Lab Setup

Creating Virtual Machines for Malware Analysis

Requirements

- Use VirtualBox or VMWare to create Virtual Machines (VM)
- VirtualBox is free

  https://www.virtualbox.org/wiki/Downloads

- VMWare has two versions:

  1. VMWare Workstation Pro (30 day trial)
  2. VMWare Workstation Player (free) – but cannot create snapshots

- Install Windows 7 SP1 64-bit (because Ghidra needs 64-bit)

  - If you don't have it, just google for an iso image from Internet, or, buy from ebay.
- Although most malware is 32-bit, they can also run on 64-bit windows
- 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 the VM after configuring it

Configuring the VM

- Disable Windows Update
- Disable Windows Defender
- Disable Hide Extensions
- Show Hidden Files and Folders
- Disable ASLR
- Disable Windows Firewall
- Create a Snapshot