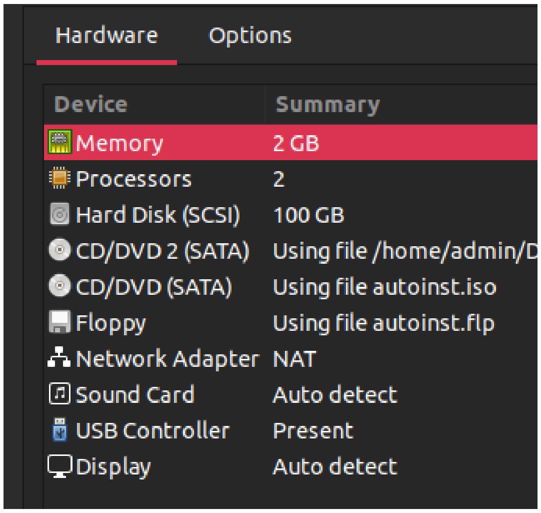
# The Security Tools

Ensuring that the tools that we will be using are provisioned properly is an essential part of setting up the environment. Deciding on what tools I wanted to incorporate was not very difficult because I wanted to become familiar with tools and systems that are commonly used. Naturally, I decided to go with Nessus as my vulnerability scanner and Splunk as my SIEM.

When it came to configuration, Nessus was a breeze. I decided to host the service on one of the Ubuntu VMs. The process was as simple as downloading Nessus Essentials and running a command in the terminal that is ‘sudo service nessusd start’. Once the service has started, open a web browser and search for ‘localhost:8834’ to access the client. Create an account to access the dashboard and all of the configuration is complete.

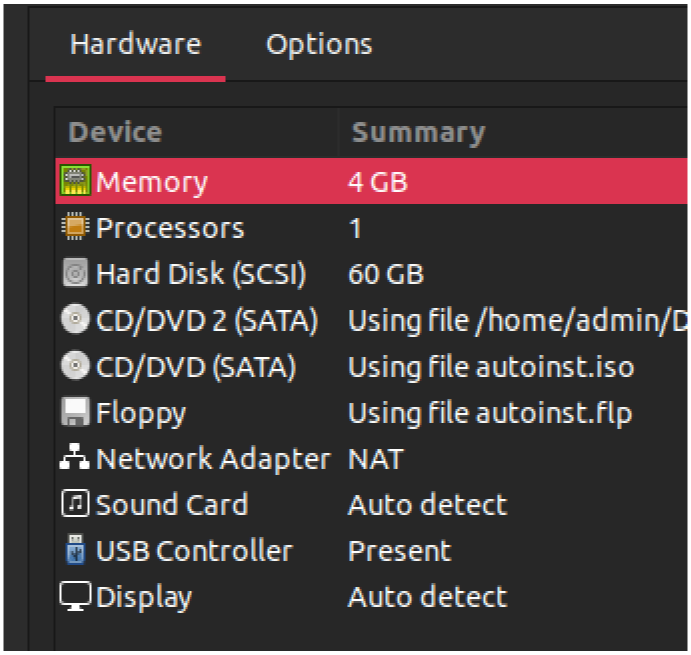
While Nessus was quite simple to install and configure, Splunk was a different story. Before going and downloading Splunk, it is important to know how a SIEM works and that there are multiple components that need to be in place for the SIEM to function properly. The components that I incorporated were the Splunk Indexer for data storage and querying and the Splunk Universal Forwarder for sending data to be stored by the indexer. The two services are hosted on the two Ubuntu VMs.



| Device | Summary |
|---|---|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 100 GB |
| CD/DVD 2 (SATA) | Using file /home/admin/D |
| CD/DVD (SATA) | Using file autoinst.iso |
| Floppy | Using file autoinst.flp |
| Network Adapter | NAT |
| Sound Card | Auto detect |
| USB Controller | Present |
| Display | Auto detect |

I started with the SIEM/Indexer, which is hosted on the same VM as Nessus. In order to download Splunk, you need to sign up for an account on their website. After signing up, you are presented with a number of different file types that you can download. I downloaded the ‘.tgz’ file. To install the service from the ‘.tgz’ file, you need to open a terminal from the “Downloads” directory and run

the command “sudo tar xvzf ‘splunk_package_name.tgz’ -C /opt” . Then, change the directory with the command “cd /opt/Splunk/bin” . To start  the indexer, run “sudo ./splunk start”, accept the license agreement, and create an admin account.
As previously stated, the Universal Forwarder will be hosted on an Ubuntu machine. For the Universal Forwarder, navigate to the Splunk website and copy the wget link for the download. Open a terminal and run the command “tar xvzf ‘splunk_package_name.tgz’”. To start the forwarder, run “/opt/splunkforwarder/bin/splunk start”, accept the license, and create an admin account. Now you will need to configure the indexer to be able to receive logs from the universal forwarder.
Navigate again to the Splunk dashboard on the other Ubuntu VM. Select the receiving service and select the “configure receiving” option. Set the port default to 9997. Go back to the machine with the forwarder and run the command “op/splunkforwarder/bin/splunk add forward-server (IP of indexer machine):9997”. Finally, run the command “add command opt/splunkforwarder/bin/splunk add monitor /var/log”. You should now be able to query the indexer from the dashboard using SQL queries and logs will populate from the universal forwarder.



| Device | Summary |
|---|---|
| Memory | 4 GB |
| Processors | 1 |
| Hard Disk (SCSI) | 60 GB |
| CD/DVD 2 (SATA) | Using file /home/admin/D |
| CD/DVD (SATA) | Using file autoinst.iso |
| Floppy | Using file autoinst.flp |
| Network Adapter | NAT |
| Sound Card | Auto detect |
| USB Controller | Present |
| Display | Auto detect |

While this may seem like a relatively seamless process, there were some issues that I ran into. There were issues with the permissions when trying to run the commands for Splunk. I had to run a script to give myself access to all of the directories, which I should have had anyways because I was using sudo commands and a root account. I do not have a ton of experience with Linux/Ubuntu, so I had to find the commands that change ownership. The command I ran to solve this issue was “sudo chown -R ‘username’ -opt”.

# Resources

Splunk Download Guide

https://hurricanelabs.com/splunk-tutorials/from-zero-to-splunk-how-to-install-splunk-on-a-linux-vm-in-minutes/

Universal Forwarder Setup Guide

https://www.youtube.com/watch?v=smyLZ6ataK0