

**Network administration**

A grey logo on a black background

Description automatically generated

May 7, 2024

lighthouse labs

By: Curtis R. Crawford

**Table of Contents**

Cover Page0

Table of Contents1

Introduction2

Network Devices Information3

Network Devices Information Cont’d4

Screen Captures5

**Screen Captures Cont’d6**

Screen Captures Cont’d7

Current Network Topology8

Network Topology Recommendations9

Information Collection Methodology10

References & Citations11

Thank you12

**INTRODUCTION**

In this report, we shall review the following:  
  
Network devices discovered within the EVE “Main Lab” network. The information presented includes device designations, host names, IP addresses, MAC addresses, operation systems, open ports, and the ARP ping scan time.

Screen captures of where I located the information on ZenMap.

A peak into what the current network topology looks like.

Recommendations as to how I think that topology could be improved.

My methodology for collection the device’s information.

Any references used within this document and where I researched techniques/methods.

*Let’s begin.*

**Network Devices Information**

**-------------------------------------------------------------------------------------------------------------------------------**

Machine Designation: **Windows1**

Device Host Name: DESKTOP-WIN10PRO

IP Address: 172.16.14.50

MAC Address: 50:01:00:02:00:01

OS: Microsoft Windows XP SP2

Ports: Port 3389 (tcp)-[ms-wbt-server]

Port 5357 (tcp)-[http]

ARP Ping Scan: 1.61s

**-------------------------------------------------------------------------------------------------------------------------------**

Machine Designation: **KaliOpenVas**

Device Host Name: Kali

IP Address: 172.16.14.51

MAC Address: 50:01:00:07:00:01

OS: Linux 4.X|5.X (Kali GNU/Linux Rolling 2023.2)

Ports: 0 Open Ports

ARP Ping Scan: 1.61s

**-------------------------------------------------------------------------------------------------------------------------------**

Machine Designation:  **Linux**

Device Host Name: user-pc

IP Address: 172.16.14.52

MAC Address: 50:01:00:05:00:01

OS: Linux 4.X|5.X (Ubuntu 20.04.6 LTS)

Ports: Port 80 (tcp)-[http]

Port 3306 (tcp)-[mysql]

Port 3389 (tcp)-[ms-wbt-server]

Port 9200 (tcp)-[rtsp]

ARP Ping Scan: 1.61s

**-------------------------------------------------------------------------------------------------------------------------------**

Machine Designation: **Winserver1**

Device Host Name: WIN-SERVER-2022

IP Address: 172.16.14.53

MAC Address: 50:01:00:01:00:01

OS: Microsoft Windows Server 2022

Ports: Port 80 (tcp)-[http]

Port 135 (tcp)-[msrpc]

Port 139 (tcp)-[netbios-ssn]

Port 445 (tcp)-[microsoft-ds]

Port 1801 (tcp)-[msmq]

Port 2103 (tcp)-[zephyr-clt]

Port 2105 (tcp)-[eklogin]

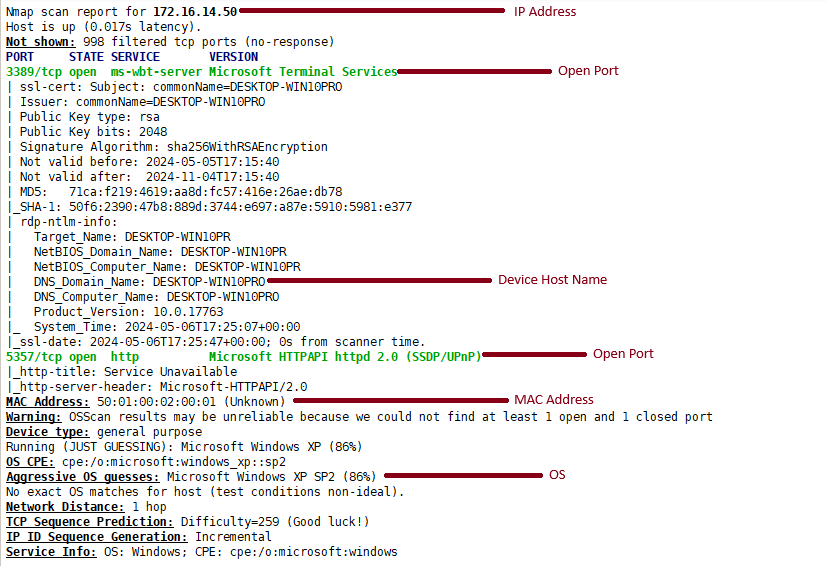
Port 2107 (tcp)-[msmq-mgmt]

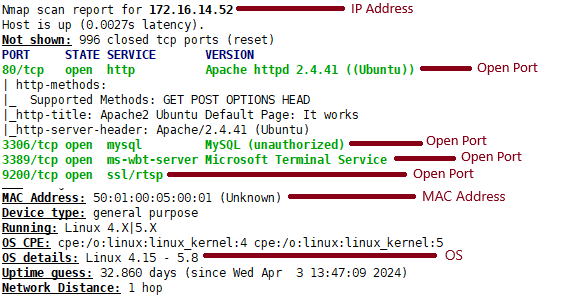
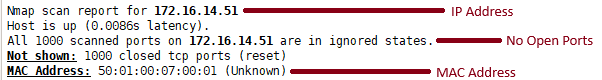
Port 3389 (tcp)-[ms-wbt-server]

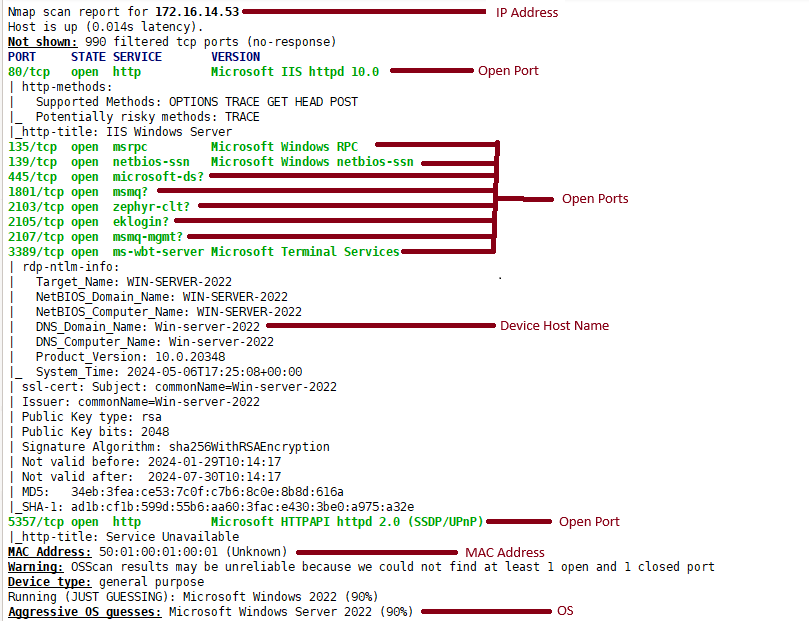
Port 5357 (tcp)-[http]

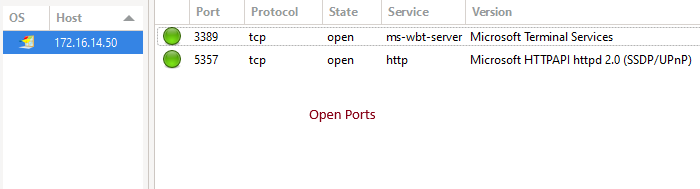
ARP Ping Scan: 1.61s

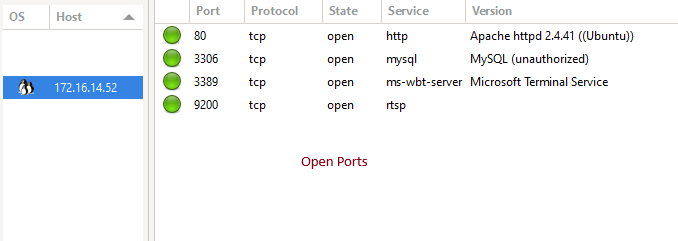
**Screen Captures**

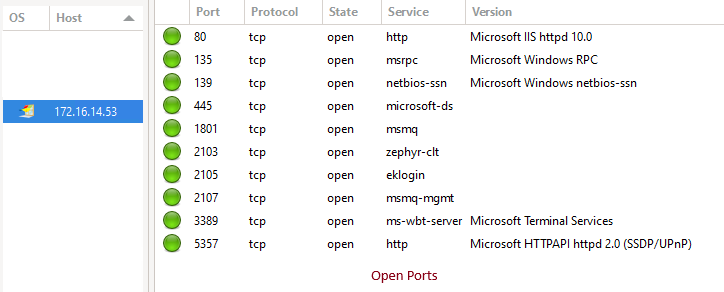












**Current Network Topology**

* Network is connected directly to the Internet.
* No visible protection.
* All devices are connected directly to the Network.

A diagram of computer network

Description automatically generated

**Network Topology Recommendations**

* All devices connected to the Network now have their own personal VPN.
* Network Router is now 2nd in line to the Internet for further protection.
* Network Router focuses on communication between the machines.
* Edge Router takes precedence on connecting with the Internet and intercepting threats.
* Firewall added for additional security.

A diagram of a network

Description automatically generated

**Information Collection Methodology**

“Information collection methodology refers to the systematic approach or techniques used to gather data or information for a particular purpose. In the context of network devices, the information collection methodology could involve various techniques such as:

\*Network Scanning: Utilizing tools like Nmap or Wireshark to scan the network for active devices, open ports, and services running on those devices.

\*ARP Ping Scan: Using Address Resolution Protocol (ARP) ping scan to discover devices within the local network by sending ARP requests and analyzing responses.

\*Port Scanning: Conducting port scans to identify open ports on devices, which can provide insights into the services running on those devices.

\*OS Fingerprinting: Employing techniques to identify the operating systems running on network devices, such as examining network responses or analyzing TCP/IP stack behaviors.

Manual Inspection: Physically inspecting network devices, checking their configurations, and documenting relevant information like IP addresses, MAC addresses, and host names.

Querying Network Infrastructure: Interacting with network infrastructure components such as routers, switches, or firewalls to gather information about connected devices and network topology.

Asset Management Systems: Leveraging asset management tools or systems to automatically collect and maintain information about network devices, including hardware specifications, software versions, and configurations.

\*Interviews and Documentation Review: Conducting interviews with network administrators or reviewing existing documentation to gather information about the network infrastructure and devices.

The methodology chosen depends on factors such as the scope of the information required, the size and complexity of the network, available resources, and the level of access and permissions granted for information gathering activities.” – ChatGPT (2024)

\*The methods I personally used. The information was gathered primarily through an Intense Scan on ZenMap of the Network. Confirmations were made with WireShark that was running in the background during the ZenMap’s scan. While the Device Host Names for Kali & Linux couldn’t be located on either program, their names were already listed on the existing documentation (EVE).

**References & Citations**

* Bitlock Security (2021). “Zenmap Tutorial | Learn Zenmap Basics and Run Basic Scans (2021)”
  + - <https://www.youtube.com/watch?v=Vbl_mj5z6U8>
* ChatGPT (2024). “What is Information Collection Methodology”.
  + - [https://www.chatgpt.com](https://www.youtube.com/watch?v=Vbl_mj5z6U8)
* LighthouseLabs (2024). “Training for the Final Lab”
  + - <https://web.compass.lighthouselabs.ca/p/13/workbooks/cyber-flex-c01w03/activities/2824?journey_step=201&workbook=388>
* Microsoft Paint (2024). Editing all included screenshots.
  + - <https://www.microsoft.com/en-ca/windows/paint>
* Windows Snipping Tool (2024). Taking all included screenshots.
  + - <https://apps.microsoft.com/detail/9mz95kl8mr0l?hl=en-US&gl=US>
* Microsoft Word (2024). Writing this report.
  + - <https://www.microsoft.com/en/microsoft-365/word?market=af>
* Smartdraw (2024). Drawing my Network Topology.
  + - <https://app.smartdraw.com>
* ConceptDraw (2023). “What is a Virtual Private Network”
  + - <https://www.conceptdraw.com/How-To-Guide/virtual-private-networks>
* ImgFlip (2024) “Cheers Meme”
  + - <https://imgflip.com/s/meme/Leonardo-Dicaprio-Cheers.jpg>



Thank you for taking the time to review my report!