Self-Hosted Malware Analysis Lab

Lab Layout - Self-Hosted (VirtualBox)

Download VirtualBox

Link: https://www.virtualbox.org/wiki/Downloads

Download Windows 10 Enterprise

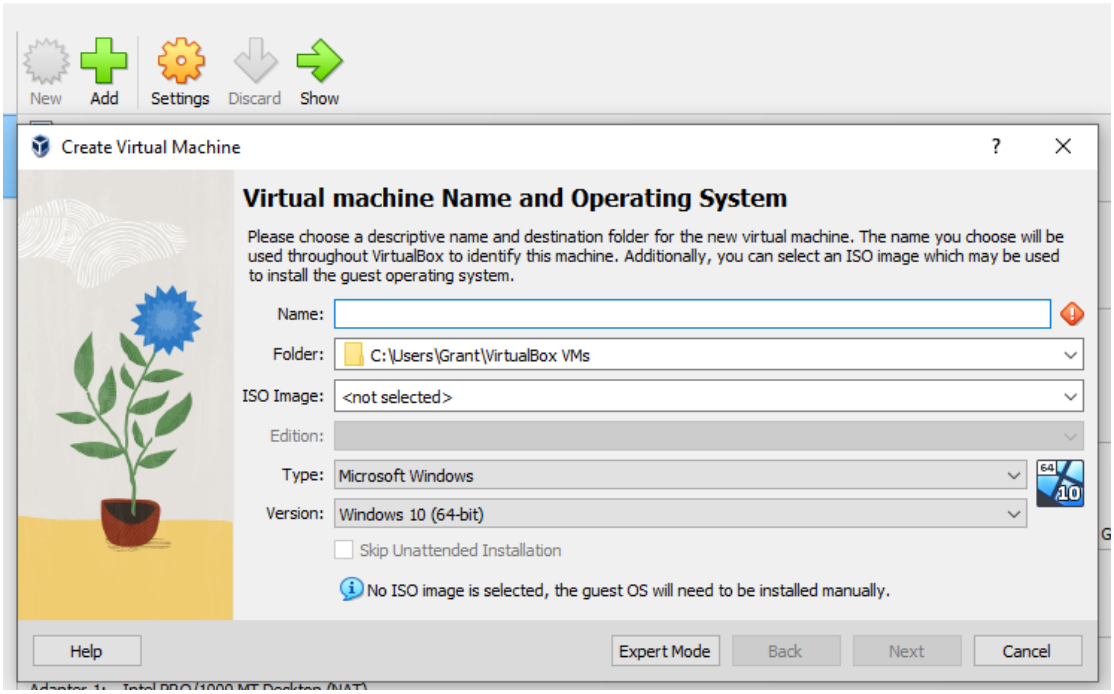
Link:

- https://info.microsoft.com/ww-landing-windows-10-enterprise.html
- https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise

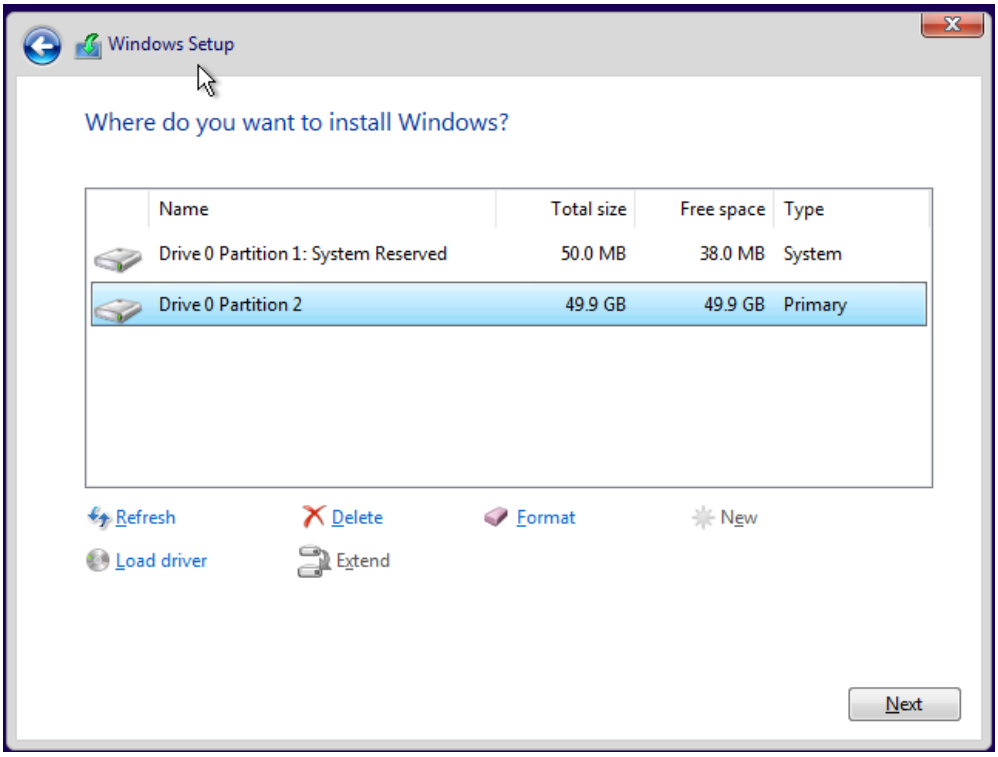
Download Remnux

Link: https://docs.remnux.org/install-distro/get-virtual-appliance

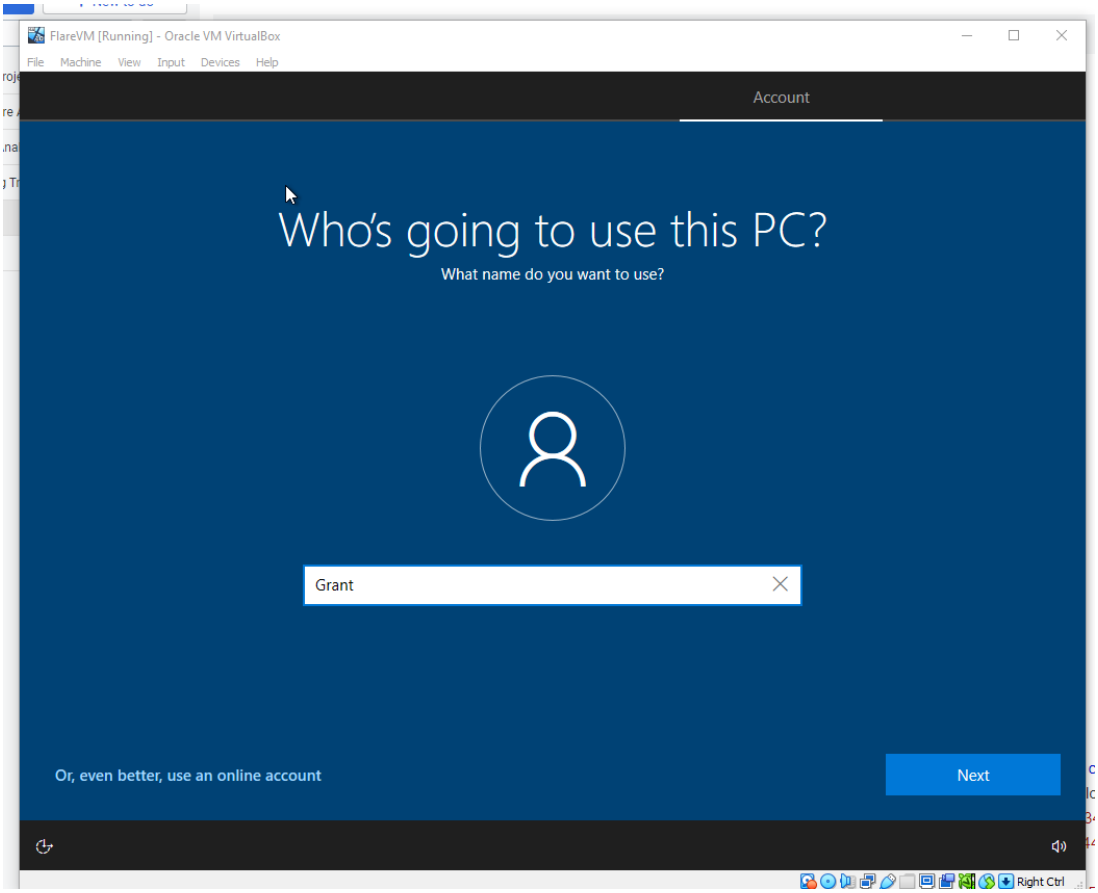
Setup Windows 10 With Guest Additions



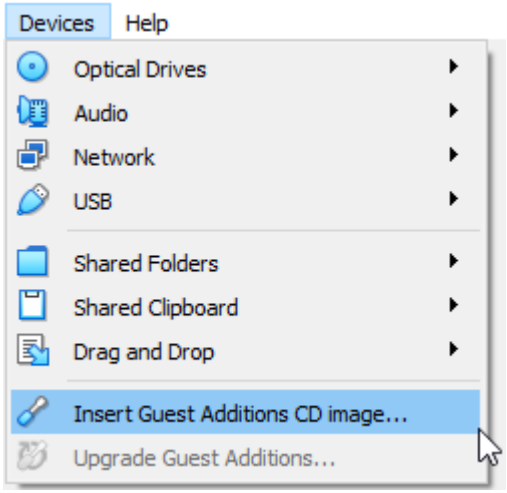
Create a new Virtual Machine.



Create a new partition.



Choose "Domain Join".



Devices -> Insert Guest Additions CD Image

Go to "This PC" -> CD Drive Virtualization -> Run the `VBoxWindowsAdditions-amd64` -> Reboot Device.

Setup FlareVM

Download Chrome or Firefox: https://www.google.com/chrome/ | https://www.mozilla.org/en-US/firefox/new/

Optional

Download Windows Terminal:

- Download the VCLibs package. In a PowerShell window, run: `wget https://aka.ms/Microsoft.VCLibs.x64.14.00.Desktop.appx -usebasicparsing -o VCLibs.appx`
- Download the Windows Terminal MSIX bundle from the provided link: `wget https://github.com/microsoft/terminal/releases/download/v1.15.3465.0/Microsoft.WindowsTerminal_Win10_1.15.3465.0_8wekyb3d8bbwe.msixbundle -UseBasicParsing -o winterminal.msixbundle`
- In a PowerShell admin window, add the VCLibs package: `Add-AppxPackage [C:\path\to\downloaded\VCLibs.appx]`
- In a PowerShell admin window, run: `Add-AppxPackage [C:\path\to\downloaded\winterminal.msixbundle]`
- (Optional) Pin Windows Terminal to the task bar

Disable proxy auto detect setting

- In the Windows search bar, search “proxy settings”,
- Switch "Automatically detect settings" button off

Disable Windows Defender
Disable Tamper Protection

- Search "Defender", open Defender settings and set all Defender Settings to off.

Disable Windows Defender in GPO

- In the Windows Search Bar, search and select "edit group policy"
- In GPO, navigate to → Administrative Templates → Windows Components → Microsoft Defender Antivirus → Enable “Turn off Microsoft Defender Antivirus”

Disable Windows Firewall

- GPO → Administrative Templates → Network → Network Connections → Windows Defender Firewall → Domain Profile → Disable “Protect All Network Connections”
- Do the same but for the Standard profile

Take a snapshot.

Download + Install FlareVM:

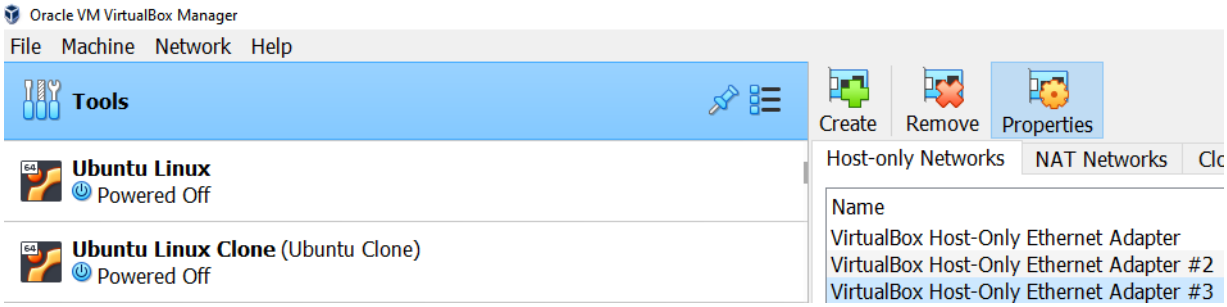
- In PowerShell Admin prompt, run: `(New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\\install.ps1")`
- Change directories to the Desktop
- Run: `Unblock-File .\\install.ps1`
- Run: `Set-ExecutionPolicy Unrestricted`
  - Accept the prompt to set the ExecPol to unrestricted if one appears
  - Run: `.\\install.ps1`
  - Follow the rest of the prompts and continue with the installation.

Take Snapshot
This is the base FlareVM installation.

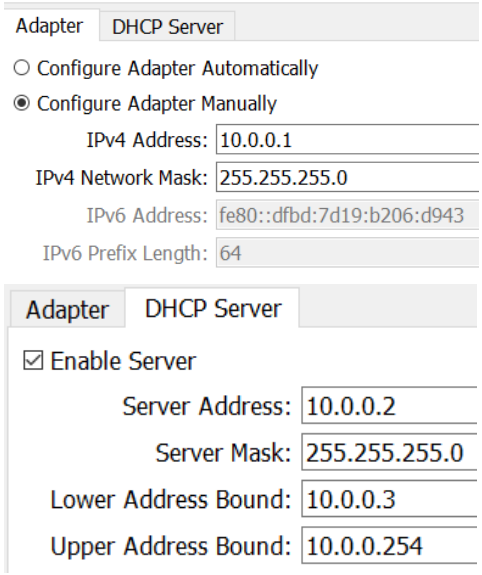
VirtualBox Network Settings

Create an isolated host-only adapter network for Windows 10 machine and Remnux to talk to each other.

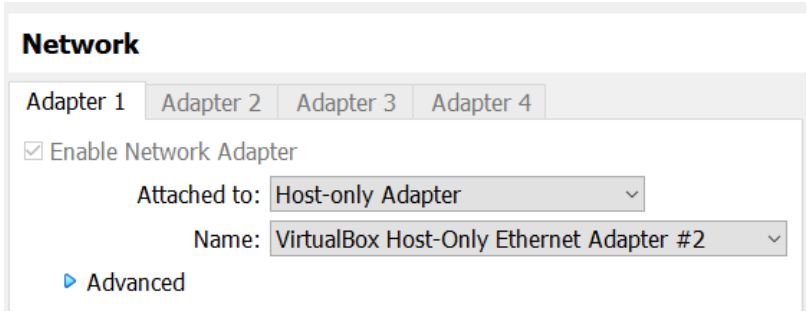
1. Create a new Host-only Network.



2. Right Click -> Properties. Set IPv4 Address to a separate private range (ex. 10.0.0.1). Set DHCP Server address to x.x.x.2, lower bound to x.x.x.3 and upper to x.x.x.254



3. Ensure all VMs are using Host-only Adapter, Isolated Ethernet Adapter.



Creating a Fake Network in Remnux

Run `inetsim` in command prompt to start network service.

Edit the config file in `/etc/inetsim/inetsim.conf`.

- Uncomment `start_service dns`
- Set the `service_bind_address` to 0.0.0.0
- Set the DNS Default IP to IP address of Remnux VM address. (10.0.0.4)

Serving Valid HTTP Responses

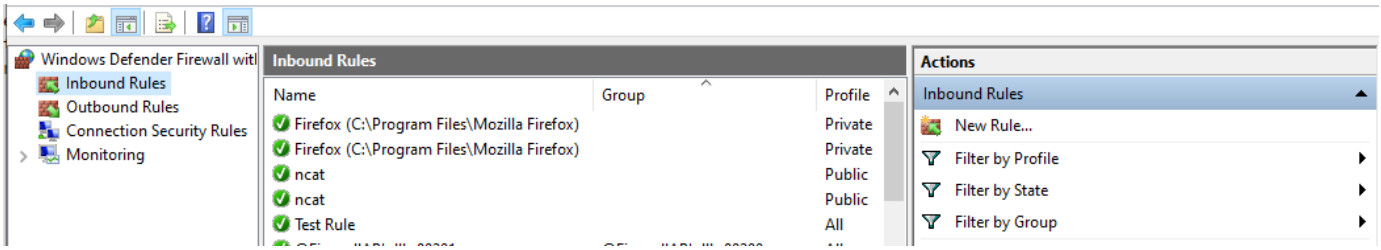
In the Windows Box:

- Enter the IP address of Remnux to receive a standard 200 response.
- http://10.0.04/malware.exe: Always serves a test binary when typing in (.exe) extension.
- my_malware.info: Serves a valid DNS response for any URL.

Windows Firewall Inbound Rule

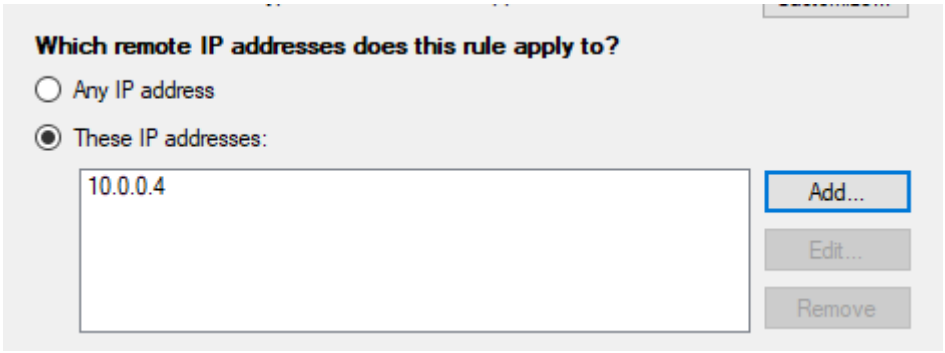
If Remnux can't ping the FlareVM host, add an inbound rule to allow all traffic through from the Remnux IP address.

Open Windows Defender Firewall.



Click "Inbound Rules" -> "New Rule..."

Choose Custom -> Next, All Programs -> Next, Leave default Protocol and Ports -> Next



Under the remote IP addresses, choose "Add", enter the Remnux IP address (10.0.0.4).

Choose "Allow the connection", leave default for Profile, Name the rule -> Finish.