

DESIGNING A SANDBOX ENVIRONMENT FOR MALWARE TESTING: A QUALITATIVE STUDY OF MALWARE DETECTION AND ANALYSIS IN CYBER FORENSICS

Dominik Kania - BSc (Hons) Computing (Computer Networks and Cyber Security) | Email: 1702026@student.uwtsd.ac.uk

Introduction

The main challenge in malware research is gathering meaningful information without putting devices of the study authors or systems at jeopardy. This study sought to provide new information and pave the way for future research in the field of malware analysis, by comparing results from different malware samples. This work introduced a use of sandbox environment created specifically for this project, which takes advantage of hybrid malware analysis. This isolated setting was configured in a way that a host operating system is always safeguarded from malware propagation.

Aim and Objectives

The primary aim of the research is to identify different forms of malware and scrutinise their behaviour in a controlled environment. The following are the main objectives of the research:

- To conduct extensive research into malware analysis.
- To develop a secure and isolated testing environment for malware analysis.
- To detect and analyse malware activity in a virtualized environment.
- To perform an experiment in a sandbox environment to explore possible risks.
- To investigate and assess the results of the experiment.
- To document and discuss the experimental data.

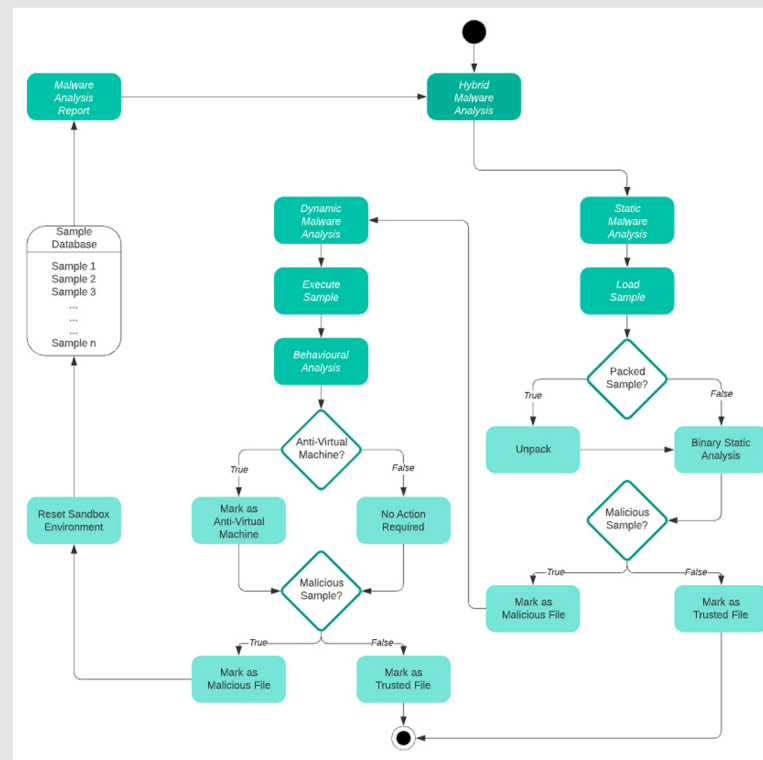
Research

The following are some of the most notable findings presented in the literature review:

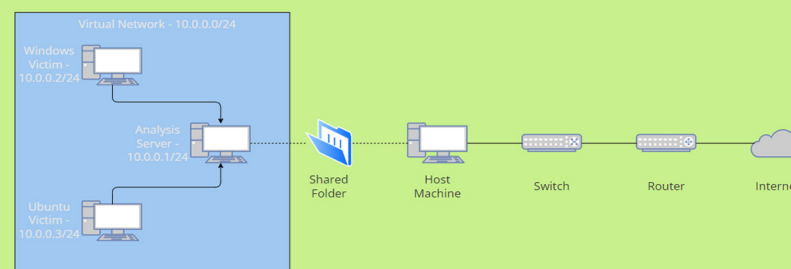
- Malware research has long been a source of contention in the realm of cybersecurity.
- Testing is indispensable for pinpointing the provenance of an attack, rebuilding operational settings, and discouraging malicious activities by identifying commonalities in digital information.
- The purpose of information acquisition is to gather strong material that can be analysed to produce persuasive and reliable responses to the questions addressed.

Design and Implementation

The project began with the creation of a sandbox environment, which was subsequently safeguarded and prepared for malware testing. This environment made use of a virtual network independent from the host system and the Internet. In addition, numerous malware analysis tools were installed on each virtual machine, making it possible for the study of malicious samples. This arrangement is presented using a real-world use case in which the behaviour of the most well-known computer viruses is examined.



Network Diagram

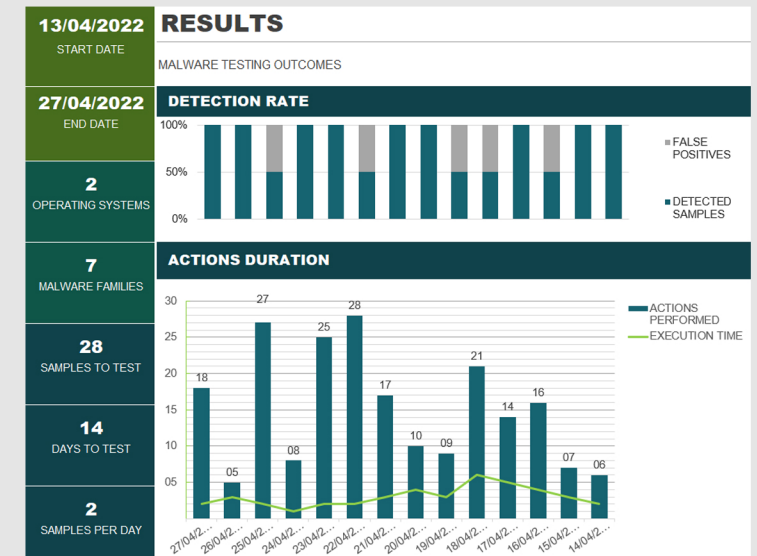


Results

The security of the created sandbox environment was evaluated, and no vulnerabilities were discovered. Various forms of malware files were deployed, with some of the more sophisticated instances capable of eluding testing systems if incorrectly designed.

The hybrid malware analysis approach utilized in this experiment was adopted to increase the adequacy and accuracy of existing research studies. The suggested technique exceeds the conventional independent tools in producing more accurate findings and detecting every malicious file in the system.

The effectiveness of this method was tested for a malware assault that occurred in a setting that simulated the real-world scenario. The findings of the investigation demonstrate that the proposed tools will be effective for identifying and evaluating various forms of malware.



Conclusion

This experiment has demonstrated the various kinds of techniques and methods for analysing a specific malware. Numerous studies have shown that a particular piece of malware cannot be evaluated with a single solution. The findings from the experiment demonstrate that each malware analysis solution employs a unique parameter and approach to examine the detrimental script. Finally, the aim of the project was achieved through the project objectives that were successfully completed.