# **CTF Topic: Malware Analysis**



# **Introduction**



Hybrid Analysis is a powerful tool used for automated malware analysis, combining static and dynamic analysis techniques. This tool helps in identifying, analysing, and reporting potential threats in software, providing a comprehensive understanding of malware behaviour.

# **Tools and requirements**

**Sample Malware File**: Download a benign malware sample for analysis.

**Internet Connection**: Required for accessing Hybrid Analysis and downloading files.

**Virtual Machine**: Optional but recommended for safe malware analysis.

# **Link (File)**

**Malware sample:** <https://www.mediafire.com/file/5dgavjehrsfbmsa/Randomfile.exe/file>

**Hybrid Analysis Platform:** <https://www.hybrid-analysis.com/>

# 

# **Scenario**

You have received a suspicious file that you suspect to be malware. Your task is to use Hybrid Analysis to investigate the file, identify its behaviour, and determine the potential threat it poses. This will help you understand how to use Hybrid Analysis for real-world malware analysis.

# **Process to Perform**

**Step 1: Upload the File**: Go to the Hybrid Analysis website and upload the malware sample file.

**Step 2: Analyze the File**: Once uploaded, Hybrid Analysis will perform static and dynamic analysis on the file. Shouldn't have to add email on it just click on i agree and i am not a robot and continue.

**Step 3: Review the Report**: Examine the generated report to understand the behaviour and characteristics of the file.

# **Let's Begin The Challenge**

# **Question 6**

Flag 1: What is the name of the file you upload for analysis on Hybrid Analysis?

Answer: sandy.exe.bat

Flag captured.

Flag 2: Based on the Hybrid Analysis report, what is the overall threat level of the file?

Answer: 35/100

Flag Captured.

FLag 3: What is the SHA256 of the given malware file?

Answer: [fcb942ca20c50949a1f7e5b10dbe7b8eb66a6301357c602b41081df5408d6323](https://www.hybrid-analysis.com/search?query=context:fcb942ca20c50949a1f7e5b10dbe7b8eb66a6301357c602b41081df5408d6323&block_redirect=1)

Flag Captured.

# **Hint**

