## Executive Summary

This lab focused on setting up a malware analysis enviromnent using a virtualbox, flare-vm and windows operating system. The key activities were pre-installation process in configuring the vm which included allocating enough storage capacity disabling windows updates, windows defender and creating a snapshot. Flare-vm was installed together with other necessary configurations.

## Lab objectives

The primary goal of this lab was to set up a malware analysis environment that will conduct reverse engineering.

The goal is to use Flare-VM to ensure the environmment is fit for malware analysis.

## Tools and Resources used

Oracle Virtualbox: To host our windows 10 OS

Windows ISO file:To host our Flare VM

Flare-VM : Our malware analysisi and reverse engineering environment

## Methodology

I had an already pre-installed oracle virtual machine. I downloaded windows 10 ISO file from microsoft official store. After download was complete, I started the process of adding the ISO file to my oracle virtualbox. I ensured therewas a storage capacity of more than 60GB and a ram of atleast 2GB.

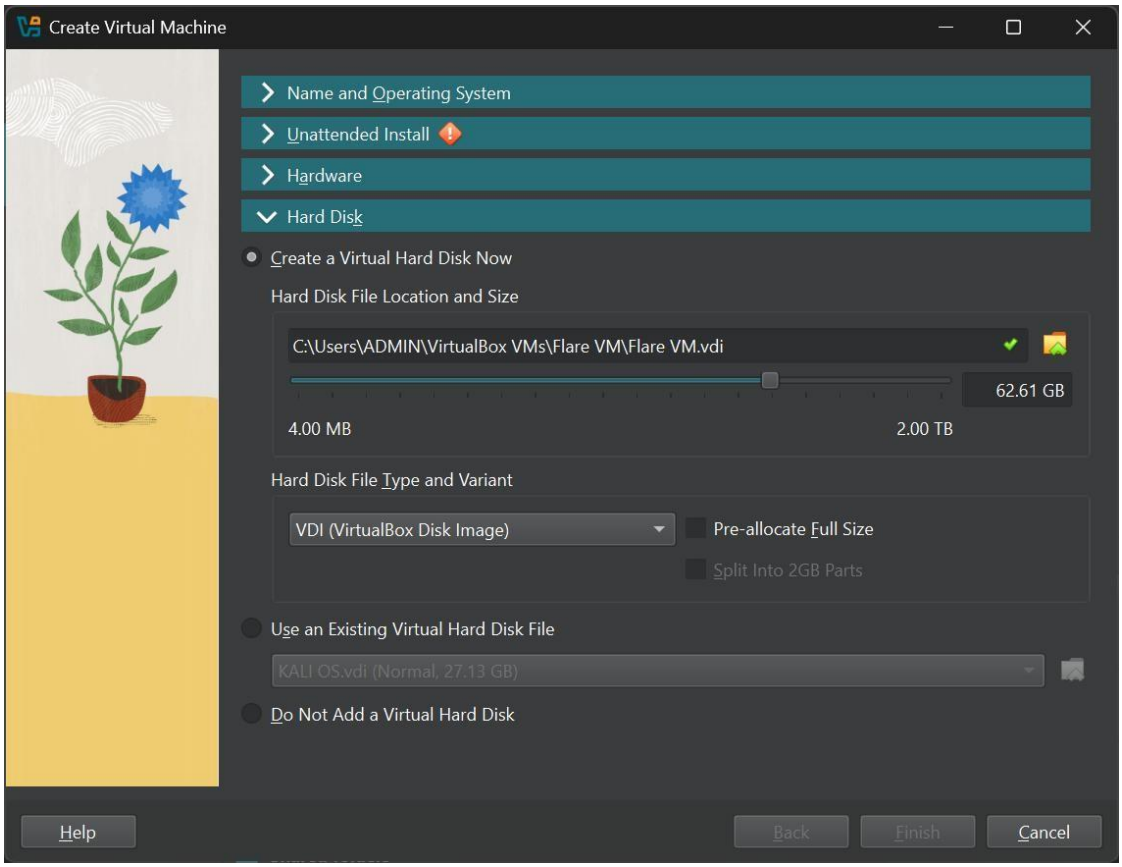

Figure 1: Allocating storage capacity for flare vm

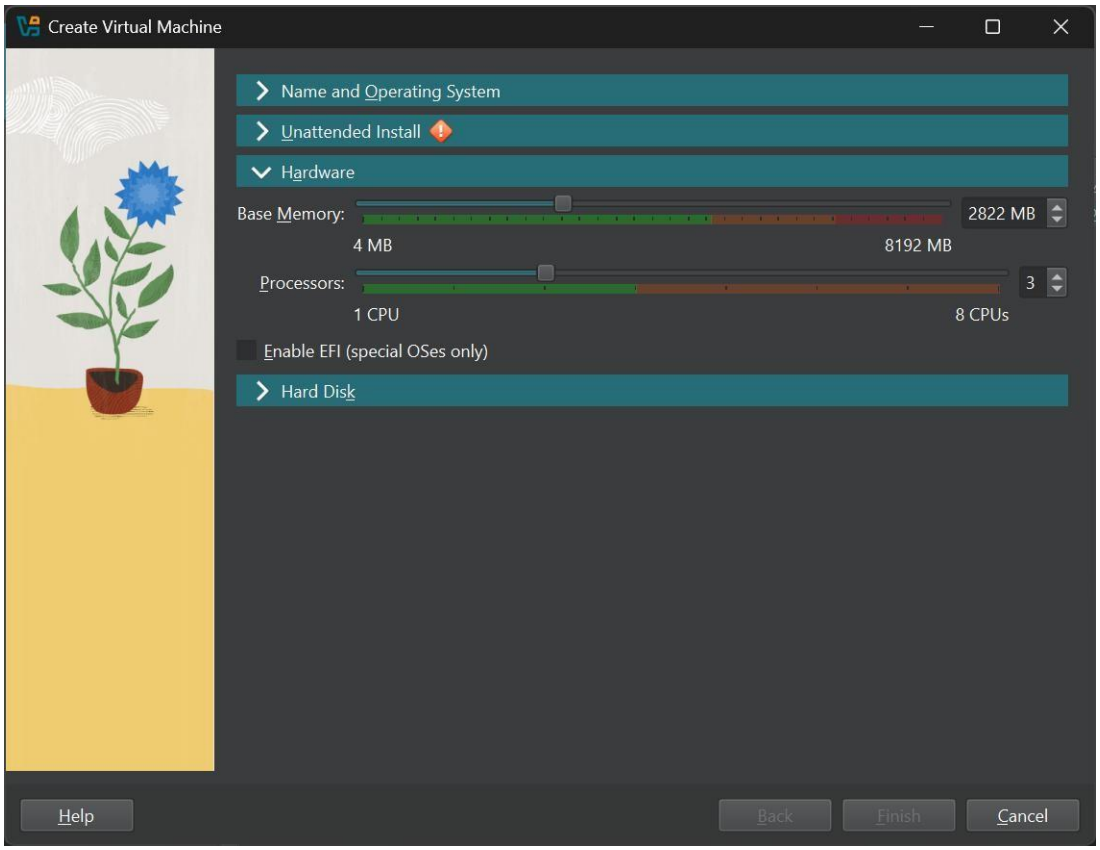

Figure 2: Allocating RAM and CPUs using oracle VM

After installing the windows vm, I had to install guest addition tools that include full screen and shared folder capability where I selected my documents folder from my host OS and save a snapshot.

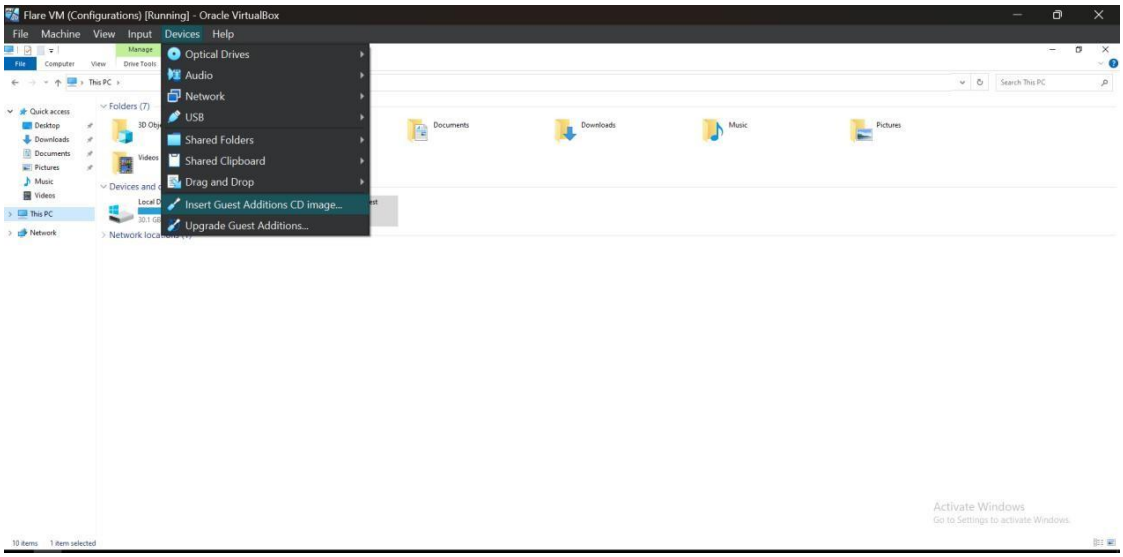

Figure 3: Inserting guests additions

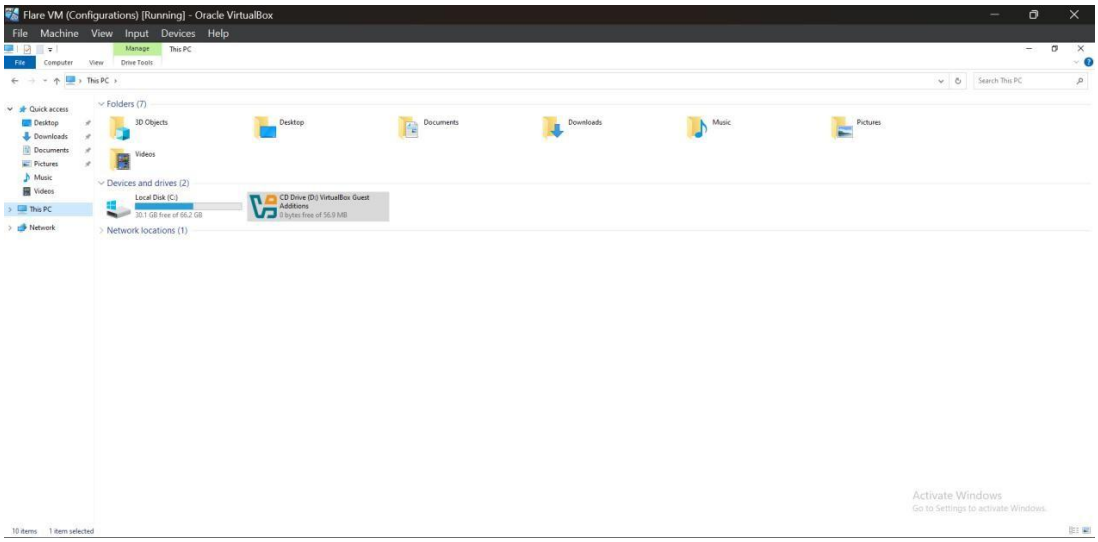

Figure 4: Continuation of inserting guest additions on windows

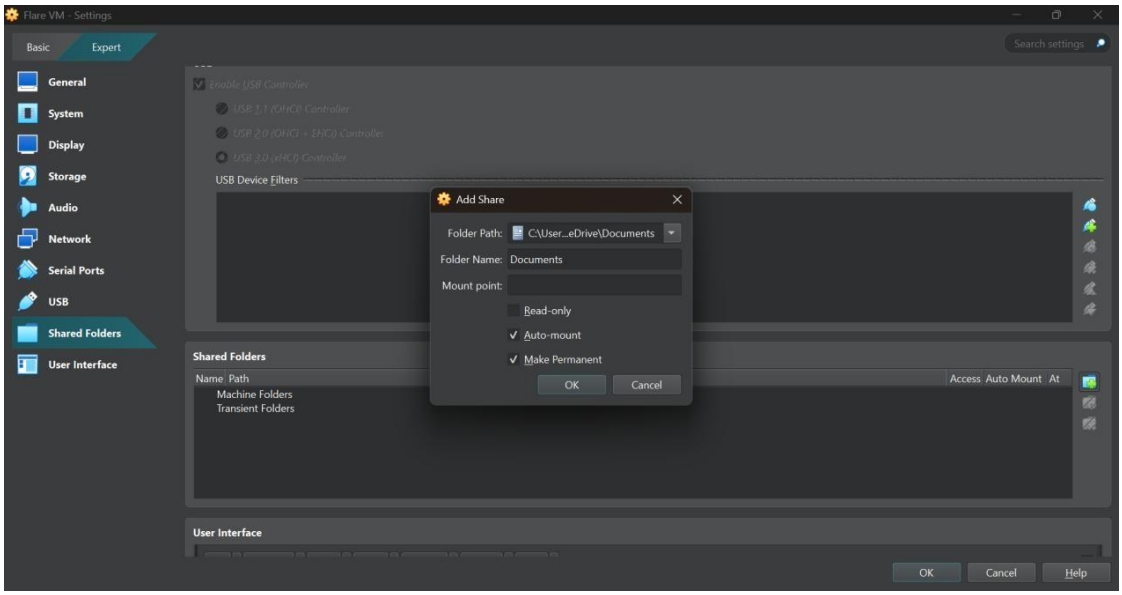

Figure 5: Linking shared folder

The next step was to disable windows updates using group policy. Unlike group policy, pausing windows updates manually is only temporary.

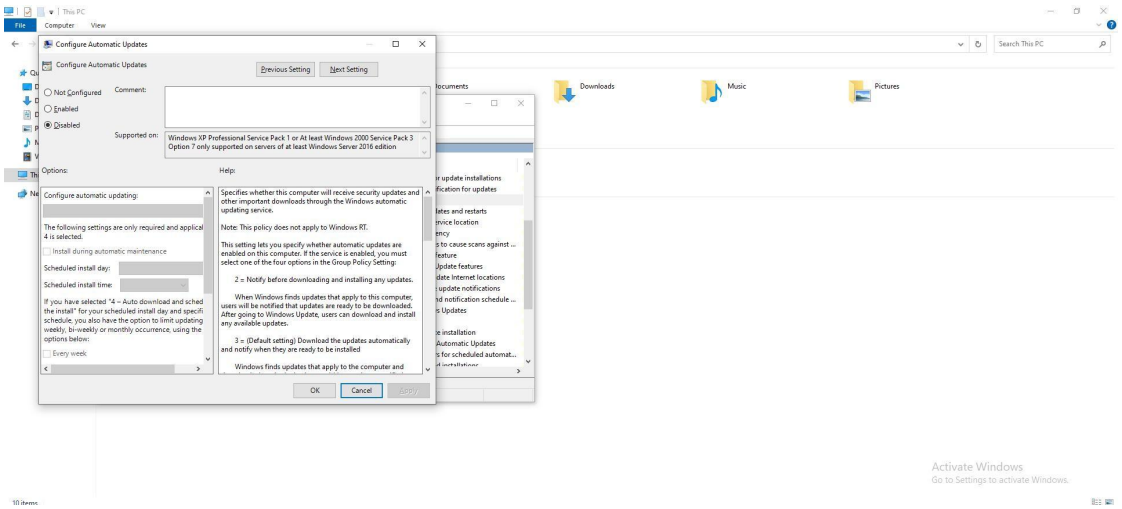

Figure 6: Disabling windows updates using group policy

The next step was to disable windows defender by using group policy. Also turning off tamper protection in the windows security  in the virus and threat protection section is required. Aside from that, turning off real time protection is key since it acts as an  immediate layer of defense.

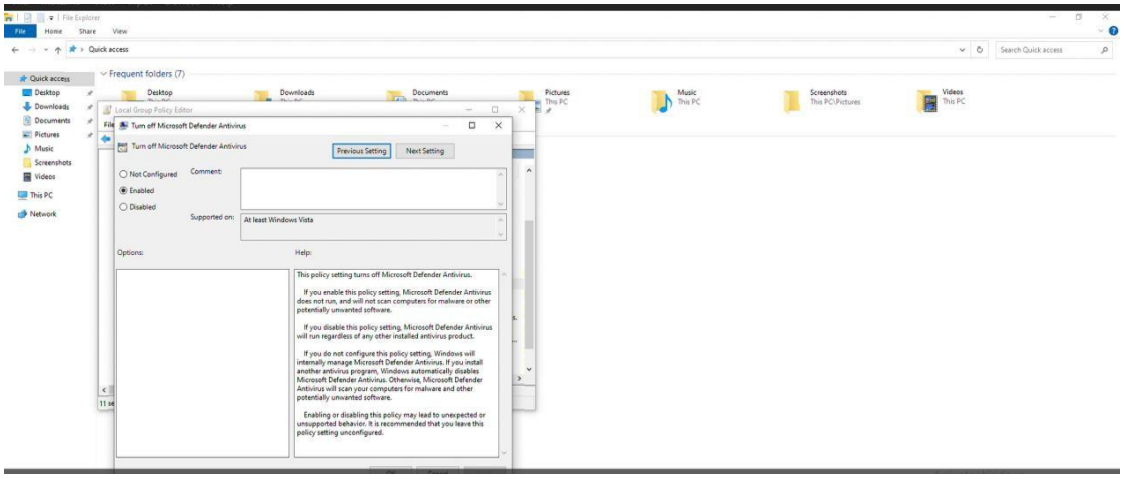

Figure 7: Disabling windows defender

To ensure all files and folders are visisble, I had to enable shared folder and uncheck hidden extensions.

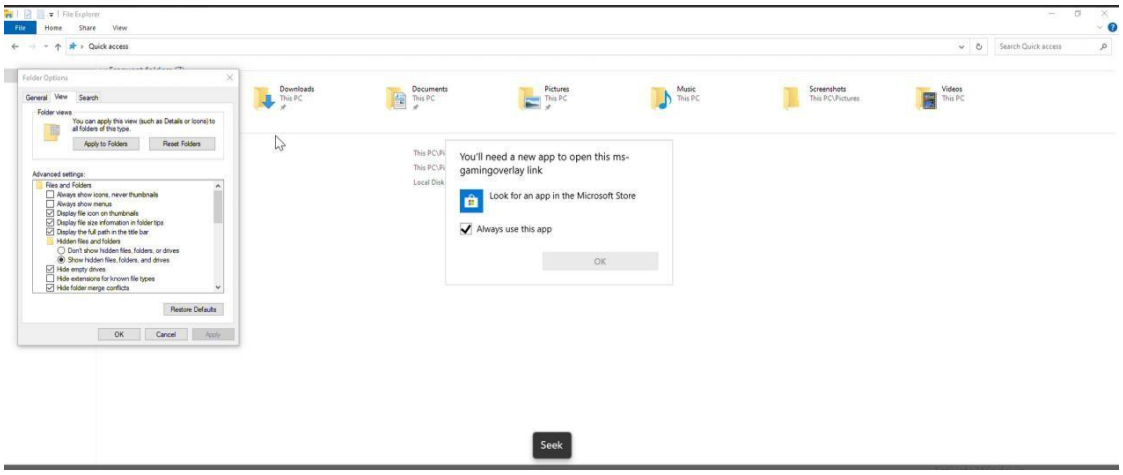

Figure 8: Making hidden folders and files visible

Powershell played a key role in installing flare vm following a step by step command from mandiant github repository. After a couple of hours, my flare vm was fully installed.

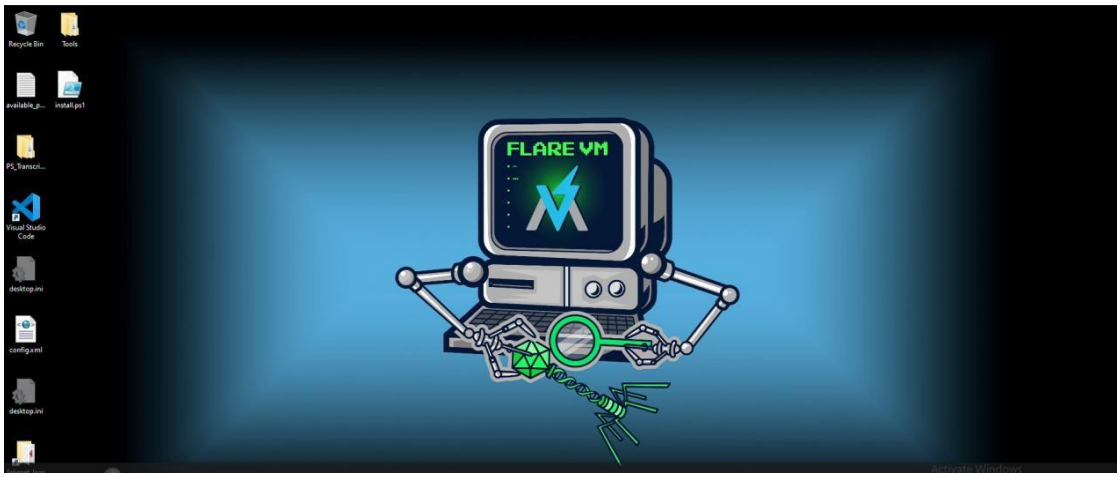

Figure 9: Flare VM

**Challenges and Solutions**

I had a error in installing ghidra.vm. The flare vm had downloaded an outdated ghidra and I had to uninstall and install manually using the commands ‘choco uninstall ghidra -y’ and ‘choco install ghidra -y to fix the errors’.

Dependencies such as ida.plugin.xrefer, idr.vm, malware-jail and sfextract gave errors and had to be installed manually. Aside from that, errors kept coming up while installing flare vm because of not properly disabling windows defenders. To fix the error I had to turn off tamper protection to completely disable micrososft antivirus.

**Conclusion**

Flare vm installation encompasses a wide area in virtualbox configuration for example guest additions and using group policy to disable security policies. It also teaches the virtue of patience and carefully following instructions.

For quicker and successful installation, one has to ensure thete is stable internet and be patient during the installation.

**Recommendations**

Taking snapshots is necessary to revert changes when necessary.
Stable internet is highly recommended for smooth and quicker installation.
Ensuring windows defender is completely disabled before installation of the flare vm.

**References**


- Downloading windows 10. Retrieved from https://support.microsoft.com/en-us/windows/create-installation-media-for-windows-99a58364-8c02-206f-aa6f-40c3b507420d

- Denham, B., & Thompson, D. R. (2022, October). Ransomware and malware sandboxing. In *2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0173-0179). IEEE.

- Franko, A. (2024). A Practical Approach to Malware Exploration: Setting up a Dedicated Analysis Lab.

- Installing flare vm. Reterived from https://github.com/mandiant/flare-vm

- Windows defender (2024, March. Retrieved from https://answers.microsoft.com/en-us/windows/forum/all/how-can-i-permanently-disable-or-remove-windows/7e3ce6d4-231f-4bee-912c-3cc031a9bf8d