# **CTF Topic: Hybrid Analysis**

# **1. Introduction**



A Trojan, also known as a Trojan horse, is a type of malware that disguises itself as legitimate software or code to gain unauthorized access to a computer or network. It is a type of malicious software that is designed to trick users into installing or running it, often by pretending to be a harmless file or program.

# **2. Tools and requirements**

Mediafire

HybridAnalysis

# **3. Scenario**



You got some random message on facebook claiming a reward for you. If you want to check whether it's malicious or not you want to check and perform the process as mentioned in the process to perform.

# **4. Process to follow while performing CTF**



Step 1: Download the sandy.exe.bat from the Link\_1 given below.

Step 2: Go to the Link\_2 and paste it.

Link\_1: <https://www.mediafire.com/file/6yhi1b7x91gquat/sandy.exe.bat/file>

Link\_2: <https://hybrid-analysis.com/>

# 

# **5. Let's Begin The Challenge**

# **Question**

**Flag 1: What the file was?**

**Answer: trojan**

**Flag Captured.**

**Flag 2: How much percentage does it detect?**

**Answer: 4%**

**Flag Captured.**

# **Hint**

