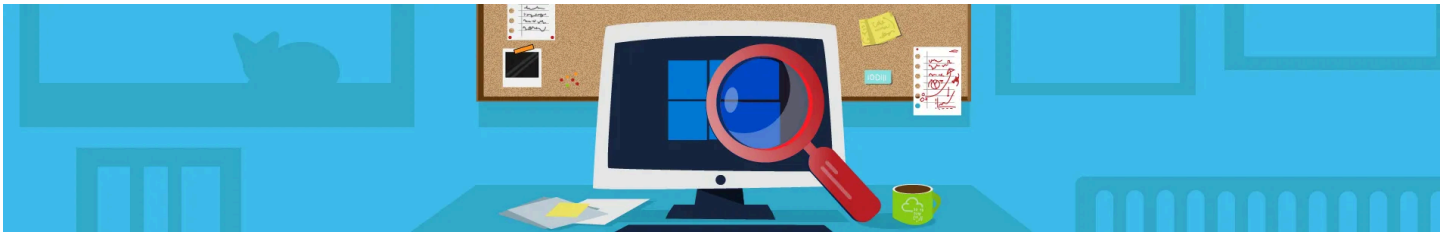
Secret Recipe-Tryhackme Writeup

MAGESH · Following
3 min read · Aug 21, 2024

Perform Registry Forensics to Investigate a case.

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/registry4n6

Task 1:Introduction

Storyline

Jasmine owns a famous New York coffee shop **Coffely** which is famous city-wide for its unique taste. Only Jasmine keeps the original copy of the recipe, and she only keeps it on her work laptop. Last week, James from the IT department was consulted to fix Jasmine's laptop. But it is suspected he may have copied the secret recipes from Jasmine's machine and is keeping them on his machine.

His machine has been confiscated and examined, but no traces could be found. The security department has pulled some important **registry artifacts** from his device and has tasked you to examine these artifacts and determine the presence of secret files on his machine.

NOTE: We'll use registry explorer tool and you can refer to the cheatsheet here.

Task 2:Windows Registry Forensics

What is the Computer Name of the Machine found in the registry?

> *What is the Computer Name of the Machine found in the registry?*

Ans: JAMES

SYSTEM\CurrentControlSet\Control\ComputerName \ComputerName

> *When was the Administrator account created on this machine? (Format: yyyy-mm-dd hh:mm:ss)*

Ans: 2021–03–17 14:58:48

SAM\Domains\Account\Users you'll have narrow columns when you click users, make sure to expand to view.

> *What is the RID associated with the Administrator account?*

Ans: 500

The **Relative Identifier (RID)** is a part of a Security Identifier (SID) that uniquely identifies a user or a group within a domain. In Windows, each user and group account has a SID, and the RID is the last portion of that SID.**RID** refers to the user ID in the SAM (Security Account Manager) database.

> *How many User accounts were observed on this machine?*

Ans: 7

chech for the names folder

> *There seems to be a suspicious account created as a backdoor with RID 1013. What is the Account Name?*

Ans: bdoor

> *What is the VPN connection this host connected to?*

Ans: ProtonVPN

Look for NetworkList in Software Hive

> *When was the first VPN connection observed? (Format: YYYY-MM-DD HH:MM:SS)*

Ans: 2022–10–12 19:52:36

> *There were three shared folders observed on his machine. What is the path of the third share?*

Ans: C:\RESTRICTED FILES

search for shared in find and you'll see a folder named shared

> *What is the Last DHCP IP assigned to this host?*

Ans: 172.31.2.197

SYSTEM\CurrentControlSet\Services\Tcpip \Parameters\Interfaces

we already have a hint 172.**.*.***

> *The suspect seems to have accessed a file containing the secret coffee recipe. What is the name of the file?*

Ans: secret-recipe.pdf

Recent Files: NTUSER.DAT\Software\Microsoft\Windows \CurrentVersion\Explorer\RecentDocs

> *The suspect ran multiple commands in the run windows. What command was run to enumerate the network interfaces?*

Ans: pnputil /enum-interfaces

NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer.

> *In the file explorer, the user searched for a network utility to transfer files. What is the name of that tool?*

Ans: netcat

NTUSER.DAT\Software\Microsoft\Windows \CurrentVersion\Explorer\WordWheelQuery

The Wordwheelquery is a registry key associated with the search history in Windows, specifically within the context of the Windows Explorer

> *What is the recent text file opened by the suspect?*

Ans: secret-code.txt

NTUSER.DAT\Software\Microsoft\Windows \CurrentVersion\Explorer\RecentDocs

> *How many times was Powershell executed on this host?*

Ans: 3

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Go through each key until we find one with a count, view to the right and scroll for powershell. same applies for the next questions as well

> *The suspect also executed a network monitoring tool. What is the name of the tool?*

Ans: wireshark

> *Registry Hives also notes the amount of time a process is in focus. Examine the Hives. For how many seconds was ProtonVPN executed?*

Ans: 343

convert minutes into seconds

> *Everything.exe is a utility used to search for files in a Windows machine. What is the full path from which everything.exe was executed?*

Ans: C:\Users\Administrator\Downloads\tools\Everything\Everything.exe

THANK YOU FOR READING!!! ❤️ 💫

Registry Tryhackme Digital Forensics

Following

Written by MAGESH

40 Followers · 11 Following

Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH

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

In System Weakness by MAGESH

Boogeyman 3-Tryhackme Writeup

The Boogeyman emerges from the darkness again.

Sep 2, 2024

MAGESH

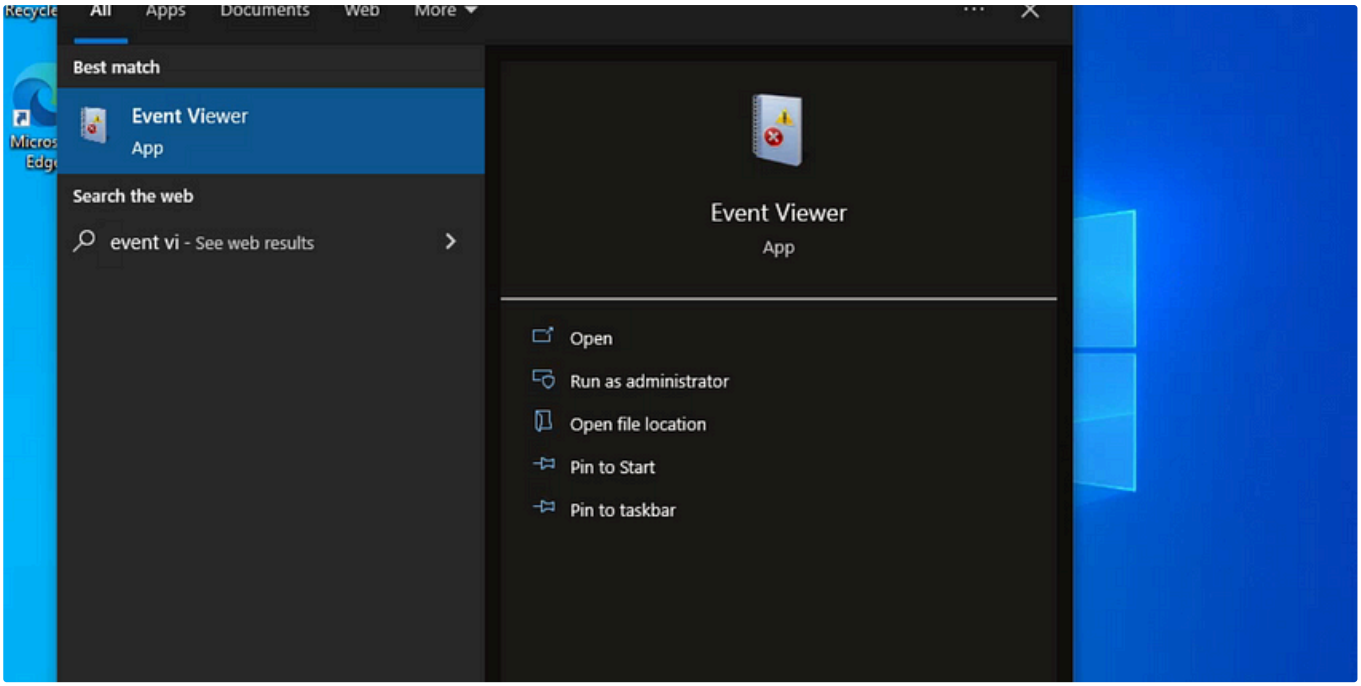
Hashing Basics-Tryhackme Writeup

Learn about hashing functions and their uses in password verification and file integrity checking.

Oct 25, 2024 2

See all from MAGESH

Recommended from Medium



AYNUR BALCI

Windows Event

Analyze the event with ID 4624, that took place on 8/3/2022 at 10:23:25. Conduct a similar investigation as outlined in this section and...

Oct 31, 2024 11

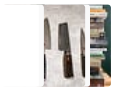
In System Weakness by MAGESH

Boogeyman 3-Tryhackme Writeup

The Boogeyman emerges from the darkness again.

Sep 2, 2024

Lists

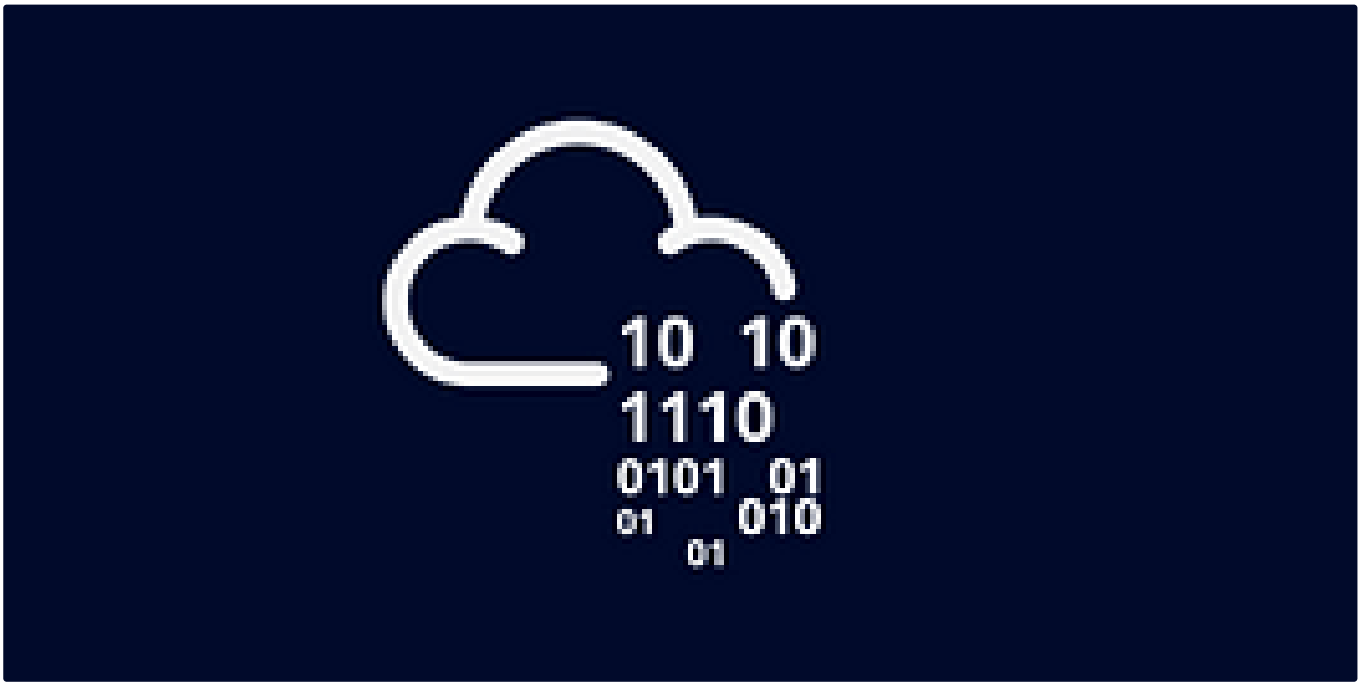


Staff picks
798 stories · 1566 saves

Stories to Help You Level-Up at Work
19 stories · 915 saves

Self-Improvement 101
20 stories · 3212 saves

Productivity 101
20 stories · 2714 saves



In T3CH by Axoloth

TryHackMe | Brute Force Heroes | WriteUp

Walkthrough room to look at the different tools that can be used when brute forcing, as well as the different situations that might favour...

Oct 3, 2024 51

IritT

Introduction to SIEM — Cyber Security 101-Security Solutions -TryHackMe Walkthrough

An introduction to Security Information and Event Management.

Nov 12, 2024

Jawstar

Advent of Cyber '24 Side Quest Anwers { T 1 }

T1: Operation Tiny Frostbite

Jan 6 2

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50