Lab Setup

Creating a Virtual Machine for Malware Analysis

Requirements

- VirtualBox (free)
  - https://www.virtualbox.org/wiki/Downloads
- VMWare
  - 1. VMWare Workstation Pro (30 days trial)
  - 2. VMWare Workstation Player (free) - can't create snapshots

- Install Windows 7 Ultimate 64-bit
- Install Guest Addition Tools (for full screen and shared folder capability)
- Create a Shared Folder (to exchange files between guest and host)
- Create a base snapshot of VM after configuring it

Configuring the VM

- Disable Windows Update
- Disable windows defender (services.msc)
- Disable hide extensions
- Show hidden files and folders
- Disable Adress Space Layout randomization ASLR (To prevent randomization of memory address)
    - Step 1: Open regedit
    - Step 2: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
    - Step 3: Add a new Dword key: MoveImages
    - Step 4: Add a corresponding value: 0
- Disable windows firewall
- Create a snapshot

Install flare VM

- Start your machine
- Install Google Chrome
- Visit https://github.com/mandiant/flare-vm
- Download the Zip file
- Update Windows Powershell to V5.1
- Check your version using get-host | select-object version
- Run the following command in your power shell:
  - Set-ExecutionPolicy unrestricted
  - .\install.ps1
- It could take 4 hours