Mission Name

ForensicsTest

History Background

In the previous mission, ETHAN is arrested by Claire and Tarain. Claire and Ethan are going to work together to catch the SHAX hackers and both must be tested on their skills.

Technical High-Level Overview

Player must put in practice his knowledge about Virus and AntiVirus. For testing Claire, player will receive Windows Defender events. The goal of this mission is to catch threat virus name that was spread on Phaldra´s computer.

Short Mission Description

You´re going to be tested to ensure that virus knowledge is up to date. Please catch the threat name of the virus on Phaldra´s computer.

Mission Description

Player must put in practice his knowledge about Virus and AntiVirus. You´re going to be tested to ensure that virus knowledge is up to date. Please catch the threat name of the virus on Phaldra´s computer.

Location

SYLVARCON | EBAND DEPARTMENT - RECON HQ

Tools

- Event Log Explorer
- Evtx_dump

Questions

Which executable launched the alert on Windows Defender?

- Phaldra_test.exe

What is the event id related to the detection of the malware?

- 1117

Which is the name of Phaldra´s computer?

- DESKTOP-15P11BS

Hints

1. Use any application which allows you to open EVTX files
2. Use Event Log Explorer application
3. Search for the word “Ransomware”

Write Up

Linux Method - no root necessary

- apt install libevtx-utils
- apt install python3-evtx
- https://github.com/williballenthin/python-evtx
- Git clone https://github.com/williballenthin/python-evtx.git

Once installed, we search the script to search for the event id 1116 or 1117, and you will get name of the virus on Phaldra´s computer: Ransom:Win32/Stop.A!MTB

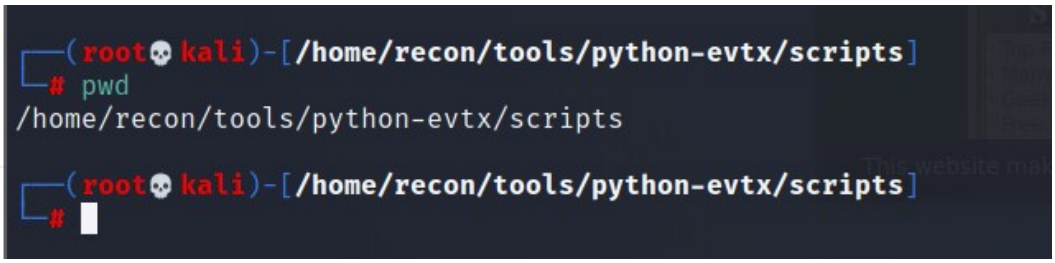

Figure 1

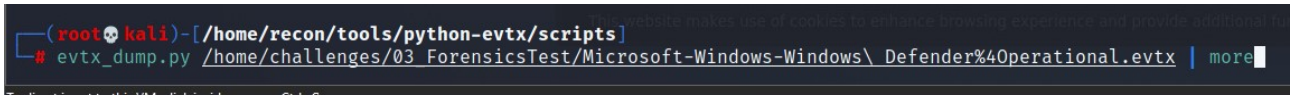

Figure 2

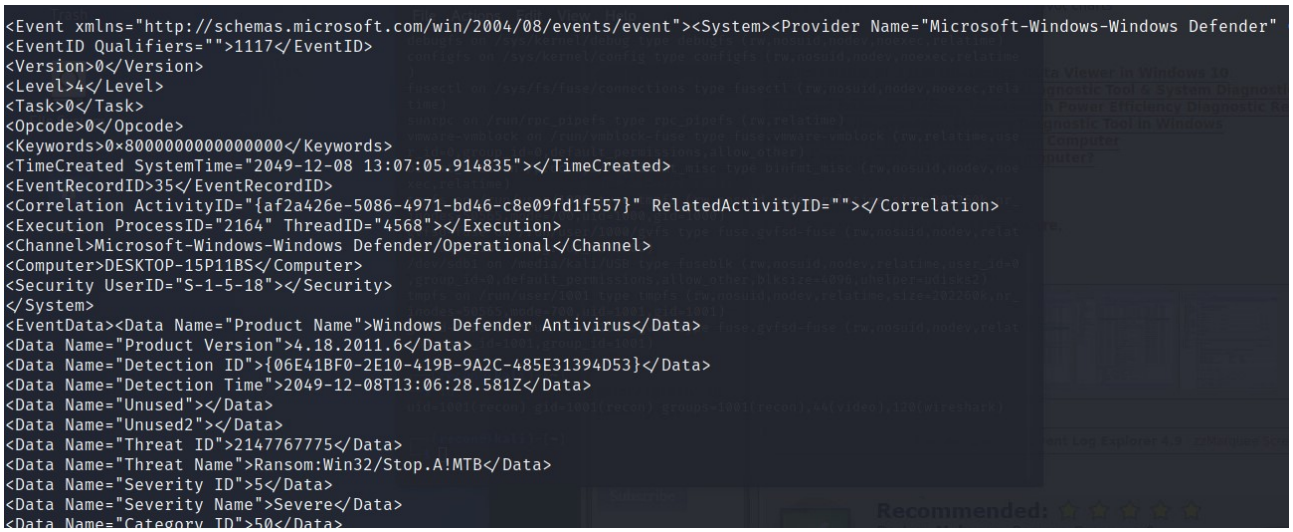

Figure 3

Windows Method

First of all, player should locate which tool can analyse, for example: Event Log Explorer

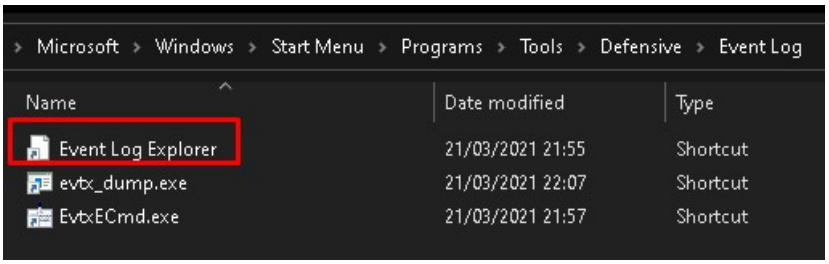

Figure 4

Later, player must analyse events to locate virus name on Phaldra´s Computer, opening EVTX file in this way:

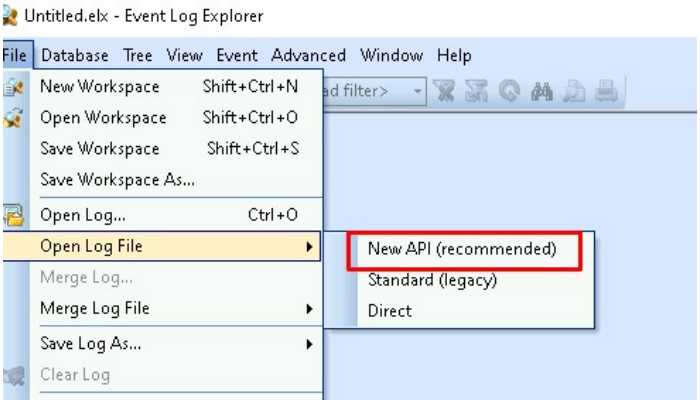

Figure 5

Once opened, search for the event id 1116 or 1117, and you will get name of the virus on Phaldra´s computer: Ransom:Win32/Stop.A!MTB

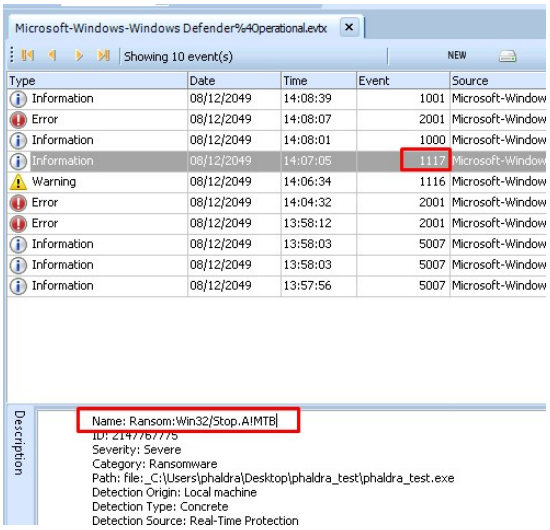

Figure 6

Flag Information

flag{Ransom:Win32/Stop.A!MTB}