Digital forensic analysis on malware infected virtual machines

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Author: Caleb Thomas; 2304862@student.uwtsd.ac.uk

Supervisor: Carlene Campbell

School of
Applied Computing

Introduction

With the increase of the dependency of technology digital forensics is becoming more prevalent now than ever with the uptake in technology being used in crime and it being carried out over cyberspace. Digital forensics is used in investigations to recover and analyse data to use as evidence.

Aim

Evaluate the impact of contaminated malware and retrieve any recoverable data with the use of digital forensic tools.

Objectives

- Research five digital forensic tools that will be efficient to recover malware systems.
- Simulate two malware infected virtual machines.
- Extract any information that can be recovered.
- Analyze the data recovered from the infected system.
- Produce a forensic report to showcase the findings.
- Document and write-up final project report for submission.

Research Overview

Digital forensic tools:

FTK Imager: A Free tool that Is able to create an exact copy of hard drive to allow for inspection without worry of the original copy being altered. [1]

Wireshark: An open-source tool used to capture and analyse packets on a network. Including live packets of data on a network allowing for real time monitoring. [2]

Methods of analysis

- **Dynamic Analysis:** The process of activating malware in a controlled environment allowing for malware to be observed.
- **Static Analysis:** The process of using tools to analyse the malware to analyse it without activating it allowing, so it's structure can be understood

For the experiment, both kinds of analysis were carried out to provide more variety to the results [3]

Design and implementation

Oracle VirtualBox was used to host the four victim virtual machines and an analysis virtual machine. The OS for the analysis machine was Kali Linux and the OS for the victim machines are Windows 11, Windows Server 2022, Debian, and Ubuntu. **Figure 1** shows the network topology of the virtual machines. In addition, they are connected through an internal network adapter to prevent malware from escaping.

The WannaCry ransomware that was used for the analysis on the Windows systems was taken from theZoo malware directory. While the Eicar virus was taken from the Eicar website and used to test the Linux systems.

Testing and Evaluation

Hash results:

When creating an MD5 hash on the Eicar file and running it on the virus total website detected that it Is used to test anti virus software and that 64 out of the 66 anti virus software were able to recognise the hash. While the MD5 hash on the WannaCry file showed that 65 out of the 66 anti virus software were able to recognise the hash.

Wireshark results

When trying to run the WannaCry ransomware on the windows machines it refused to execute despite disabling firewalls and windows built in security defender. When using Wireshark, it showed WannaCry trying it to access a port that could not be found (as shown in **Figure 2**). With further research it was discovered that modern windows systems have a prebuilt in patch against the eternal blue exploit.

Eicar provided no changes to the internal files. However, Wireshark demonstrated that Eicar had tried to communicate and access different ports on the system. One of the ports it could communicate with is port 5353 . This port Is used to communicate with Multicast DNS (mDNS) protocol which is used to announce IP addresses without the need for a DNS server.

54	7.443654025	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
56	7.444016028	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
119	34.448166738	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
121	34.448458465	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
123	34.448755185	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
125	34.448987586	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
127	34.449243285	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
131	34.963404560	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
135	35.968957120	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)
139	36.972585956	192.168.1.1	192.168.1.4	ICMP	104	Destination unreachable (Port unreachable)

Figure [2]: Wireshark Port Unreachable

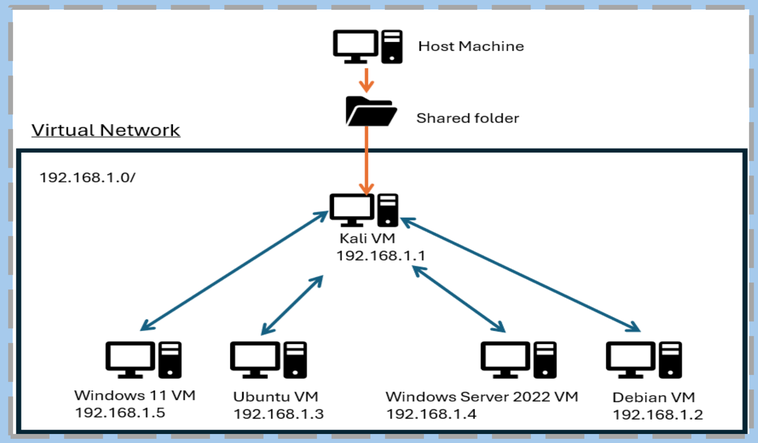

Figure [1]: Network Topology

Conclusion

Due to there being no changes in the files it meant that hard drive-based forensics could not be carried out. However, even though the main aim of the project could not be carried out it does not mean there are no results to take from the project. It showed that Windows 11 and Windows server 2019 and above systems by default have eternal blue patched into them preventing WannaCry ransomware using the eternal blue exploit to infect windows systems.

In addition to that the Linux systems infected with the Eicar virus did not infect the files on the hard drive. However, using Wireshark, it was able to detect the Eicar virus trying to communicate with ports on the network. The virus was able to successfully communicate with the Multicast DNS protocol which can be used to communicate with other devices on the network exposing a security risk.

References

[1] Exterro, "Ftk-imager," Exterro, N/A. [Online]. Available: https://www.exterro.com/digital-forensics-software/ftk-imager. [Accessed 26 March 2026].

[2] Wireshark, "Chapter 1. Introduction", Wireshark, [Online]. Available: 3 https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html[Accessed 26 April 2026]

[3] S. S. Apoorv Kumar Sinha, "Integrated Malware Analysis Sandbox for Static and Dynamic Analysis," in 14th International Conference on Computing Communication and Networking Technologies, Delhi, India, 2023.