Intro to Malware Analysis

How to install FlareVM using Powershell on Windows 10

Overview

The FlareVM malware analysis environment is a collection of software that is installed on top of a working Windows 7, 8, 8.1, or 10 machine. In this course, we recommend using a Windows 10 (64 bit edition) Virtual Machine provided by the Microsoft website, as shown in our videos. To install FlareVM, we will use an installation script in the Boxstarter framework.

Steps

1. Open the Powershell interface using the Run As Administrator command.
2. At the prompt, type **Set-ExecutionPolicy Unrestricted** and press ENTER.
3. At the prompt, type **iex ((New-Object System.Net.WebClient).DownloadString('http://boxstarter.org/bootstrapper.ps1')); get-boxstarter -Force** (all on one line) and press enter. This will take about 1-2 minutes on most systems.
4. At the prompt, type **Import-Module C:\ProgramData\Boxstarter\Boxstarter.Chocolatey\Boxstarter.Chocolatey.psm1** (all on one line) and press ENTER. This will take about 1-2 minutes on most systems.
5. At the prompt, type **Install-BoxstarterPackage -PackageName https://raw.githubusercontent.com/fireeye/flare-vm/master/flarevm_malware.ps1** (all on one line) and press ENTER. This will take about 20-30 minutes, will cause your system to reboot several times, and you will have to enter the password each time it reboots (**Passw0rd1**).
6. Once this is all completed, you will have a brand new FlareVM desktop ready for use.