



# Creating an environment for Malware Analysis

# What is needed

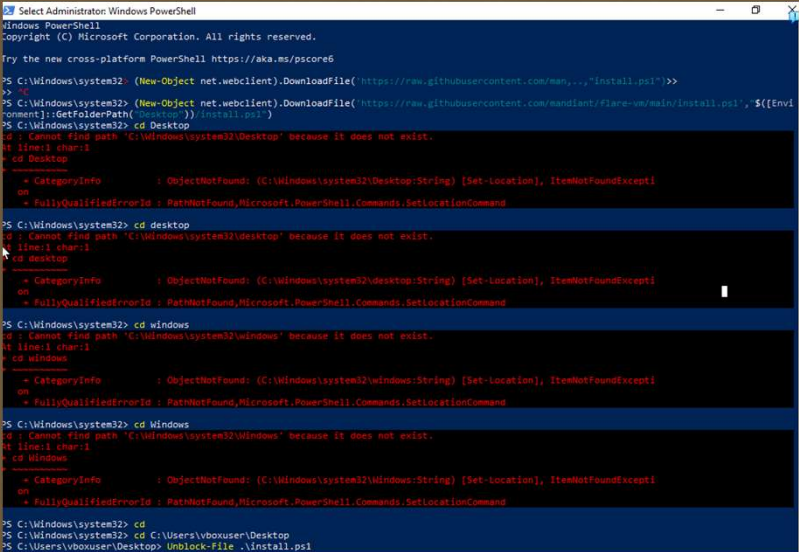
- Access to a Hypervisor- I use Virtualbox
- Windows 10 or 11 ISO
- Remnux Linux distro for the tools for analysis-This is installed on windows host
- Flare VM for the environment

# Starting with Windows Machine

- When you access your windows machine you will first turn off updates for 7 days. This will prevent it from updating during installation. Next, you will go into defender and within Virus protection turn off Virus scanning and Tamper Protection. Next you will open Powershell as Admin.

# Installing Flare VM

- Run the command (New Object net.webclient).DownloadFile('https://raw.githubusercontent.com/Mandiant/flare-vm/main/install.ps1','\${Environment}::GetFolderPath("Desktop")/install.ps1')
- Then it will pop a normal line after
- Youll navigate to your desktop directory
- Cd C:/Users/<insert your name here/Desktop>
- From here you will install the file for Flarevm



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

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

PS C:\Windows\system32> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1')>>
>>
PS C:\Windows\system32> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1', '${Environment}::GetFolderPath("Desktop")/install.ps1')
PS C:\Windows\system32> cd Desktop
cd : Cannot find path 'C:\Windows\system32\Desktop' because it does not exist.
At line:1 char:1
~ cd Desktop
~
~ CategoryInfo          : ObjectNotFound: (C:\Windows\system32\Desktop:String) [Set-Location], ItemNotFoundException
~ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd desktop
cd : Cannot find path 'C:\Windows\system32\desktop' because it does not exist.
At line:1 char:1
~ cd desktop
~
~ CategoryInfo          : ObjectNotFound: (C:\Windows\system32\desktop:String) [Set-Location], ItemNotFoundException
~ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd windows
cd : Cannot find path 'C:\Windows\system32\windows' because it does not exist.
At line:1 char:1
~ cd windows
~
~ CategoryInfo          : ObjectNotFound: (C:\Windows\system32\windows:String) [Set-Location], ItemNotFoundException
~ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd windows
cd : Cannot find path 'C:\Windows\system32\Windows' because it does not exist.
At line:1 char:1
~ cd windows
~
~ CategoryInfo          : ObjectNotFound: (C:\Windows\system32\Windows:String) [Set-Location], ItemNotFoundException
~ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd
PS C:\Windows\system32> cd C:\Users\vbouser\Desktop
PS C:\Users\vbouser\Desktop> Unblock-File .\install.ps1
```



# Installing continued

- Input Unblock-File .\install.ps1
- Next you'll input Set-ExecutionPolicy Unrestricted
- Since this is a lab environment you would input A
- Then we will run .\install.ps1
- Let it run through its script
- Any warnings use Y for the lab environment
- It will have you populate your password for the machine

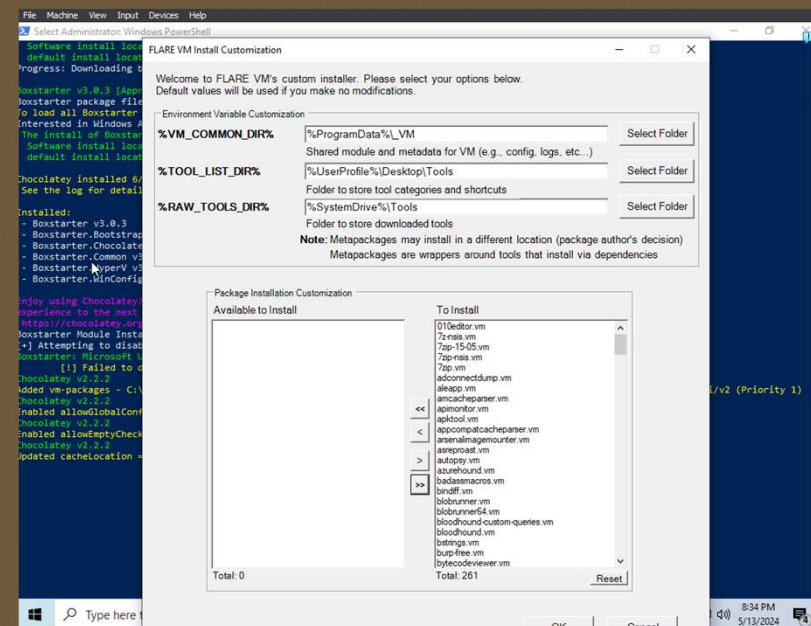
```
PS C:\Windows\system32> cd
PS C:\Windows\system32> cd C:\Users\vboxuser\Desktop
PS C:\Users\vboxuser\Desktop> Unblock-File .\install.ps1
PS C:\Users\vboxuser\Desktop> Set-ExecutionPolicy Unrestricted

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"): a
PS C:\Users\vboxuser\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"): A
PS C:\Users\vboxuser\Desktop> .\install.ps1
[*] Installing with PowerShell version 5.1.19041.3803
[*] 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 'vboxuser' 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...
[*] Windows Defender service is disabled
[*] Hint: https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
[*] Hint: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
[*] Hint: https://github.com/jeremybeamer/tools/blob/master/disable-defender.ps1
[*] You are welcome to continue, but may experience errors downloading or installing packages
[*] Do you still wish to proceed? (Y/N): Y
[*] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): Y
[*] Getting user credentials ...
```

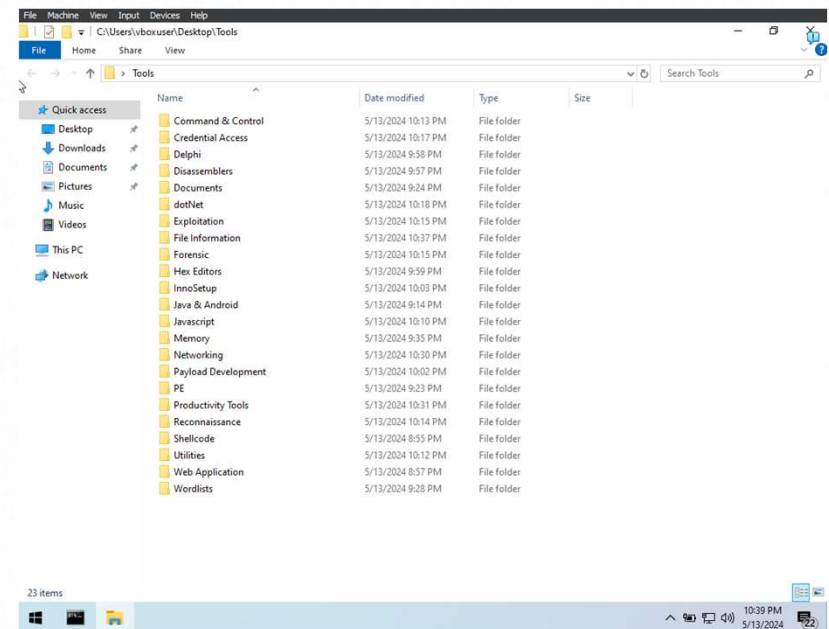
# Flare VM install console

- With this tool you can now choose to install certain tools from the list, or a few or all.



# Once you finish the install

- The install takes a long time, and will restart a lot. Once it finishes you will have a host of new icons on your desktop. Tools is where your tools you selected to download will be located. Before you run anything in it, make sure you only run your network locally within the VM.



# Installing Remnux

- You can access remnux from [remnux.org](https://remnux.org)
- If you're using virtual box you will select the virtual box ova
- If you're running a different HyperVisor you will select General OVA
- Once you download the file, run the checksum hash on it as it says in step 2

## Step 1: Download the Virtual Appliance File

The REMnux virtual appliance approximately 5 GB. It comes as an industry-standard OVA file, which you can import into your virtualization software. It's based on Ubuntu 20.04 (Focal).

Decide which OVA file to download. Unless you're using Oracle VM VirtualBox, get the general OVA file. If you're using VirtualBox, get the VirtualBox version. Download your preferred OVA file:

General OVA    VirtualBox OVA

This VirtualBox OVA file is specifically for VirtualBox. Get the general version from the other tab if you're using other hypervisors:

Download the VirtualBox OVA file from [Box](#) (primary) or [SourceForge](#) (mirror)

✓ Some browsers (e.g., Brave) change the extension of the OVA file after downloading it, possibly giving it the incorrect .ovf extension. If that happens, rename the file so it has the .ova extension before proceeding.

## Step 2: Confirm the Hash the OVA File

Validate the SHA-256 hash of the downloaded file using a tool such as `sha256sum` or `shasum` to make sure it matches this expected value:

General OVA Hash    VirtualBox OVA Hash

The general OVA file:

76a12cc8ccf482e83f84b42ebfd9019ae47cf27915d0c2d686a9a407f8ee51ab



# After installing Remnux, you're free to play!

- After installing Remnux, you are free to run static or dynamic analysis. Make sure you do it in a safe environment and run network locally in the VM.

