

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

The screenshot displays a desktop environment with several windows open. The primary window is Zenmap, which is configured for a 'Ping scan' on the target '192.168.4.1/24'. The 'Fisheye' view is selected, showing a central 'localhost' node connected to several other nodes: 192.168.4.185, 192.168.4.203, 192.168.4.1, 192.168.4.54, 192.168.4.22, and 192.168.4.48. The interface includes a sidebar with navigation options like 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. Below the main view, there are settings for 'Fisheye on ring' (1.00), 'with interest factor' (2.00), and 'and spread factor' (0.50). A 'Filter Hosts' section shows 'Leganto - Reading List'. At the bottom, there is a section for 'Instructor Information' for Angel L. Hueca, including contact details and office hours.

Overlaid on the Zenmap window is a Windows Command Prompt window. It displays the output of the command 'ipconfig /all', showing network configuration details for the 'Ethernet adapter Local Area Connection* 1' and 'Wireless LAN adapter Local Area Connection* 2'. The output includes the Link-local IPv6 Address, Autoconfiguration IPv4 Address, Subnet Mask, and Default Gateway.

In the bottom right corner, a calendar for February 2021 is visible, showing the dates from 1 to 28. The calendar is titled 'INFO7350 37392 Syst & C...' and indicates the current date is February 23 at 6pm.

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.

The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.4.48/24' and the 'Profile' is 'Quick scan plus'. The 'Command' field contains 'nmap -sV -T4 -O -F --version-light 192.168.4.48/24'. The 'Hosts' tab is selected, showing a list of hosts on the left and the 'Nmap Output' pane on the right.

Hosts:

- 192.168.4.1
- 192.168.4.22
- 192.168.4.48
- 192.168.4.54
- 192.168.4.185
- 192.168.4.203

Nmap Output:

nmap -sV -T4 -O -F --version-light 192.168.4.48/24

Network Distance: 1 hop

Nmap scan report for 192.168.4.54
Host is up (0.019s latency).
Not shown: 94 filtered ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
3306/tcp	open	mysql	MySQL (unauthorized)
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp	open	tcpwrapped	

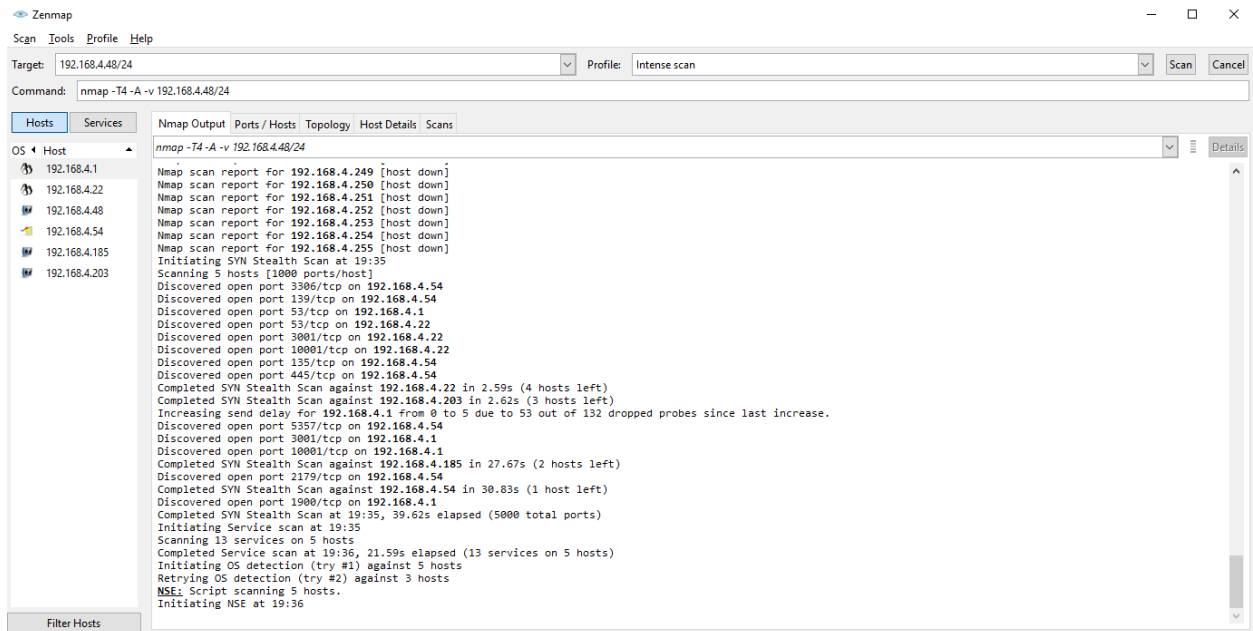
MAC Address: C0:B8:83:51:EE:A6 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (86%), Microsoft Windows XP SP2 (85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.4.203
Host is up (0.036s latency).
All 100 scanned ports on 192.168.4.203 are closed
MAC Address: 08:97:98:14:35:9A (Compal Information (kunshan))
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (5 hosts up) scanned in 42.73 seconds

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) => It 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).

Zenmap

Scan Tools Profile Help

Target: 192.168.4.48/24 Profile: Intense scan, all TCP ports Scan Cancel

Command: nmap -p 1-65535 -T4 -A -v 192.168.4.48/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.4.1

192.168.4.22

192.168.4.54

192.168.4.185

192.168.4.203

Nmap scan report for 192.168.4.231 [host down]

Nmap scan report for 192.168.4.232 [host down]

Nmap scan report for 192.168.4.233 [host down]

Nmap scan report for 192.168.4.234 [host down]

Nmap scan report for 192.168.4.235 [host down]

Nmap scan report for 192.168.4.236 [host down]

Nmap scan report for 192.168.4.237 [host down]

Nmap scan report for 192.168.4.238 [host down]

Nmap scan report for 192.168.4.239 [host down]

Nmap scan report for 192.168.4.240 [host down]

Nmap scan report for 192.168.4.241 [host down]

Nmap scan report for 192.168.4.242 [host down]

Nmap scan report for 192.168.4.243 [host down]

Nmap scan report for 192.168.4.244 [host down]

Nmap scan report for 192.168.4.245 [host down]

Nmap scan report for 192.168.4.246 [host down]

Nmap scan report for 192.168.4.247 [host down]

Nmap scan report for 192.168.4.248 [host down]

Nmap scan report for 192.168.4.249 [host down]

Nmap scan report for 192.168.4.250 [host down]

Nmap scan report for 192.168.4.251 [host down]

Nmap scan report for 192.168.4.252 [host down]

Nmap scan report for 192.168.4.253 [host down]

Nmap scan report for 192.168.4.254 [host down]

Nmap scan report for 192.168.4.255 [host down]

Initiating SYN Stealth Scan at 19:37

Scanning 5 hosts [65535 ports/host]

Discovered open port 139/tcp on 192.168.4.54

Discovered open port 135/tcp on 192.168.4.54

Discovered open port 53/tcp on 192.168.4.1

Discovered open port 53/tcp on 192.168.4.22

Discovered open port 3386/tcp on 192.168.4.54

Discovered open port 445/tcp on 192.168.4.54

SYN Stealth Scan Timing: About 1.99% done; ETC: 20:03 (0:25:30 remaining)

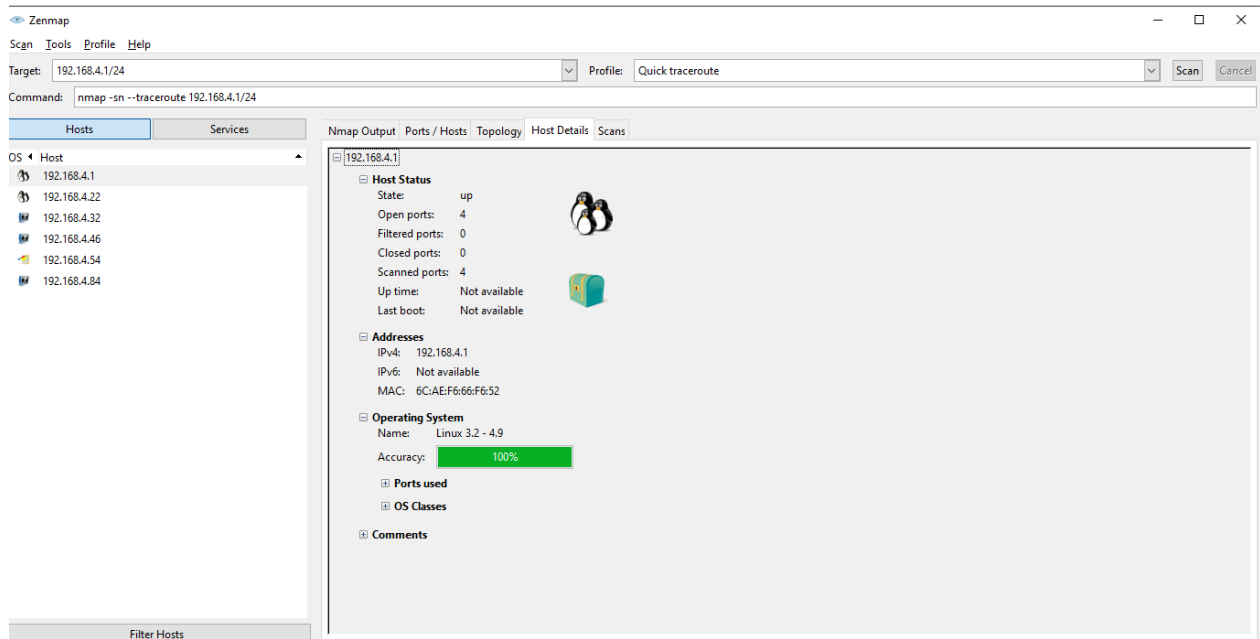
SYN Stealth Scan Timing: About 3.30% done; ETC: 20:08 (0:29:45 remaining)

Filter Hosts

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.

The screenshot shows the Zenmap application window. The 'Target' field is set to '192.168.4.1/24' and the 'Profile' is 'Quick traceroute'. The 'Command' field shows 'nmap -sn --traceroute 192.168.4.1/24'. The 'Hosts' tab is selected, showing a list of hosts: 192.168.4.1, 192.168.4.22, 192.168.4.32, 192.168.4.46, 192.168.4.54, and 192.168.4.84. The 'Nmap Output' tab is also visible, showing the scan results for each host. The results include the host's IP address, MAC address, and traceroute information.

Hosts:

- 192.168.4.1
- 192.168.4.22
- 192.168.4.32
- 192.168.4.46
- 192.168.4.54
- 192.168.4.84

Nmap Output:

```
nmap -sn --traceroute 192.168.4.1/24
1 18.00 ms 192.168.4.22

Nmap scan report for 192.168.4.32
Host is up (0.12s latency).
MAC Address: 08:71:90:C5:EF:40 (Intel Corporate)

TRACEROUTE
HOP RTT ADDRESS
1 120.00 ms 192.168.4.32

Nmap scan report for 192.168.4.46
Host is up (0.20s latency).
MAC Address: 28:7F:CF:D6:29:32 (Intel Corporate)

TRACEROUTE
HOP RTT ADDRESS
1 203.00 ms 192.168.4.46

Nmap scan report for 192.168.4.54
Host is up (0.15s latency).
MAC Address: C8:88:83:51:EE:A6 (Intel Corporate)

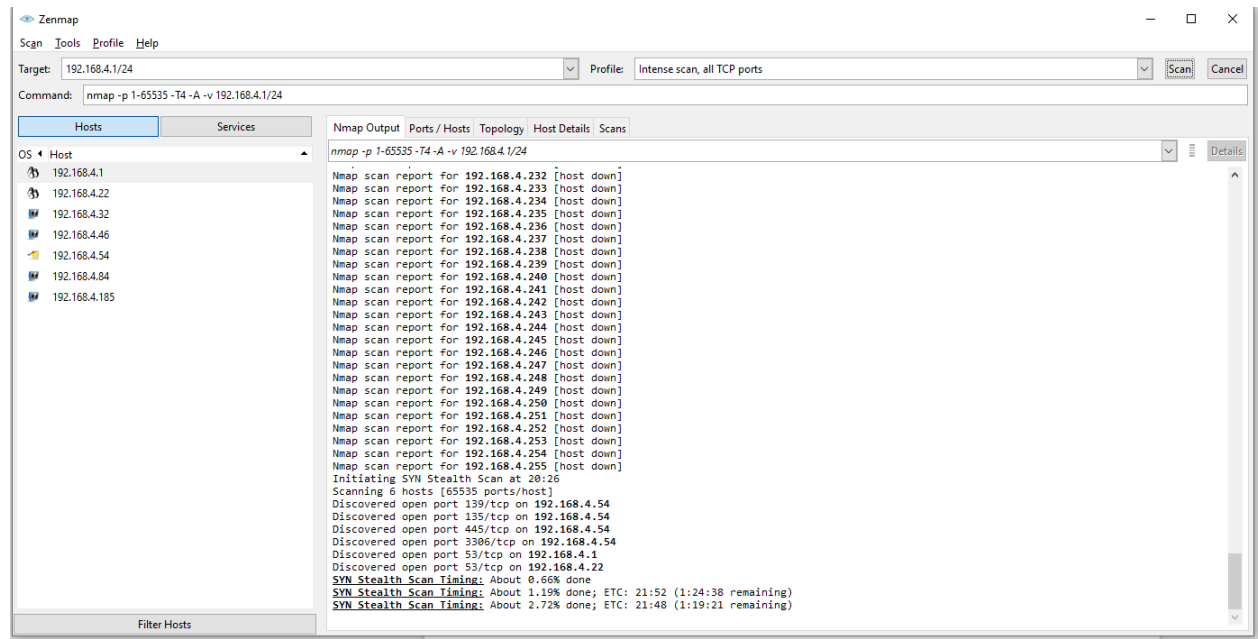
TRACEROUTE
HOP RTT ADDRESS
1 148.94 ms 192.168.4.54

Nmap scan report for 192.168.4.84
Host is up (0.11s latency).
MAC Address: 12:CA:FB:AB:E2:EB (Unknown)

TRACEROUTE
HOP RTT ADDRESS
1 109.00 ms 192.168.4.84

Nmap done: 256 IP addresses (6 hosts up) scanned in 4.54 seconds
```

nmap -p 1-65535 -T5 -A -v 192.168.4.1/24 (Intense scan, all TCP Ports) => It 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 F			
<div> <div> Product TestOut Security Pro 7.0.15 ▼ </div> <div> Resources to Show <input checked="" type="checkbox"/> Exams <input checked="" type="checkbox"/> Labs <input type="checkbox"/> Lessons <input type="checkbox"/> Videos </div> <div> <input type="checkbox"/> Date Range Start <input type="text"/> End <input type="text"/> </div> </div>			
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			
5.2.5 Section Quiz			