Network Administration Project

**Table of contents:**

* **Introduction**
* **Methodology**
* **Network Device Information**
* **Analysis and Documentation**
* **Conclusion**
* **References**

# 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.
* Included screenshots from Zenmap and Wireshark to visually support the presented findings.
* Developed a topology diagram showing the network layout.

# Network Device information:

**Machine designation**: **Windows 1**

**Device Host Name**: DESKTOP-WIN10PR

**IP address**: 172.16.14.50

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

**Operating System & version**: microsoft: windows\_xp and 10.0.17763

**Open ports with associated services:**

* Port 135
* Port 139
* Port 445
* Port 3389
* Port 5357

**ARP Ping Scan elapsed time:** Completed ARP Ping Scan at 18:20, 0.26s elapsed (1 total hosts).

**Wireshark Analysis:** Monitored communication on the ports 3389 and 5357.

**Machine designation**: **Winserver**

**Device Host Name**: win-server-2022

**IP address**: 172.16.14.53

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

**Operating System & version**: Microsoft Windows 2022 and 10.0.20348

**Open ports with associated services:**

* Port 135
* Port 139
* Port 445
* Port 1801
* Port 2103
* Port 2105
* Port 2107
* Port 3389

**ARP Ping Scan elapsed time:** Completed ARP Ping Scan at 10:25, 0.20s elapsed.

**Wireshark Analysis:** Monitored communication on the ports and verified traffic.

**Machine designation**: **Linux**

**Device Host Name**: Not specified in Scan but checked in Linux the name is user-pc

**IP address**: 172.16.14.52

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

**Operating System & version**: Linux 4.15 - 5.8

**Open ports with associated services:**

* Port 80(HTTP)
* Port 3306(MYSQL)
* Port 3389(ms-wbt-server))

**ARP Ping Scan elapsed time:** Completed ARP Ping Scan at 19:28, 0.19s elapsed (1 total hosts)

**Wireshark Analysis:** Analyzed communication on the ports 80, 3306,3389.

**Machine designation**: **Kalilinux**

**Device Host Name**: Not specified in Scan.

**IP address**: 172.16.14.51

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

**Operating System & version**: Unable to detect the operating system in the scan.

**Open ports with associated services:** No open ports

**ARP Ping Scan elapsed time:** Completed ARP Ping Scan at 19:28, 0.19s elapsed (1 total hosts)

**Wireshark Analysis:** No open ports to analyze.

**Machine designation**: **VPC**

**Device Host Name**: Not specified in Scan.

**IP address**: 172.16.14.101

**MAC address**: 00:50:79: 66:68:03

**Operating System & version**: Unable to detect the operating system.

**Open ports with associated services:** Many open ports

**ARP Ping Scan elapsed time:** Completed ARP Ping Scan at 15:06, 0.17s elapsed. **Wireshark Analysis:** Analyzed the traffic.

# Analysis and Documentation:

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.

Following are the screenshots of each device displaying the scan results obtained using Zenmap.

A document with text and numbers

Description automatically generated A screenshot of a scan report

Description automatically generated

1. **Zenmap scan on Windows1 2. Zenmap scan on Winserver**

# A screenshot of a document Description automatically generated A screenshot of a computer Description automatically generated

**3. Zenmap scan on Linux 4. Zenmap scan on KaliLinux**

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.

A document with text and numbers

Description automatically generated A screenshot of a computer program

Description automatically generated

**5.Zenmap scan on VPC.**

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.

A screenshot of a computer

Description automatically generated

6.The provided screenshot represents a sequence of packet captures for Windows1.

**Packet details:**

Packet Number: 818

Source IP: 172.16.14.3

Destination IP: 172.16.14.199

Protocol: TCP

Source Port: 3389

Destination Port: 60036

This packet represents a TCP communication from the source IP 172.16.14.3 to the destination IP 172.16.14.199 on port 60036. The packet length is 54 bytes.

In the screenshot, Line 1 signifies Layer 1, with the MAC address located directly beneath in Layer 2. Moving down the layers, Layer 3 contains the IP address, while Layer 4 includes the source and destination ports.

A screenshot of a computer

Description automatically generated

7. The provided screenshot represents a sequence of packet captures for the Winserver.

**Packet details:**

Packet Number: 5758

Source IP: 172.16.14.3

Destination IP: 172.16.22.199

Protocol: TCP

Source Port: 3389

Destination Port: 60036

This packet represents a TCP communication from the source IP 172.16.14.3 to the destination IP 172.16.22.199 on port 60036. The packet length is 107 bytes.

In the screenshot, Line 1 signifies Layer 1, with the MAC address located directly beneath in Layer 2. Moving down the layers, Layer 3 contains the IP address, while Layer 4 includes the source and destination ports.

A screenshot of a computer

Description automatically generated

8. The provided screenshot represents a sequence of packet captures for Linux.

**Packet details:**

Packet Number: 544

Source IP: 172.16.14.3

Destination IP: 172.16.14.52

Protocol: TCP

Source Port: 9432

Destination Port: 80

This packet represents a TCP communication from source IP 172.16.14.3 to destination IP 172.16.14.52 on port 80. The packet length is 72 bytes.

In the screenshot, Line 1 signifies Layer 1, with the MAC address located directly beneath in Layer 2. Moving down the layers, Layer 3 contains the IP address, while Layer 4 includes the source and destination ports. The Get response in the last field is Layer 7.

A screenshot of a computer

Description automatically generated

9.The provided screenshot represents a sequence of packet captures for KaliLinux.

**Packet details:**

Packet Number: 406

Source IP: 173.33.22.199

Destination IP: 172.16.14.3

Protocol: TCP

Source Port: 60036

Destination Port: 3389

This packet represents a TCP communication from the source IP 173.33.22.199 to the destination IP 172.16.14.3 on port 3389. The packet length is 60 bytes. In the screenshot, Line 1 signifies Layer 1, with the MAC address located directly beneath in Layer 2. Moving down the layers, Layer 3 contains the IP address, while Layer 4 includes the source and destination ports. There is an acknowledgement field which has the frame number.

A screenshot of a computer

Description automatically generated10. The provided screenshot represents a sequence of packet captures for VPC.

**Packet details:**

Packet Number: 43373

Source IP: 172.16.14.3

Destination IP: 172.16.14.101

Protocol: ARP

This packet represents a ARP communication and the request is initiated by the source 172.16.14.3 seeking the MAC address corresponds to the IP address 172.16.14.101.

# Network Topology:

A computer screen shot of a network

Description automatically generated

**11. Topology Representation with Network Segmentation**

For security reasons, I segmented kali by both server and VLAN, serving specific security purposes. This approach helps restrict direct access from client machines to the security and testing segment, strengthening overall security measures.

Winserver and Linux function as internal server segments, managing files and hosting webservers.

For windows1 and VPC, I have placed them on the same server to facilitate easy communication.

# 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.

# Acknowledgement and References:

In this project, I utilized the following tools:

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

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