**Setting Up Your Malware Analysis Lab with VMware and FLARE-VM**

This guide will walk you through the process of setting up a secure environment for malware analysis using VMware Workstation and the FLARE-VM toolset. We'll start by installing VMware Workstation on your Windows 11 machine, then create and configure a Windows 10 virtual machine, and finally install and configure FLARE-VM within that virtual machine.

**Prerequisites:**

* A physical machine running Windows 11 with administrator privileges.
* Sufficient hard drive space (at least 50GB recommended) and RAM (at least 8GB recommended, 16GB or more is ideal for running virtual machines).
* A stable internet connection.
* A VMware Workstation license or the free VMware Workstation Player for non-commercial use.
* A Windows 10 ISO file.

**Step 1: Installing VMware Workstation**

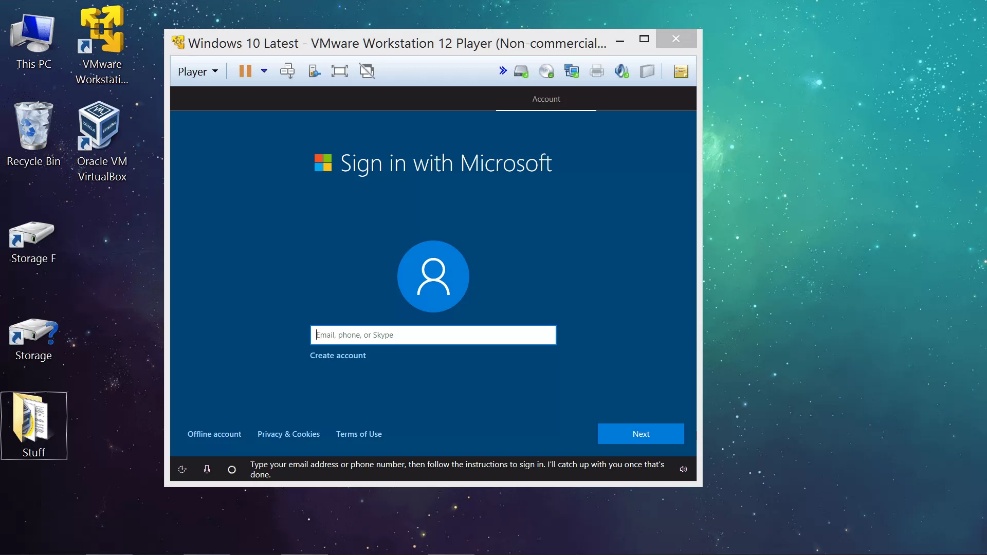
VMware Workstation allows you to run virtual machines on your physical computer.

1. **Download VMware Workstation:**
   * Open your web browser and navigate to the VMware website.
   * Locate the download section for VMware Workstation Pro or VMware Workstation Player, depending on your license or needs.
   * Download the appropriate installer for Windows.
2. **Run the Installer:**
   * Once the download is complete, locate the installer file (usually a .exe file) in your Downloads folder.
   * Double-click the installer to begin the installation process.
3. **Follow the Installation Wizard:**
   * You will be presented with a setup wizard. Click "Next" to continue.
   * **License Agreement:** Read the End-User License Agreement (EULA) carefully. If you agree to the terms, check the "I accept the terms in the License Agreement" box and click "Next."
   * **Custom Setup:** On the "Custom Setup" screen, you can choose the installation location and whether to install enhanced virtual keyboard driver and add VMware to the system PATH. For most users, the default settings are sufficient. Click "Next."
   * **Check for Product Updates:** You can choose whether to check for product updates on startup. Select your preference and click "Next."
   * **Join the VMware Customer Experience Improvement Program:** Decide if you want to participate in the program. Select your preference and click "Next."
   * **Shortcuts:** Choose where you want to place shortcuts for VMware Workstation. The default locations are usually fine. Click "Next."
   * **Begin Installation:** Click "Install" to start the installation process.
   * **Completion:** Once the installation is complete, click "Finish." You may be prompted to restart your computer. It's generally a good idea to do so.

**Step 2: Creating and configuring a Windows 10 Virtual Machine**

Now, we'll create a virtual machine that will host your FLARE-VM installation.

1. **Launch VMware Workstation:**
   * Open VMware Workstation from the Start Menu or the desktop shortcut you created.
2. **Create a New Virtual Machine:**
   * In the VMware Workstation window, click on "Create a New Virtual Machine." This will open the New Virtual Machine Wizard.
3. **Configuration Type:**
   * Select "Typical (recommended)" and click "Next."
4. **Guest Operating System Installation:**
   * Choose "Installer disc image file (ISO)."
   * Click "Browse..." and locate the Windows 10 ISO file you have downloaded.
   * VMware may detect the operating system. Click "Next."
5. **Windows Installation Information:**
   * Enter the product key if you have one. You can also choose to skip this and activate Windows later.
   * Enter the desired "Full name," "User name," and "Password" for the administrator account in the virtual machine.
   * Click "Next."
6. **Virtual Machine Name and Location:**
   * Enter a descriptive name for your virtual machine (e.g., "FLARE-VM Lab").
   * Choose a location on your hard drive where you want to store the virtual machine files. Ensure you have enough free space. Click "Next."
7. **Disk Size:**
   * Specify the maximum disk size for your virtual machine. A minimum of 40GB is recommended, but 60GB or more is better for installing tools and storing malware samples.
   * Select "Store virtual disk as a single file" for better performance. Click "Next."
8. **Hardware Customization (Optional but Recommended):**
   * Before clicking "Finish," click on the "Customize Hardware..." button.
   * **Memory (RAM):** Allocate an appropriate amount of RAM to the virtual machine. For decent performance, allocate at least 4GB (4096 MB). If your host machine has more RAM, you can allocate 8GB or more.
   * **Processors:** Assign the number of processor cores you want to dedicate to the virtual machine. Assigning 2 or more cores is recommended for better performance.
   * **Network Adapter:** Ensure the network adapter is set to "NAT" (Network Address Translation) by default. This will allow the virtual machine to access the internet through your host machine's connection. For malware analysis, you might later want to change this to a Host-Only network to isolate the VM.
   * Click "Close" after making your adjustments.
9. **Finish Creation:**
   * Click "Finish" on the New Virtual Machine Wizard. VMware Workstation will now create the virtual machine and automatically start the Windows 10 installation process.
10. **Install Windows 10:**
    * Follow the on-screen instructions to complete the Windows 10 installation within the virtual machine. This process is like installing Windows on a physical machine.



**Requirements: FLARE VM**

**FLARE-VM should ONLY be installed on a virtual machine**. The VM should satisfy the following requirements:

* Windows >= 10
* PowerShell >= 5
* Disk capacity of at least 60 GB and memory of at least 2GB
* Usernames without spaces or other special characters
* Internet connection
* Tamper Protection and any Anti-Malware solution (e.g., Windows Defender) Windows Defender disabled, preferably via Group Policy
* Windows Updates Disabled

**Step 1: Pre-installation**

Once Windows 10 is installed and running in your virtual machine, you can proceed with installing FLARE-VM.

1. **Start the Windows 10 Virtual Machine:**
   * If the virtual machine is not already running, select it in the VMware Workstation library and click "Power on this virtual machine."
2. **Log in to Windows 10:**
   * Enter the password you set during the Windows 10 installation.
3. **Prepare the Virtual Machine:**
   * **Take a Snapshot:** Before making any significant changes, it's crucial to take a snapshot of your virtual machine. This allows you to revert to a clean state if something goes wrong during the FLARE-VM installation.
     + In the VMware Workstation menu, go to "VM" > "Snapshot" > "Take Snapshot..."
     + Enter a descriptive name for the snapshot (e.g., "Clean Windows 10") and click "Take Snapshot."
   * **Install VMware Tools:** VMware Tools enhances the performance and integration of the virtual machine with the host system.
     + In the VMware Workstation menu, go to "VM" > "Install VMware Tools."
     + This will mount a virtual CD-ROM in the virtual machine. Open File Explorer in the VM and run the VMware Tools installer. Follow the on-screen instructions to complete the installation and restart the virtual machine when prompted.
   * **Disable Windows Defender:** FLARE-VM installation can be disrupted by Windows Defender. It is recommended to disable it.
     + Open "Windows Security" from the Start Menu.
     + Go to "Virus & threat protection" and click on "Manage settings" under "Virus & threat protection settings."
     + Turn off "Real-time protection."
     + Turn off "Cloud-delivered protection."
     + Turn off "Automatic sample submission."
     + Scroll down to "Exclusions" and click on "Add an exclusion." Add an exclusion for the entire C: drive.
   * Disable Windows Updates
     + Open Settings.
     + Click on Update & Security.
     + Click on Windows Update.
     + Click the "Pause updates for 7 days" option.
   * **Enable Internet Access:** Ensure your virtual machine has internet access. If you used the default "NAT" setting for the network adapter, it should have internet connectivity.
4. **FLARE-VM installation:**
   * Open a web browser (e.g., Microsoft Edge) within the Windows 10 virtual machine.
   * Navigate to the FLARE-VM GitHub repository: <https://github.com/mandiant/flare-vm>
   * Download the installation script installer.ps1 to your Desktop:
     + (New-Object net.webclient).DownloadFile(‘https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps’,”$([Environment]:: GetFolderPath(“Desktop”))\.install.ps1”)
   * Unblock the installation script:
     + Unblock-File .\install.ps1
     + **Enable script execution:** Set-ExecutionPolicy Unrestricted -Scope CurrentUser
     + If you receive an error saying the execution policy is overridden by a policy defined at a more specific scope, you may need to pass a scope in via Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force. To view execution policies for all scopes, execute Get-ExecutionPolicy -List
5. Finally, execute the installer script as follows: .\install.ps1
   * + To pass your password as an argument: .\install.ps1 -password <password>
     + To use the CLI-only mode with minimal user interaction: .\install.ps1 -password <password> -noWait -noGui
     + To use the CLI-only mode with minimal user interaction and a custom config file: .\install.ps1 -customConfig <config.xml> -password <password> -noWait -noGui
6. After installation it is recommended to switch to host-only networking mode and take a VM snapshot

**Advanced Settings**

**Installer Parameters:** Below are the CLI parameter descriptions.

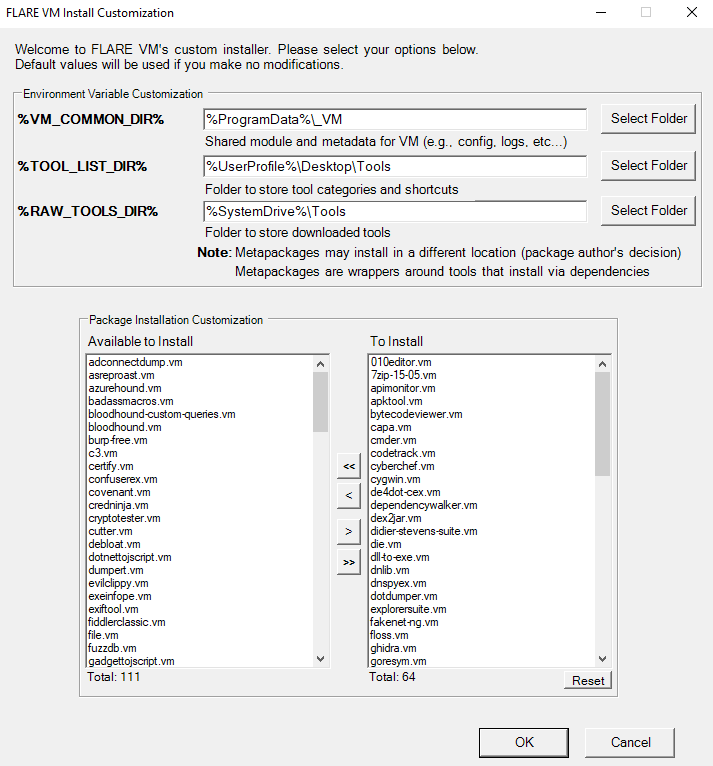
|  |  |
| --- | --- |
| -password <String> | Current user password to allow reboot resiliency via Boxstarter. The script prompts for the password if not provided. |
| -noPassword [<SwitchParameter>] | Switch parameter indicating a password is not needed for reboots |
| -customConfig <String> | Path to a configuration XML file. May be a file path or URL. |
| -customLayout <String> | Path to a taskbar layout XML file. May be a file path or URL. |
| -noWait [<SwitchParameter>] | Switch parameter to skip installation message before installation begins. |
| -noGui [<SwitchParameter>] | Switch parameter to skip customization GUI. |
| -noReboots [<SwitchParameter>] | Switch parameter to prevent reboots (not recommended). |
| -noChecks [<SwitchParameter>] | Switch parameter to skip validation checks (not recommended). |

Get full usage information by running Get-Help .\install.ps1 -Detailed .

**Installer GUI**

The Installer GUI is displayed after executing the validation checks and installing Boxstarter and Chocolatey (if they are not installed already). Using the installer GUI you may customize:

* + Package selection
  + Environment



**Configuration**

The installer will download [config.xml](https://raw.githubusercontent.com/mandiant/flare-vm/main/config.xml) from the FLARE-VM repository. This file contains the default configuration, including the list of packages to install and the environment variable paths. You may use your own configuration by specifying the CLI-argument -customConfig and providing either a local file path or URL to your config.xml file. For example:

.\install.ps1 -customConfig https://raw.githubusercontent.com/mandiant/flare-vm/main/config.xml

**Taskbar Layout**

The installer will use [CustomStartLayout.xml](https://raw.githubusercontent.com/mandiant/flare-vm/main/CustomStartLayout.xml) from the FLARE-VM repository. This file contains the default taskbar layout. You may use your own configuration by specifying the CLI-argument -customLayout and providing a local file path or URL to your CustomStartLayout.xml file. For example:

.\install.ps1 -customLayout https://raw.githubusercontent.com/mandiant/flare-vm/main/CustomStartLayout.xml

**Things to consider:**

Items in the .xml that are not installed will not display in the taskbar (no broken links will be pinned)

Only applications (.exe files) or shortcuts to applications can be pinned.

If you like to pin something that isn’t an application, consider create a shortcut that points to cmd.exe or powershell with arguments supplied that will perform that actions you would like.

If you would like to make something run with admin rights, consider making a shortcut using VM-Install-Shortcut with the flag -runAsAdmin and pinning the shortcut.

**Post installation Steps**

You can include any post installation steps you like in the configuration inside the tags apps, services, path-items, registry-items, and custom-items.

For example:

To show known file extensions:

<registry-items>

<registry-item name="Show known file extensions" path="HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" value="HideFileExt" type="DWord" data="0"/>

</registry-items>

For more examples, check the default configuration file: config.xml.

**Troubleshooting**

If your installation fails, please attempt to identify the reason for the installation error by reading through the log files listed below on your system:

* + %VM\_COMMON\_DIR%\log.txt
  + %PROGRAMDATA%\chocolatey\logs\chocolatey.log
  + %LOCALAPPDATA%Boxstarter\boxstarter.log

Ensure you are running the latest version of the FLARE-VM installer and that your VM satisfies the requirements.

**Package Error**

Packages fail to install from time to time -- this is normal. The most common reasons are outlined below:

1. Failure or timeout from Chocolatey or MyGet to download a .nupkg file
2. Failure or timeout due to remote host when downloading a tool
3. Intrusion Detection System (IDS) or AV product (e.g., Windows Defender) prevents a tool download or removes the tool from the system
4. Host specific issue, for example when using an untested version
5. Tool fails to build due to dependencies
6. Old tool URL (e.g., HTTP STATUS 404)
7. Tool's SHA256 hash has changed from what is hardcoded in the package installation script

Reasons **1-4** are difficult to fix since we do not control them. If an issue related to reasons **1-4** is filed, it is unlikely we will be able to assist.

We can help with reasons **5-7** and welcome the community to contribute fixes as well! Please [report the bug in VM-Packages](https://github.com/mandiant/VM-Packages/issues/new?labels=%3Abug%3A+bug&template=bug.yml) providing all the information requested.