Tobby Lie
CSCI 4723
Homework 4

Bash Report

My code essentially continually loops in a structure that is: call nmap on 192.168.10.*/24 using grep in order to get only the open ports listed, write that result into an initial log file, save the lines from the log file into an array, pause for 5 minutes and then do this again except with a new log file and new array variable. At the end of each loop, we want to then loop through all elements in the newer array and check if there are any elements in the newer array that are not contained in the initial array, if this is true, then we notate the time and which port was discovered.

The way my code was tested was to first have Kali VM1 and Windows VM open initially, in this initial scan my first log file captured all ports open meaning the ports open in Windows VM. After 10 minutes, Kali VM2 is started and the command python -m SimpleHTTPServer 8008 is executed, Kali VM1 will then run nmap again which then picks up port 8008 open on the Kali VM2 ip.

I have three log files, the first to capture an initial scan of open ports, the second to capture all open ports after 10 minutes and a third log file to notate those changes and new ports that were opened after the initial scan.