Sherlock: Unit42

* + - Very Easy

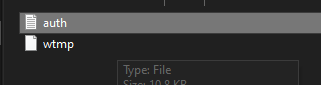
# Challenge Description :

**In this Sherlock, you will familiarize yourself with Sysmon logs and various useful EventIDs for identifying and analyzing malicious activities on a Windows system. Palo Alto's Unit42 recently conducted research on an UltraVNC campaign, wherein attackers utilized a backdoored version of UltraVNC to maintain access to systems. This lab is inspired by that campaign and guides participants through the initial access stage of the campaign.**

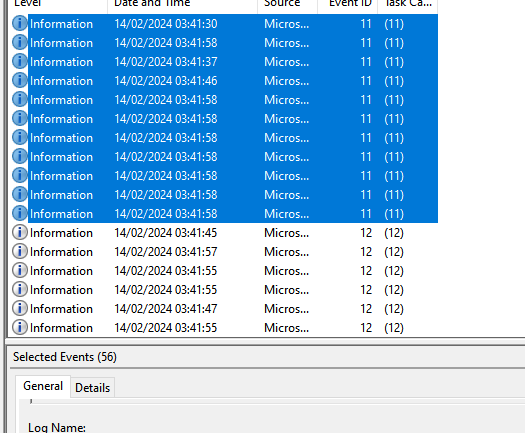
**Just Answer 8 Tasks**

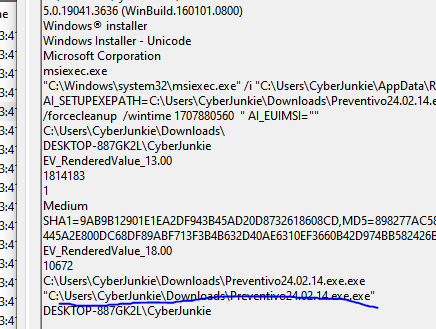
# Getting Down to the Task:

* **First download the ZIP file and extract the contents of the ZIP, after that start opening the log files based on the challenges description. We are only given a Windows event log to analyze.**

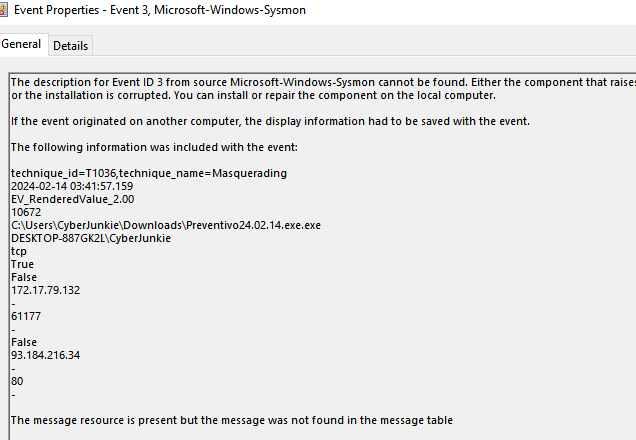
****

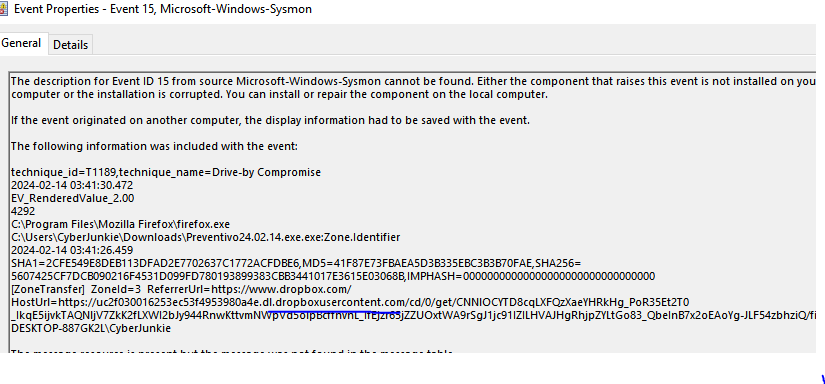
* **Opening it up with a Windows machine we can use the Event Viewer to filter it and go though each event.**
* **To answer Task 1 we can easily just select all the Events with the ID of 11 to get the answer.**

****

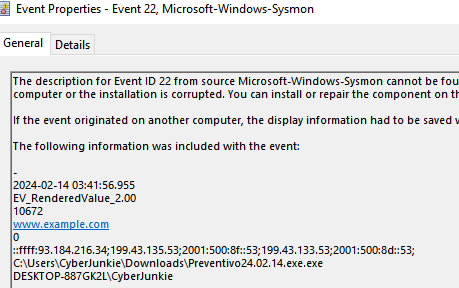
****

* **Going through the events we see a persistent .exe file that keeps appearing. This is the answer to Task 2**
* **Further down the events we see the answer to Task 7 and Task 3**

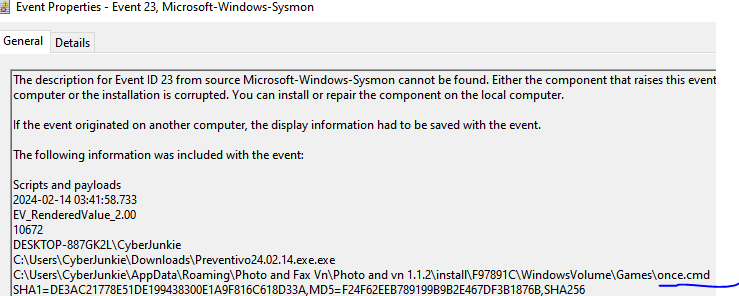
****

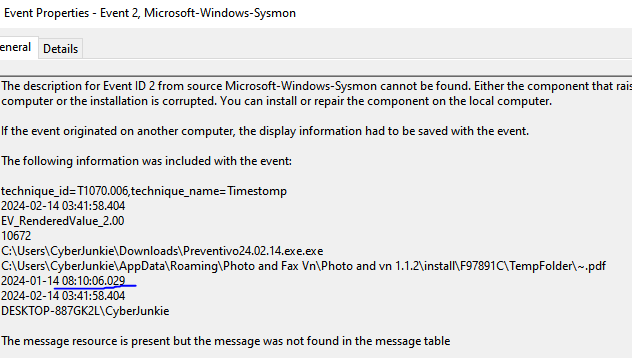
****

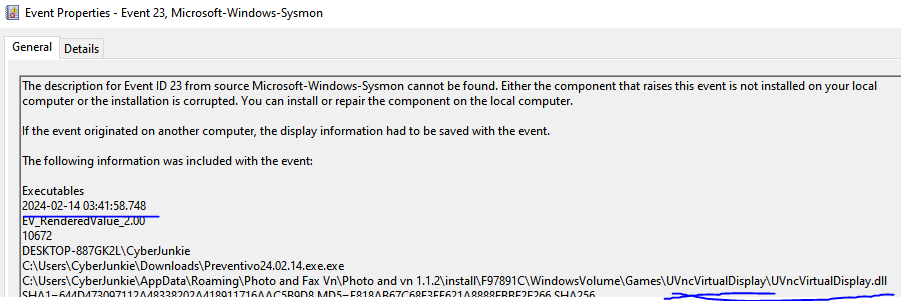
* **Getting to the rest of the Tasks done we continue going through the Event logs. We hit the answer to Task 6**

****

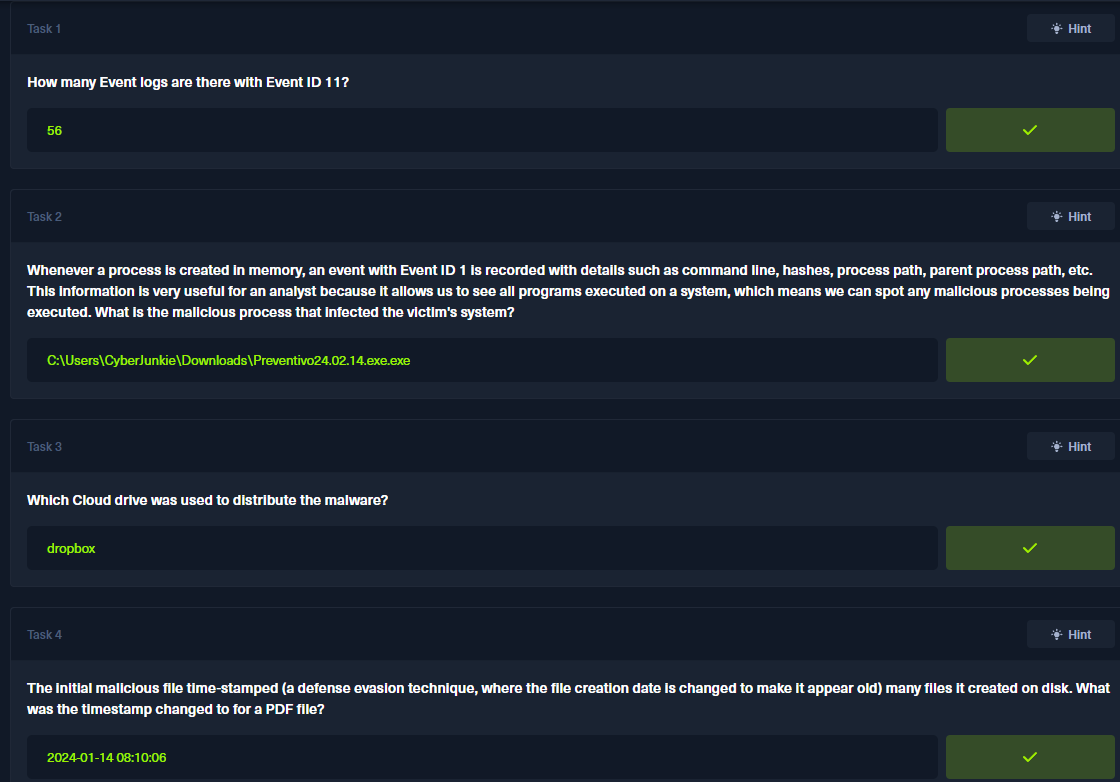
* **I finished the Events, but a quick double check shows I missed a good few like Task 8 ,Task 5 and Task 4**

****

****

****

* **This should be all the answers to the Tasks.**

****

****

**Sherlock Brutus - Birdo**