NETWORK ADMINISTRATION

Project 1

Table of Contents

TABLE OF CONTENTS **0**

EMAIL TO MANAGER **2**

INTRODUCTION **3**

FUNCTIONS **3**

NETWORK DEVICE DATA **3**

ZENMAP/NMAP SCANNED DATA 4
DEVICE DATA 5

METHODOLOGY **5**

WIRESHARK CAPTURE **6**

172.16.14.50 WINDOWS1 6
172.16.14.51 KALI 7
17.16.14.52 LINUX 7
172.16.14.53 WINDSERVER 7
172.16.14.101 VPC 7

TOPOLOGY **8**

REFERENCES **8**

Email to Manager

Hi [Name],

Hope you are having a pleasant day. As instructed, I've scanned and analysed the 172.16.14.0/24 network. I was able to find all the available device using a ping scan through Nmap, in total there are 5 devices with the IP range from [172.16.14.50-53 & .101]. Out of the 5 machines, 1 was a Windows server, 1 was a Windows machine, and 1 was identified as a Linux machine, while the remaining two were unable to resolve a host name. However, other then the IP and MAC of all devices, I was also able to discover all ports that were open showcasing the security risk posed by all devices. Such that the Windows machines had filtered ports and the Linux machine both had less then 6 open ports, the 172.16.14.51 machine was the most secure with less then 3 open ports, and the 172.16.14.101 machine is the biggest security risk with roughly 100 open ports.

Attached below is the in-depth analysis, a breakdown of all captured data including ports and the OSI, along with the methodology used to resolve needed data.

If you have any questions or concerns, you can reach out at name@domain.ca

Regards,

Fahad Shahzad

Introduction

This report will examine the different network devices connected on 172.16.14.0/24, with a breakdown of key insights on devices between 172.16.14.50 – 172.16.14.53 along with 172.16.14.101. The report will investigate the command used to retrieve key insights and then a breakdown of why such a method was used to derive findings.

Functions

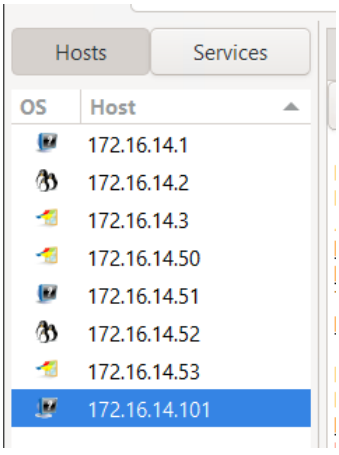
Below is a list of functions that were used in Zenmap (application used to find host/devices and services on a network) to gather information about the network and devices, along with a short description.

-sN	Prevents host discovery after port scan, when used on its own will run host discovery
-sV	Perform version detection on open ports
-T4	Speed up scans, Aggressive scan
-F	Scan a specific/top ~100 ports
-Pn	Like -sN, however -Pn treats every host as up and will not skip
-A	Used to detect operating system, host name and more
-v	Enters verbose mode providing more information, including ARP time
--version-light	Faster version scanning without instance debugging

Note I used Zenmap since Nmap was not installed on the jump host and didn't have access

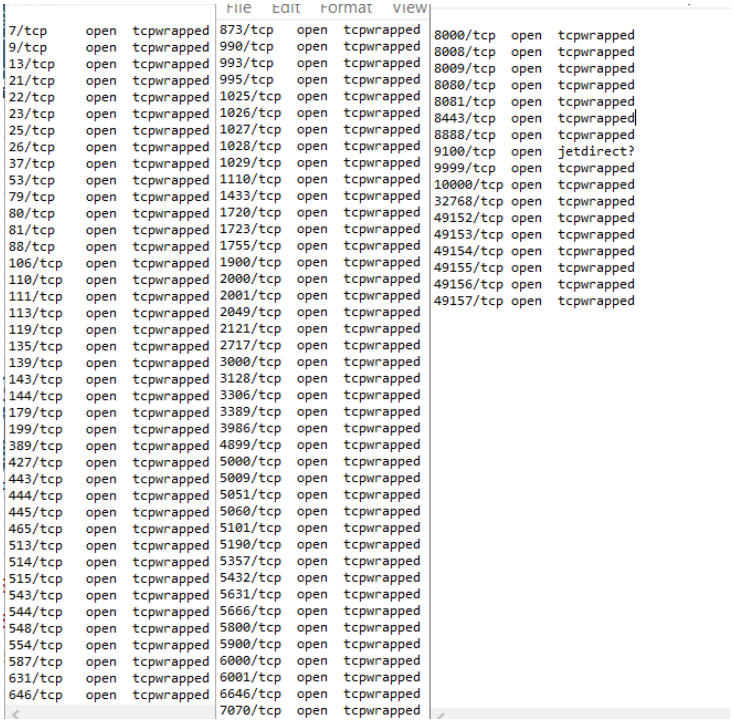
Network Device Data

Scan network for all devices, below are the results.



Zenmap/Nmap scanned data

Machine designation	Device Host Name	IP address	MAC address	Operating System & version (% aggressive scan)	Open ports with associated services	ARP Ping Scan elapsed time (s – seconds)
Windows1	DESKTOP-WIN10PRO	172.16.14.50	50:01:00:02:00:01	Microsoft Windows XP SP2 (86%)	3389 ms-wbt-server | 5357 http	0.46s
Windserver	WIN-SERVER-2022	172.16.14.53	50:01:00:01:00:01	Microsoft Windows Server 2022 (94%)	80 http | 135 msrpc | 139 netbios-ssn | 445 microsoft-ds | 3389 ms-wbt-server | 5357 http	1.05s
Linux	*No host name found*	172.16.14.52	50:01:00:05:00:01	Linux 4.15 - 5.8	80 http | 3306 mysql | 3389 ms-wbt-server | 9200 wap-wsp	0.17s
Kali	*No host name found*	172.16.14.51	50:01:00:07:00:01	*No OS detected* to many fingerprints	*No open ports found* all ports are in ignored state	0.17s
VPC	*No host name found*	172.16.14.101	00:50:79:66:68:03	*No OS match for host*	See image 1	0.17s



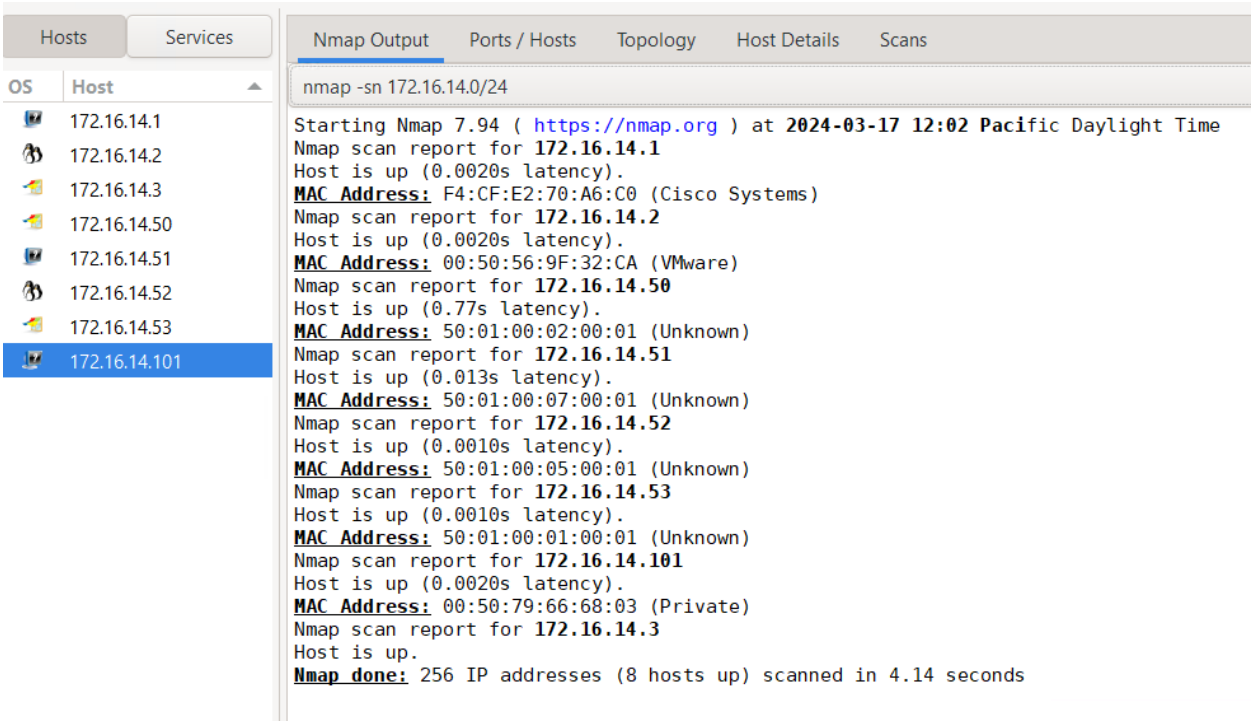
(Image1)

Device Data

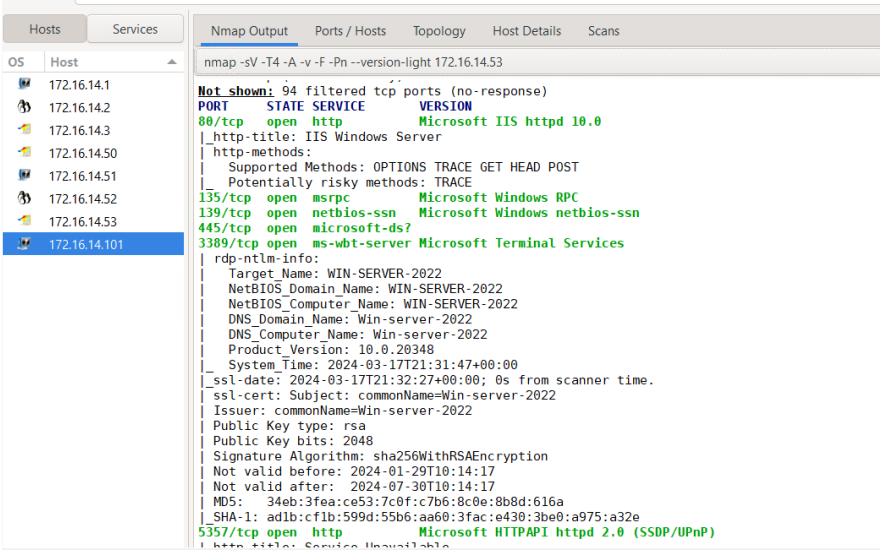
Designation	Host name	IP	MAC	OS
Windows1	DESKTOP-WIN10PRO	172.16.14.50	50:01:00:02:00:01	Windows 10 Pro
Windserver	Win-Server-2022	172.16.14.53	50:01:00:01:00:01	Windows server 2022 SE
Linux	User-pc	172.16.14.52	50:01:00:05:00:01	Ubuntu 20.04.6
Kali	Kali	172.16.14.51	50:01:00:07:00:01	Kali GNU
VPC	VPCS[1]	172.16.14.101	00:50:79:66:68:03	VPC

Methodology

First and foremost, while there were multiple options to scanning the network 172.16.14.0/24, the choice came down to what was the fastest option that will provide what the available devices/hosts are on the network which are online. The simplest option was [nmap -sn 172.16.14.0/24], which provided information such IP and MAC. (see below)



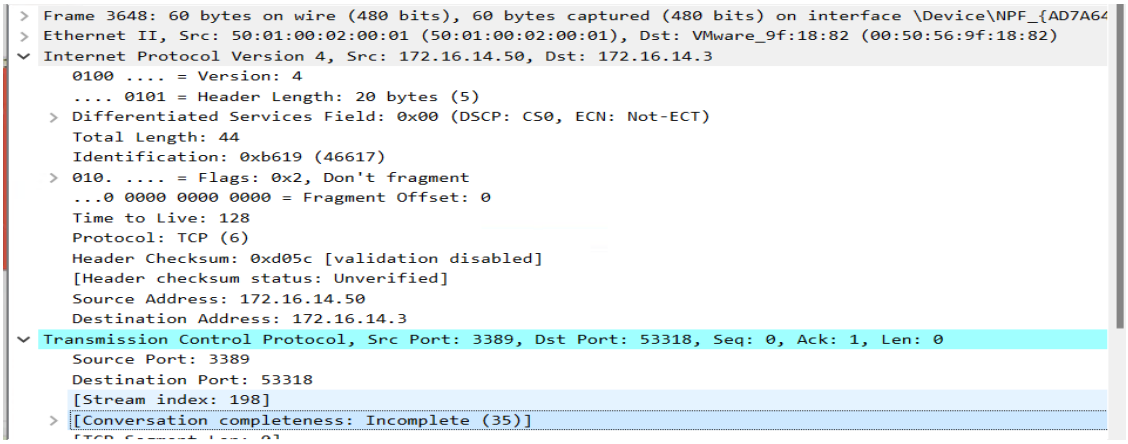
Now that we are given the host IP, searching for information on each host can be streamlined. Keeping to the same methodology of fastest option provided greatest information. With this in mind, [nmap -sV -T4 -A -v -F -Pn –version-light 172.16.14.###], gave the best results in one shot. (see below)



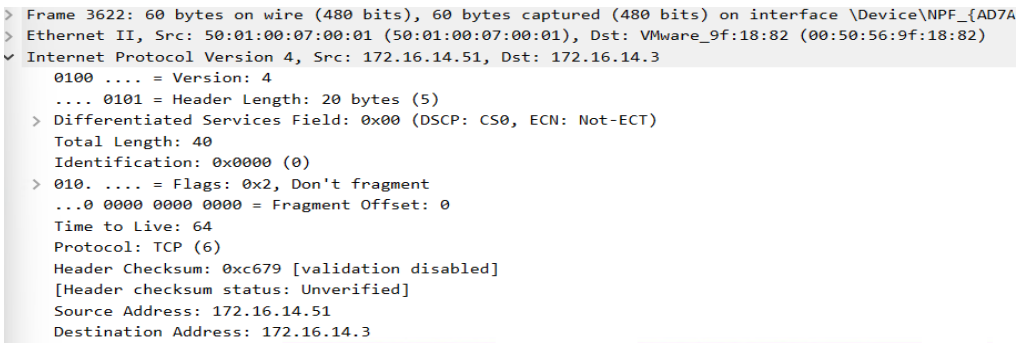
While this method was the most fruitful, it wasn't all complete. Since Windows devices and the Ubuntu Linx devise were scannable and provided more information, devices like the VPC and the Kali Linux devices, provided information no better than a ping. Even after isolating for individual parameters, scanning for one piece of information (host name), Zenmap could not find that information. Which is why [nmap -sV -T4 -A -v -F -Pn –version-light 172.16.14.###] provide the most complete information Zenmap is able to. Using these parameters, we can detect host name, IP, MAC, OS, ARP, and ports open.

Wireshark capture

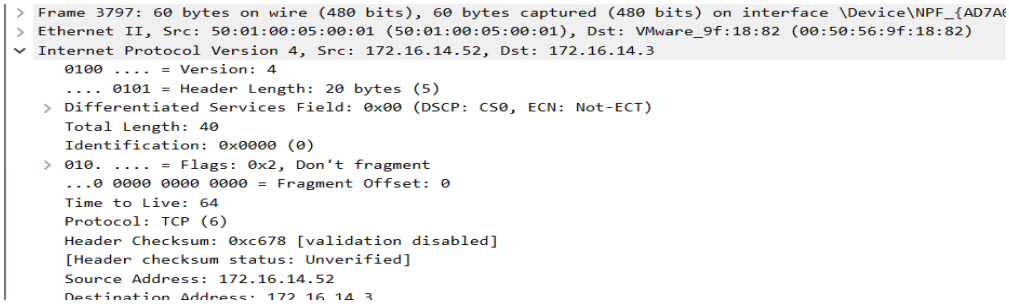
172.16.14.50 Windows1 – found on layer 3 network layer



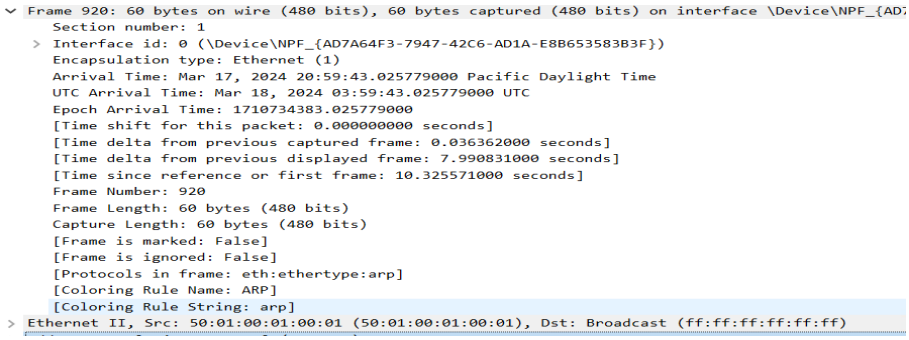
172.16.14.51 Kali - found on layer 3 network layer



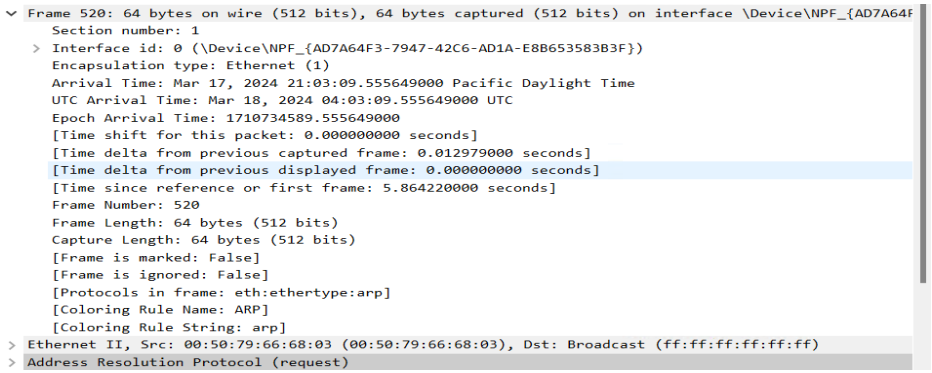
17.16.14.52 Linux - found on layer 3 network layer



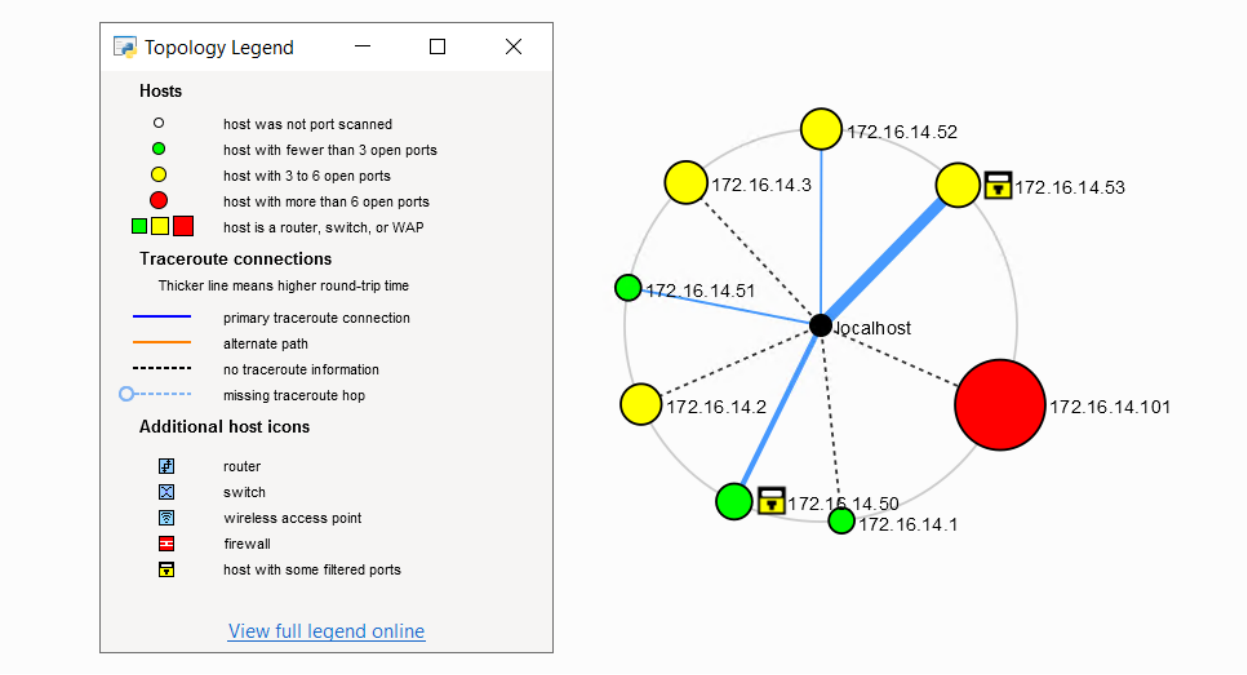
172.16.14.53 Windserver – found on layer 1 physical layer



172.16.14.101 VPC - found on layer 1 physical layer



Topology



References

Chapter 15. nmap reference guide. Chapter 15. Nmap Reference Guide | Nmap Network Scanning. (n.d.). https://nmap.org/book/man.html

House, N. (2024, February 7). Nmap Cheat Sheet 2024: All the Commands & Flags. *StationX*. https://www.stationx.net/nmap-cheat-sheet/