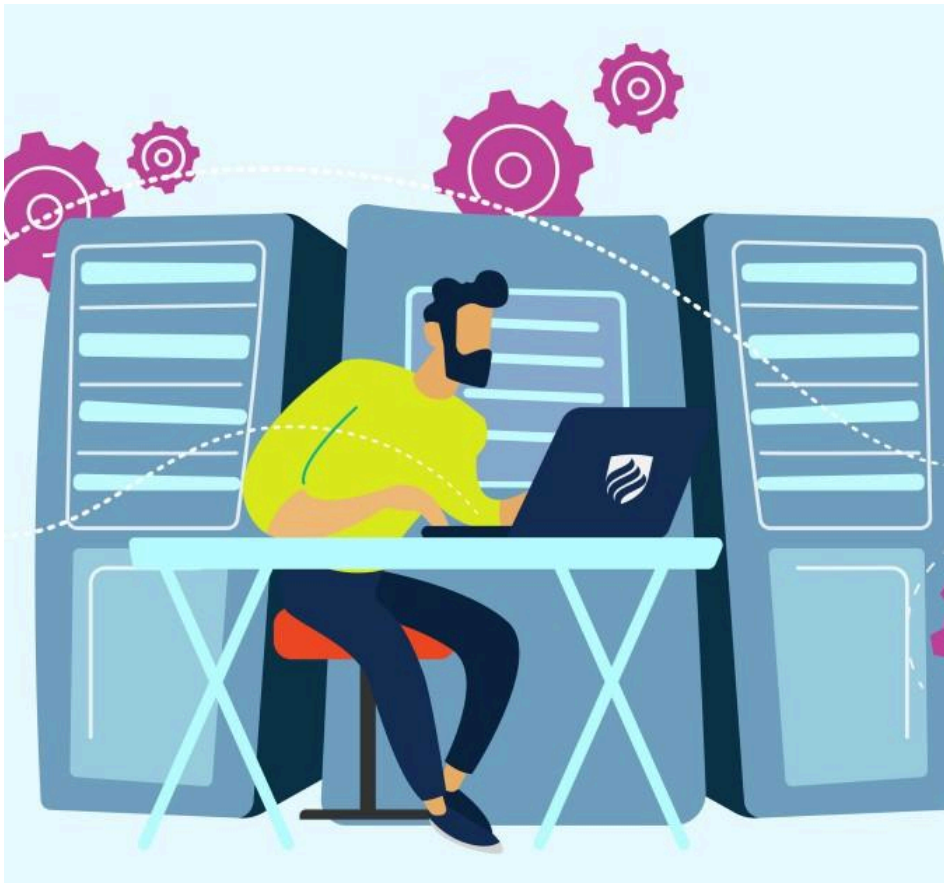
Network Administration



By: Mahad Mohamood

Table of contents

Introduction

This project involves a systematic exploration and documentation process aimed at uncovering detailed information about devices within your Lab environment. Using tools like Nmap and Wireshark, I've conducted thorough scans to identify and gather critical data on each networked device. The following three devices were discovered and analyzed : Linux kali computer, linux ubuntu device, and windows device. Below are some of the key findings post-analysis.

Key findings

- The Kali Linux virtual machine exhibited the least amount of information exposure in Zenmap scans.

- In Wireshark, the Kali Linux VM also had the lowest number of packets captured during the Zenmap scan compared to other systems.

- Windows and Linux Ubuntu systems exposed significantly more information during Zenmap scans.

- Correspondingly, these systems generated a higher volume of packets captured in Wireshark during the scan.

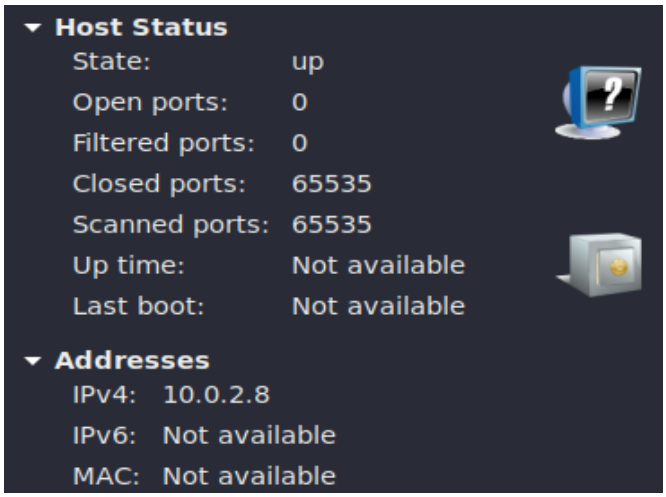
- Based on the findings, Kali Linux appears to demonstrate stronger security posture compared to Linux Ubuntu and Windows.

- The greater information exposure and higher packet capture rate observed in Windows and Linux Ubuntu suggest potentially lower security levels in these systems.

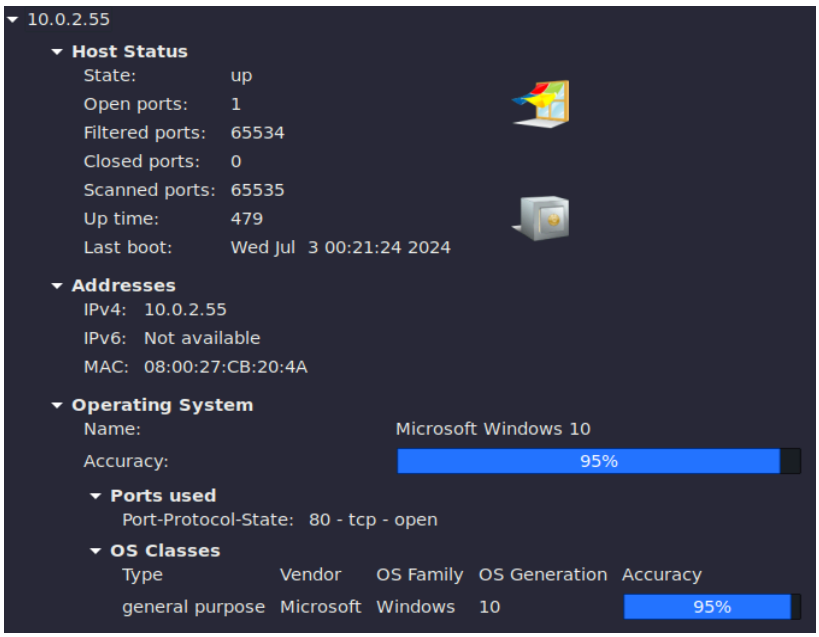
Network Devices information

The three devices were analyzed in this project via nmap. According to freecodecamp, “Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.(para.1)” Below is the name of each device followed by a nmap screenshot of the devices information.

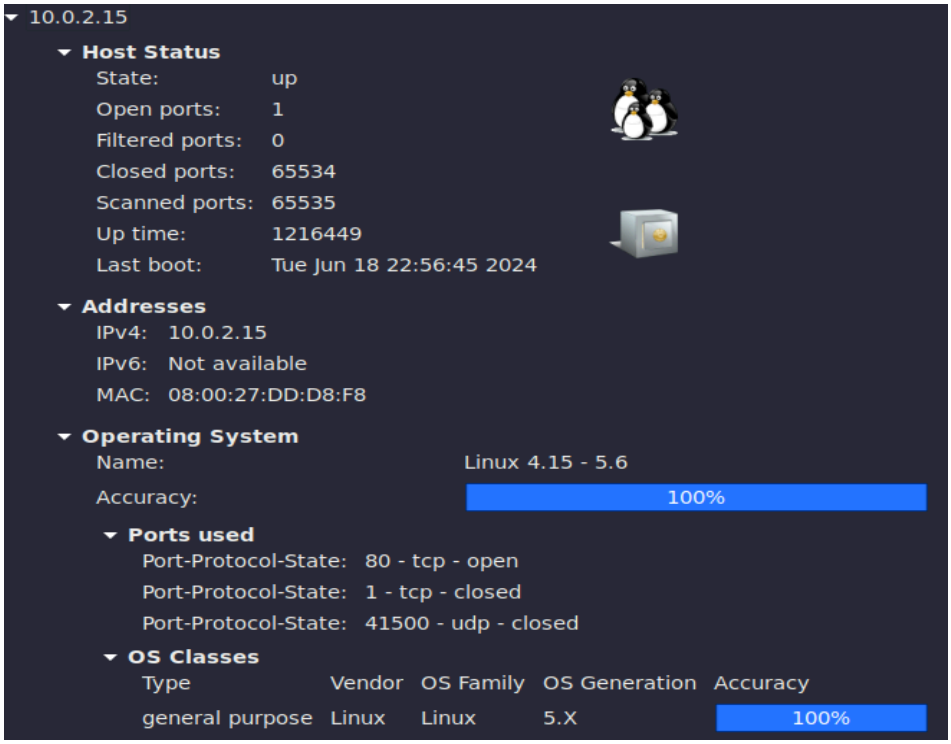
1. Virtual machine : Linux kali 10.0.2.8



2. Virtual machine : Windows:10.0.2.5



3. Virtual machine: Linux :10.0.2.15



Information collection methodology

Below is the step-by-step process that I followed when conducting the scans.

1. Three virtual machines were turned on.
2. Wireshark was launched on a Kali Linux virtual machine to monitor network traffic.
3. Zenmap, running on the same Kali Linux virtual machine, was launched and configured with an intense scan profile targeting all TCP ports.
4. The following IP addresses were sequentially scanned using Zenmap:
5. Linux kali: 10.0.2.8, Windows:10.0.2.55, Linux :10.0.2.15
6. Once all scans were completed in Zenmap, Wireshark's monitoring was halted.

Analyzing Wireshark captures

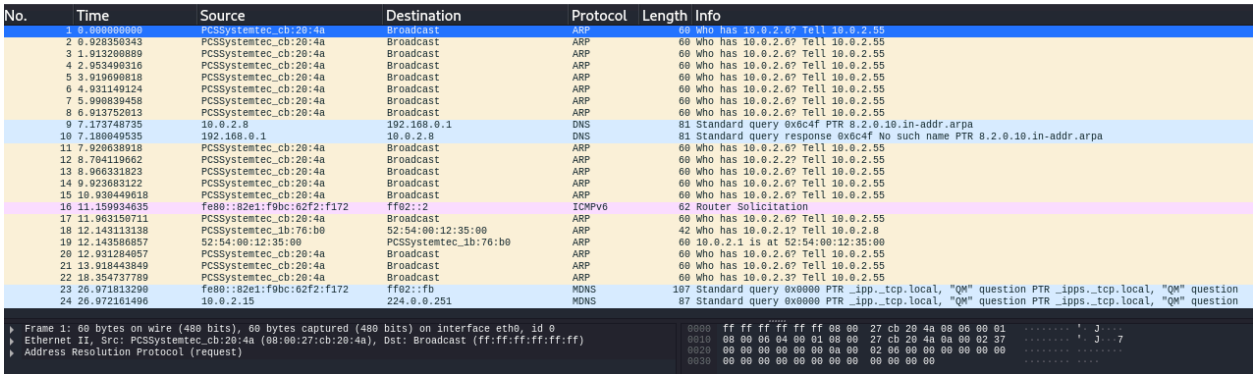
I used wireshark to analyze the traffic that was coming through my network. According to Comptia “Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.”(para. 2). Below is a brief overview of each machine that I analyzed and

some of the key findings.

1. Virtual machine : Linux kali 10.0.2.8

- The packets for this capture were few and that's how i know that it belongs to kali linux.
- The kali linux capture was terse and it did not return a lot of information.
- This could be either because it is the main vm being used to run the scans, or maybe it has some way of detecting and dodging scans.

Screenshot of capture:



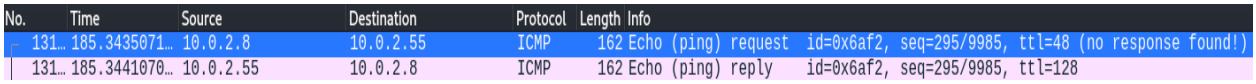
2. Virtual machine : Windows:10.0.2.55

- The packet participants are the kali linux and the windows vm, i verified them by their IP's.
- Wireshark captured more packets for windows than for the Linux Kali.

There were a lot of packets such as the one below with TCP protocol.

There were a few instances where ARP protocol was sent to identify IP's.

The two machines started to make ping requests and replies via the ICMP protocol.



There were also a few HTTP protocols with text/html

No.	Time	Source	Destination	Protocol	Length	Info
131…	99.487776472	10.0.2.8	10.0.2.55	HTTP	84	GET / HTTP/1.0
131…	99.506543848	10.0.2.55	10.0.2.8	HTTP	120	HTTP/1.1 302 Moved Temporarily (text/html)

3. Virtual machine: Linux :10.0.2.15

- The packet participants are the kali linux and the linux vm, i verified them by their IP's.
- The wireshark for linux capture had a lot more packets than the windows.

There were packets such as the one below with TCP protocol.

No.	Time	Source	Destination	Protocol	Length	Info
131102	24.953179753	10.0.2.15	10.0.2.8	TCP	74	80 → 57730 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
131103	24.953214212	10.0.2.8	10.0.2.15	TCP	54	57730 → 80 [RST] Seq=1 Win=0 Len=0
131104	25.051528277	10.0.2.8	10.0.2.15	TCP	74	57731 → 80 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM
131105	25.053253426	10.0.2.15	10.0.2.8	TCP	74	80 → 57731 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460
131106	25.053292055	10.0.2.8	10.0.2.15	TCP	54	57731 → 80 [RST] Seq=1 Win=0 Len=0

There were a few instances where ARP protocol was sent to identify IP's.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_1b:76:…	Broadcast	ARP	42	Who has 10.0.2.15? Tell 10.0.2.8
2	0.000657757	PCSSystemtec_dd:d8:…	PCSSystemtec_1b:76:…	ARP	60	10.0.2.15 is at 08:00:27:dd:d8:f8
4	0.052943652	52:54:00:12:35:00	Broadcast	ARP	60	Who has 10.0.2.8? Tell 10.0.2.1

The two machines started to make ping requests and replies via the ICMP protocol.

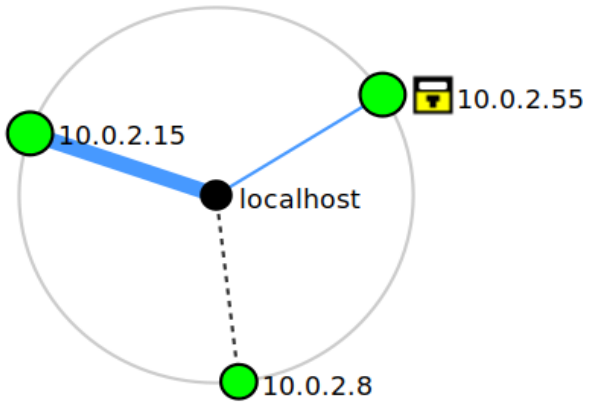
No.	Time	Source	Destination	Protocol	Length	Info
131119	25.480760095	10.0.2.8	10.0.2.15	ICMP	162	Echo (ping) request id=0x517e, seq=295/9985, ttl=56 (reply in 131120)
131120	25.482833757	10.0.2.15	10.0.2.8	ICMP	162	Echo (ping) reply id=0x517e, seq=295/9985, ttl=64 (request in 131119)

There were also a few HTTP protocols with text/html

No.	Time	Source	Destination	Protocol	Length	Info
131096	24.846067807	10.0.2.15	10.0.2.8	HTTP	310	HTTP/1.1 200 OK
131180	26.165084336	10.0.2.8	10.0.2.15	HTTP	217	OPTIONS / HTTP/1.1
131181	26.165591011	10.0.2.8	10.0.2.15	HTTP	84	GET / HTTP/1.0
131182	26.165687734	10.0.2.8	10.0.2.15	HTTP	237	GET /nmaplowercheck1719967854 HTTP/1.1

Topology

This topology was provided by the zenmap interface. It captures the basic structure of the network.



References

1. Computing Technology Industry Association (CompTIA). What Is Wireshark and How Is It Used ? Retrieved from [https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it]

2. FreeCodeCamp. What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time. Retrieved from [https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time]