Malware Analysis Basics – Practical 2 Report

Objective

The objective of this practical was to perform **basic malware analysis techniques** on a Windows executable using both **static** and **dynamic analysis** approaches. The aim was to understand how analysts inspect executable files without execution and compare the findings with sandbox-based execution results.

Tools & Environment Used

- **REMnux Linux VM** – for static malware analysis
- **Hybrid Analysis (Online Sandbox)** – for dynamic analysis
- **Sample File** – `calc.exe` (benign Windows executable)

Methodology & Implementation

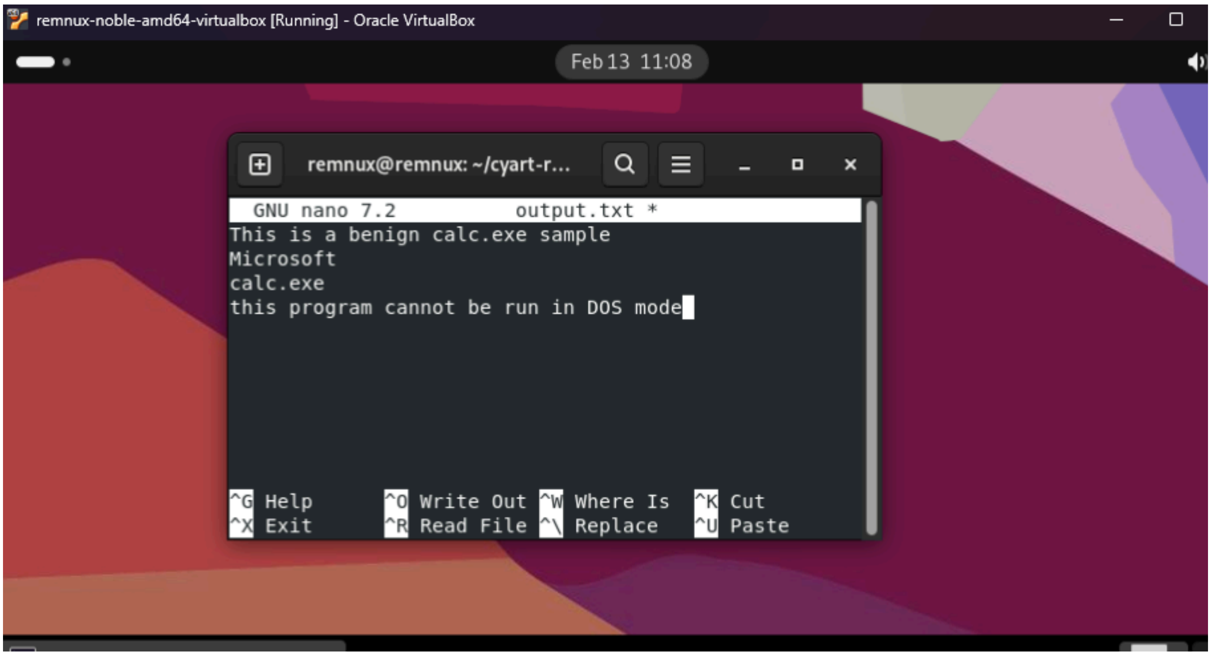
Static Analysis (REMnux)

Static analysis was performed without executing the file to ensure safety.

Command used:

```
strings calc.exe > output.txt
```

This command extracted all human-readable ASCII and Unicode strings from the executable and stored them in `output.txt` for further inspection.



remnux-noble-amd64-virtualbox [Running] - Oracle VirtualBox
Feb 13 11:08
remnux@remnux: ~/cyart-r...

```
  GNU nano 7.2              output.txt *
This is a benign calc.exe sample
Microsoft
calc.exe
this program cannot be run in DOS mode
```

^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste

Findings:

- System DLL references
- File paths and system messages
- Application-related readable text

This helped understand the internal structure of the executable without running it.

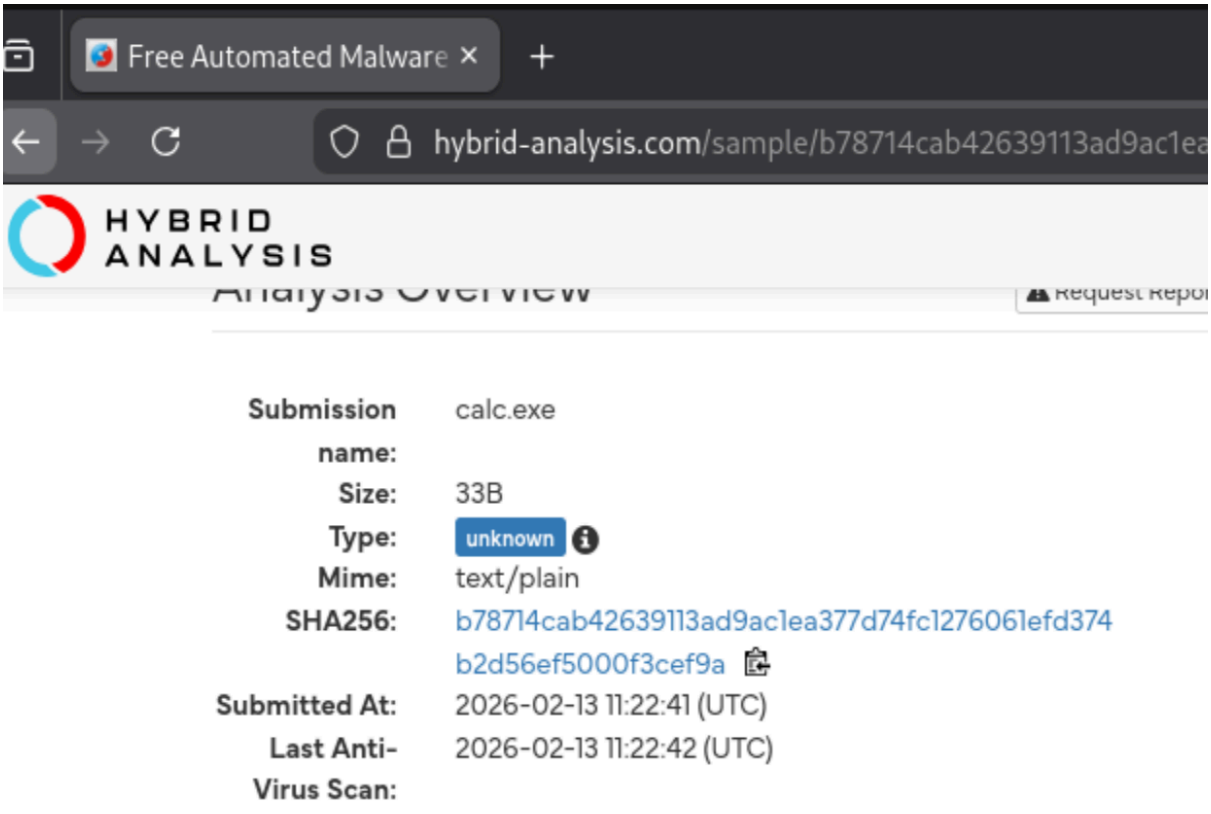
Dynamic Analysis (Hybrid Analysis)

The same executable was uploaded to **Hybrid Analysis**, which executes the file in a controlled sandbox environment.

Observed behavior:

- Legitimate calculator-related execution
- No suspicious registry or network activity
- File classified as **SAFE**

This confirmed that the executable did not show malicious behavior at runtime.



Submission name: calc.exe

Size: 33B

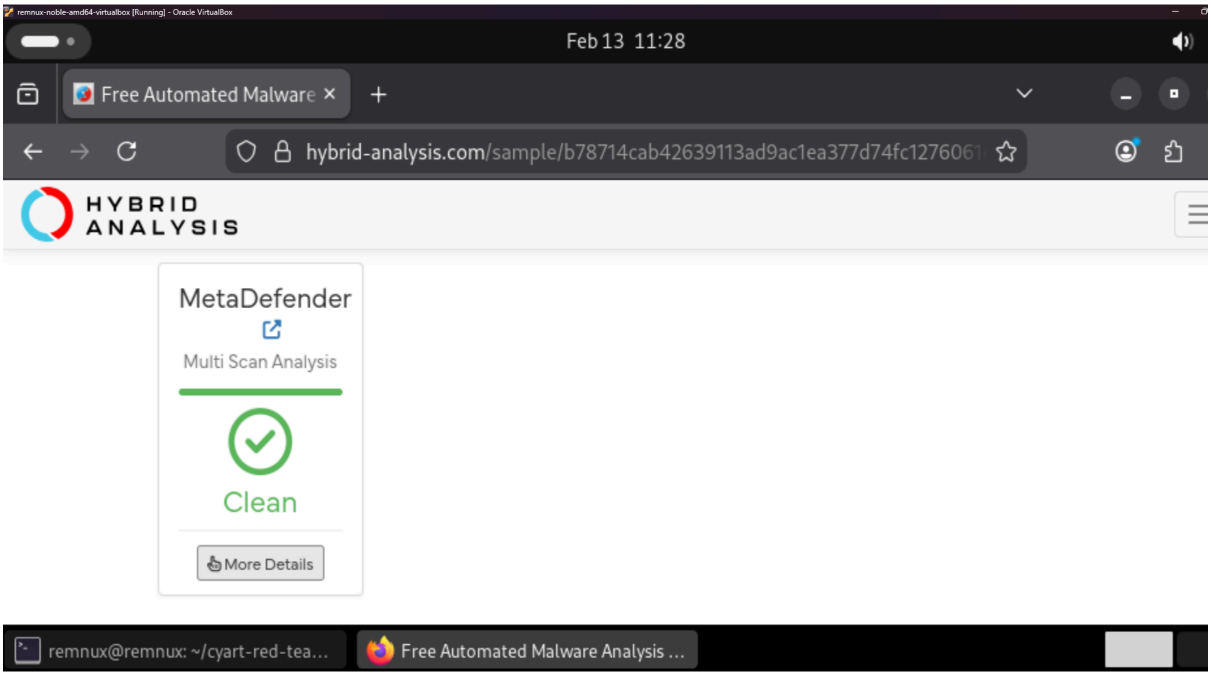
Type: unknown

Mime: text/plain

SHA256: b78714cab42639113ad9ac1ea377d74fc1276061efd374b2d56ef5000f3cef9a

Submitted At: 2026-02-13 11:22:41 (UTC)

Last Anti-Virus Scan: 2026-02-13 11:22:42 (UTC)


remnux-noble-amd64-virtualbox [Running] - Oracle VirtualBox
Feb 13 11:28
Free Automated Malware ×
hybrid-analysis.com/sample/b78714cab42639113ad9ac1ea377d74fc1276061
HYBRID ANALYSIS
More Details
remnux@remnux: ~/cyart-red-tea...
Free Automated Malware Analysis ...

MetaDefender

Multi Scan Analysis

Clean

Errors Faced & Troubleshooting

Issue Encountered	Resolution
Confusion between static and dynamic analysis	Understood that static analysis does not execute files
No terminal output after running `strings`	Learned that output redirection (`>`) saves results to a file
File marked SAFE in Hybrid Analysis	Understood that benign files are valid for methodology demonstration

Learning Outcomes

Through this practical, I learned:

- The difference between **static** and **dynamic** malware analysis
- How to safely analyze executables without execution
- How sandbox environments classify file behavior
- Why benign samples are used for training and exams
- How to document findings professionally

Conclusion

This practical successfully demonstrated the core concepts of malware analysis using safe tools and techniques. Static analysis provided insight into the internal structure of the executable, while dynamic analysis confirmed its legitimate behavior. The exercise strengthened foundational malware analysis skills and improved understanding of real-world analyst workflows.