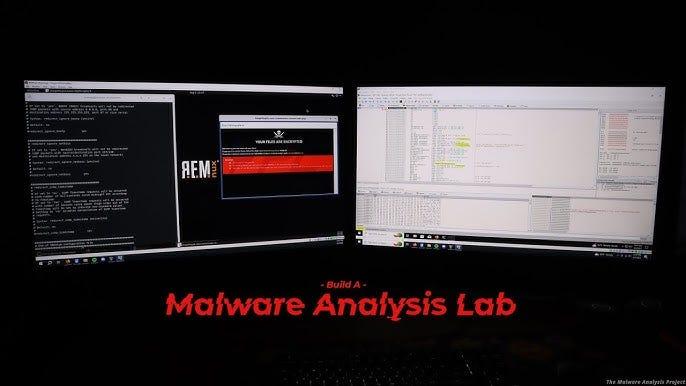
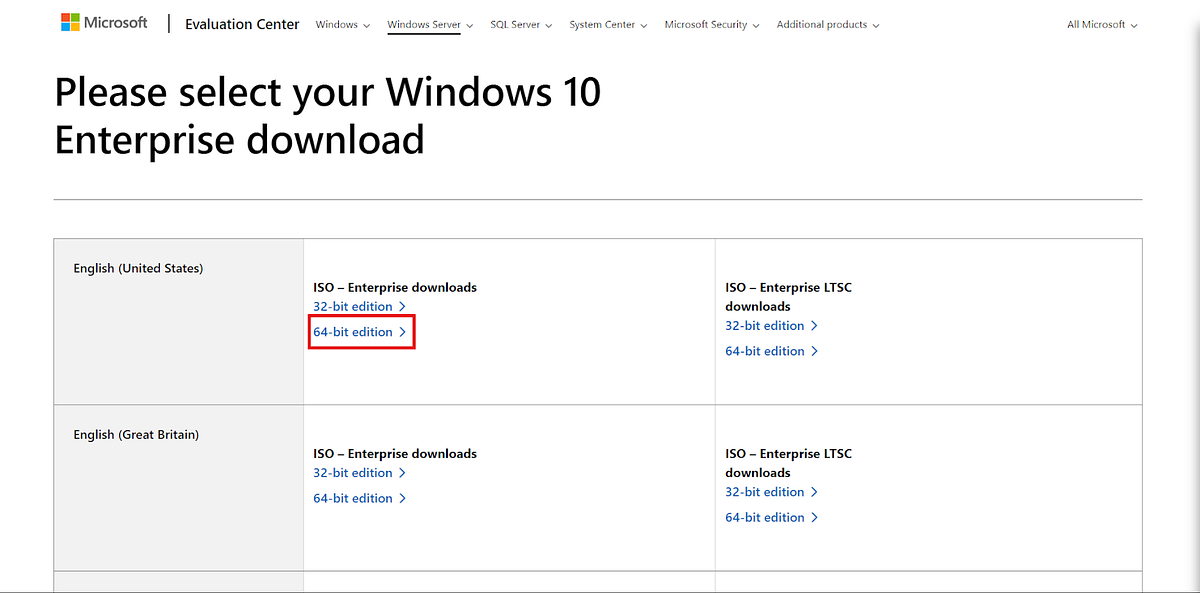
### **MALWARE ANALYSIS LAB SETUP**

****

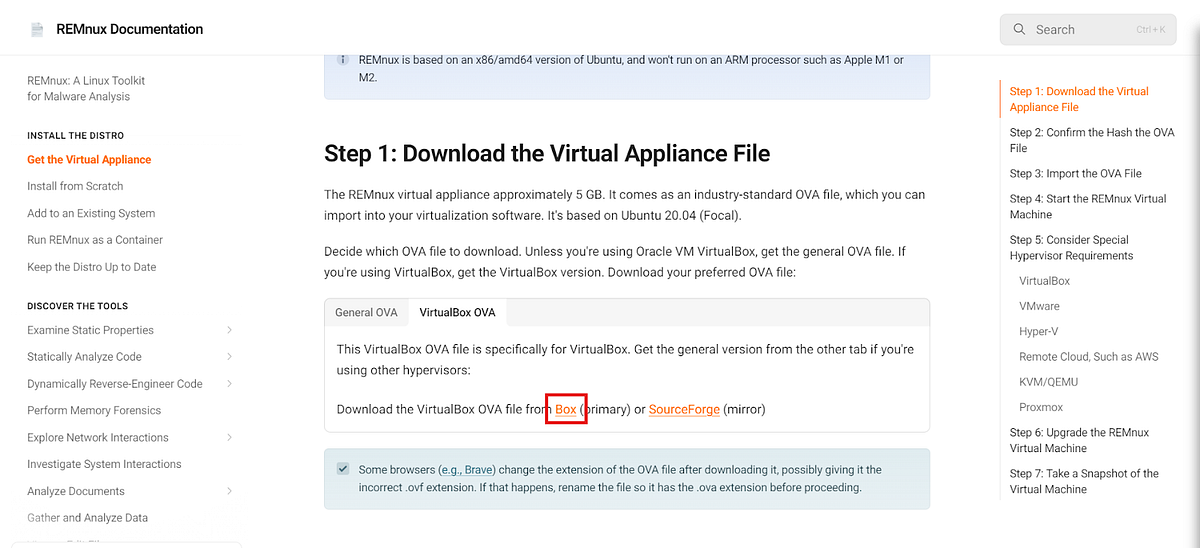
Here I create a sandbox environment to safely detonate and analyse the malware samples. For this I am using the FlareVM(a collection of software installation scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a virtual machine (VM)) and Remnux(a Linux toolkit for reverse-engineering and analysing malicious software) on the Virtual box Hypervisor. The Remnux VM acts as a C2 server.

#### **Windows Virtual Machine Installation:**

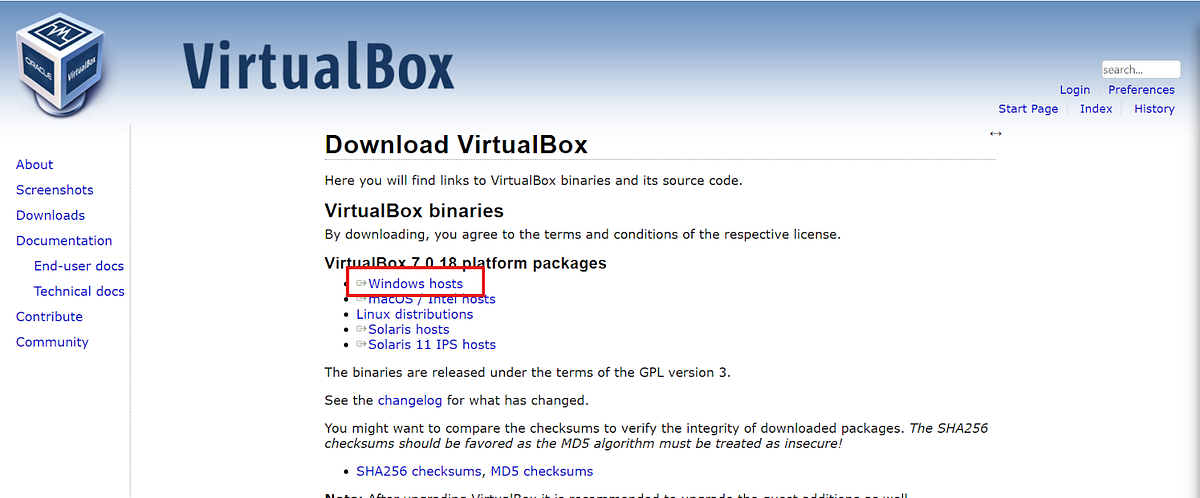
Let us start by downloading the Windows 10 iso image available [here](https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise)

Windows ISO Download

Next we download the Remnux Virtual Appliance from [here](https://docs.remnux.org/install-distro/get-virtual-appliance).

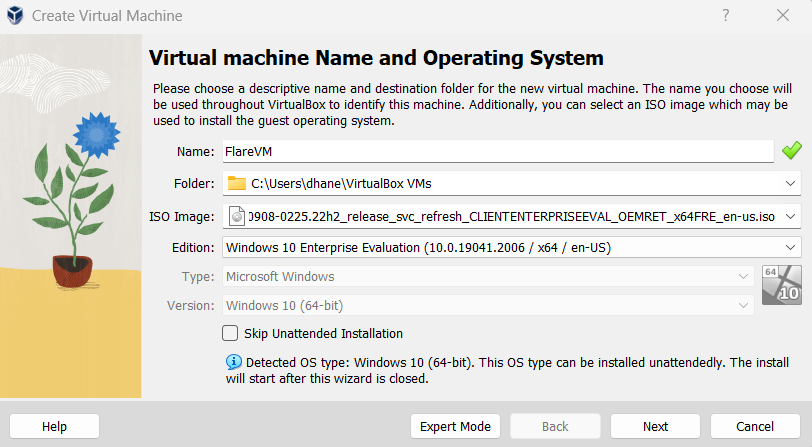


Download the Virtual box from [here](https://www.virtualbox.org/wiki/Downloads). As I am using the windows host I downloaded the windows hosts package.

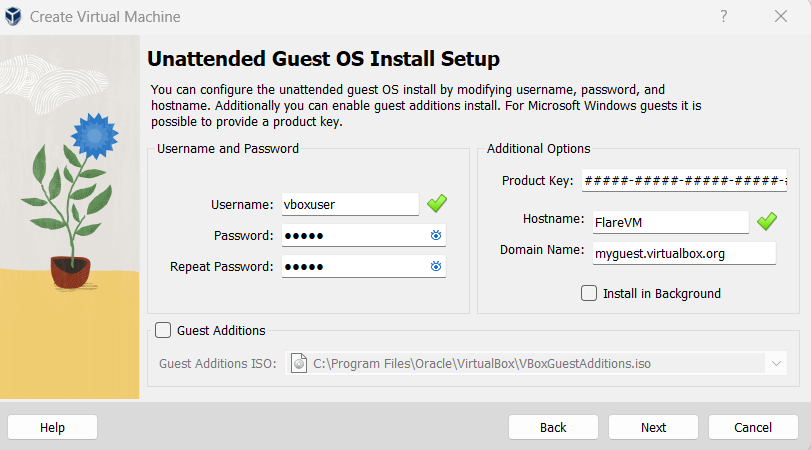


Now start setting up the VM for flareVM. First create the Windows virtual machine.

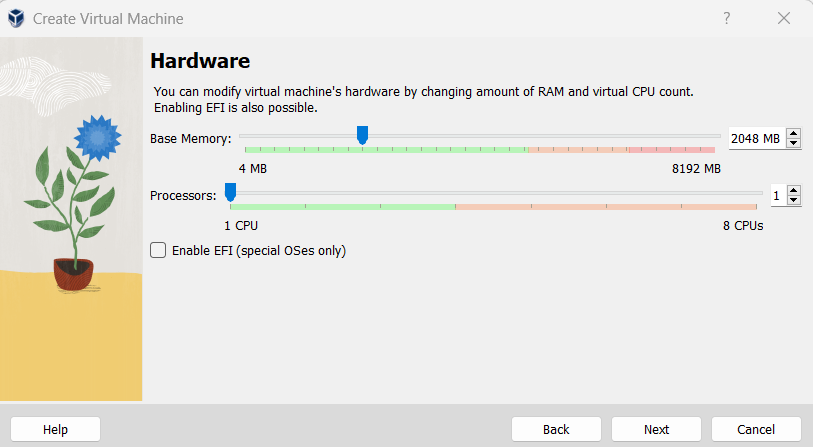
Open Virtual Box > Machines > New. Give the virtual machine a name and select the downloaded windows-10 iso image and click next.



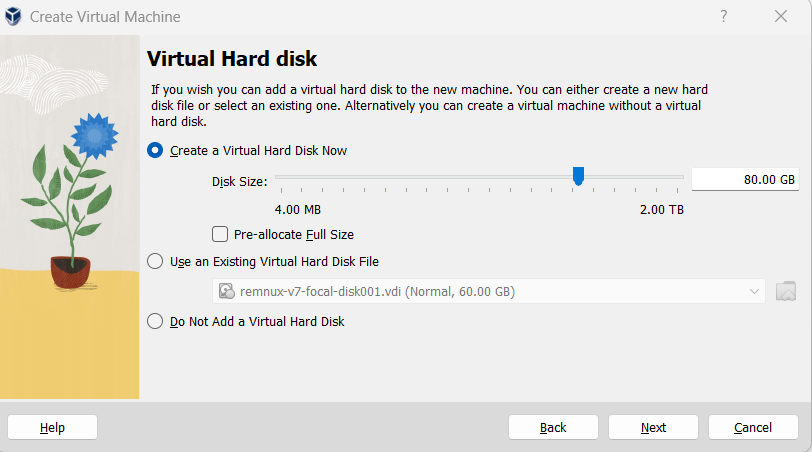
Then select the Username and password and click next



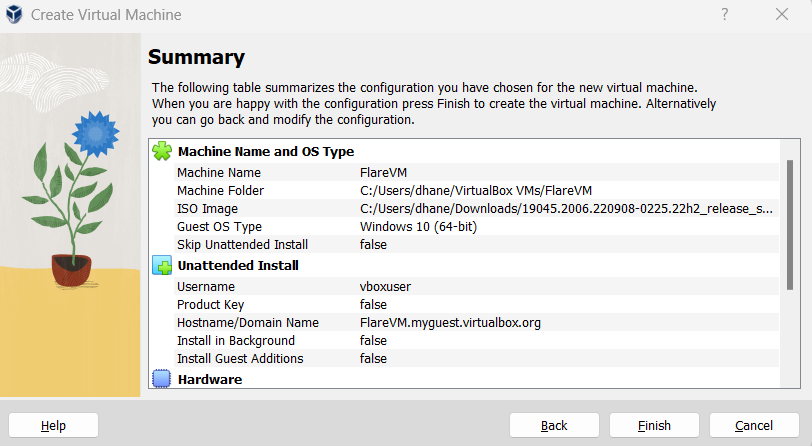
Now select the amount of RAM for the virtual machine and click next.



Now select the amount of storage for the virtual machine. As FlareVM is a collection of several tools it requires at least 60GB of Disk space. Here I chose 80GB. Now click next.



Now check the configuration and click finish. Virtual machine creation will start. This might take several minutes.

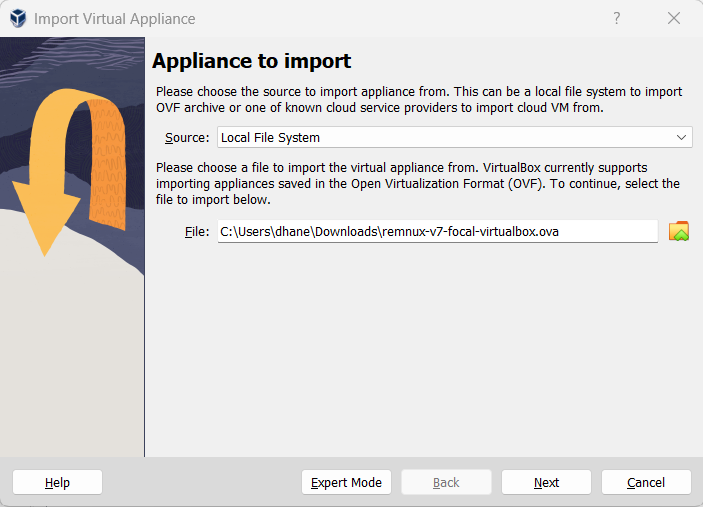


**Remnux Installation:**

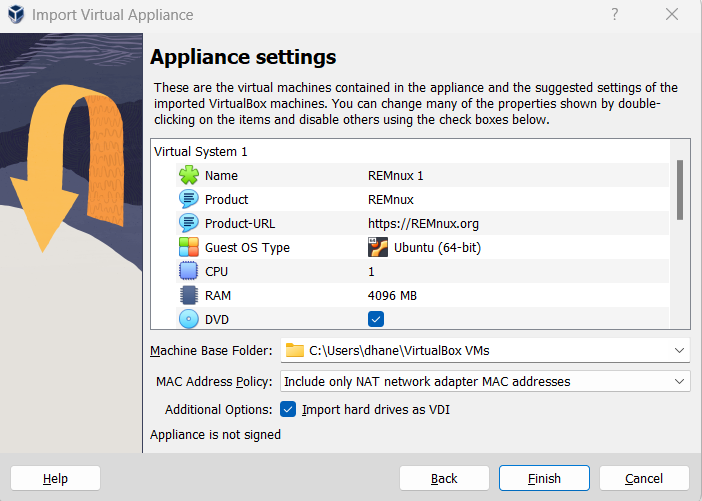
As we downloaded the prebuilt REMnux VM we can directly start by importing the ova to virtual box.

Open VirtulaBox > File > Import Appliance or Ctrl+I.

Locate the ova file and specify the path and click next



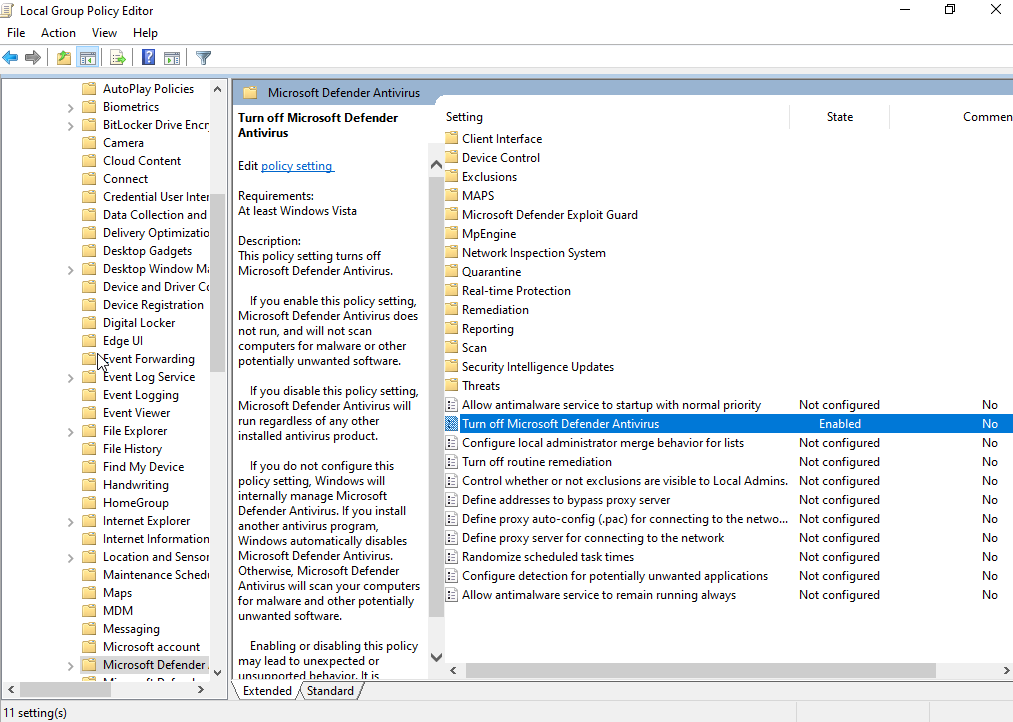
We can leave everything default and click next. The VM import will start and the REMnux VM will be ready.



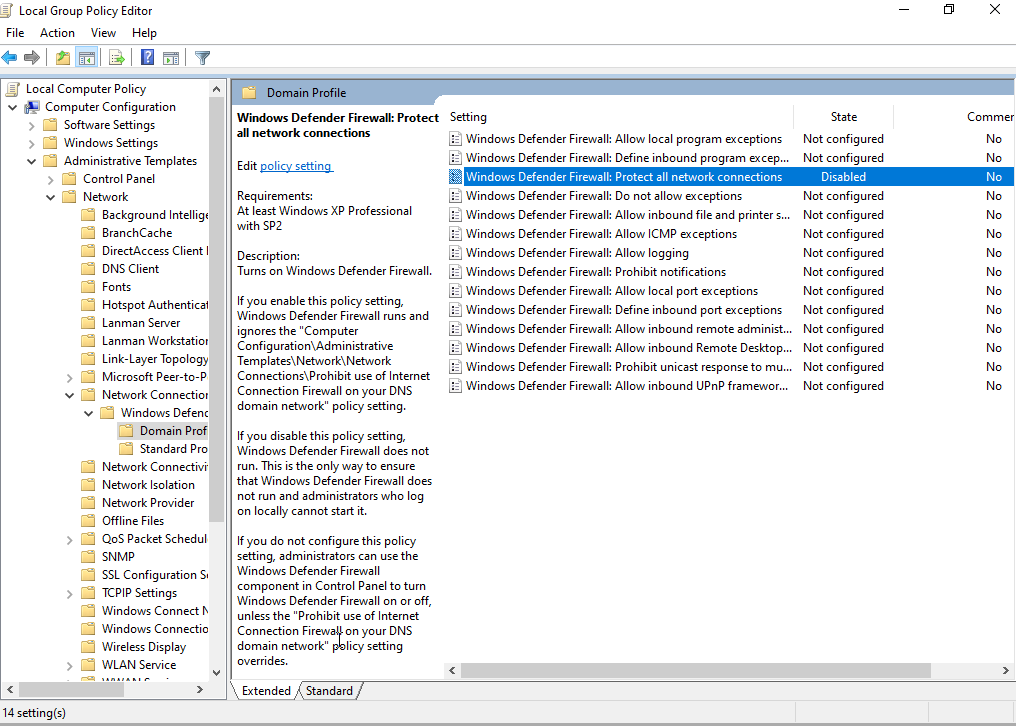
**FlareVM setup on the Windows-10 VM:**

I am going to install the FlareVM in the newly created Windows 10 Virtual Machine. To install FlareVM we need to disable some of the Windows default security configurations.

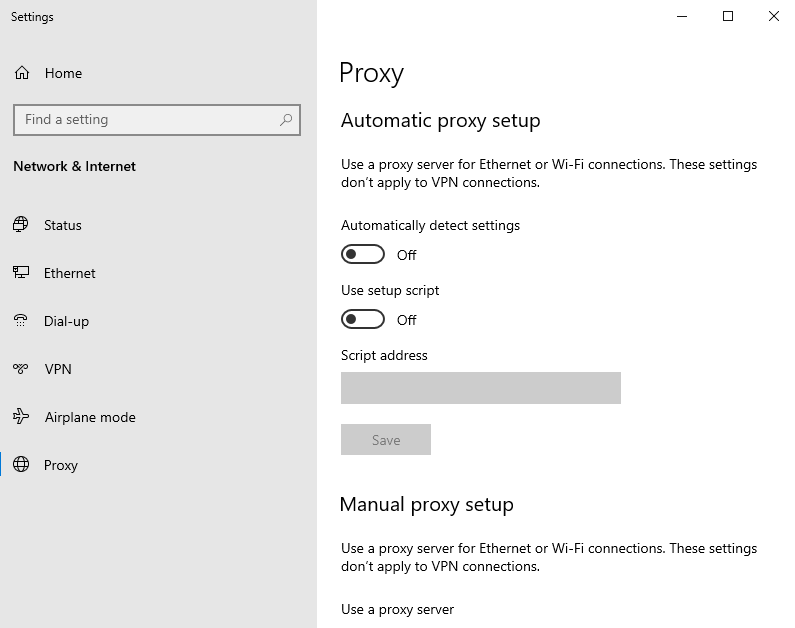
From start navigate to the group policy editor. In the group policy editor navigate to Administrative Templates > Windows Components > Microsoft Defender Antivirus. Under this double click the “Turn off Microsoft Defender Antivirus” option and click enable and click apply and OK.



Now navigate to Administrative Templates > Network > Network Connections > Windows Defender Firewall > Domain Profile. Under this select the “Protect all connections” options and disable it. Do the same under the Standard Profile. Now exit out of the GPO editor.

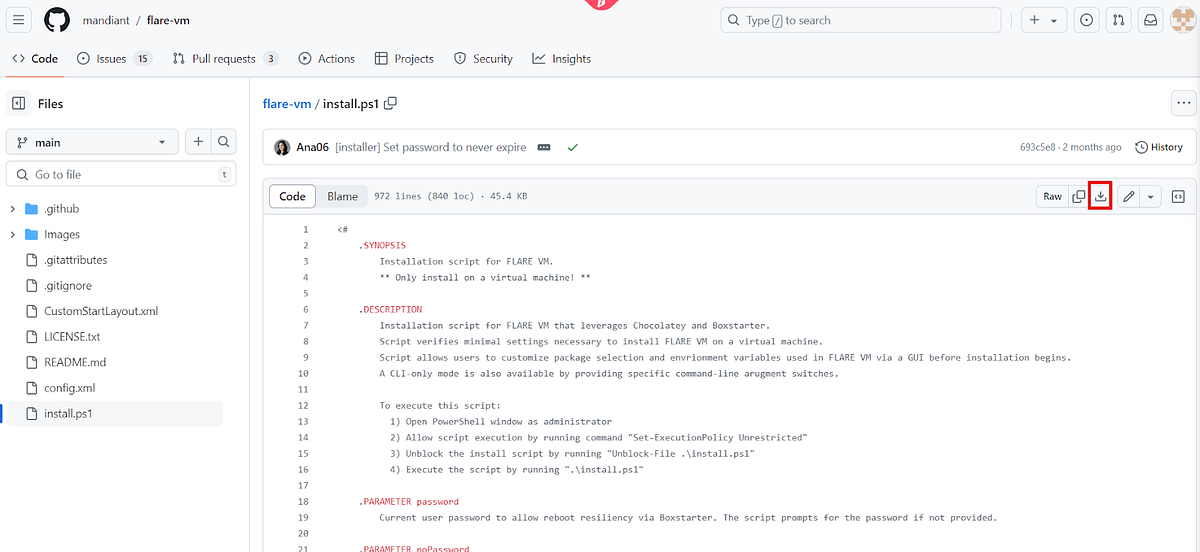


Now in the Start menu search for “Proxy settings” and open it. Here turn off the “Automatically detect settings” option. Now exit from the settings.



Now the Virtual machine is configured to install FlareVM.

We can download the required scripts from the github repository [here](https://github.com/mandiant/flare-vm/blob/main/install.ps1). Navigate to the github repository and click download.



The install.ps1 file is downloaded. This script contains all the commands required to install various tools and packages for the FlareVM.

Now open the Powershell in Administrator mode and navigate to the path where the file is located.

Here we need to perform two commands in order to allow the script to run on the system.

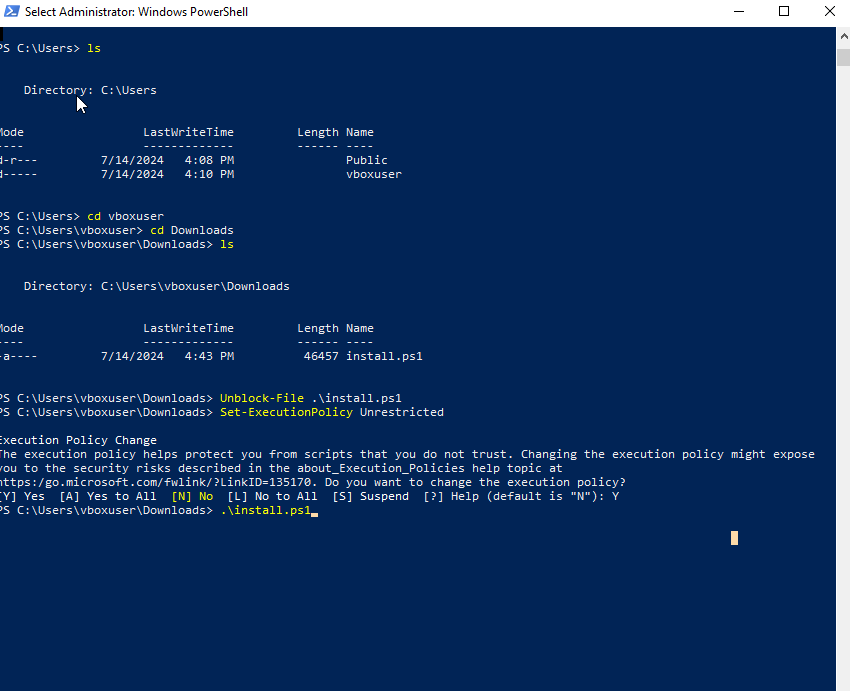
* Unblock-File .\install.ps1(This command allows to run the files downloaded from internet)
* Set-ExecutionPolicy Unrestricted(This command loads all the configuration files and runs all scripts)

Once we execute these commands our install.ps1 script will be ready to execute.

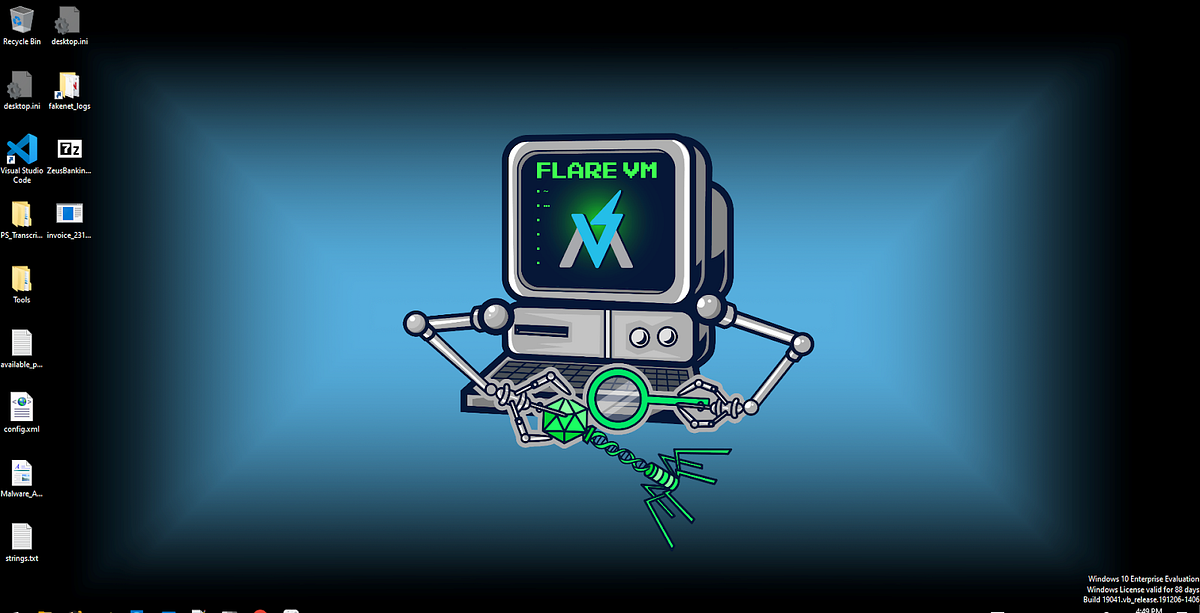
Before proceeding to execute the script it is ideal to take a snapshot of the Virtual machine so that we can revert back to the same stage in case the FlareVM execution fails.

Now we can run the install.ps1 script using the following command

* .\install.ps1



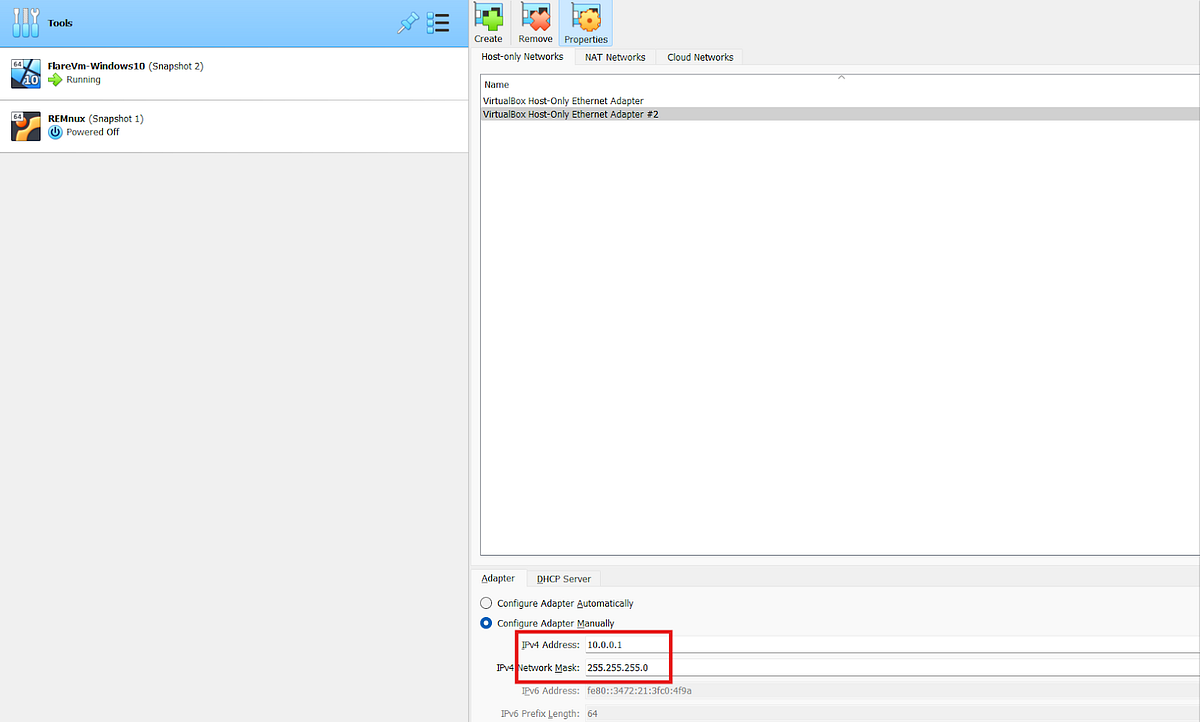
Now the installation has started. This might take several minutes and the system will restart multiple times during the installation process. Once the installation is complete a text file opens which contains all the installed programs. Now our FlareVM is ready.



**Network Configuration:**

Before detonating the malware samples for analysis we should make sure that the malware doesn’t infect our host machine. For this we need to isolate both our FlaVM and REMnux virtual machines.

Go to Virtual Box > Tools > Network and click create host-only network adapter. Now go to the newly created adapter and choose the configure adapter manually option and use the following configuration.



And the under DHCP server choose the following configuration.



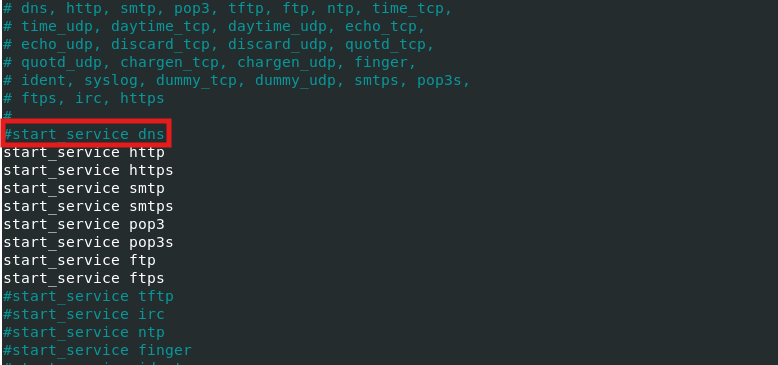
This allows for the two machines to communicate between each other but does not allow any other communication. This creates a sandbox environment to safely test the malware.

**Configuring REMnux:**

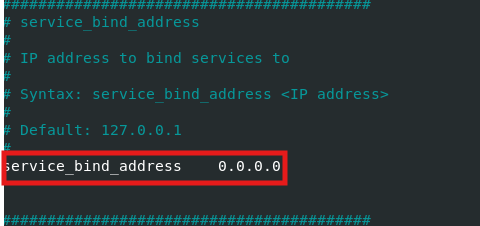
In the REMnux VM we need to configure the INetSim(a software suite for simulating common internet services in a lab environment).

Open the REMnux virtual machine and navigate to /etc/inetsim directory. Here we need to edit the inetsim.conf file.

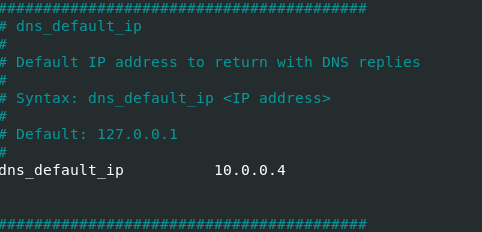
Navigate to the services and uncomment the start\_dns\_service.



Now scroll down and un-comment the service\_bind\_address and change it to 0.0.0.0.



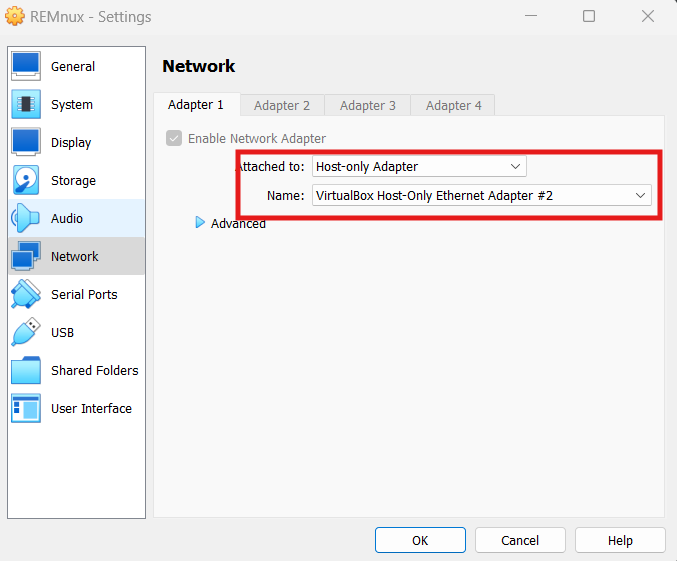
Now move to the bottom of the file and under dns\_default\_ip section uncomment the dns\_default\_ip line and change it to 10.0.0.4



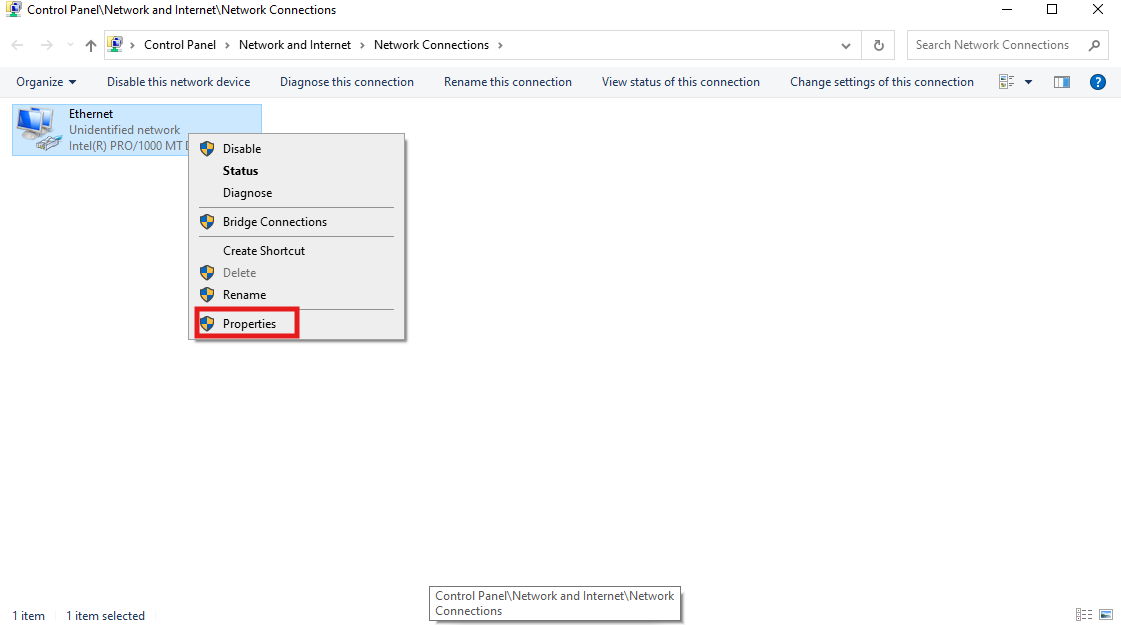
Click Ctrl+x on nano and save and exit.

Now for both the VM’s change the following option.

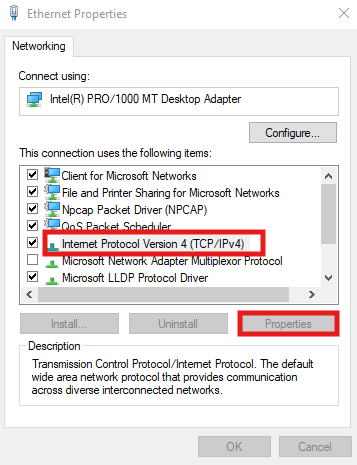
Machine > Settings > Network under this Adapter-1 select Host-Only Adapter and select the Adapter we created.



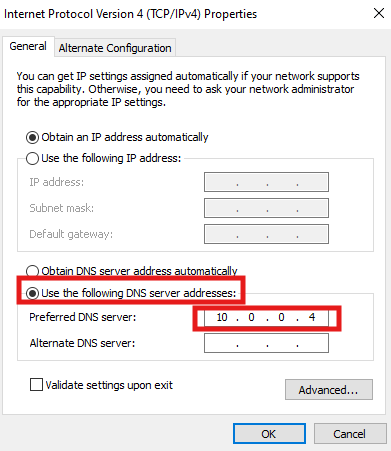
Now in FlareVM virtual machine go to Ethernet Settings > Change Adapter Options > Ethernet > Properties



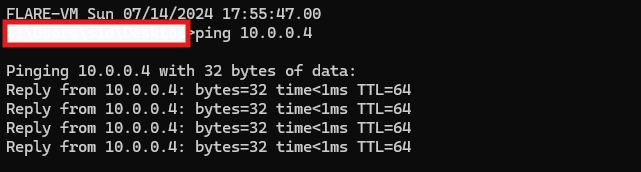
Under properties select Internet Protocol Version4(TCP/IPV4) option and select properties.



Here select use the following DNS server address and specify 10.0.0.4 as the preferred DNS server.

Edit DNS server address

Now the internet will be cut off to the FlareVM and our two VM’s can communicate with each other. We can check this by opening a browser on FlareVM and try ping 10.0.0.4.

Ping to check if the VM’s can communicate

Now our Malware analysis lab is set up and ready to detonate and test the malware samples.