<Name Omitted>

Cyber Defense Overview

Lab 1 Report

**IMPORTANT NOTE:** In order for Kali Linux to see the network data between all of the VMs, it had to be set on ‘promiscuous mode’ in the advanced network settings for the box.

**Part 2**

For part 2, I used nmap 192.168.61.100-105 to scan a small part of the IP range reserved for the host network (based on the IP range I was using).

**Part 3**

In order to complete part 3, I first used nc -l -u 8000 > received.txt on my Ubuntu machine in order to listen to port 8000 and output the results to a text file. Then, I used nc -u 192.168.61.102 8000 on my openSUSE machine in order to send messages from my suse machine to the ubuntu one.

**Part 4**

An easy way to find the packet without directly knowing the IP addresses (even though I did know the IP addresses and could’ve easily searched in such a way) was finding the ACK request between two machines on the network and then searching for the packet with a timestamp afterword that was sent. Another clue was the length of the packet, as it couldn’t be too small for the entire message to get through. Additionally, I could have used the IP addresses to search for the packet and the protocol (because I used the nc command with a -u, it used UDP).

The flag in the PCAP file begins at byte 42 in packet number 17, timestamp 85.228330213.