Malware analysis

**01 – creating a safe lab environment**

# Creating a safe lab environment

**Lab Description:** The ability to create and customize a safe lab environment is crucial for analyzing malware. The goal of this lab is to demonstrate the ability to create configurations that provide virtual machine isolation and demonstrate the ability to apply these concepts to your own virtual lab environment.

**Lab Environment:** For this lab, you will be creating your own lab environment. You will need the following to complete this lab:

* A host system capable of virtualization – this typically requires Intel’s VT-x support enabled through the BIOS or UEFI firmware
* It is recommended to use a host system that has at least 40 GB of hard drive space, utilizes a solid-state drive, has an i5 or new processor and can allocate at least 512 MB of RAM for a single virtual machine.
* Access to any one of the following virtualization software providers:
  + VirtualBox – Linux, Mac OS X, Windows
  + VMWare Workstation Player – Linux, Windows
* An operating system to install. This step can vary based on student access to operating system software. If possible, install a Windows-based OS such as Windows 7. If unable to obtain a Windows license, install a Linux distribution such as Ubuntu Desktop from Ubuntu.org.

The end result of this lab is to create a single virtual machine that utilizes host-only networking.

**Lab Files that are Needed:** No additional files are needed for this lab.

**STEP 1 – Install Virtualization Software**

Using the virtualization software listed above, install the software in your host OS. Provide a screenshot clearing showing the virtualization software you used and its successful installation.

**STEP 2 – Create Your Virtual Machine**

Using the guest OS you selected, install the guest OS in your virtual machine. If uncertain about any configuration option during setup, select the default. Give your VM the following resources:

CPU – Single core  
 Memory – 512 MB  
 Hard-drive – 20 GB Linux, 40 GB Windows

Provide a screenshot showing this configuration from within the guest OS. For example, in Windows you could use the properties page from My Computer.

**STEP 3 – Configure Networking**

For the final step, configure your VM to use host-only networking. This is accomplished through the networking section of the virtual machines configuration. This is NOT configured inside the guest OS. Provide screenshots of the following:

* The configuration setting through your virtualization software
* Open up a terminal or command window and try to ping a publicly accessible system, such as google.com. The ping should fail using host-only networking as the guest OS should NOT have a route to the internet
* The output from running the *ipconfig/ifconfig* utility in the guest OS from a command window or terminal. Clearly show the IP assigned to the guest OS

## What to submit

Submit a Microsoft Word document or PDF that includes answers to the questions posed along with screenshots demonstrating the installation of the virtual machine.