Project : Network Administration

Submitted By: Sukhvir Kaur Sahota

**Table of Contents**

1. Introduction Page -2
2. Network Devices Information Page -3
3. Information Collection Methodology Page -4

3.1 For Windows1 From EVE Topology Page -4

3.2 For Kali From EVE Topology Page -6

3.3 For Linux From EVE Topology Page -7

3.4 For WinServer1 From EVE Topology Page -8

1. OSI Layer Model Page -11
2. Topology Page -13
3. Reference and Citation Page -14

**1. Introduction**

This report is about the basic functions done by Network administration in their work and the tools and technologies which help with the job. Let's start with understanding network administration.

According to Solarwinds, Network Administration’s goal is to manage, monitor, protect and maintain the company's network(1). To perform the job various packet analysis tools are available in the market. We are going to discuss tools such as Wireshark, Zenmap and nmap and how they play an important role in finding and optimizing the performance of the system.

Zenmap and nmap are the same tools and both are popular tools for scanning the ports , services and IP ranges. Nmap security scanner is a command-line-based multi-platform (Windows, Mac OS X, Linux etc.) network scanning application whereas, Zenmap is the official Nmap security scanner GUI (Graphical User Interface) version of Nmap.(3)

Wireshark is another free network packet analyser tool which captures data in as much detail as possible and the captured data can be used in real time as well as offline. Best part of it is , it allows you to break down the packet into categories for deep analysis.(4)(5). The Zenmap(Image 1) and Wireshark(Image 2) overview looks like the Images below.

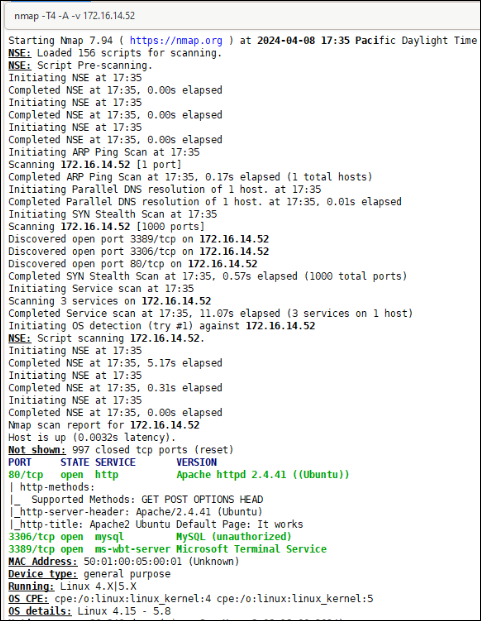


Image 1- Zenmap sample

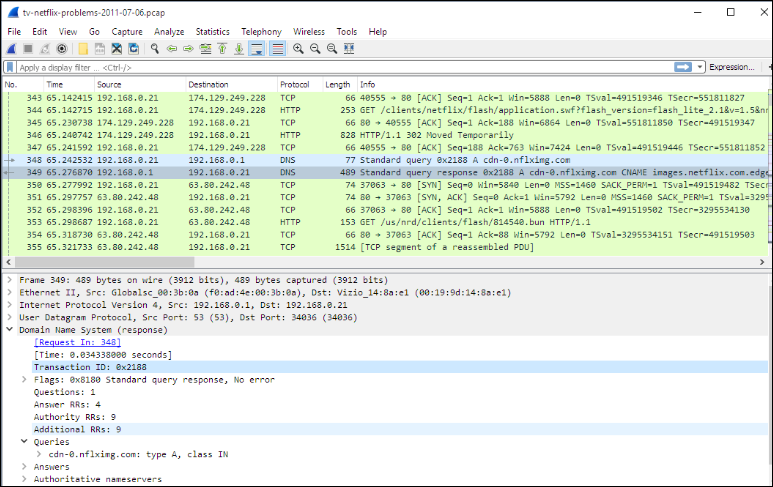


Image 2- Wireshark Sample

**2. Network Devices Information**

For this project we are working on EVE Topology in the JumpHost of Remote Desktop connection. The EVE Topology consists of 5 Machines as shown in the Image 3. We have 2 windows servers named Windows 1 and Winserver, Kali machine and Linux server.

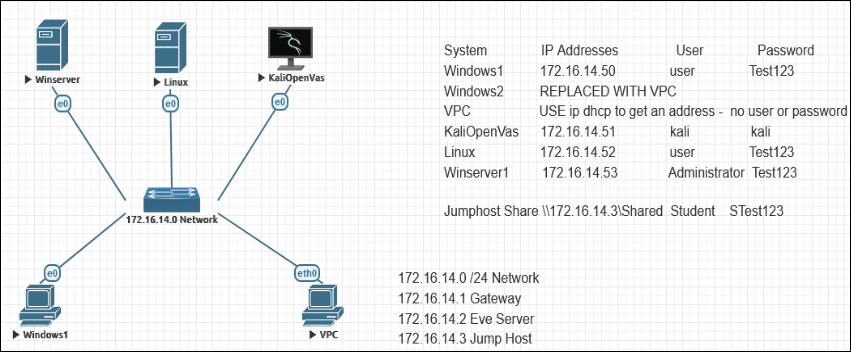


Image 3: EVE Topology

For every System shown in topology, my goal is to collect information of the

* Device details such as Hostname and Machine Designation.
* IP address.
* What Operating system each device is on and the version used.
* Open Ports for each device if any (NOTE: I will discuss with my team if the open ports are required for our organization’s daily goals and if not I would recommend closing them).
* ARP Ping Scan’s escape time.

**3. Information Collection Methodology**

To Collect the information of every Machine, I have used the Zenmap on the Jump Host and for additional information I used nmap on the Kali machine as well. To cross check the information I also used the analysis on wireshark to match the details.

Steps performed to collect information

1. In the JumpHost machine of my Virtual environment, Open Wireshark.
2. Start recording on the Ethernet0 connection of wireshark and capture the PCAP file while running the commands in Zenmap or the command line.
3. Do Intense scan on Zenmap GUI to complete scan of each machine of EVE Topology. I used the following commands T4 -A -v <Ip-address>, where

* T4 - Aggressive scan
* -A - Enabled OS detection, version detection, script scanning, and traceroute
* -v - Version details
* <Ip-address> - Ip address of device which is mentioned in Topology diagram details.

1. Once the scan is completed, record and capture information of Machine Designation, Device host name, IP address, MAC address, Operating system and version, Open Port with associated services, ARP Ping Scan elapsed time.
2. Crosscheck references the Information captured from Zenmap GUI with Wireshark PCAP file.

The points below give you more details on collected data.

**3.1 For Windows1 From EVE Topology**

For Collecting the following information I used Zenmap Intense Scan with command nmap -T4 -A -v 172.16.14.50.

The following points shows the Scan results on

* Machine Designation : Windows 1 (Found from Image 3 -Topology Diagram)
* Device Host Name



* Ip 172.16.14.50



* MAC address 50:01:00:02:00:01



* The Target name info gives details on device name and Aggressive OS guesses section shows the version Xp of windows with version SP2.
* 2 open ports 3389 which can be used for ms-wet-server and 5357 for http.
* ARP PIng Scan elapsed time of 0.17seconds.



Image 4 is from Wireshark capture which represents the connection success from Jumphost to Windows 1 machine.

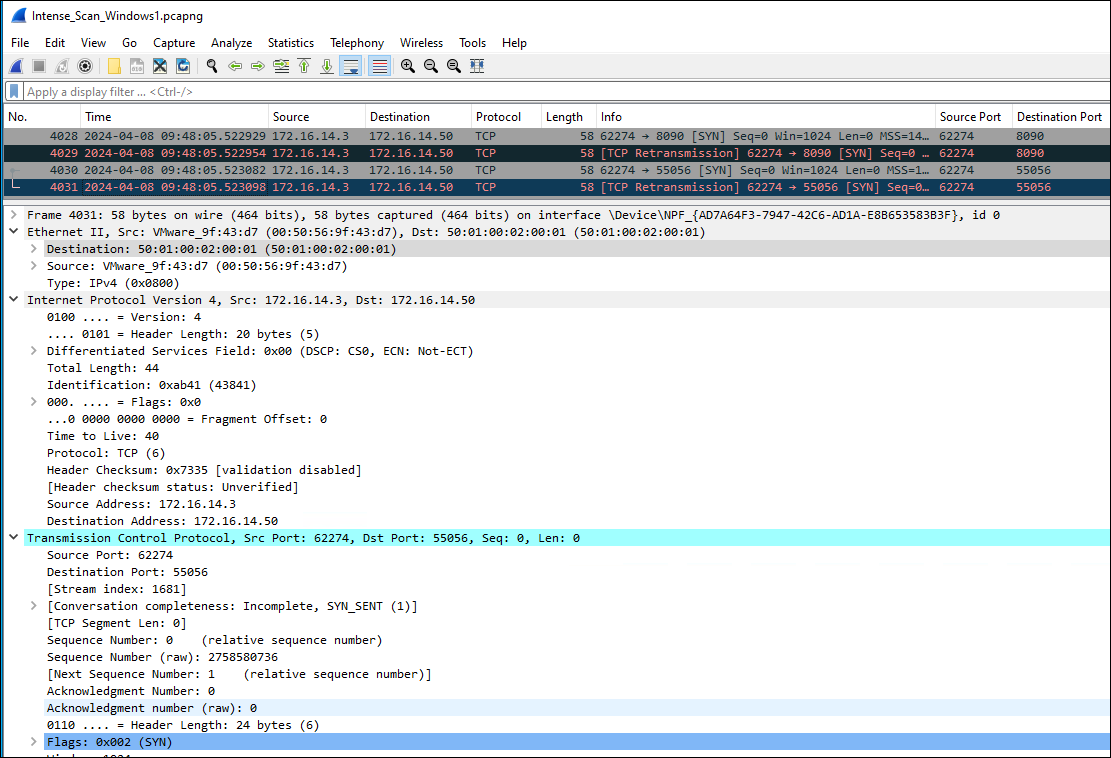


Image 4

**3.2 For Kali From EVE Topology**

For Collecting the following information I used Zenmap Intense Scan with command nmap -T4 -A -v 172.16.. I used “$sudo nmap 172.16.14.51” to capture details of Open Ports and OS versions because all details were not captured by Zenmap.

The following information has been collected from Zenmap

* Machine Designation : KaliOpenVas (Found from Image 3 -Topology Diagram)
* Device hostname: command “$ whoami”



* Ip 172.16.14.51



* MAC address 50:01:00:07:00:01

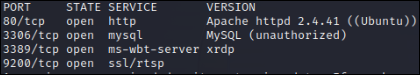


* ARP PIng Scan elapsed time of 0.17seconds



* 4 Open ports ( From Kali, command “$sudo nmap 172.16.14.51”)

1. 80 - http
2. 3306- mysql
3. 3389 -ms-wbt-server
4. 9200 - ssl/rtsp



* OS and version details (From Kali, command “$sudo nmap 172.16.14.51”)



Image 5 is from Wireshark capture which represent the connection success from Jumphost to Kali machine

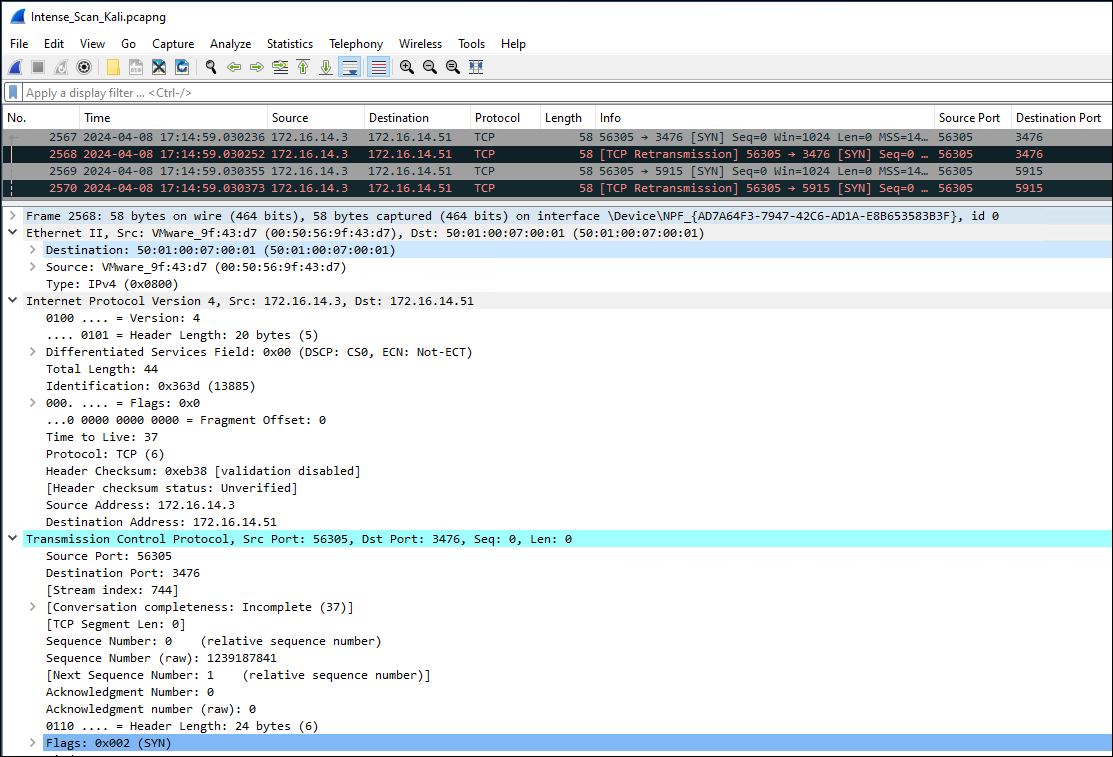


Image 5

**3.3 For Linux From EVE Topology**

For Collecting the information I used Zenmap Intense Scan with command nmap -T4 -A -v 172.16.14.52. The device hostname from Linux command terminal, the zenmap was not showing that detail so had to check it manually on linux machine via command $hostname.

The following information has been collected

* Machine Designation : Linux (Found from Image 3 -Topology Diagram)
* Device hostname from Linux command terminal, command $hostname.



* Ip 172.16.14.52



* MAC address 50:01:00:05:00:01

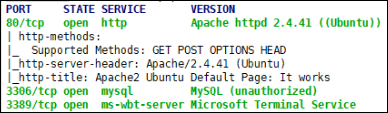


* 3 Open ports

1. 80 - http,

2. 3306- mysql

3. 3389 -ms-wbt-server



* OS details which shows its Linux 4.15 - V5.8



* ARP Ping Scan elapsed time



Image 6 is from Wireshark capture which represents the connection success from Jumphost to Linux machines.

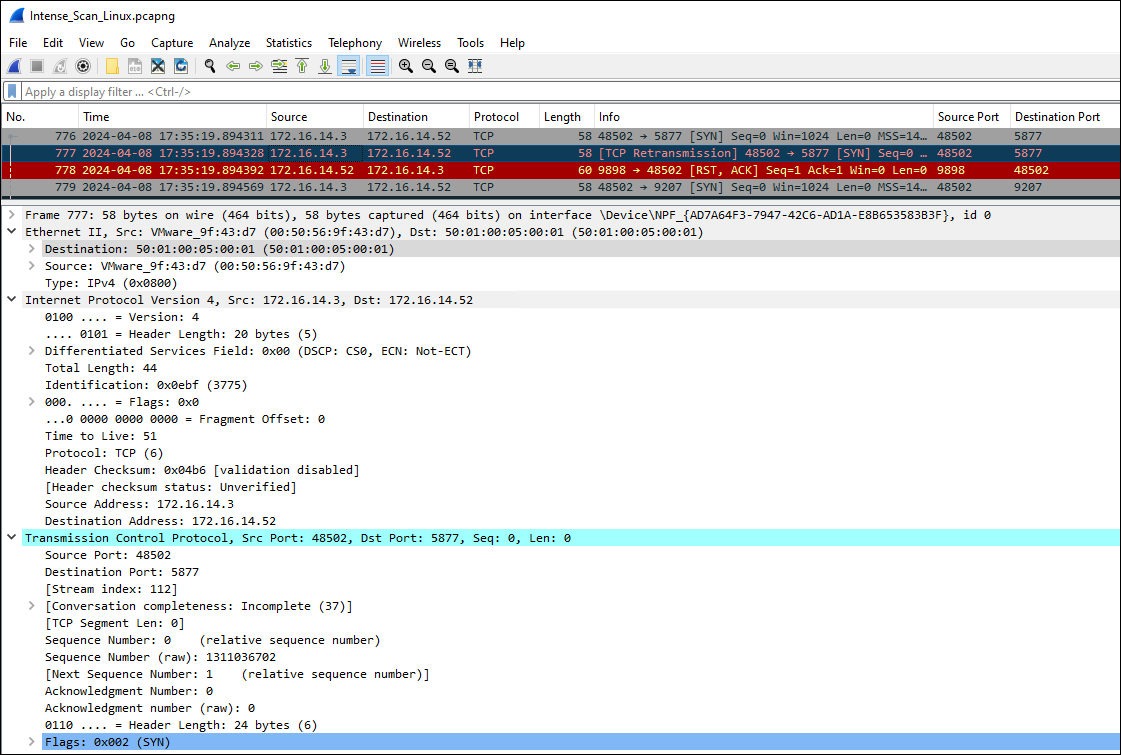


Image 6

**3.4 For WinServer From EVE Topology**

For Collecting the information I used Zenmap Intense Scan with command nmap -T4 -A -v 172.16.14.53.

The following are the Scan results

* Machine Designation : WinServer (Found from Image 3 -Topology Diagram)
* Device hostname



* Ip 172.16.14.53



* MAC address 50:01:00:01:00:01

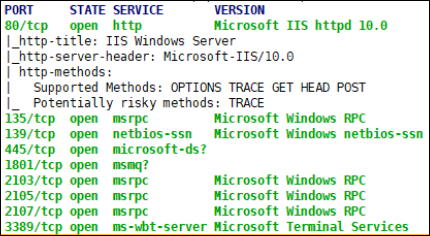


* OS details: Windows server 2022 Version



* 10 Open ports

1. 80- http
2. 135 - ms rpc
3. 139 - netbios-ssn
4. 445 - microdsoft-ds?
5. 1801 - msmq?
6. 2103 - ms rpc
7. 2105 -ms rpc
8. 2107 - ms rpc
9. 3389 - ms -wbt-server
10. 5357 - http



* ARP PIng Scan elapsed time of 0.17seconds



Image 7 is from Wireshark capture which represents the connection success from Jumphost to Winserver machine**.**

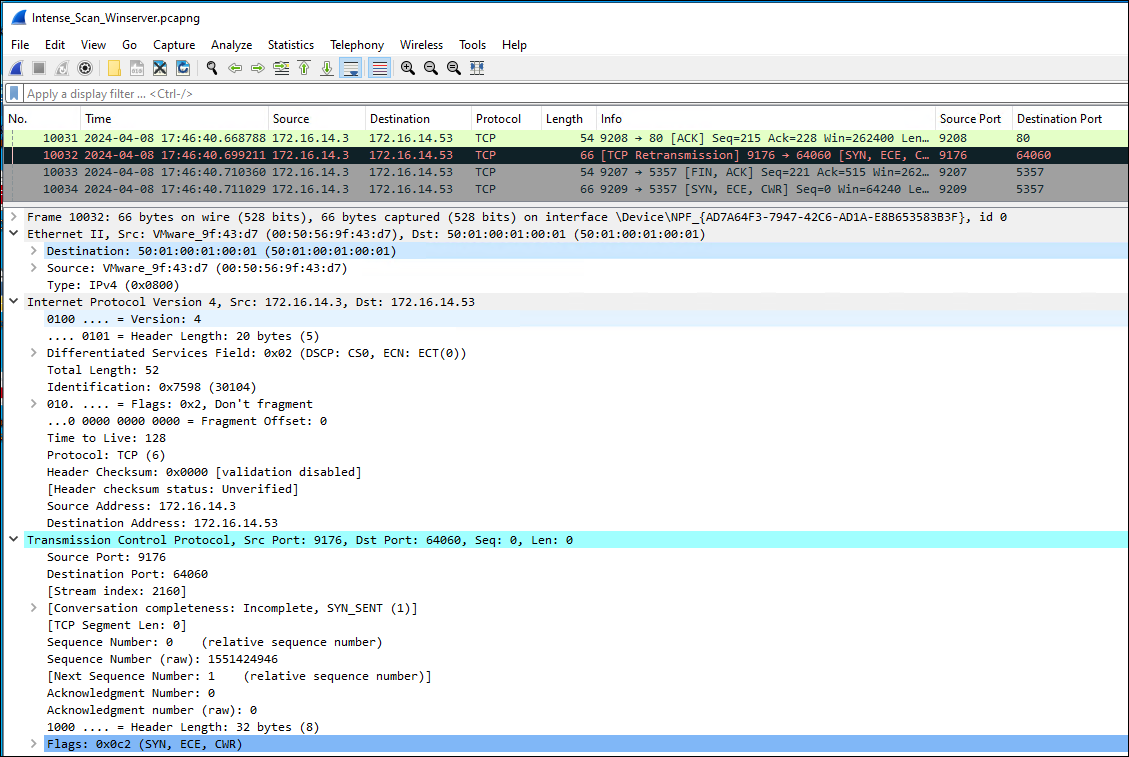
****

Image 7

The Table Shows the details of all Machines.

|  | **Windows1** | **KaliOpenVas** | **Linux** | **Winserver1** |
| --- | --- | --- | --- | --- |
| **Machine designation** | Windows 1 | Kali | Linux | Winserver 1 |
| **Device Host Name** | DESKTOP-WIN10PRO | kali | user-pc | WIN-SERVER-2022 |
| **IP address** | 172.16.14.50 | 172.16.14.51 | 172.16.14.52 | 172.16.14.53 |
| **MAC address** | 50:01:00:02:00:01 | 50:01:00:07:00:01 | 50:01:00:05:00:01 | 50:01:00:01:00:01 |
| **Operating System & version** | Microsoft Windows Xp | Apache httpd 2.4.41 ((Ubuntu)) | Linux 4.15 -5.8 | Microsoft Windows server 2022 |
| **Open ports with associated services** | 3389- ms-wbt-server  5357- http | 80 -http  3306 - mysql  3389 - ms-wbt-server  9200 - ssl/rtsp | 80 - http  3306- mysql  3389 -ms-wbt-server | 80- http  135 - ms rpc  139 - netbios-ssn  445 - microdsoft-ds?  1801 - msmq?  2103 - ms rpc  2105 -ms rpc  2107 - ms rpc  3389 - ms -wbt-server  5357 - http |
| **ARP Ping Scan elapsed time** | 0.17s | 0.17s | 0.17s | 017s |

**4. OSI Layer**

OSI layer consists of 7 layers and every layer stores Information of different protocols. In this Project we focus on 3 layers.

*Layer 2:* Data Link Layer which contains the Mac address .

*Layer 3:* Network Layer: which represents the IP address along with version

*Layer 4:* Transport Layer, which represents Port Number.

In All wireshark Images Every selected packet has Information of Source and destination, IP version, Source and destination port and many more. Below are the screenshots showing where to locate the data on Wireshark captures for all 4 machines.

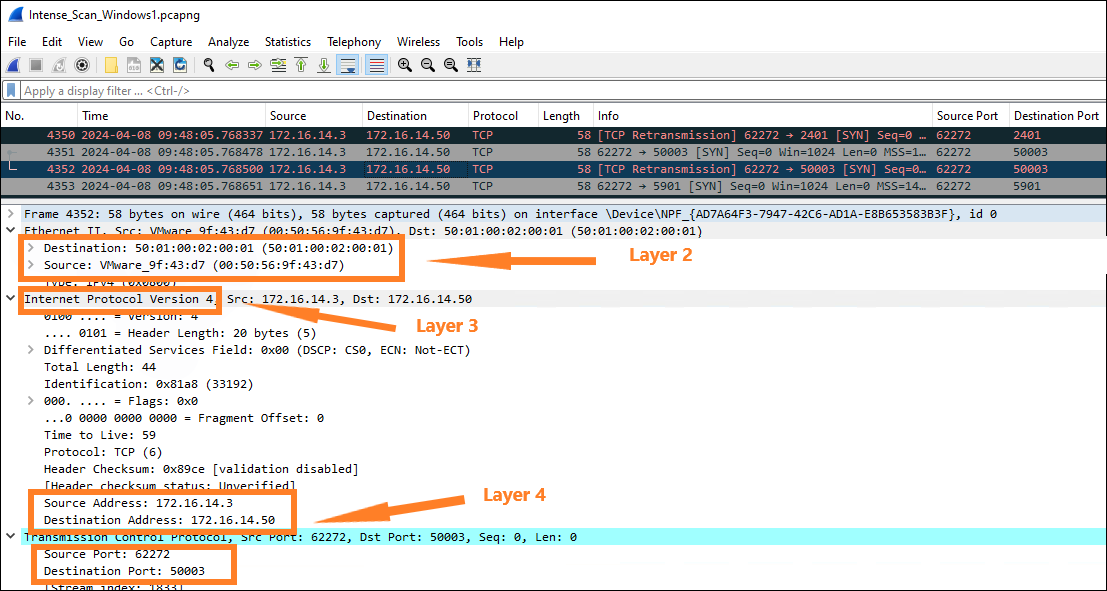


Image 8 - Windows1

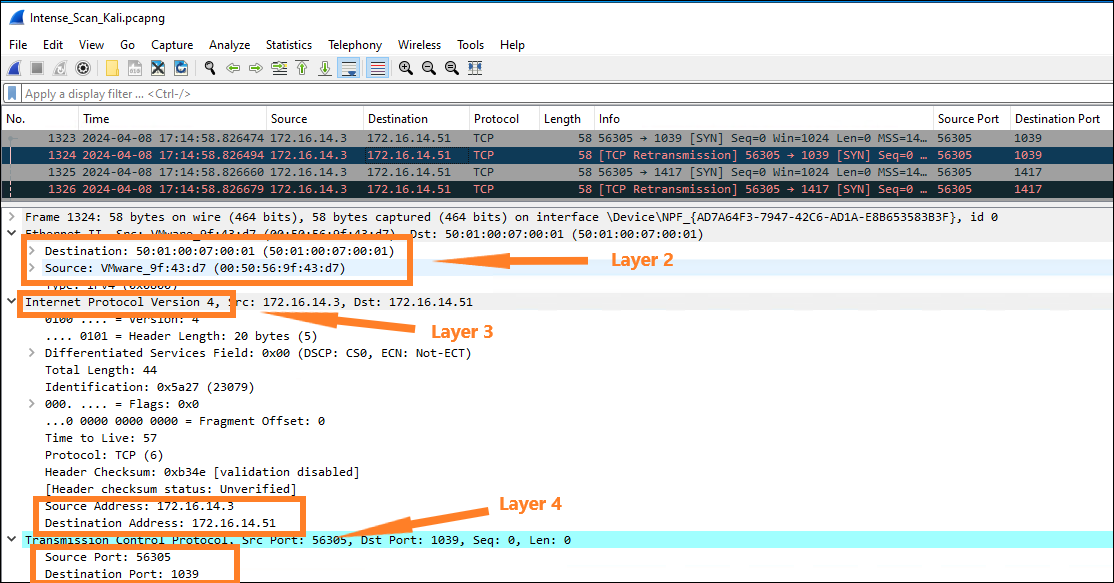


Image 9 - Kali

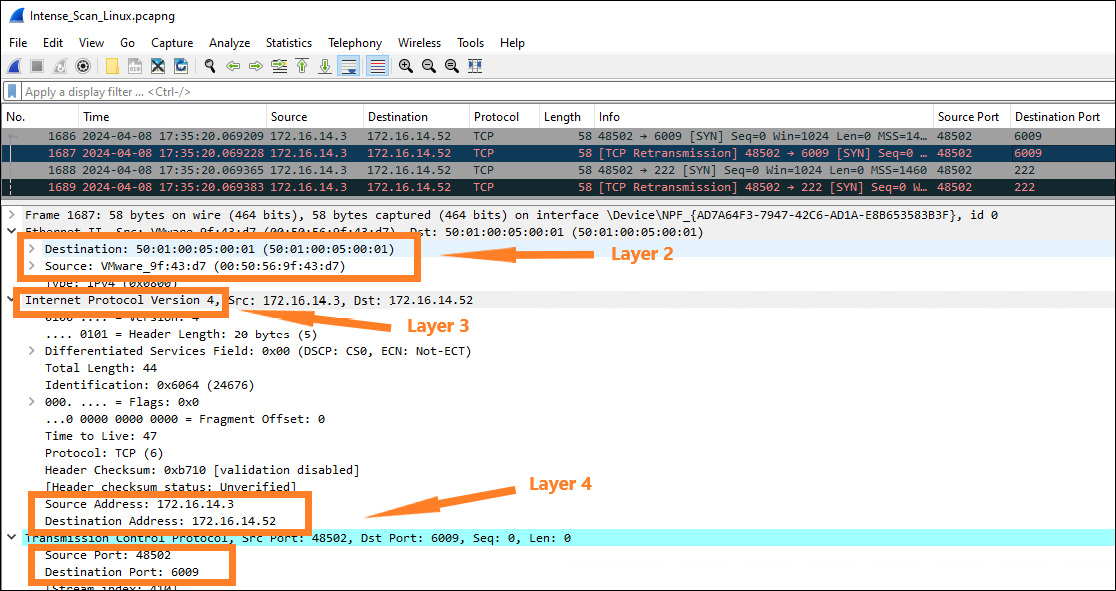


Image 10 -Linux

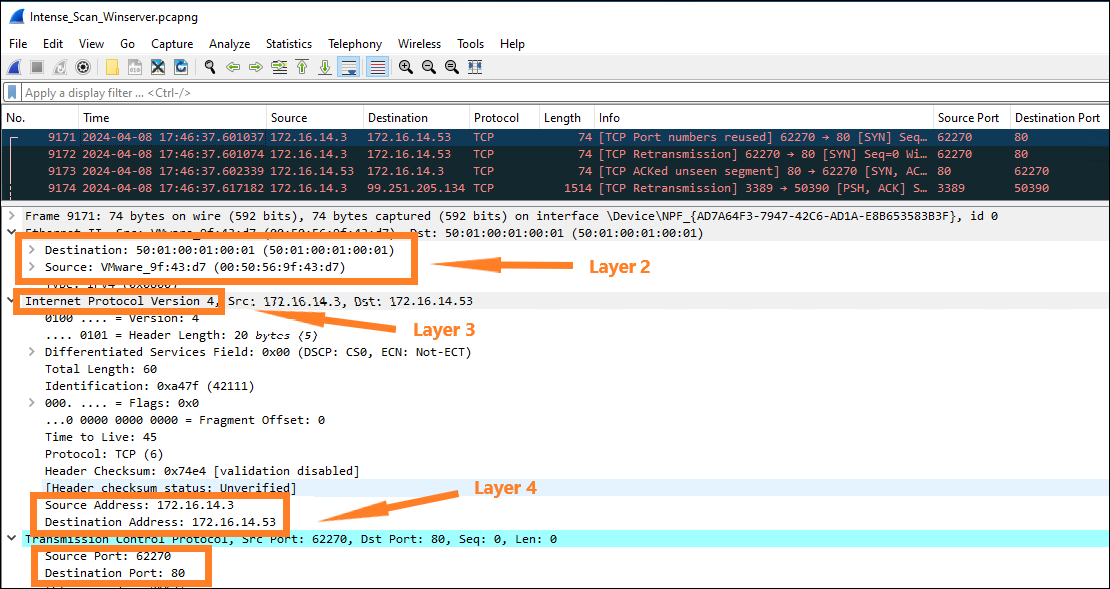


Image 11 -Winserver

**5. Topology Diagram**

In the topology Diagram to make it a bit secure we can use VLAN and firewall.

Firewall will provide an extra layer of protection. VLANs can improve performance for devices on them by reducing the amount of traffic a given endpoint sees and processes. VLANs break up broadcast domains, reducing the number of other hosts from which any given device sees broadcasts(2).

The main reason to use VLANs is that it allows you to segment your physical network into smaller and more secure subnets, which in turn can reduce the risk of data breaches or unauthorized access. The VLAN switch is a network switch that has the capability to create multiple virtual networks on a single physical infrastructure, allowing for better organization, security, and performance of the network.(6)

The table shows how I added VLAN for additional security and the Image shows how it will look in the topology Diagram.

| **System** | **IP address range** | **VLAN assignment** |
| --- | --- | --- |
| Windows1 | 192.168.10.0 | 10 |
| Kali | 192.168.20.0 | 20 |
| Linux | 192.168.15.0 | 15 |
| VPC | 192.168.25.0 | 25 |
| WinServer1 | 192.168.30.0 | 30 |

****

Image - 12

**6. References and Citation**

1. *What is network administration? - IT Glossary | SolarWinds*. (n.d.). <https://www.solarwinds.com/resources/it-glossary/network-administration>
2. Slattery, T., & Burke, J. (2022, June 3). VLAN (virtual LAN). Networking. https://www.techtarget.com/searchnetworking/definition/virtual-LAN
3. Alahmad, Y. (2023, October 25). Zenmap vs Nmap: Which One to Use (and When)? StationX. <https://www.stationx.net/zenmap-vs-nmap/#:~:text=Nmap%20security%20scanner%20is%20a%20command-line-based%20multi-platform%20%28Windows%2C,scanner%20GUI%20%28Graphical%20User%20Interface%29%20version%20of%20Nmap>.
4. What is Wireshark and how to use it | Cybersecurity | CompTIA. (n.d.). CompTIA. <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>
5. Chapter 1. Introduction. (n.d.). <https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs>
6. What is a VLAN? (n.d.). <https://web.compass.lighthouselabs.ca/p/14/days/w01d3/activities/2798>