Malware Analysis (REMnux)

1. Objective

The objective of this task is to perform basic static and dynamic malware analysis on a benign executable using REMnux and Hybrid Analysis.

2. Tools Used

- REMnux
- strings
- peframe
- Hybrid Analysis

3. Static Analysis

Static analysis was performed without executing the file.

strings Analysis

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

peframe Analysis

```
peframe calc.exe > peframe-report.txt
```

4. Dynamic Analysis

The executable was uploaded to Hybrid Analysis for behavioral inspection.

Observed Behaviors

- File metadata inspection
- API call analysis

- No malicious behavior detected (benign sample)

5. Comparison Summary

Tool	Observation
strings	Extracted readable strings
peframe	PE structure analysis
Hybrid Analysis	Behavioral analysis

6. Conclusion

The analysis demonstrated the difference between static and dynamic malware analysis techniques and how they complement each other in malware investigations.