Capture The Flag (CTF) Report

# Challenge Title:

[Very Easy] Caving

# Introduction

The "[Very Easy] Caving" challenge is part of the Business CTF 2024 hosted by Hack The Box. This challenge falls under the Forensics category and is designed to test participants' ability to analyze and extract information from given data files. The objective is to identify and retrieve specific flags hidden within the provided datasets using various forensic tools and techniques.

This report will detail the tools used, the methodology employed, the results obtained, the lessons learned, the challenges faced, and the overall conclusion drawn from participating in this CTF challenge.  
  
The challenge can be accessed via the following GitHub repository: [Business CTF 2024 - Forensics - [Very Easy] Caving.](https://github.com/hackthebox/business-ctf-2024/tree/main/forensics/%5BVery%20Easy%5D%20Caving)

# Tools Used

For the "[Very Easy] Caving" challenge, the following tools were utilized to analyze and extract the required information:

* **Chainsaw:**
  + **Description:** Chainsaw is a command-line utility designed for quick triage and extraction of critical forensic artifacts from Windows event log files.
  + **Usage:** Utilized to parse through Windows event logs efficiently, allowing for the identification and extraction of relevant data points pertinent to the challenge.
* **Findstr**
  + **Description**: findstr is a command-line tool in Windows that searches for strings within files.
  + **Usage**: Used to search through text files for specific strings and patterns, aiding in the identification of the required flag within the provided data files.
* **CyberChef**
  + **Description**: CyberChef, often referred to as "The Cyber Swiss Army Knife," is a web-based tool that provides a wide range of functions for data manipulation, analysis, and encryption.
  + **Usage**: This was used to decode the final encoded string containing the Flag.

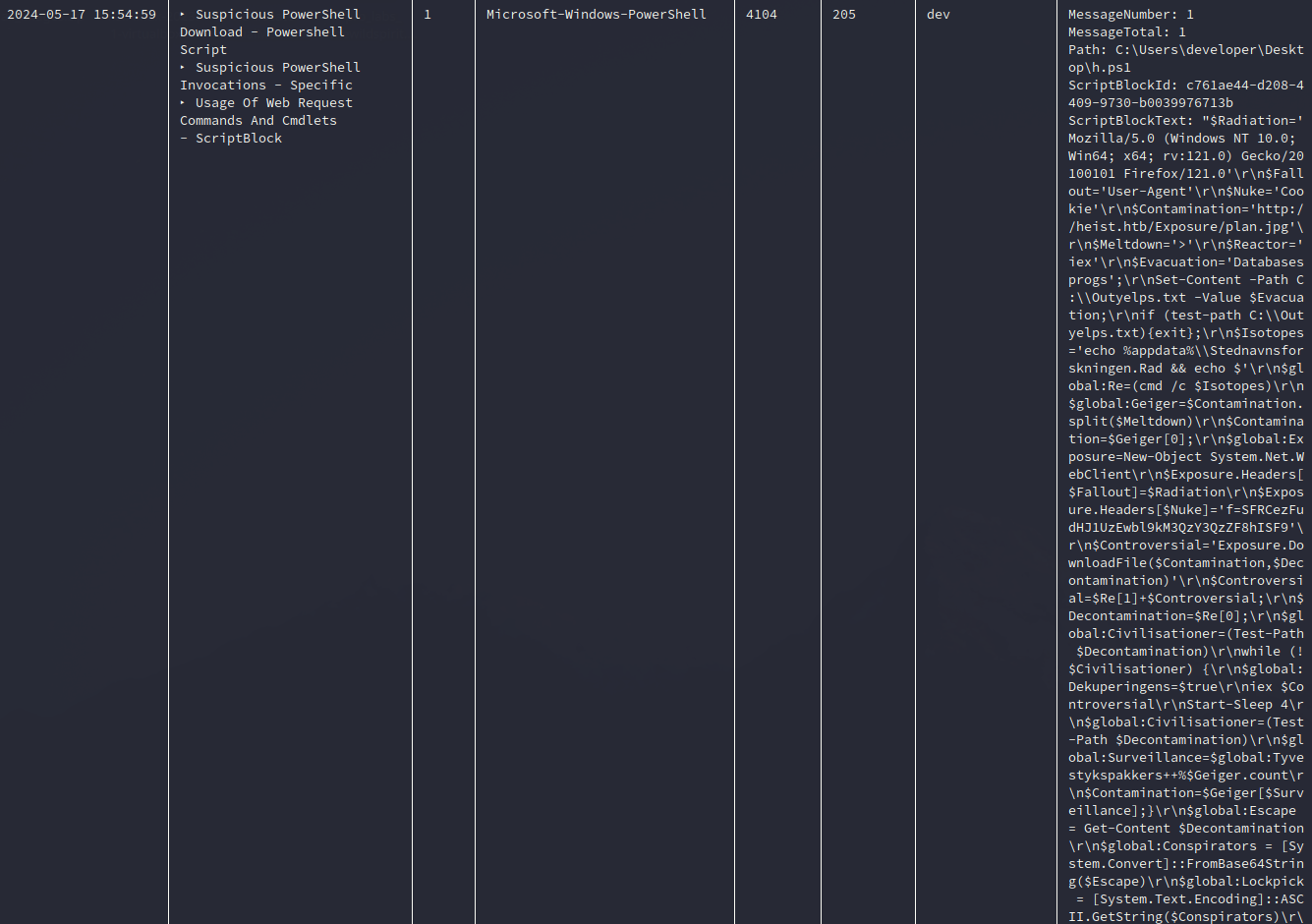
These tools were instrumental in efficiently navigating and analyzing the data provided in the challenge, allowing for a thorough forensic investigation and the successful retrieval of the hidden flag.

# Methodology & Results

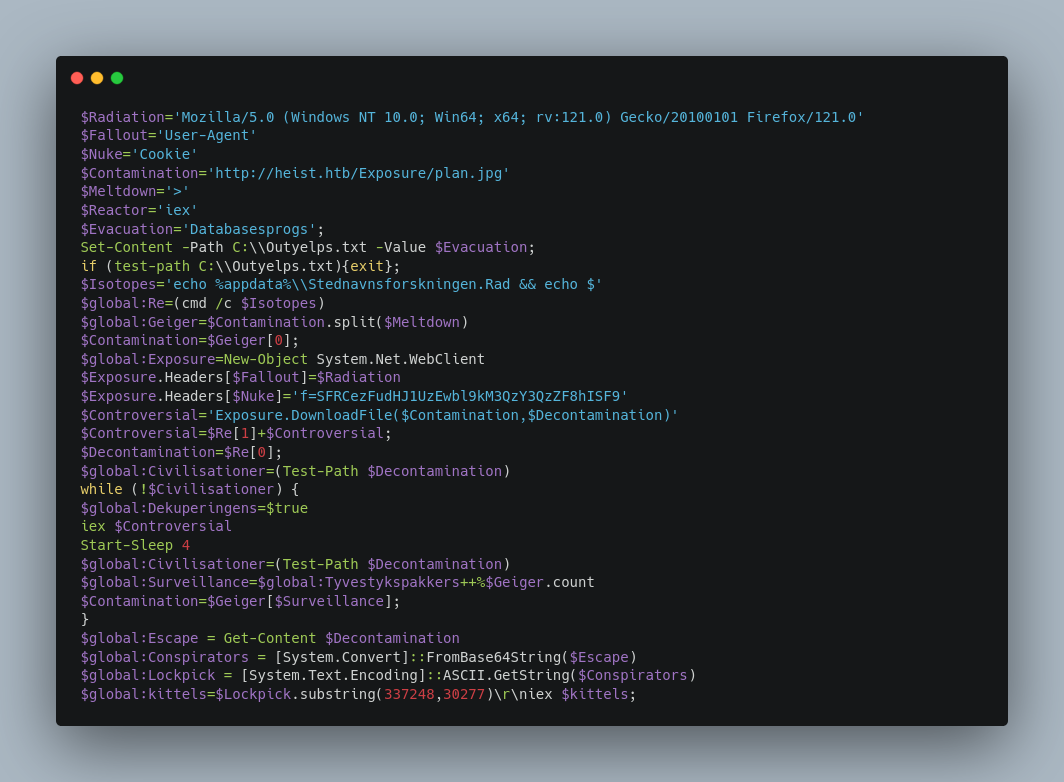
In the "[Very Easy] Caving" challenge, the following methodology was employed to analyze and extract the required information from the provided data files:

1. **Identification of Data Type**:
   * Upon examining the provided files, it was identified that we were dealing with Windows Event Logs. These logs are crucial for forensic analysis as they contain records of various activities and events on a Windows system.
2. **Parsing Event Logs with Chainsaw**:
   * **Tool Used**: Chainsaw
   * **Explanation**: The **hunt** command within Chainsaw was used to parse the Windows event logs. Chainsaw is efficient for quickly triaging and extracting forensic artifacts from event log files.
   * **Sigma Rules**: To enhance the parsing process, Sigma rules were utilized. These rules were downloaded from the SigmaHQ repository ([Sigma Rules GitHub](https://github.com/SigmaHQ/sigma)). Sigma rules are standardized format rules for writing detections, making it easier to identify suspicious activities within the logs.
   * **Output**: The results of the parsing process were outputted to a CSV file, which allowed for easier examination and further analysis.
   * **Command Executed**:  
     chainsaw.exe hunt -s "Z:\CTF Shared Folder-2\tools-and-add-ons\sigma-rules\sigma" -m mappings/sigma-event-logs-all.yml "Z:\CTF Shared Folder-2\business-ctf-2024-main\business-ctf-2024-main\forensics\[Very Easy] Caving\release\forensics\_caving\Logs" --full --output output\_folder –csv
3. **Searching for Suspicious Activities**:
   * **Tool Used**: findstr
   * **Command**: The **findstr** command was used to search through the CSV file for any mentions of the word "Suspicious". The command helps in quickly filtering out relevant entries from large text files.
   * **Result**: The search returned one result that contained the word "Suspicious", indicating a potential lead for further investigation.
   * **Command Executed**:  
     Findstr “Suspicious” sigma.csv
4. Reviewed the suspicious Script:
   * After analysing the script it was identifed that when downloading the next stage from http://heist.htb/Exposure/plan.jpg, the attacker adds two headers. The first is the user-agent and the second one is a custom cookie which looks like this f=SFRCezFudHJ1UzEwbl9kM3QzY3QzZF8hISF9. Let's decode it.
   * Using Cyberchef, this Base64 encoded string was decoded to HTB{Redacted}

# Images

Chainsaw Results:  


Malicious Script:



# Conclusion & Lessons Learned

Overall, I enjoyed this CTF – It allowed me to gain knowledge into the Chainsaw tool and the different options I can leverage to search Windows Event Logs.

I also gained a better understanding into Sigma rules, which are essentially the Windows event log equivalent to Yara/Snort Network rules.