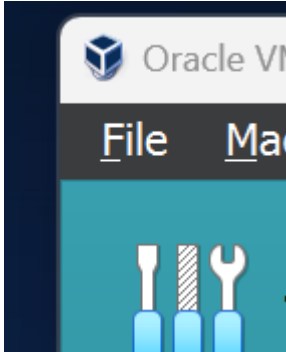


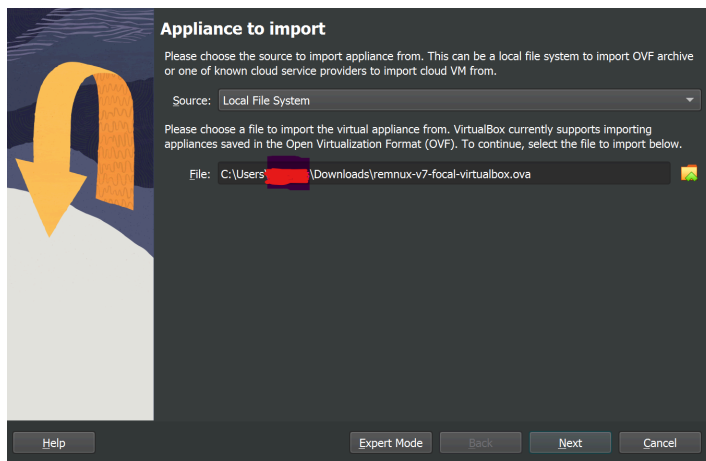
## Malware Analysis Lab Project Remnux set up and configuration

### Part 2

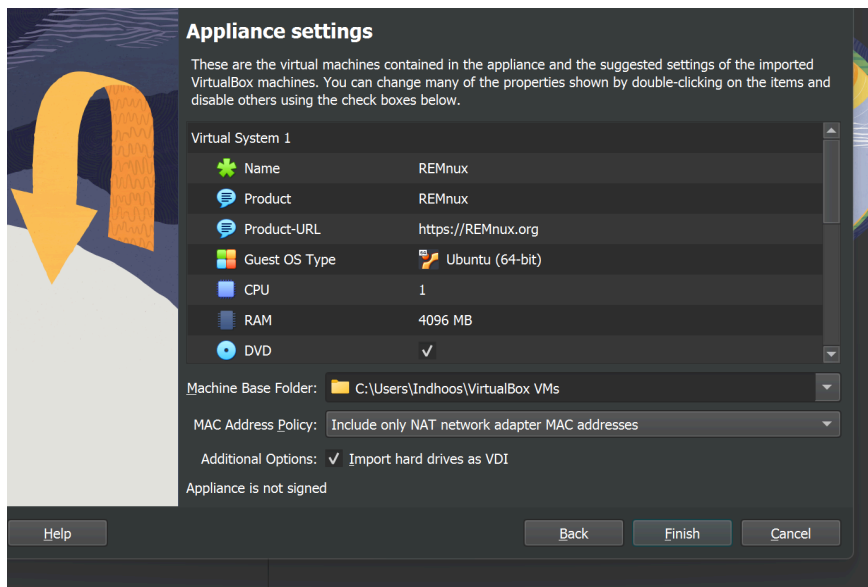
1. I've successfully installed Remnux, and the installation is complete.
2. Now, let's set up Remnux. Go back to VirtualBox, click on "File," then choose "Import Appliance," and proceed with the following steps.



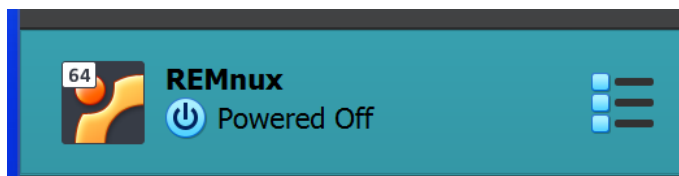
Select "Import Appliance," click the small "folder icon," navigate to your Downloads folder, and choose the Remnux installation file for importing.



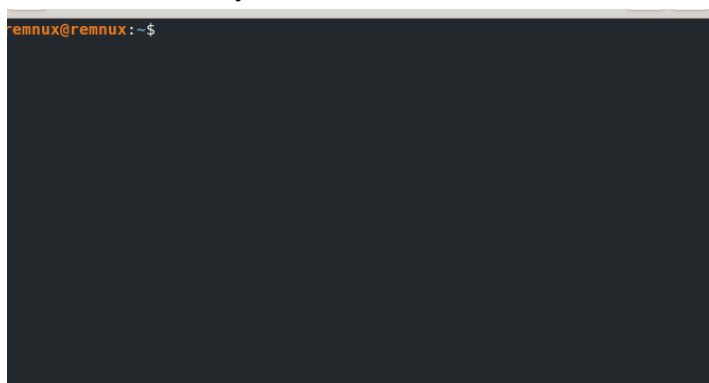
Click "Next," use the default settings, and then click "Finish." Now, wait for a few minutes as Remnux gets imported.



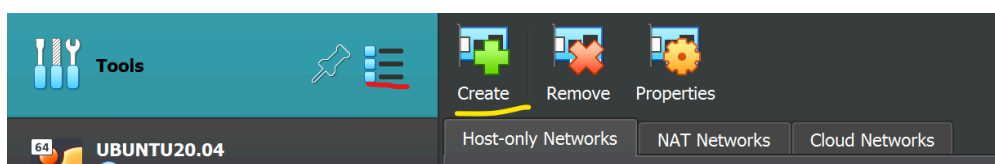
Double-click or click "Start" to launch Remnux.



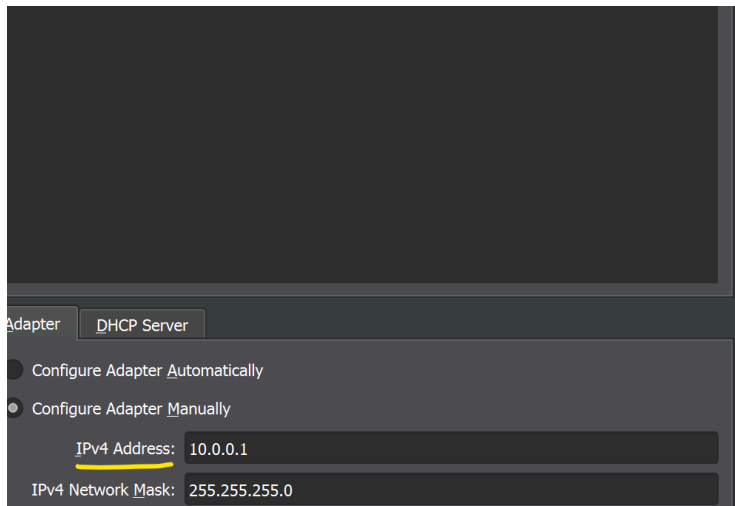
Great! Now that Remnux is open, you're ready to use its tools for various security and malware analysis tasks



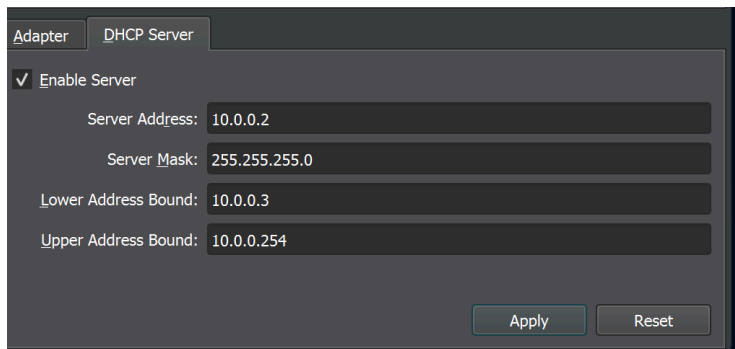
In VirtualBox, go to "File," then select "Tools," and click on the "three horizontal lines" icon. From there, choose "Network" and then select "Create" to set up your own network.



When you see the IPv4 Address, enter 10.0.0.1. Click "Apply" and confirm by clicking 'Yes.'

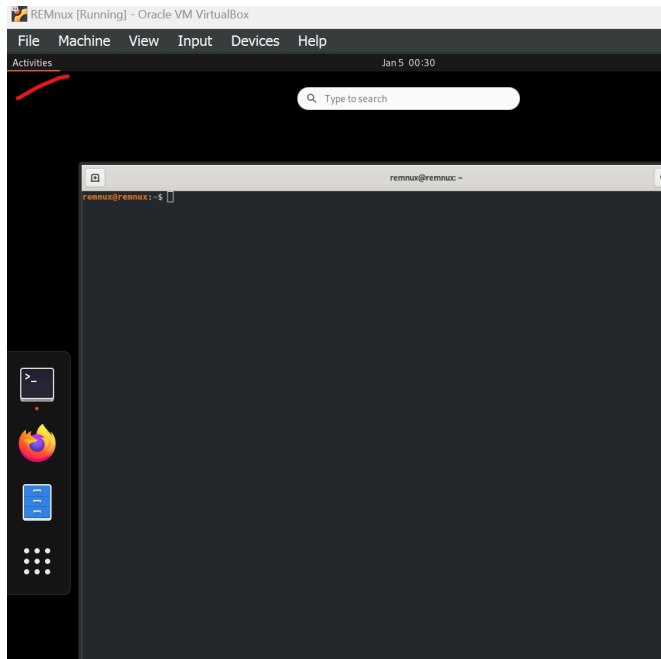


For the DHCP Server, enable it by ticking the "Enable Server" box, set the DHCP Server to 10.0.0.2, and leave the other settings as they are. Click "Apply." After this, you will have three network adapters configured.



3. This virtual network configuration will enable communication between Remnux and Flare VM while restricting access to the internet and other external connections. As Flare VM continues to install, let's go back to Remnux and configure a few settings in the Remnux configuration file.

4. Access the "activity bar" and click on "Terminal" to open the terminal.



5. I'll be using a network utility called "inetSim," which allows me to impersonate various services like DNS, FTP, SMTP, and more. To use inetSim, I need to make some changes to the configuration file in Remnux.
6. Execute this command in Remnux. `cd /etc/inetSim` and click enter then do `sudo nano inetSim.conf` then press enter.

```
remnux@remnux:~$ cd /etc/inetSim
remnux@remnux:/etc/inetSim$ sudo nano inetSim.conf
```

7. Now, using the arrow keys, navigate down and remove the commenting from the line. `"start_service dns"`

```
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
```

Additionally, remove the commenting for "service\_bind\_address" and set it to 0.0.0.0.

```
#service_bind_address 10.10.10.1
```

```
service_bind_address 0.0.0.0
```

Continue scrolling down until you reach the specified section or line you want to modify like "reach dns\_default\_ip" and uncomment the dns\_default\_ip and i am going to change the ip to our remnux ip which is 10.0.0.4

```

# 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          10.10.10.1

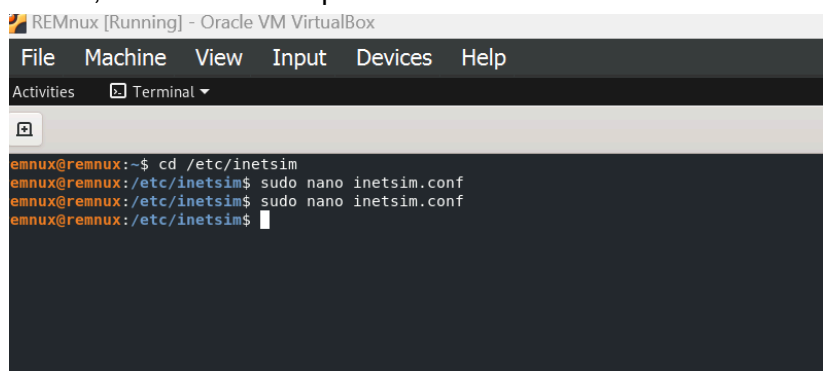
```

```

# 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

```

At this point, you are satisfied with the settings. Proceed to press "CTRL + X," then type "y," and press "Enter" to exit out of the configuration view and return to the home screen, as shown in the picture below.

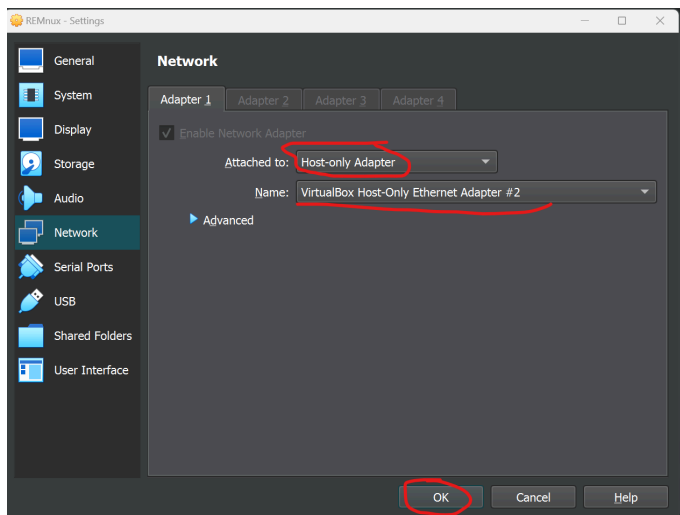


```

REMnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
emnux@remnux:~$ cd /etc/inetsim
emnux@remnux:/etc/inetsim$ sudo nano inetsim.conf
emnux@remnux:/etc/inetsim$ sudo nano inetsim.conf
emnux@remnux:/etc/inetsim$

```

Now, go to "Machine," then "Settings," and select "Network." Change from Nat to Host-only Adapter, and underneath, choose Adapter 2 or 3 – either one will work.

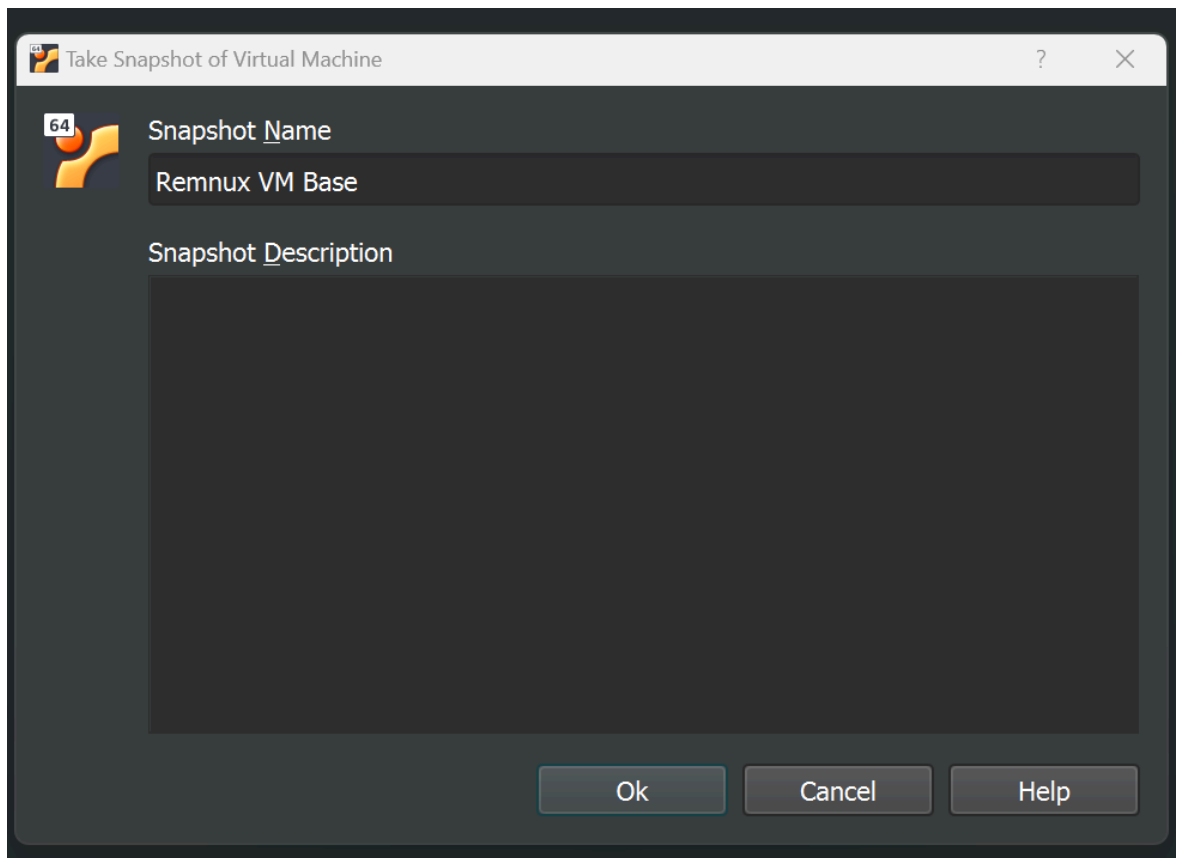


Returning to Flare VM...

Now, in Remnux, execute the command "ping 10.0.0.3" and press Enter. If you see a ping reply, as shown in the picture below, it confirms successful communication between both virtual machines.

```
remnux@remnux:/etc/inetsim$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data:
64 bytes from 10.0.0.3: icmp_seq=1 ttl=128 time=0.912 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=128 time=1.13 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=128 time=2.14 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=128 time=0.593 ms
64 bytes from 10.0.0.3: icmp_seq=5 ttl=128 time=0.463 ms
64 bytes from 10.0.0.3: icmp_seq=6 ttl=128 time=0.385 ms
64 bytes from 10.0.0.3: icmp_seq=7 ttl=128 time=1.11 ms
^C
--- 10.0.0.3 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6079ms
rtt min/avg/max/mdev = 0.385/0.960/2.135/0.553 ms
remnux@remnux:/etc/inetsim$
```

- Great! Now it's time to take a snapshot. This snapshot will serve as your base installation, allowing you to revert back to a clean environment after you've completed the malware detonation.
- Navigate to "Machine," take a Snapshot, name it "Remnux VM Base," and click OK.



Congratulations! You have successfully set up your own self-hosted Malware Analysis Lab. If you have any further questions or if there's anything else I can help you with, feel free to ask. Happy analyzing!