# **CTF Topic: Cuckoo Sandbox**



# **Introduction**



Malware analysis is a crucial aspect of cybersecurity, involving the examination of malicious software to understand its functionality, origins, and potential impact. Cuckoo Sandbox is a powerful open-source tool designed for automated malware analysis. It allows security researchers and analysts to safely execute suspicious files in a controlled environment to observe their behaviour and gather essential forensic data.

# **Tools and requirements**

Cuckoo Sandbox (<https://cuckoo.cert.ee/> )

Basic understanding of malware analysis concepts

# **Link (File)**

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

# **Scenario**

You are tasked with analysing a suspicious file obtained from a phishing campaign. The file appears to be a Trojan that has been observed targeting financial institutions.

# **Process to Perform**

Step 1: Open the Cuckoo Sandbox using the given link(<https://cuckoo.cert.ee/>).

Step 2: Submit the downloaded malware sample to Cuckoo Sandbox for analysis.

Step 3: Analyse the generated reports and identify key indicators of compromise (IOCs).

# **Let's Begin The Challenge**

# **Question**

**Question 1:** What is the MD5 of the given malware file?

Answer:

Hint : df16f0aea1e99def77d77d014668026a

Flag captured.

**Question 2:** What is the CRC32 of the given malware file?

Answer:

Hint:EF2D5D07

Flag Captured.

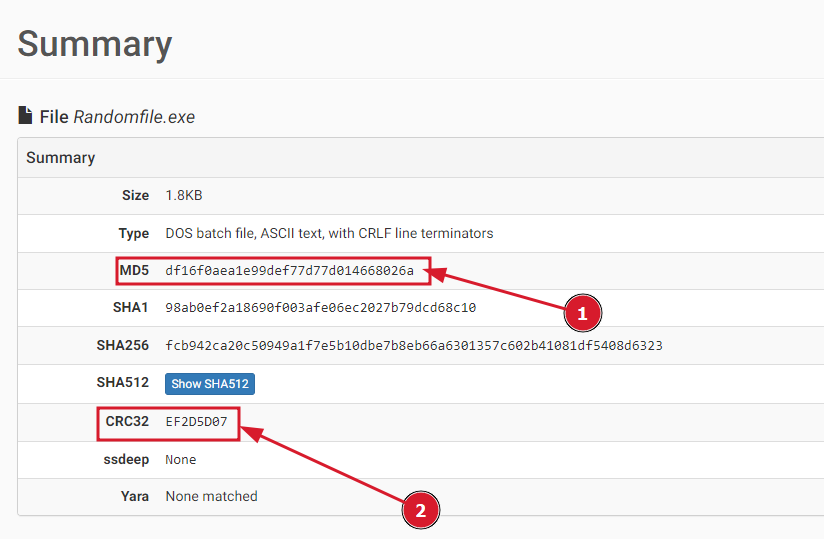
**Question 3:** What is the cvss score of the given malware file?

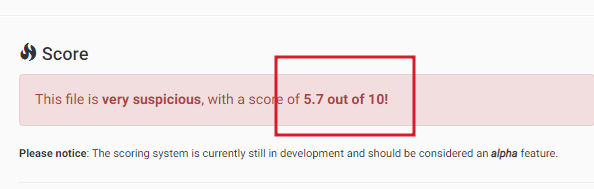
Answer:

Hint: 5.7

Flag captured.

# **Hint**



****