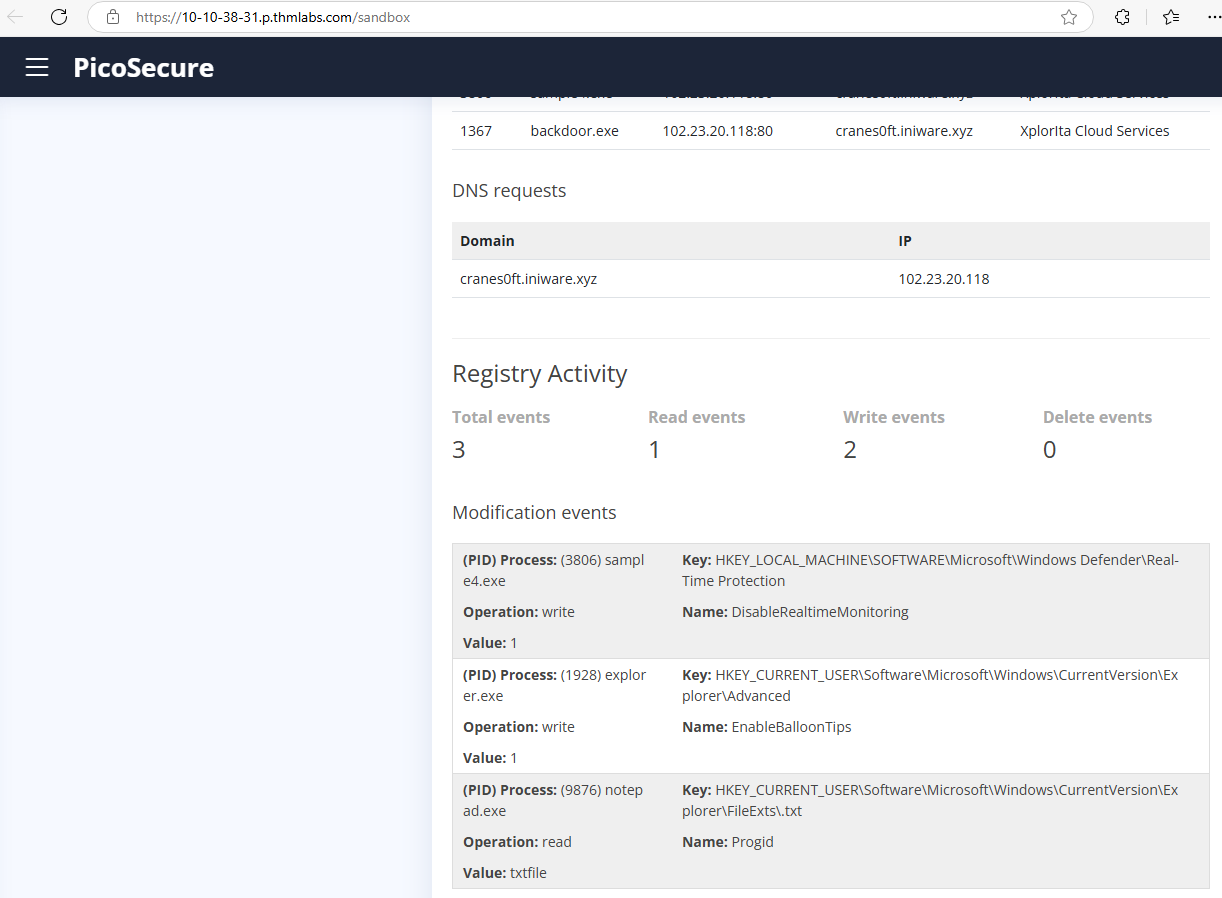


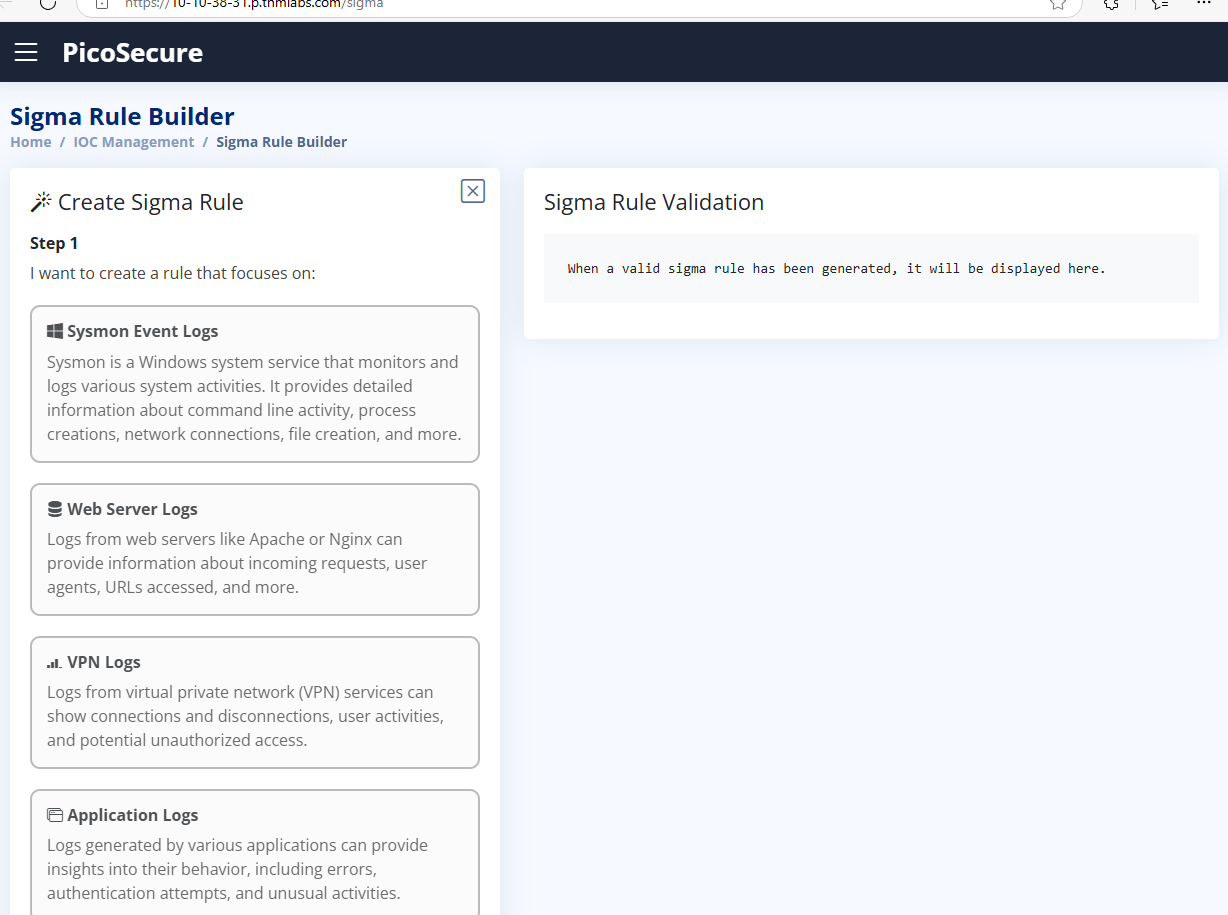


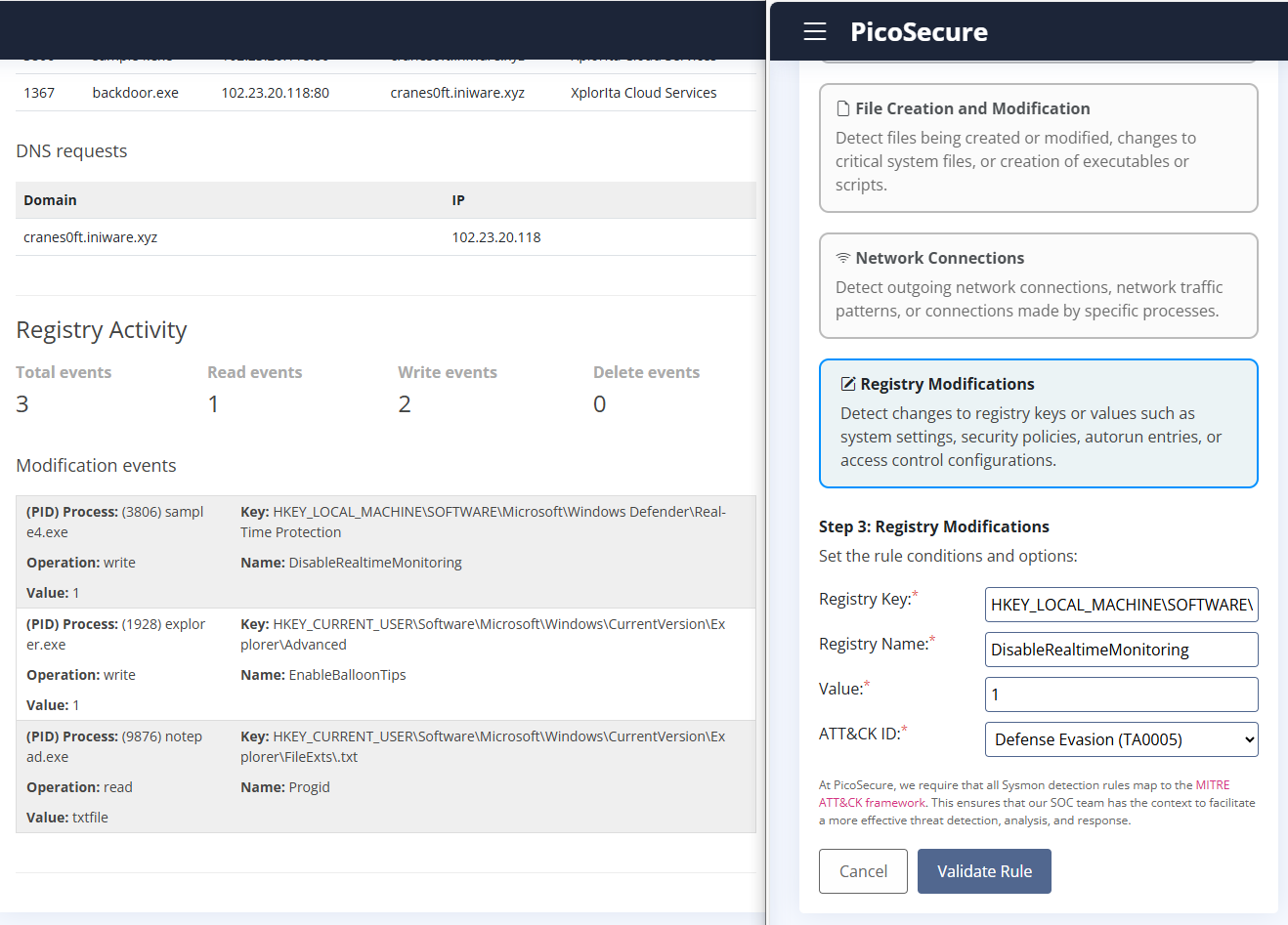
4. What is the fourth flag you receive after successfully detecting **sample4.exe**?

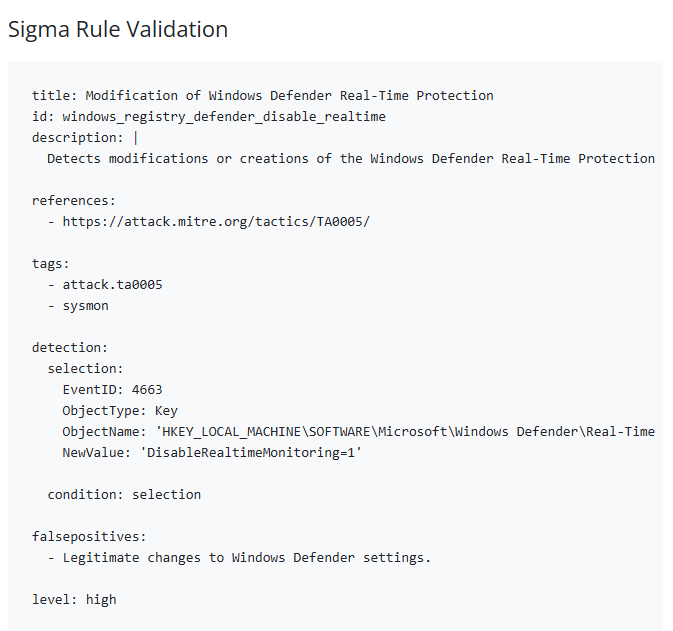


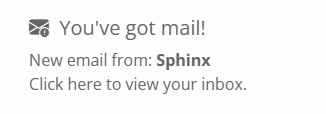


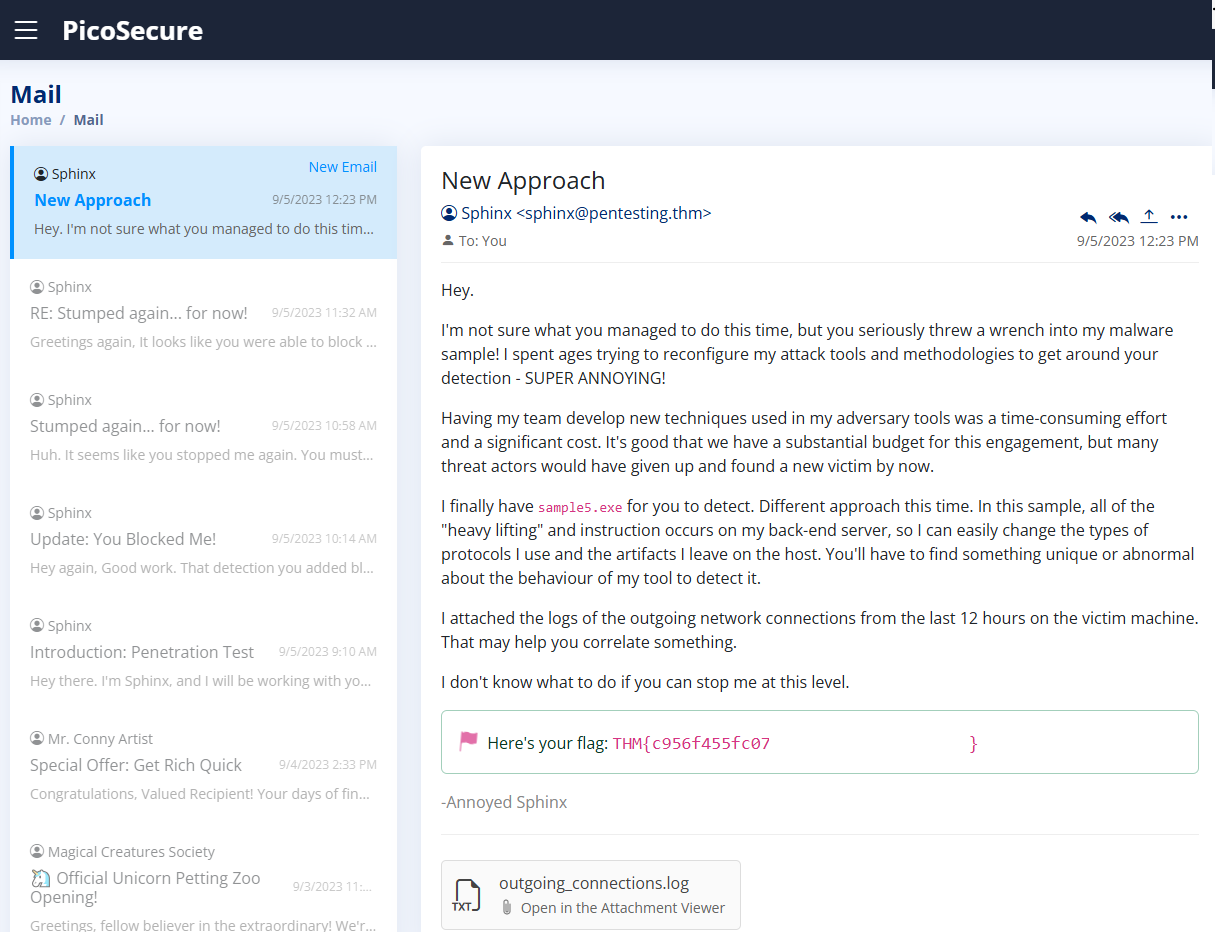




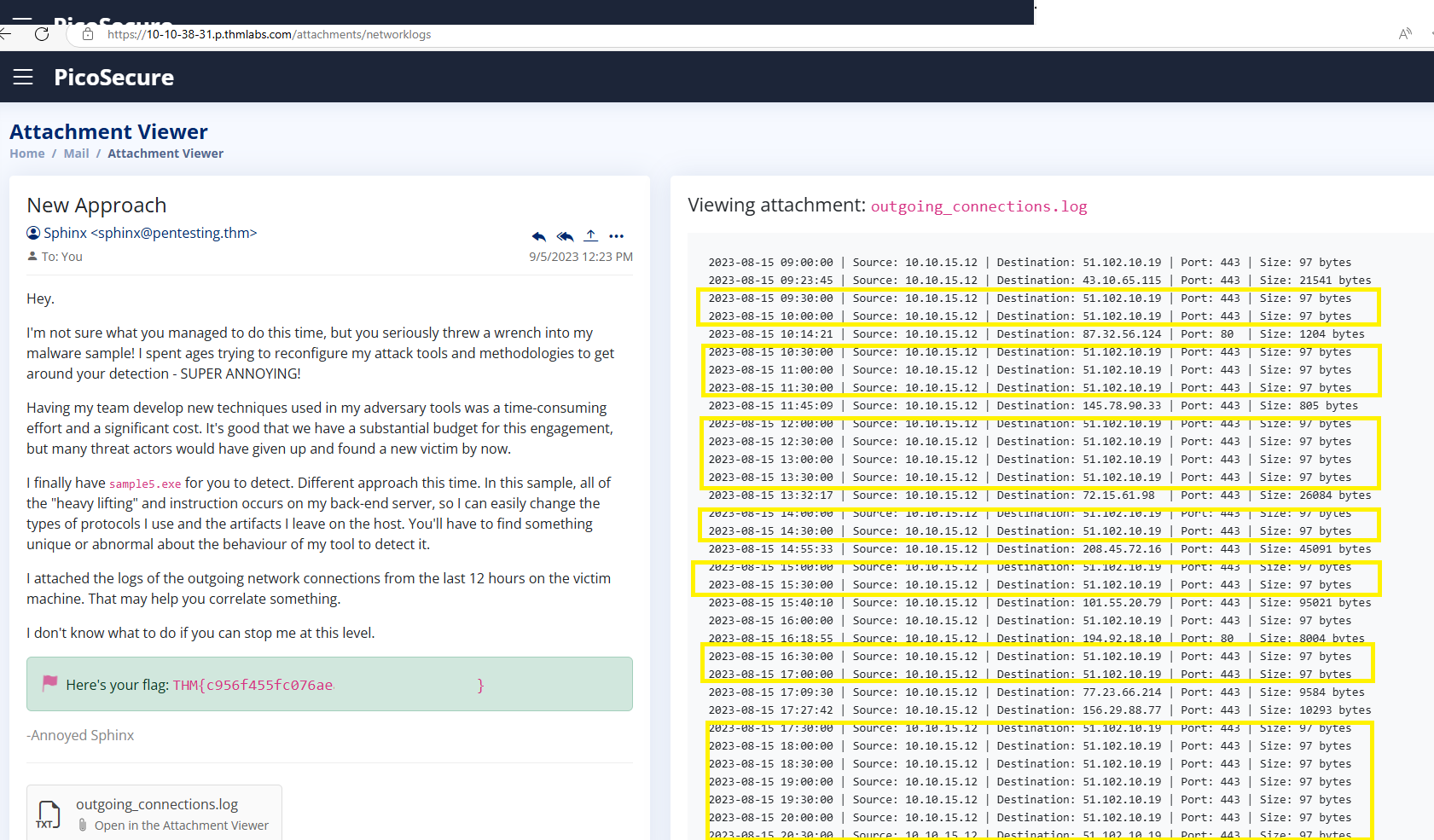


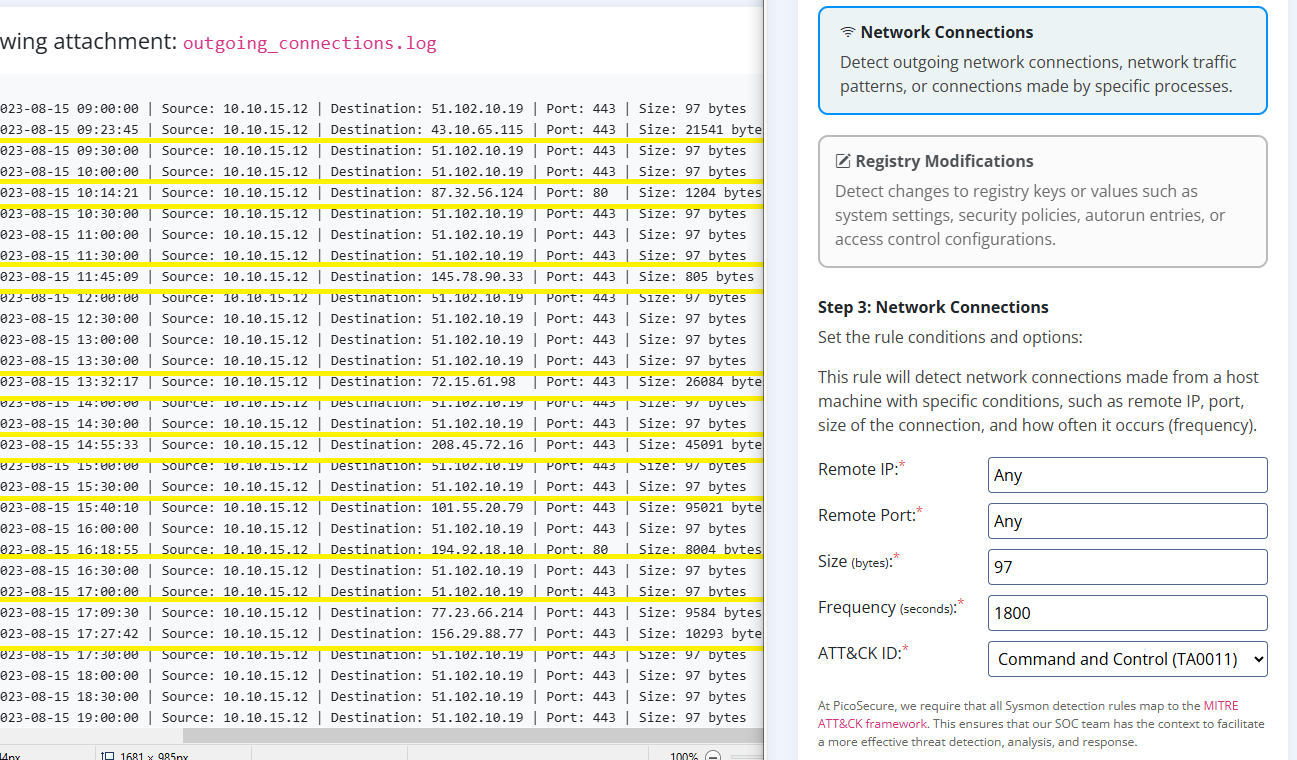




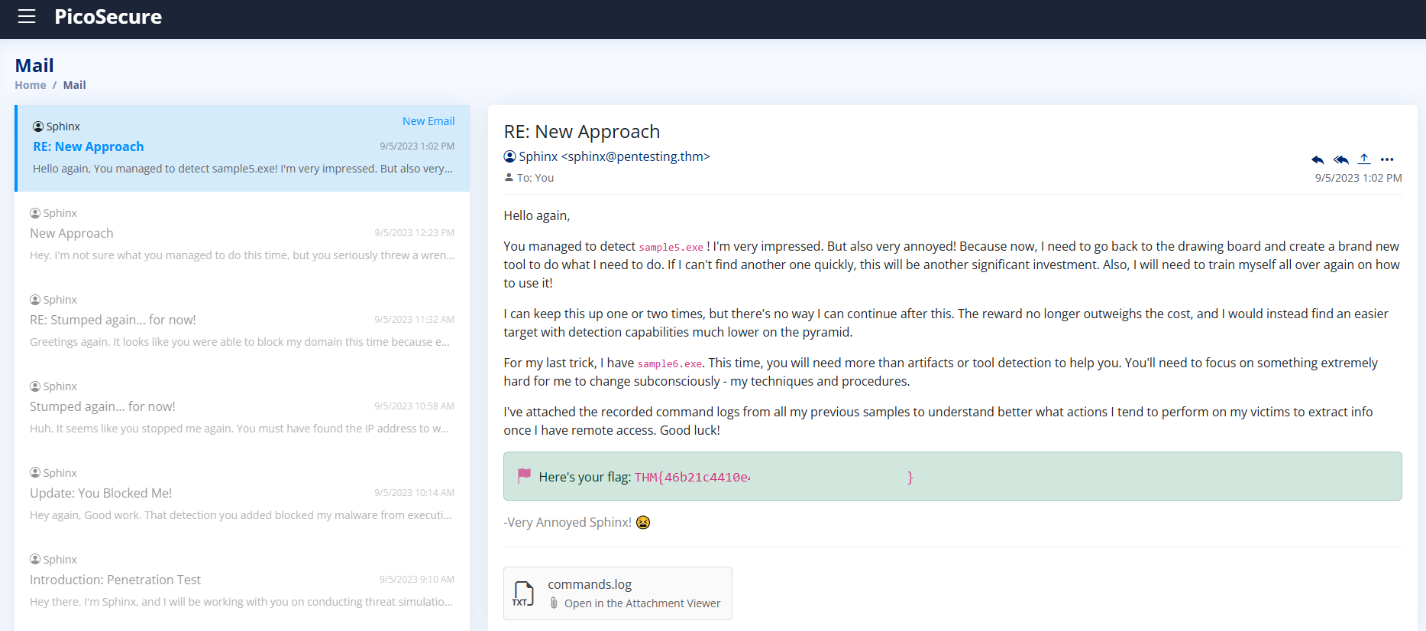


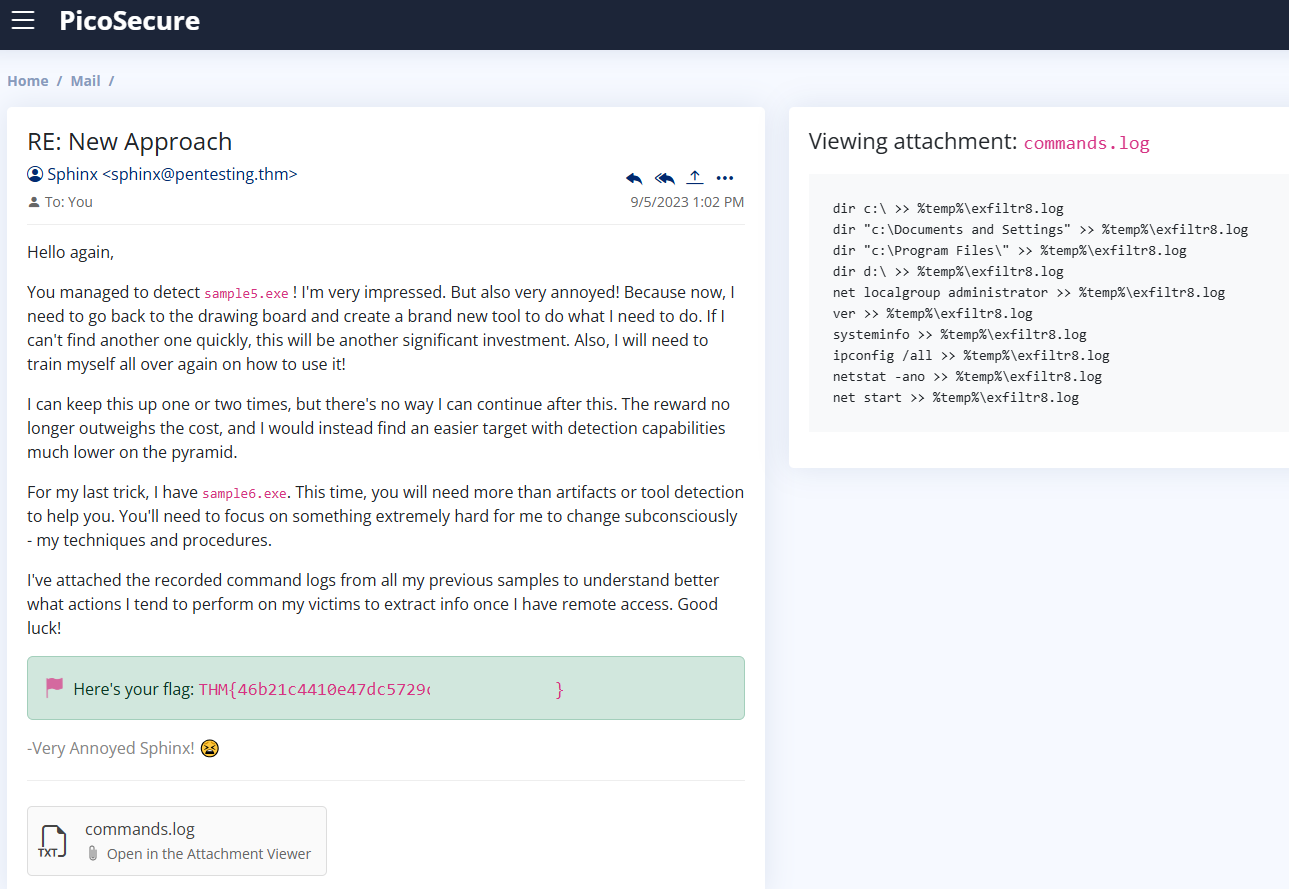
5. What is the fifth flag you receive after successfully detecting **sample5.exe**?



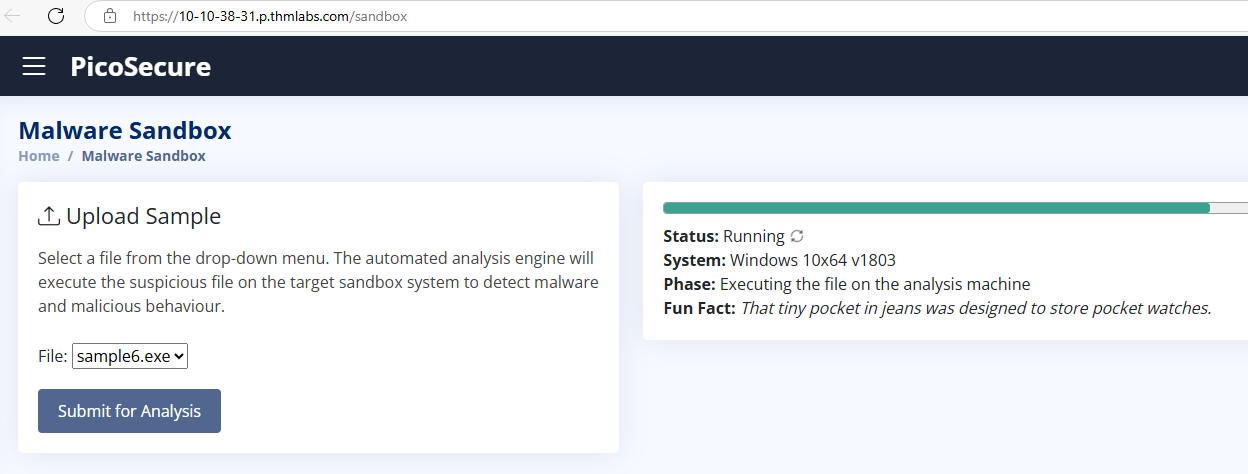


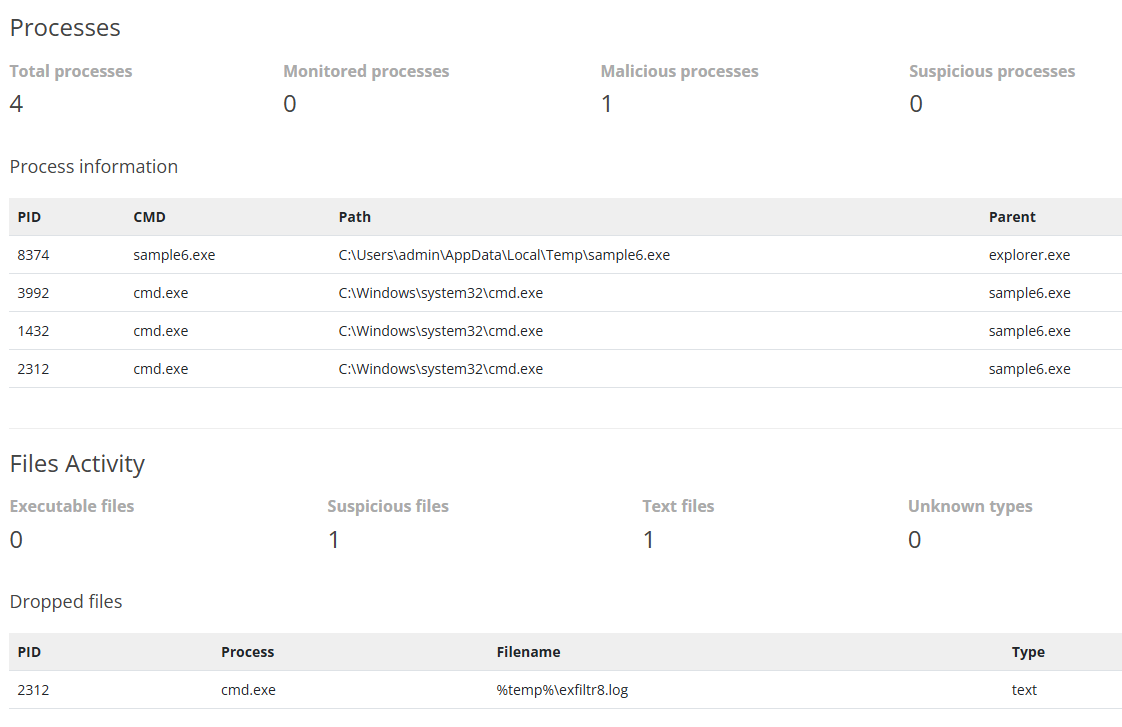


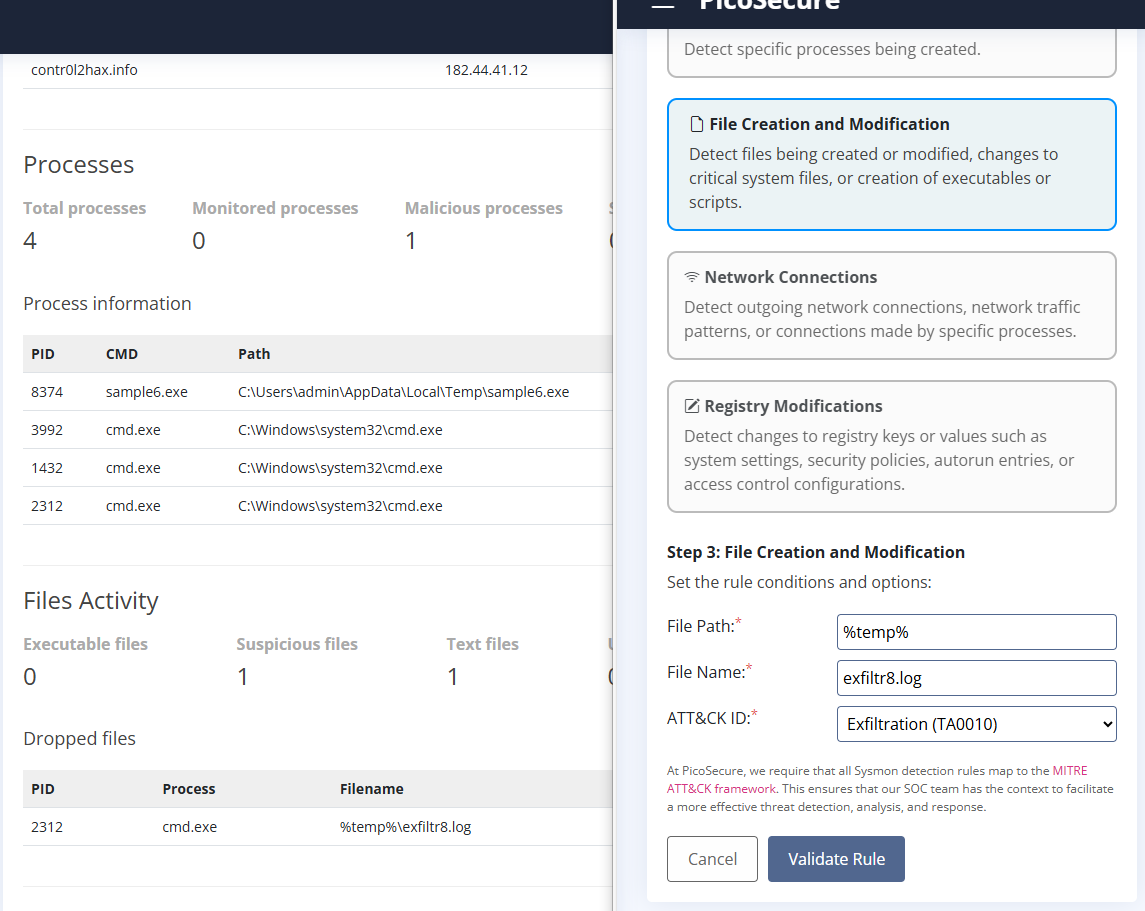




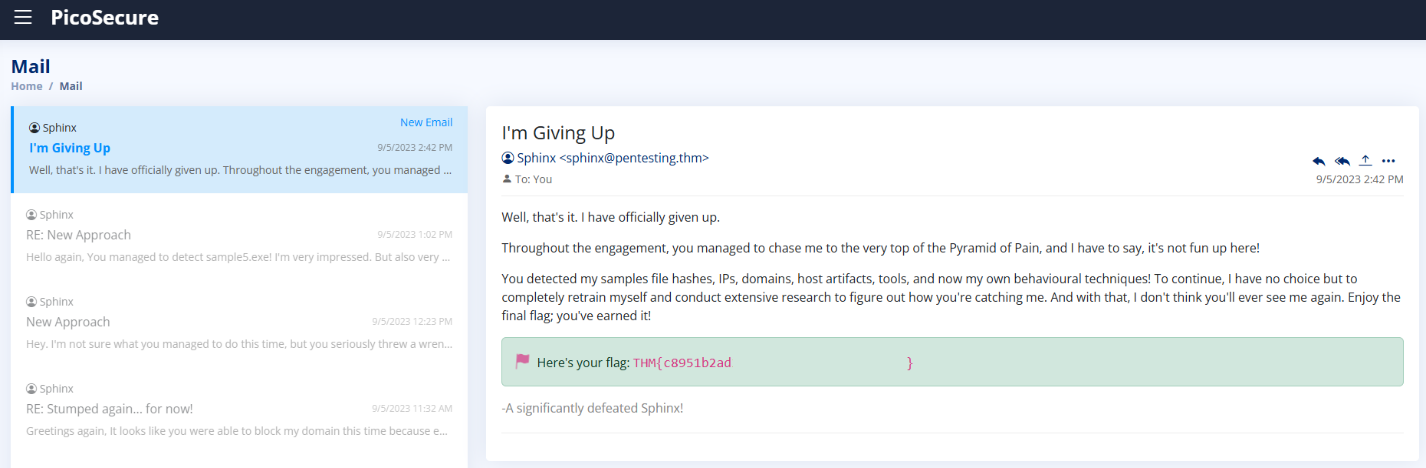
6. What is the final flag you receive from Sphinx?











This TryHackMe practice module was a lot of fun! It simulates real-world situations and tools that SOC analysts use daily. I really enjoyed how each level increased in difficulty, allowing me to be creative and crafty in my approach to detecting attacks.

* Attackers can employ a variety of techniques, and there are numerous methods for detecting and preventing these attacks!
* Having (and understanding) multi-layered defense is important!