IR Timeline Analysis -Tryhackme Writeup

MAGESH · Follow
3 min read · May 24, 2024

Learn about timeline analysis using various tools and scenarios.

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become a member.
https://tryhackme.com/signup?referrer=633819acb90069005f4fd623.

Link to the room https://tryhackme.com/r/room/dfirtimelineanalysis

Task 1:Introduction

In digital investigations, the more forensic data you have, the more complex things will be to process and analyze. It is, therefore, important to establish a sequence of events by extracting vital information and identifying a chronology of events that would have resulted in a breach or security incident. As forensic analysts, we delve deep into the intricate layers of digital artifacts to reconstruct the sequence of events, uncovering crucial details that shed light on the who, what, when, and how of a cyber incident. In this room, we embark on a journey to master the art of timeline analysis, learning how to wield tools like Log2Timeline with finesse to extract actionable intelligence from the vast sea of data contained within disk images.

Task 2:Basics of Timeline Analysis

> *When security events are reviewed sequentially against time, what is this known as?*

Ans: Timeline Analysis

> *When a file is created, what timestamp tag would it have?*

Ans: birth

> **Converting event timestamps into UTC can be described as?**

Ans: Time synchronization

Task 3:Artifact Acquisition & Processing

> *What specific data source provides detailed information regarding user interactions within a digital environment?*

Ans: File system metadata

Task 4:Timelines with Log2Timeline

> *What argument is used with Log2Timeline to indicate our output file?*

Ans: — storage-file

> *Based on the Jimmy_timeline.plaso file, how many event sources are parsed after running `pinfo.py` against the storage file?*

Ans: 4982

> **On the same timeline file, how many events were generated for the firefox_history?**

Ans: 50

> *Based on the B4DM755 timeline, what time was the interview.txt file created? (hh:mm:ss)*

Ans: 14:02:34

Create a Plaso file then a CSV file and investigate it.

Task 5:Timeline Analysis with Timesketch

> *How many data types were in the Jimmy Supertimeline sketch?*

Ans: 48

> *How many entries were in the EVTX Gap Analysis under the Jimmy Supertimeline?*

Ans: 34870

> *Which search engine did Jimmy Wilson use to search for "how to disappear without a trace?"*

Ans: bing

Search through the browser search records from the Analyzer.

> *What is the path of the program that was called to initiate Microsoft Antimalware Service?*

Ans: C:\Program Files\Microsoft Security Client\MsMpEng.exe

check the graph

Task 6:Timeline Analysis Practical

> *How many event sources were identified?*

Ans: 189100

Run pinfo.py against the timeline.

> *How many events were generated from the* `dpkg` *parser?*

Ans: 14718

> *How many total tags were set?*

Ans: 5408

psort.py -o null — analysis tagging — tagging-file tag_linux.txt Timeline_Challenge.plaso

> *What is the highest tagged element?*

Ans: login_failed

> *Under which username does the cronjob that executes app.py run?*

Ans: smokey

Check the syslog:cron:task_run data type on Timesketch

> *What is the hash of the successful SSH login with the PID 1669?*

Ans: a2407e0f3c80d01d2369f15e2b8aa279e790eaa0b1d20ab71cd35c2c7f5aee71

Check the syslog:ssh:login data type on Timesketch

THANK YOU FOR READING!!! ❤️ 💫

Follow

Written by MAGESH

36 Followers · 11 Following

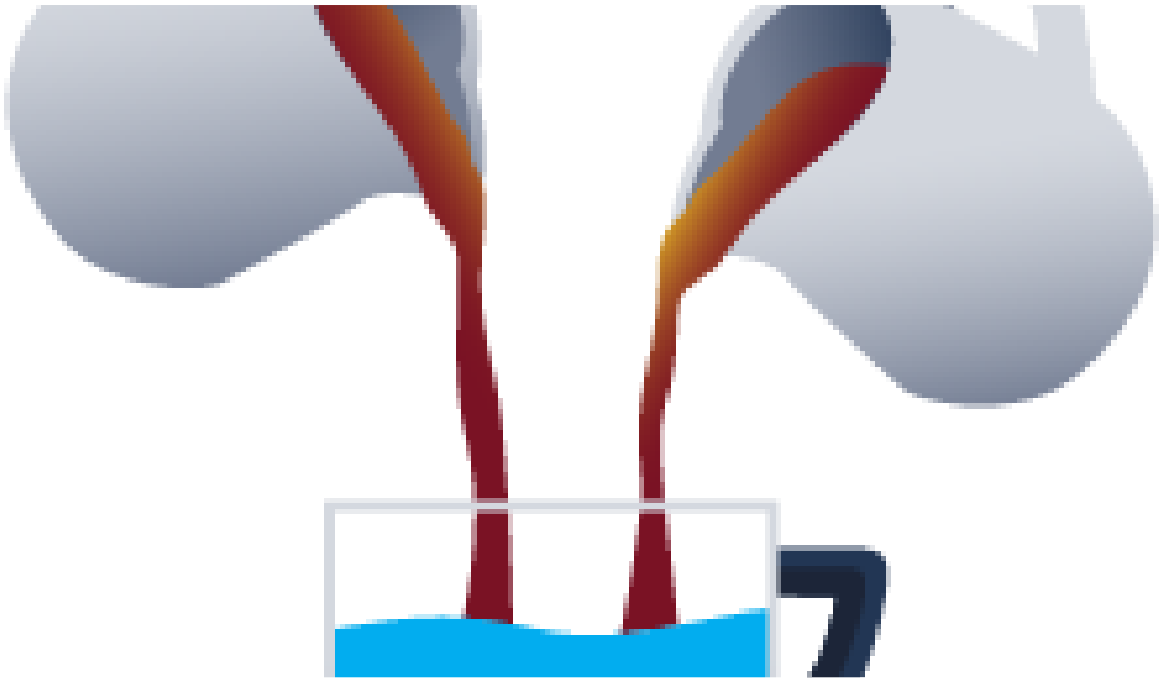
Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

MAGESH

OAuth Vulnerabilities-Tryhackme Walkthrough

Learn how the OAuth protocol works and master techniques to exploit it.

Sep 5, 2024 1

MAGESH

Windows PowerShell-Tryhackme Writeup

Discover the “Power” in PowerShell and learn the basics.

Oct 23, 2024 8

MAGESH

Race Conditions -Tryhackme Writeup

Learn about race conditions and how they affect web application security

Jun 13, 2024

See all from MAGESH

Recommended from Medium

Fritzadriano

Retracted—TryHackMe WriteUp

IInvestigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

Sep 4, 2024 50

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

Lists

Staff picks

793 stories · 1549 saves

Stories to Help You Level-Up at Work

19 stories · 909 saves

Self-Improvement 101

20 stories · 3184 saves

Productivity 101

20 stories · 2698 saves

IritT

Nmap — TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024

In System Weakness by Joseph Alan

TryHackMe Critical Write-Up: Using Volatility For Windows Memory Forensics

This challenge focuses on memory forensics, which involves understanding its concepts, accessing and setting up the environment using tools...

Jul 18, 2024 46 1

MAGESH

SigHunt-Tryhackme Writeup

You are tasked to create detection rules based on a new threat intel.

Oct 15, 2024

Haircutfish

TryHackMe Room—Summit

This is a subscribers only room on TryHackMe. It was created by TryHackMe. Here it the link to said room, TryHackMe Room—Summit.

Sep 12, 2024

See more recommendations