

Evaluating the effectiveness and performance of a range of anti-virus software

Shannon Wallace(1901768) Computer Networks & Cyber Security

Introduction

This project is about evaluating the effectiveness and performance of an anti-virus software. Technology usage has grown massively over the few years. Due to growth, users of the internet are vulnerable to malware due to the lack of security on devices.

Aim

Evaluate the effectiveness and performance of an anti-virus software against malware simulators

Objectives

- Testing a range of anti-virus software usefulness
- To analyze and evaluate the results of anti-virus software efficiency
- To conduct a review and recommend a software features based on their performance
- To highlight the important and raise awareness of a recommended anti-virus software

Research

The research was conducted to help with the experiment:

- Different types of malware and the impact
- Impact of malware over the years
- How does malware work and how to identify it?
- What is anti-virus software?
- How does an anti-virus software work?
- Virtualisation
- Simulation software

Design & Implementation

The experiment required:

- Two virtual machines
Windows 10 and Windows 8
- Four anti-virus software
Norton, MacAfee, Avast and Bitdefender
- Three malware simulators
Trojan, Ransomware, Infection money
- Hardware and networking monitoring tool
NZXT and wire shark

The experiment went into 3 stages

- detection(Before),
- Performance,
- Detection(After)

Figure 1 shows two machines windows 10 and windows 8 and then a laptop. The laptop is the main device and will have two virtual machines on the device. The two virtual machines will be connected to a virtual network.

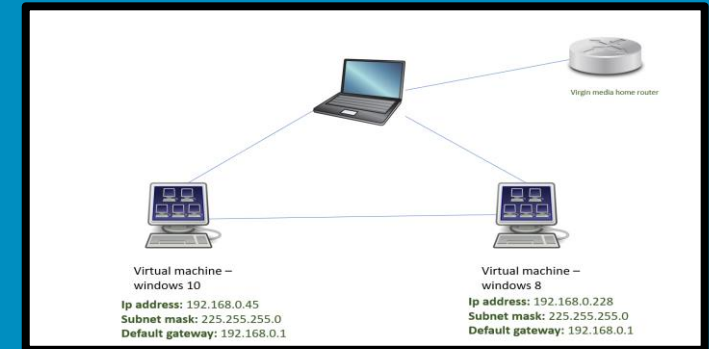


Figure 1: Network topology

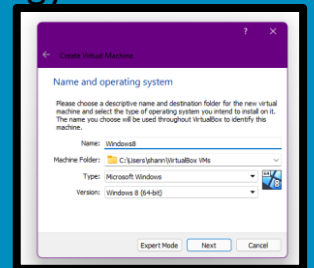


Figure 2: VM setup

Results & Conclusion

The experiment conclusion is that Bitdefender and Avast had the worst performance. However, are the best detection. The reason why they are not recommended is due to the performance issues that happened in the tests. Both anti-virus software was slow and froze the device, which is clearly shown in the graphs. Norton did not provide the results as expected, it failed 2/3 tests against malware. MacAfee was the best at providing protection and performance based on results.

The aim of this project was to evaluate the effectiveness and performance of anti-virus software. The objectives gave structure to the project which helped in conducting a literature review. The design and implementation helped conduct the experiment. Overall, the experiment was a success as most of the anti-virus software did provide protection.

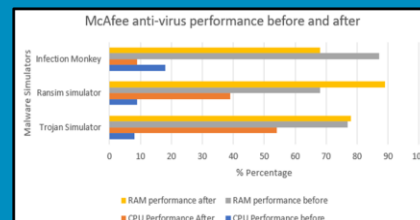


Figure 5: McAfee performance

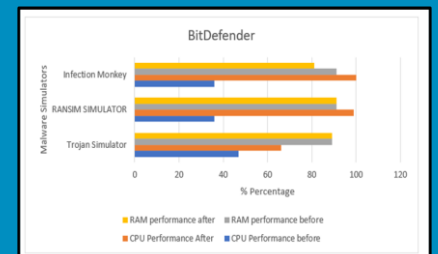


Figure 3: Bitdefender performance

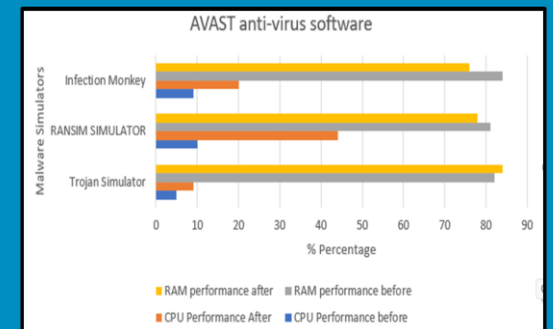


Figure 4: AVAST performance