Lab 0: Lab Setup Instructions

Objectives

- Extract SEC760 VMs for the local environment
- Connect Networking to lab environment

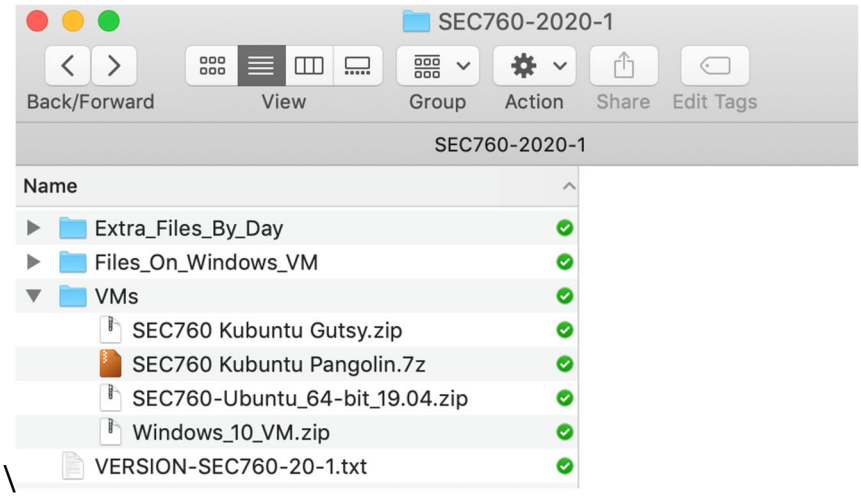
This lab is for students that download the course media prior to class. Most exericses use Virtual Machines locally on Student supplied equipment. For specific exercises, additional VMs will be provided remotely.

Lab – Step-by-Step Instructions

Virtual Machine Configuration

Several Linux Virtual Machines (VMs) and a Windows VM will be used during this class; getting them networked correctly is important.

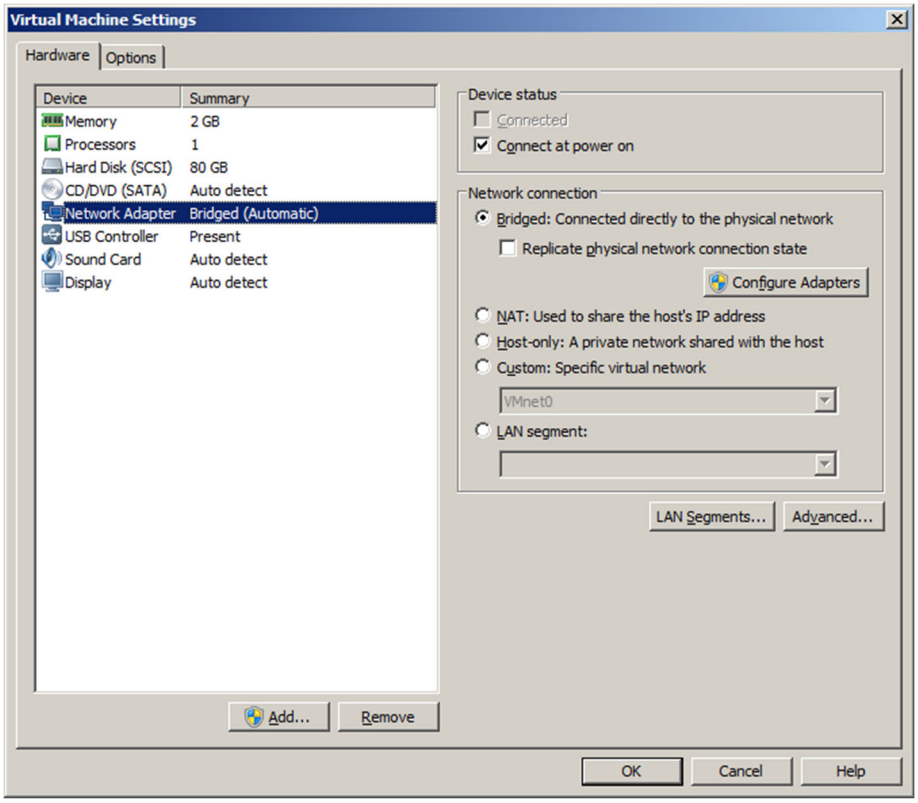
1. VMs are compressed in either ZIP or 7-ZIP formats. If needed, install a 7-zip utility on your host.



2. Next, uncompress everything from the "VMs" directory onto your local drive. For most situations, it is faster to copy the archives to your disk before uncompressing them

3. After the files are uncompressed, run VMware, select "Open a Virtual Machine," and open each VM.

4. Ensure ALL 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 every VM.

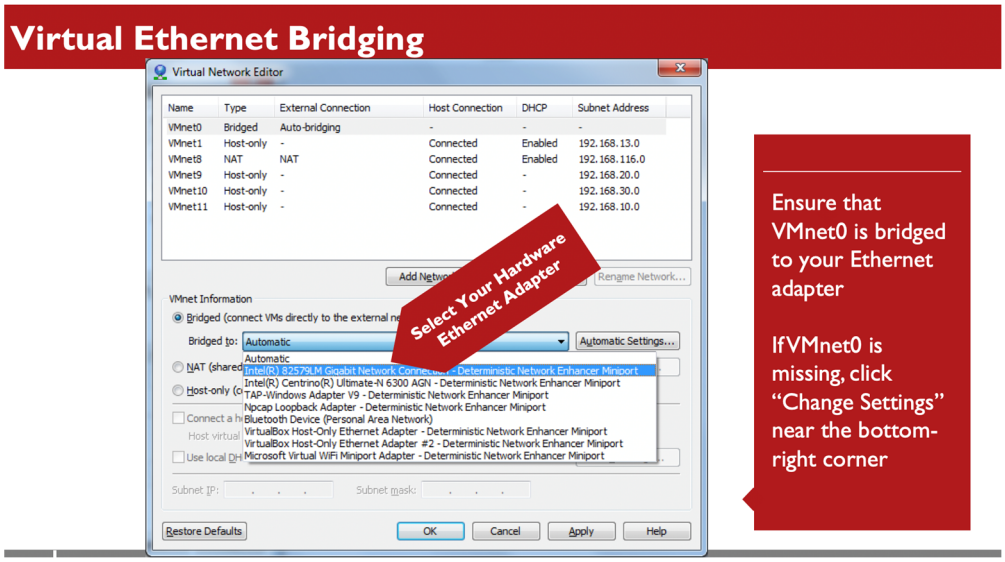
VMware Workstation Bridged Networking Configuration

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.

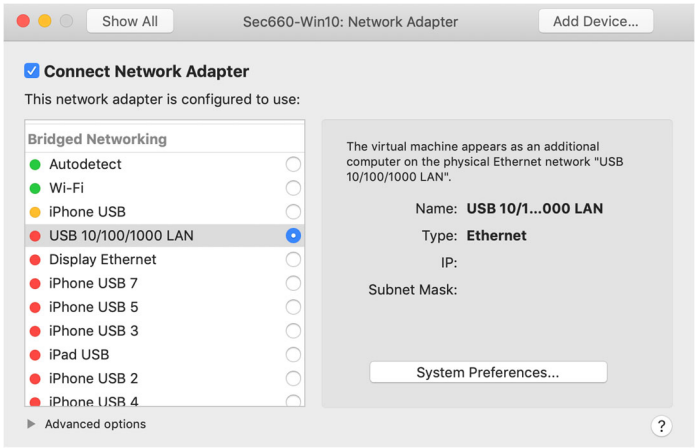
VMware Fusion Bridged Networking Configuration

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.

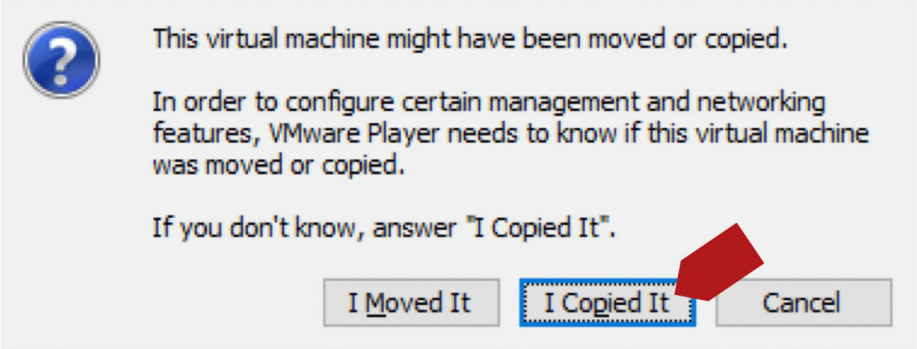


Once you've selected the radio button associated with your network adapter, you may be prompted for a password. Submit the password, click OK, and close the Network Adapter Window.

Boot ALL VMs

6. Boot ALL Linux and Windows Virtual Machines from the course media.

   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 Linux, log in to the guest machine using the following credentials:

   Username = deadlist

   Password = deadlist

8. The "deadlist" user has been given sudo permissions for everything. When root access is needed, use the following command:

   ```
   # sudo -i
   ```

9. Change both passwords as each user to something 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.

10. On Windows use the VMware Guest menu to send CTRL-ALT-DEL to the guest and select "Change password". Change **student**'s password from **sansinstitute** to something you will remember.

Networking for Remote Lab Access for OnDemand Students (NO Live Instructor)

Please follow the instructions provided at https://connect.labs.sans.org/ to connect to the lab environment. You will be using an HTML5 lab interface and will not need a VPN connection as needed during live events.

Networking for Remote Lab Access for LiveOnline or Simulcast Students

Use the SANS **My Labs** features at **https://www.sans.org/** after logging in. Under **My Online Training,** select **My Labs** and follow the on-screen instructions.

- You'll need to set up at least your course Windows virtual machine so it can access the Internet. Ensure it is 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 https://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**.
- As an alternative, you can use Linux or MacOS to connect to the lab environment, but you will be connecting to a potentially dangerous network at your own risk. SANS has provided VPN configurations for these cases in addition to the Windows VPN configuration. Note the Windows native RDP client will provide the most seamless experience for remote labs.

Networking for Local Lab Access for On-Premise Students

Your Instructor will have specific instructions for connecting to remote machines.

Change Desired Guest Keyboard and Regional Settings if Preferred

These Virtual Machines ship with English-US language and QWERTY keyboard mappings. If other settings are desired, use the guest's onscreen keyboard to configure them appropriately.

Make a CLEAN Snapshot

Be sure to power down all VMs, then make a CLEAN snapshot of each one. A snapshot of a powered-off VM will not consume much additional space, but will be useful to reset your VM to the pre-class configuration.

Conclusion

In this lab setup, you have extracted and configured the Linux Virtual Machines (VMs) and Windows VM images for the SEC760 course. Every VM has been pre-configured to suit this course.