Name: Shubhan Singh

Class: SE Comps B

Roll no.: 2022300118

**CCN Experiment 8**

NMAP

**Aim:** Network Mapping using Nmap

**Objective:** The objective of this lab assignment is to introduce students to NMAP, a powerful network scanning tool widely used for network discovery and security auditing. Through this assignment, students will gain hands-on experience in using NMAP to scan networks, identify open ports, detect operating systems, and gather valuable information about networked devices.

**Requirements:**

● Access to a computer with NMAP installed (can be installed on Windows, Linux, or macOS).

● Basic understanding of networking concepts

Tasks:

1. Installation and Setup:

○ Install NMAP on your system if not already installed. (<https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/>)

○ Familiarize yourself with the basic syntax and options of NMAP.

2. Basic Scanning:

○ Perform a simple ping scan on a target IP address to determine its availability.

A screen shot of a computer

Description automatically generated

○ Conduct a TCP SYN scan on a target IP range to identify open ports.

3. Service Version Detection:

○ Perform a service version detection scan on a target IP to identify the version of services running on open ports.

4. Operating System Detection:

○ Use NMAP to detect the operating system of a target device.

5. Scripting with NMAP:

○ Write a simple NMAP script to automate a scanning task of your choice.

**Problem Statements:**

1. Scan a given network range and identify all active hosts.

A screenshot of a computer program

Description automatically generated

1. Identify the top 5 most commonly open ports on a specific target.

A computer screen shot of a program

Description automatically generated

1. Determine the MAC address of a target device using NMAP.

(given in previous output)

1. Perform a scan to detect the presence of HTTP and HTTPS services on a target network.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. Find out if a particular host has FTP service running on it.

A computer screen with white text

Description automatically generated

1. Identify the SSH version running on a given host.

A screenshot of a computer error

Description automatically generated

1. Scan a range of IP addresses and list all hosts that have Telnet service running.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A black background with white text

Description automatically generated

1. Determine the operating system of a target host using NMAP.

A computer screen shot of text

Description automatically generated

1. Identify any SQL services running on a given network.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. Find out if a specific host has Remote Desktop Protocol (RDP) enabled.

A computer screen with white text

Description automatically generated

1. Scan a target network and determine if any hosts are running DNS services.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Detect if a host has SNMP (Simple Network Management Protocol) enabled.

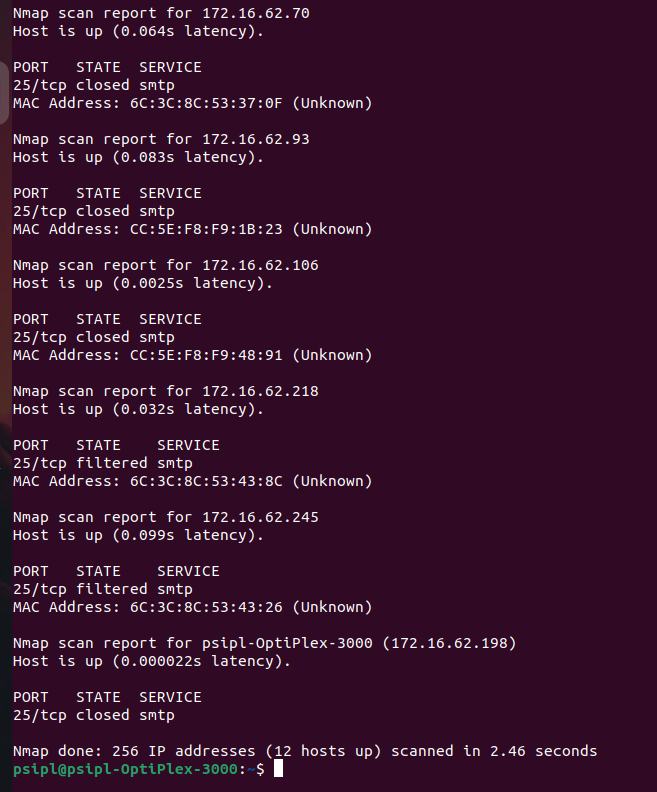
A computer screen with white text

Description automatically generated

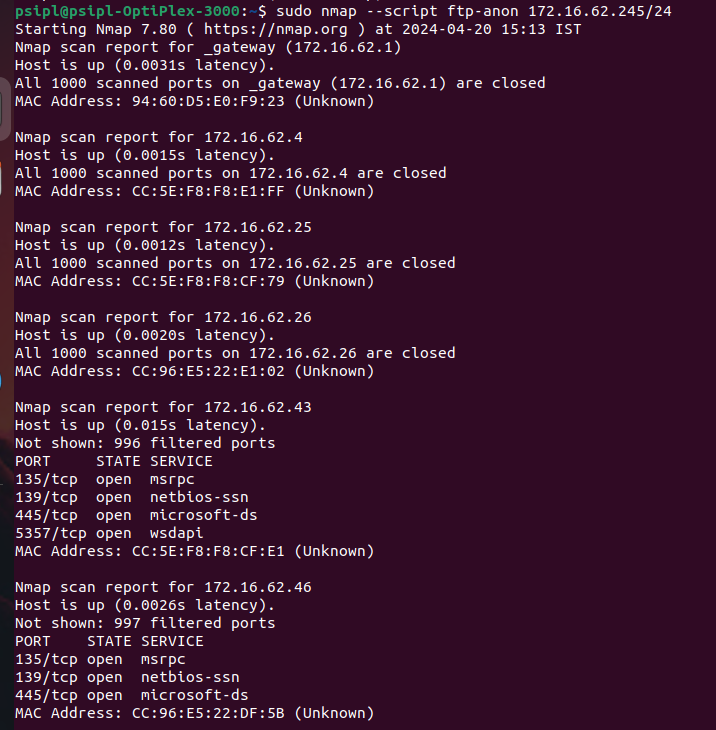
1. Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network.

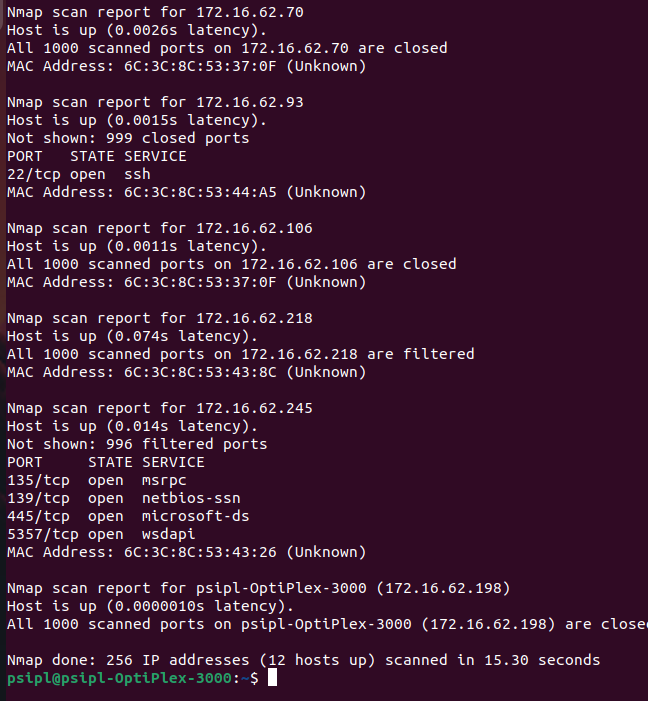
A screenshot of a computer program

Description automatically generated



1. Determine if a target network has any active FTP servers allowing anonymous login.





1. Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Detect if a target host has any open NFS (Network File System) shares.

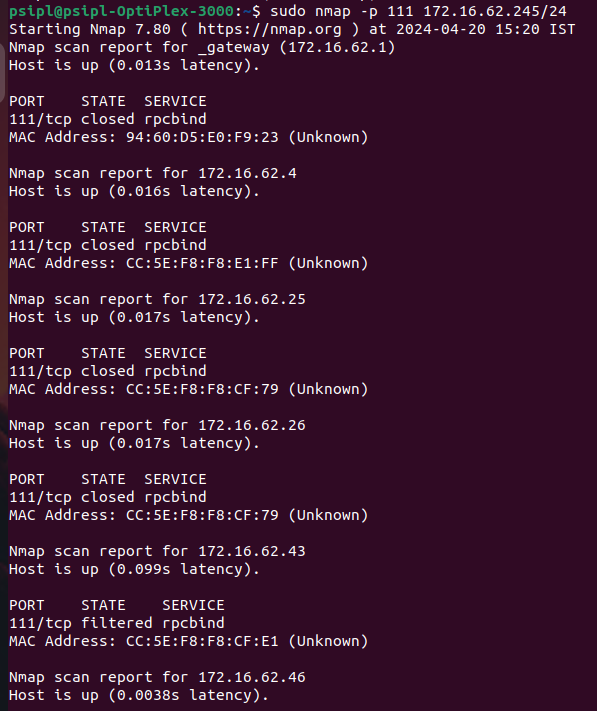
A computer screen with white text

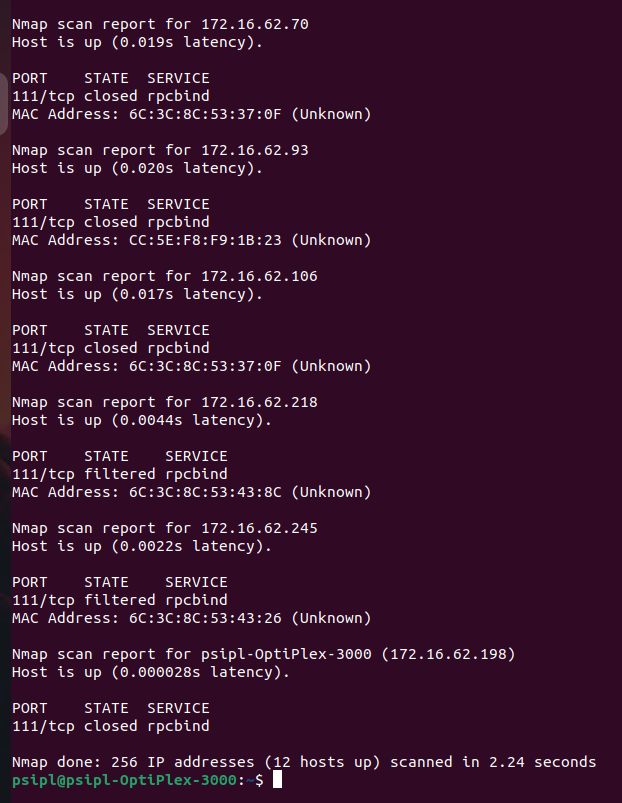
Description automatically generated

1. Identify the presence of any MySQL database servers on a given network.

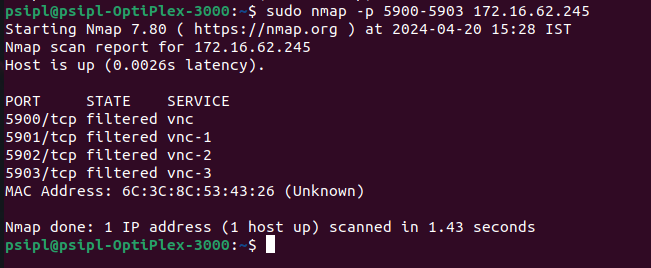
(already shown in SQL server scan)

1. Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.

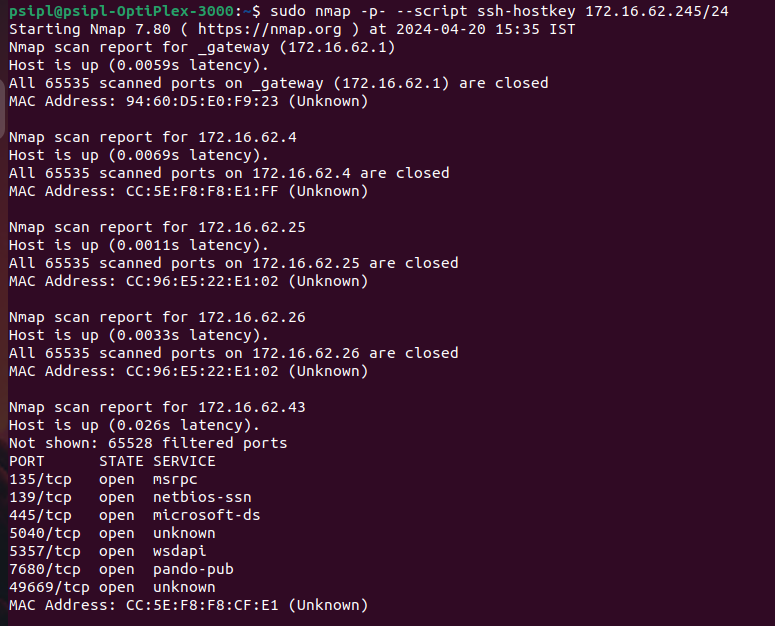


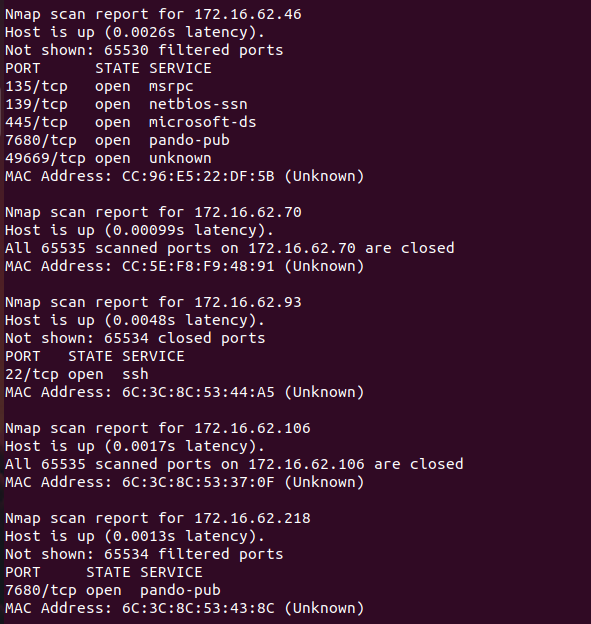


1. Detect if a specific host has any open VNC (Virtual Network Computing) ports.



1. Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.





A computer screen shot of a computer

Description automatically generated