**Academic Task–3**

Submitted in partial fulfilment of the requirements for the class assignment of

# Subject: INT-301

**OPEN SOURCE TECHNOLOGY**



Submitted to:

**Dr. MANJOT KAUR**

Submitted By:

# HARI SAURABH YADAV (Reg. no. 11906428)

Topic:

Network Administrator

**Index**

1. Introduction

1.1The Objective of the Project

1.2 Description of the Project

2. System Description

2.1 Nessus Open-Source Software

2.2

3. Analysis Report

3.1 Ip Address and Machine

3.2 Machine and Ip address

3.3 Final Result of Nessus

4. References

5. Github-link

**Chapter 1**

**Introduction**

**What is a network administrator?**

A network administrator is a professional responsible for managing and maintaining computer network systems. Their role involves configuring, monitoring, and troubleshooting network hardware, software, and infrastructure components such as servers, routers, switches, firewalls, and other networking equipment.

Some of the specific tasks performed by network administrators include:

1. Designing and implementing network infrastructure Installing and configuring network equipment
2. Monitoring network performance and security Diagnosing and resolving network issues
3. Creating and managing user accounts and access privileges Implementing network policies and procedures
4. Ensuring data backups and disaster recovery plans are in place
5. Keeping up-to-date with new networking technologies and trends.

Network administrators may work in a variety of settings, including businesses, government agencies, non-profits, and educational institutions. They may also work for managed service providers (MSPs) that provide network services to multiple clients.[1]

* 1. **Objective of the Project**

This project's main goal is to ensure that the network is available, reliable, and secure. They are responsible for monitoring network performance, diagnosing and resolving network issues, creating and managing user accounts and access privileges, implementing network policies and procedures, and ensuring data backups and disaster recovery plans are in place.

* 1. **Description of the Project**

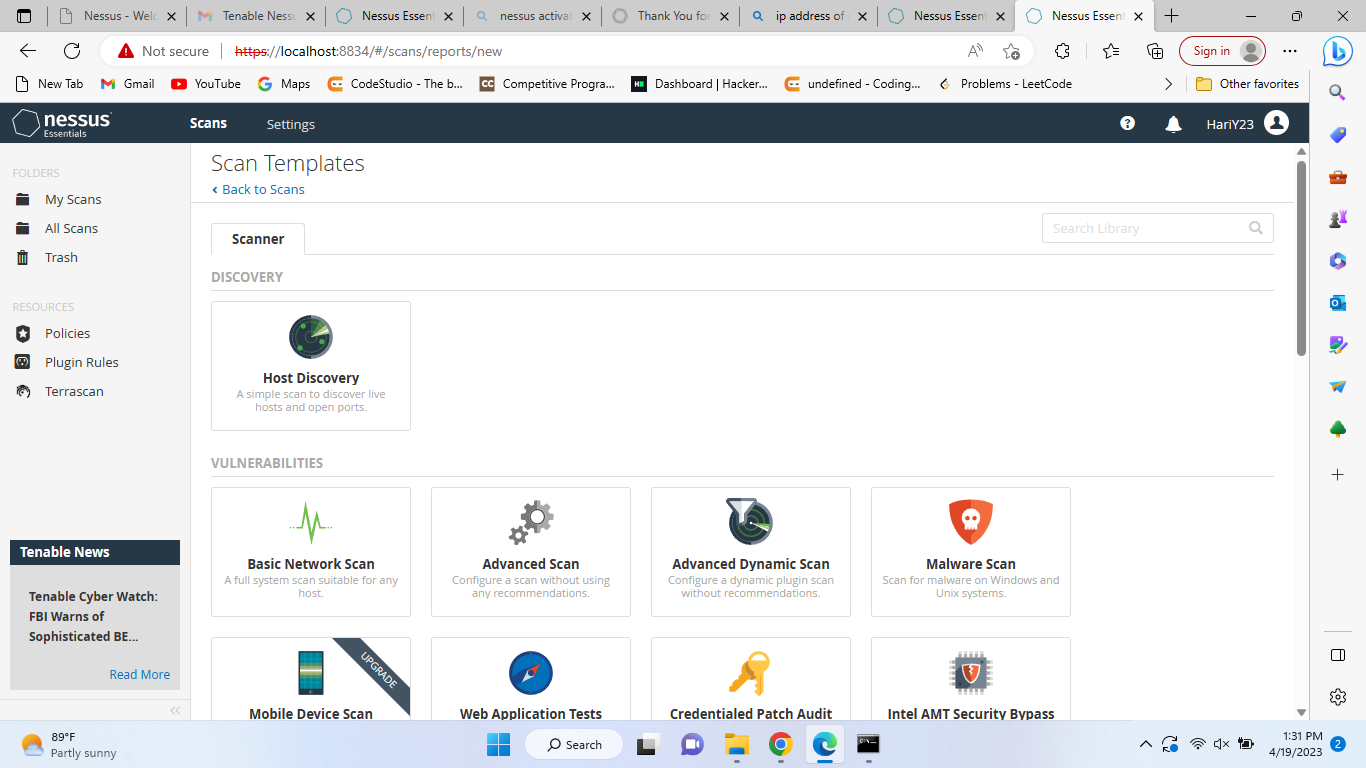
A popular open-source Nessus, I have used will tell us how much vulnerability has in any specific machine IP address.

**Chapter 2**

**System Description**

**2.1 Nessus Open-Source Software**

I have used Nessus open-source technology which is freely available on the internet. Firstly, I downloaded this then I installed it on my Windows-11 machine.



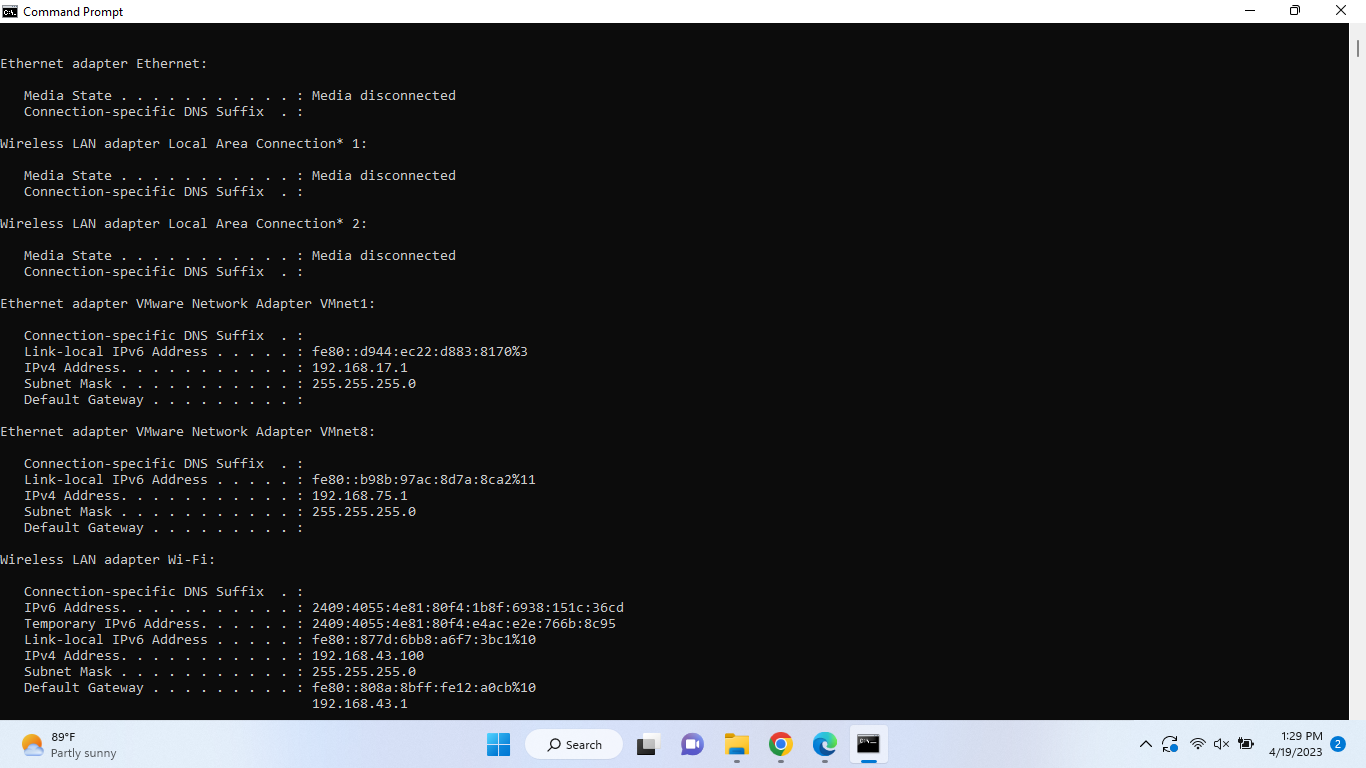
**Figure 2.1 Installed Nessus Software**

**Chapter 3**

**Analysis Report**

**3.1 Ip Address and Machine**

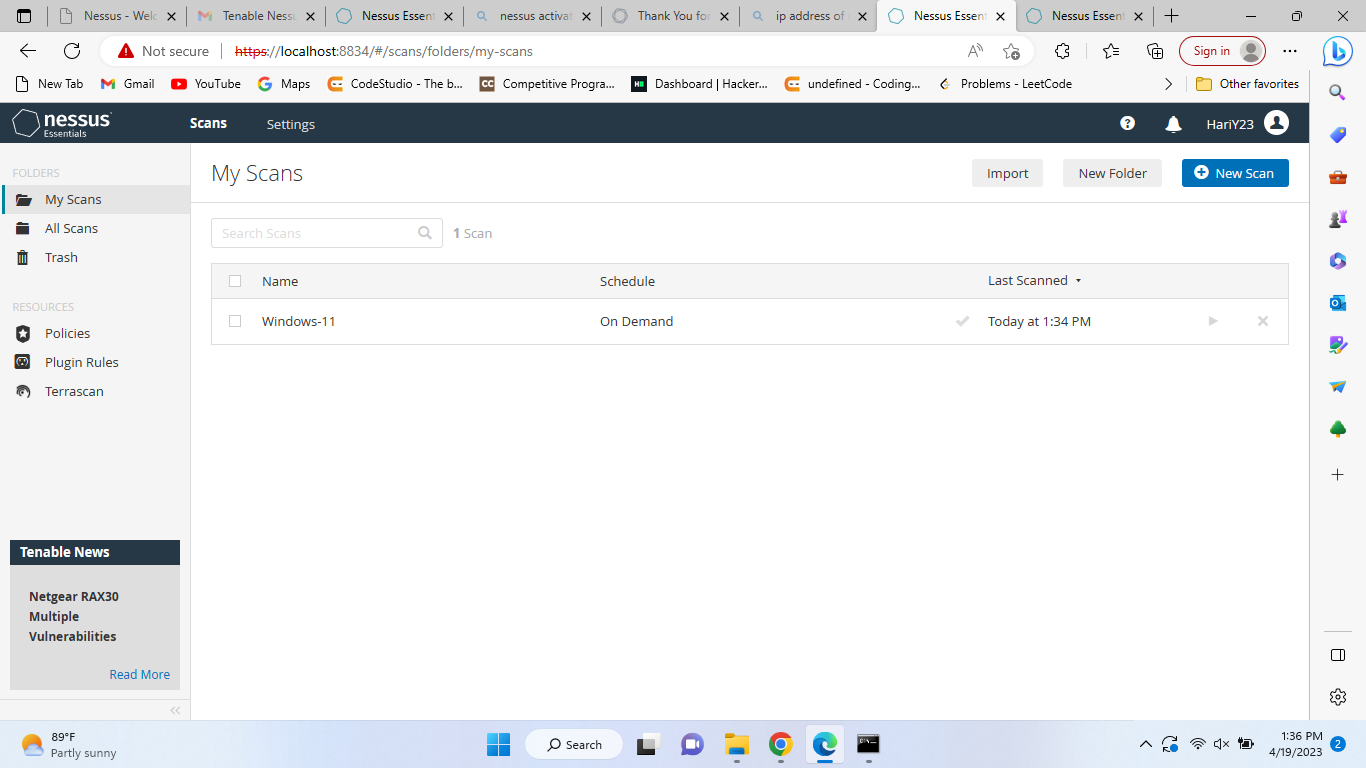
An IP address is a unique identifier assigned to every device connected to a computer network that uses the Internet Protocol for communication. It is a numerical label that allows devices to communicate with each other over the Internet and other networks. After installing this, I checked my IP address on the system by using the command prompt and the command – “ipconfig”



**Figure 3.1 Checking IP Address**

**3.2 Machine and Ip address**

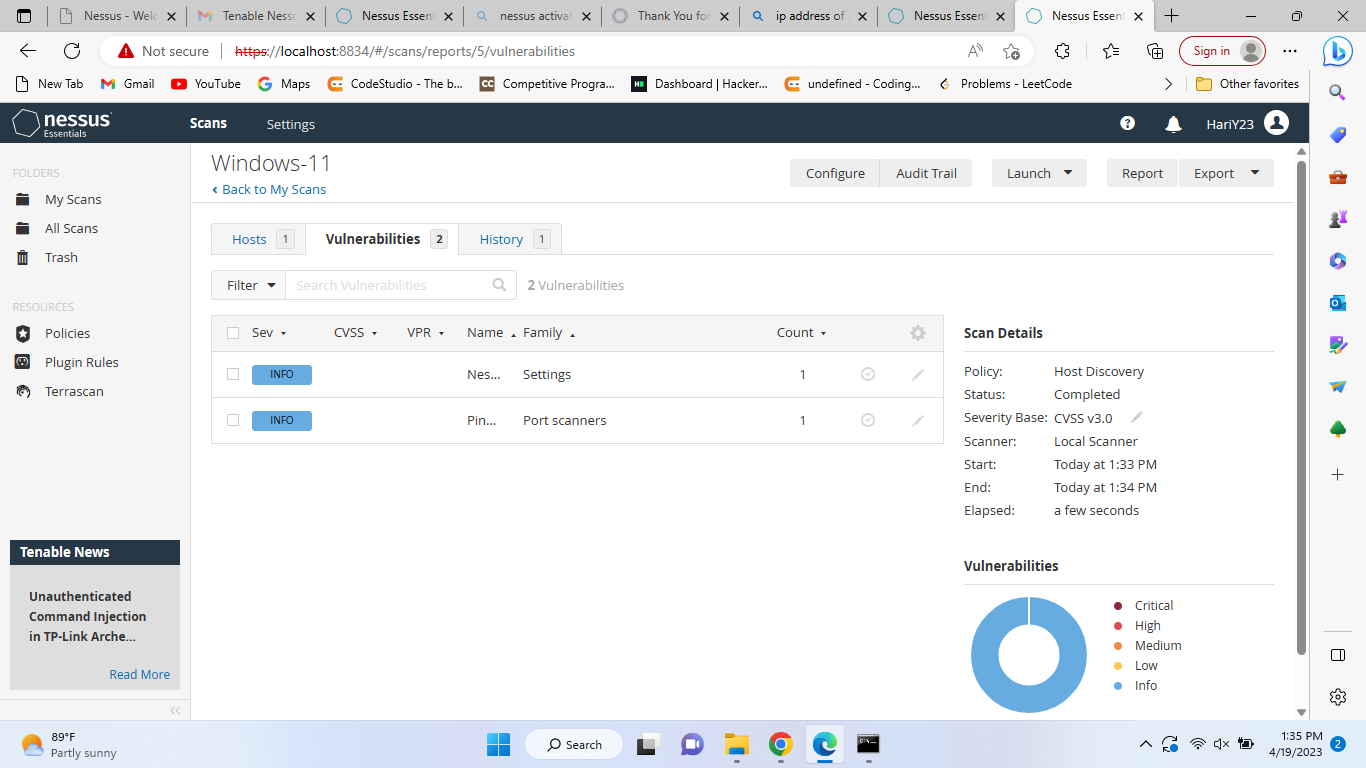
And now we have to add this(Ip-add) we have to add in Nessus software for recognizing the vulnerability of the machine network.



**Figure 3.2 Adding Ip address and Machine for Scanning**

**3.3 Final Result of Nessus**

When we complete scanning by using Nessus’s Software we get some output like the Host of the machine and what type of vulnerabilities we have.



**Figure 3.3 Getting 2 vulnerabilities of Ip 192.168.43.1 of the machine Windows-11.**

**4. References**

1. [www.comparitech.com](http://www.comparitech.com/)
2. [www.techtarget.com](http://www.techtarget.com/)
3. <https://cybersecurity.att.com/>
4. <https://bestructured.com/>
5. [www.digitalocean.com](http://www.digitalocean.com/)
6. <https://portswigger.net/>
7. <https://safetyspecial.com/>
8. <https://resources.infosecinstitute.com/>
9. [www.csoonline.com](http://www.csoonline.com/)
10. [www.nvlpubs.nist.gov](http://www.nvlpubs.nist.gov/)