**Table of Contents**

## INTRODUCTION

### What is Network Administration?

Network administration seeks to manage, monitor, secure, and service an organization's network.
This definition has four major elements;

1. Managing the network: this involves identifying devices that are connected to the organization's network.
2. Monitor the network: monitoring the network involves inspecting connected devices or any devices that attempt to connect to the network.
3. Securing the network: involves protecting the network from unwanted or malicious attacks.
4. Servicing the network: involves offering reparatory services in the event of an attack.

This definition highlights the importance of network administration which is the day-to-day management of networks.

### Executive Summary

#### Key Findings

Preliminary findings revealed that the environment was not secure and was at risk of attack by external entities.

#### Monitoring Summary

This report sought to monitor three VMs, Linux Server, KaliOpenVas, and Windows 11. A preliminary check was successful for all three VMs and there were anomalies due to network cessation.

#### Incident Summary

This project revealed the inadequacy of the set-up.

#### Recommendations

1. Firewall Configuration: this is essential in protecting the environment and having a firewall will block unnecessary traffic between VLANs and other potential threats.
2. Access Control Lists: these are recommended to restrict access and to ensure that only authorized devices have access to communicate through VLANs.
3. Regular Reviews: Regular audits such as this ensure that the environment is secure and make adjustments when needed.
4. Network Monitoring: Enabling network monitoring tools to keep track of traffic and detect suspicious activity.

**Network Devices Information**
**Linux Server**

| Machine Designation | Server | OSI Layer |
|---|---|---|
| Device Host Name | Linux 4.15-5.6 | |
| IP Address | 10.0.2.4 | Layer 3-Network Layer |
| MAC Address | 08:00:27:DD:D8:F8 | Layer 2-Data link Layer |
| Operating System and Version | Ubuntu 2.4.52 | Layer 6-Processes |
| Open ports | 80 | Layer 4-Transport |
| ARP Ping Scan Elapsed Time | 0.066673400ms | Layer 3-Network Protocol |

**Windows**

| **Machine Designation** | **Windows 11** | **OSI Layer** |
|---|---|---|
| Device Host Name | Microsoft Windows 11Desk | |
| IP Address | 10.0.2.6 | Layer 3-Network Layer |
| MAC Address | 08:00:27:CB:20:4A | Layer 2-Data link Layer |
| Operating System and Version | Microsoft Windows 10, 82540EM | Layer 6-Processes |
| Open ports | 80/TCP | Layer 4-Transport |
| ARP Ping Scan Elapsed Time | 0.006822716ms | Layer 3-Network Protocol |

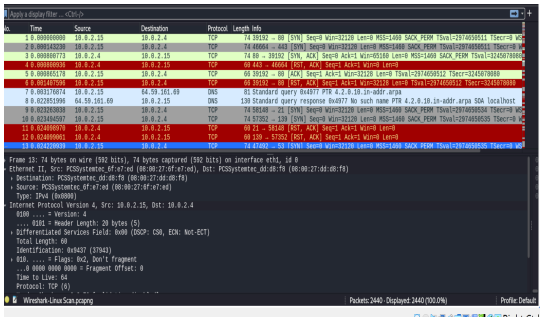
**KaliOpenVas**

| Machine Designation | Server | OSI Layer |
|---|---|---|
| Device Host Name | Oracle VirtualBox virtual NIC | |
| IP Address | 10.0.2.15 | Layer 3-Network Layer |
| MAC Address | 08:00:27:6F;E7:ED | Layer 2-Data link Layer |
| Operating System and Version | Not provided | Layer 6- Processes |
| Open ports | 00 | Layer 4-Transport |
| ARP Ping Scan Elapsed Time | 0.11s | Layer 3-Network Protocol |

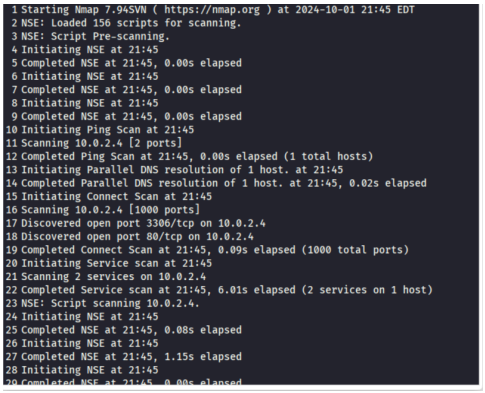
**Information Collection Methodology**

For this research, the method of information collection was network mapping. Network mapping, commonly called Nmap, is a command-based tool used to scan IP addresses, ports, and detect installed applications (Shivanandhan, 2020).
Commands such as nmap “-sS”, “-a”, “-A”, and “-T4” perform specific scans. This research utilized the ‘Nmap -T4 -A -v -O’ command to perform an aggressive scan of the network environment. This scan revealed information such as the device name, IP address, MAC address, and open ports, as required.
I also utilized Wireshark; a network packet analyzer which captures live packets for observation. In some cases, Wireshark is used to troubleshoot network problems, examine security problems, and in this case, it was used to get familiar with the network environment.
The images below were captured during the scans of the environment

## Linux

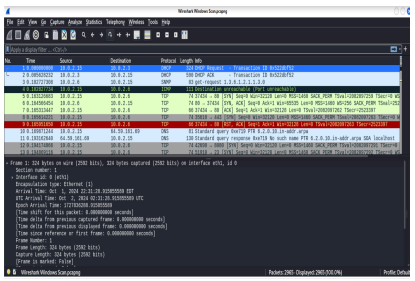


**1.1** Wireshark Capture

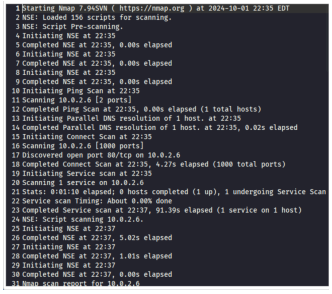



**1.2** Linux Nmap Capture

## Windows

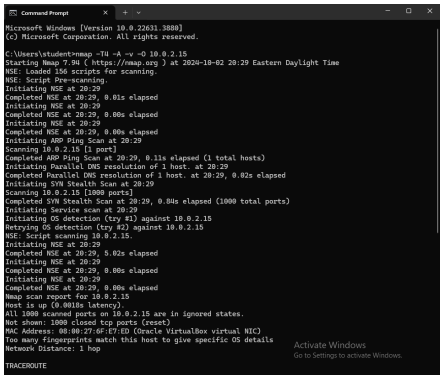


2.1 Nmap Screen Capture

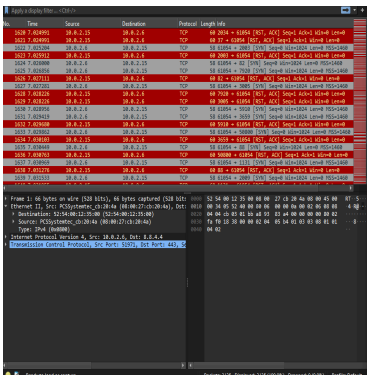



2.2 Wireshark Screen Capture

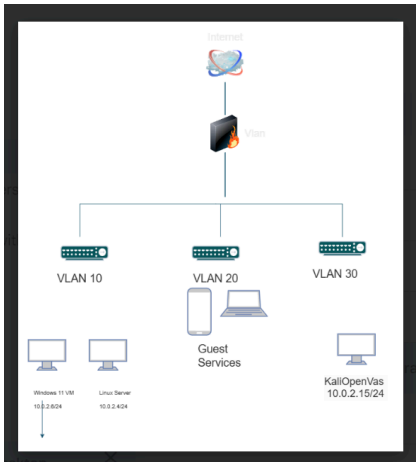
## KaliOpenVas




3.1 Wireshark Kali Capture



3.2 Nmap Screenshot



4. Topology Diagram

**References**

Lyon, G. (2009). *Nmap Network Scanning The Official Nmap Project Guide to Network Discovery and Security Scanning*. https://nmap.org/book/

NA, N. (2024). *Screenshot of Nmap Capture* [Photograph]. Nmap. https://nmap.org

Sharpe, R., Warnicke, E., & Lamping, U. *Wireshark User's Guide* (4th ed.). https://www.wireshark.org/docs/wsug_html_chunked/PreAbout.html

Shivanandhan, M. (2020, October 2). *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time*. Retrieved October 5, 2024, from https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

SolarWinds (2024). *What is Network Administration?* Retrieved October 2, 2024, from https://www.solarwinds.com/resources/it-glossary/network-administration