Network Administration Project

TABLE OF CONTENTS

Introduction:

This report aims to provide an analysis of the network and documentation of devices.

Tools used: Zenmap and Wireshark.

I employed Zenmap for device identification on the network and Wireshark to capture and analyze the network traffic. The data gathered includes detailed information about each device from Zenmap scans, along with the packet level details.

Methodology:

This report involves a systematic approach to gather, verify and document information about the devices within the network. The following steps outline the methodology used for this project.

- Turned on all the devices and tools.
- Identified all the devices using Zenmap scans and captured network packets using Wireshark to know the communication patterns.
- Physically accessed devices to double check the information obtained from Zenmap and Wireshark.
- Developed a topology diagram showing the network layout.

Network Device information:

Machine Designation	**Device Host Name**	**IP Address**	**MAC Address**	**Operating System, version**	**ARP Ping scan elapsed time**
Windows 1	Desktop-WI N10PRO	172.16.14. 50	50:01:00:02: 00:01	MS Window 10.0.17763.107	0.26s
Winserver	WIN-SERVER-2022	172.16.14. 53	50:01:00:01: 00:01	Microsoft Windows 2022 and 10.0.20348.	0.20s
Linux	User-pc	172.16.14. 52	50:01:00:05: 00:01	Ubuntu Version 20.04.6 LTS	0.19s
Kali Linux	Kali	172.16.14. 51	50:01:00:07: 00:01	KALI GNU/LINUX VERSION 6.1.0-Kali9-amd 64	0.19s
VPC	NA	172.16.14. 101	00:50:79: 66:68:03	NA	0.17s

Machine Designation: Windows

1.Nmap Scans:

```
Nmap scan report for 172.16.14.50
Host is up (0.0045s latency).
Not shown: 995 closed tcp ports (reset)
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?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DESKTOP-WIN10PR
|   NetBIOS_Domain_Name: DESKTOP-WIN10PR
|   NetBIOS_Computer_Name: DESKTOP-WIN10PR
|   DNS_Domain_Name: DESKTOP-WIN10PRO
|   DNS_Computer_Name: DESKTOP-WIN10PRO
|   Product_Version: 10.0.17763
|_  System_Time: 2024-03-11T16:58:05+00:00
| ssl-cert: Subject: commonName=DESKTOP-WIN10PRO
| Issuer: commonName=DESKTOP-WIN10PRO
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-11-13T12:13:00
| Not valid after:  2024-05-14T12:13:00
| MD5:   0bf8:bff2:baf2:48b1:bcaf:e2f1:994c:a5f6
|_SHA-1: f536:d8a6:b8e5:cebb:8859:86d3:2243:e899:3f0f:a0bc
|_ssl-date: 2024-03-11T16:58:29+00:00; -2s from scanner time.
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Ports

The 995 ports scanned but not shown below are in state: **closed**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

FIG: The above two screenshots represent the scans with their open ports

2.Process of Discovery:

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device's IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

2.a. Port 135 – msrpc(Microsoft WindowsRPC):

OSI Layer-4

Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server.

2.b. Port 139 – netbios-ssn(Microsoft Windows netbios-ssn):

OSI layer 4

NetBIOS is a protocol used for file and print sharing under all current versions of Windows. While this is not a problem, the way that the protocol is implemented can be. There are a few vulnerabilities associated with leaving this port open.

2.c. Port 445 –microsoft-ds:

OSI layer 7

TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445.

2.d. Port 3389 –microsoft-ds:
OSI layer 7
This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389. Individual connections will timeout, but a low bandwidth
continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

2.e. Port 5357:
OSI layer 7
Used by Microsoft Network Discovery should be filtered for public networks. Disabling Network Discovery for any public network profile should close the port unless it's being used by another potentially malicious service.
To disable Network Discovery for a public profile, navigate to:
- Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings
- disable Network Discovery for any public network

Machine designation: **Winserver**

3. Nmap Scans:

```
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

172.16.14.53(online)

Address
- 172.16.14.53 - (ipv4)
- 50:01:00:01:00:01 - (mac)

Ports
The 990 ports scanned but not shown below are in state: **filtered**

Port	State	Service	Reason	Product	Version	Extra info
80	tcp open	http	syn-ack	Microsoft IIS httpd	10.0	
135	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp open	microsoft-ds	syn-ack			
1801	tcp open	msmq	syn-ack			
2103	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
2105	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
2107	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
3389	tcp open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
5357	tcp open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP

FIG: The above two screenshots represent the Zenmap scans with their open ports

4. Process of Discovery:

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device's IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

4.a. Port 80(Microsoft IIS httpd):

OSI Layer-7
Hyper Text Transfer Protocol (HTTP) - port used for web traffic. Some broadband routers run a web server on port 80 or 8080 for remote management. WAN Administration can (and should, in most cases) be disabled using the Web Admin interface. Any Desk remote desktop software uses TCP ports 80, 443, 6568, 7070 (direct line connection)

4.b. Port 135 – msrpc(Microsoft WindowsRPC):

OSI Layer-4
Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server.

4.c. Port 139 – netbios-ssn(Microsoft Windows netbios-ssn):

OSI layer 4
NetBIOS is a protocol used for file and print sharing under all current versions of Windows. While this is not a problem, the way that the protocol is implemented can be. There are a few vulnerabilities associated with leaving this port open.

4.d. Port 445 –microsoft-ds:

OSI layer 7
TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445.

4.e. Port 3389 –microsoft-ds:

OSI layer 7
This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389.

Individual connections will timeout, but a low bandwidth continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

4.f. Port 5357:

OSI layer 7
Used by Microsoft Network Discovery should be filtered for public networks. Disabling Network Discovery for any public network profile should close the port unless it's being used by another potentially malicious service.

To disable Network Discovery for a public profile, navigate to:
- Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings
- disable Network Discovery for any public network.

Machine designation: **Linux**

5. Nmap Scan:

Nmap Scan Report - Scanned at Tue Mar 12 10:45:35 2024

Scan Summary

Nmap 7.94 was initiated at Tue Mar 12 10:45:35 2024 with these arguments:
nmap -T4 -A -v 172.16.14.52

Verbosity: 1; Debug level 0

172.16.14.52(online)

Address
- 172.16.14.52 - (ipv4)
- 50:01:00:05:00:01 - (mac)

Ports

The 997 ports scanned but not shown below are in state: **closed**

Port	State	Service	Reason	Product	Version	Extra info
80 tcp	open	http	syn-ack	Apache httpd	2.4.41	(Ubuntu)
3306 tcp	open	mysql	syn-ack	MySQL		unauthorized
3389 tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Service		

Remote Operating System Detection
- Used port: **80/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **38892/udp (closed)**
- OS match: **Linux 4.15 - 5.8 (100%)**

Traceroute Information
- Traceroute data generated using port /

Hop	Rtt	IP	Host
1	2.40	172.16.14.52	

Misc Metrics

Metric	Value
Ping Results	
System Uptime	2107344 seconds (last reboot: Sat Feb 17 00:23:32 2024)
TCP Sequence Prediction	Difficulty=256 (Good luck!)
IP ID Sequence Generation	All zeros

FIG: The above screenshot represents the Zenmap scans with their open ports

6. Process of Discovery:

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device's IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

6.a. Port 80 –(syn-ack Apache httpd):
OSI Layer-7
Hyper Text Transfer Protocol (HTTP) - port used for web traffic. Some broadband routers run a web server on port 80 or 8080 for remote management. WAN Administration can (and should, in most cases) be disabled using the Web Admin interface. Any Desk remote desktop software uses TCP ports 80, 443, 6568, 7070 (direct line connection).

6.b. Port 3306-MySQL):
OSI Layer-7
MySQL database server connections. MySQL 5.5.8, when running on Windows, allows remote attackers to cause a denial of service via a crafted packet to TCP port 3306.

6.c. Port 3389 –(microsoft Terminal Service):
OSI Layer-7
This port is vulnerable to Denial-of-Service attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389.

Individual connections will timeout, but a low bandwidth continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection.

Machine designation: **Kalilinux**

7. Nmap Scan:

Nmap Scan Report - Scanned at Mon Mar 11 11:22:41 2024

Scan Summary

Nmap 7.94 was initiated at Mon Mar 11 11:22:41 2024 with these arguments:
nmap -T4 -A -v 172.16.14.51

Verbosity: 1; Debug level 0

172.16.14.51(online)

Address
- 172.16.14.51 - (ipv4)
- 50:01:00:07:00:01 - (mac)

Ports
The 1000 ports scanned but not shown below are in state: **closed**

Remote Operating System Detection
Unable to identify operating system.

- Used port: **1/tcp (closed)**
- Used port: **39495/udp (closed)**

Traceroute Information
- Traceroute data generated using port /

Hop	Rtt	IP	Host
1	3.02	172.16.14.51	

Misc Metrics

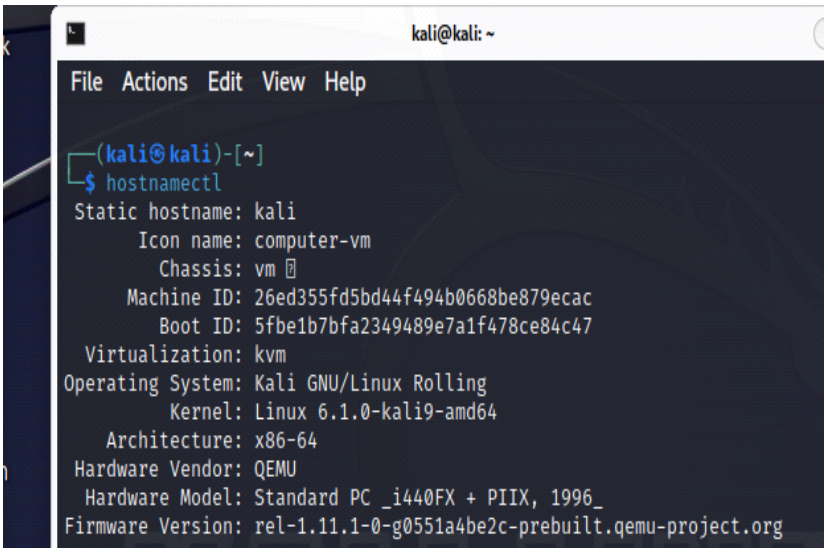
Metric	Value
Ping Results	

FIG: The above screenshot represents the Zenmap scans with their open ports

8. Process of Discovery:

To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device's IP address. Afterward, I compared the Zenmap results with the documentation of system information and inspected the network traffic in Wireshark.

Unable to detect the operating system in Zenmap scans. But below attaching the screenshot of system information when checked externally.



Machine designation: **VPC**

9. Nmap Scan:

Nmap Scan Report - Scanned at Mon Mar 11 15:06:10 2024

Scan Summary

Nmap 7.94 was initiated at Mon Mar 11 15:06:10 2024 with these arguments:
nmap -T4 -A -v 172.16.14.101

Verbosity: 1; Debug level 0

172.16.14.101(online)

Address

- 172.16.14.101 - (ipv4)
- 00:50:79:66:68:03 - Private (mac)

Ports

Port	State	Service	Reason	Product	Version	Extra info
1	tcp open	tcpwrapped	syn-ack			
3	tcp open	tcpwrapped	syn-ack			
4	tcp open	tcpwrapped	syn-ack			
6	tcp open	tcpwrapped	syn-ack			
7	tcp open	tcpwrapped	syn-ack			
9	tcp open	tcpwrapped	syn-ack			
13	tcp open	tcpwrapped	syn-ack			
17	tcp open	tcpwrapped	syn-ack			
19	tcp open	tcpwrapped	syn-ack			
20	tcp open	tcpwrapped	syn-ack			
21	tcp open	tcpwrapped	syn-ack			
22	tcp open	tcpwrapped	syn-ack			
23	tcp open	tcpwrapped	syn-ack			
24	tcp open	tcpwrapped	syn-ack			
25	tcp open	tcpwrapped	syn-ack			
26	tcp open	tcpwrapped	syn-ack			
30	tcp open	tcpwrapped	syn-ack			
32	tcp open	tcpwrapped	syn-ack			
33	tcp open	tcpwrapped	syn-ack			
37	tcp open	tcpwrapped	syn-ack			
42	tcp open	tcpwrapped	syn-ack			
43	tcp open	tcpwrapped	syn-ack			
49	tcp open	tcpwrapped	syn-ack			
53	tcp open	tcpwrapped	syn-ack			
70	tcp open	tcpwrapped	syn-ack			
79	tcp open	tcpwrapped	syn-ack			
56737	tcp open	tcpwrapped	syn-ack			
56738	tcp open	tcpwrapped	syn-ack			
57294	tcp open	tcpwrapped	syn-ack			
57797	tcp open	tcpwrapped	syn-ack			
58080	tcp open	tcpwrapped	syn-ack			
60020	tcp open	tcpwrapped	syn-ack			
60443	tcp open	tcpwrapped	syn-ack			
61532	tcp open	tcpwrapped	syn-ack			
61900	tcp open	tcpwrapped	syn-ack			
62078	tcp open	tcpwrapped	syn-ack			
63331	tcp open	tcpwrapped	syn-ack			
64623	tcp open	tcpwrapped	syn-ack			
64680	tcp open	tcpwrapped	syn-ack			
65000	tcp open	tcpwrapped	syn-ack			
65129	tcp open	tcpwrapped	syn-ack			
65389	tcp open	tcpwrapped	syn-ack			

Remote Operating System Detection

Unable to identify operating system.

- Used port: **9100/tcp (open)**

Traceroute Information

- Traceroute data generated using port /

Hop	Rtt	IP	Host
1	1.74	172.16.14.101	

Misc Metrics

Metric	Value
Ping Results	
TCP Sequence Prediction	Difficulty=255 (Good luck!)
IP ID Sequence Generation	Randomized

file:///C:/Users/user1/Desktop/wireshark%20and%20zenmap%20captures/VPC.xml 3/12/2024
Nmap Scan Report - Scanned at Mon Mar 11 15:06:10 2024 Page 22 of 22

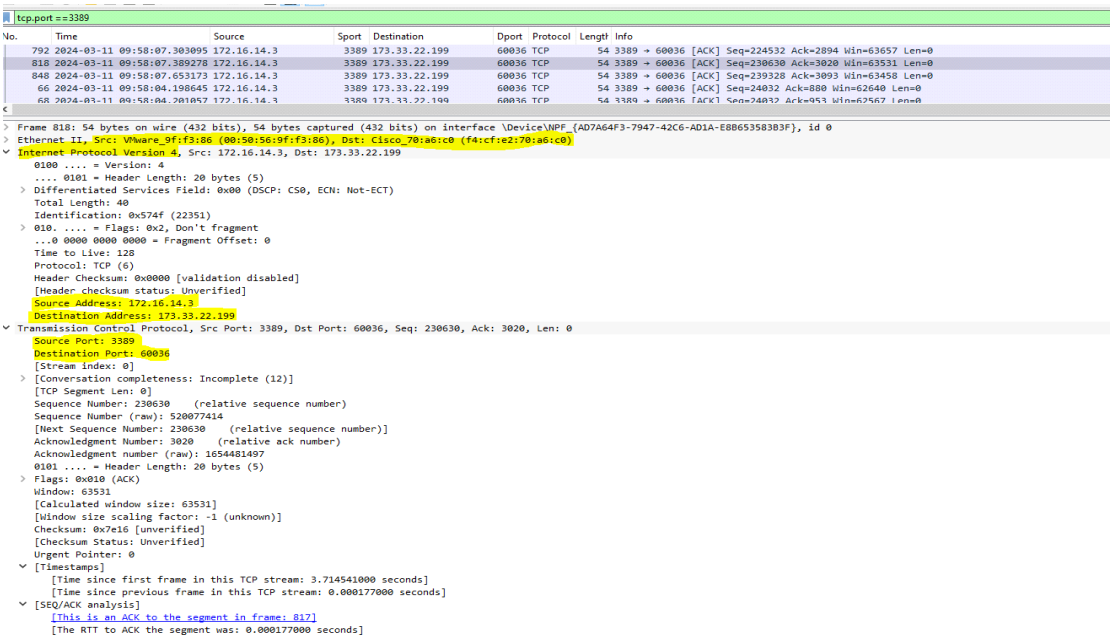
Fig: Zenmap scan on VPC.

10. Process of Discovery:

For the VPC, I acquired a manual IP address in the terminal using the command “ip dhcp”. Subsequently, I conducted the Zenmap scan using that IP address. To validate the information gathered by Zenmap, I began documenting the network system details from all the devices. Then, I carried out the Zenmap scan utilizing the device’s IP address. In addition to the Zenmap scan, I initiated the packet capture in Wireshark by clicking on the start button. After collecting the required information, I stopped Wireshark from capturing packets.

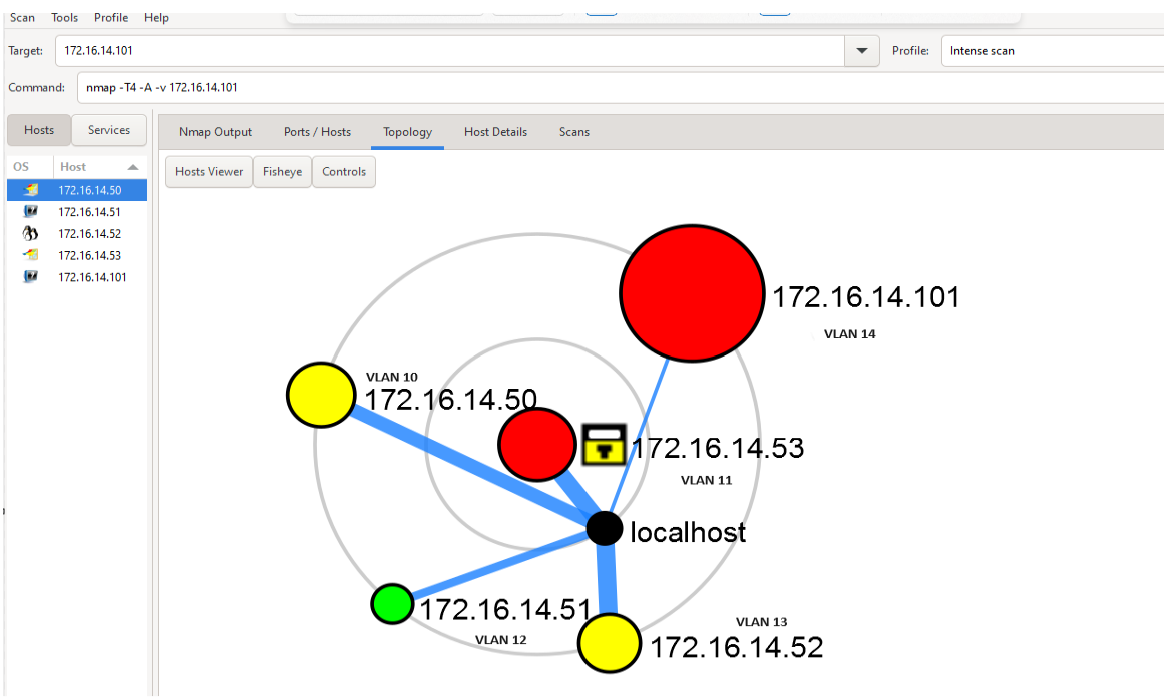
Wireshark Captures:

I initiated packet capture by launching the Wireshark application, selecting the desired network interface. Utilized tools like Zenmap for network scanning and examined the results within Wireshark. Applied filters to pinpoint specific packets based on the port numbers. Analyzed the captured packets to assess network activity and gather information.



The above provided screenshot represents a sequence of packet captures.

Topography:



Topology Representation collected from Zenmap.

In our network topology, we have implemented VLANs to enhance our overall network performance and security. It allows us to logically segment our network into distinct domains, each with its own VLAN ID and associated network devices.

Conclusion:

In conclusion, strengthening network security involves the implementation of VLANs as they serve to isolate various types of traffic, providing a mechanism to restrict unauthorized access effectively.

References:

Port 80, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=80

Port 139, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=139

Port 135, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=135

Port 445, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=445

Port 3389, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=3389

Port 3306, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=3389

Port 5357, Details. n.d.SpeedGuide. https://www.speedguide.net/port.php?port=5357

Zenmap version 7.94, developed by Nmap Software LLC. https://nmap.org/zenmap/)

Wireshark Version 4.2.2(v4.2.2-0-g404592842786), developed by Gerald Combs and contributors. https://www.wireshark.org/

Linux command cheat sheet https://phoenixnap.com/kb/linux-commands-cheat-sheet