



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

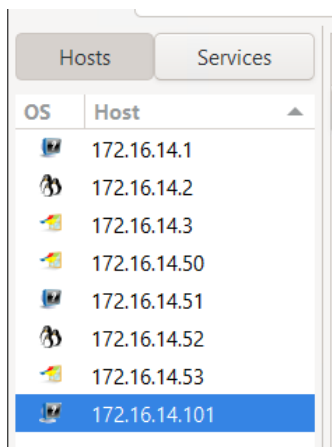
Below is a list of functions that were used in Zenmap (application used to find host/devices and services on a network) to gather information about the network and devices, along with a short description.

-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.



The screenshot shows the Zenmap application interface with the 'Hosts' tab selected. It displays a list of discovered hosts with their IP addresses and corresponding OS detection icons. The host 172.16.14.101 is highlighted in blue at the bottom of the list.

OS	Host
	172.16.14.1
	172.16.14.2
	172.16.14.3
	172.16.14.50
	172.16.14.51
	172.16.14.52
	172.16.14.53
	172.16.14.101

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

			File Edit Format View		
7/tcp	open	tcpwrapped	873/tcp	open	tcpwrapped
9/tcp	open	tcpwrapped	990/tcp	open	tcpwrapped
13/tcp	open	tcpwrapped	993/tcp	open	tcpwrapped
21/tcp	open	tcpwrapped	995/tcp	open	tcpwrapped
22/tcp	open	tcpwrapped	1025/tcp	open	tcpwrapped
23/tcp	open	tcpwrapped	1026/tcp	open	tcpwrapped
25/tcp	open	tcpwrapped	1027/tcp	open	tcpwrapped
26/tcp	open	tcpwrapped	1028/tcp	open	tcpwrapped
37/tcp	open	tcpwrapped	1029/tcp	open	tcpwrapped
53/tcp	open	tcpwrapped	1110/tcp	open	tcpwrapped
79/tcp	open	tcpwrapped	1433/tcp	open	tcpwrapped
80/tcp	open	tcpwrapped	1720/tcp	open	tcpwrapped
81/tcp	open	tcpwrapped	1723/tcp	open	tcpwrapped
88/tcp	open	tcpwrapped	1755/tcp	open	tcpwrapped
106/tcp	open	tcpwrapped	1900/tcp	open	tcpwrapped
110/tcp	open	tcpwrapped	2000/tcp	open	tcpwrapped
111/tcp	open	tcpwrapped	2001/tcp	open	tcpwrapped
113/tcp	open	tcpwrapped	2049/tcp	open	tcpwrapped
119/tcp	open	tcpwrapped	2121/tcp	open	tcpwrapped
135/tcp	open	tcpwrapped	2717/tcp	open	tcpwrapped
139/tcp	open	tcpwrapped	3000/tcp	open	tcpwrapped
143/tcp	open	tcpwrapped	3128/tcp	open	tcpwrapped
144/tcp	open	tcpwrapped	3306/tcp	open	tcpwrapped
179/tcp	open	tcpwrapped	3389/tcp	open	tcpwrapped
199/tcp	open	tcpwrapped	3986/tcp	open	tcpwrapped
389/tcp	open	tcpwrapped	4899/tcp	open	tcpwrapped
427/tcp	open	tcpwrapped	5000/tcp	open	tcpwrapped
443/tcp	open	tcpwrapped	5009/tcp	open	tcpwrapped
444/tcp	open	tcpwrapped	5051/tcp	open	tcpwrapped
445/tcp	open	tcpwrapped	5060/tcp	open	tcpwrapped
465/tcp	open	tcpwrapped	5101/tcp	open	tcpwrapped
513/tcp	open	tcpwrapped	5190/tcp	open	tcpwrapped
514/tcp	open	tcpwrapped	5357/tcp	open	tcpwrapped
515/tcp	open	tcpwrapped	5432/tcp	open	tcpwrapped
543/tcp	open	tcpwrapped	5631/tcp	open	tcpwrapped
544/tcp	open	tcpwrapped	5666/tcp	open	tcpwrapped
548/tcp	open	tcpwrapped	5800/tcp	open	tcpwrapped
554/tcp	open	tcpwrapped	5900/tcp	open	tcpwrapped
587/tcp	open	tcpwrapped	6000/tcp	open	tcpwrapped
631/tcp	open	tcpwrapped	6001/tcp	open	tcpwrapped
646/tcp	open	tcpwrapped	6646/tcp	open	tcpwrapped
			7070/tcp	open	tcpwrapped

(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)

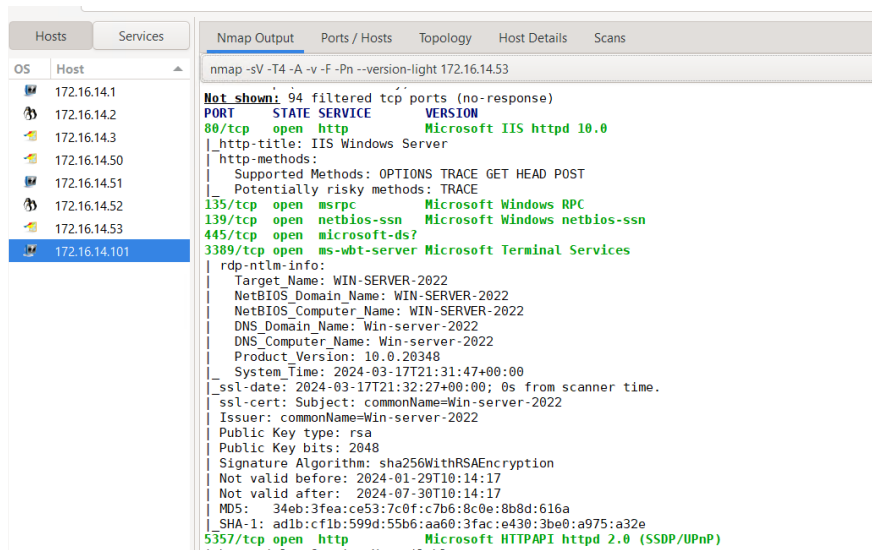
The screenshot shows the Nmap ScanTool interface. On the left, a list of hosts is displayed with their IP addresses: 172.16.14.1, 172.16.14.2, 172.16.14.3, 172.16.14.50, 172.16.14.51, 172.16.14.52, 172.16.14.53, and 172.16.14.101. The 'Nmap Output' tab is selected, showing the following scan results:

```

nmap -sn 172.16.14.0/24

Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-17 12:02 Pacific Daylight Time
Nmap scan report for 172.16.14.1
Host is up (0.0020s latency).
MAC Address: F4:CF:E2:70:A6:C0 (Cisco Systems)
Nmap scan report for 172.16.14.2
Host is up (0.0020s latency).
MAC Address: 00:50:56:9F:32:CA (VMware)
Nmap scan report for 172.16.14.50
Host is up (0.77s latency).
MAC Address: 50:01:00:02:00:01 (Unknown)
Nmap scan report for 172.16.14.51
Host is up (0.013s latency).
MAC Address: 50:01:00:07:00:01 (Unknown)
Nmap scan report for 172.16.14.52
Host is up (0.0010s latency).
MAC Address: 50:01:00:05:00:01 (Unknown)
Nmap scan report for 172.16.14.53
Host is up (0.0010s latency).
MAC Address: 50:01:00:01:00:01 (Unknown)
Nmap scan report for 172.16.14.101
Host is up (0.0020s latency).
MAC Address: 00:50:79:66:68:03 (Private)
Nmap scan report for 172.16.14.3
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 4.14 seconds
  
```

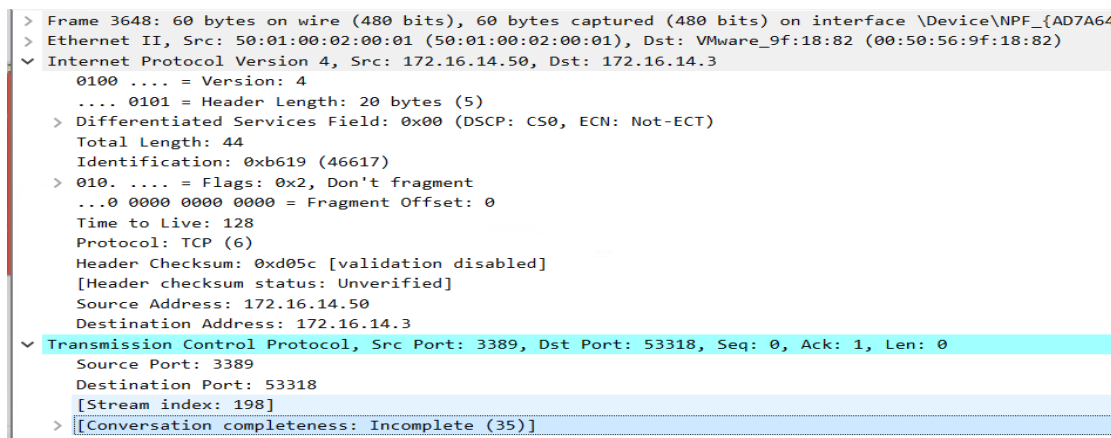
Now that we are given the host IP, searching for information on each host can be streamlined. Keeping to the same methodology of fastest option provided greatest information. With this in mind, [`nmap -sV -T4 -A -v -F -Pn --version-light 172.16.14.###`], gave the best results in one shot. (see below)



While this method was the most fruitful, it wasn't all complete. Since Windows devices and the Ubuntu Linux device 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

```
> Frame 3622: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F}
> Ethernet II, Src: 50:01:00:07:00:01 (50:01:00:07:00:01), Dst: VMware_9f:18:82 (00:50:56:9f:18:82)
✓ Internet Protocol Version 4, Src: 172.16.14.51, Dst: 172.16.14.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
    > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xc679 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.14.51
    Destination Address: 172.16.14.3
```

17.16.14.52 Linux - found on layer 3 network layer

```
> Frame 3797: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F}
> Ethernet II, Src: 50:01:00:05:00:01 (50:01:00:05:00:01), Dst: VMware_9f:18:82 (00:50:56:9f:18:82)
✓ Internet Protocol Version 4, Src: 172.16.14.52, Dst: 172.16.14.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
    > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xc678 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.14.52
    Destination Address: 172.16.14.3
```

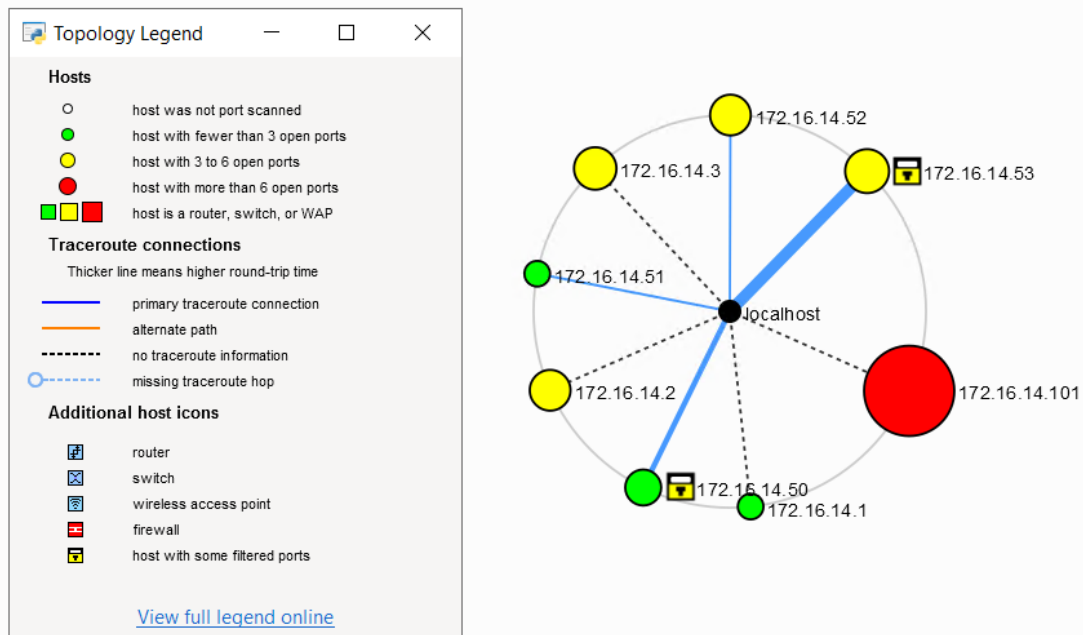
172.16.14.53 Windserver – found on layer 1 physical layer

```
✓ Frame 920: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F})
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 17, 2024 20:59:43.025779000 Pacific Daylight Time
  UTC Arrival Time: Mar 18, 2024 03:59:43.025779000 UTC
  Epoch Arrival Time: 1710734383.025779000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.036362000 seconds]
  [Time delta from previous displayed frame: 7.990831000 seconds]
  [Time since reference or first frame: 10.325571000 seconds]
  Frame Number: 920
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
  > Ethernet II, Src: 50:01:00:01:00:01 (50:01:00:01:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

172.16.14.101 VPC - found on layer 1 physical layer

```
✓ Frame 520: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{AD7A64F3-7947-42C6-AD1A-E8B653583B3F})
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 17, 2024 21:03:09.555649000 Pacific Daylight Time
  UTC Arrival Time: Mar 18, 2024 04:03:09.555649000 UTC
  Epoch Arrival Time: 1710734589.555649000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.012979000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 5.864220000 seconds]
  Frame Number: 520
  Frame Length: 64 bytes (512 bits)
  Capture Length: 64 bytes (512 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
  > Ethernet II, Src: 00:50:79:66:68:03 (00:50:79:66:68:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Address Resolution Protocol (request)
```


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/>