Name: Hemant Jain

Lab Progress Report Due Date: 2/15/2021

Current Week Since Start Date: Week 4 (2/16/2021– 2/22/2021)

Reporting Week: From Feb 10, 2021 to Feb 17, 2021

Summary about the TestOut Module-4 Learning:

From the TestOut LabSim, I learnt about the Manageable Network Plan which is the process created by NSA to assist in the making of the network manageable, defensible and secure. Reading about the different milestone starting from the Prep for the document, Mapping into the network, Protecting it out using the various network security protocols, maintaining the constant uptime and ranging the control of the access to the network to the specified persons. It gave me an insight how important and difficult it is to manage the network and baseline the management for it.

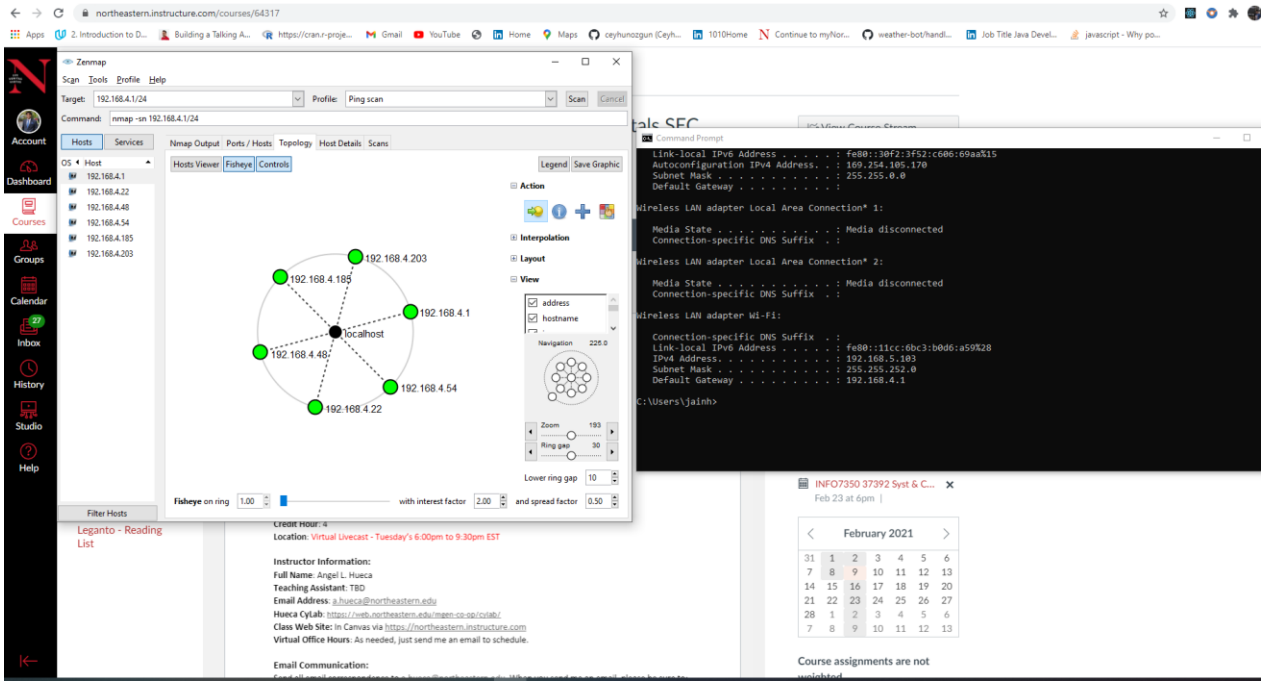
Continuing in the Windows Hardening and operating systems some terminologies like hardening, hotfix, patch, and service pack. Detailing out specifically on the hardening on the system and using the controlled login for the configuration baselines.
Followed-up with the hands-on exercise where they given us out with the VM with Windows operating systems following and setting out some restrictions to the users and remove the access from some the applications available to the user operators.
Giving a brief insight about the two type of the storages for large amount of data namely Network Attached Storage (NAS)and Storage Area network (SAN).

Reading about the various network data transfer security protocols for the safe transition of data using the TCP/IP Protocols such as FTP, TFTP, SCP, SFTP, FTPS. Managing out the file systems permissions and the two different types of permissions namely shared and NTFS. Both used the shared discretionary access control list (DACL) for the controlling access. NTFS authorizations is to assign Co-owner share consents to Everyone.
Use NTFS consents to control get to. Utilize the rule of slightest benefit by allotting NTFS permissions as it were to fundamental bunches and by doling out as it were the vital authorizations to those groups. Indeed, in spite everybody has share consents, as it were the clients or bunches with NTFS permissions will have access.

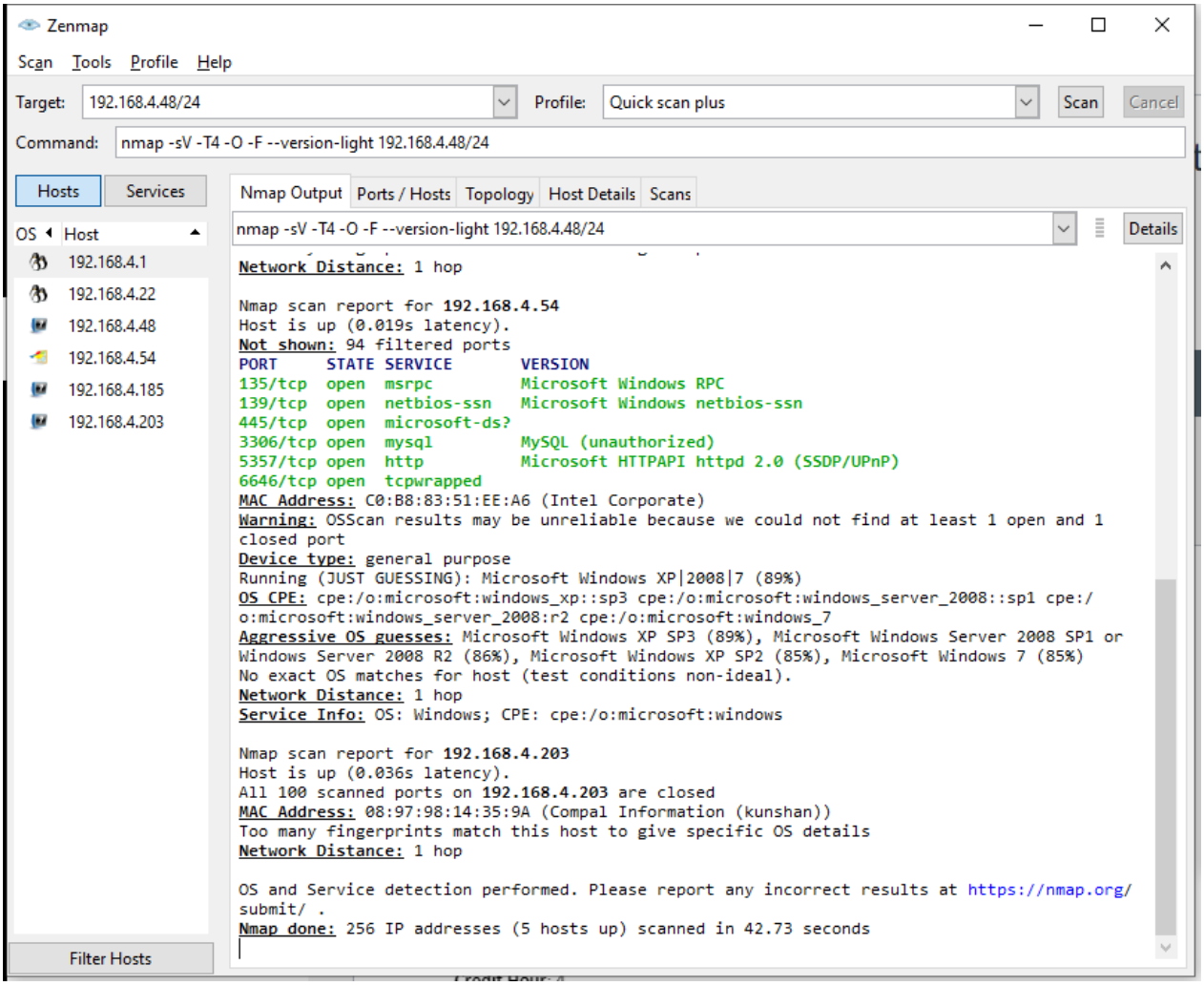
At the end follow-up with the Linux host security facts and various security tasks commands to replicate around in the Kali Linux environment or Windows local environment was amazing experience hands-on demo lab. Lastly, learnt how to configure the iptables firewalls and how to accept and drop and reject the connections using some set of rule commands in the iptables.

In-class Lab Homework:

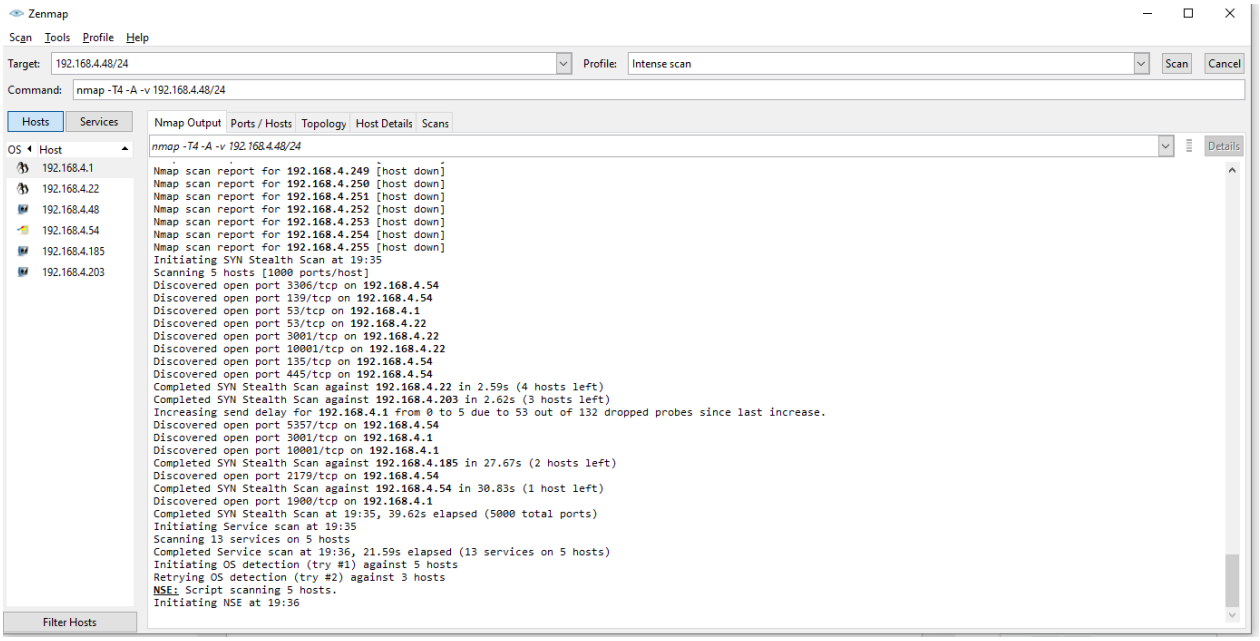
nmap -sn 192.168.4.1/24 (Ping Scan (Fisheye View)) => *This command only pings the target but does not scan any port*



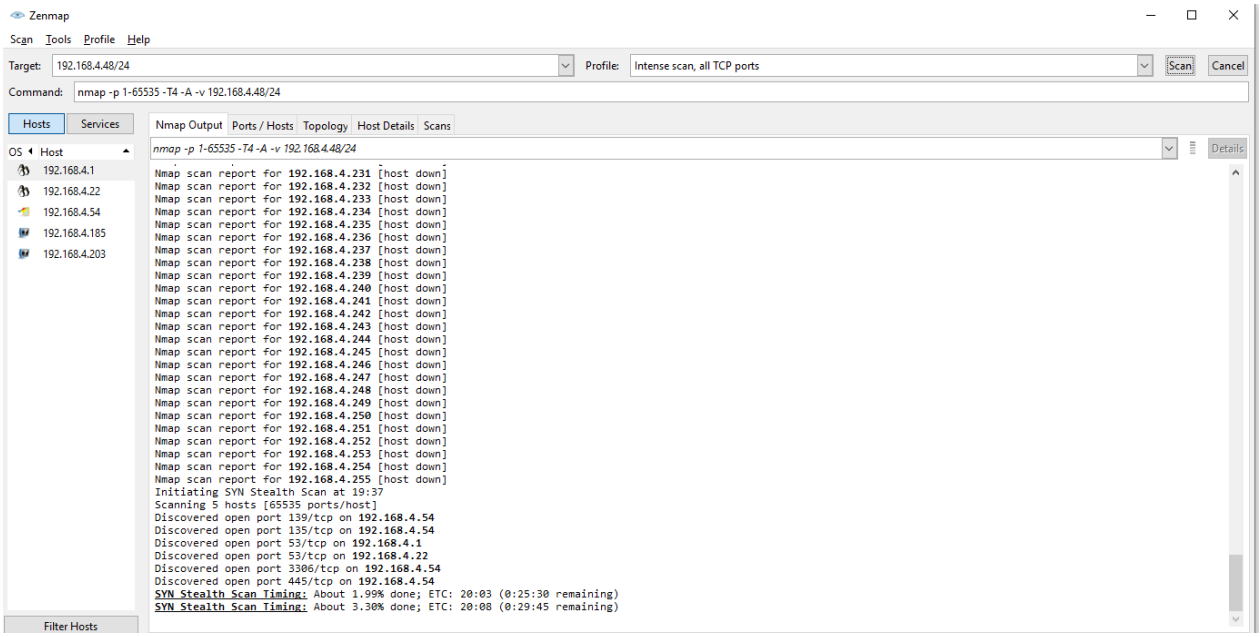
nmap -sV -T4 -O -F –version-light 192.168.4.1/24 (Quick Scan Plus) => ***This command scans only limited number of TCP ports. i.e. Top 100 most common TCP ports.***



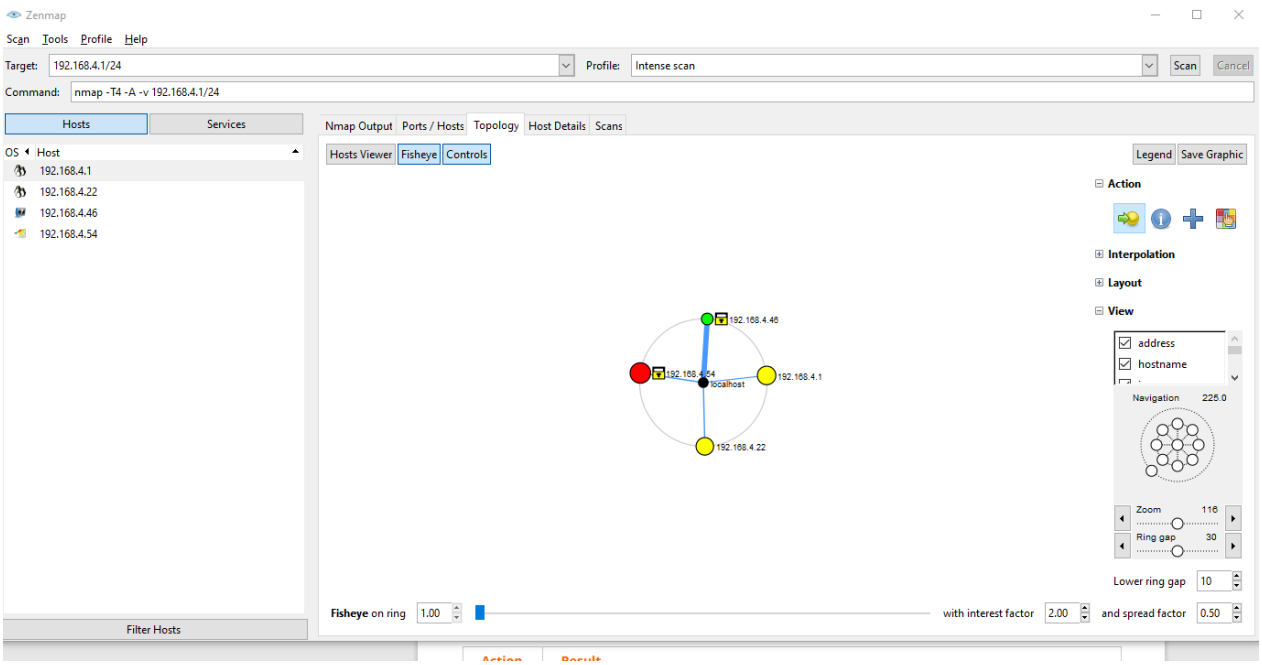
nmap -T4 -A -v 192.168.4.1/24 (Intense Scan) => ***This scans the most common TCP ports quickly and also determines the OS type, their services as well as versions.***



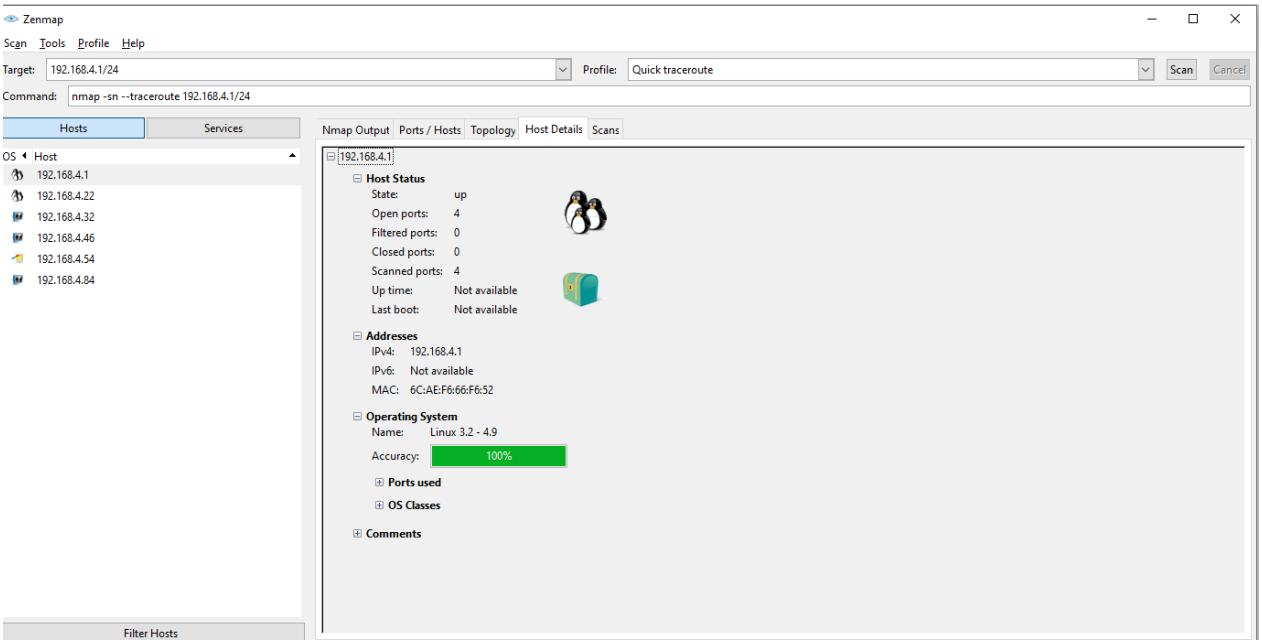
nmap -p1 -65535 -T4 -A -v 192.168.4.48/24 (Intense Scan, all TCP Ports) => I*t takes time to scan all the ports, Nmap usually scans top 1000 most common ports. However, Intense Scan, all TCP Ports asks Nmap to scan all the ports from 1–65535(max).*



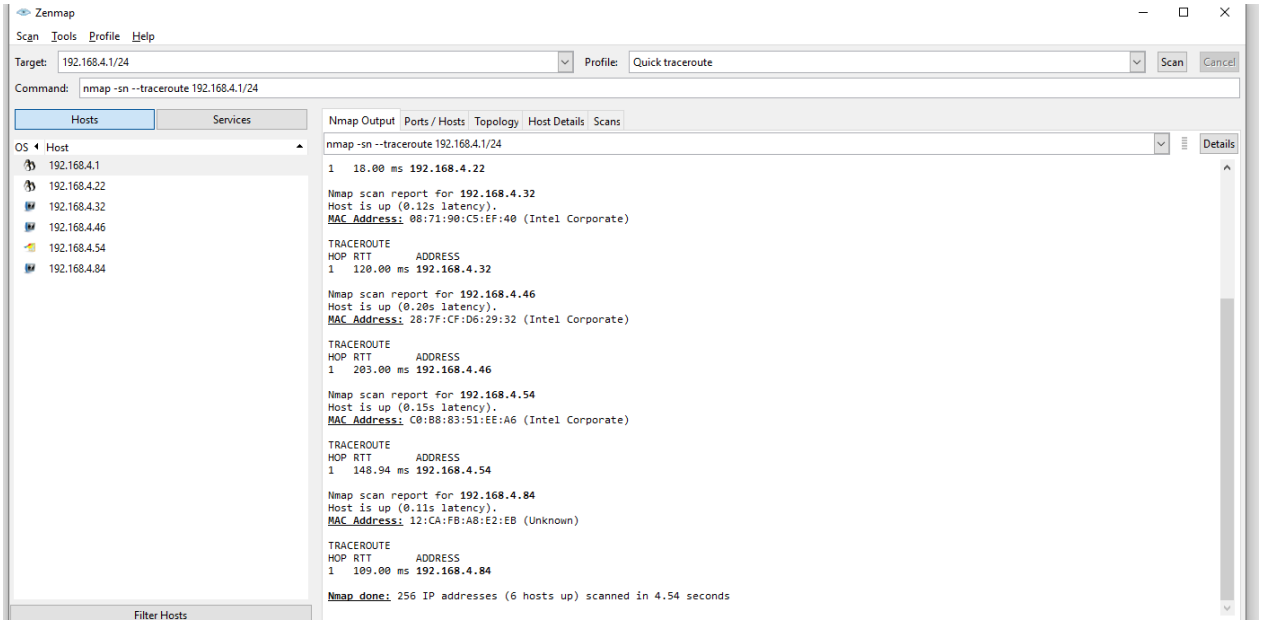
nmap –T4 -A -v 192.168.4.1/24 (Intense Scan) => ***This scans the most common TCP ports quickly and also determines the OS type, their services as well as versions.***



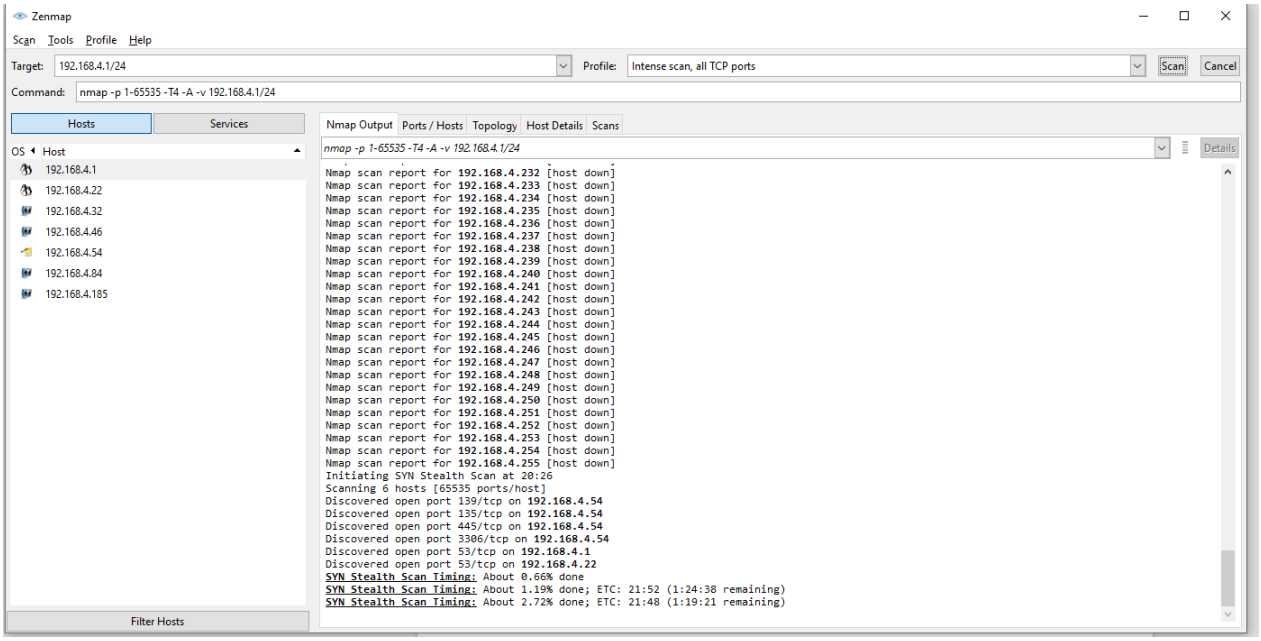
nmap -sn --traceroute 192.168.4.1/24 (Quick Traceroute(Host Details)) => *This command will traceroute and ping all the hosts defined in a target.*



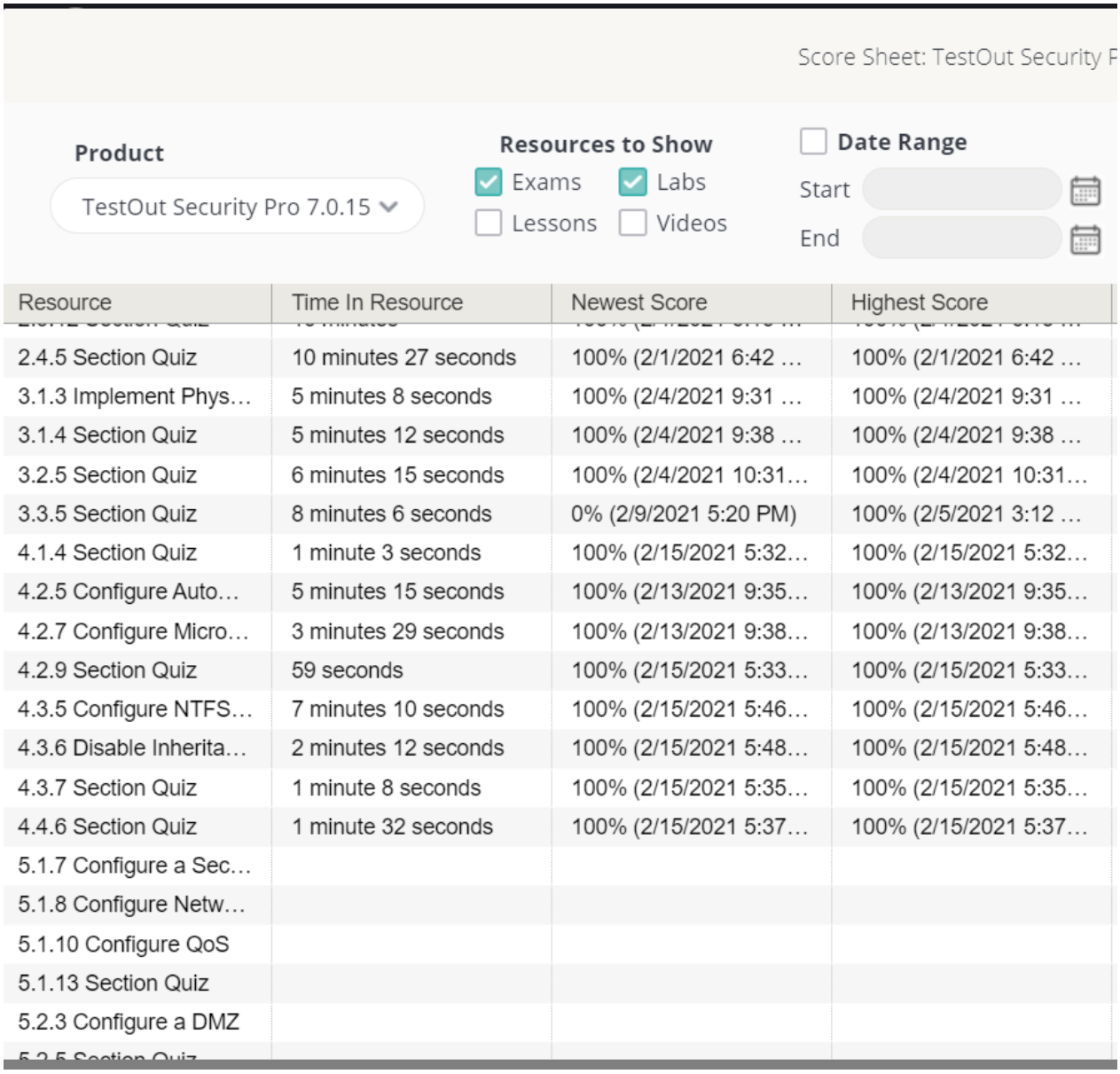
nmap -sn --traceroute 192.168.4.1/24 (Quick Traceroute) => ***This command will traceroute and ping all the hosts defined in a target.***



nmap -p 1-65535 -T5 -A -v 192.168.4.1/24 (Intense scan, all TCP Ports) => I*t takes time to scan all the ports, Nmap usually scans top 1000 most common ports. However, Intense Scan, all TCP Ports asks Nmap to scan all the ports from 1–65535(max).*



Progress Embedded Image of Progress Report from LabSim:



Score Sheet: TestOut Security P

Product: TestOut Security Pro 7.0.15

Resources to Show: Exams, Labs, Lessons, Videos

Date Range: Start, End

Resource	Time In Resource	Newest Score	Highest Score
2.4.5 Section Quiz	10 minutes 27 seconds	100% (2/1/2021 6:42 …	100% (2/1/2021 6:42 …
3.1.3 Implement Phys…	5 minutes 8 seconds	100% (2/4/2021 9:31 …	100% (2/4/2021 9:31 …
3.1.4 Section Quiz	5 minutes 12 seconds	100% (2/4/2021 9:38 …	100% (2/4/2021 9:38 …
3.2.5 Section Quiz	6 minutes 15 seconds	100% (2/4/2021 10:31…	100% (2/4/2021 10:31…
3.3.5 Section Quiz	8 minutes 6 seconds	0% (2/9/2021 5:20 PM)	100% (2/5/2021 3:12 …
4.1.4 Section Quiz	1 minute 3 seconds	100% (2/15/2021 5:32…	100% (2/15/2021 5:32…
4.2.5 Configure Auto…	5 minutes 15 seconds	100% (2/13/2021 9:35…	100% (2/13/2021 9:35…
4.2.7 Configure Micro…	3 minutes 29 seconds	100% (2/13/2021 9:38…	100% (2/13/2021 9:38…
4.2.9 Section Quiz	59 seconds	100% (2/15/2021 5:33…	100% (2/15/2021 5:33…
4.3.5 Configure NTFS…	7 minutes 10 seconds	100% (2/15/2021 5:46…	100% (2/15/2021 5:46…
4.3.6 Disable Inherita…	2 minutes 12 seconds	100% (2/15/2021 5:48…	100% (2/15/2021 5:48…
4.3.7 Section Quiz	1 minute 8 seconds	100% (2/15/2021 5:35…	100% (2/15/2021 5:35…
4.4.6 Section Quiz	1 minute 32 seconds	100% (2/15/2021 5:37…	100% (2/15/2021 5:37…
5.1.7 Configure a Sec…			
5.1.8 Configure Netw…			
5.1.10 Configure QoS			
5.1.13 Section Quiz			
5.2.3 Configure a DMZ			