Mohamedwali Mumin

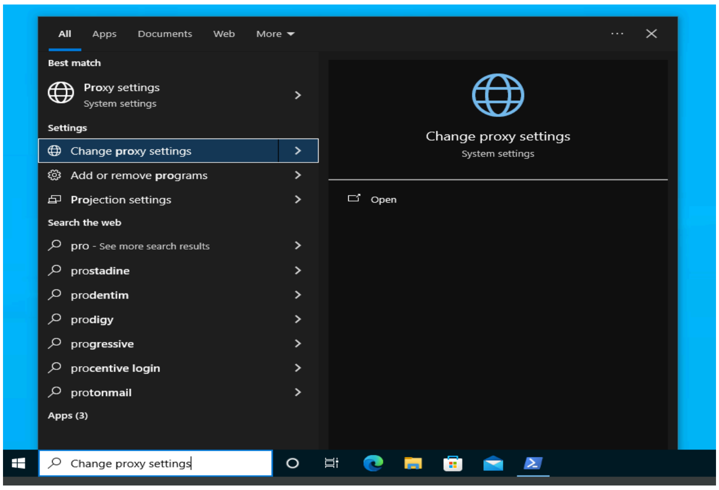
Building a Malware Analysis Lab (Self-Hosted & Cloud) Project

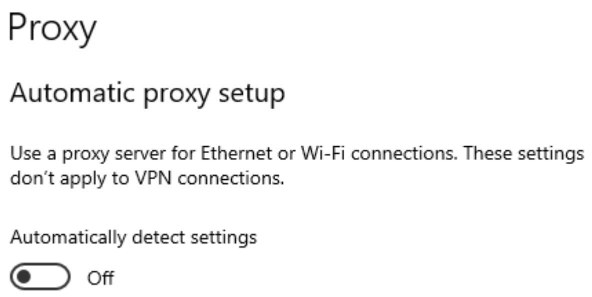
Part 1

1. Download Windows 10 Enterprise - this will be our pretend "victim" computer where we'll test the malware.
2. Also, get Remnux as a virtualbox OVA.
3. While waiting for Remnux to download:
4.
5. Set up a Windows 10 Flair VM.
6. When everything is set up, download your favorite web browser, Chrome,Brave, etc.
7. With Chrome installed, let's adjust some settings.

To install Flare VM, you'll need to tweak some default settings on Windows.

1. Start by going to your Windows search bar and searching for "proxy settings." Click on "Change proxy settings" and switch off "Automatically detect settings."




Proxy

Automatic proxy setup

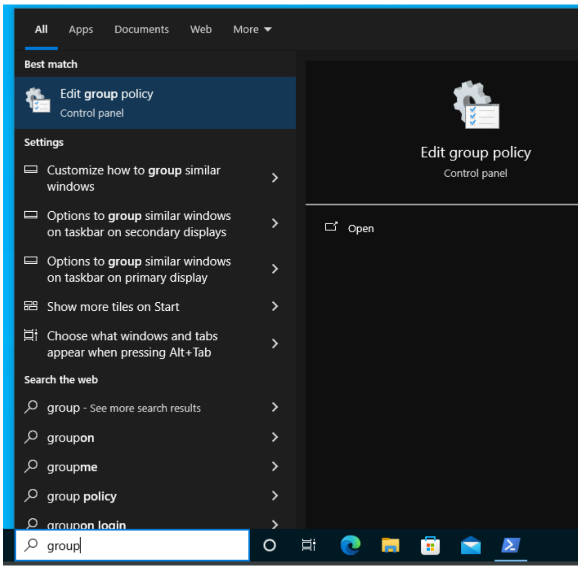
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings

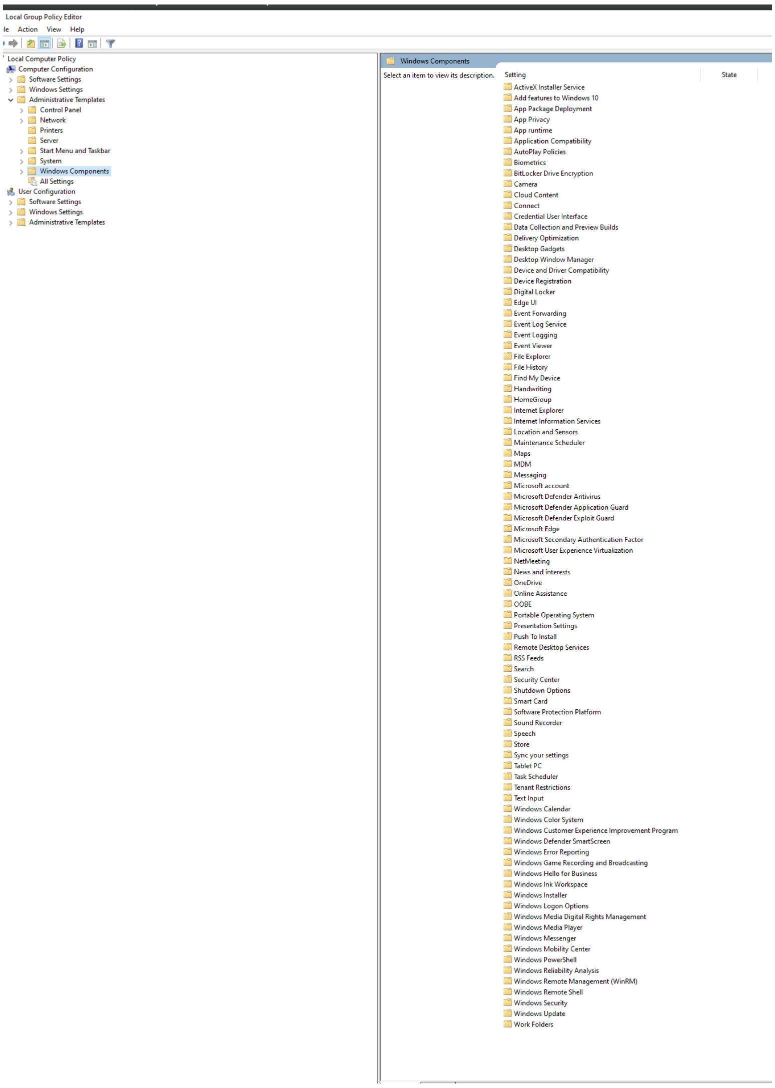
● Off

2. Next, disable Windows Defender. This is important because Windows Defender may interfere with the detonation of many common malware variants. Make sure to turn it off to ensure smooth execution when testing malware.
3. Returning to the search bar, type "defender," click on Windows Security, navigate to 'Virus & Threat Protection,' and under 'Virus & Threat Protection Settings,' click 'Manage Settings.' Turn off all the protections listed there, and then exit out. With real-time protection off, you can simply close the Windows Security window.

4. Next, let's configure some settings in the Windows Group Policy (GPO). Go back to the search bar, type "Group," and select 'Edit group policy.'


All
Apps
Documents
Web
More
Best match
Edit group policy
Control panel
Settings
Customize how to group similar windows
Options to group similar windows on taskbar on secondary displays
Options to group similar windows on taskbar on primary display
Show more tiles on Start
Choose what windows and tabs appear when pressing Alt+Tab
Search the web
group - See more search results
groupon
groupme
group policy
groupon login
Edit group policy
Control panel
Open
group

5. Once you've opened 'Edit group policy,' navigate to "Administrative Templates," then "Windows Components," and go to 'Microsoft Defender Antivirus.' Inside, double-click on 'Turn off Microsoft Defender Antivirus,' choose 'Enable,' apply the changes, and click 'OK.'

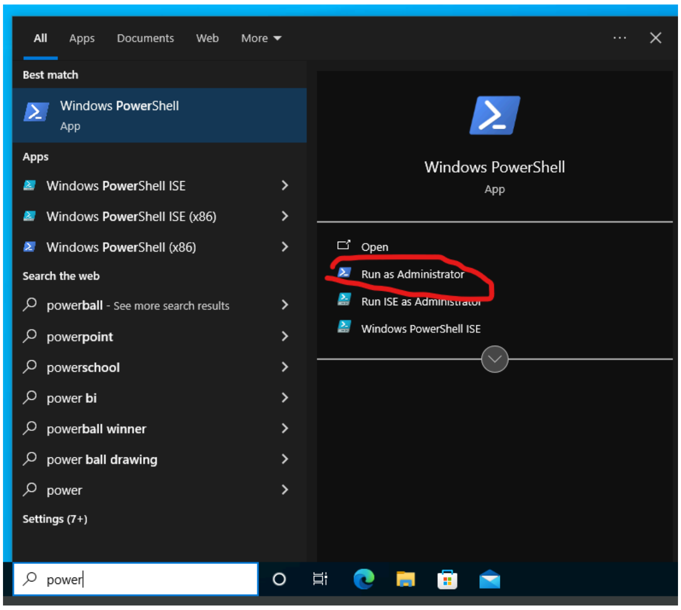


6. To turn off the Windows Firewall, go to "Administrative Templates," then click on "Network," followed by "Network Connections." Choose 'Windows Defender Firewall' and click on 'Domain Profile.' Double-click on "Windows Defender Firewall: Protect all network connections," select 'Disabled,' apply the changes, and then click 'OK.'

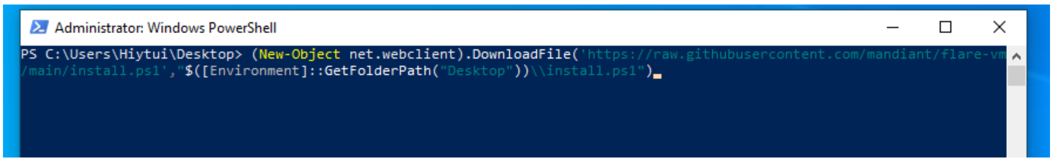
   Now, go back to Windows Defender Firewall, click on 'Standard Profile,' and double-click on "Windows Defender Firewall: Protect all network connections." Choose 'Disabled,' apply the changes, and then click 'OK.'

7. At this point, you've configured the necessary settings for Flare VM installation. Exit out of all the settings and applications.

8. Now, create a snapshot for Flare VM. After the snapshot, you'll be prepared to install Flare VM via PowerShell. Open PowerShell as an administrator and navigate to the desktop using the command: cd C:\Users\Yourname\Desktop

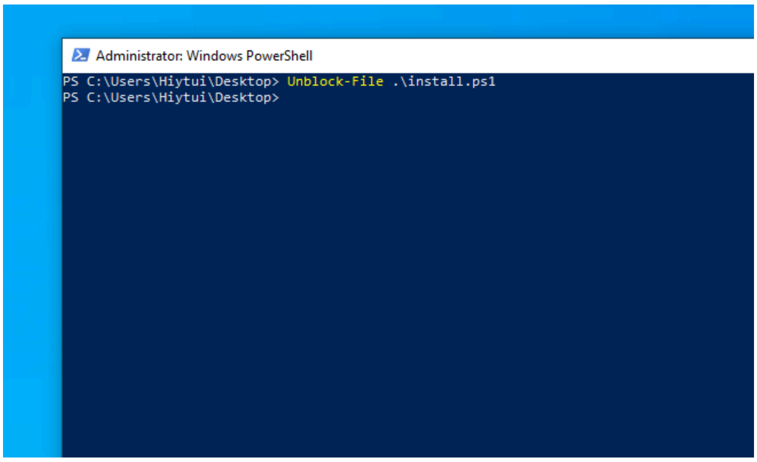


9. After that run this command in powershell administrator in the picture below. (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\\install.ps1")



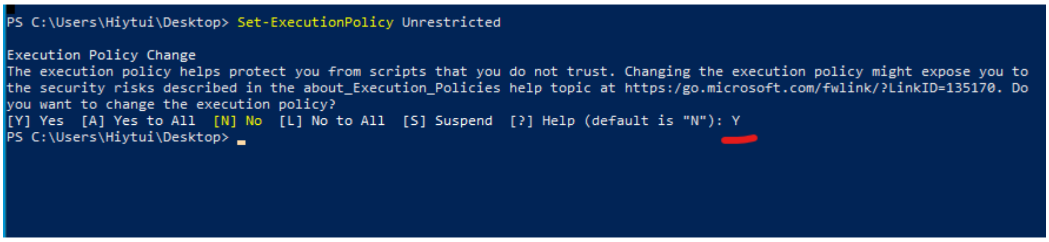
```
PS C:\Users\Hiytui\Desktop> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm
/main/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\\install.ps1")
```

Next unblock the file using this command Unblock-File .\install.ps1



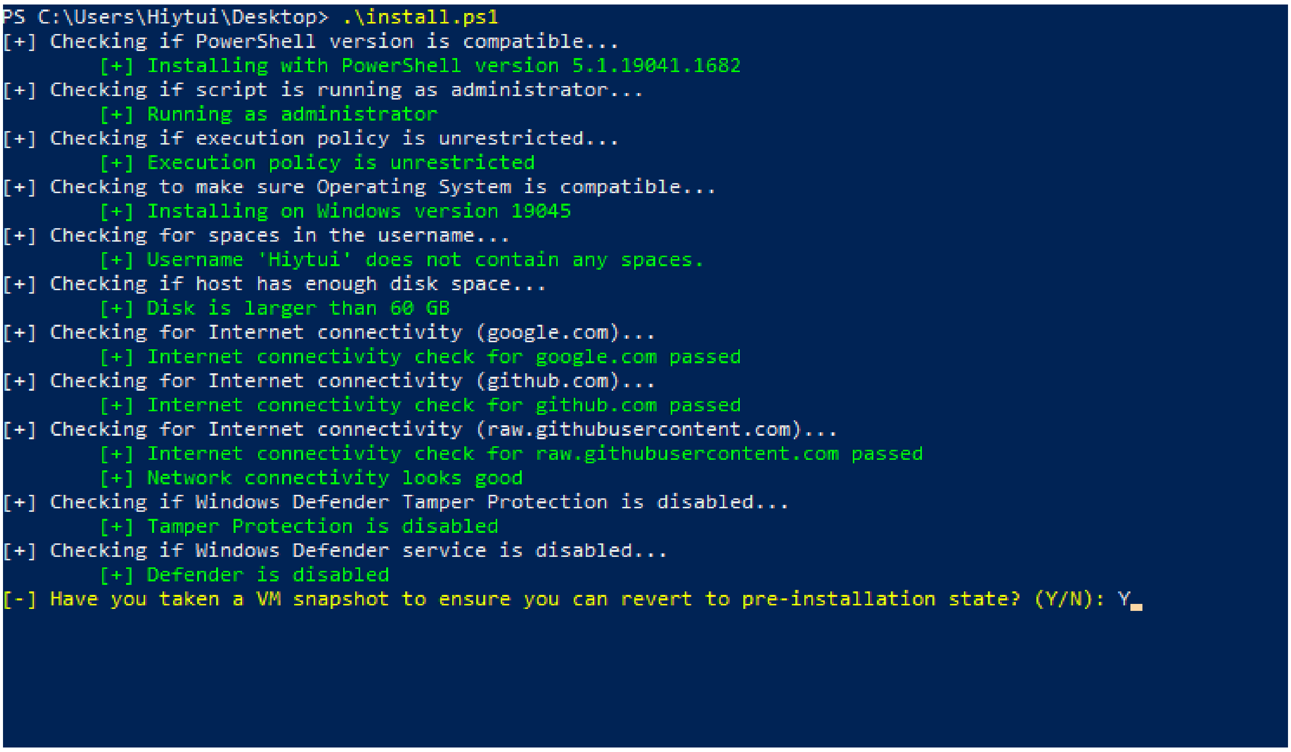
```
PS C:\Users\Hiytui\Desktop> Unblock-File .\install.ps1
PS C:\Users\Hiytui\Desktop>
```

Then run Set-ExecutionPolicy Unrestricted. then “Y” “hint “ its better to write on the powershell.



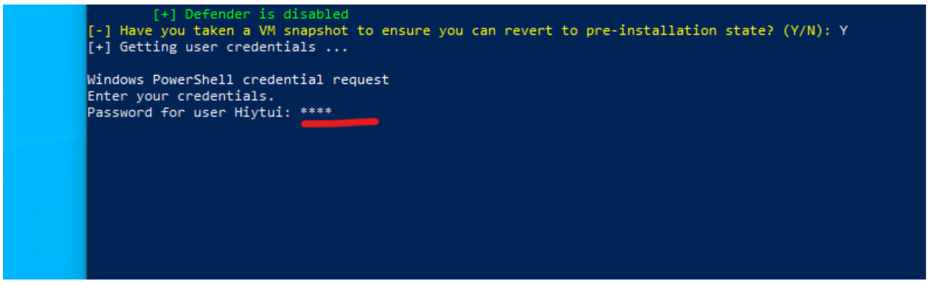
```
PS C:\Users\Hiytui\Desktop> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to
the security risks described in the about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do
you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
PS C:\Users\Hiytui\Desktop> _
```

Now it's time to execute the installation PowerShell script by entering the following command. .\install.ps1

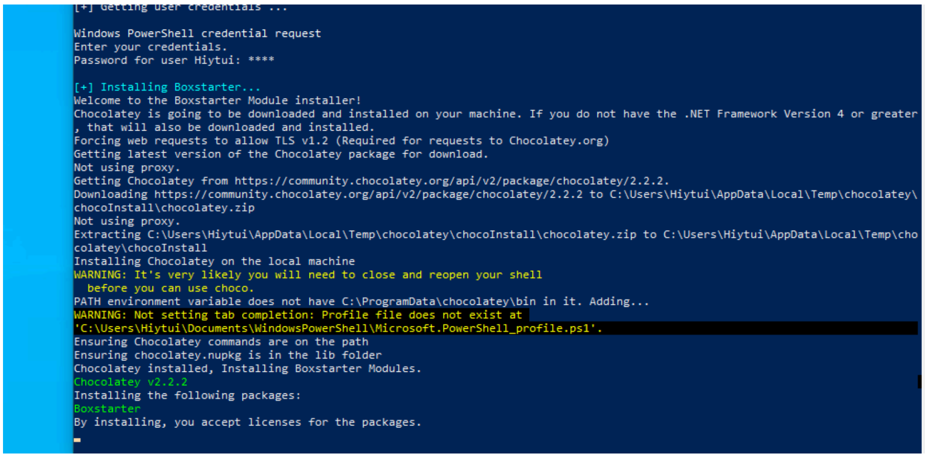


```
PS C:\Users\Hiytui\Desktop> .\install.ps1
[+] Checking if PowerShell version is compatible...
        [+] Installing with PowerShell version 5.1.19041.1682
[+] Checking if script is running as administrator...
        [+] Running as administrator
[+] Checking if execution policy is unrestricted...
        [+] Execution policy is unrestricted
[+] Checking to make sure Operating System is compatible...
        [+] Installing on Windows version 19045
[+] Checking for spaces in the username...
        [+] Username 'Hiytui' does not contain any spaces.
[+] Checking if host has enough disk space...
        [+] Disk is larger than 60 GB
[+] Checking for Internet connectivity (google.com)...
        [+] Internet connectivity check for google.com passed
[+] Checking for Internet connectivity (github.com)...
        [+] Internet connectivity check for github.com passed
[+] Checking for Internet connectivity (raw.githubusercontent.com)...
        [+] Internet connectivity check for raw.githubusercontent.com passed
        [+] Network connectivity looks good
[+] Checking if Windows Defender Tamper Protection is disabled...
        [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
        [+] Defender is disabled
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
```

During this step, you will be prompted to enter the credentials you previously set up. Follow the instructions as shown in the picture below and allow the process to proceed with the download.

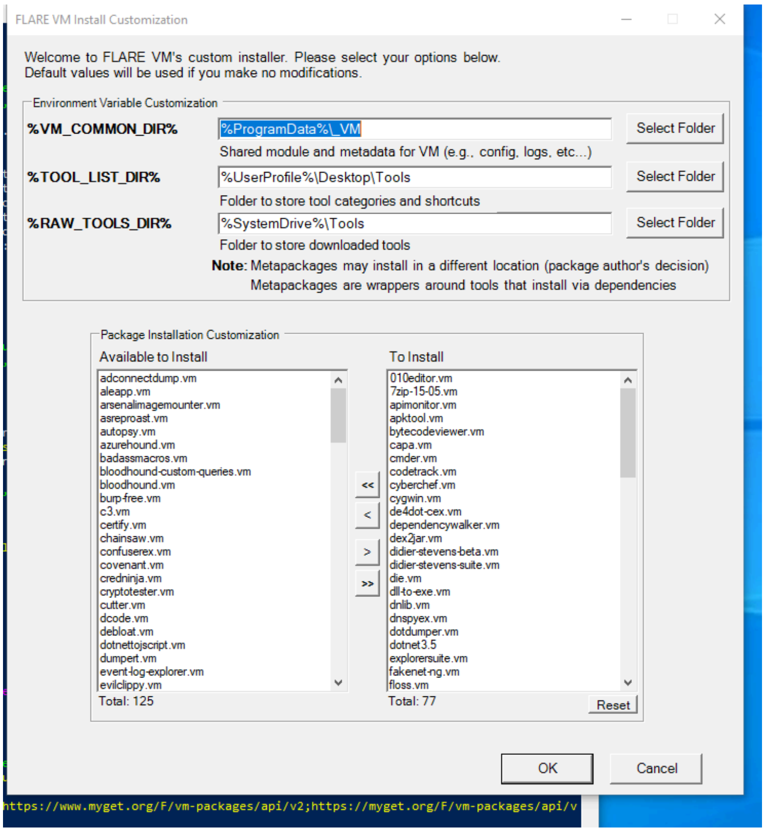


```
        [+] Defender is disabled
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user Hiytui: ****
```



```
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user Hiytui: ****

[+] Installing Boxstarter...
Welcome to the Boxstarter Module installer!
Chocolatey is going to be downloaded and installed on your machine. If you do not have the .NET Framework Version 4 or greater
, that will also be downloaded and installed.
Forcing web requests to allow TLS v1.2 (Required for requests to Chocolatey.org)
Getting latest version of the Chocolatey package for download.
Not using proxy.
Getting Chocolatey from https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2.
Downloading https://community.chocolatey.org/api/v2/package/chocolatey/2.2.2 to C:\Users\Hiytui\AppData\Local\Temp\chocolatey\
chocoInstall\chocolatey.zip
Not using proxy.
Extracting C:\Users\Hiytui\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\Hiytui\AppData\Local\Temp\cho
colatey\chocoInstall
Installing Chocolatey on the local machine
WARNING: It's very likely you will need to close and reopen your shell
  before you can use choco.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at
'C:\Users\Hiytui\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Ensuring Chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder
Chocolatey installed, Installing Boxstarter Modules.
Chocolatey v2.2.2
Installing the following packages:
Boxstarter
By installing, you accept licenses for the packages.
```

10. A dialog box will appear, taking approximately 1 minute to pop up. During this time, essential installation packages for the tools required for malware analysis will be installed. Simply click "OK" when prompted.



FLARE VM Install Customization

Welcome to FLARE VM's custom installer. Please select your options below.
Default values will be used if you make no modifications.

Environment Variable Customization

%VM_COMMON_DIR% %ProgramData%_VM
Shared module and metadata for VM (e.g., config, logs, etc...)

%TOOL_LIST_DIR% %UserProfile%\Desktop\Tools
Folder to store tool categories and shortcuts

%RAW_TOOLS_DIR% %SystemDrive%\Tools
Folder to store downloaded tools

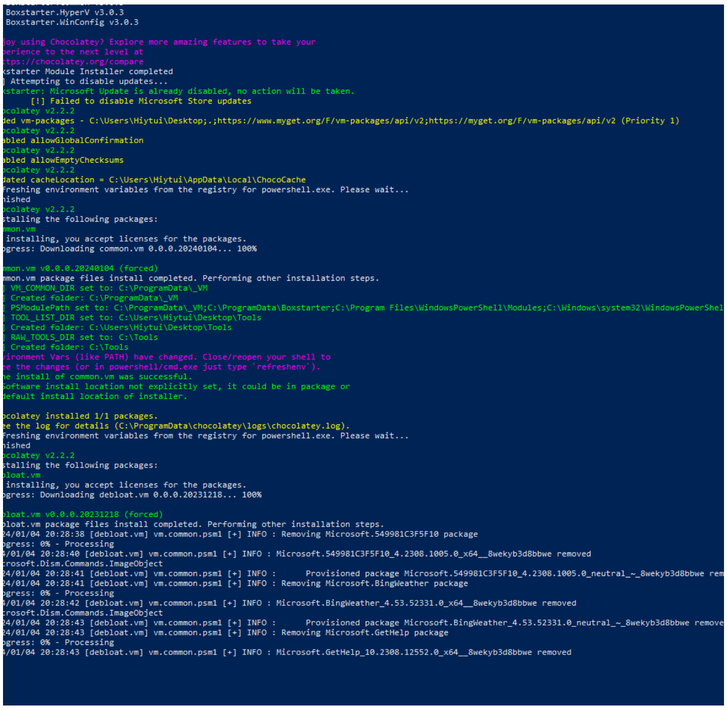
Note: Metapackages may install in a different location (package author's decision)
Metapackages are wrappers around tools that install via dependencies

Package Installation Customization

Available to Install
adconnectdump.vm
aleapp.vm
arsenalimagemounter.vm
asreproast.vm
autopsy.vm
azurehound.vm
badassmacros.vm
bloodhound-custom-queries.vm
bloodhound.vm
burp-free.vm
c3.vm
certify.vm
chainsaw.vm
confuserex.vm
covenant.vm
credninja.vm
cryptotester.vm
cutter.vm
dcode.vm
debloat.vm
dotnettojscript.vm
dumpert.vm
event-log-explorer.vm
evilclippy.vm
Total: 125

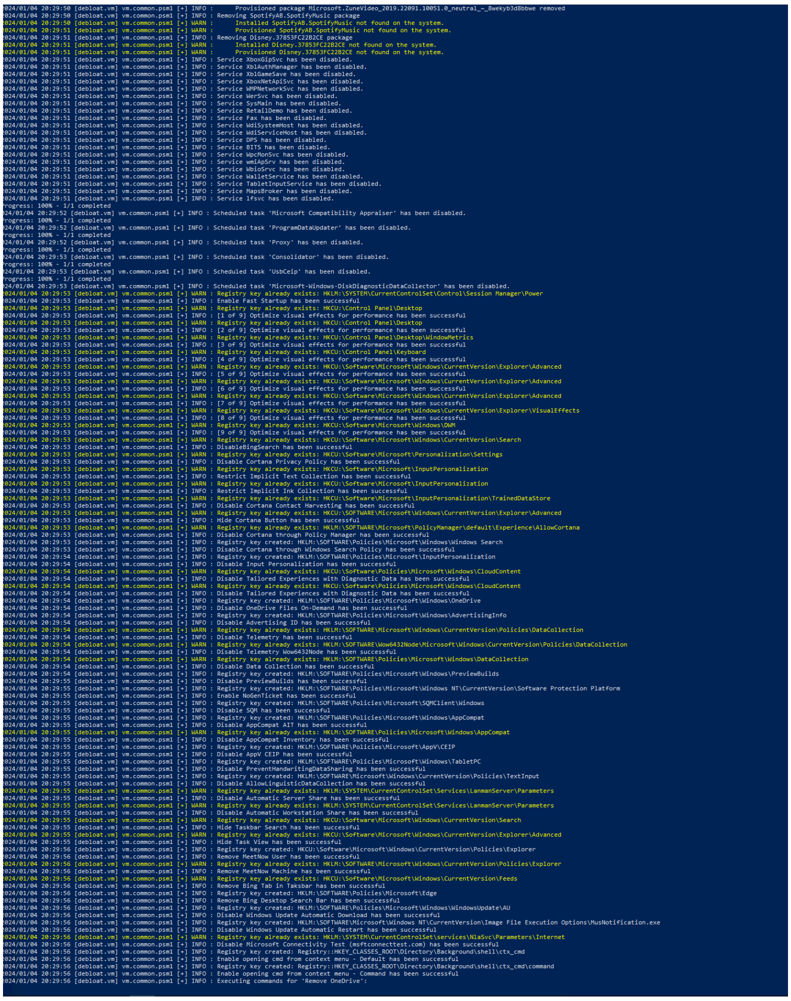
To Install
010editor.vm
7zip-15-05.vm
apimonitor.vm
apktool.vm
bytecodeviewer.vm
capa.vm
cmder.vm
codetrack.vm
cyberchef.vm
cygwin.vm
de4dot-cex.vm
dependencywalker.vm
dex2jar.vm
didier-stevens-beta.vm
didier-stevens-suite.vm
die.vm
dll-to-exe.vm
dnlib.vm
dnspyex.vm
dotdumper.vm
dotnet3.5
explorersuite.vm
fakenet-ng.vm
floss.vm
Total: 77

```
https://www.myget.org/F/vm-packages/api/v2;https://myget.org/F/vm-packages/api/v
```



```
 Boxstarter.HyperV v3.0.3
 Boxstarter.WinConfig v3.0.3

joy using Chocolatey? Explore more amazing features to take your
perience to the next level at
tps://chocolatey.org/compare
xstarter Module Installer completed
] Attempting to disable updates...
xstarter: Microsoft Update is already disabled, no action will be taken.
      [!] Failed to disable Microsoft Store updates
ocolatey v2.2.2
ded vm-packages - C:\Users\Hiytui\Desktop;.;https://www.myget.org/F/vm-packages/api/v2;https://myget.org/F/vm-packages/api/v2 (Priority 1)
ocolatey v2.2.2
abled allowGlobalConfirmation
ocolatey v2.2.2
abled allowEmptyChecksums
ocolatey v2.2.2
dated cacheLocation = C:\Users\Hiytui\AppData\Local\ChocoCache
freshing environment variables from the registry for powershell.exe. Please wait...
nished
ocolatey v2.2.2
stalling the following packages:
mmon.vm
 installing, you accept licenses for the packages.
ogress: Downloading common.vm 0.0.0.20240104... 100%

mmon.vm v0.0.0.20240104 (forced)
mmon.vm package files install completed. Performing other installation steps.
] VM_COMMON_DIR set to: C:\ProgramData\_VM
] Created folder: C:\ProgramData\_VM
] PSModulePath set to: C:\ProgramData\_VM;C:\ProgramData\Boxstarter;C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShel
] TOOL_LIST_DIR set to: C:\Users\Hiytui\Desktop\Tools
] Created folder: C:\Users\Hiytui\Desktop\Tools
] RAW_TOOLS_DIR set to: C:\Tools
] Created folder: C:\Tools
vironment Vars (like PATH) have changed. Close/reopen your shell to
ee the changes (or in powershell/cmd.exe just type `refreshenv`).
he install of common.vm was successful.
Software install location not explicitly set, it could be in package or
default install location of installer.

ocolatey installed 1/1 packages.
ee the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
freshing environment variables from the registry for powershell.exe. Please wait...
nished
ocolatey v2.2.2
stalling the following packages:
bloat.vm
 installing, you accept licenses for the packages.
ogress: Downloading debloat.vm 0.0.0.20231218... 100%

bloat.vm v0.0.0.20231218 (forced)
bloat.vm package files install completed. Performing other installation steps.
24/01/04 20:28:38 [debloat.vm] vm.common.psm1 [+] INFO : Removing Microsoft.549981C3F5F10 package
ogress: 0% - Processing
4/01/04 20:28:40 [debloat.vm] vm.common.psm1 [+] INFO : Microsoft.549981C3F5F10_4.2308.1005.0_x64__8wekyb3d8bbwe removed
crosoft.Dism.Commands.ImageObject
24/01/04 20:28:41 [debloat.vm] vm.common.psm1 [+] INFO :      Provisioned package Microsoft.549981C3F5F10_4.2308.1005.0_neutral_~_8wekyb3d8bbwe rem
24/01/04 20:28:41 [debloat.vm] vm.common.psm1 [+] INFO : Removing Microsoft.BingWeather package
ogress: 0% - Processing
4/01/04 20:28:42 [debloat.vm] vm.common.psm1 [+] INFO : Microsoft.BingWeather_4.53.52331.0_x64__8wekyb3d8bbwe removed
crosoft.Dism.Commands.ImageObject
24/01/04 20:28:43 [debloat.vm] vm.common.psm1 [+] INFO :      Provisioned package Microsoft.BingWeather_4.53.52331.0_neutral_~_8wekyb3d8bbwe remove
24/01/04 20:28:43 [debloat.vm] vm.common.psm1 [+] INFO : Removing Microsoft.GetHelp package
ogress: 0% - Processing
4/01/04 20:28:43 [debloat.vm] vm.common.psm1 [+] INFO : Microsoft.GetHelp_10.2308.12552.0_x64__8wekyb3d8bbwe removed
```

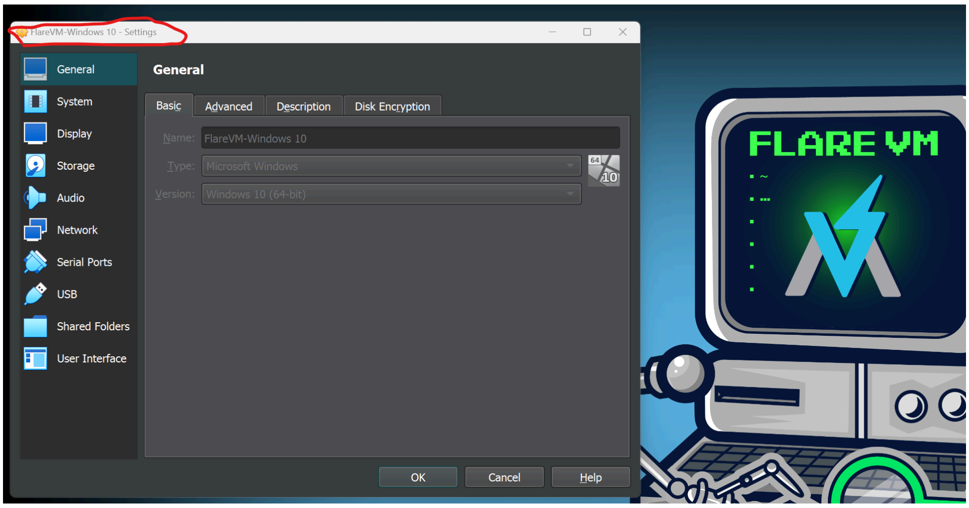
In this scenario, allow Flare VM to be installed via the PowerShell script. The installation process may take anywhere from 10 minutes to an hour, depending on your connection speed. Refer to the picture below for progress updates.



```
2024/01/04 20:29:50 [debloat.vm] vm.common.psm1 [+] INFO :      Provisioned package Microsoft.ZuneVideo_2019.22091.10051.0_neutral_~_8wekyb3d8bbwe removed
2024/01/04 20:29:50 [debloat.vm] vm.common.psm1 [+] INFO : Removing SpotifyAB.SpotifyMusic package
2024/01/04 20:29:50 [debloat.vm] vm.common.psm1 [+] WARN :      Installed SpotifyAB.SpotifyMusic not found on the system.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] WARN :      Provisioned SpotifyAB.SpotifyMusic not found on the system.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Removing Disney.37853FC22B2CE package
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] WARN :      Installed Disney.37853FC22B2CE not found on the system.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] WARN :      Provisioned Disney.37853FC22B2CE not found on the system.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service XboxGipSvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service XblAuthManager has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service XblGameSave has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service XboxNetApiSvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WMPNetworkSvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WerSvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service SysMain has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service RetailDemo has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service Fax has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WdiSystemHost has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WdiServiceHost has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service DPS has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service BITS has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WpcMonSvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service wmiApSrv has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WbioSrvc has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service WalletService has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service TabletInputService has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service MapsBroker has been disabled.
2024/01/04 20:29:51 [debloat.vm] vm.common.psm1 [+] INFO : Service lfsvc has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:52 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'Microsoft Compatibility Appraiser' has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:52 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'ProgramDataUpdater' has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:52 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'Proxy' has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'Consolidator' has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'UsbCeip' has been disabled.
Progress: 100% - 1/1 completed
024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Scheduled task 'Microsoft-Windows-DiskDiagnosticDataCollector' has been disabled.
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Power
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Enable Fast Startup has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Control Panel\Desktop
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [1 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Control Panel\Desktop
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [2 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Control Panel\Desktop\WindowMetrics
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [3 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Control Panel\Keyboard
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [4 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [5 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [6 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [7 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [8 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\DWM
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : [9 of 9] Optimize visual effects for performance has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Search
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : DisableBingSearch has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Personalization\Settings
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Disable Cortana Privacy Policy has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\InputPersonalization
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Restrict Implicit Text Collection has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\InputPersonalization
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Restrict Implicit Ink Collection has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\InputPersonalization\TrainedDataStore
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Disable Cortana Contact Harvesting has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Hide Cortana Button has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Microsoft\PolicyManager\default\Experience\AllowCortana
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Disable Cortana through Policy Manager has been successful
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\Windows Search
2024/01/04 20:29:53 [debloat.vm] vm.common.psm1 [+] INFO : Disable Cortana through Windows Search Policy has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\InputPersonalization
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Input Personalization has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Policies\Microsoft\Windows\CloudContent
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Tailored Experiences with Diagnostic Data has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Policies\Microsoft\Windows\CloudContent
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Tailored Experiences with Diagnostic Data has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\OneDrive
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable OneDrive Files On-Demand has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Advertising ID has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Telemetry has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\DataCollection
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Telemetry Wow6432Node has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Disable Data Collection has been successful
2024/01/04 20:29:54 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable PreviewBuilds has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Enable NoGenTicket has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\SQMClient\Windows
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable SQM has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\AppCompat
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable AppCompat AIT has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Policies\Microsoft\Windows\AppCompat
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable AppCompat Inventory has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\AppV\CEIP
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable AppV CEIP has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\TabletPC
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable PreventHandwritingDataSharing has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\TextInput
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable AllowLinguisticDataCollection has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable Automatic Server Share has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Disable Automatic Workstation Share has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Search
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Hide Taskbar Search has been successful
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
2024/01/04 20:29:55 [debloat.vm] vm.common.psm1 [+] INFO : Hide Task View has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKCU:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Remove MeetNow User has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Remove MeetNow Machine has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKCU:\Software\Microsoft\Windows\CurrentVersion\Feeds
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Remove Bing Tab in Taksbar has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Edge
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Remove Bing Desktop Search Bar has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Disable Windows Update Automatic Download has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MusNotification.exe
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Disable Windows Update Automatic Restart has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] WARN : Registry key already exists: HKLM:\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Disable Microsoft Connectivity Test (msftconnecttest.com) has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: Registry::HKEY_CLASSES_ROOT\Directory\Background\shell\ctx_cmd
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Enable opening cmd from context menu - Default has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Registry key created: Registry::HKEY_CLASSES_ROOT\Directory\Background\shell\ctx_cmd\command
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Enable opening cmd from context menu - Command has been successful
2024/01/04 20:29:56 [debloat.vm] vm.common.psm1 [+] INFO : Executing commands for 'Remove OneDrive':
```

After the installation is complete, ensure that there is a connection between your Remnux box and Flare VM, as shown in the picture above.

-Begin by going to the upper left corner of the Flare VM machine, click on "Settings." Here, you'll configure the predefined "host-only adapter."



FlareVM-Windows 10 - Settings

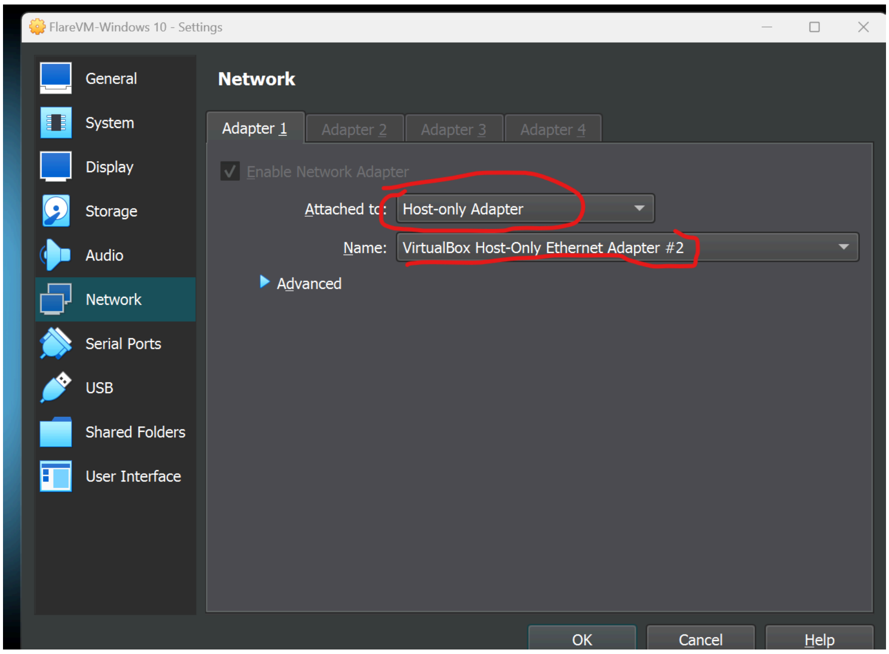
General

Name: FlareVM-Windows 10

Type: Microsoft Windows

Version: Windows 10 (64-bit)

Now, navigate to "Network" and on the right side where you see "Nat," change it to "Host-only Adapter." You can use either Adapter 2 or 3; it doesn't matter. Refer to the picture below for guidance, and once configured, click "OK."



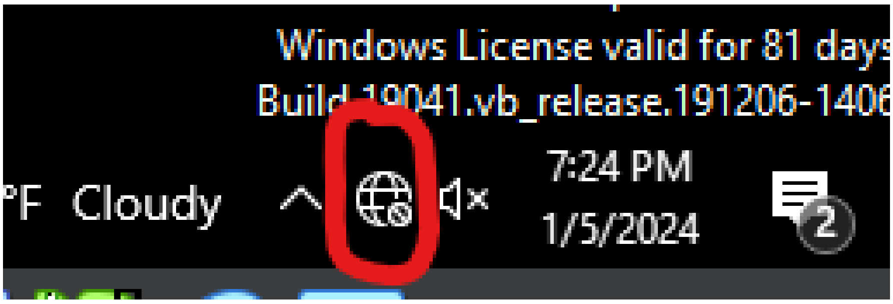
Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

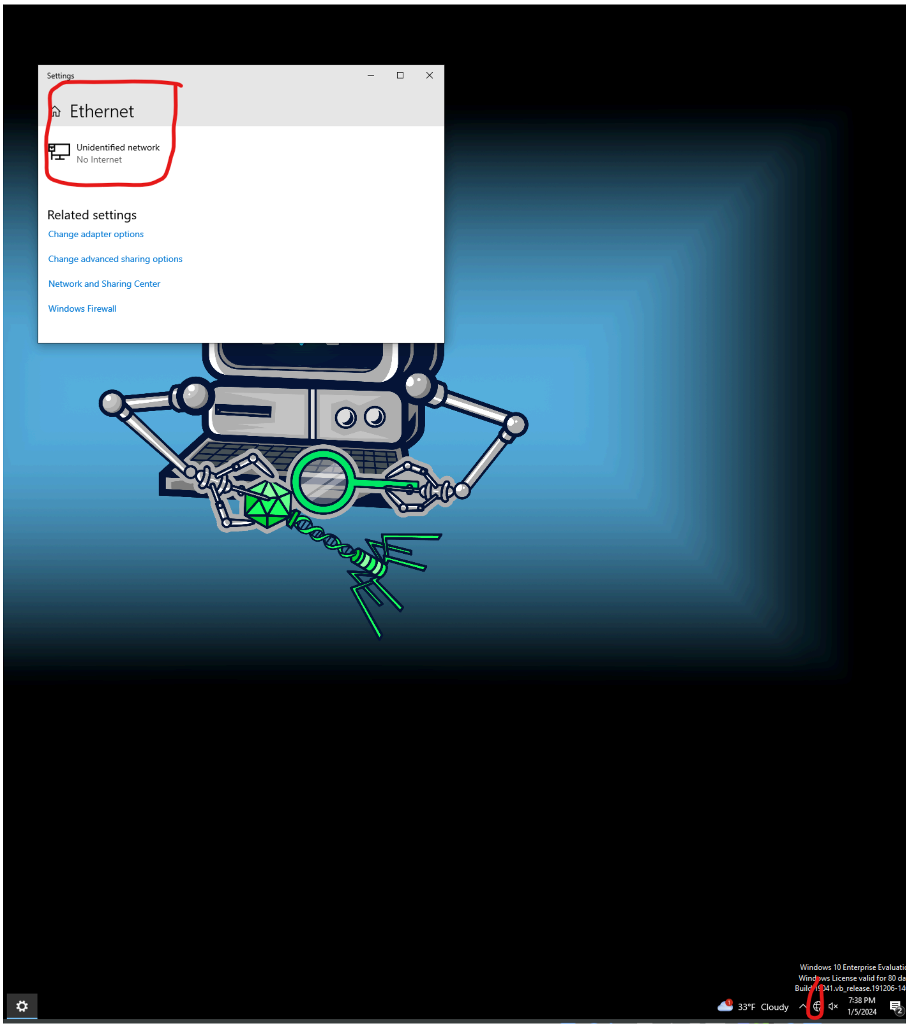
After clicking "OK," you'll notice that you no longer have an internet connection at the bottom right, which is a positive sign for the configuration



Windows License valid for 81 days
Build 19041.vb_release.191206-1406

Returning to Remnux...

After setting up the connection from Remnux, navigate to the search bar or click on the network icon to access Ethernet settings.



Settings

Ethernet

Unidentified network
No Internet

Related settings

Change adapter options

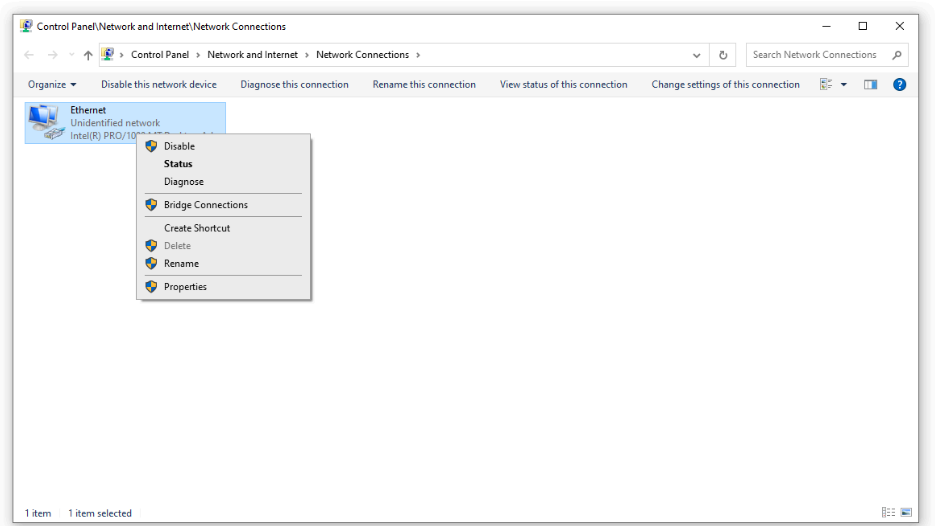
Change advanced sharing options

Network and Sharing Center

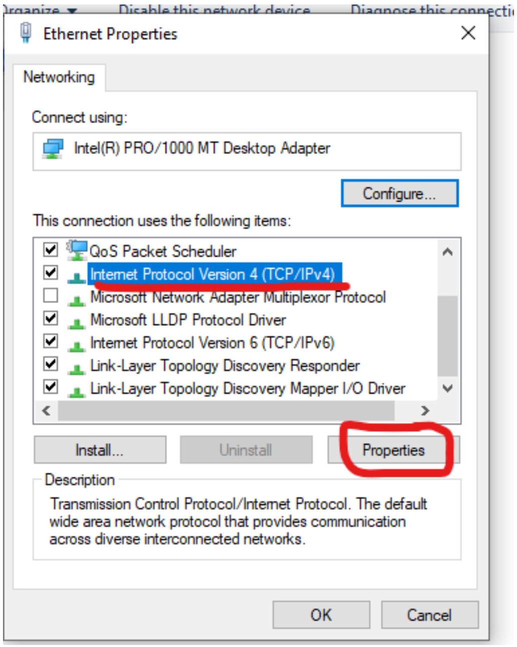
Windows Firewall

Windows 10 Enterprise Evaluati
Windows License valid for 80 da
Build 19041.vb_release.191206-14
33°F Cloudy
7:38 PM
1/5/2024

Now, click on "Change adapter options" on the right. In the pop-up window, right-click on "Ethernet," go to "Properties," and look for "Internet Protocol Version 4 (TCP/IPv4)." Click on it.


Control Panel\Network and Internet\Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet
Unidentified network
Intel(R) PRO/1000 MT Desktop Adapter
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
1 item
1 item selected

Then go to “properties”



Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

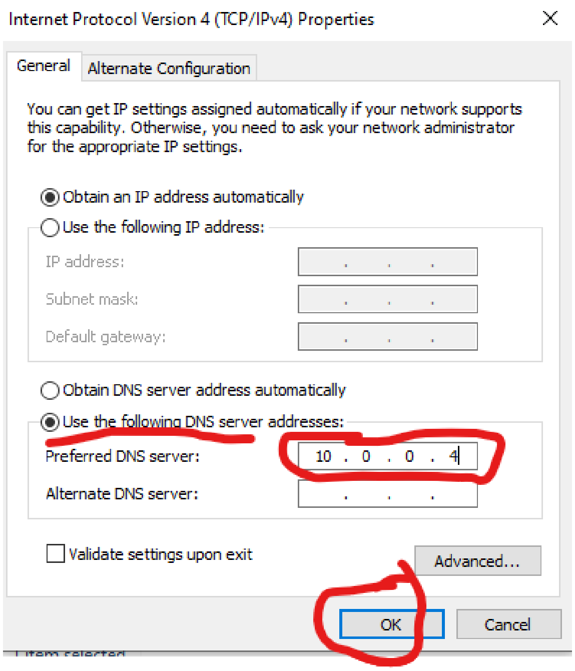
This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Finally, select "Use the following DNS server addresses" at the bottom, and you can add your "remnux" box as the DNS.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 4

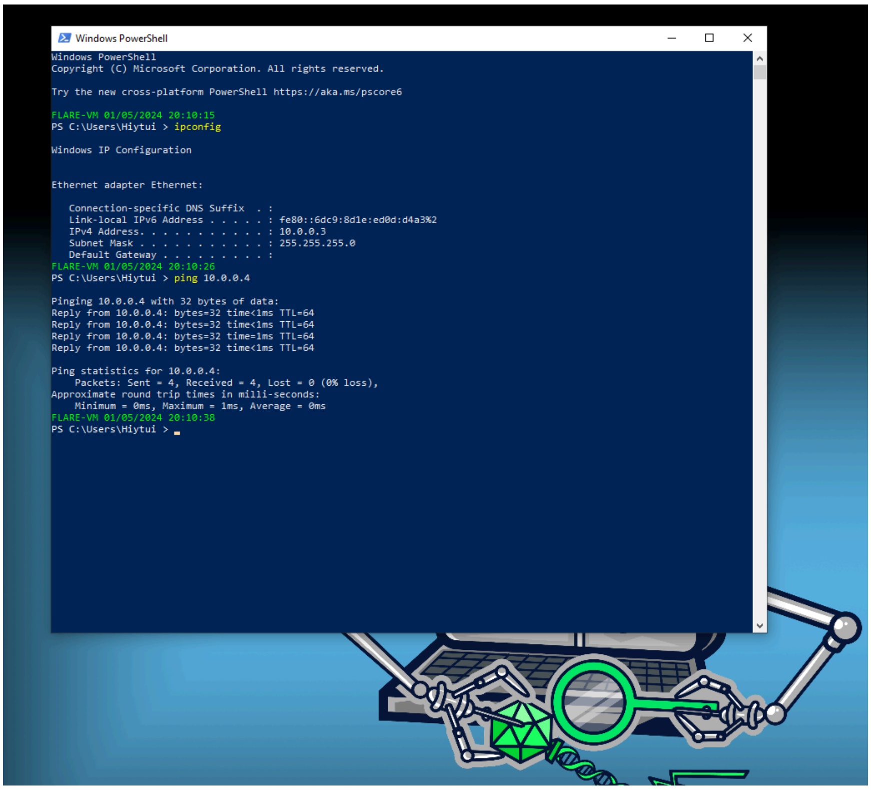
Alternate DNS server: . . .

□ Validate settings upon exit

After clicking "OK," close the Ethernet Properties, exit the Control Panel, and also close the Network Settings.

—-Now, return to the Remnux box machine……..

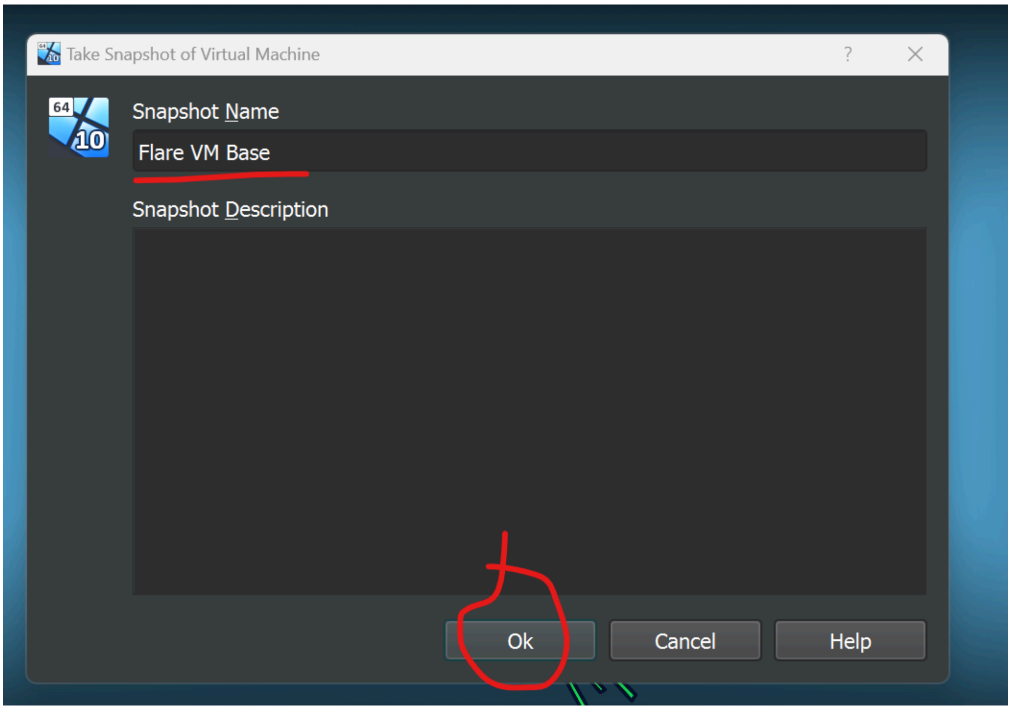
- Now, confirm the IP address of your Flare VM by running "ipconfig." Next, ping the Flare VM using the command "ping 10.0.0.4." To find PowerShell on Flare VM, click on the Windows Start icon, scroll down under "Recently added," find Windows PowerShell, and click on it. Verify communication between the virtual machines by checking for a ping reply, as shown in the picture below. This indicates successful communication between the two VMs.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

FLARE-VM 01/05/2024 20:10:15
PS C:\Users\Hiytui > ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6dc9:8d1e:ed0d:d4a3%2
   IPv4 Address. . . . . . . . . . . : 10.0.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
FLARE-VM 01/05/2024 20:10:26
PS C:\Users\Hiytui > ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64
Reply from 10.0.0.4: bytes=32 time=1ms TTL=64
Reply from 10.0.0.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
FLARE-VM 01/05/2024 20:10:38
PS C:\Users\Hiytui >
```

—Return to the Remnux box machine and follow the same steps to confirm the IP address and establish communication with the Flare VM.….

- Now, take a snapshot of the current state. This snapshot will serve as the base installation, allowing you to revert back to a clean environment after detonating malware.
- Navigate to the machine menu, select "Take Snapshot," and name it "Flare VM Base." This snapshot will be your reference point for a clean environment.



Take Snapshot of Virtual Machine

Snapshot Name: Flare VM Base

Snapshot Description