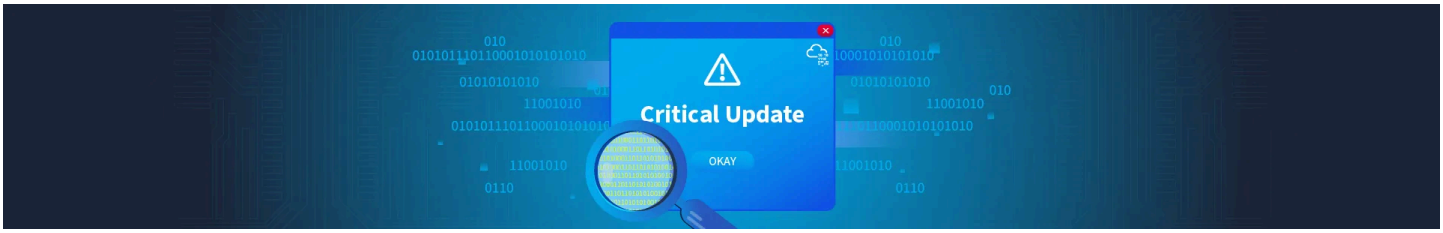
Critical-Tryhackme Writeup

MAGESH · Follow
2 min read · Aug 21, 2024

Acquire the basic skills to analyze a memory dump in a practical scenario.

This is a Free room. If you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become a member.
https://tryhackme.com/signupreferrer=633819acb90069005f4fd623



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

Task 1:Introduction

In this room, we'll learn how to extract essential information and artifacts when performing a memory forensic task in a compromised machine using the Windows OS. First, we'll learn basic memory forensics concepts before setting up our working environment. Next, we'll learn how to get basic information about the compromised target and how to search for suspicious activity. Finally, we will extract interesting data that may help us identify potential malicious actors.

Task 2:Memory Forensics

> *What type of memory is analyzed during a forensic memory task?*

Ans: RAM

> *In which phase will you create a memory dump of the target system?*

Ans: Memory Acquisition

Task 3:Environment & Setup

> *Which plugin can help us to get information about the OS running on the target machine?*

Ans: Windows.info

> *Which tool referenced above can help us take a memory dump on a Linux OS?*

Ans: LIME

> *Which command will display the help menu using Volatility on the target machine?*

Ans: vol -h

Task 4:Gathering Target Information

> *Is the architecture of the machine x64 (64bit) Y/N?*

Ans: y

> *What is the Verison of the Windows OS*

Ans: 10

> *What is the base address of the kernel?*

Ans: 0xf8066161b000

Task 5:Searching for Suspicious Activity

> *Using the plugin “windows.netscan” can you identify the IP address that establish a connection on port 80?*

Ans: 192.168.182.128

grep 80 along with cmd

> *Using the plugin "windows.netscan," can you identify the program (owner) used to access through port 80?*

Ans: msedge.exe

> *Analyzing the process present on the dump, what is the PID of the child process of critical_updat?*

Ans: 1612

grep for 1648 (pid of critical_updat)

> *What is the time stamp time for the process with the truncated name critical_updat?*

Ans: 2024–02–24 22:51:50.000000

Task 6:Finding Interesting Data

> *Analyzing the "windows.filescan" output, what is the full path and name for critical_updat?*

Ans: C:\Users\user01\Documents\critical_update.exe

> *Analyzing the "windows.mftscan.MFTScan" what is the Timestamp for the created date of important_document.pdf?*

Ans: 2024–02–24 20:39:42.000000

> *Analyzing the updater.exe memory output, can you observe the HTTP request and determine the server used by the attacker?*

Ans: SimpleHTTP/0.6 Python/3.10.4

THANK YOU FOR READING!!! 💔💫

Digital Forensics | Tryhackme | Memory Analysis

Follow

Written by MAGESH

39 Followers · 11 Following

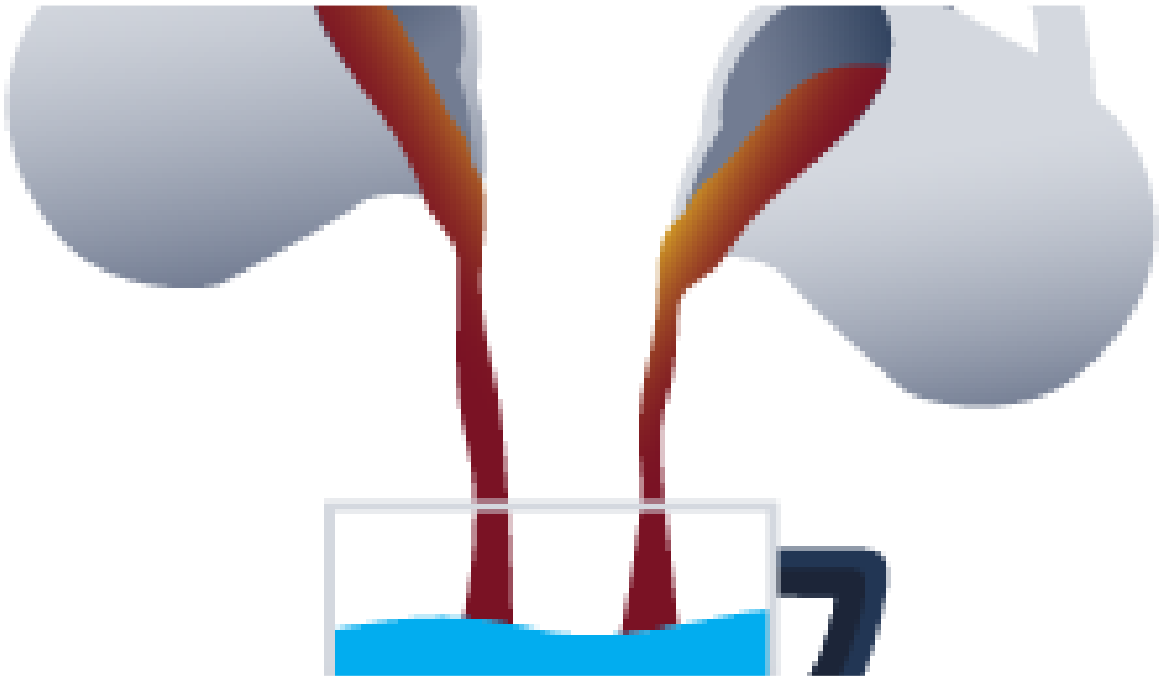
Cybersecurity | Tryhackme

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.

MAGESH

Windows PowerShell-Tryhackme Writeup

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

Oct 23, 2024 8

MAGESH

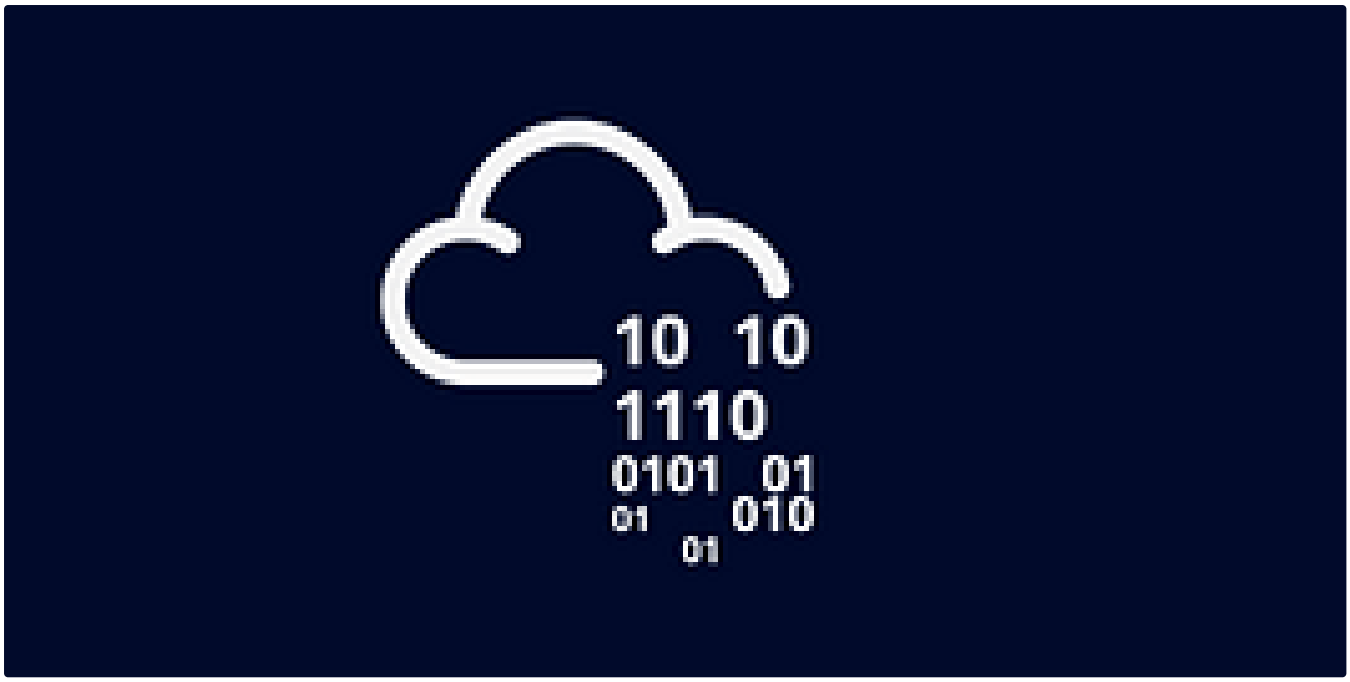
Race Conditions -Tryhackme Writeup

Learn about race conditions and how they affect web application security

Jun 13, 2024 1

See all from MAGESH

Recommended from Medium



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

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

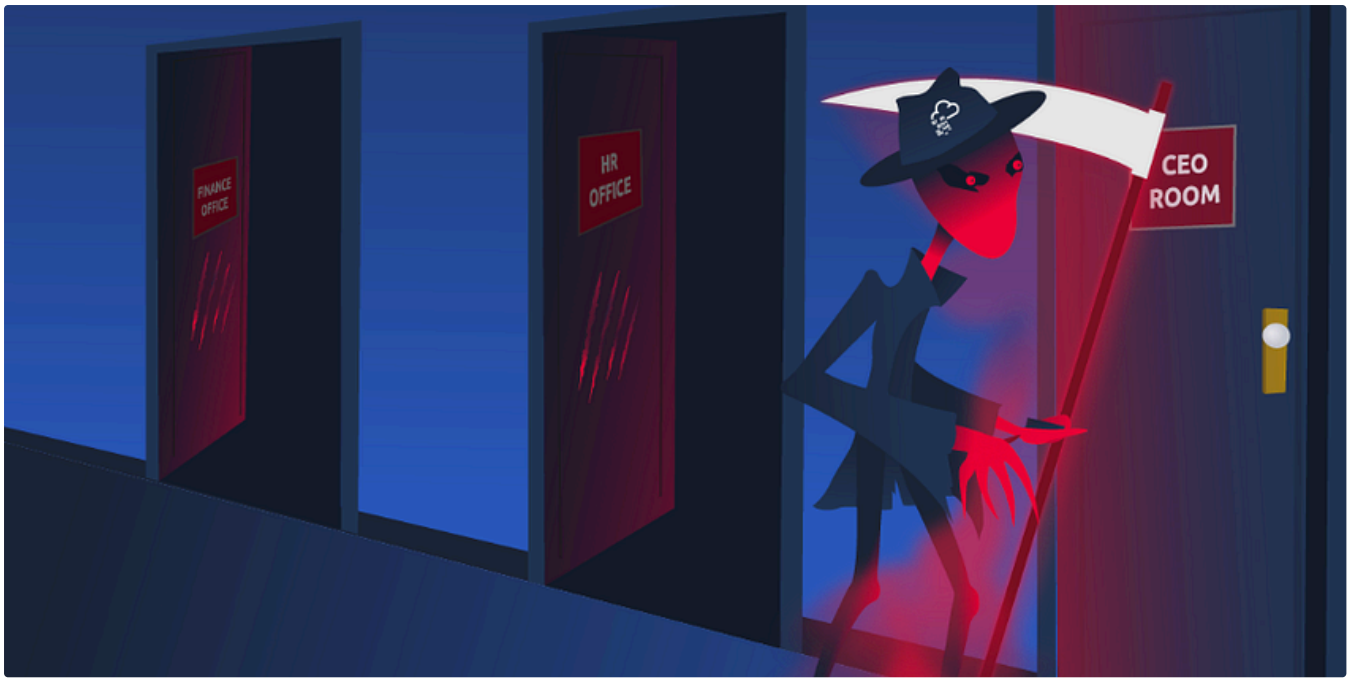
20 stories · 2714 saves

IritT

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

An introduction to Security Information and Event Management.

Nov 12, 2024

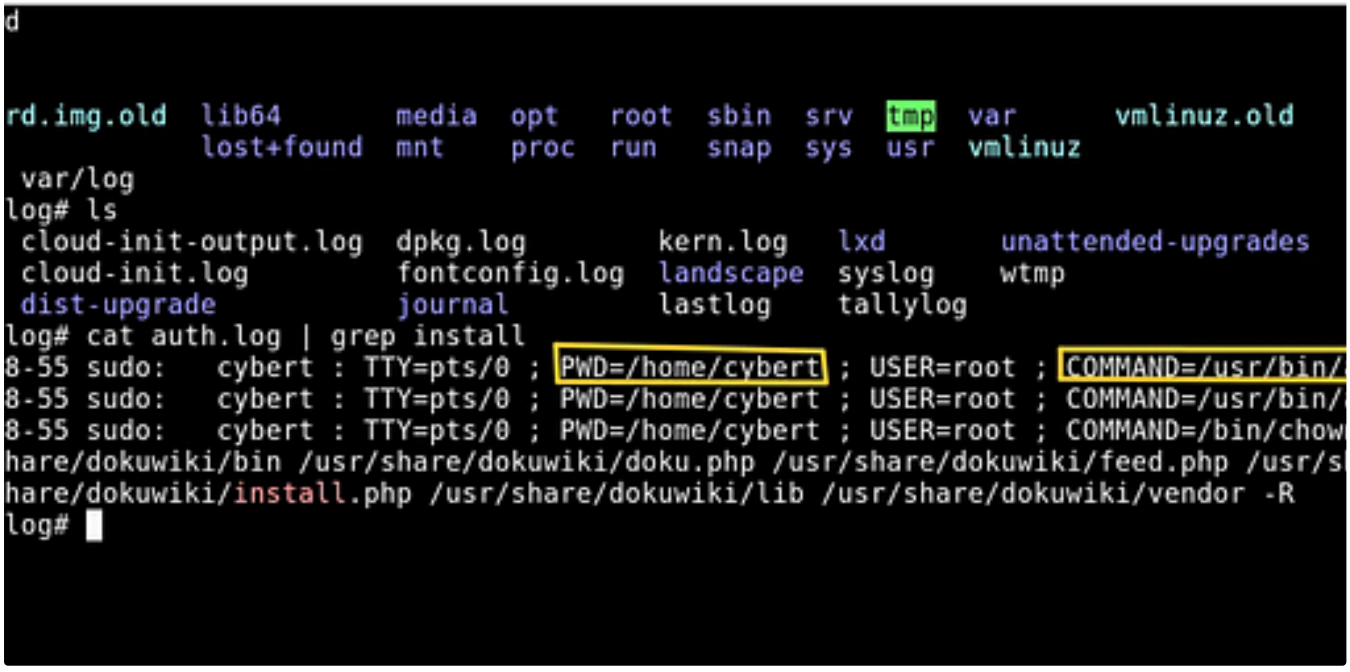


Drew Arpino

TryHackMe—Boogeyman 3 Challenge Walkthrough

A Domain Forensic Investigation using Kibana

Jan 6 1



Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

Oct 22, 2024

In InfoSec Write-ups by Momal Naz

TryHackMe | Simple CTF | Walkthrough | By HexaHunter

Step-by-step guide to solving the Simple CTF room for beginners.

Sep 9, 2024 5

See more recommendations