Network Administration Report

Table of content

1. Executive summary……………………………………………………I
2. Introduction Section……………………….………………………….II
3. Network Device Information………………………….……………. III
4. Information Collection Methodology………………………………. IV
5. References and Citation……………………………………………...V
6. **Executive Summary**

This documentation provides a comprehensive overview of all the devices in the lab networks, including the operating systems. It includes designated IP addresses, open ports, and ARP scans using Wireshark and Nmap to scan different IP addresses to find ports.

1. **Introduction Section**
2. **Network Administration**

Network administration aims to manage, monitor, maintain, secure, and service an organization’s network. It primarily consists of security, maintaining network quality and management, However, the specific tasks and procedures may vary depending on the size and type of an organization.

Network Monitoring: Monitors traffic patterns, the condition of the network infrastructure, and network-connected devices. Monitoring is crucial to maintaining its network quality and security. It detects anomalous activity, network problems, and excessive bandage usage

Network management: This is an administrative task that aims to implement, plan, and configure. This involves

* Installing security updates and upgrading the firmware on networking devices, including the firewall, switches and router
* Redesigning the network based on changing organizational requirement

Network Security: To ensure the network is safe, the network uses a variety of strategies, to stop attackers in the network, for instance, it makes use of a variety of techniques, such as intrusion detection and malware software

**3. Network Device Information**

This is an overview of my lab environment which includes Virtual machines that I will be working on, each serving a role.

* Windows 11: I will be running Ip configuration to access my IP address on my finding while running the cmd line under the directory of C:\Users\student>, so the command line will be C:\Users\student>ipconfig

A screenshot of a computer

Description automatically generated

* Linux Server/ubuntu: To check the IP address which is 127.0.0.1

A screenshot of a computer

Description automatically generated

* Kali OpenVAS: With this machine, I ran the IP configuration using the cmd terminal to ip address, which is under eth0

A computer screen shot of white text

Description automatically generated

The screenshots below show the list of Ip addresses and Mac addresses

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Mac Address: This is found in Layer 2 which is the datalink. This is a unique identifier for the Network interface, often found on the network interface card(NIC). This is required when trying to locate a device or performing a diagnostic on a network device. For example, if a laptop has both an Ethernet cable port and built-in Wi-Fi there will be two Mac addresses shown in the system configuration.

A computer screen with white text and blue text

Description automatically generated

Ports: This is found in the transport layer of the network; A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Every port is linked to a particular service or process for example emails and websites go through different ports even though they arrive at a computer via the same internet connection. It makes it easier for computers to distinguish between different types of traffic.

A screenshot of a computer

Description automatically generated

A diagram of a computer network

Description automatically generated

**4. Information Collection Methodology**

This is the process or series of steps to conduct research, understand the problem, and resolve the problem. The data helps information security and cybersecurity uncover information about a potential target. During the gathering, I used two tools which are Wireshark and Nmap/ Zenmap

* Wireshark: This is a framework that analyzes packets through devices, the source address will be the IP address, while the destination address is where the information is sent which can be in the form of a Mac address
* Zenmap: This is the official Nmap Security Scanner, it is a multi-platform. A free and open-source application that aims to make beginners easy to use, while providing an advanced feature for experienced users

**5*. Reference and Citation***

<https://www.solarwinds.com/resources/it-glossary/network-administration>

<https://www.techtarget.com/searchnetworking/definition/MAC-address>

<https://nmap.org/zenmap/#:~:text=Zenmap%20is%20the%20official%20Nmap,features%20for%20experienced%20Nmap%20users>.

https://cybertalents.com/blog/a-quick-how-to-guide-to-information-gathering-for-cybersecurity#:~:text=Information%20gathering%2C%20or%20data%20collection,to%20have%20in%20the%20field.