STEP BY STEP MALWARE ANALYSIS LABSET-UP

AMMAR HAKIM HARIS

Contents

HYPERVISOR INSTALLATION

1. Go to https://www.virtualbox.org/wiki/Downloads and choose the installer according to your host architecture.

2. Once downloaded. Proceed with the installation with all default settings.

## 3. VirtualBox should launch automatically.

WINDOWS 10 OS INSTALLATION

1. To install the first OS, go to https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise to get the ISO.


2. It will request certain information from you. Register details for your free ISO.

3. Once downloaded, go to VirtualBox – click New button to configure the VM details. Then click Next

4. Configure your Memory and Processor amount.
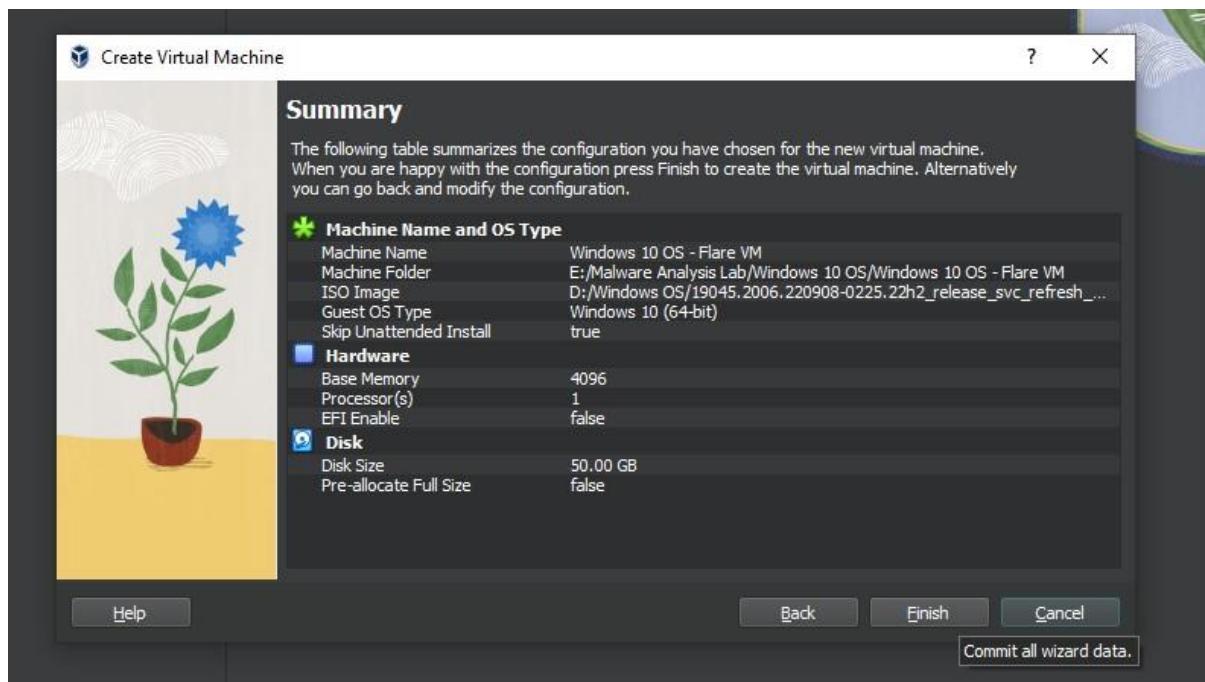
5. For Virtual Hard Disk – you can set it to default. Then click Next.

6. Check the details to confirm the configuration before click Finish.
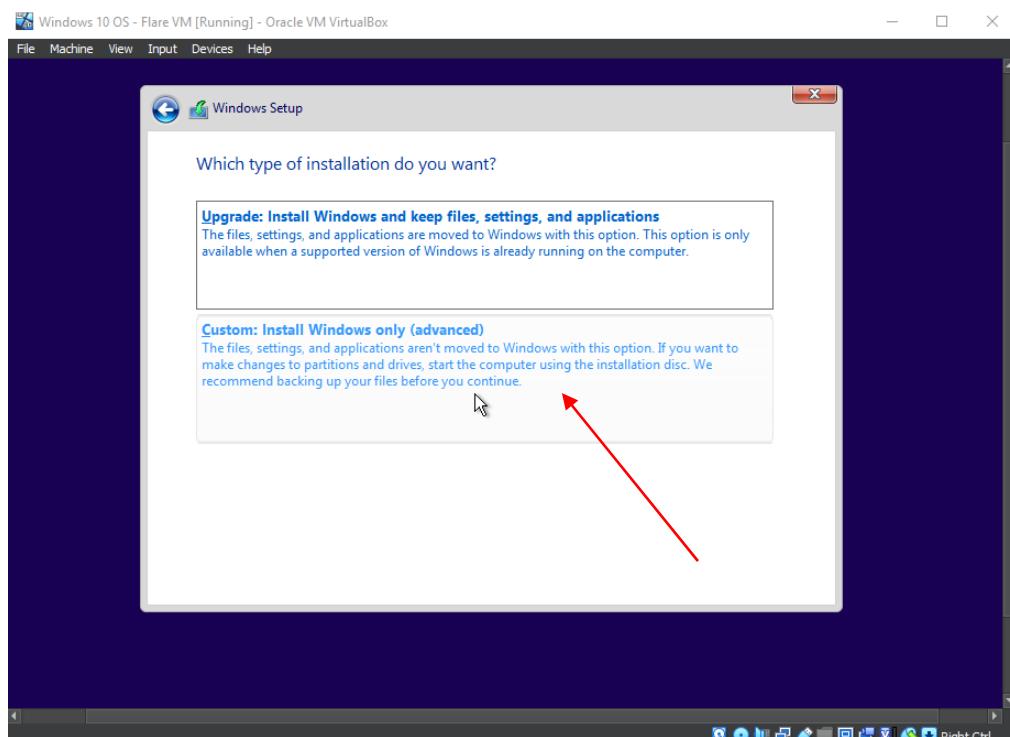
7. After click Finish, initialize it by clicking Start and the machine will start installation process.

8. Choose Custom installation.

9. Click New then Apply before you click Next.
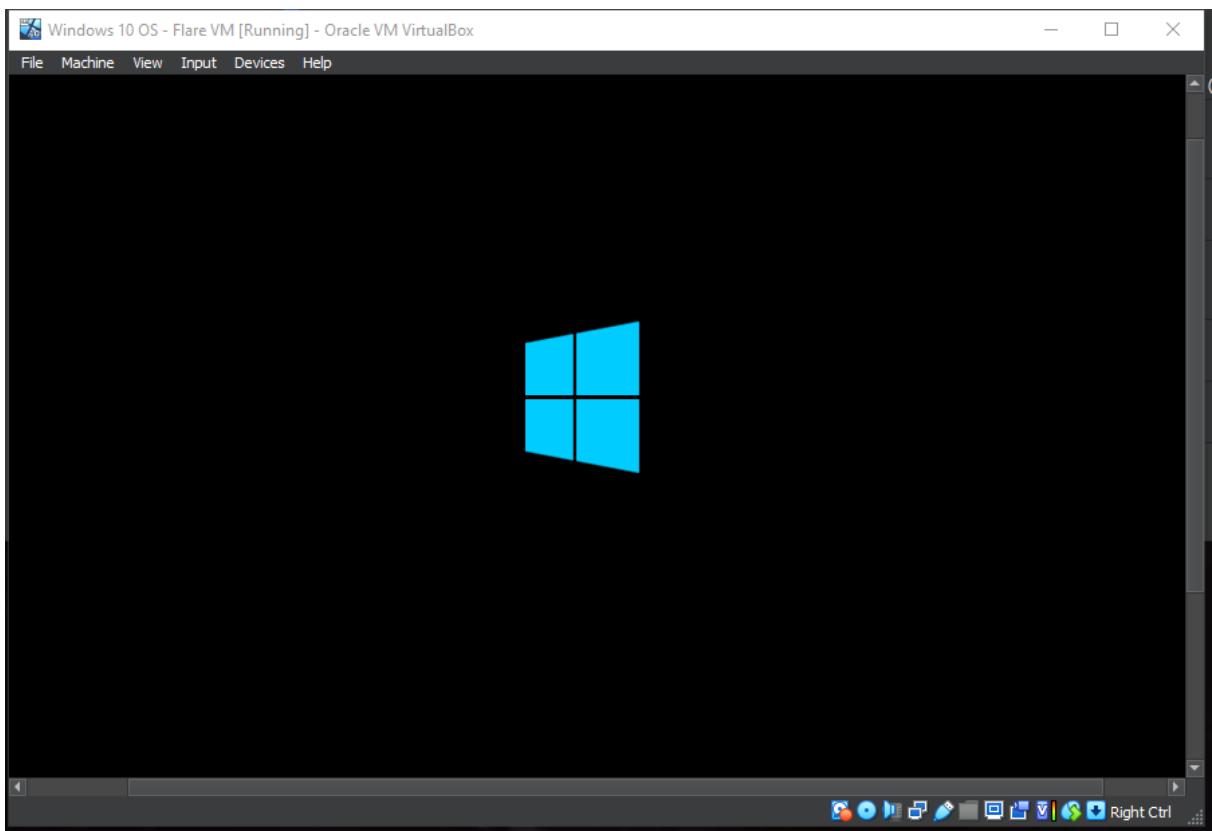
10. Let the installation process complete and this will takes sometimes depending on your resources.

11. The machine will go into booting screen before next step.
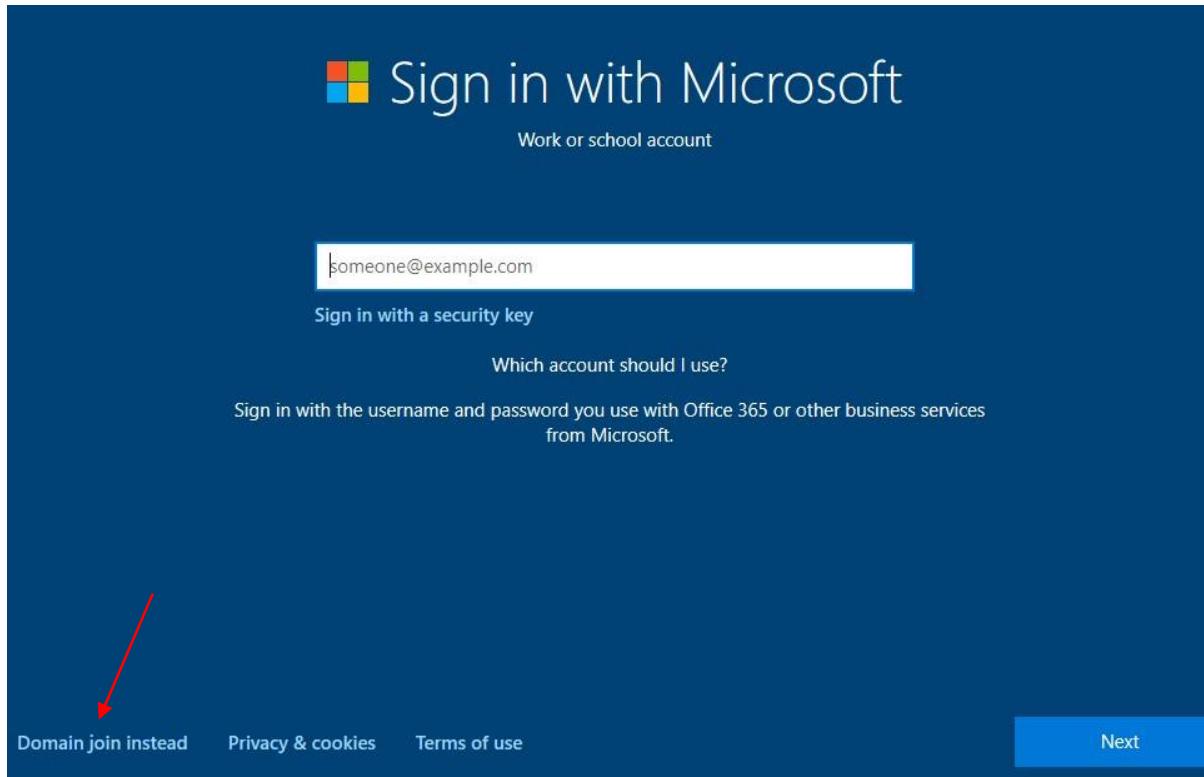
Select Region, Keyboard based on your preferences.

12. You don't have to sign in with Microsoft, select Choose Domain join instead before click Next
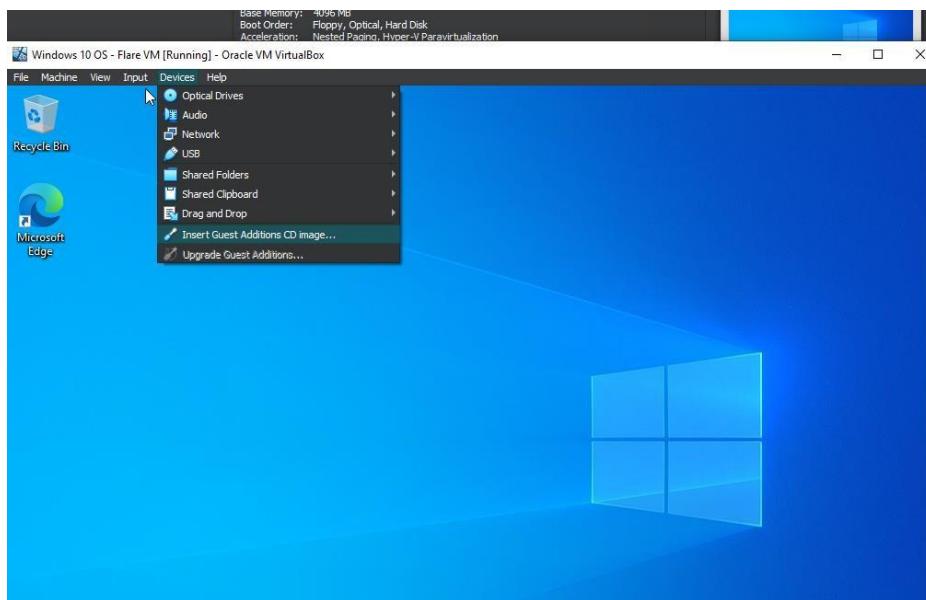
13. Complete the necessary set-up process until you see the Windows desktop.

14. Then, go to Devices – Insert Guest Edition Cd image to set up better viewing display of your VM.
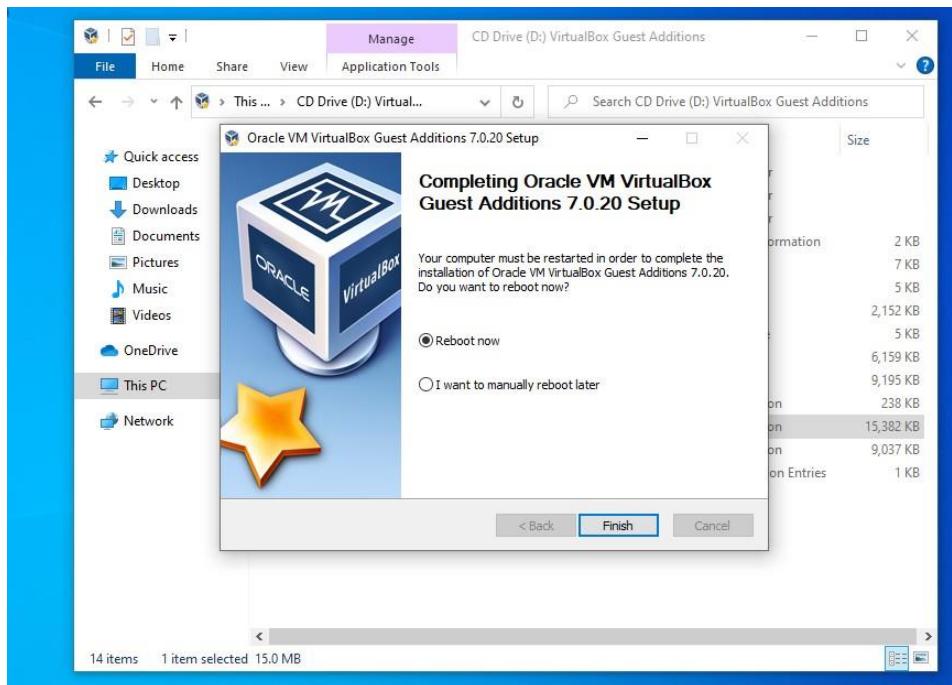
Go to This PC, and double click CD Drive then choose suitable configuration for the installation.

It will reboot once you click Finish.
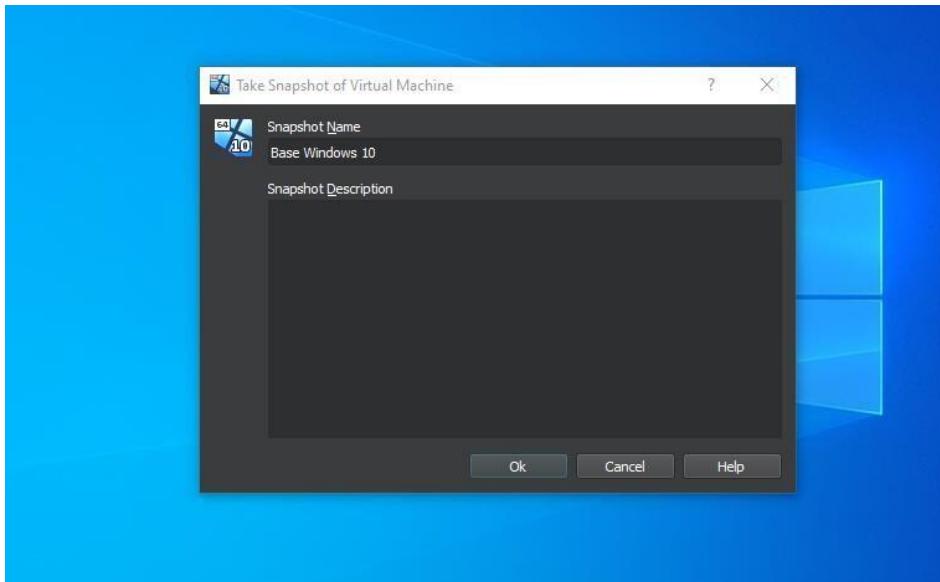
15. Don't forget to take snapshot at this phase before you proceed with next step. Just go to the TaskBar and select Machine.

Name the snapshot accordingly. This will allow you to return to this base phase if there is error prompted during next configuration.


16. Then suspend your virtual machine to proceed with REMnux installation

REMnux INSTALLATION

17. Go to https://docs.remnux.org/install-distro/get-virtual-appliance , then select VirtualBox OVA. You will be able to download it from the Box.

18. Download the file into the same directory created just now for easy access. Go to the installer once download completed and choose Open with VirtualBox Manager.
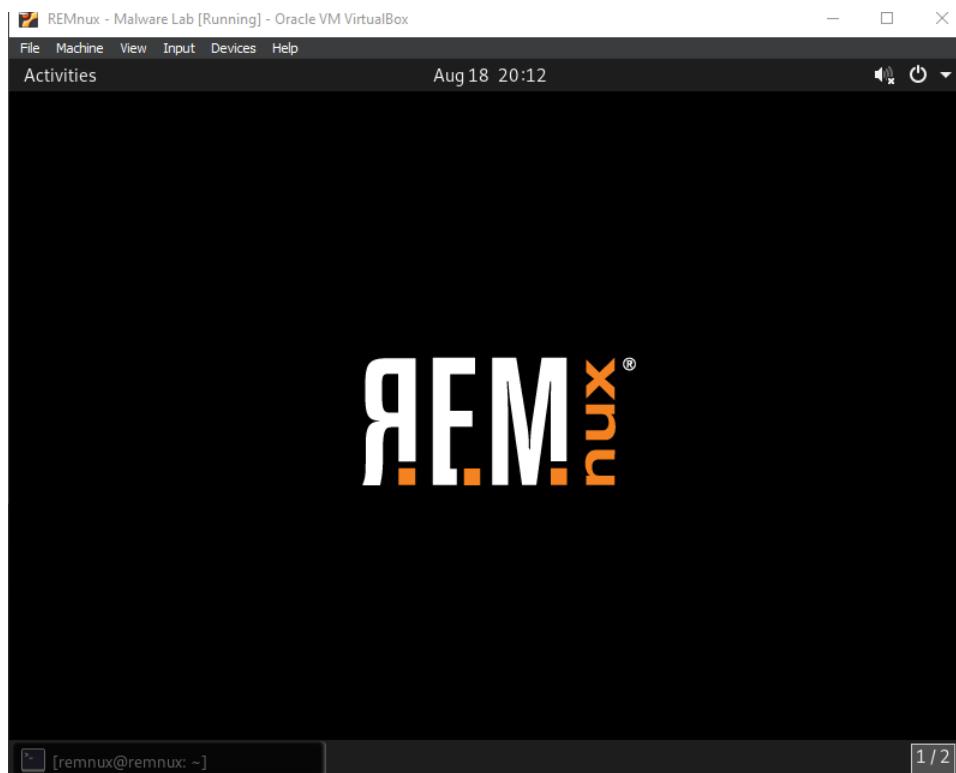
19. Set the VM accordingly before you click Finish.

Allow it to complete the set-up, then Power On the REMnux VM.
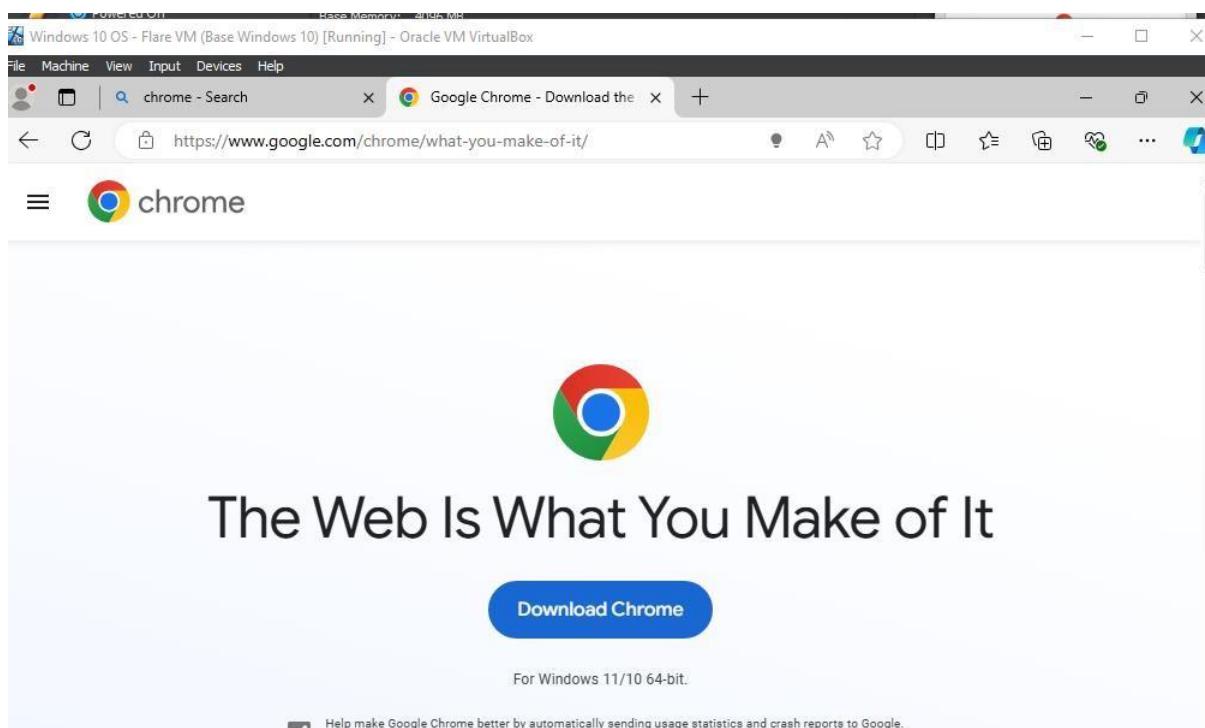
20. You should see REMnux VM running after the booting process completed.

Power Off REMnux machine.
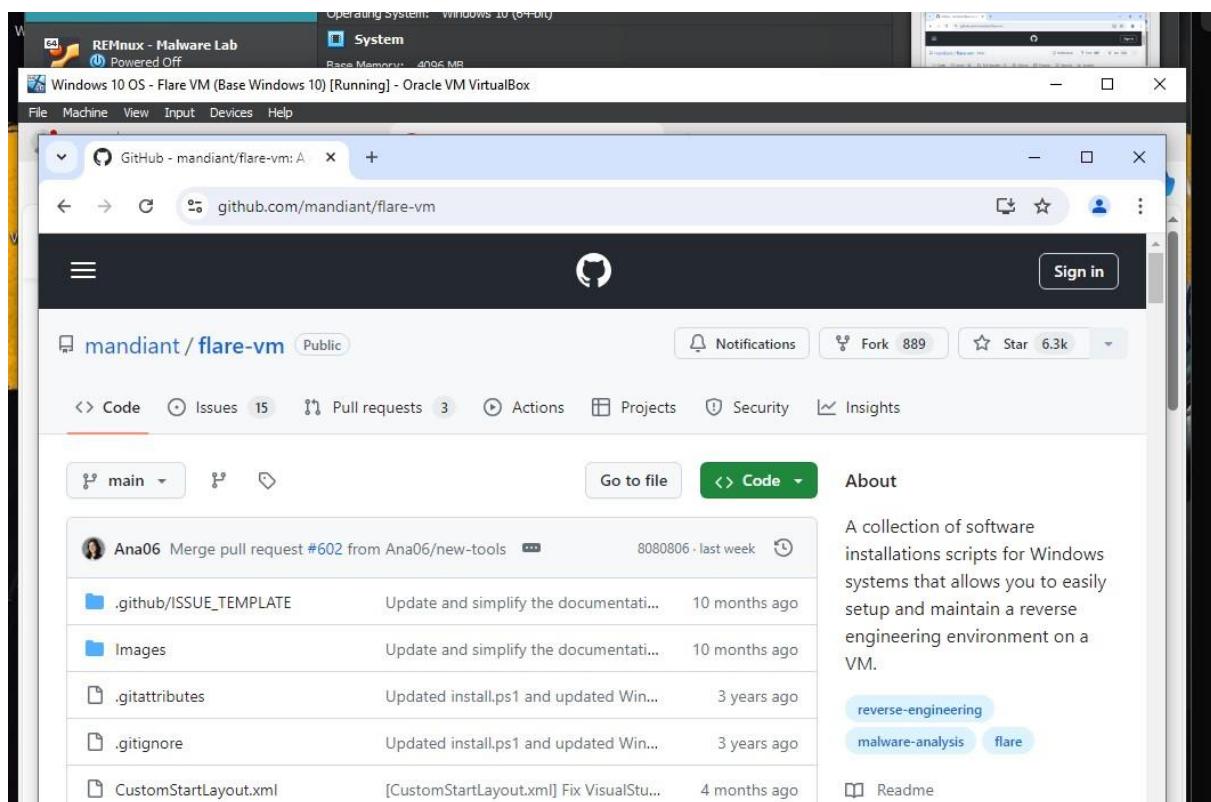
FLARE VM INSTALLATION

21. First install chrome browser into the Windows 10 OS VM.

22. Then go to https://github.com/mandiant/flare-vm

Copy link address of installer.ps1
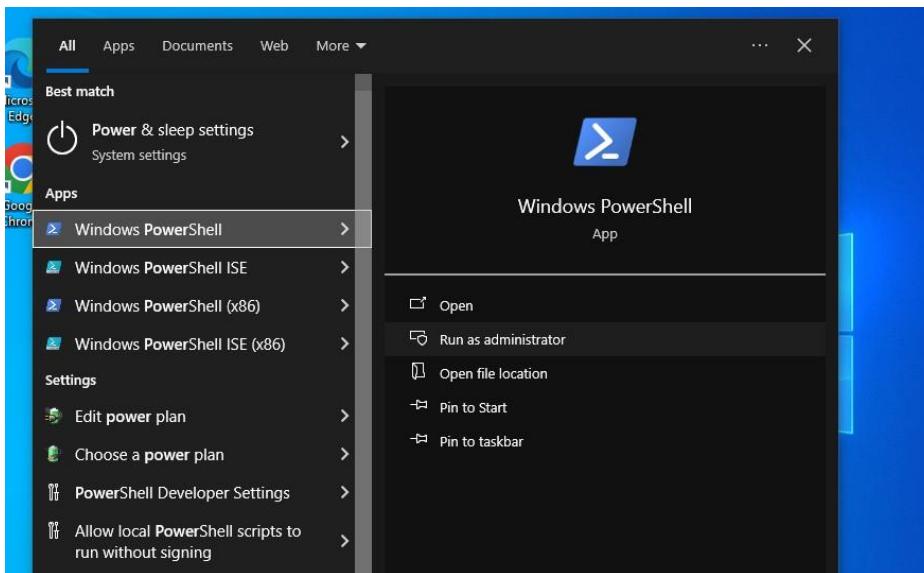
23. Open Windows PowerShell by run it as Administrator.

24. Then run this command Set-ExecutionPolicy Unrestricted
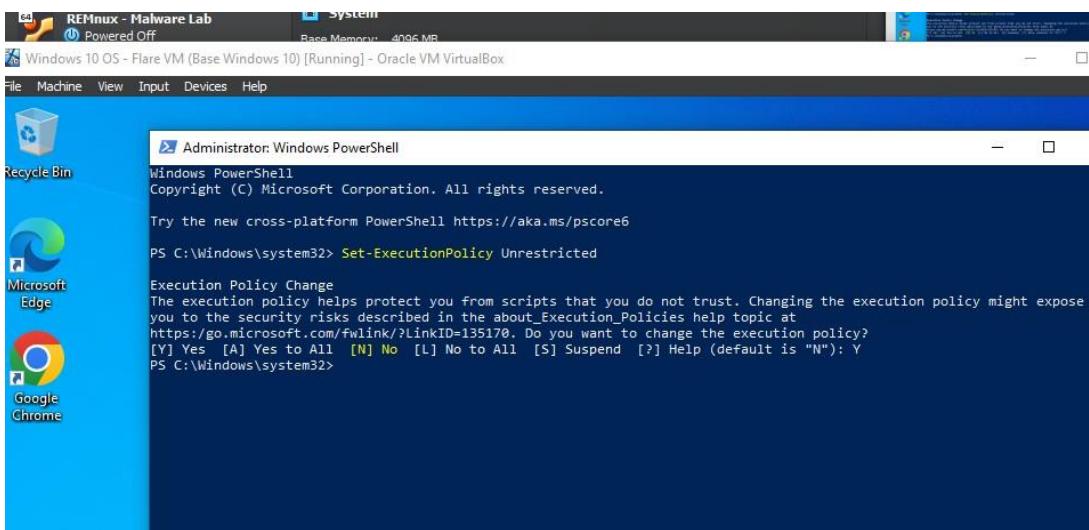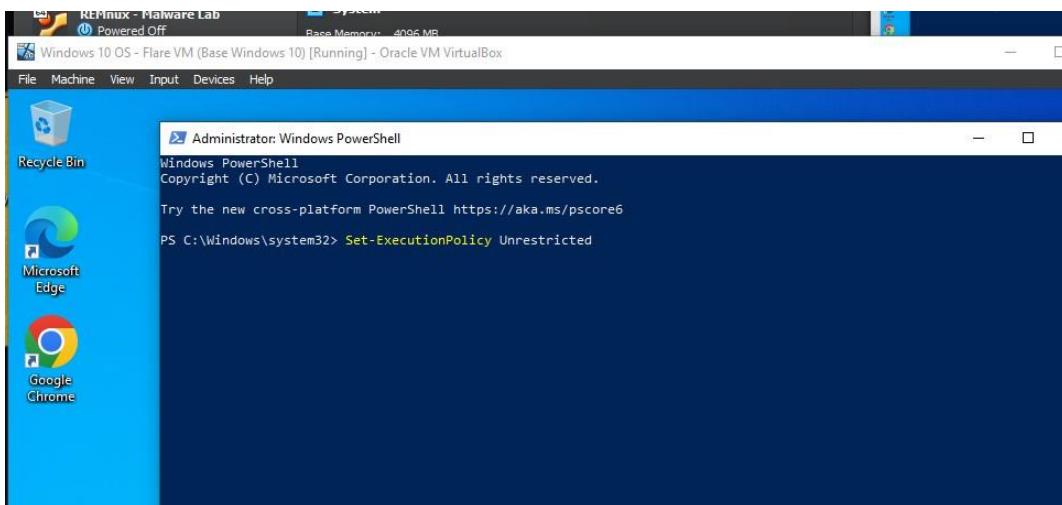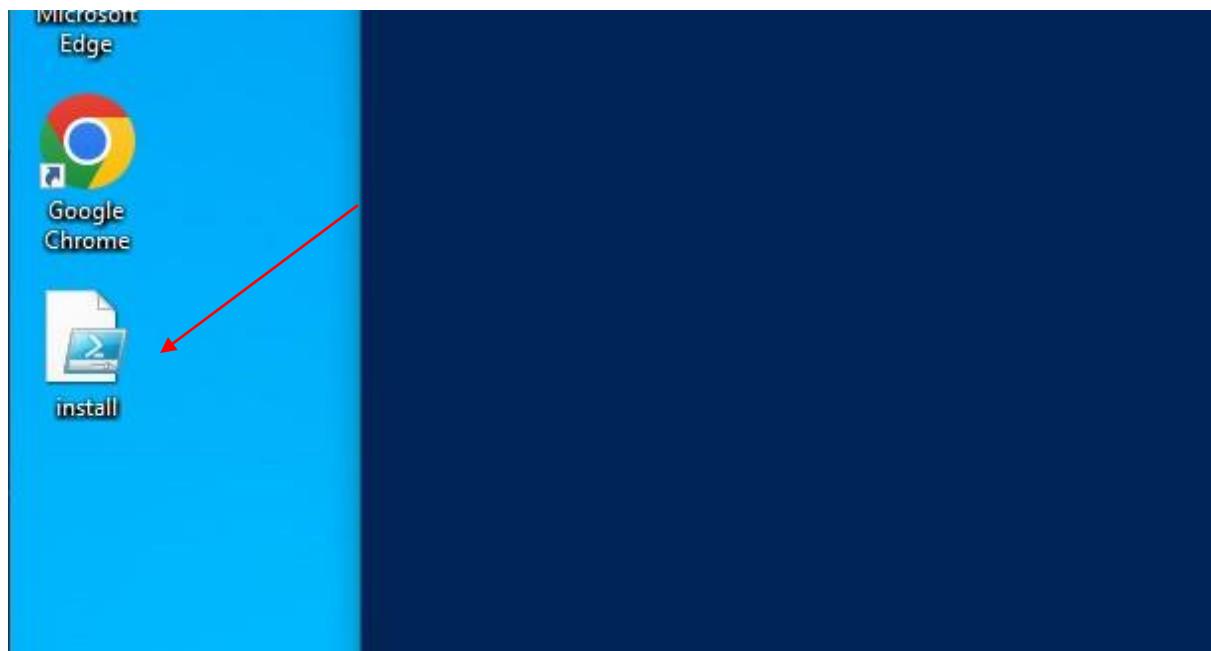
25. Run wget https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1
-UseBasicParsing -outfile <your desktop directory>
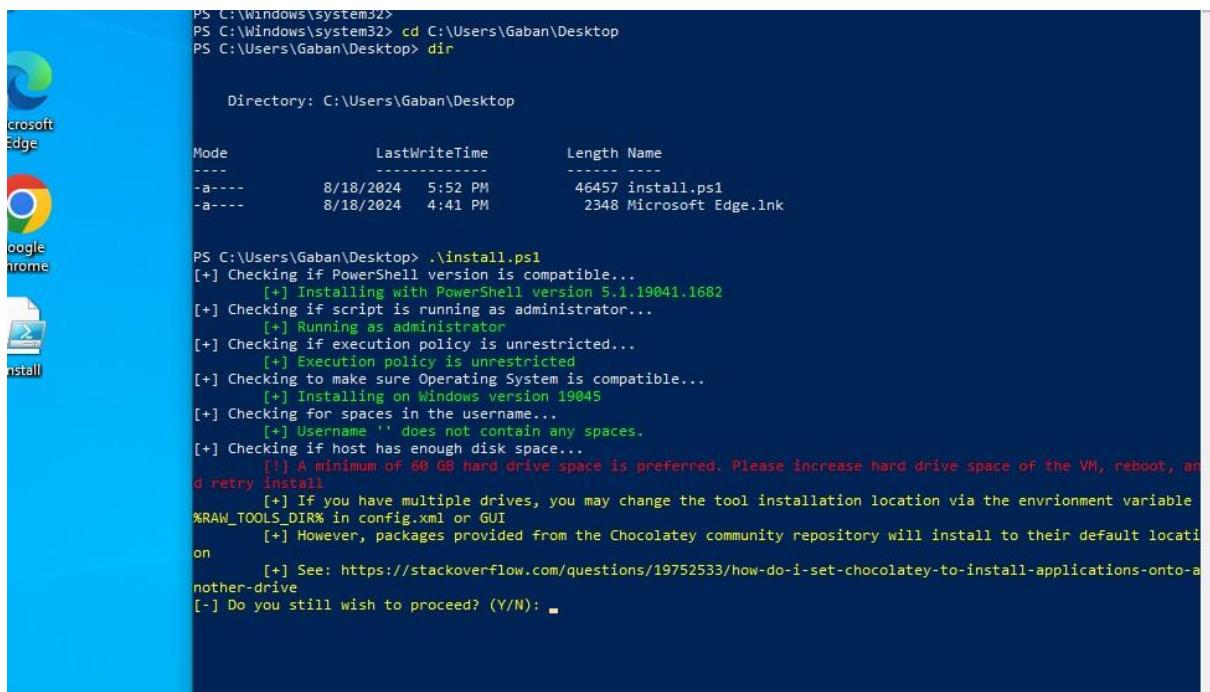
After that you should see install file in the desktop.

26. Change directory to desktop - cd <your desktop directory> . Then run command .\install.ps1

27. This installation will take a long time, so allow it to complete the installation. Proceed with default installation till VM reboot and complete installation. Don't forget to take snapshot for base Flare VM. You should see new desktop feature once everything installed.

SPECIAL NETWORK CONFIGURATION
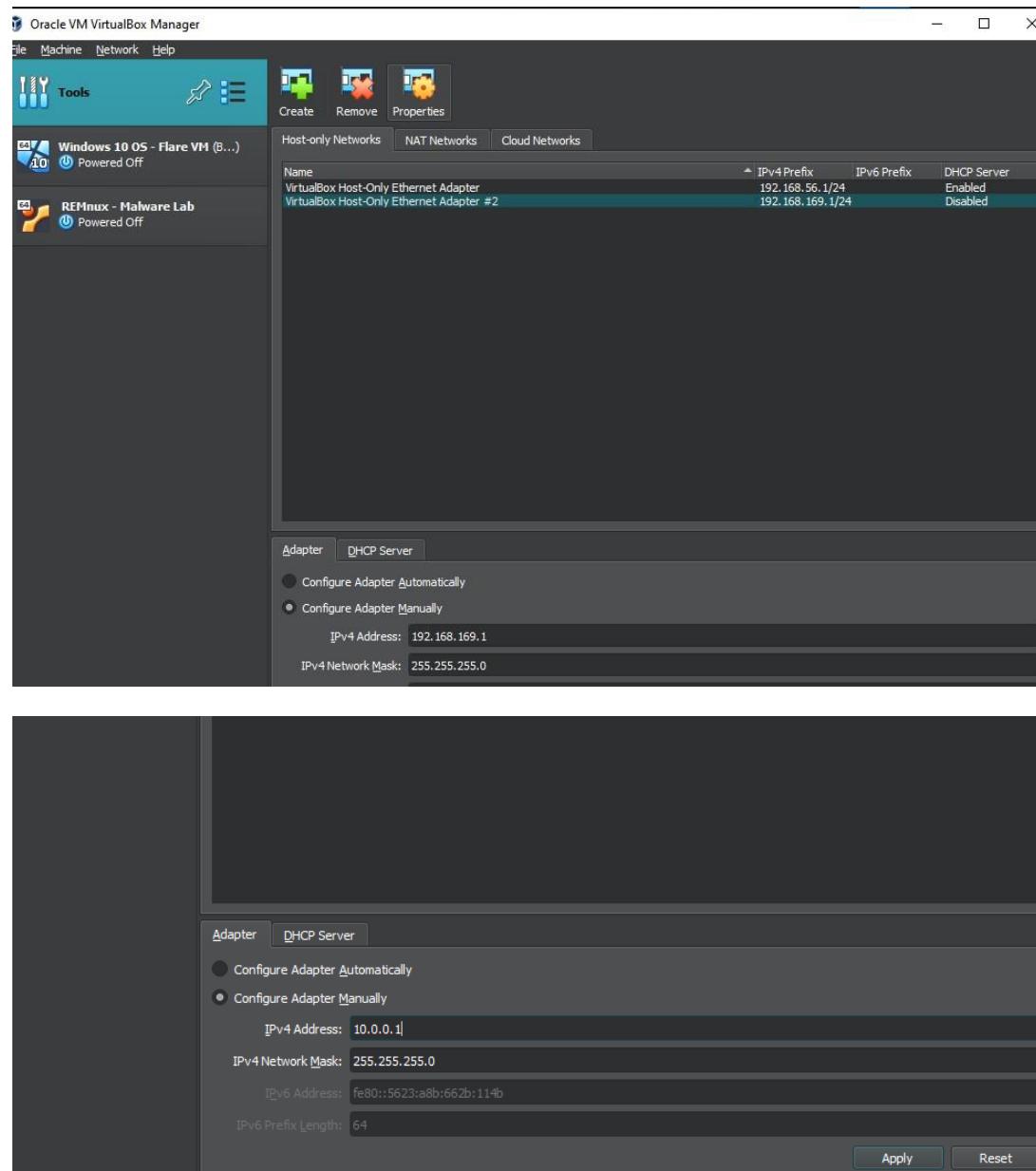
28. For special network configuration, go to VirtualBox – Tools – Network Manager.

29. Then click Create to duplicate another adapter for this setting. So, both VM will only communicate with each other to prevent your host get infected with malware once detonated.
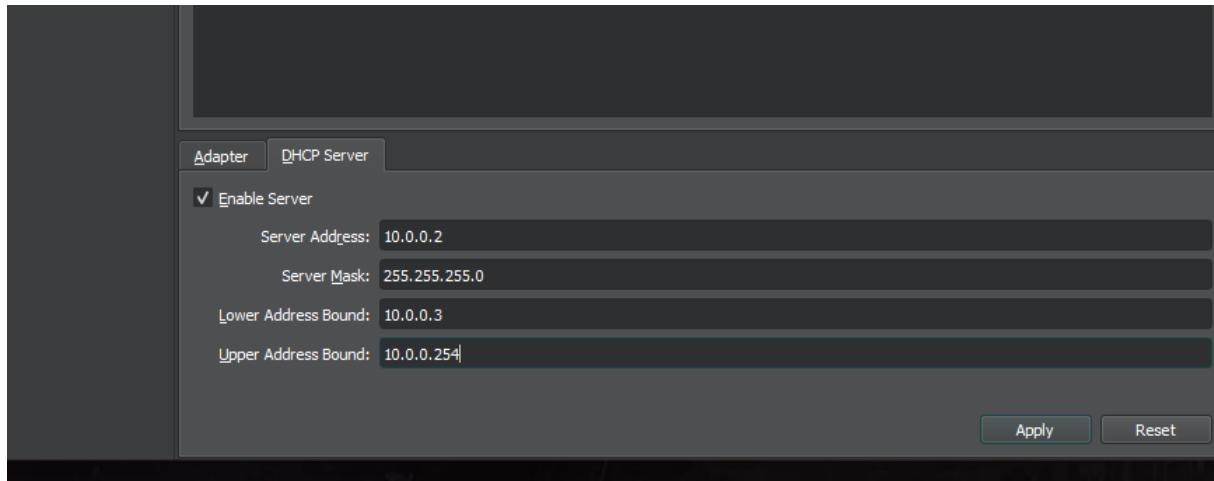
30. Enable the DHCP Server and configure the adapter manually to 10.0.0.1 for IPV4
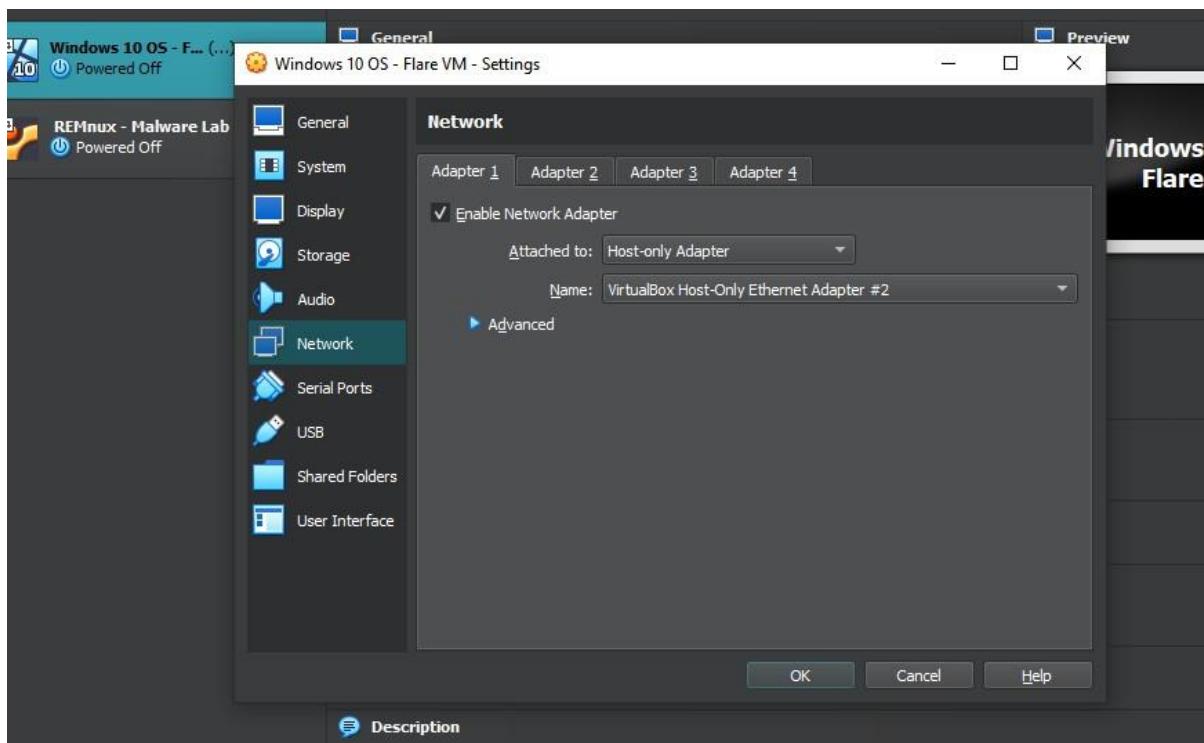
31. Then go to DHCP Server tab to change the Server Address to 10.0.0.2. Change Lower and Upper accordingly as well. Click apply

NETWORK CONFIGURATION FOR VM

Windows 10 – Flare VM
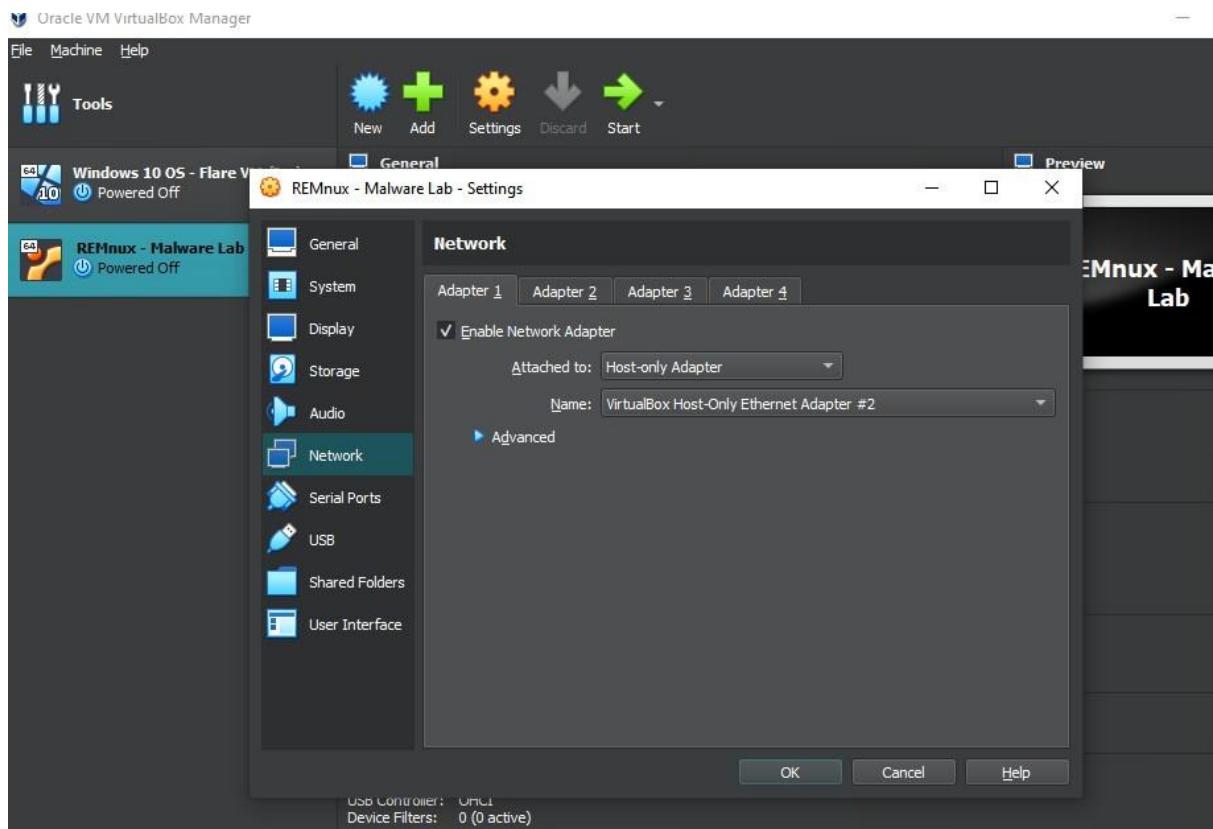
32. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check another Adapter as well. Then click OK
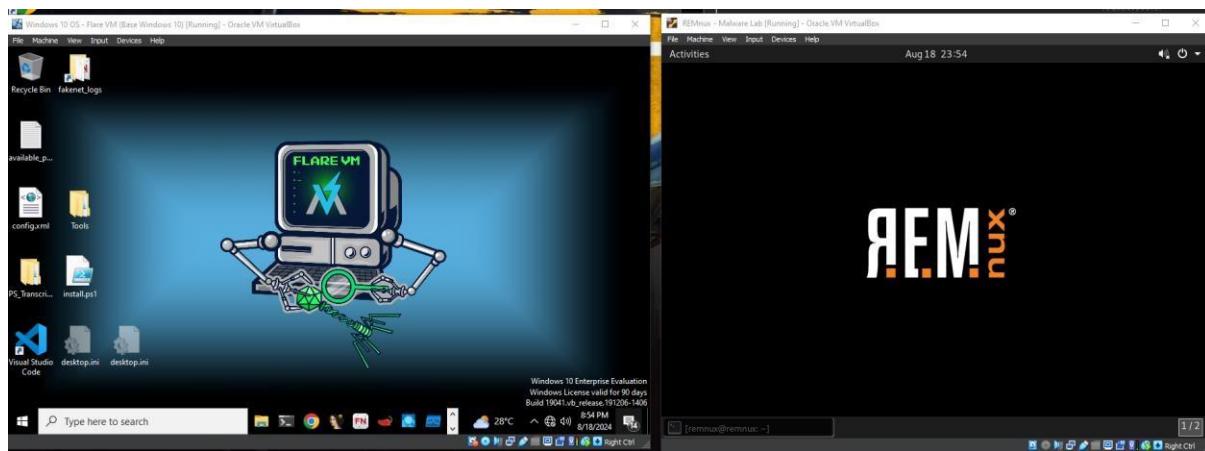
REMnux VM

33. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check other Adapter as well. Then click OK

34. Power ON both VM to check their connectivity
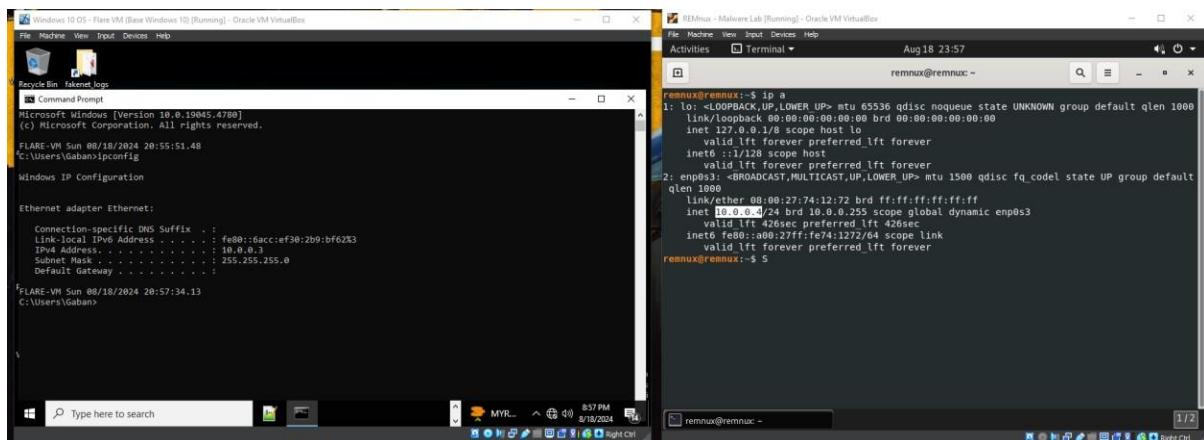
Launch Terminal for both VM

Check adapter internet setting in REMnux VM and Flare VM.
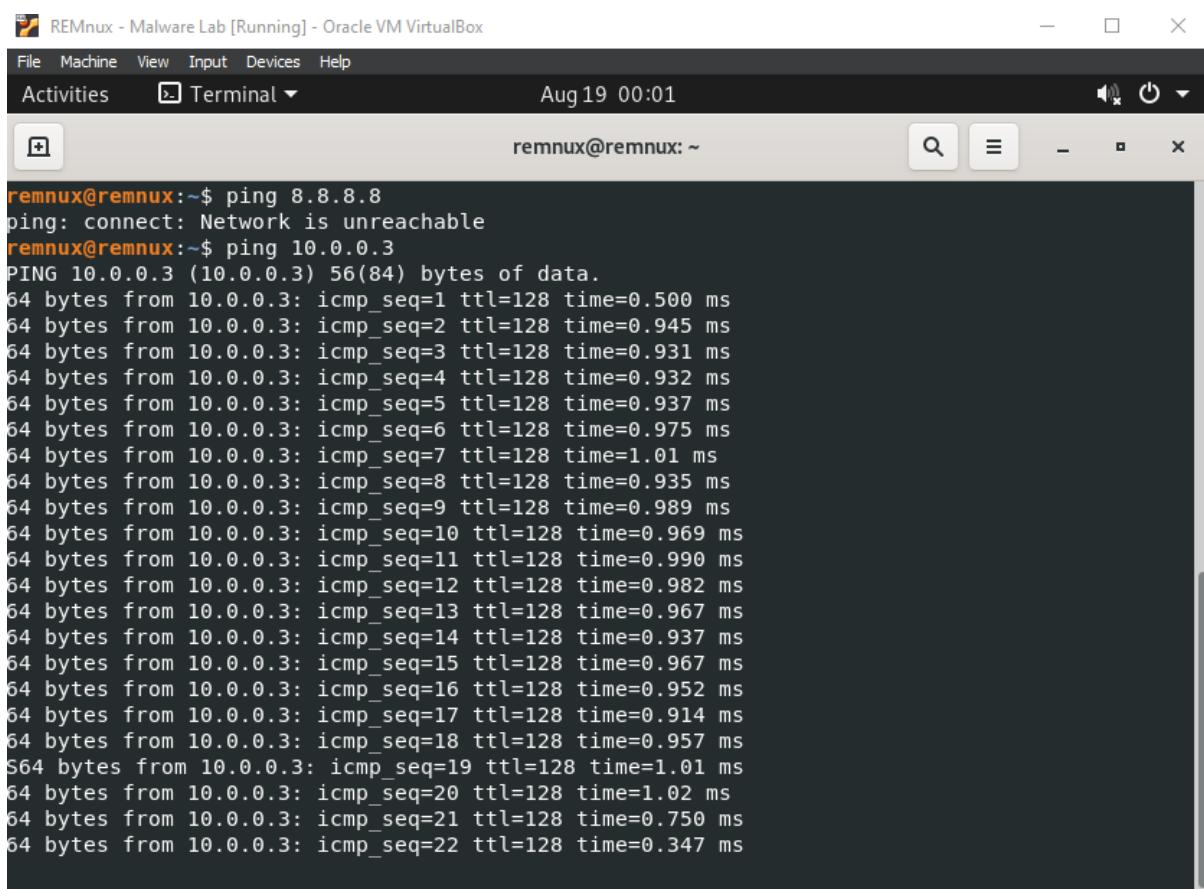
By running the command ip a for REMnux VM and ipconfig for Flare VM.
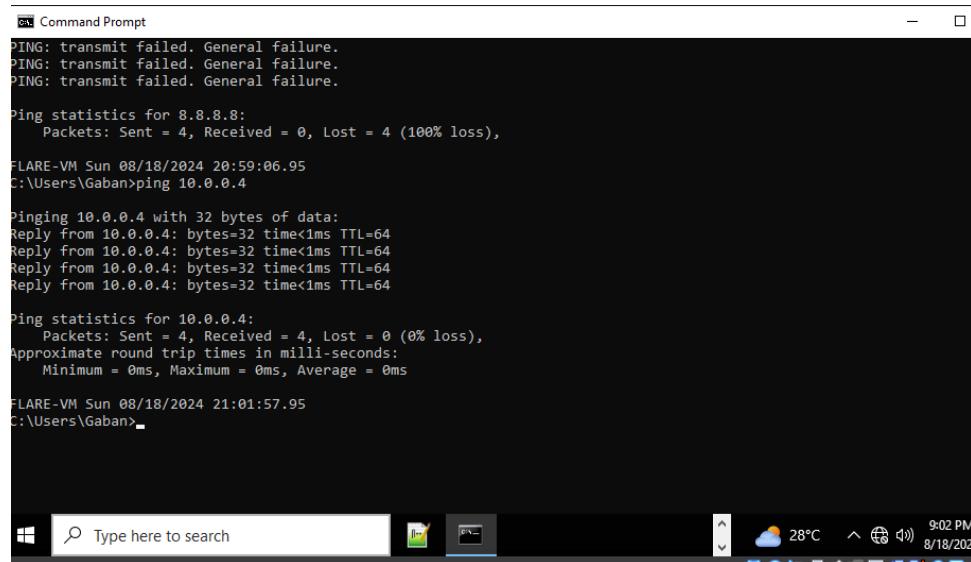
35. You also can try to run ping command for both VM to 8.8.8.8 to check the connection.

Then ping each other VM to see if they can communicate with each other

Windows – Flare VM

SET UP INETSIM

Internet Simulator
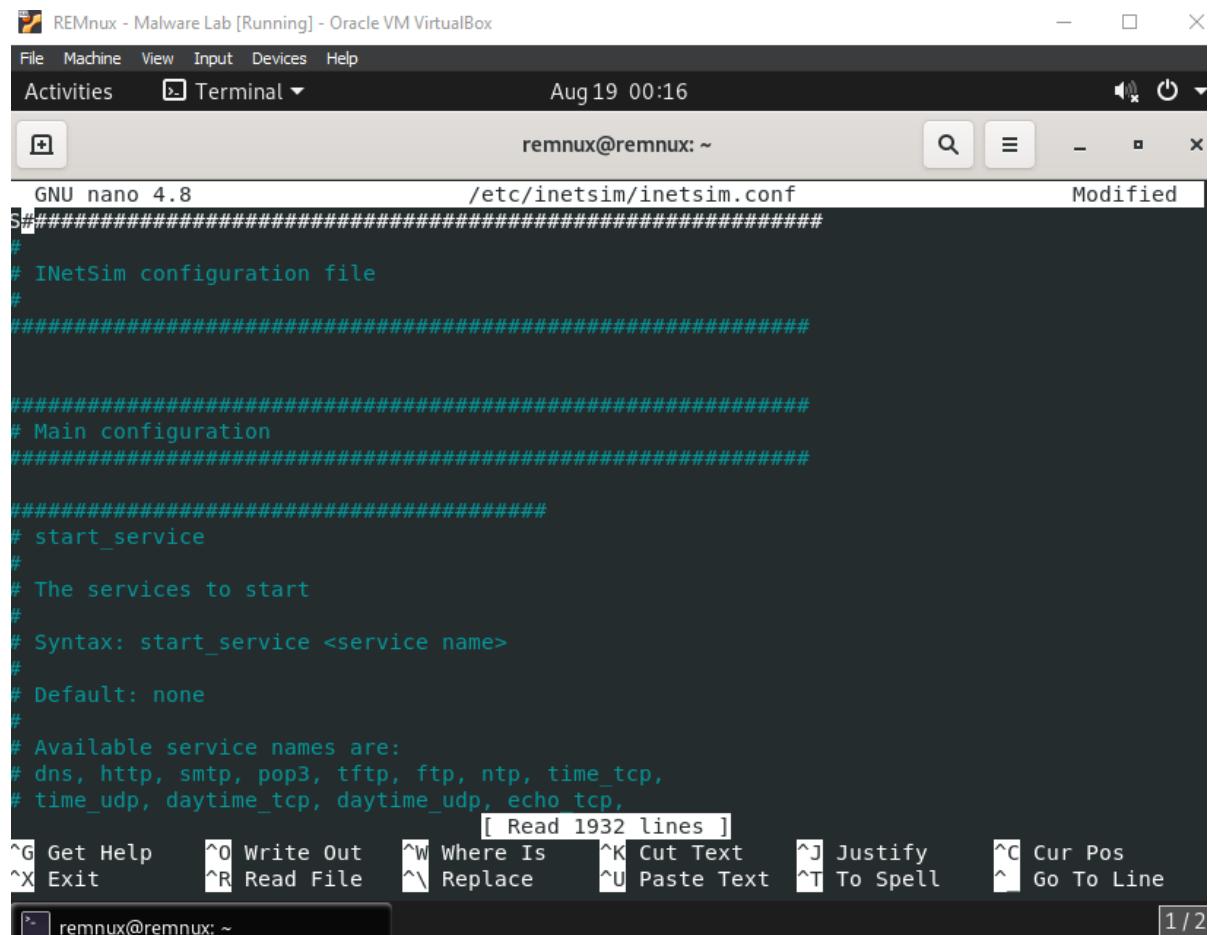
36. Open Terminal then run inetsim to check the services. All up and running except DNS server.

37. Hence terminate inetsim CTRL + C. Run sudo nano /etc/inetsim/inetsim.conf

*Uncommented start_service dns and

```
###########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip          10.0.0.4

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T
```

38. Open another Terminal to run ip a to ensure the ip address of REMnux box.
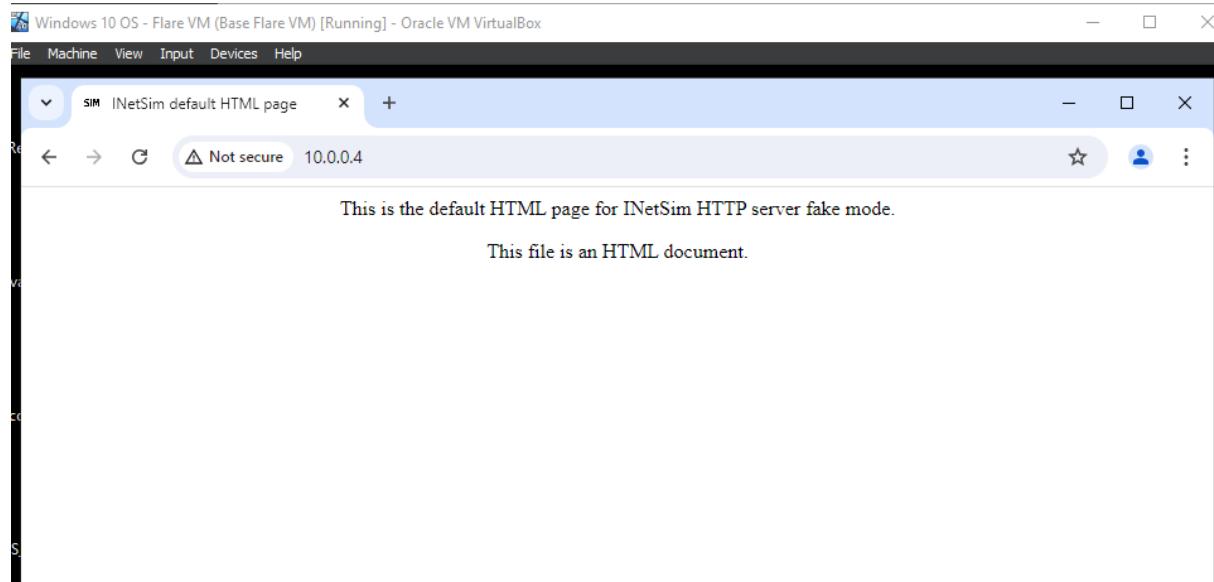
CNTRL + O then CNTRL + X to save and exit. Run inetsim again to see the changes.

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:     /var/log/inetsim/
Using data directory:    /var/lib/inetsim/
Using report directory:  /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1737) ===
Session ID:     1737
Listening on:   10.0.0.4
Real Date/Time: 2024-08-19 00:32:14
Fake Date/Time: 2024-08-19 00:32:14 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 1741)
  * smtps_465_tcp - started (PID 1745)
  * smtp_25_tcp - started (PID 1744)
  * ftp_21_tcp - started (PID 1748)
  * ftps_990_tcp - started (PID 1749)
  * https_443_tcp - started (PID 1743)
  * pop3s_995_tcp - started (PID 1747)
  * pop3_110_tcp - started (PID 1746)
  * http_80_tcp - started (PID 1742)
 done.
Simulation running.
```

Go to Flare VM, then open browser key in the REMnux ip address to check.
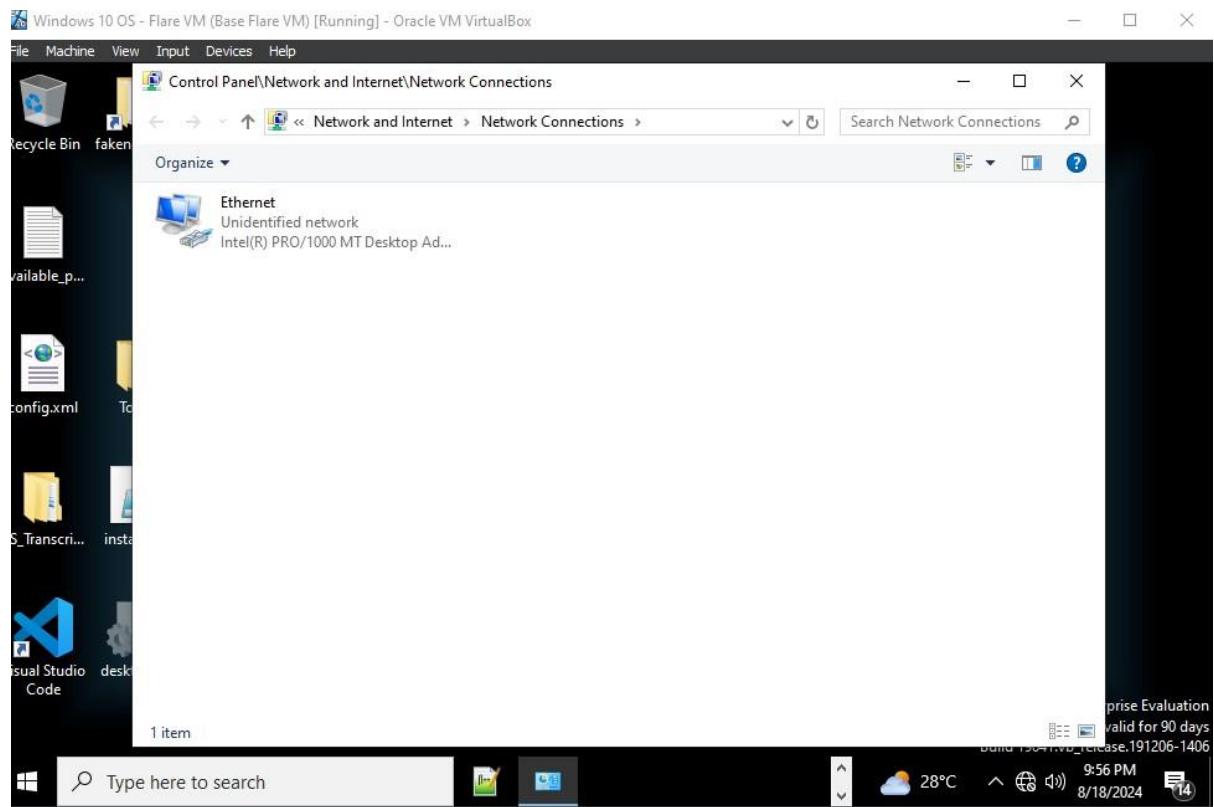
39. It shows the default HTML page or HTTP server fake mode is successful.
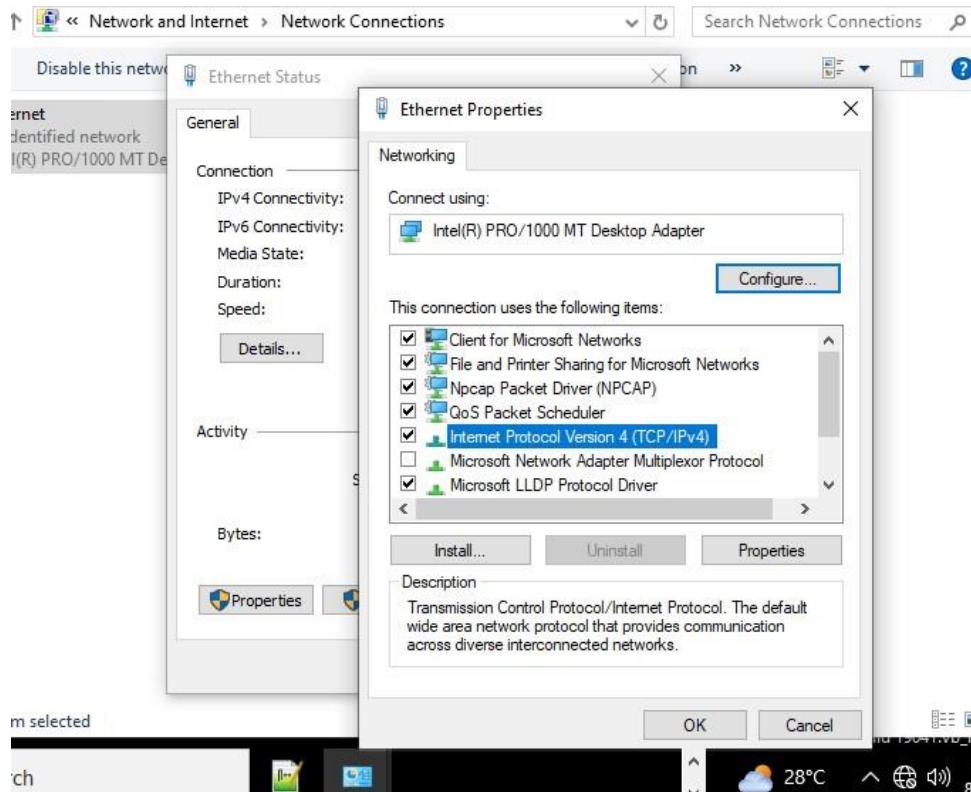
LAST STEP

40. In Flare VM, go to START menu and open Network Connection
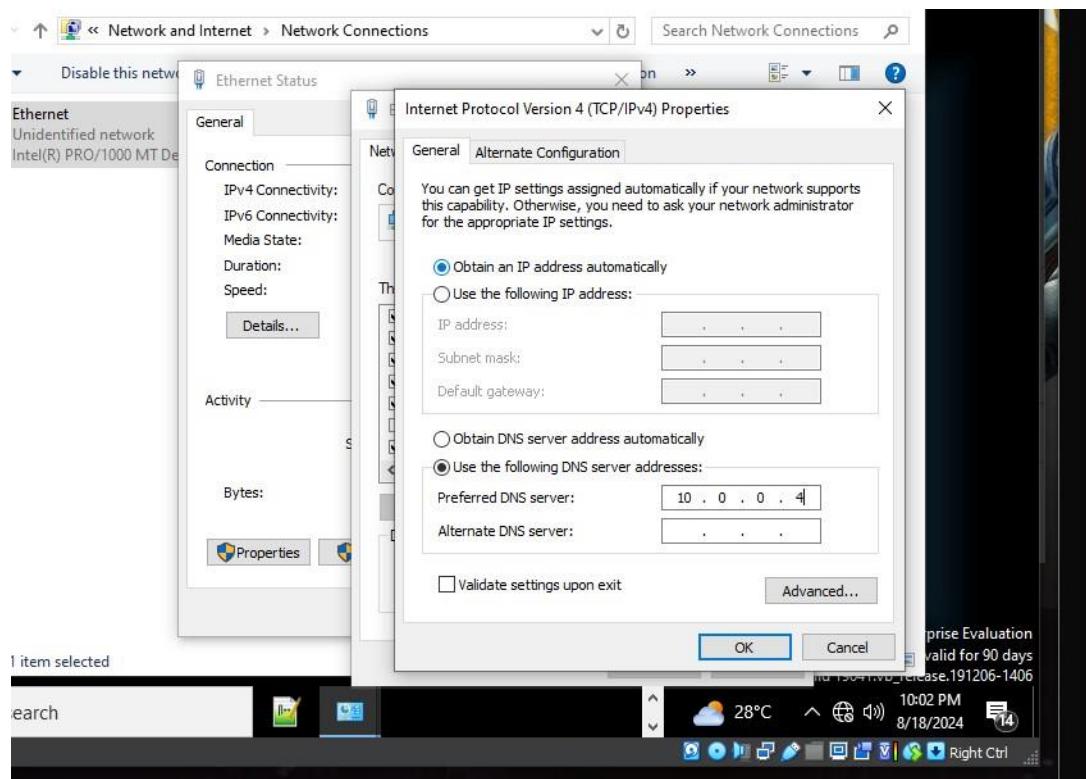

Double click then open Properties

41. Choose Internet Protocol Version 4, click Properties. Configure as below picture:
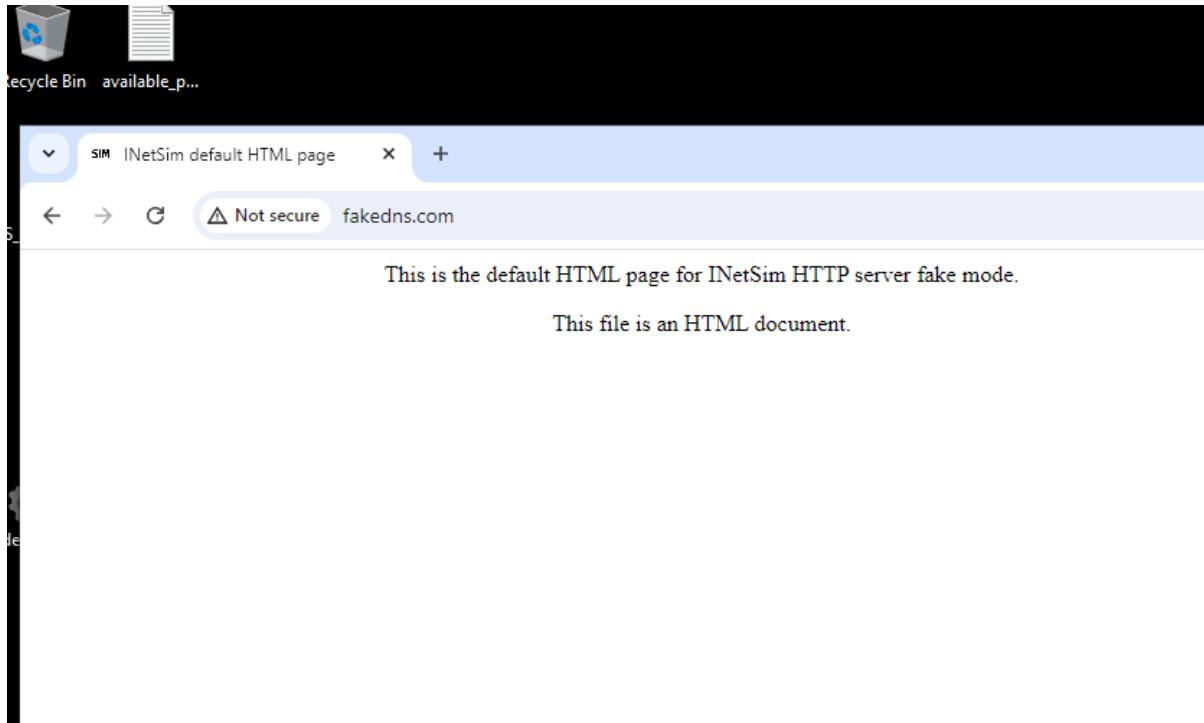
Set the IP address for DNS server to the INETSIM in the REMnux Box.

Click OK and EXIT.

42. With this by typing any web address in browser, it will direct you to the Fake HTML page provided INETSIM is running in the REMnux Box.

Now you are ready to play with some malwares!!!

References:

https://www.youtube.com/watch?v=qA0YcYMRWyI&t=3224s

https://www.youtube.com/watch?v=i8dCyy8WMKY