Lab Setup

For my IR lab, I decided to use VitualBox to simulate a live networking environment. I chose this software mainly because it seemed like the best value to cost ratio for my purposes, as it's free to use with plenty of useful features. VirtualBox allowed me to create an entirely digital network running on the same host. This network was organized in such a way that any traffic heading to the internal network has to go through the PFSense firewall first. To do this, I first downloaded the ISO file for PFSense and imported it into VirtualBox. In the settings of the machine, I gave it the default 1 GB of RAM and two NICs. The first NIC was connected to my home network through a bridged connection in my host machine. It received an IP of 192.168.1.27, which showed that the device was communicating on the network properly and getting a response from DHCP. For the second NIC, a new subnet was created and will contain the virtual network of my lab environment and had the subnet of 192.168.56.0/24. Naturally, the PFSense firewall will act as a gateway, so that resides at 192.168.56.1. In the PFSense configuration, I made sure that the WAN was set to my home network and the LAN was set to that newly created subnet. I also made sure that the firewall did not allow malicious traffic from the internal subnet to infect my home network by setting rules that allowed connections through the router gateway, but not to the other devices on my network.

Next, I added the Security Onion ISO (downloaded from the Security Onion website) to act as a network forensics system. I gave it two NICs, 4GB of Ram, and 4 processors. For one of the NIC's, I assigned the address of 192.168.56.2 and set the gateway to the PFSense LAN IP address. I left the second blank for now, as it will be configured later. This installation wasn't as smooth as the PFSense box, however. Upon installing the Security Onion OS, I tried to update using 'sudo soup' to bring the box up to date, which resulted in a prompt for the path to the installation disk. The issue with this, is that VirtualBox automatically removes the disk from the virtual drive. I had to manually add the ISO to the disk drive, which then booted into the security onion installer. I realized my mistake and powered the machine off, then changed the boot order for the machine to boot the hard drive first. This allowed me to use /dev/cdrom in the path prompt, resulting in a successful update.

For my forensics Investigation machine as well as my vulnerability scanner, I chose Kali Linux due to my prior experience and familiarity with the distro, as well as the many useful tools that are included. The Kali box was a simple set up, I just downloaded the OVA from the Kali website and imported it to VirtualBox. The only real set up I did to this machine was create my user and set the IP address to 192.168.56.3.

It's important to have proper system logging in a network like this, especially since I will need it to determine what is happening to the network. This system is using Ubuntu because it's the most common and popular distribution of Linux among regular users. This machine is housed at 192.168.56.4. I attempted to install SIFT onto this machine, but I could not seem to get it installed properly. I scoured the internet and tried various suggestions, but the required commands simply would not run properly. If I were to guess, this is due to proper packages not being installed to handle these commands, but I thought it would be easier to just use my Kali machine for the forensics investigation aspect of the network and abandon the idea of using SIFT for right now. Finally, I added a basic Windows 7 client to act as an infected machine. The IP address of that box is at 192.168.56.5. In the future, I will work on setting up each component of the lab so that the configuration suits the needs of the rest of the course.