LAB TITLE: LAB SETUP.

STUDENT NAME: BRIAN NJIRU.

STUDENT ID: 2025/ACTI/6177.

COURSE NAME: ADVANCED CYBERSECURITY OPERATION AND THREAT INTELLIGENCE.

INSTRUCTOR NAME: AMINU IDRIS.

DATE OF SUBMISSION 13TH FEBRUARY 2025.

VERSION: 1.0

Contents

TABLE OF FIGURES.

1. EXECUTIVE SUMMARY

1.1 Purpose of the lab.

The lab focused on setting up a malware analysis lab in a virtual environment using FLARE-VM. FLARE-VM is a collection of software installation scripts for windows systems that allows you to easily setup and maintain a reverse engineering environment on a virtual machine (VM).

1.2 Key Activities.

The lab required the following activities to be performed:

1. Virtual Machine setup.
2. Windows 10 preparation for FLARE-VM installation.
3. Installation of FLARE-VM.

1.3 Major Findings.

The lab showed that FLARE-VM is a robust reverse engineering environment with a wide variety of tools for malware analysis and reverse engineering.

2. LAB OBJECTIVES.

The primary objective of the lab was to setup FLARE-VM on a virtual machine.

3. TOOLS AND RESOURCES USED.

The lab required that a variety of essential tools and software resources used to ensure that the lab objective was fully met.

The following are the tools used in this lab:

3.1 VMware Workstation Pro 17.

VMware Workstation Pro 17 is a Type 2 (hosted) hypervisor that runs on the x64 version of Windows and Linux operating systems. It enables users to set up virtual machines on a single physical machine and use them simultaneously along with the host machine.

VMware was used as the hypervisor in this lab.

3.2 Windows 10 ISO.

Windows 10 is a major release of Microsoft's Windows NT operating system. Windows 10 was used as the guest OS on which FLARE-VM was installed.

3.3 FLARE-VM

FLARE-VM is a reverse engineering and malware analysis environment for Windows systems with a vast array of software analysis tools. FLARE-VM was used as the environment for malware analysis and reverse engineering.

4. METHODOLOGY.

The following steps were followed to setup FLARE-VM:

4.1 Download Windows 10 Disc Image.

I downloaded the windows 10 media creation tool from Microsoft's website and went ahead to create and ISO file for windows 10.

4.2 Create a Windows 10 Virtual Machine (VM).

I created a Windows 10 VM that met all the requirements for running FLARE-VM. The following steps were followed:

4.2.1 Create a New Virtual Machine in VMware.

I opened VMware Workstation and navigated to the home tab.

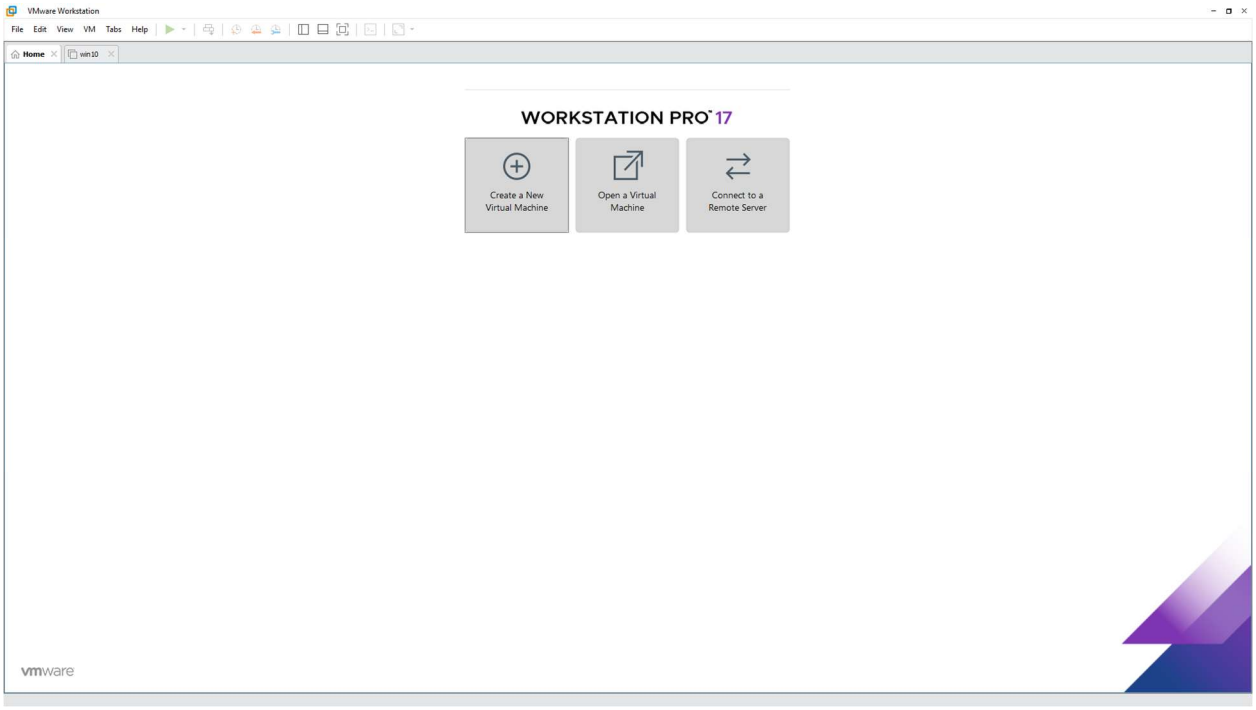

Figure 1: VMware Workstation Home tab

I then clicked on the Create a New Virtual Machine option. VMware presented me with the New Virtual Machine Wizard.

4.2.2 New Virtual Machine Wizard, Configuration selection.

After selecting the Create a New Virtual Machine option, VMware presented me with the New Virtual Machine Wizard.

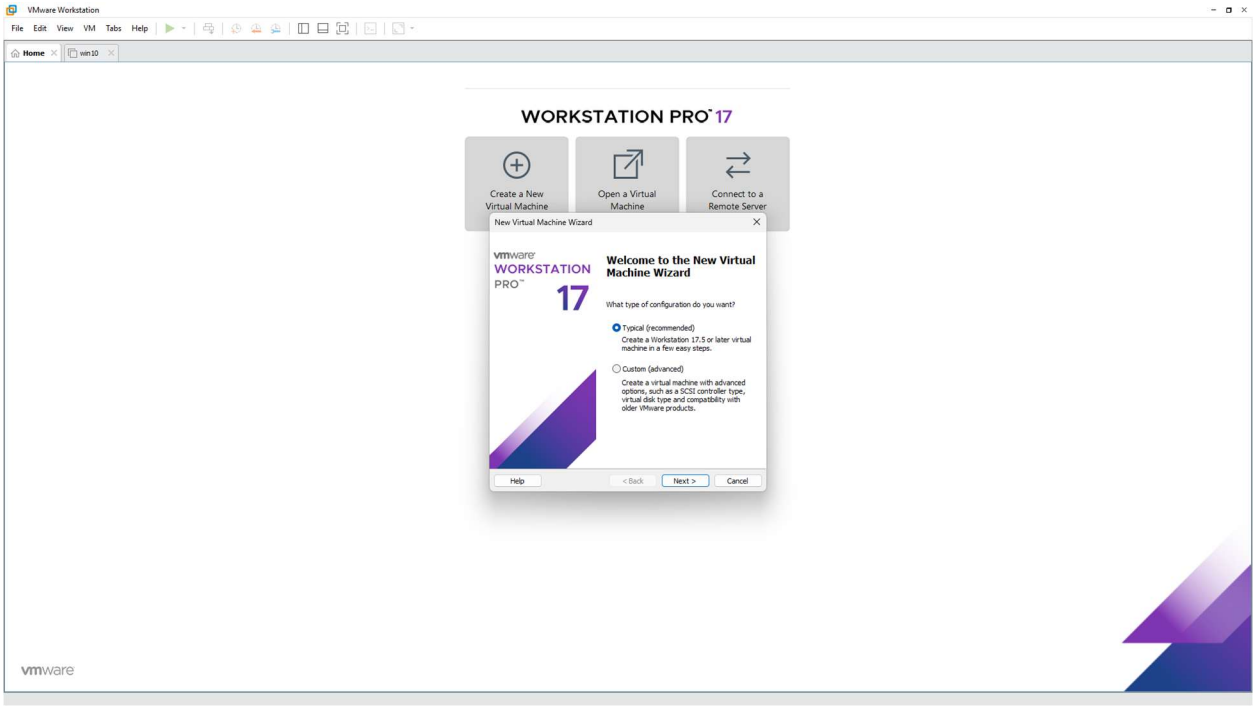

Figure 2: New Virtual Machine Wizard in VMware.

I left the selection on “Typical (Recommended)” because the virtual machine does not require the advanced options specified by the “Custom (Advanced)” option. I then clicked on next.

4.2.3 Choose the Windows 10 Disc Image.

The New Virtual Machine Wizard proceeded to the next step where it required me to choose the Guest Operating System (OS) installation file.

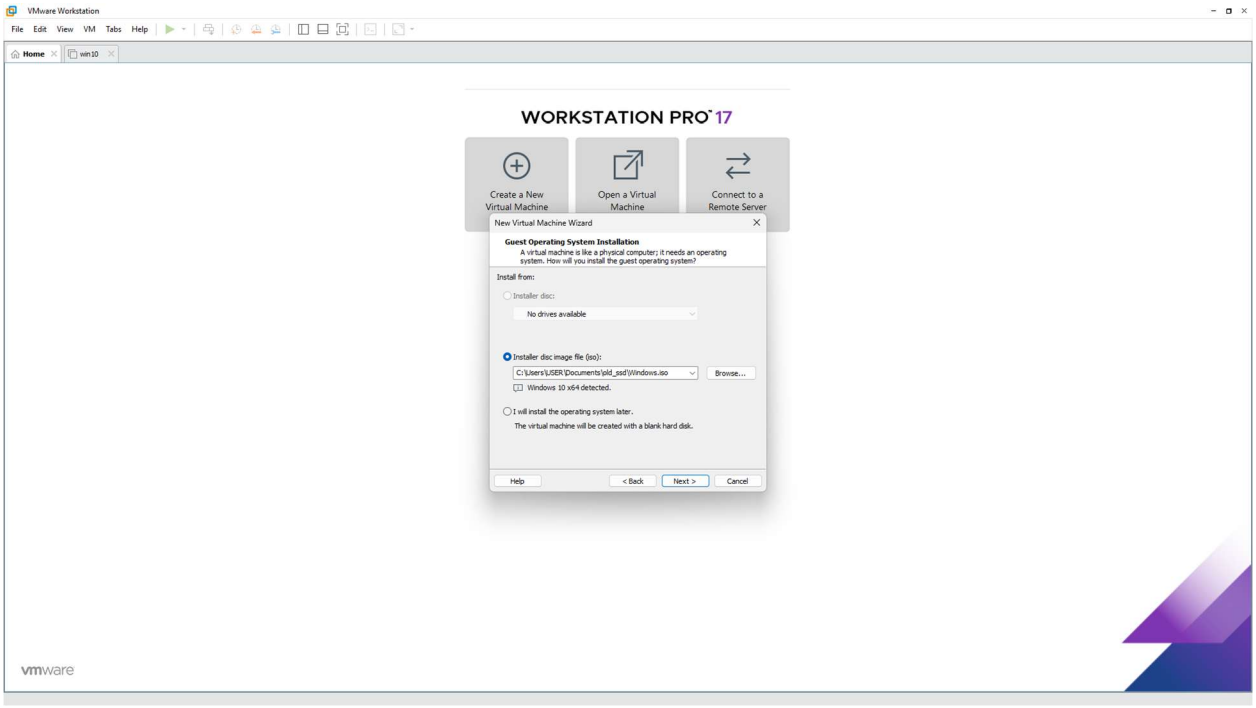

Figure 3: Guest OS installation

I specified the location of the Windows 10 Disc Image and clicked on Next.

4.2.4 Choose the Name and location for the Virtual Machine.

I then gave my Virtual Machine a name. I chose the name “win10” for the machine as it specifies the Operating System at a glance and because it is the only Windows 10 Virtual Machine in my specified lab folder in VMware. I left the location for the Virtual Machine on default and clicked on next.

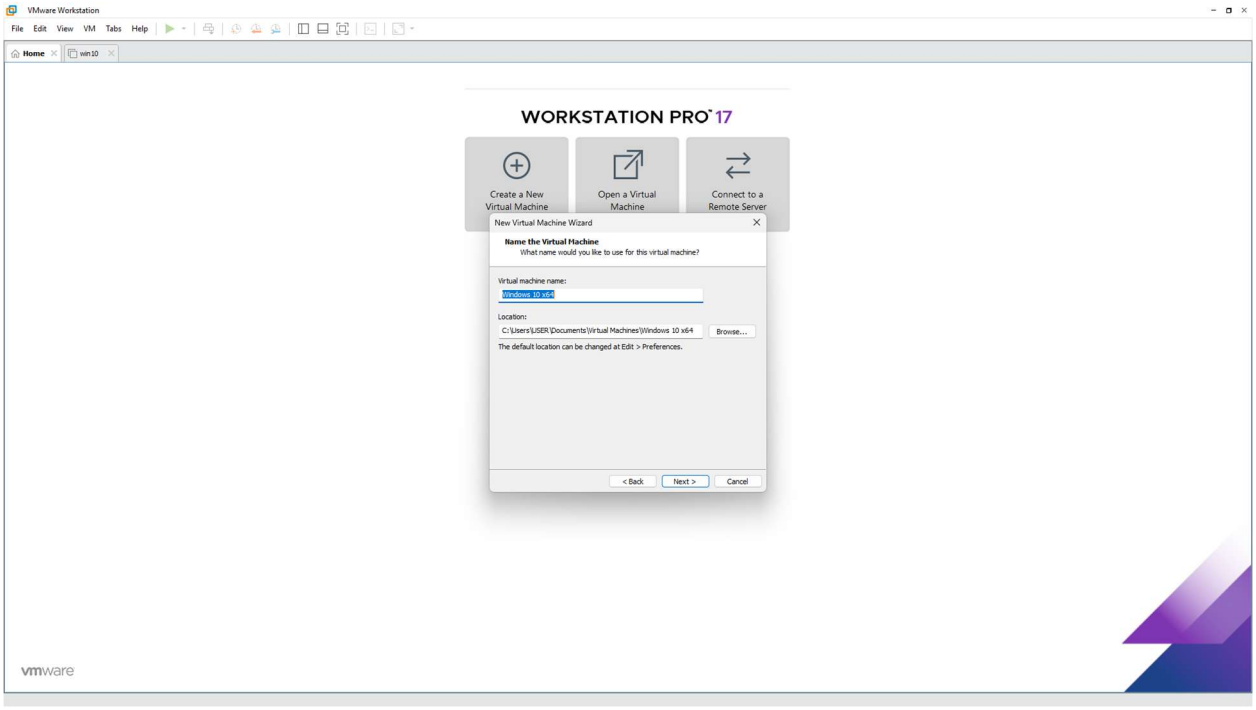

Figure 4: Choosing a name for the virtual machine

4.2.5 Specify the Disk Capacity of the Virtual Machine.

I specified the disk capacity of the Windows 10 Virtual Machine based on the requirements of FLARE-VM. FLARE-VM requires at least 60gb of storage for installation. I chose a Disk Size of 60gb which is also the recommended size for a Windows 10 Virtual Machine on VMware. After that, I clicked on next.

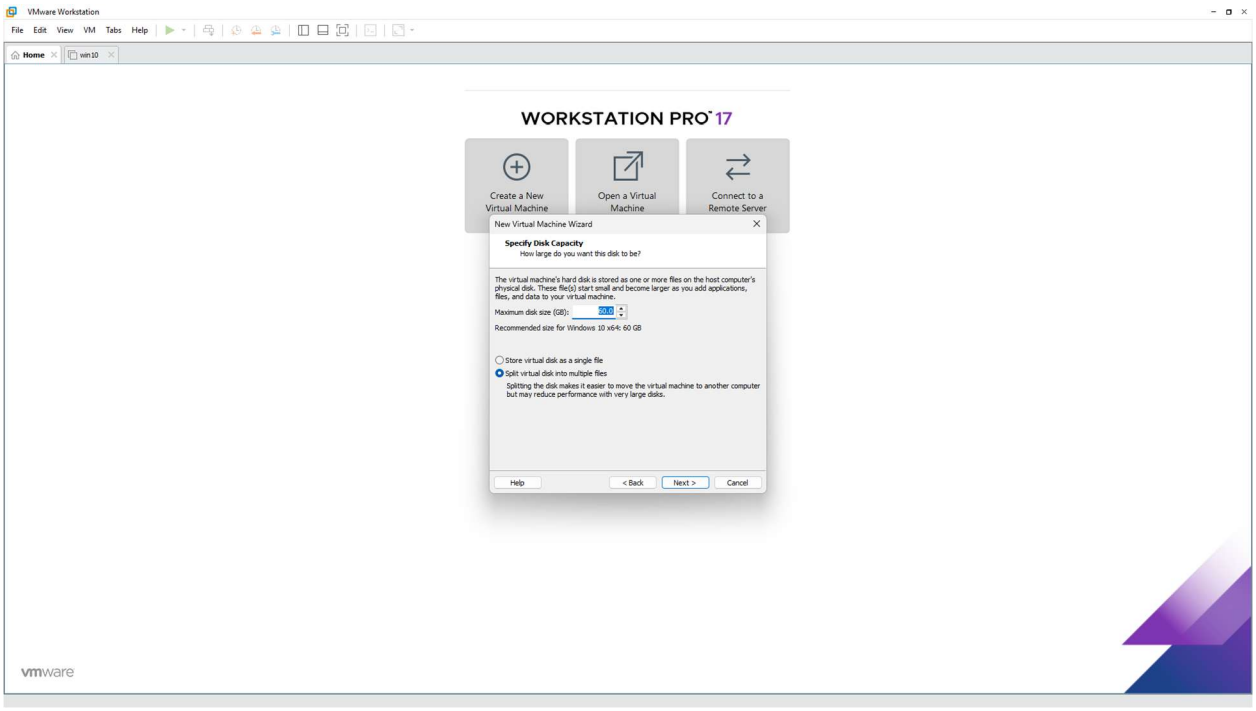

Figure 5: Specifying the disk capacity of the VM

4.2.6 Customize Hardware for the Virtual Machine

The New Virtual Machine Wizard presented me with the final step in the creation of a New Virtual Machine. I clicked on the “Customize hardware” option to change a few settings.

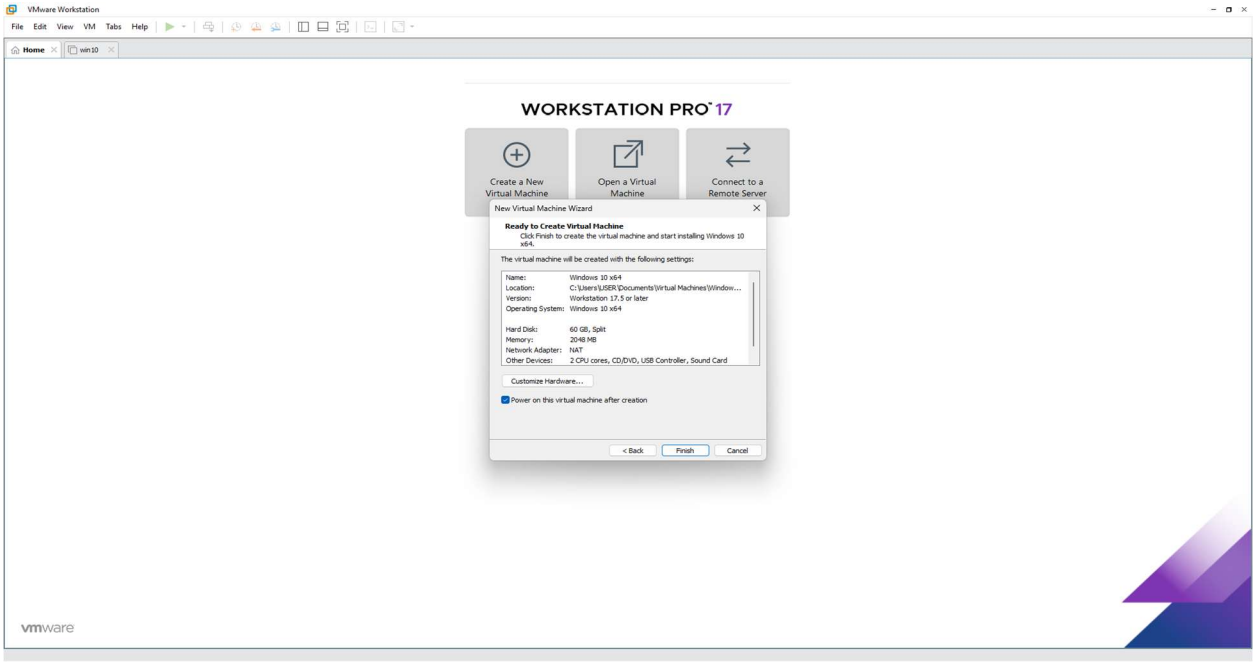

Figure 6: Final step of creating a New Virtual Machine in VMware

I customized the given hardware options to increase the amount of RAM allocated from 2048mb to 4096mb for better performance. I left the Network Adapter on the NAT (Network Address Translation) mode for internet connectivity, I later changed it to the Host-only mode to isolate the network environment. I then clicked finish.

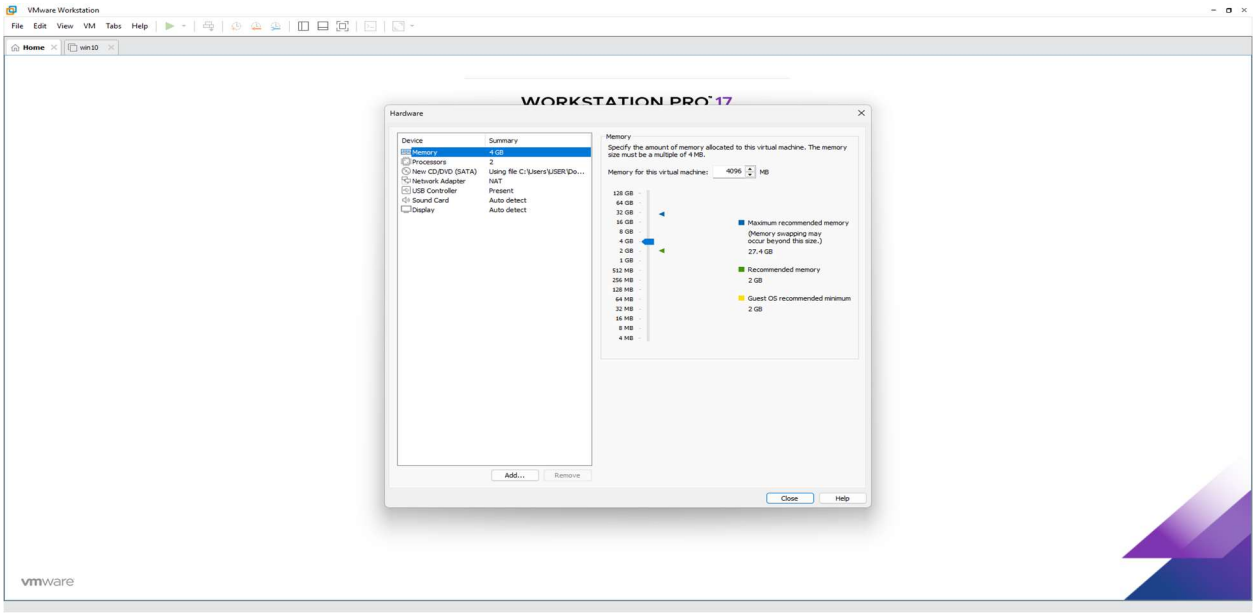

Figure 7: Changing the RAM size allocated to the VM.

4.3 Install Windows 10 inside the Virtual Machine.

The “win10” VM was successfully created and was then ready for me to install the Windows 10 operating system.

4.3.1 Power on the win10 VM.

I selected the newly created win10 VM from the side bar library and clicked on the “Power on this Virtual Machine” option.

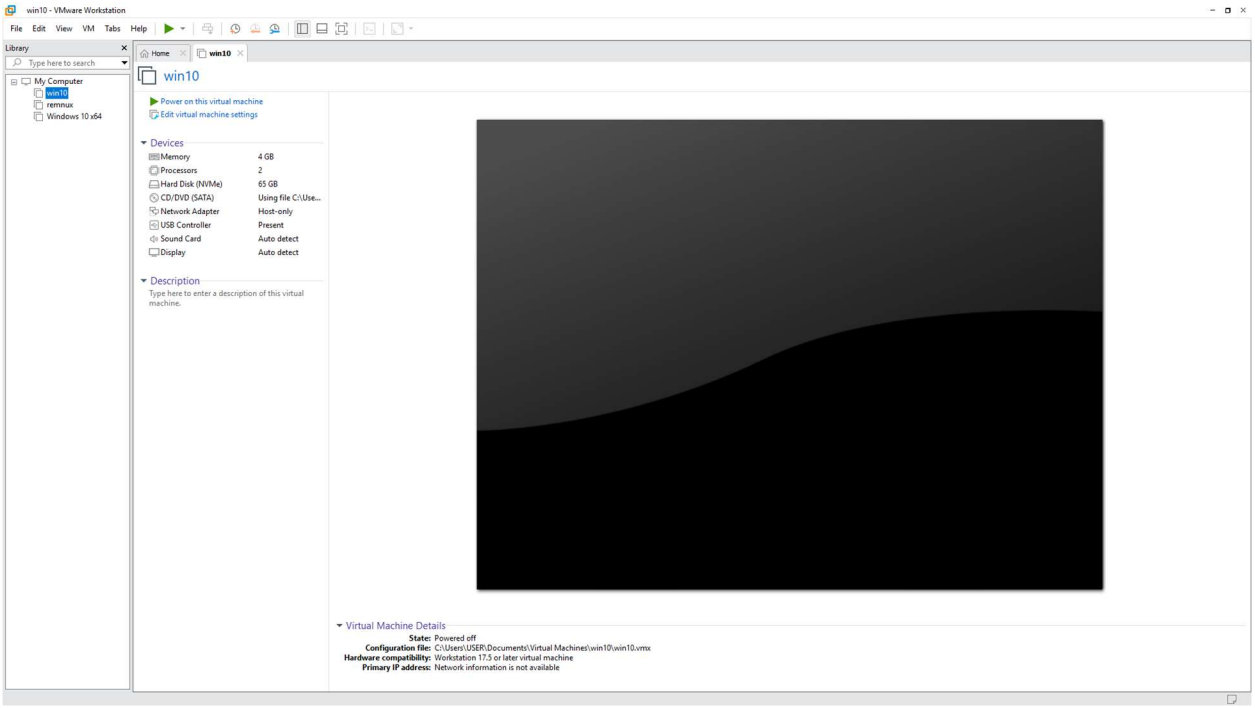

Figure 8: Powering on the win10 VM.

4.3.2 Install windows 10.

I booted the virtual machine and proceeded with the windows 10 installation.

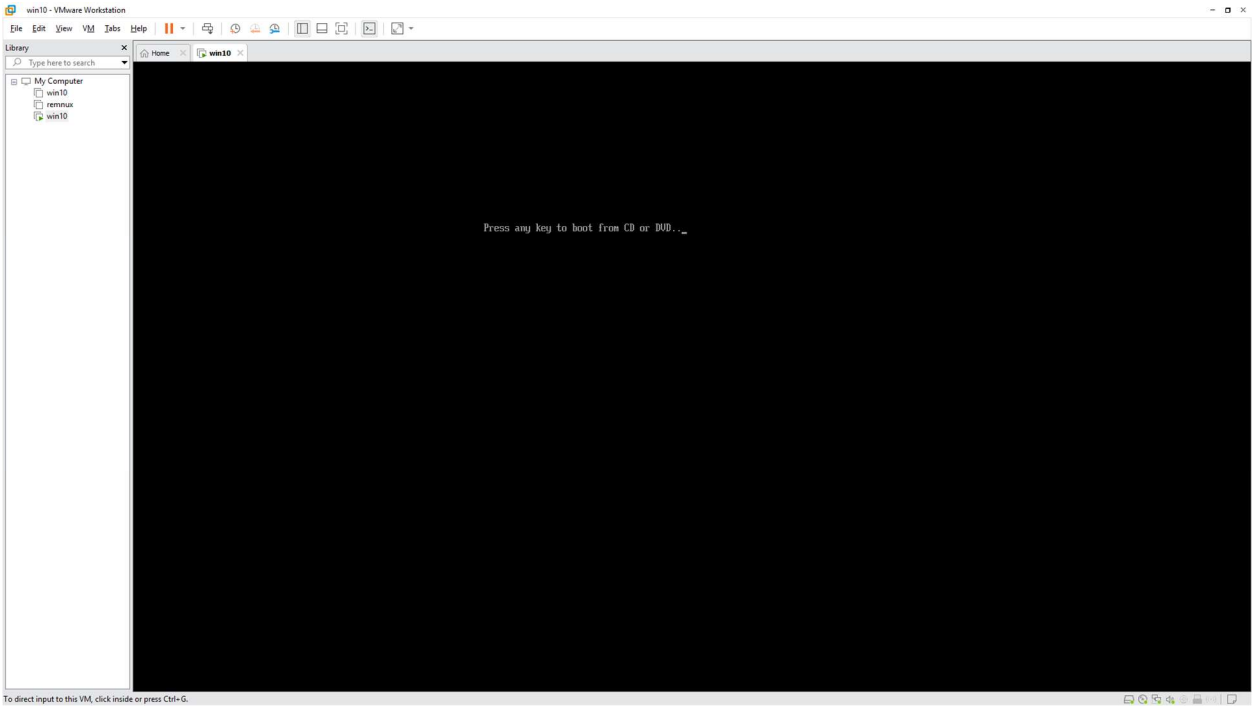

Figure 9: Booting the VM

I pressed any button and the windows installation disc started its process.

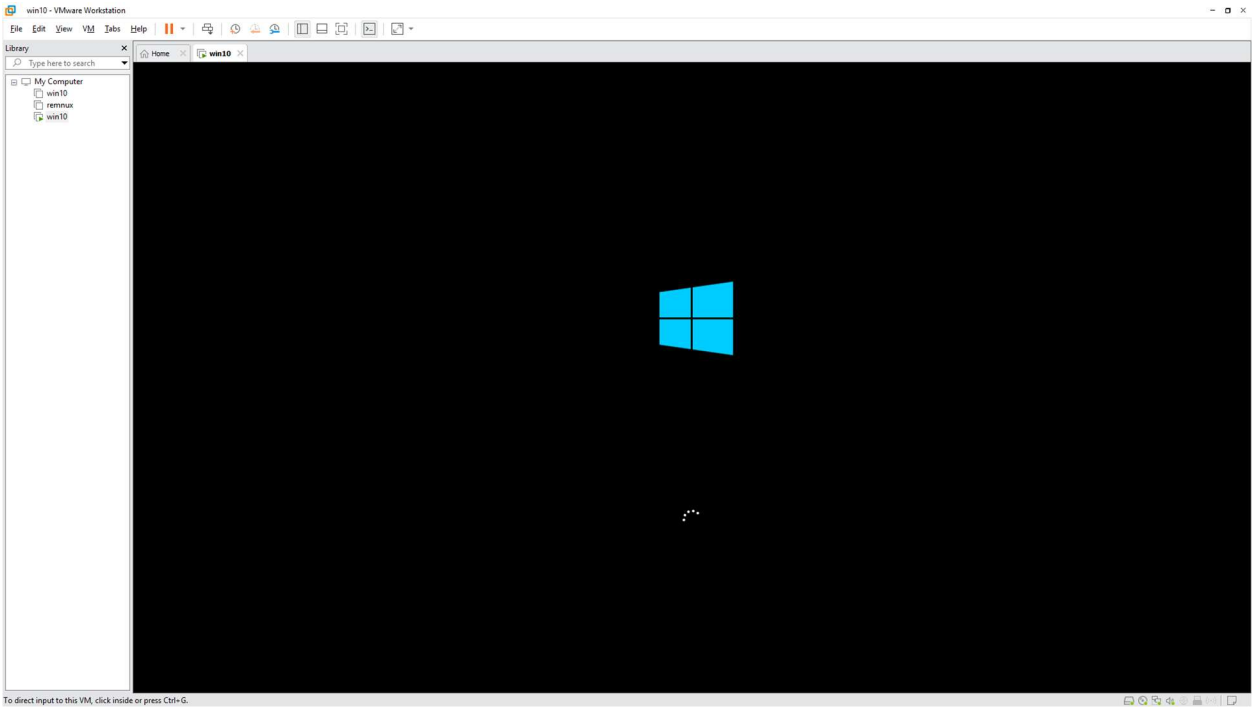

Figure 10: Windows 10 installation media starting.

I chose my preferred language and clicked on next.

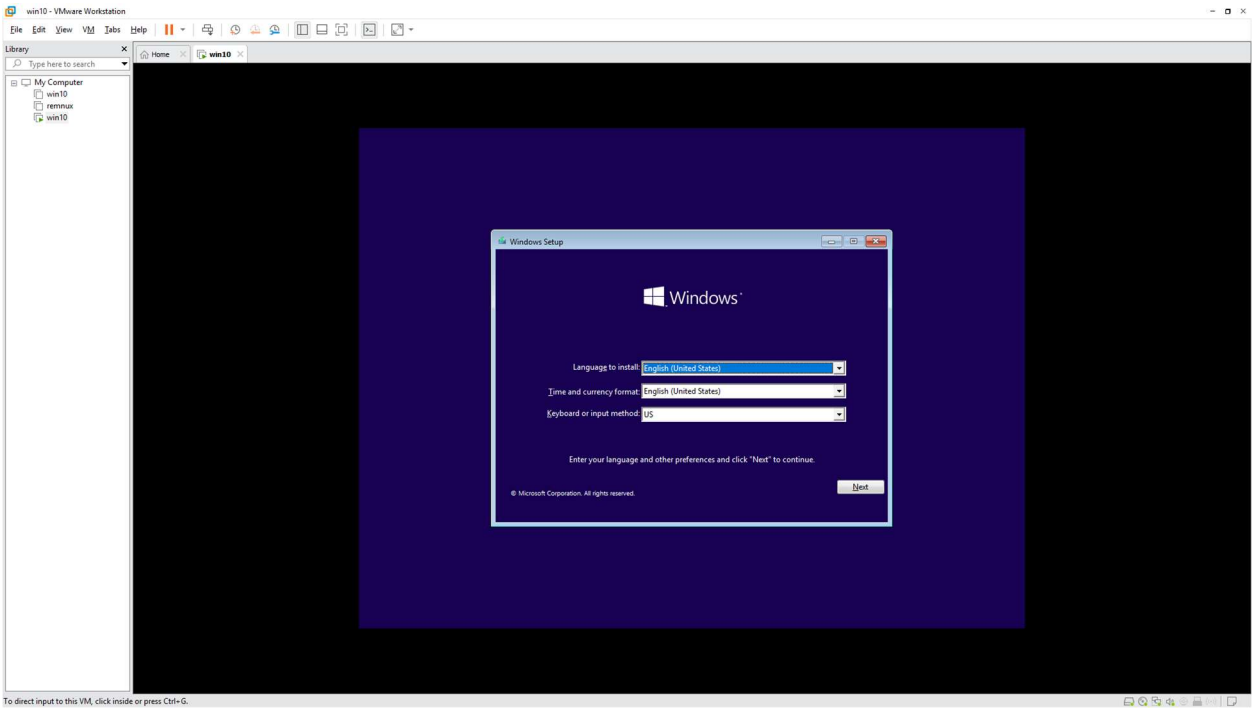

Figure 11: Selecting language for installation.

After selecting the language, I clicked on the “Install Now” button and the installation began.

I specified Windows 10 pro as the version I wanted to install.

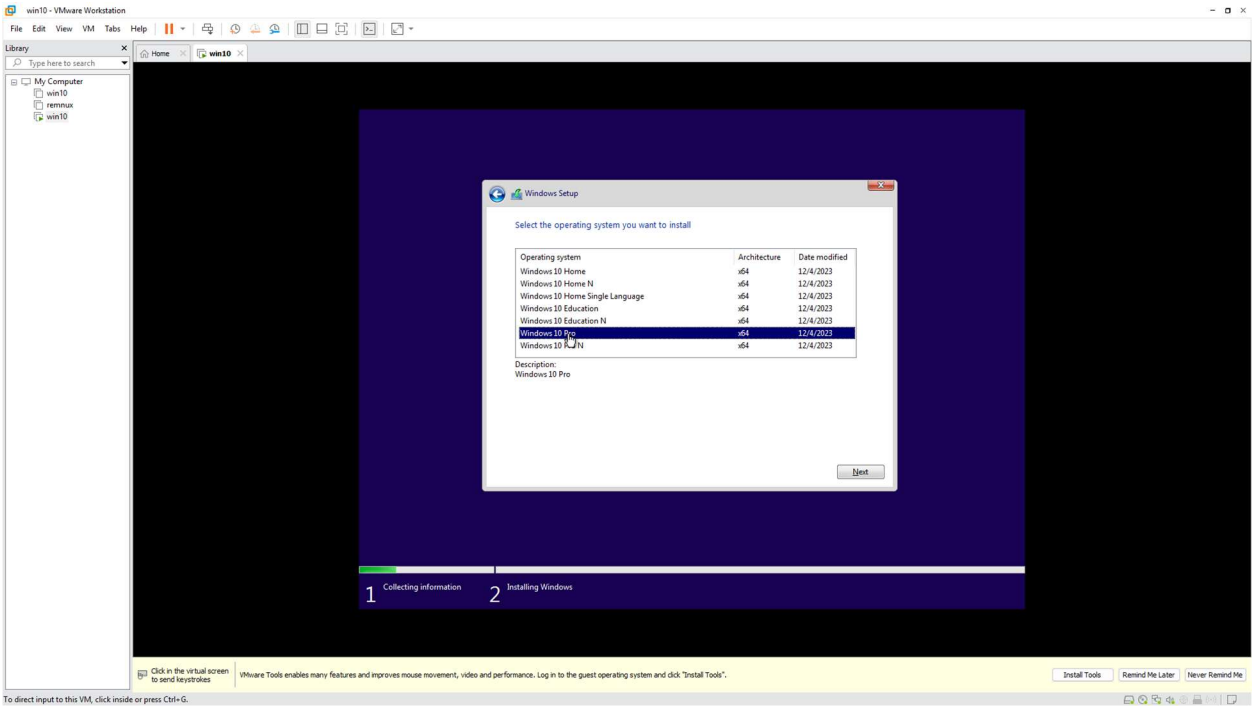

Figure 12: Selecting which Windows 10 variant to install.

I then accepted the license terms and clicked on next.

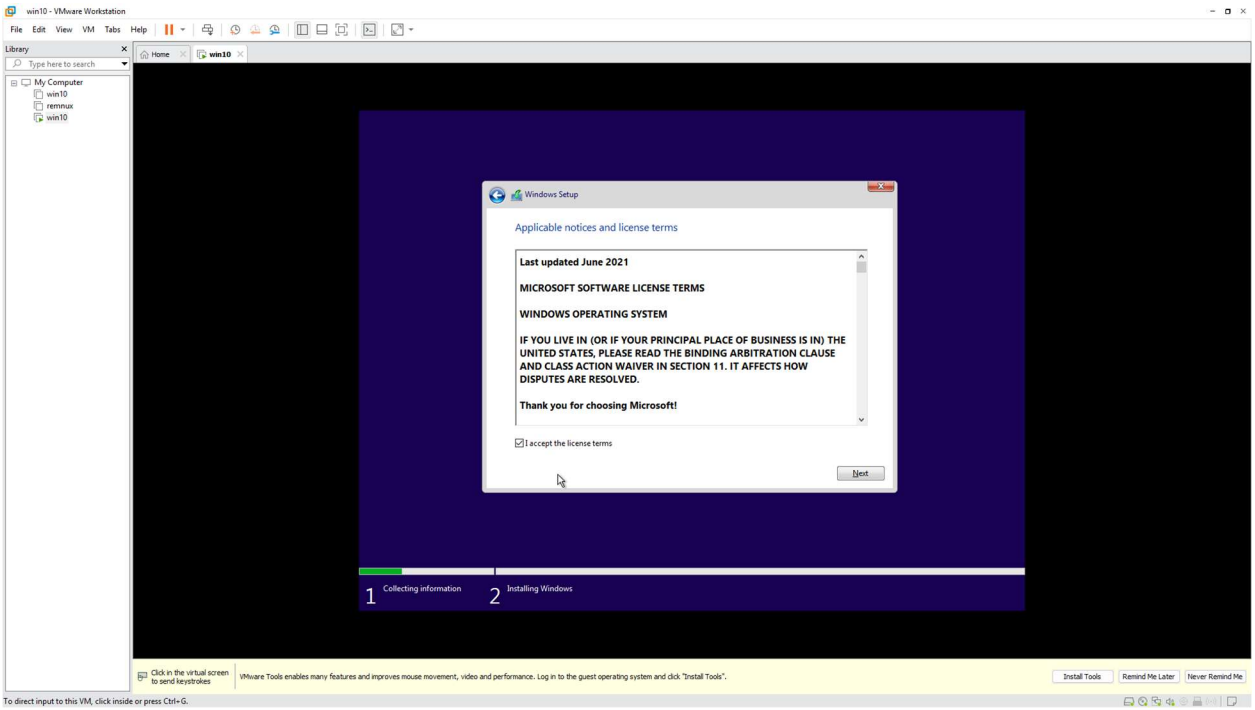

Figure 13:Accepting the license terms.

I chose a custom installation type because I was installing windows 10 on a system that did not have windows 10 installed on it prior to the current windows 10 installation.

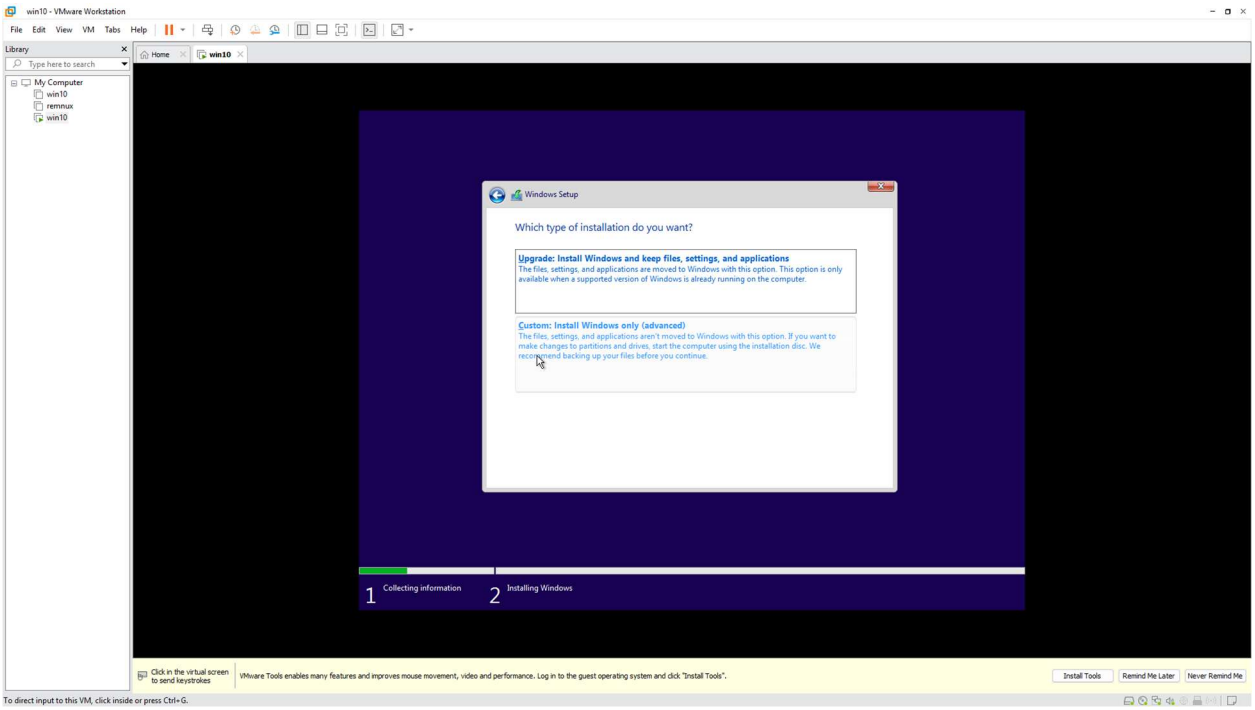

Figure 14:Selecting the type of installation for windows 10.

I specified the 60gb drive that I created as the location where I wanted to install windows 10, it was the only option there and there was no need to create a new drive.

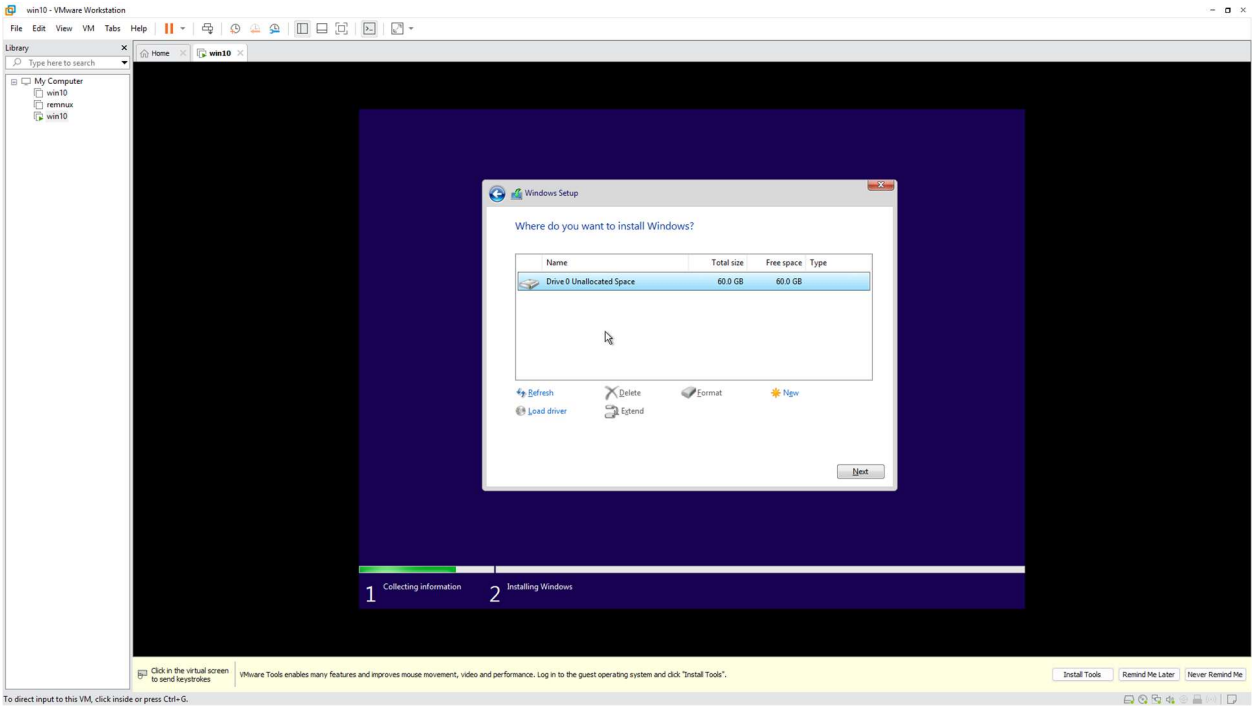

Figure 15: Selecting storage location for windows 10

The windows 10 installation finally began. I installed it as I would on a normal computer.

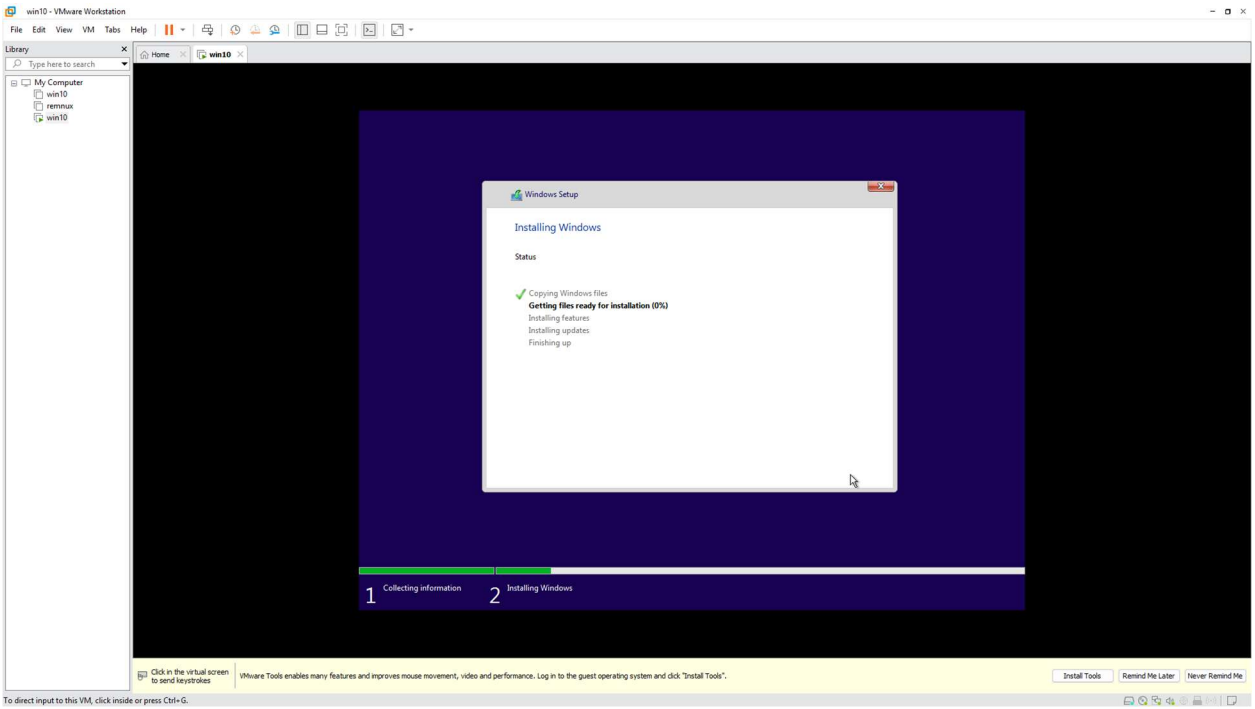

Figure 16: windows 10 installing

4.3.3 Deselect Privacy settings.

During the setup, the windows 10 installation prompted me with privacy settings which I toggled off.

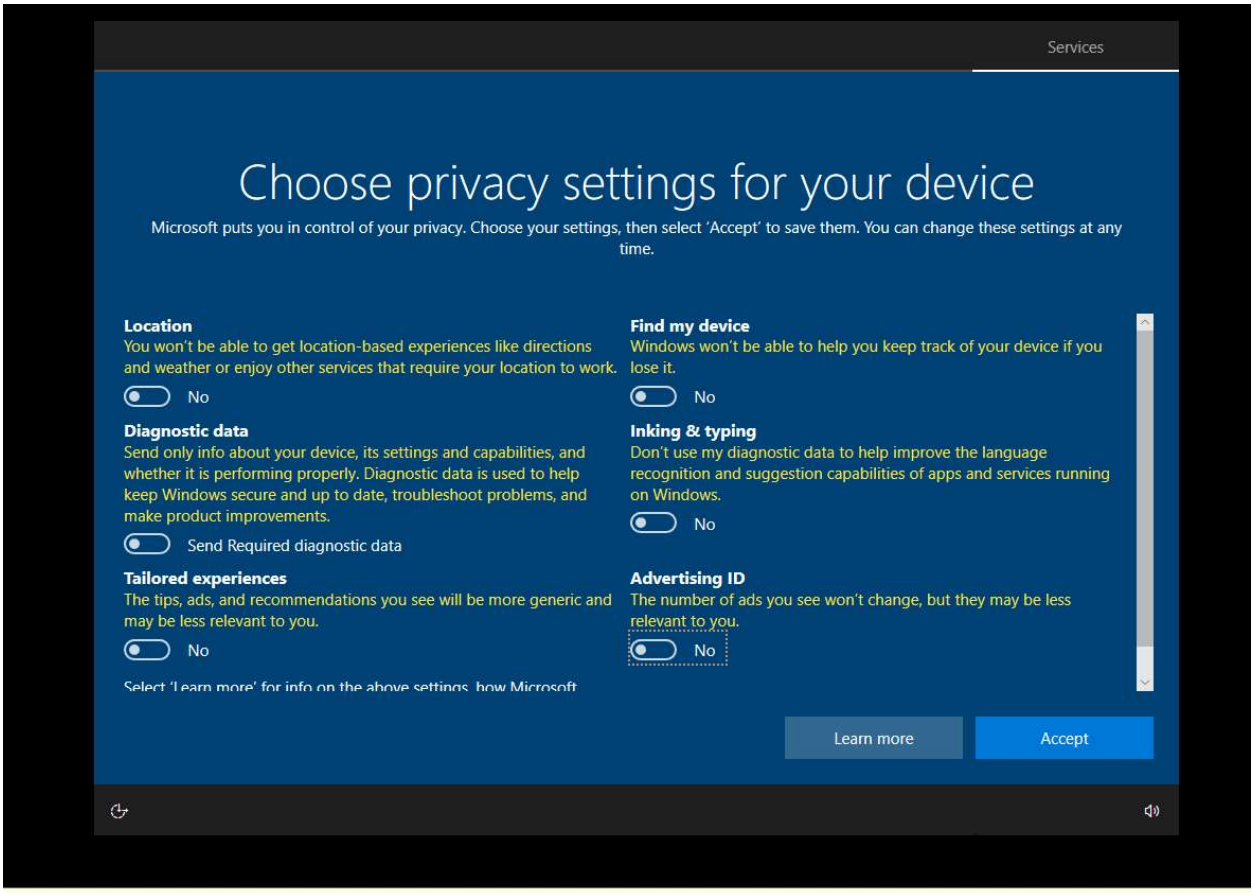

Figure 17:Toggling off the privacy settings.

4.3.4 Install VMware Tools

I installed VMware tools which adjust the windows 10 operating system. This makes windows 10 run smoothly inside VMware and provides features such as full-screen mode.

To install the VMware tools, I clicked on the “VM” option in the VMware toolbar. I then selected the “Install VMware tools” option from the dropdown menu that appeared.

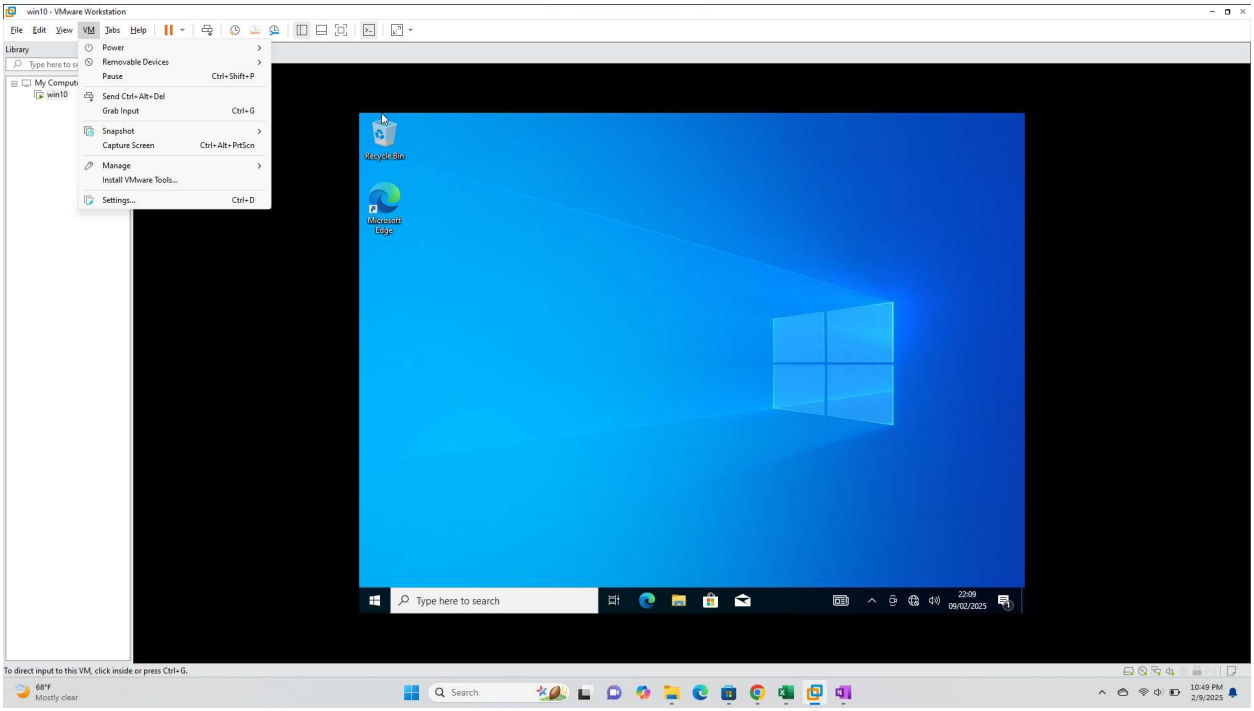

Figure 18: Selecting the "Install VMware tools" option.

I then went back into the win10 VM and opened “This PC” using File Explorer. Once there, I double clicked on DVD Drive (D:) VMware tools.

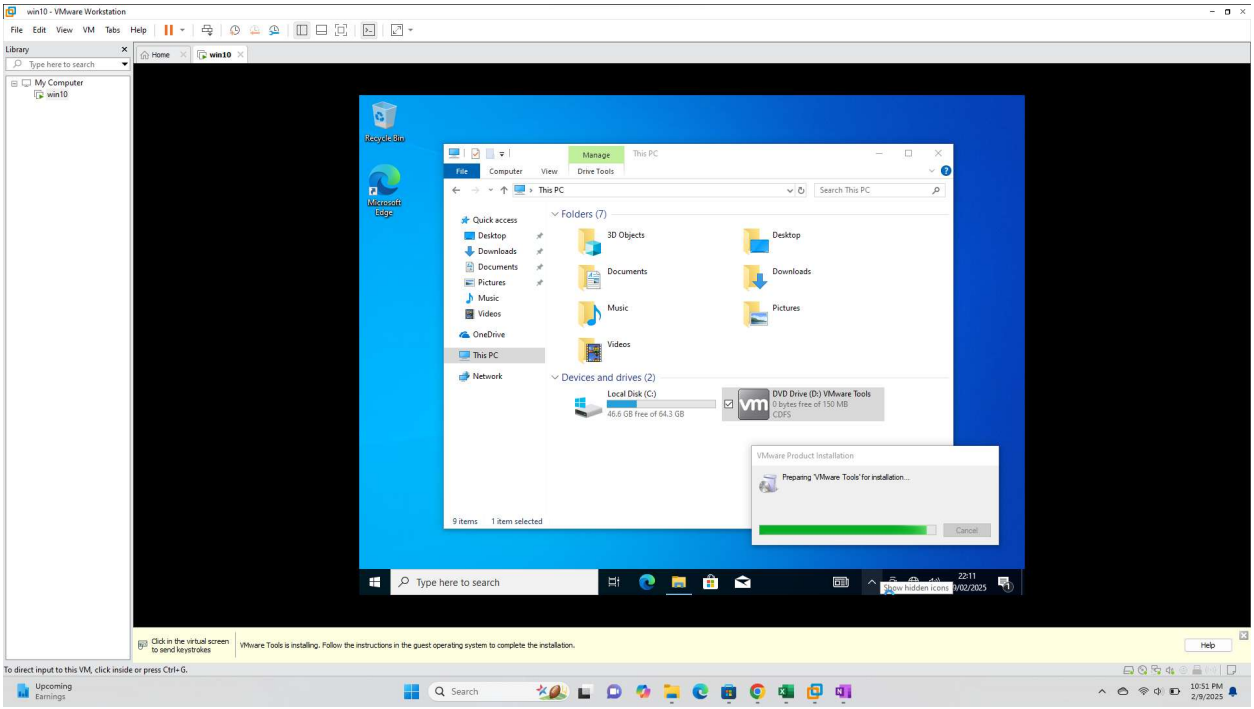

Figure 19: Installing VMware tools from the VMware DVD Drive.

After installing VMware tools, I was prompted to restart the VM which I did.

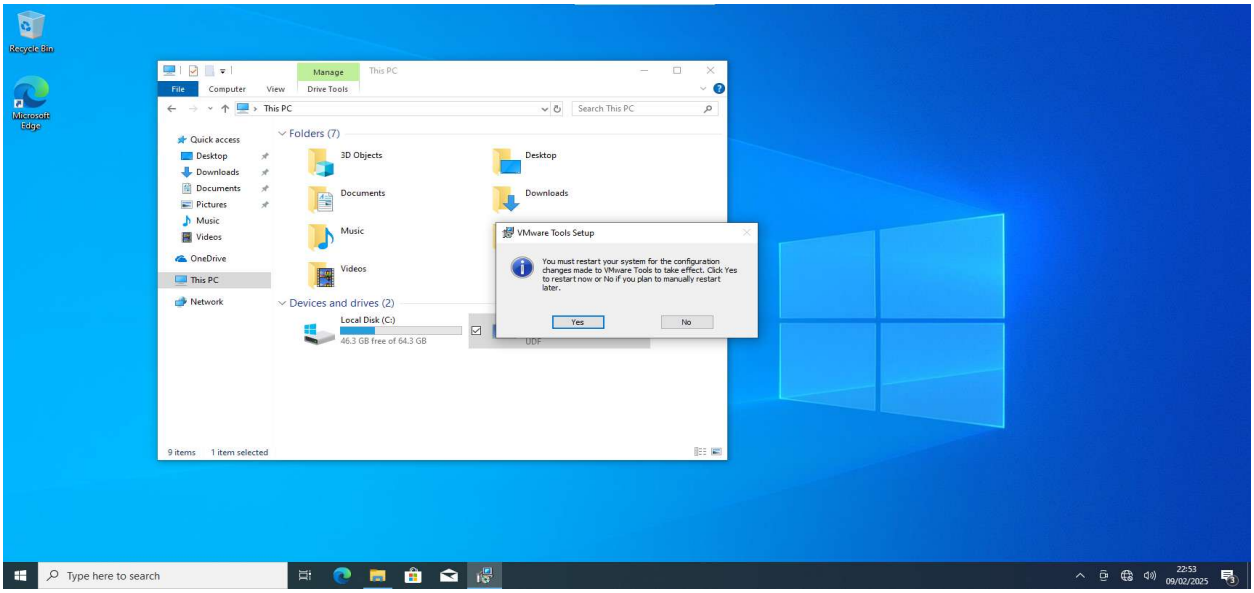

Figure 20: Restarting the VM after installing VMware tools.

4.3.5 Setup a Shared Folder.

I proceeded to create a shared folder which will enable me to send malware samples from my Host-OS to the win10 VM. I chose the folder to be read-only and selected the “enable until next power off or suspend” option.

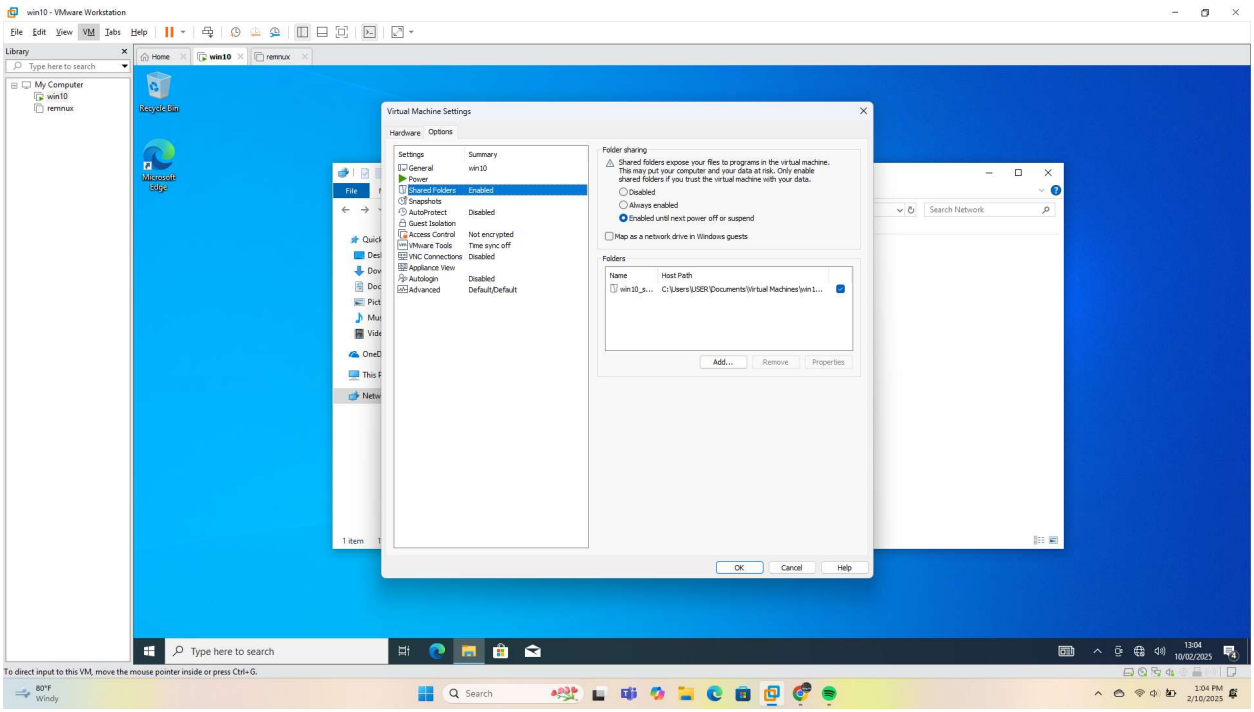

Figure 21:Setting up a shared folder.

4.4 Disable Windows Update.

I started to prepare the windows 10 Virtual Machine for the FLARE-VM installation by first disabling windows updates.

4.4.1 Open Local Group Policy Editor

I first opened the Local Group Policy editor by searching for “gpedit.msc” and opening it.

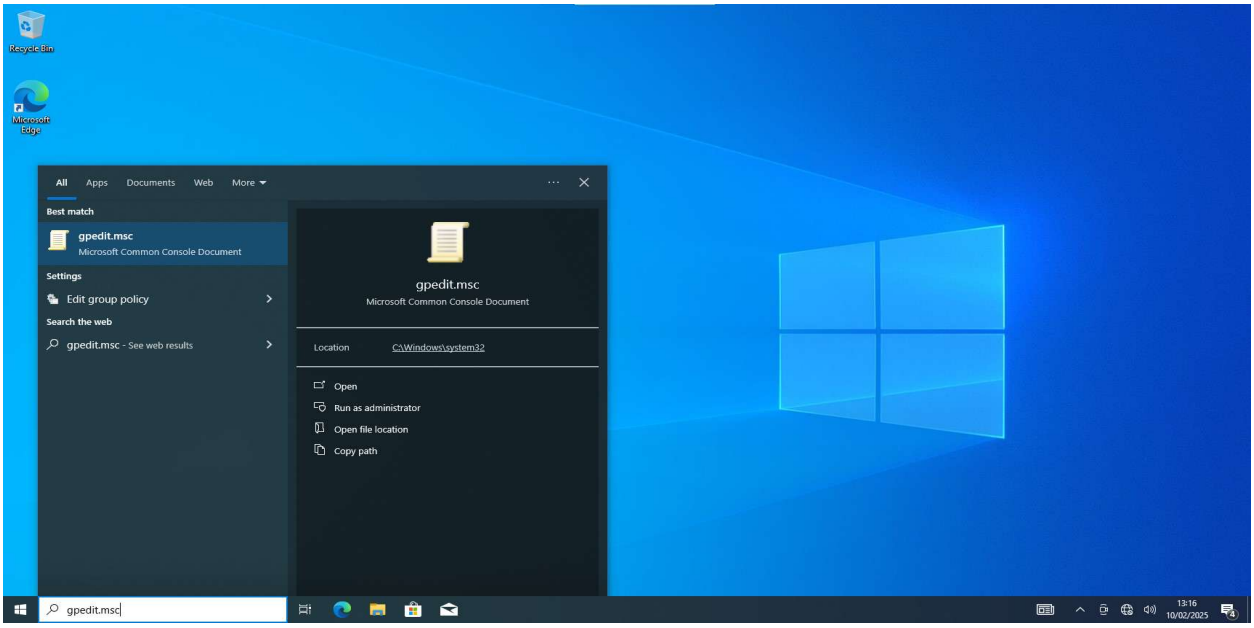

Figure 22:Opening Local Group Policy editor.

4.4.2 Locate Windows Update in Local Group Policy Editor

I then located the Windows Update setting in “Computer configuration > Administrative Templates > Windows Components > Windows Update”.

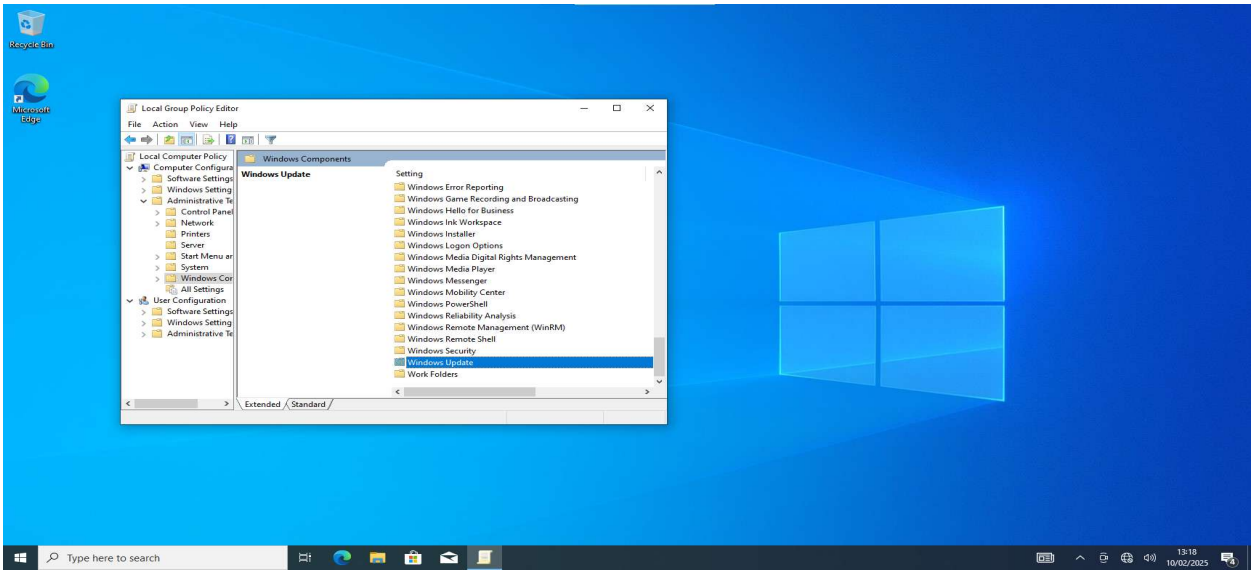

Figure 23:Locating the windows update setting.

4.4.3 Disable Automatic Updates.

I double clicked on it to configure the automatic updates.

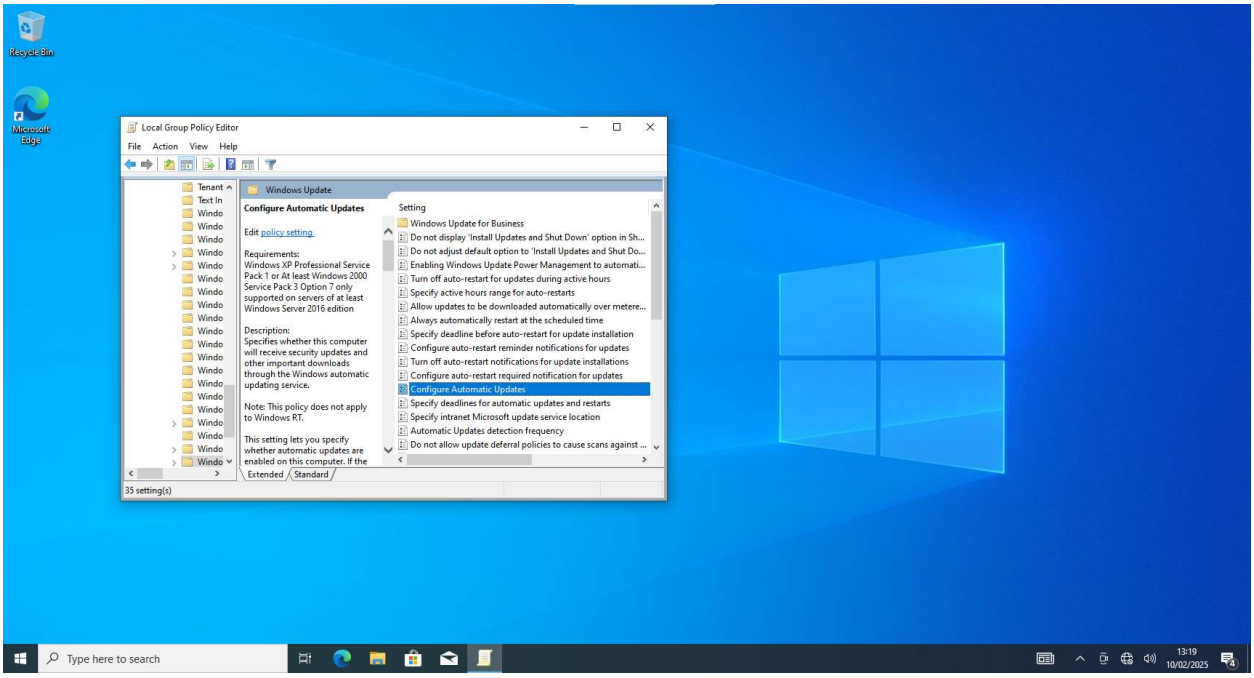

Figure 24:Configuring automatic updates.

I proceeded to double click on the “Configure Automatic Updates” setting to open its editor. I then chose the “Disabled” option to disable automatic updates. I clicked ok afterwards.

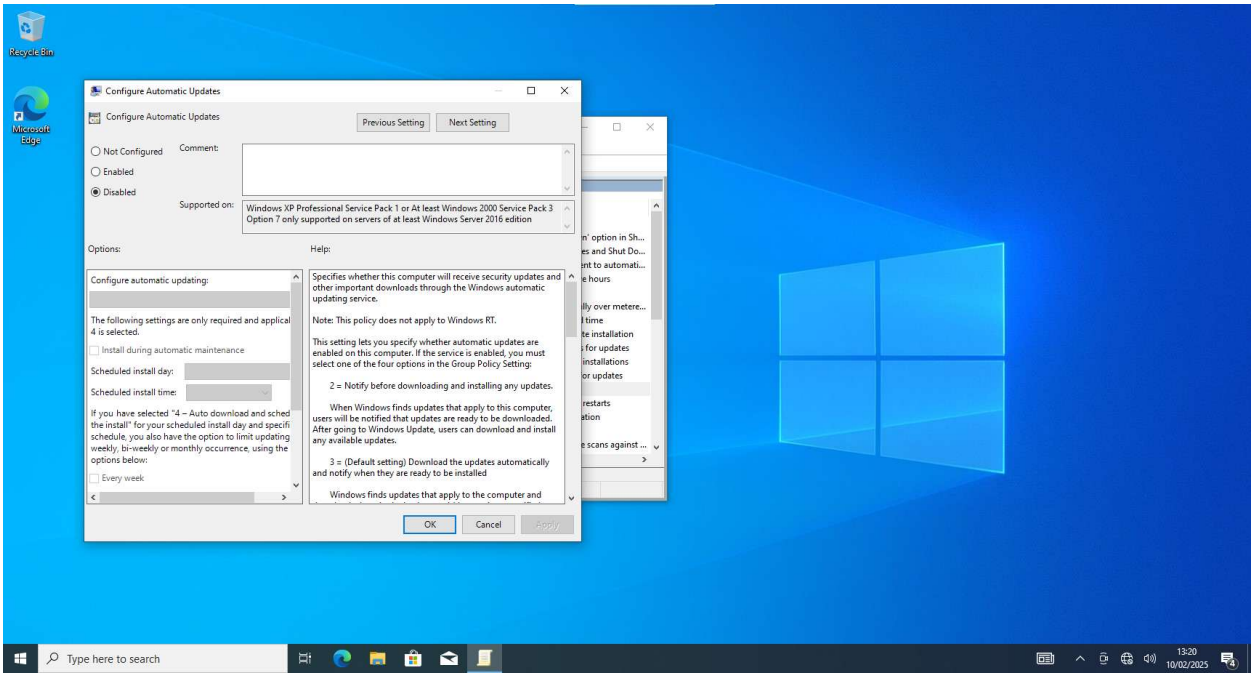

Figure 25:Disabling automatic updates

4.5 Disable Tamper Protection.

I disabled tamper protection in the following steps.

4.5.1 Open Windows Security

I opened windows security by searching for it on the search bar and pressing enter.

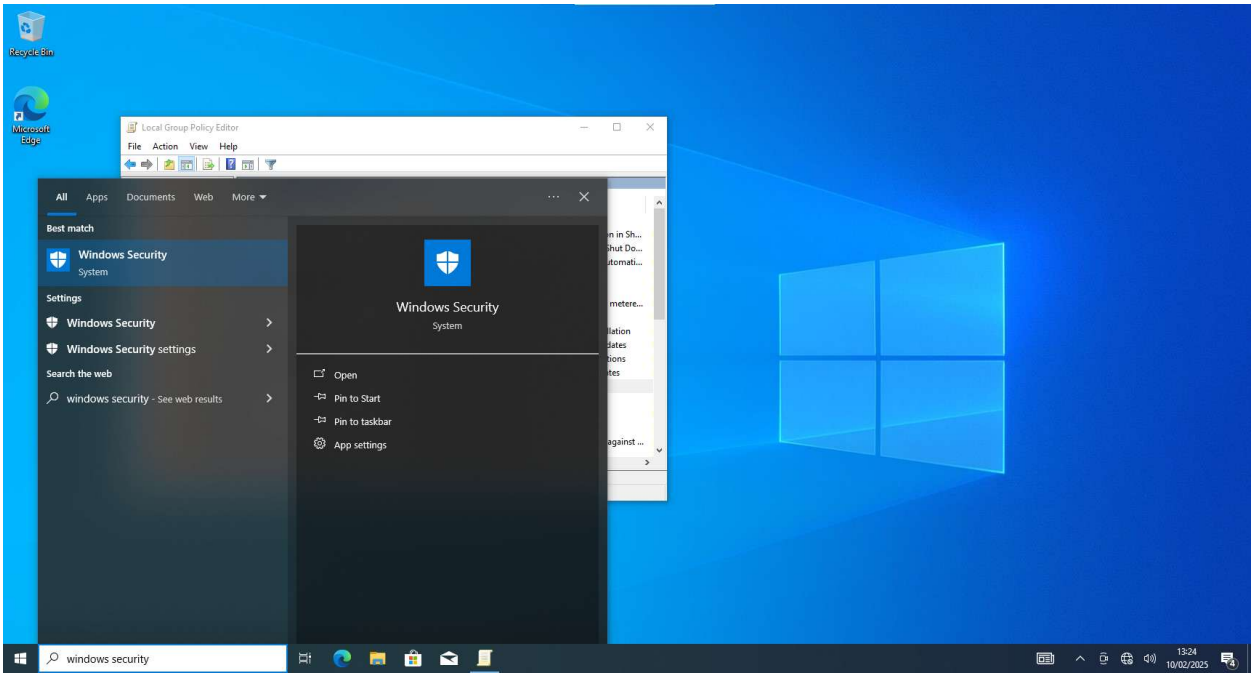

Figure 26: Opening Windows Security.

4.5.2 Navigate to Virus and Threat Protection

After Opening Windows Security, I navigated to Virus and Threat Protection by Clicking on the shield icon named “Virus and threat protection” and then opening virus and threat protection settings.

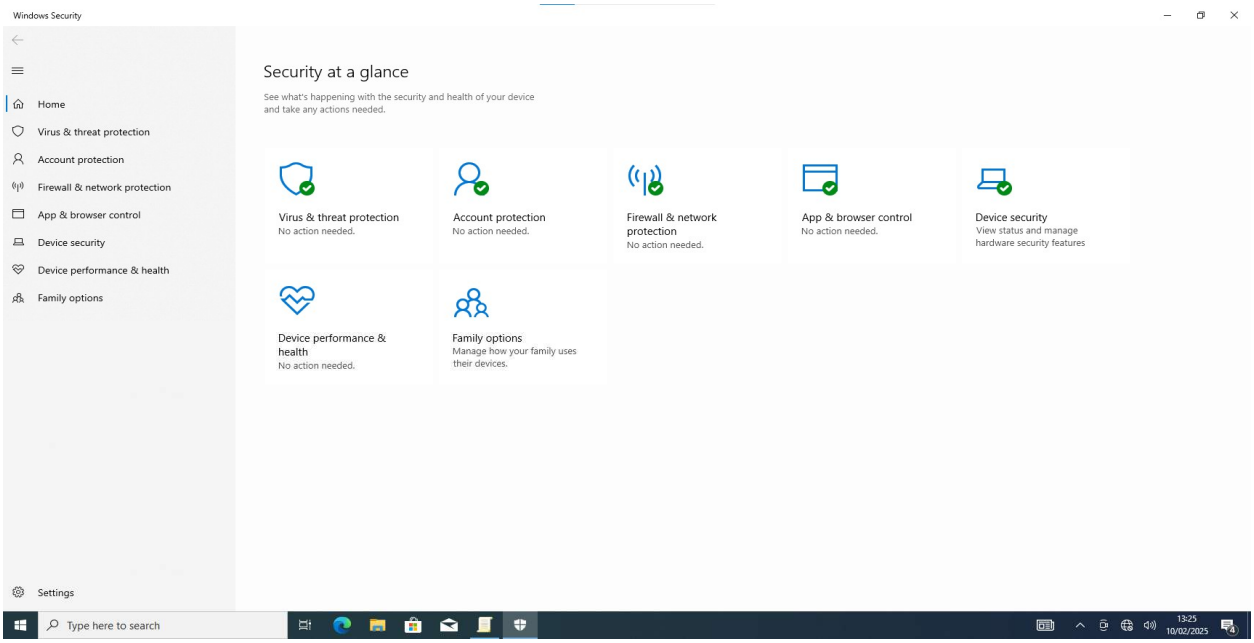

Figure 27: Navigating to Virus and Threat Protection

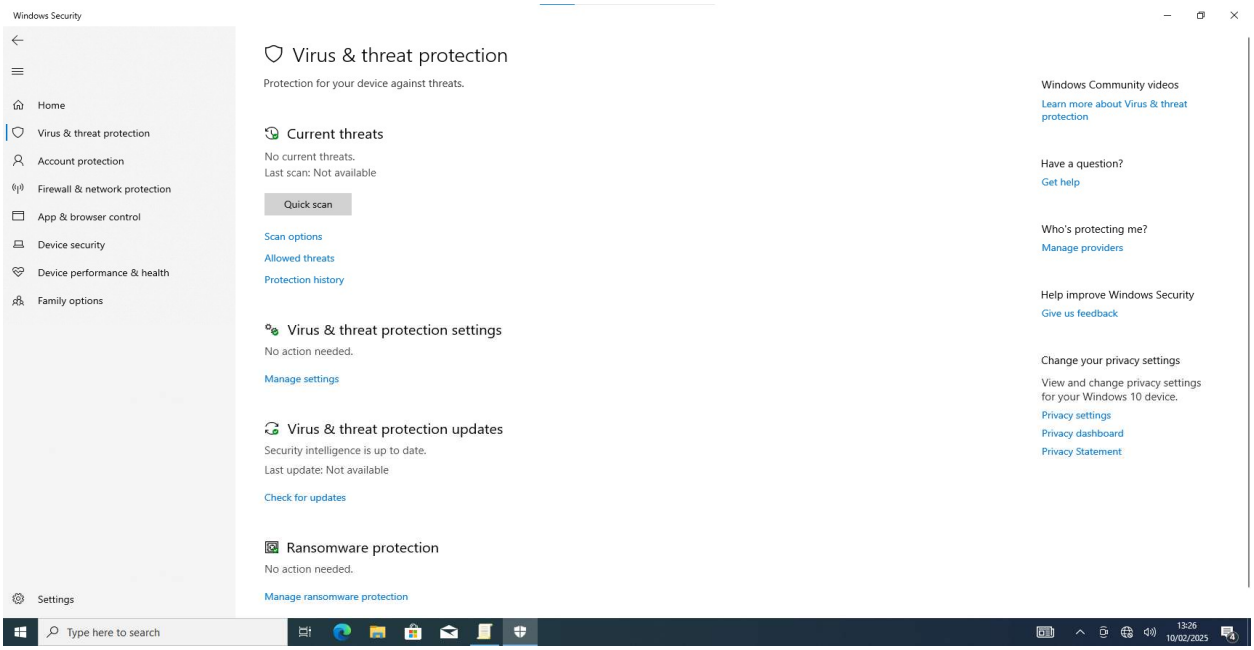

Figure 28: Navigating to the Virus and threat protection settings.

4.5.3 Disable Tamper Protection Option.

I opened Virus and threat protection and proceeded to toggle off all the settings which include:

Real-time protection, Cloud-delivered protection, automatic sample submission and finally tamper protection.

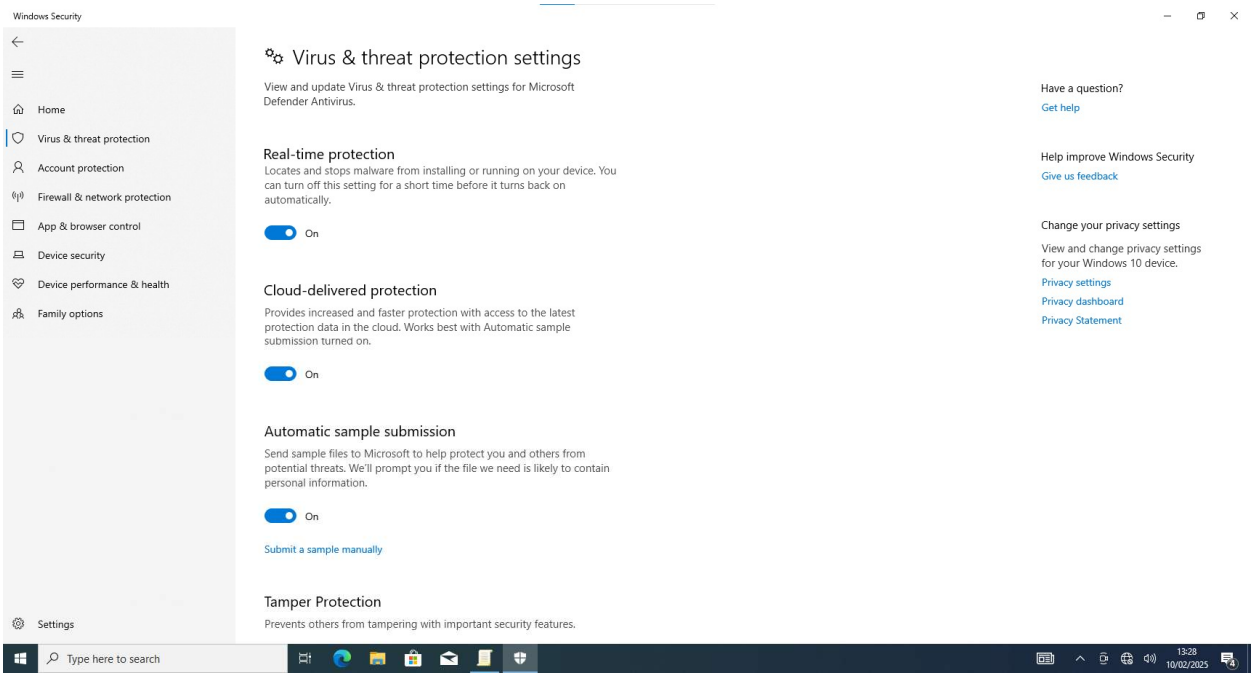

Figure 29:Virus and threat protection settings toggled on.

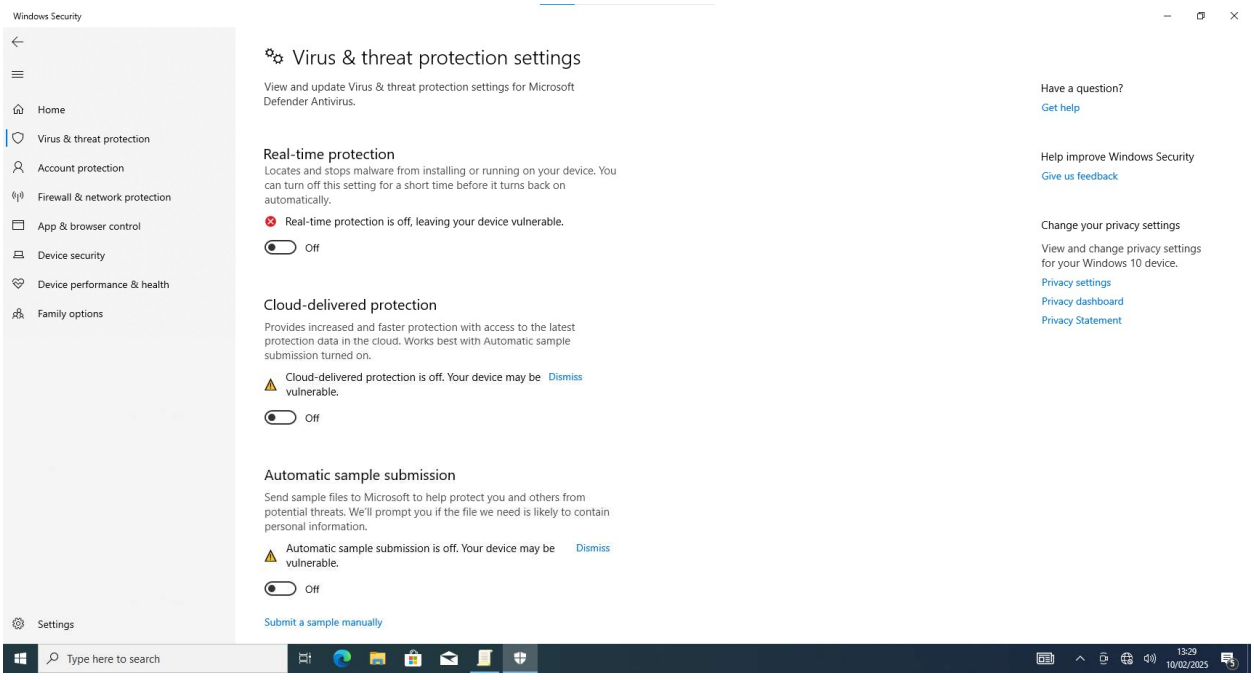

Figure 30: Virus and threat protection settings toggled off.

4.6 Disable Microsoft Defender Antivirus.

I turned off Microsoft Defender Antivirus in the following steps.

4.6.1 Open Local Group Policy Editor.

I opened the local group policy editor by searching for “gpedit.msc” on the search bar and hitting enter.

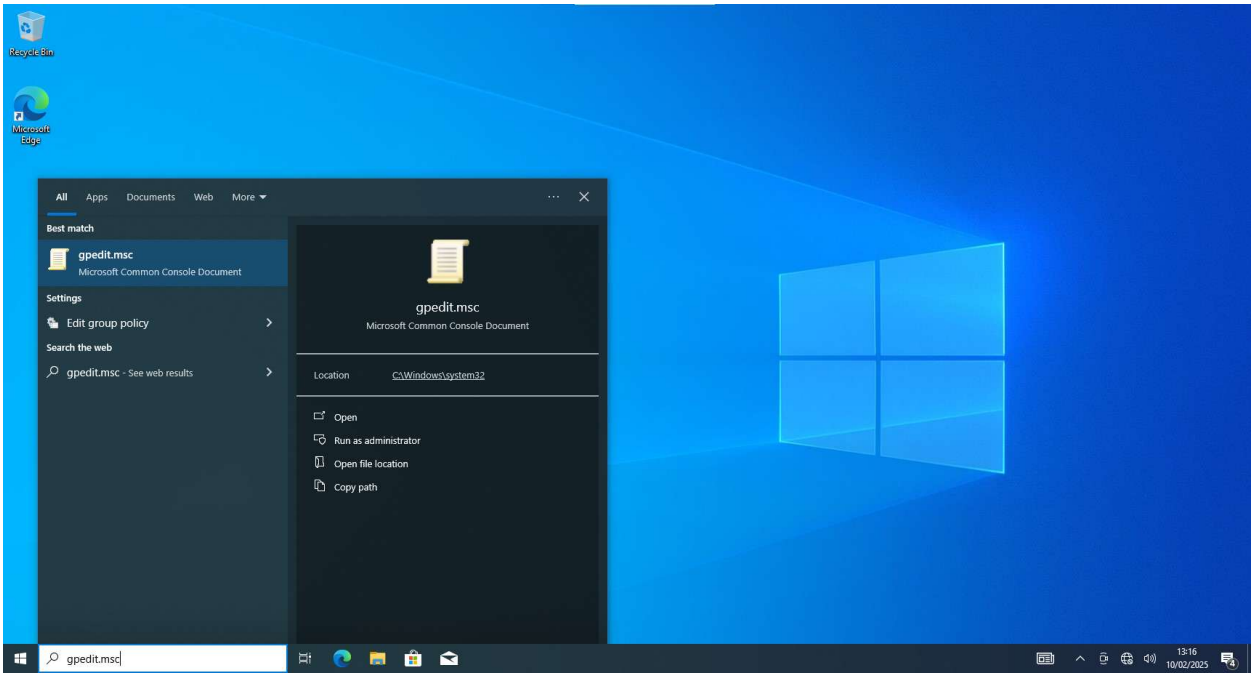

Figure 31: Opening local group policy editor to disable Microsoft Defender.

4.6.2 Locate Microsoft Defender Antivirus.

I proceeded to locate Microsoft Defender Antivirus inside the Local Group Policy editor. It was located under “Computer configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus”. I double clicked on it.

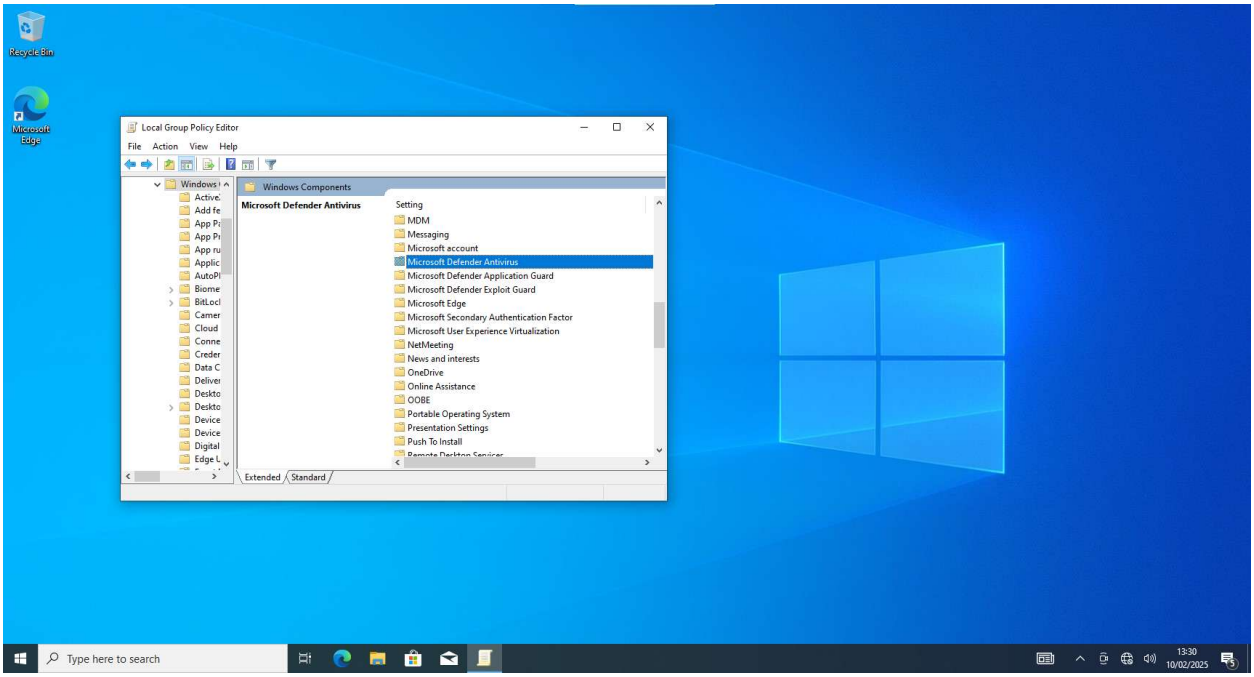

Figure 32: Locating Microsoft Defender Antivirus.

4.6.3 Disable Microsoft Defender.

After double clicking on Microsoft Defender, I located the “Turn off Microsoft Defender Antivirus” option and I proceeded to enable it.

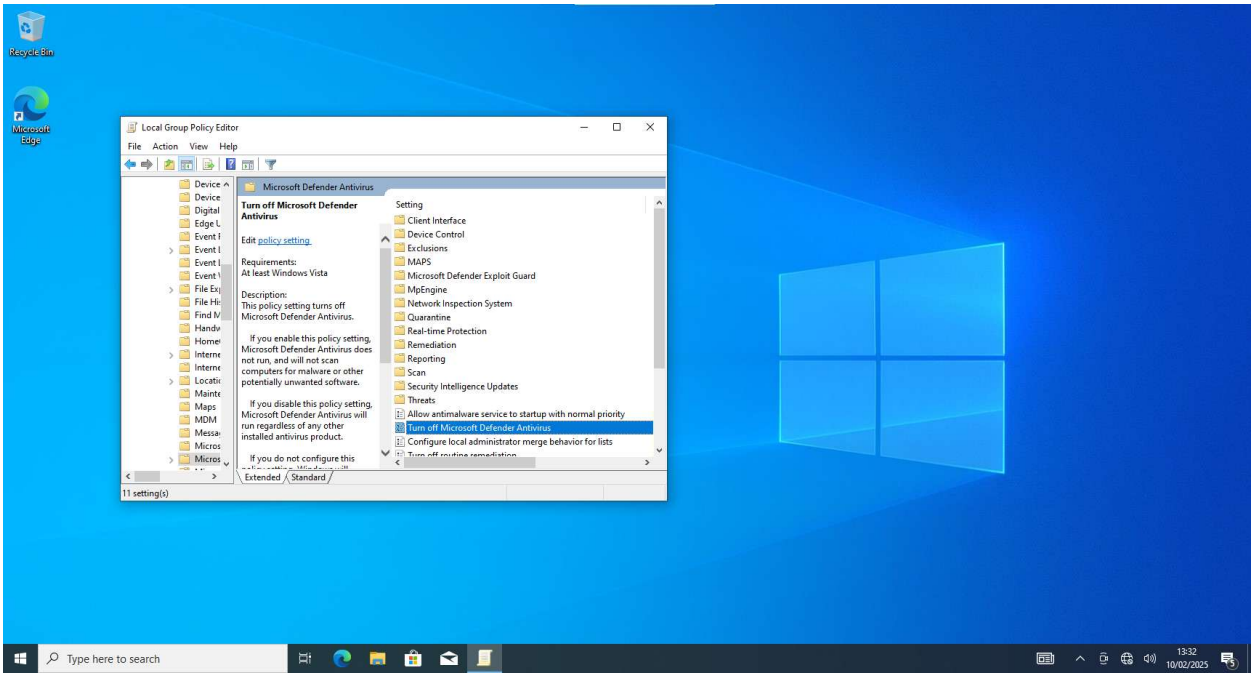

Figure 33:Locating the "Turn off Microsoft Defender Antivirus setting".

4.7 Take a Snapshot of the VM.

I took a snapshot of the virtual machine to save the then current state of the windows 10 VM. I named preFlareVM and gave it a brief description.

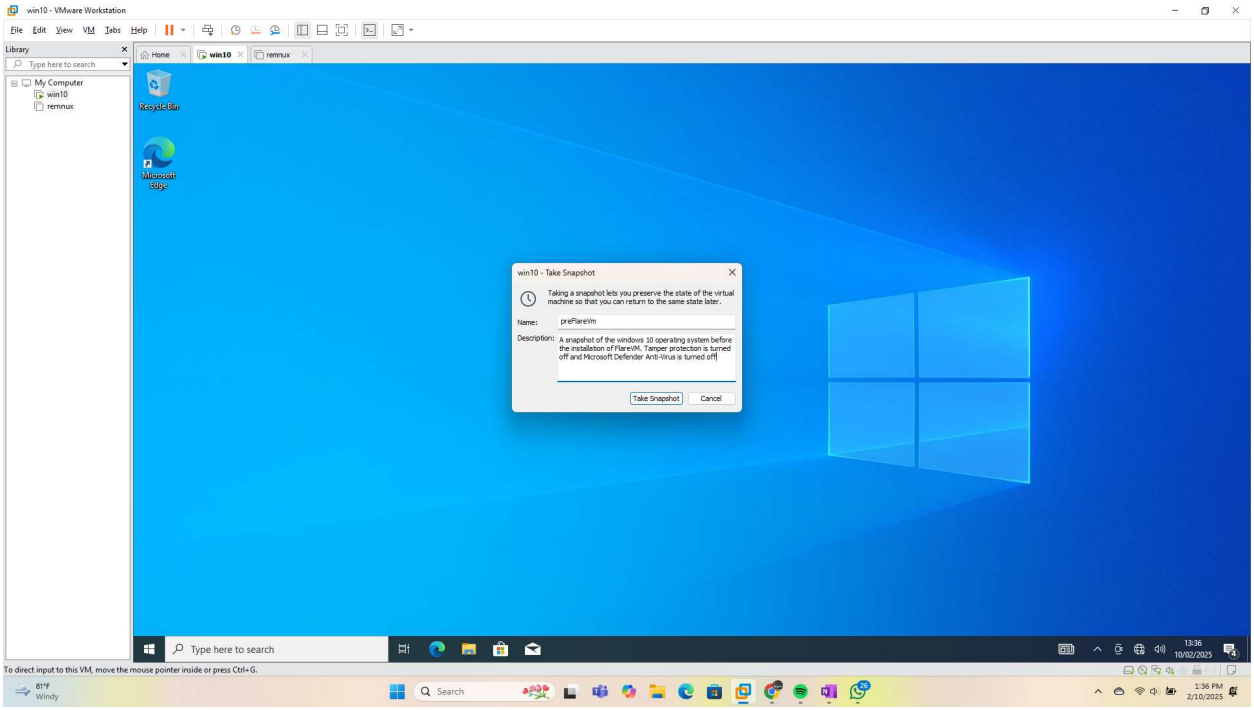

Figure 34: pre-flareVm snapshot.

4.8 Install FLARE-VM

I started to install FLARE-VM because the windows 10 virtual machine was ready for FLARE-VM.

4.8.1 Establish Internet Connection.

I confirmed that the virtual machine had an internet connection because the Network Adapter was set to NAT mode.

4.8.2 Download FLARE-VM installer script.

I opened PowerShell with administrative privileges and ran the command for downloading the FLARE-VM installation script and navigated to the desktop where it was downloaded to.

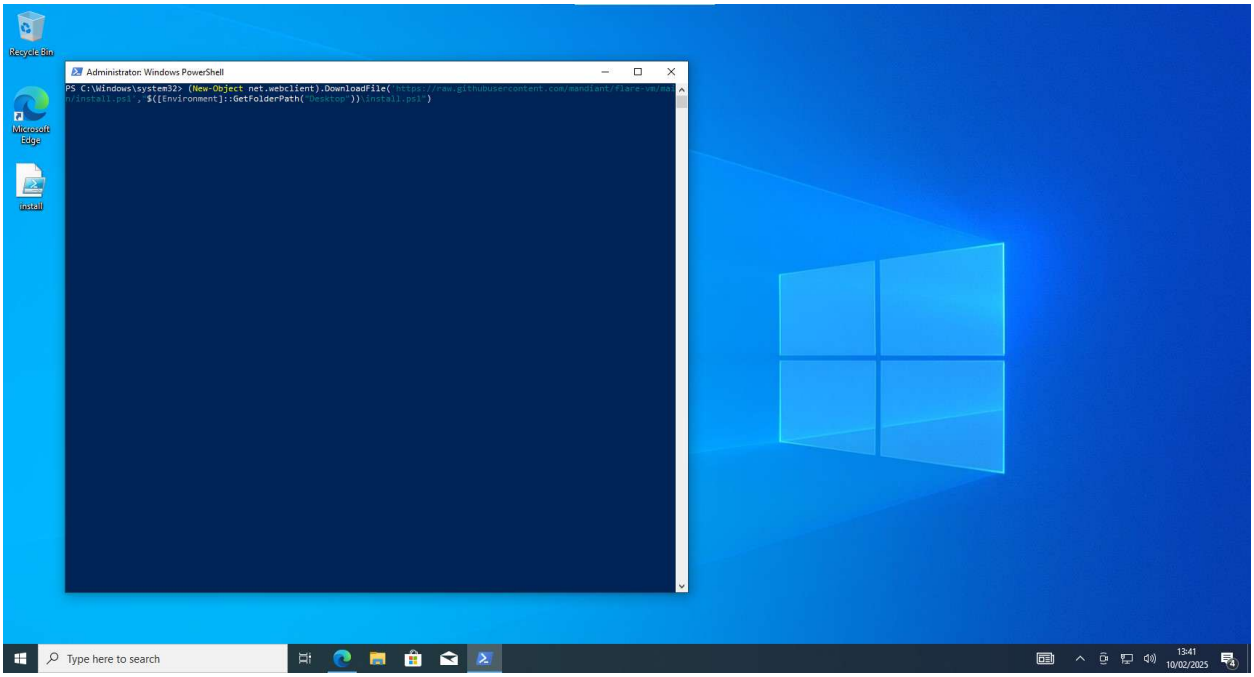

Figure 35: Downloading FLARE-VM installation script.

4.8.3 Unblock the Installation script

I proceeded to unblock the installer.ps1 file for it to be able to run.

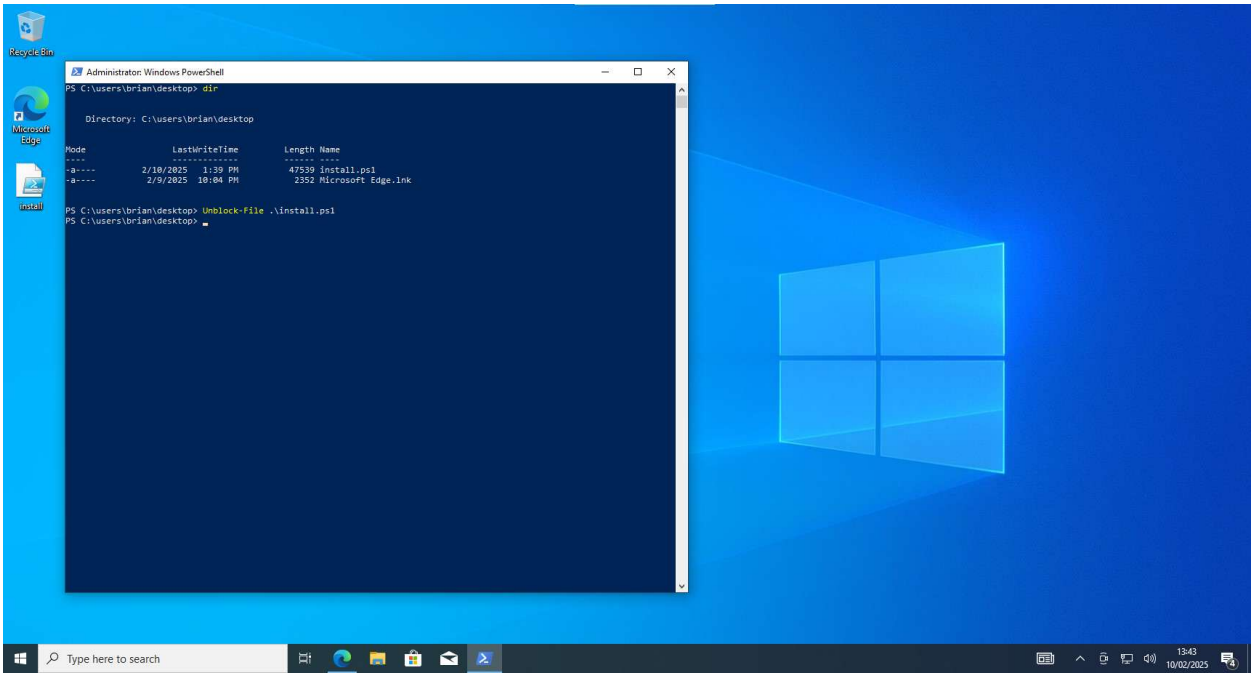

Figure 36: Unblocking the installer script.

4.8.4 Change execution policy.

I changed the execution policy to enable the installer perform privileged operations on the windows 10 virtual machine.

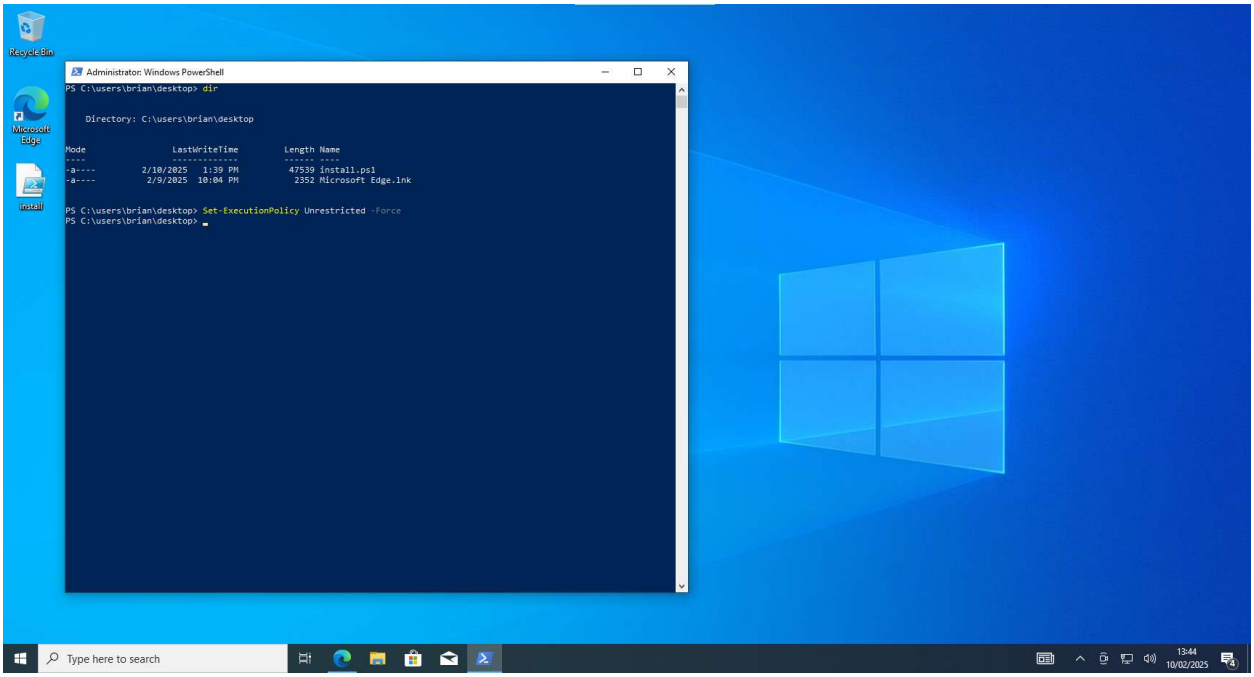

Figure 37: Changing the execution policy

4.8.5 Run installation script.

I proceeded to run the installer.ps1 file and let FLARE-VM install.

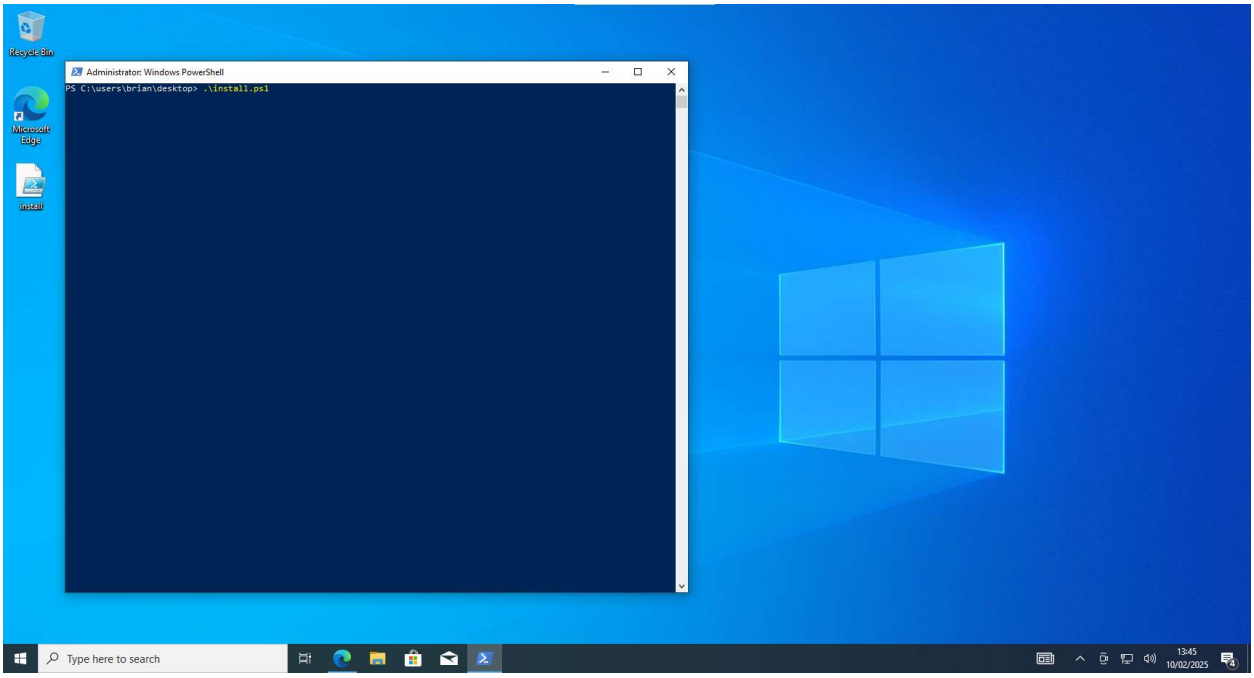

Figure 38:Running the installer script.

The FLARE-VM installation began and I was asked whether I had taken a snapshot, to which I responded with “y” to mean yes, since I did in fact take a snapshot of the system.

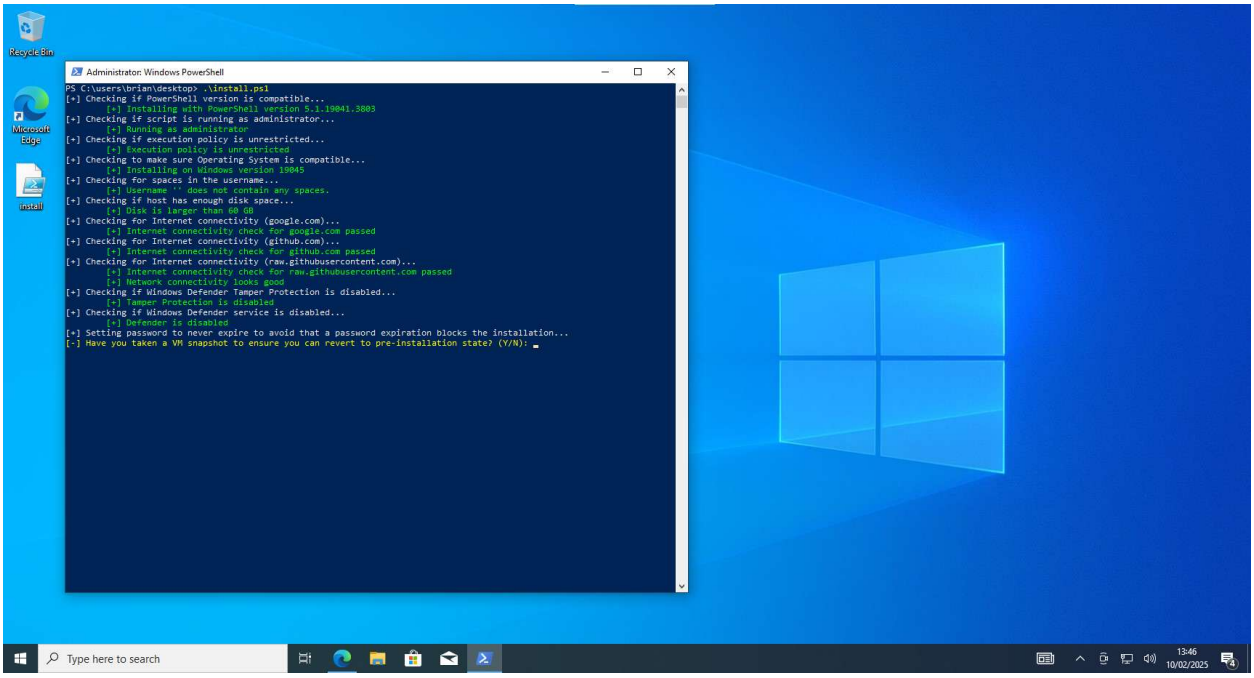

Figure 39:Snapshot confirmation during FLARE-VM installation.

After responding yes to the prompt about whether or not I took a snapshot, I was prompted to enter the credentials for the windows 10 virtual machine which I set up during installation.

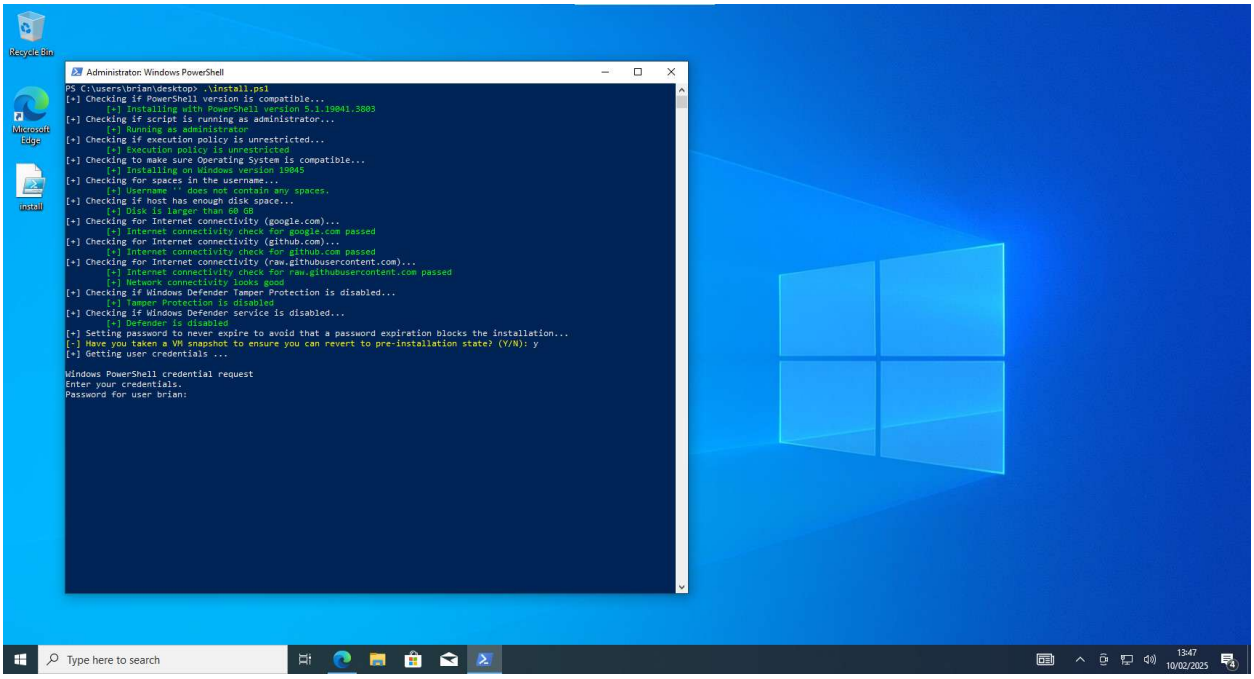

Figure 40:Prompt for credentials during FLARE-VM installation.

After entering my credentials, FLARE-VM began installing. Chocolatey is installed to install everything else using the Boxstarter Module installer.

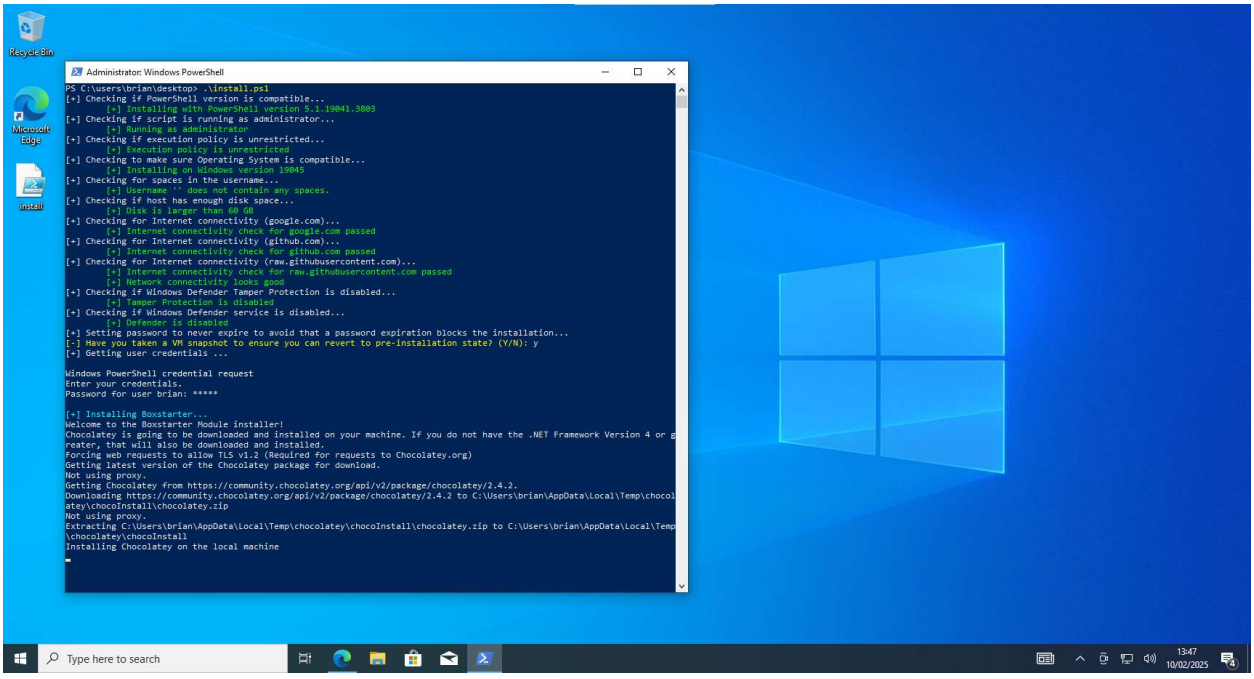

Figure 41: FLARE-VM installation begins by installing chocolatey

I was then presented with the FLARE-VM Install Customization window. I left everything on default and pressed ok.

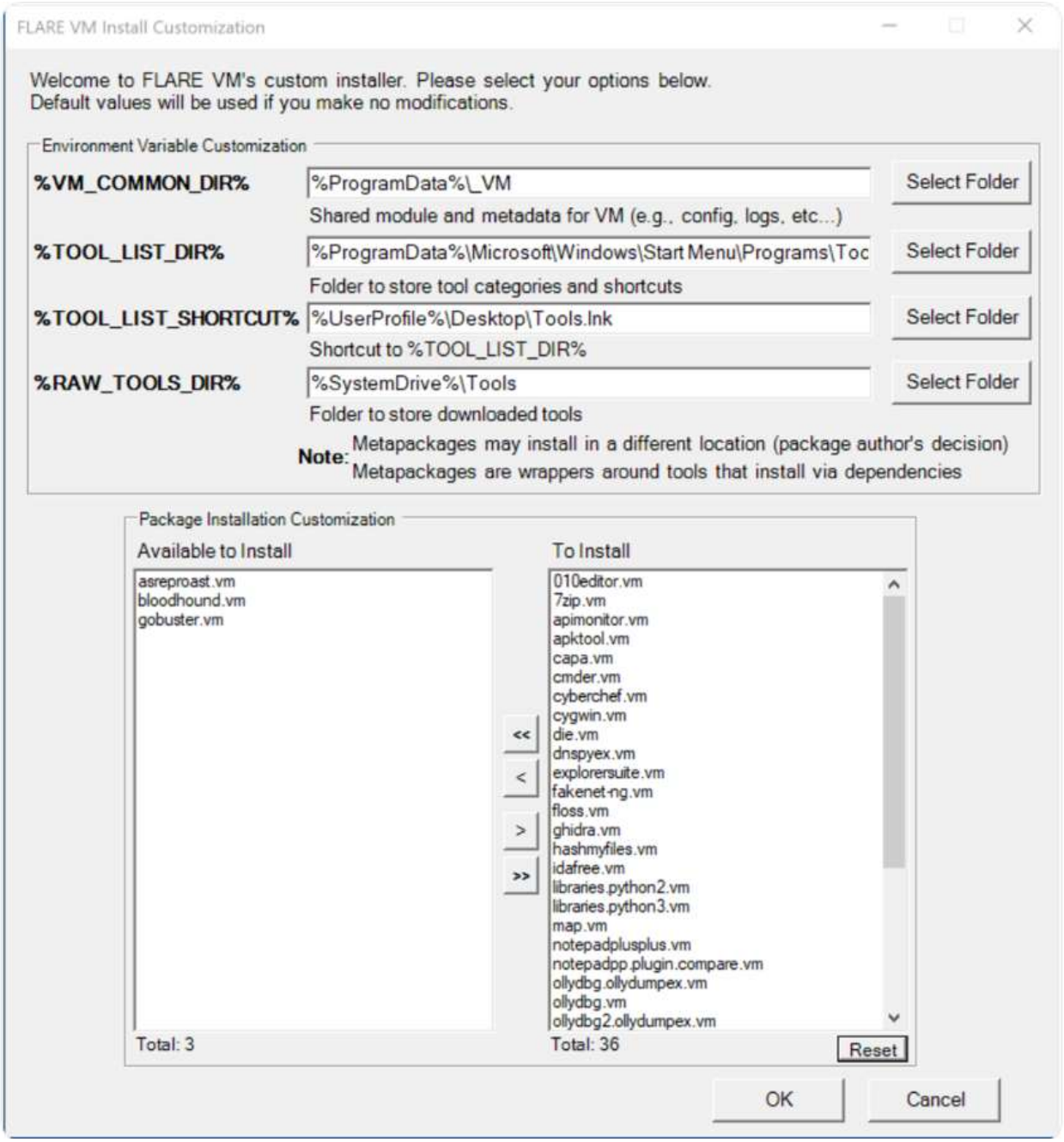

Figure 42:FLARE-VM Install Customization window.

The installation then proceeded as expected and FLARE-VM was fully installed on my windows 10 virtual machine. After the installation I was presented with a log of the installation stored in a file named “log.txt”.

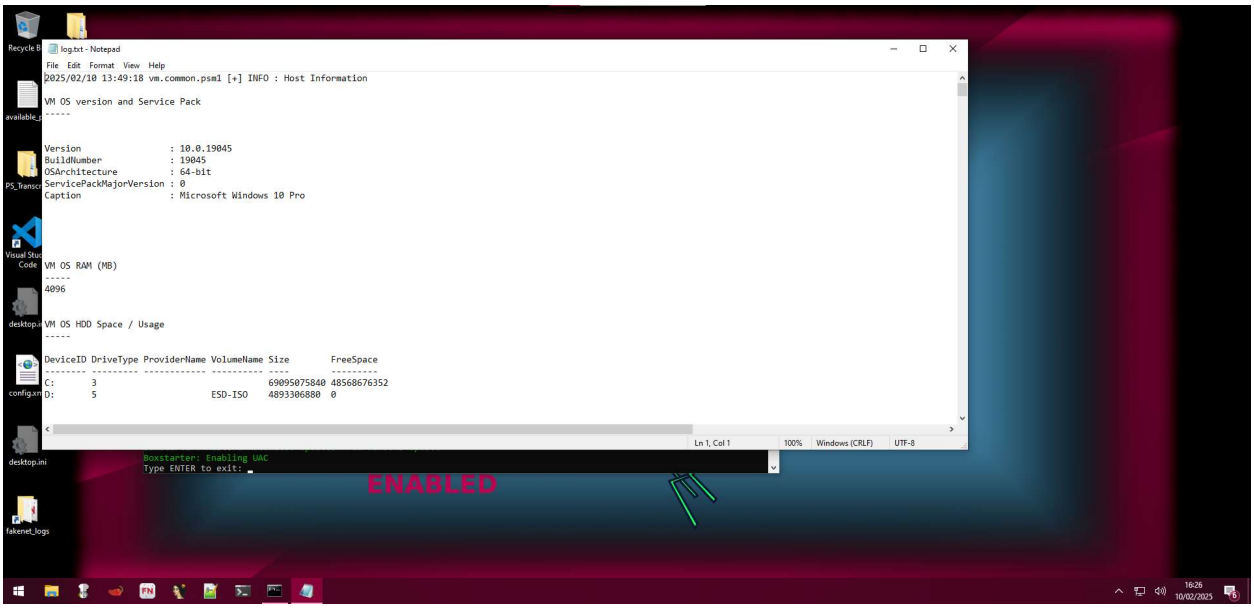

Figure 43: Installation logs after FLARE-VM was installed.

4.9 Take a Snapshot

I took a snapshot of the FLARE-VM system to save its state. This snapshot will be important because I will need to a point to go back to after I ran malware inside the virtual machine. I named the snapshot “Flare Vm” and gave it a brief description.

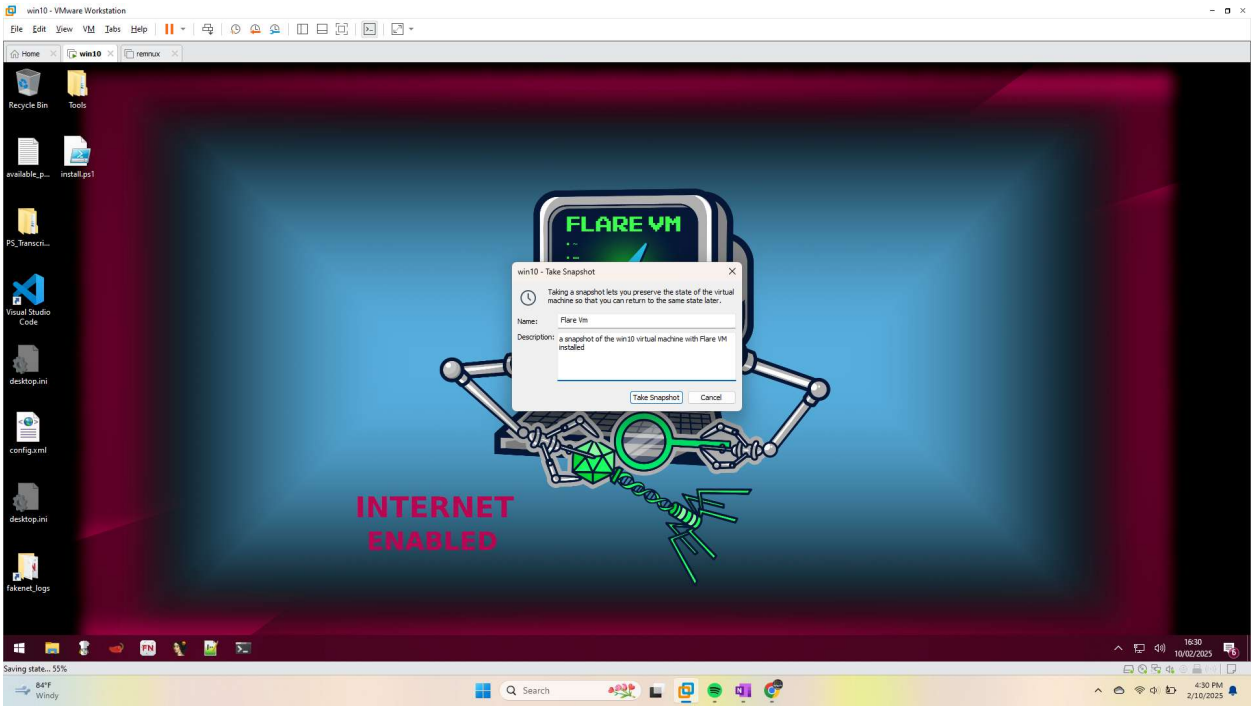

Figure 44: FLARE-VM snapshot.

5. SCREENSHOTS AND EVIDENCE.

I took a variety of screenshots during the installation process which are evidence of the installed system.

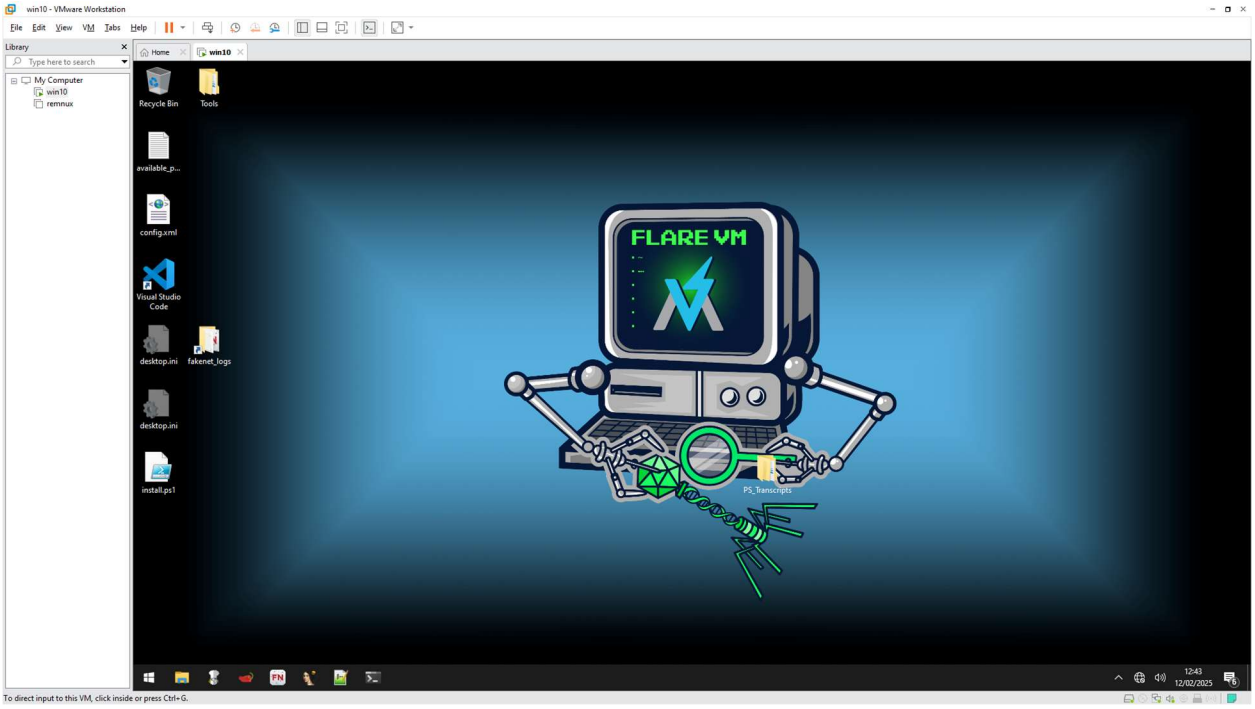

Figure 45:FLARE-VM fully installed with internet connectivity disabled.

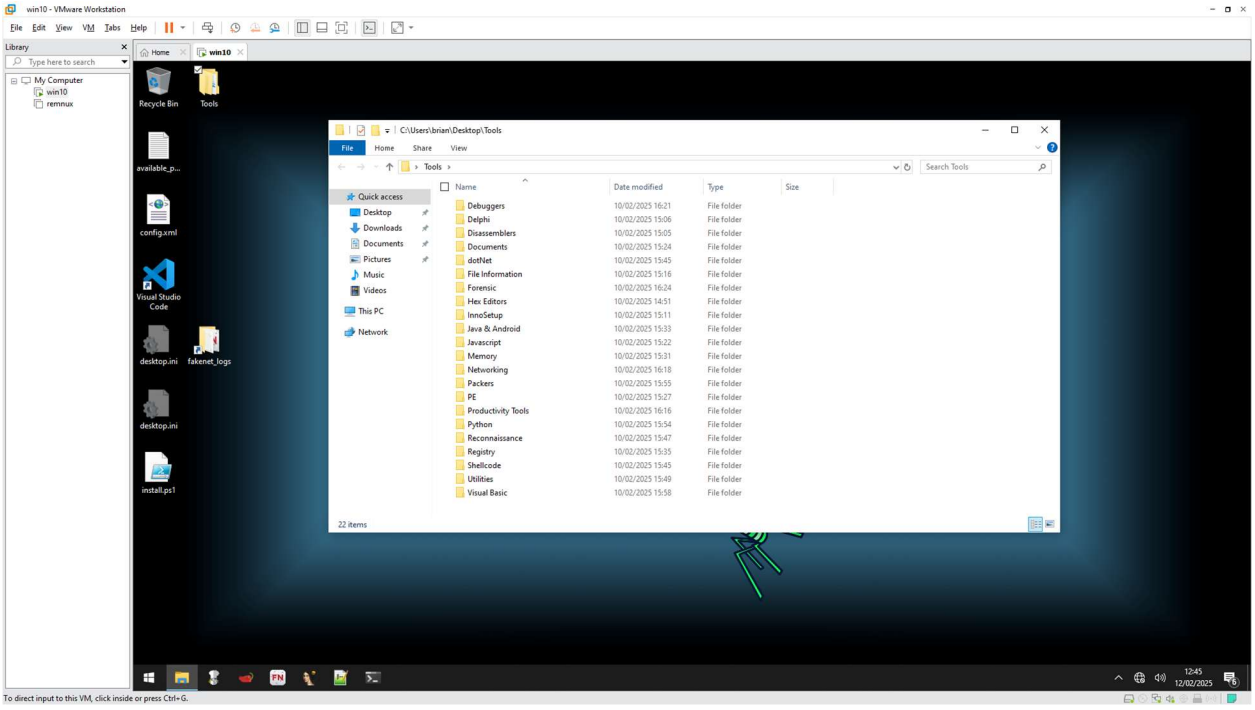

Figure 46: Tools folder in the desktop.

6. ANALYSIS AND FINDINGS.

I proceeded to analyze the FLARE-VM environment and I documented the following findings.

6.1 Vast array of malware analysis tools.

I found out that FLARE-VM had a very large number of cutting-edge tools that are used in malware analysis and reverse engineering.

6.1.1 Debuggers

I established that FLARE-VM had the following debuggers but was not limited to these only:

1. WinDbg.
2. X32dbg.
3. X64dbg.

6.1.2 Disassemblers.

I established that FLARE-VM had the following debuggers but was not limited to these only.

1. Ghidra.
2. IDA pro.

6.1.3 Networking tools.

I found the following tools that were used to create fake networks for malware analysis and network analysis tools.

1. Wireshark.
2. FakeNet.
3. Internet_detector.
4. WinDump.

FLARE-VM has a lot of other tools that tools for malware analysis and reverse engineering.

6.2 Malware samples provided for practice.

I found out that FLARE-VM contains malware samples from the book, “Practical Malware Analysis” by Andrew Honig and Michael Sikorski. This is extremely important for practice since the book is a recommended resource by experts in the field of Malware analysis and Reverse engineering.

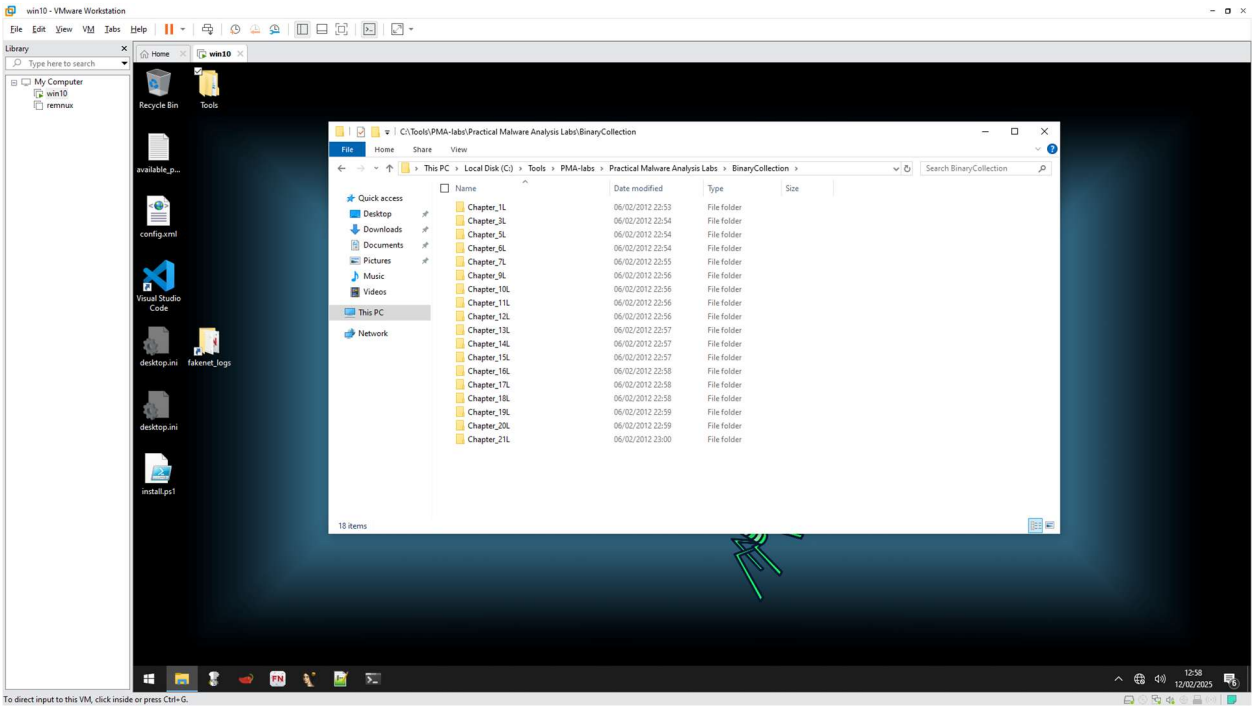

Figure 47:Practical Malware Analysis lab malware samples provided in FLARE-VM.

7. CHALLENGES AND SOLUTIONS.

I found the lab to be fairly straightforward and easy but I did encounter one challenge during the Lab Setup process.

7.1 Windows 10 home lacks access to Local Group Policy editor.

I installed windows 10 home in my initial windows 10 installation and took a snapshot. I tried to access the Local Group Policy editor to disable Windows Updates but I could not access the management console. I concluded that windows 10 home does not have access to such functions.

7.1.1 Solution to lack of access to Local Group Policy editor.

I decided to begin the windows 10 installation again and select windows 10 pro during the installation process. This fixed my problem and I proceeded with the installation.

8. CONCLUSION.

I concluded that FLARE-VM is the best and quickest way to setup a malware analysis and reverse engineering lab. I found the installation process fairly intuitive with very little possibilities for errors.

FLARE-VM is a robust sandbox environment tailored for beginners and seasoned professionals alike.

9. RECOMMENDATIONS

I would recommend the following during this lab setup.

9.1 Install Windows 10 pro.

I would recommend that everyone to choose windows 10 pro when they will install the windows 10 operating system as the guest OS. This will avoid some issues such as being unable to access the local group policy editor.

9.2 Run the virtual machine on a capable host machine.

I would recommend that the virtual machine and hypervisor run on a computer with adequate RAM and storage to be able to allocate the required quantity. You cannot change the size of the disk of the virtual machine after taking a snapshot, so to avoid having to restart the whole installation process from scratch, allocate adequate space for the FLARE-VM environment.

10. REFERENCES.

Windows 10 ISO download: https://www.microsoft.com/en-us/software-download/windows10ISO

Disabling windows update guide: https://www.windowscentral.com/how-stop-updates-installing-automatically-windows-10

Disabling Tamper protection Guide: https://superuser.com/a/1757341

Installation guide: Lab Setup.pdf document provided by the institution.