**NITHIN THOMAS NINAN ERUTHICKAL**

**8866468**

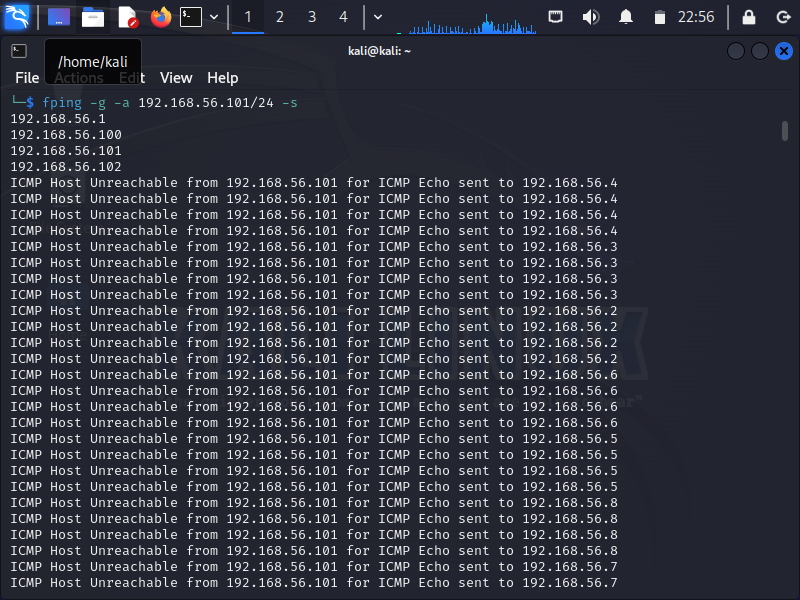
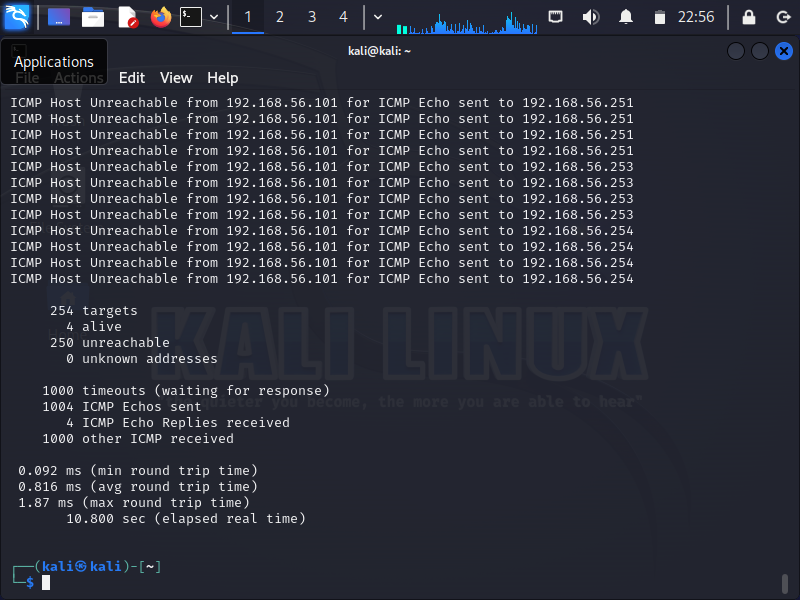
**Assignment #4**

**12-Feb-2024**

**Task 1**

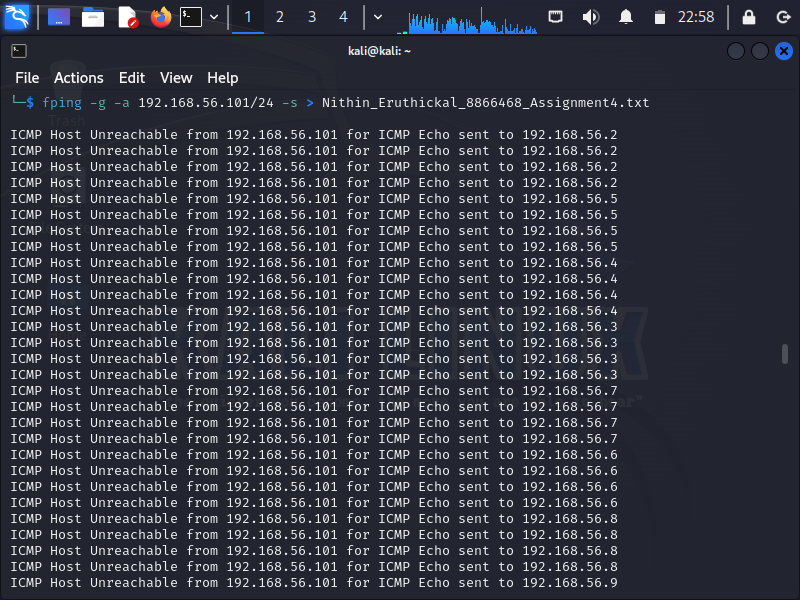
Launch the fping command line tool and select the parameters to display the active systems (-a), create a target list (-g), and obtain cumulative statistics (-s).

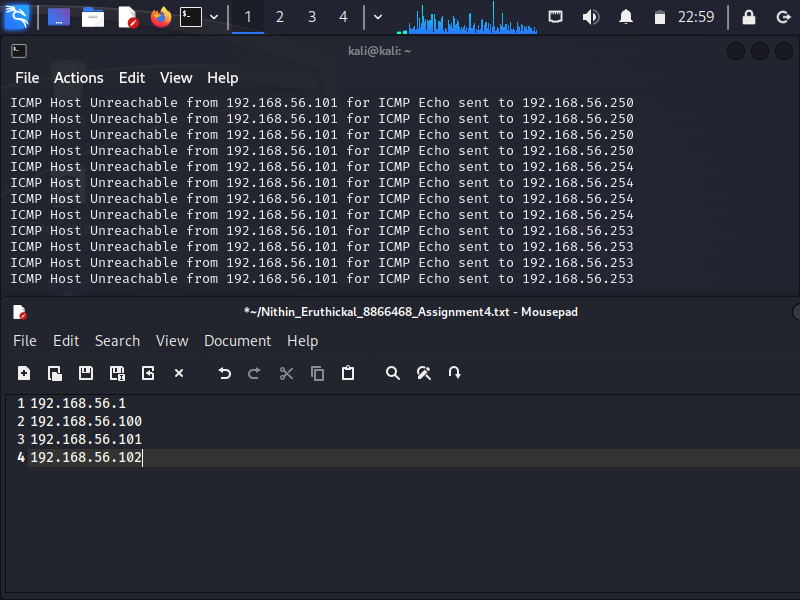
Run the following command: fping -g -a 192.168.56.101/24-s

The command is used to save the active systems ip to text file

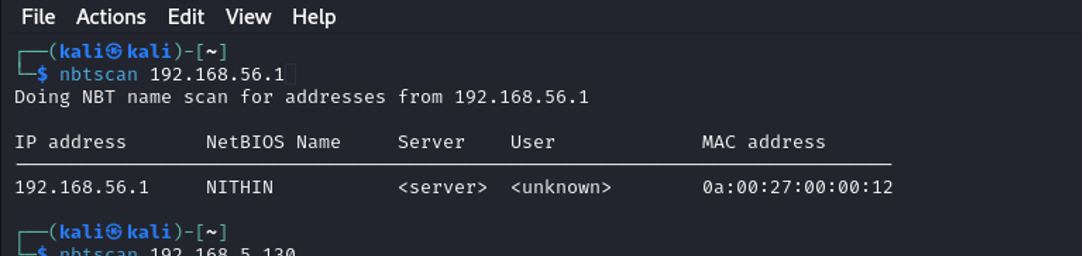
Command used: fping -g -a 192.168.56.101/24 s > Nithin\_Eruthickal\_8866468\_Assignment4.txt

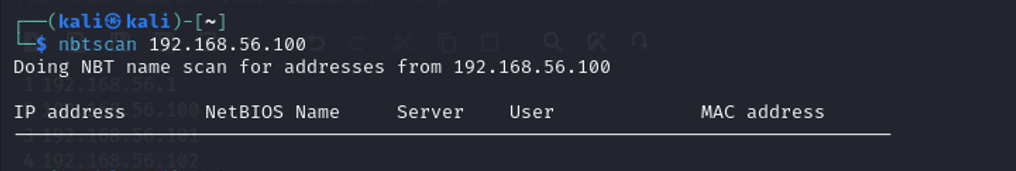


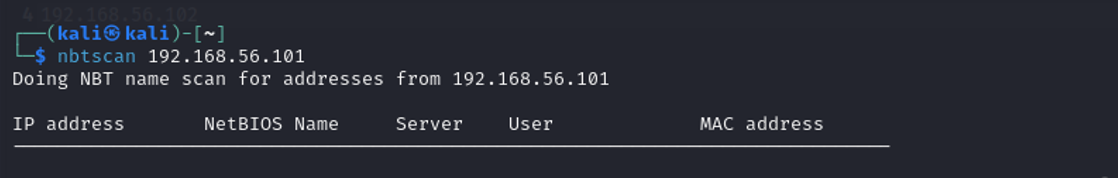


We use the command nbtscan to scan the ip address of each system.

The command can be used to find IP Address,NetBIOS Name, Sever,User and MAC Address.

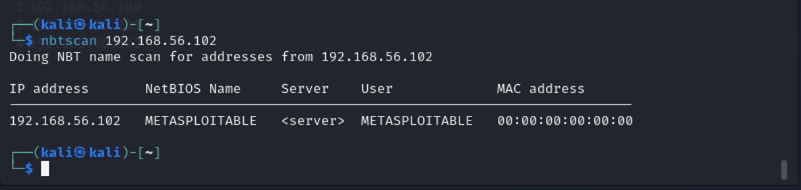






We found the IP address of the target system

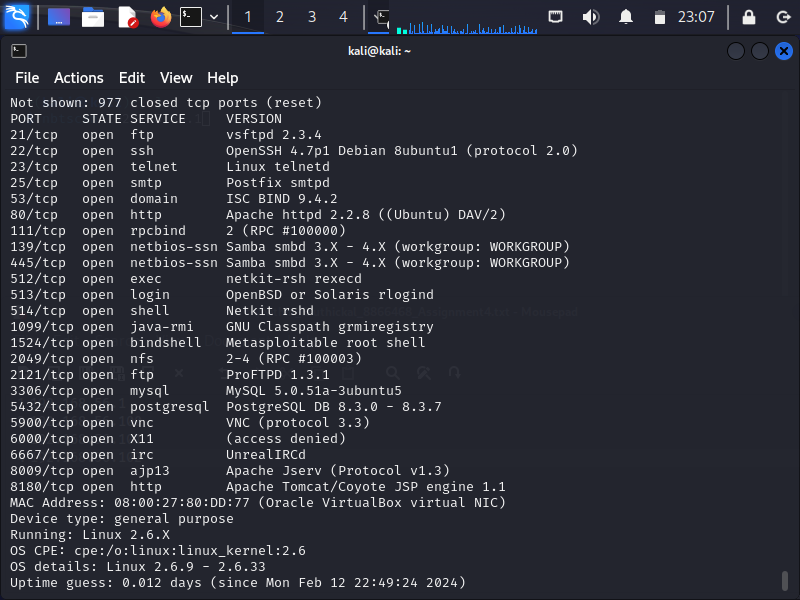
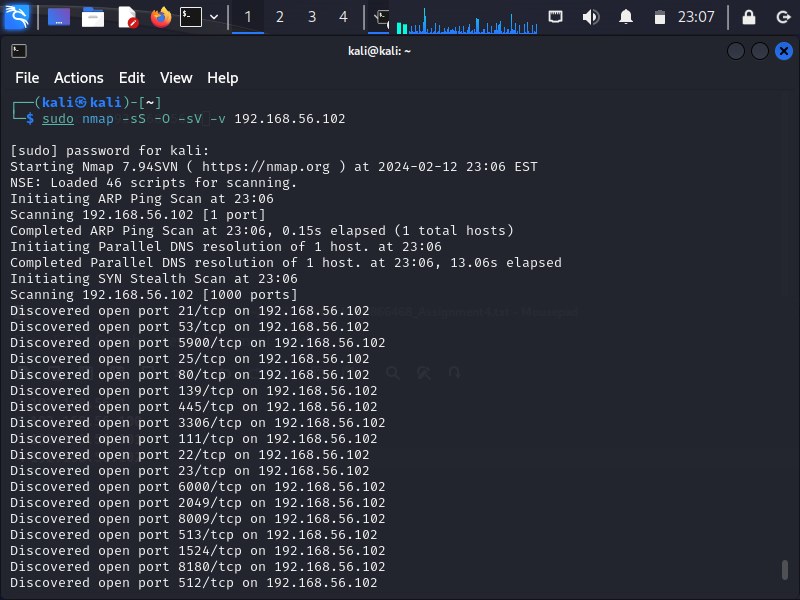
IP address: 192.168.56.102



**Task 2**

sudo nmap -sS -O -sV -v 192.168.56.102

Using this command, we can run an NMAP scan with the following options: Verbose output, OS and version identification, TCP SYN, and





**ftp**

A common network protocol called FTP (File Transfer Protocol) is used to move files over TCP-based networks like the Internet from one server to another. In order for FTP to function, two connections must be established between the systems that are attempting to communicate.

# When was it released?

# In April 1971, Abhay Bhushan introduced File Transfer Protocol (FTP) as a component of the ARPANET standard, which served as the forerunner of the contemporary internet. It has seen several modifications and versions since then.

**Is it the newest version? If not, when was it updated?**

The latest formal specification for FTP was defined in RFC 959, which was published in October 1985.

**Is there a known vulnerability for this service?**

* Many vulnerabilities in FTP implementations have been found throughout time as a result of problems such inadequate input validation, inappropriate access limits, and a lack of encryption.
* FTP bounce attacks are a prevalent vulnerability that allow an attacker to use the FTP server as a proxy to scan ports on other systems or networks. Unauthorized access or information exposure may result from this.
* Furthermore, if FTP is not utilized over a secure connection (FTP over TLS/SSL), it is vulnerable to eavesdropping and man-in-the-middle attacks since it normally transfers data in plain text.

**References**

* Wikipedia contributors. (2024, February 5). *File transfer protocol*. Wikipedia. https://en.wikipedia.org/wiki/File\_Transfer\_Protocol
* *The TCP/IP Guide - FTP Overview, history and Standards*. (n.d.). http://www.tcpipguide.com/free/t\_FTPOverviewHistoryandStandards.htm
* *RFC 959: File Transfer Protocol*. (n.d.). IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc959