**Network Administration Project Report**

Prepared by: Harsh Patel

Date: December 9, 2024

[**Executive Summary/Introduction 3**](#_gjdgxs)

[**Network Devices Information 3**](#_xl3yfj6lny6n)

[**Information Collection Methodology 3**](#_dvufna885bif)

[**Recommended Topology 3**](#_1fob9te)

[**References 4**](#_2et92p0)

# **Executive Summary/Introduction**

This report describes my project for which I used three virtual machines on different operating systems that are Kali Linux, Windows 11, and Ubuntu Linux. This project was done on Kali Linux using two tools Wireshark and Nmap. The purpose of this project was to perform a network scan and analysis using Nmap and Wireshark to check for open ports and network vulnerabilities, describe how I did it, and make a suggestion for better network segmentation based on scan results.

# **Network Devices Information**

**FOR WINDOWS 11**

|  |  |  |
| --- | --- | --- |
| Device Host Name | Windows11-Deskt | Windows Screenshot    Captured on Nmap scan |
| IP Address | 10.0.2.6 | Windows  From Kali Terminal (nmap scan) |
| MAC Address | 08-00-27-CB-20-4A | From Windows    From Nmap scan |
| OS & Version | Windows 11 | from windows  from nmap |
| Open Ports | Port 80 HTTP |  |
| ARP Ping Scan elapsed time | 0.06s |  |
| OSI Layer header each of the addresses and port’s # | Layer 1- Ethernet Layer 2 – MAC Addresses Layer 3 - IP Addresses Layer 4 - Protocol |  |

**FOR UBUNTU LINUX**

|  |  |  |
| --- | --- | --- |
| Device Host Name | Linux-Server | Ubuntu Linux  Nmap Scan |
| IP Address | 10.0.2.4/24 | Ubuntu Linux  Nmap scan |
| MAC Address | 08:00:27:dd:d8:f8 | Ubuntu Linux   Nmap scan |
| OS & Version | Ubuntu Linux | Ubuntu Linux   Nmap scan |
| Open Ports | Port 21 FTP Port 3306  Port 80 HTTP |  |
| ARP Ping Scan elapsed time | 0.06s |  |
| OSI Layer header each of the addresses and port #’s | Layer 1- Ethernet Layer 2 - MAC Addresses Layer 3 - Ip Addresses Layer 4 - Protocol |  |

# **Information Collection Methodology**

Below are the Steps on how I got the results.

1. Opened Oracle Virtual Box and turned on all Virtual Machines (Kali, Windows &Ubuntu)
2. Opened Wireshark on Kali and started the packet capture. (Did separately for both Windows and Ubuntu)
3. On Kali terminal started Nmap aggressive scan using the following commands.  
   For Windows: sudo nmap -T4 -A -v 10.0.2.6  
   For Ubuntu Linux: sudo nmap -T4 -A -v 10.0.2.4
4. Stopped the capture as soon as the scan was completed to avoid capturing unnecessary packets.
5. Started assessing the scans and looked for the information and took screenshots to document those findings.
6. Verified the information of the scan on the actual machine and took the screenshot of information on actual machine as well.
7. Used wireshark to look for OSI layer information.
8. After all the documentation and assessing the scan designed the Network Topology to make it more secure.

# **Recommended Topology**

So I have separated each of my machines on their own VLAN and that would be more secure as if One machine gets attacked or compromised We can Isolate that machine or we can cut off the whole connection from that machine so our other machines and data is safe from the attack also I have put Firewall between each machines connection to the Switch so we can open or close the port or connection to that specific machine as required and I have put one Firewall between the network/internet and my Router so that I can control the incoming traffic and also can prevent an attack or breach through internet.

A computer network diagram with many computers

Description automatically generated with medium confidence

# **References**

*NMAP cheat sheet*. (n.d.). https://cdn.comparitech.com/wp-content/uploads/2019/06/Nmap-Cheat-Sheet.pdf

*Intro to Wireshark Filtering and Analysis (Cyber Security Immersive)*. (n.d.). <https://web.compass.lighthouselabs.ca/p/cyber/days/w01d3/activities/2795>

Devopscube. (2023, November 16). 17 Best Linux Networking And Troubleshooting Commands. *DevopsCube*. <https://devopscube.com/list-linux-networking-troubleshooting-and-commands-beginners/>