Network Administration Project

W02D1

Heather Fincati

Introduction

In this report you will find my assessment of your network infrastructure, the information I have gathered for each device, the services each device uses regularly, my recommended topology for your network and the reasoning for them. I have utilized a couple tools; Wireshark and Zenmap to critically analyze your systems

Network Device Information

Machine 1

Machine Destination: Windows1
Device Host Name: DESKTOP-WIN10PRO
IP Address: 172.16.14.50
MAC Address: 50:01:00:02:00:01
Operating System & Version: Microsoft 10 v1809
Open ports with associated services:
3389/tcp open ms-wbt-server - used for Windows Remote Desktop and Remote Desktop Assistance
5357/tcp open http - 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.
ARP Ping Scan elapsed time: 0.16s elapsed

Machine 2

Machine Destination:Kali Open Vas
Device Host Name: Kali
IP Address: 172.16.14.51
MAC Address: 50:01:00:07:00:01
Operating System & Version: Kali GNU/Linux Rolling
Open Ports with Associated Services: All 1000 scanned ports on 172.16.14.51 are in ignored states. 1000 closed tcp ports
ARP Ping Scan elapsed time: 0.17s elapsed

Machine 3

Machine Destination: Linux
Device Host Name: user-pc
IP Address: 172.16.14.52

MAC Address: 50:01:00:05:00:01
Operating System & Version: Ubuntu 20.04.6 LTS
Open Ports with Associated Services:

80/tcp: http - enables the world wide web

3306/tcp: mysql - MySQL database server connections

3389/tcp rdp: used for Windows Remote Desktop and Remote Assistance connections (RDP - Remote Desktop Protocol). Also used by Windows Terminal Server.

9200/tcp: ssl/rtsp wsp - used for all API calls over HTTP. This includes search and aggregations, monitoring and anything else that uses a HTTP request

ARP Ping Scan elapsed time: 0.23s elapsed

Machine 4

Machine Destination: 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 Server 2022 v21H2
Open Ports with Associated Services:

80/tcp: http - enables the world wide web

135/tcp: msrpc - Remote Procedure Call (RPC) port 135 is used in client/server applications

139/tcp: netbios-ssn - NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be. There are a number of vulnerabilities associated with leaving this port open.

445/tcp: microsoft-ds - used for direct TCP/IP MS Networking access without the need for a NetBIOS layer.

1801/tcp: msmq - Microsoft Message Queuing (MSMQ)

2103/tcp: msrpc - Microsoft Message Queuing (MSMQ)

2105/tcp: msrpc - Microsoft Message Queuing (MSMQ)

2107/tcp: msrpc - Microsoft Message Queuing (MSMQ)

3389/tcp: ms-wbt-server - used for Windows Remote Desktop and Remote Assistance connections (RDP - Remote Desktop Protocol). Also used by Windows Terminal Server.

5357/tcp: http - 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.

ARP Ping Scan elapsed time: 0.18s elapsed

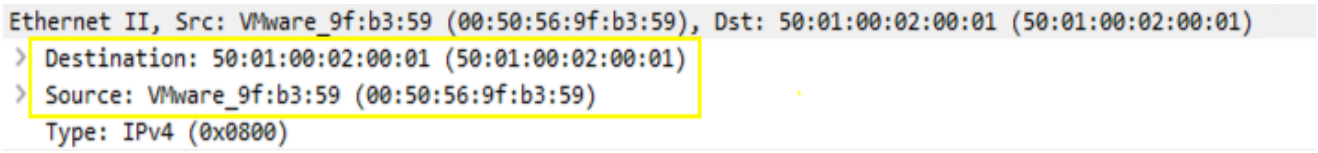
After using Zenmap to gather all of the above information it was cross referenced in Wireshark and each port and address was confirmed in the packet captures:

OSI Layer Headers

MAC Addresses are found in the Data-Link/2 Layer
IP Addresses are found in the Network/3 Layer
Port #'s are found in the Transport/4 Layer

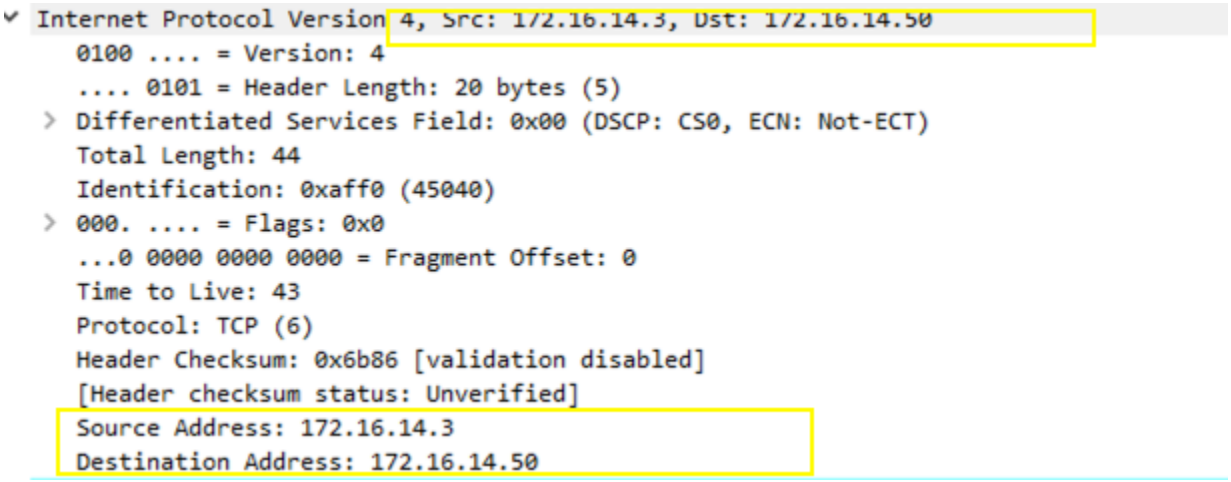
In the screen captures below please you will see where and how in Wireshark I was able to obtain this information.

Datalink/2 Layer



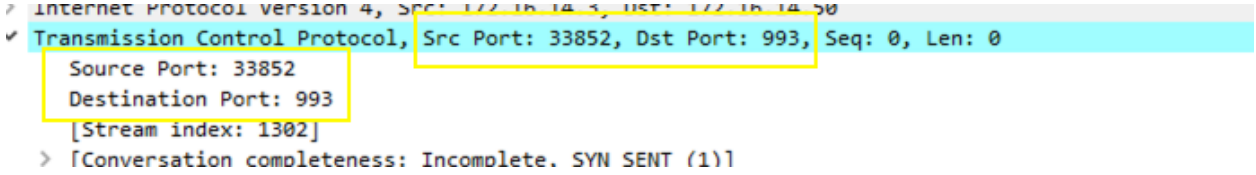
In the above screen capture you will see the Source and Destination MAC Addresses circled in yellow. This is found in the Datalink or 2nd Layer of the OSI Model. And can be seen in two places, one in the frame header of the packet capture and the other when you expand it.

Network/3 Layer



In the above screen capture you can see the Source and Destination IP addresses highlighted in yellow. They are found in the Network or 3rd Layer of the OSI Model. And can be seen in two places, one in the frame header of the packet capture and the other when you expand it.

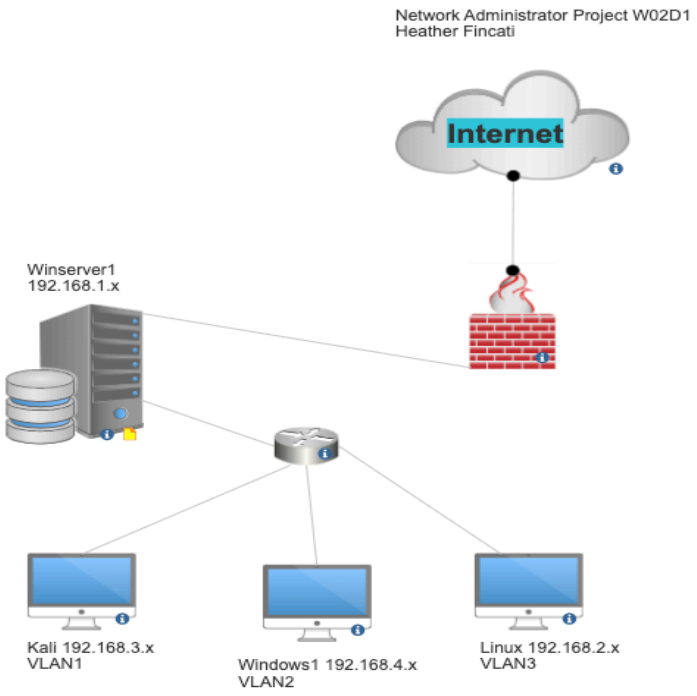
Transport/4 Layer



In the above screen capture you can see the Source and Destination Port #'s highlighted in yellow. They are found in the Transport or 4th Layer of the OSI Model. And can be seen in two places, one in the frame header of the packet capture and the other when you expand it.

Topology

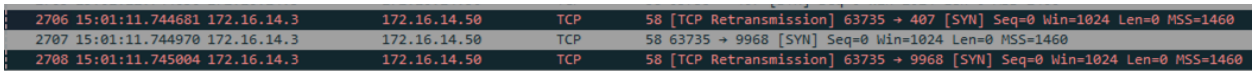
It is important to present you with the topology of your network and why it is mapped out the way it is, to get a better understanding of how each machine and the services on it affect the network, its security and create possible vulnerabilities. I have used Zenmap to learn exactly which services are on each device so I can make sure they are as secure as possible. The goal is to make the network and security as robust as possible so we add a few layers to make this happen. On the main server I have added a firewall to prevent outside attacks and segmented each user machine with VLAN's to add an extra layer of security from outside the network and within it. This is to isolate different services that are on the same physical network in order to enhance overall data security.



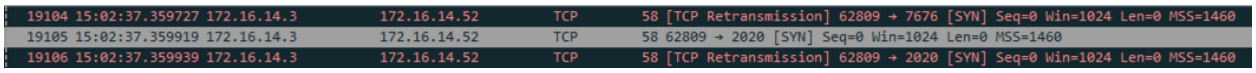
Information Collection Methodology

The data for the above network device information was gathered using Wireshark, and Zenmap software which are both open-source applications. On the screen captures I have provided you can see the data I was able to acquire from each application. The IP Addresses, MAC Addresses, open ports, and operating systems, I pulled from Zenmap when I ran an intense scan from my Jumphost machine to all the machines on the network. I was able to verify this information along with the Device host names and the OS versions being run on each machine using either the terminal command using specific commands depending on the operating system being used. I have also verified my Zenmap scans worked and were seen in Wireshark in the screen captures below.

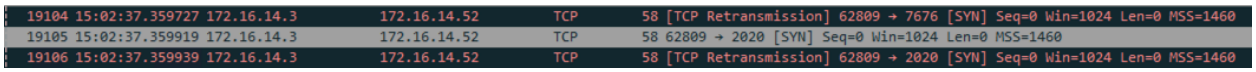
Scan from Zenmap to machine1 IP Address 172.16.14.50



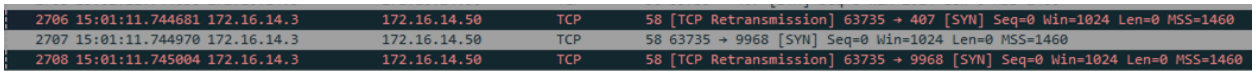
Scan from Zenmap to machine2 IP Address 172.16.14.51



Scan from Zenmap to machine3 IP Address 172.16.14.52



Scan from Zenmap to machine4 IP Address 172.16.14.53



Citations

Ports Database

SpeedGuide
https://www.speedguide.net/ports.php?filter=&sort=&p=23

17 Best Linux Networking and Troubleshooting Commands for Beginners

Bydevopscube et al.
https://devopscube.com/list-linux-networking-troubleshooting-and-commands-beginners/

ChatGPT

ChatGPT is an AI-powered language model developed by OpenAI, capable of generating human-like text based on context and past conversations.
https://chat.openai.com

SmartDraw is the Best Way to Make a Diagram

https://app.smartdraw.com/editor.aspx?credID=-59494770&depoId=54211266&flags=128#