Lab 0: Lab Setup Instructions

Objectives

- Configure the SEC660 Kali Linux virtual machine for the lab environment
- Configure the SEC660 Windows virtual machine for the lab environment

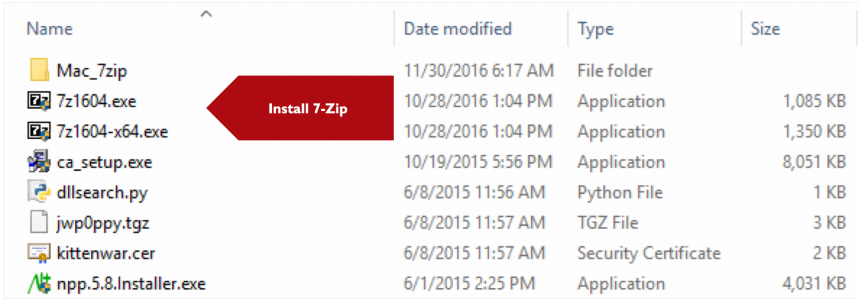
This lab is for students that download the USB image prior to class. Additional VMs used after 660.1 are covered in the course material itself.

Lab – Step-by-Step Instructions

Virtual Machine Configuration

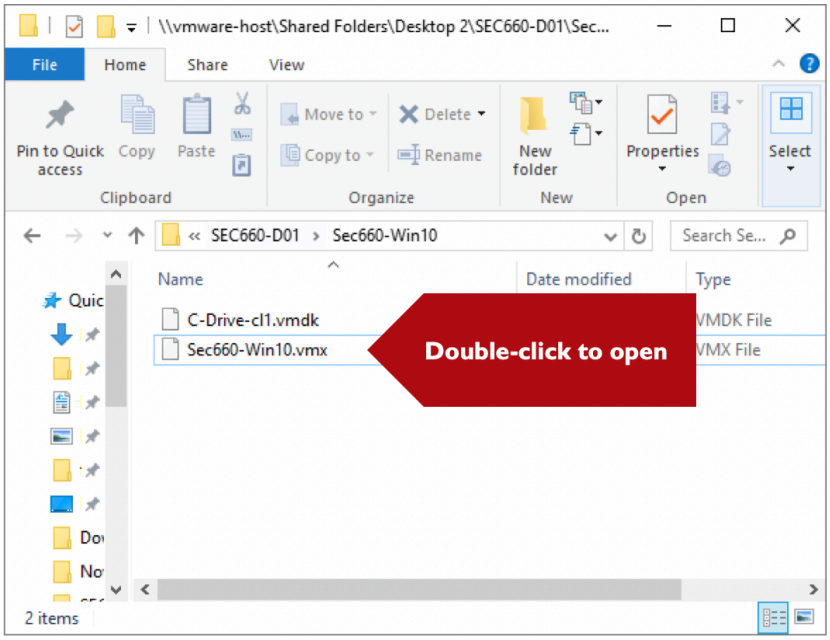
The Kali Linux Virtual Machine (VM) and the Windows VM will be used during this class; getting them networked is important.

1. Start by installing a 7-zip utility if you do not already have one available on your host. Several 7-zip utilities are on the course media, but any reliable 7-zip utility will work.

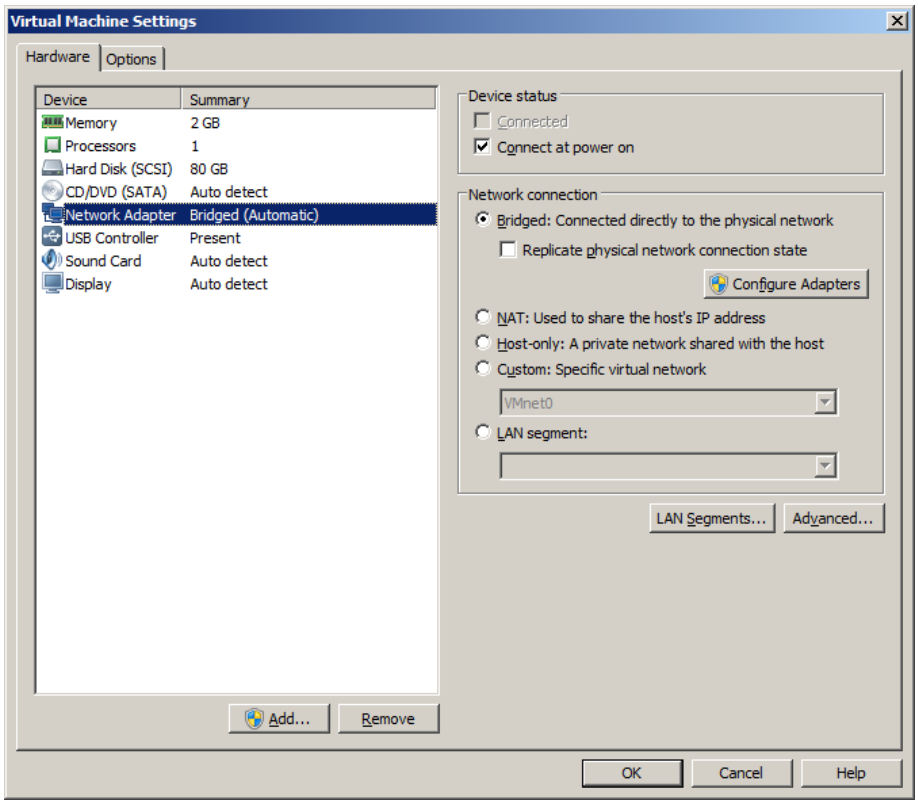


2. Next, uncompress the Kali Linux VM and the Windows VM from the USB onto your hard drive. For most situations, it is faster to copy the archives to your disk before uncompressing them. If you have limited drive capacity, extract from USB to your system disk, but be prepared for a long process.

3. After the files are unzipped, run VMware, select “Open a Virtual Machine,” and choose the folder where you extracted the course Kali VM. Then do the same thing for the Windows VM.



4. Ensure both virtual machines are bridged to your proper network interface (for in-classroom SANS training, that should be your ETHERNET adapter to physical LAN). By default, VMware bridges to an automatically selected adapter, which may temporarily work, but it is best to ensure it selects ETHERNET every time.



5. If you are bridging to a USB adapter, the adapter must be plugged into before configuring the vmnet0 to bridge to LAN (vmnetcfg.exe). If selecting your ETHERNET adapter is not possible, reboot your host with the USB adapter inserted before trying again.

The precise configuration depends on the version of VMware you are using. This workbook includes details for configuring VMware Workstation and VMware Fusion for Mac. Use the appropriate version of VMware and follow the directions for configuring bridged networking. Make sure you do this for both Kali and Windows VMs.

VMware Workstation Bridged Networking Configuration

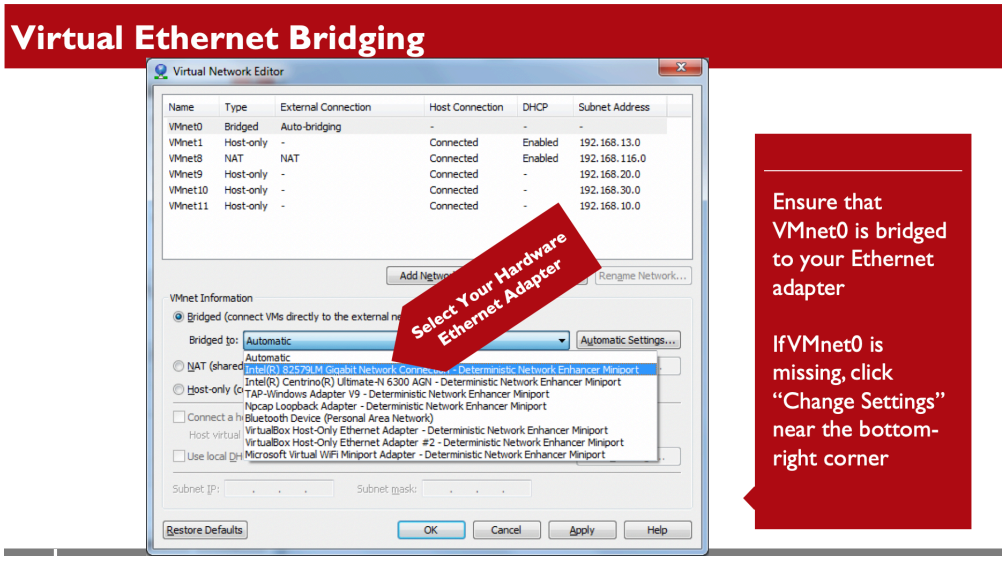
If you are using VMware Workstation for in-classroom SANS training, please follow these steps.

With the VMs booted up, at the top of the VMware screen, select Edit→Virtual Network Editor.

Near the bottom of the screen, click on the "Change Settings" button. A UAC dialog box may prompt you to accept the change. Please click "Yes" to do so.

VMnet0 interface is highlighted at the top of the screen.

Near the center of the screen, ensure that the radio button is set for "Bridged," and click on the drop-down menu where it says "Automatic" and change it to choose your ETHERNET interface. Different computers will have different names for each interface, so select the one that most likely matches your ETHERNET(LAN) interface.



At the bottom of the screen, click on "Apply" and then on "OK" to close the configuration screen.

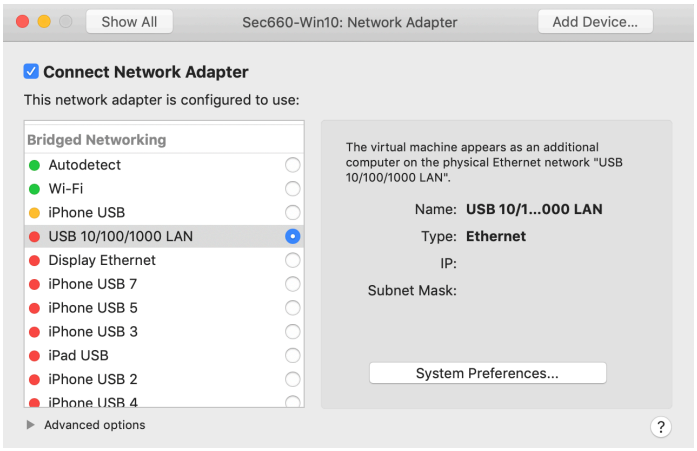
VMware Fusion Bridged Networking Configuration

If you are using VMware Fusion for Mac, to bridge to your ETHERNET interface for in-classroom SANS training, please follow these steps.

With the VM booted up, go to the Mac menu bar within Fusion and select Virtual Machine→Network Adapter→Network Adapter Settings….

Confirm that “Connect Network Adapter” is checked.

Near the middle-left part of your screen, in the section under “Bridged Networking,” click the radio button corresponding to your ETHERNET adapter. Note that in this example, the adapter is not connected, so has a red light next to it.



Once you’ve selected the radio button associated with your network adapter, you may be prompted for a password. Submit the password, click OK, and close the Network Adapter Window.

Special Note for Remote Students (SANS OnDemand, vLive, or Simulcast Students)

OLT (Online Training) students can access **My Labs** by signing in to sans.org and viewing the Account Dashboard screen. Under **My Online Training,** select **My Labs** and follow the on-screen instructions.

- You’ll need to set up your Kali Linux virtual machine and Windows virtual machine so that they both can access the internet. Both machines must be able to reach an internet destination such as **www.sans.org**.
- In VMware, please use bridged networking, and configure your machine(s) with an IP addresses that matches your environment. For the purposes of this course, it's normally simplest to use DHCP.
- Download the OpenVPN certificates from connect.labs.sans.org. Your OpenVPN key (.ovpn file) will have a filename that is unique to your SANS account.
- In Windows, put your certificates in the “C:\Program Files\OpenVPN\config” directory and start OpenVPN with **Administrator** privileges.
    - Establish an OpenVPN connection from Windows by right-clicking the OpenVPN icon in your tool tray (bottom right) and selecting **Connect**.
- In Kali Linux, place your downloaded certificates in the /etc/openvpn directory.
    - Establish the VPN connection in Kali Linux by running:
      `# openvpn --config /etc/openvpn/SEC660-*.ovpn`
- When both Windows and Kali Linux can ping 10.0.0.1, they are configured properly for the lab exercises.

Note: For all online networked labs, please use the IP address assigned to the OpenVPN interface by the DHCP server (10.0.0.X) across the VPN in the virtual lab. This IP address is viewable via the OpenVPN tool tray client in Windows and as the tap0 network interface displayed by the **ifconfig tap0** command in Kali Linux.

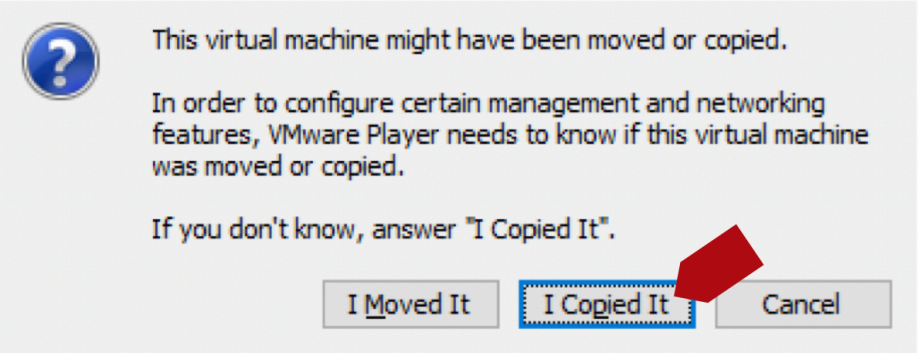
IMPORTANT NOTE: For all labs that reference eth0, you will replace it with the tap0 network interface on the command line, often using the **-i** option as follows:

```
# tcpdump -i tap0 -nv
```

Boot BOTH VMs

6. Boot your Kali Linux and Windows 10 guest systems.

   If VMware prompts you about whether you "moved" or "copied" this virtual machine, select "I copied it." If it doesn't prompt you, that's OK. This is important to reset unique ID (which triggers things like unique MAC Addresses).



7. On Kali, log in to the guest machine using the following credentials:

   Username = root

   Password = toor

8. Change root's password to a value you'll remember. We'll be connected to a network with other students in this course, and you do not want them to know the password for your Linux image.

   ```
   # passwd
   ```

   Enter your chosen password twice to set it.

9. On Windows use the VMware Guest menu to send CTRL-ALT-DEL to the guest and select "Change password". Change **student**'s password to something you will remember, and consider adding the password to any password dictionary you use in the course.

10. Gracefully shut down both VMs and make a snapshot of each. When powered off, the snapshots take negligible storage space.

Conclusion

In this lab setup, you have extracted and configured the Kali Linux Virtual Machine (VM) and Windows VM images for the SEC660 course. Both VMs have been pre-configured to suit this course.