Roll No: 09
Name: Shreya Bagade
Date: 01/09/2023

LAB ASSIGNMENT NO:08

Aim: Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.

Lab Outcome Attained: Use tools like sniffers, port scanners and other related tools for analyzing packets in a network.

Theory:

1. What is Port Scanning? What is NMAP?

Port Scanning: Port scanning is a technique used in computer networking and cybersecurity to discover open network ports on a target system. A network port is a virtual endpoint for communication, and each port serves a specific purpose (e.g., web traffic on port 80, email on port 25). Port scanning tools and techniques are commonly used by security professionals and hackers to assess the security posture of a network, identify potential vulnerabilities, and gather information about services running on a target system.

Nmap (Network Mapper): Nmap is a powerful and open-source network scanning tool that is widely used for network discovery and security auditing. It allows users to discover devices and services running on a network and provides detailed information about open ports, services, and operating systems. Nmap is known for its flexibility and extensive feature set, making it a valuable tool for both network administrators and security experts.

2. Explain in brief different states of port. (open, closed, filtered, unfiltered, open | filtered and closed | filtered)

Different States of Ports:

Open: An "open" port indicates that a network service or application is actively listening and available to accept incoming connections. This state implies that communication is possible, and a connection can be established if the client and server agree on the protocol.

Closed: A "closed" port means that there is no application or service listening on that port. The operating system may respond with a

"Connection Refused" message to indicate that no service is available.

Filtered: A "filtered" port indicates that a firewall or filtering mechanism is actively blocking incoming connection attempts to the port. The firewall may be configured to silently drop connection requests or respond with an ICMP "Destination Unreachable" message.

Unfiltered: An "unfiltered" port means that the port is accessible, but the scanner couldn't determine whether it is open or closed. This state often occurs when a firewall allows all packets, including those destined for closed ports, to pass through without filtering.

Open | Filtered: The "open | filtered" state indicates that the scanner couldn't reliably determine whether the port is open or filtered. This state can occur when a firewall or intrusion detection system (IDS) behaves in a way that obscures the true state of the port.

Closed | Filtered: The "closed | filtered" state indicates that the scanner couldn't reliably determine whether the port is closed or filtered. Similar to "open | filtered," this state can occur when a firewall or filtering device generates ambiguous responses.

3. Write the commands for following type of port scanning techniques using NMAP, Explain in 4 to 5 lines how each of them works.

TCP Connect scan:

nmap -sT ipadress

These scans are so called because UNIX sockets programming uses a system call named connect() to begin a TCP connection to a remote site. If connect() succeeds, a connection was made. If it fails, the connection could not be made (the remote system is offline, the port is closed, or some other error occurred along the way). This allows a basic type of port scan, which attempts to connect to every port in turn, and notes whether or not the connection succeeded. Once the scan is completed, ports to which a connection could be established are listed

as open, the rest are said to be closed.

TCP SYN scan:

#nmap -sS ipadress

SYN or Stealth scanning makes use of this procedure by sending a SYN

packet and looking at the response. If SYN/ACK is sent back, the port is open and the remote end is trying to open a TCP connection. The scanner then sends an RST to tear down the connection before it can be established fully; often preventing the connection attempt appearing in application logs. If the port is closed, an RST will be sent.

FIN Scan:

#nmap -sF ipaddress

The idea behind these type of scans is that a closed port should respond

with an RST upon receiving packets, whereas an open port should just

drop them (it's listening for packets with SYN set). This way, you never

make even part of a connection, and never send a SYN packet; which is

what most IDS' look out for. The FIN scan sends a packet with only the FIN flag set.

Null Scan:

#nmap -sN target

The Null Scan is a type of TCP scan that hackers — both ethical and malicious — use to identify listening TCP ports. In the right hands, a Null Scan can help identify potential holes for server hardening, but in the wrong hands, it is a reconnaissance tool. It is a pre-attack probe. A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags.

XMAS Scan:

#nmap -sX target

The Xmas Tree scan sets the FIN, URG and PUSH flags are set. This scan will work on UNIX and related systems and cause the kernel to drop the packet if the receiving port is open.

Roll No: 09
Name: Shreya Bagade
Date: 01/09/2023

ACK Scan:

#nmap -sA target

This scan type sends ACK packets to a host.

If an RST comes back, the port is classified "unfiltered" (that is, it was allowed to send its RST through whatever firewall was in place). If nothing comes back, the port is said to be "filtered", that is, the firewall prevented the RST coming back from the port.

Ping Sweep:

nmap -sP IP address of gateway

This scan type lists the hosts within the specified range that responded to a ping. It allows you to detect which computers are online, rather than which ports are open.

Service and version detection:

#nmap -sV target

Nmap attempts to identify the services running on open ports by analyzing their responses. It sends probes to determine service types and versions, providing valuable information about the target system's software stack.

Port and Port range scanning:

#nmap -p23 ipaddress scans specific port

#nmap -p23-443 ipaddress scans ports ranging from 23 to 443

These commands allow you to specify individual ports or port ranges to scan. For example, -p 80,443 scans ports 80 and 443, while -p- scans all 65,535 ports.

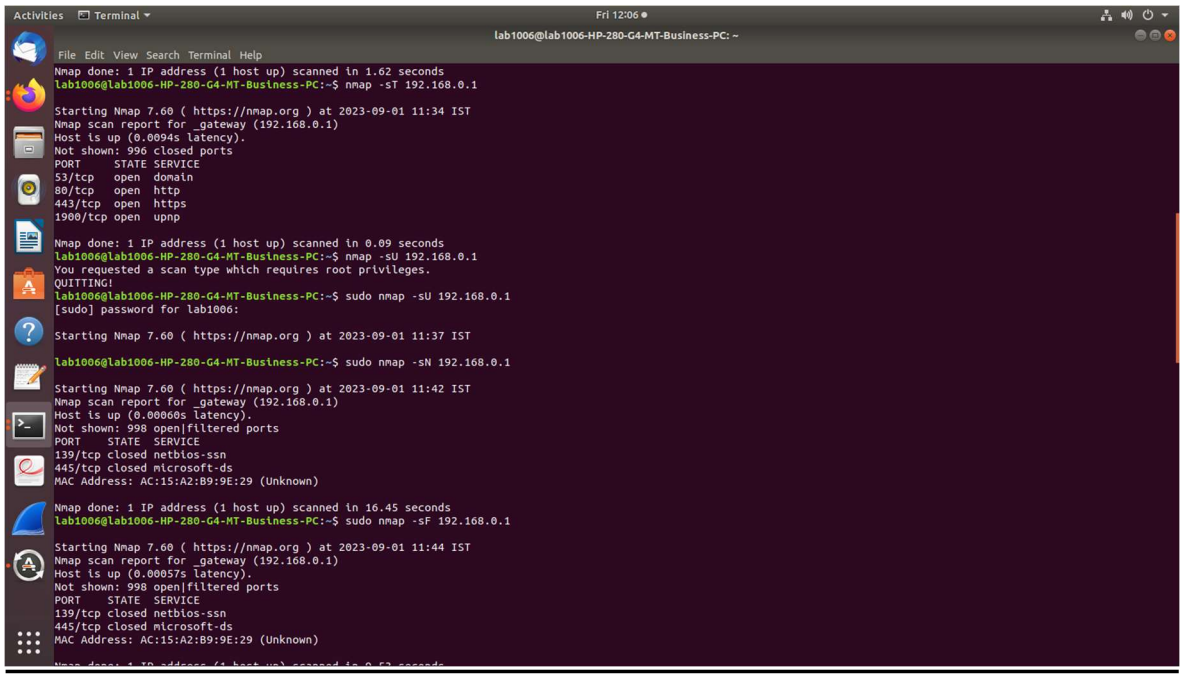
OS fingerprinting:

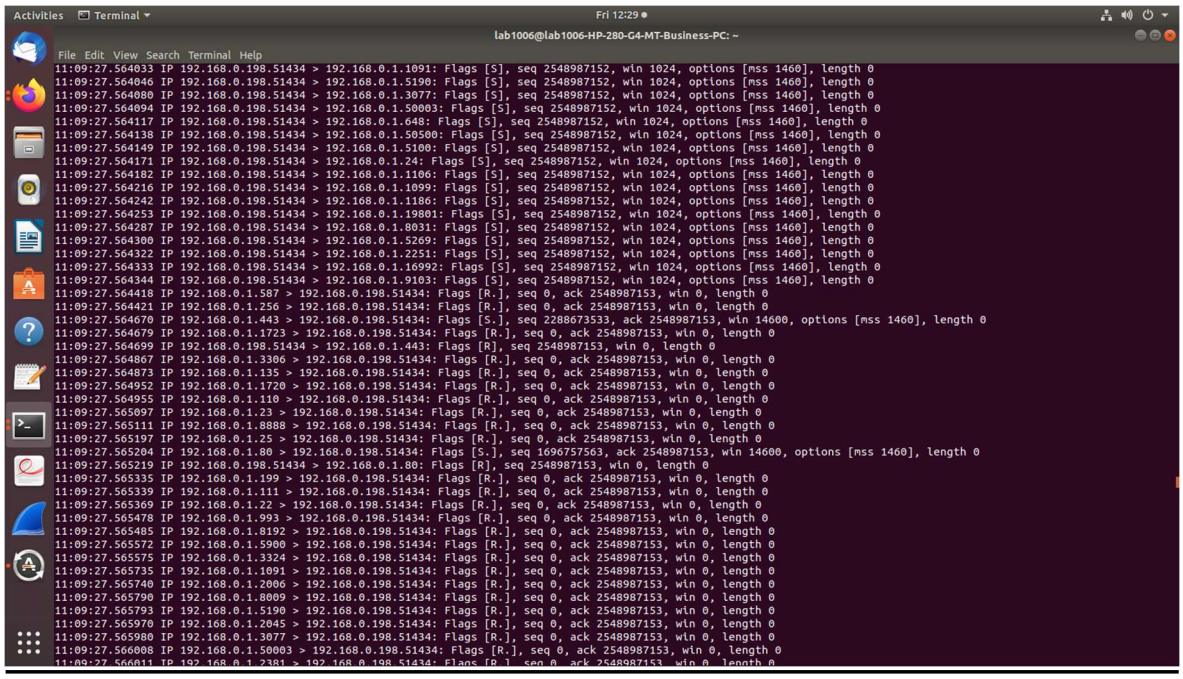
#nmap -O ipaddress

Nmap sends a series of TCP and UDP packets to the remote host and

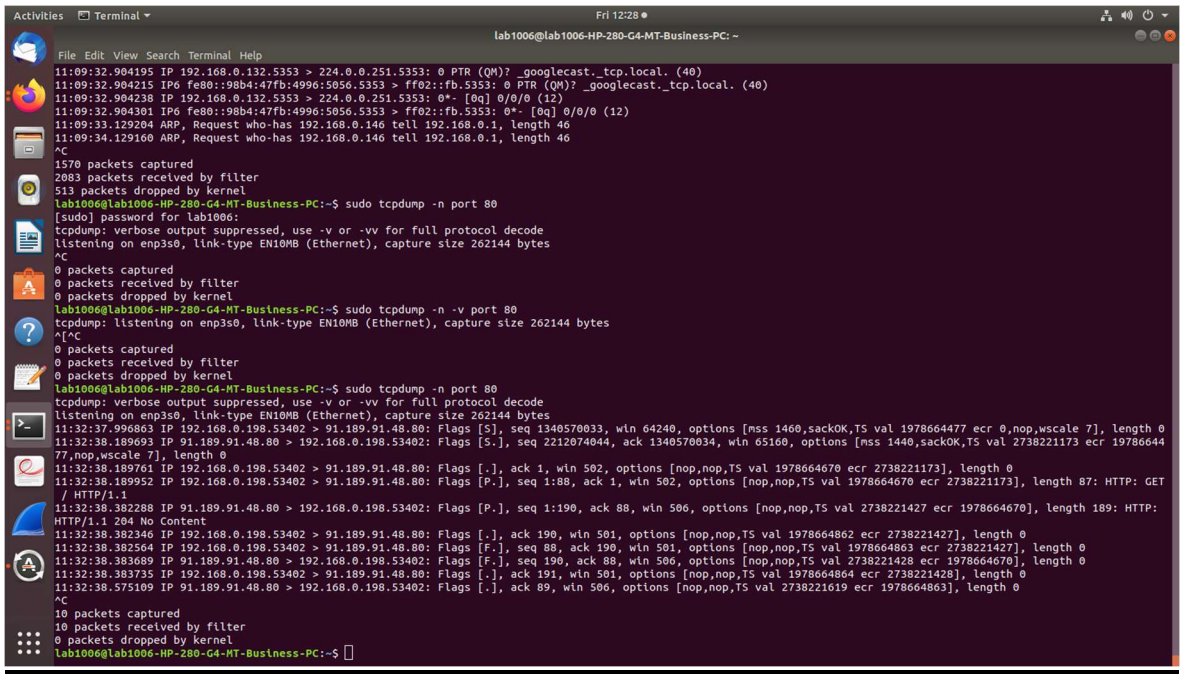
examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match.

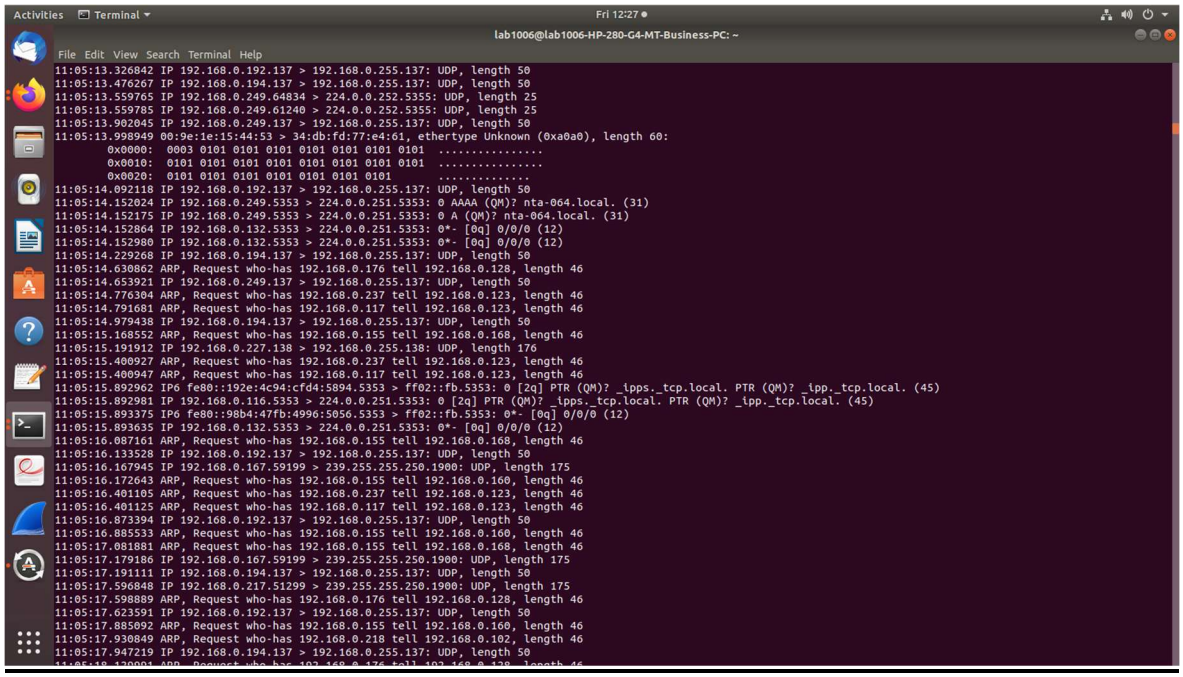
Output Screenshots:



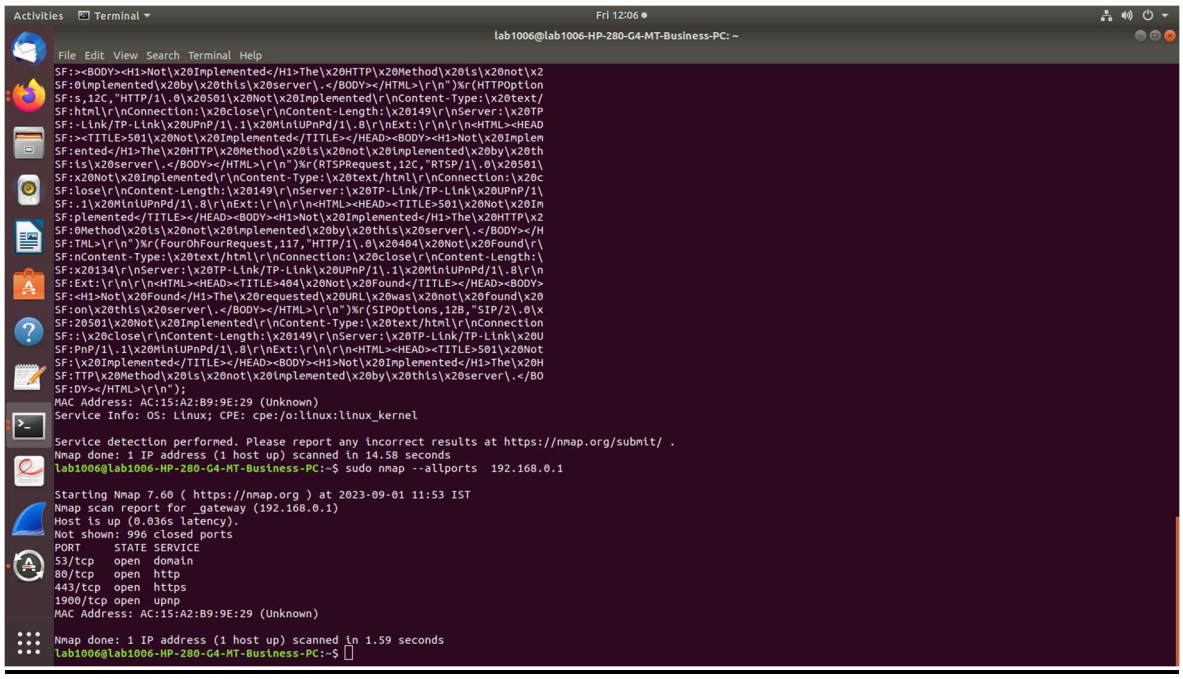


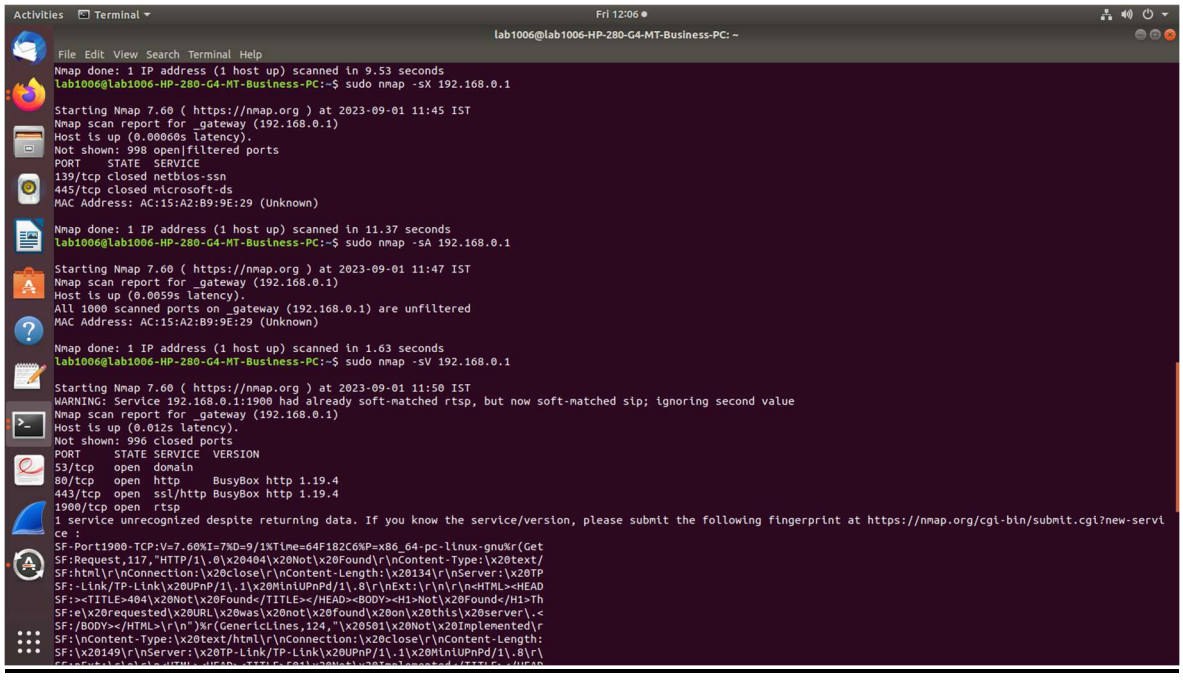
Roll No: 09
Name: Shreya Bagade
Date: 01/09/2023



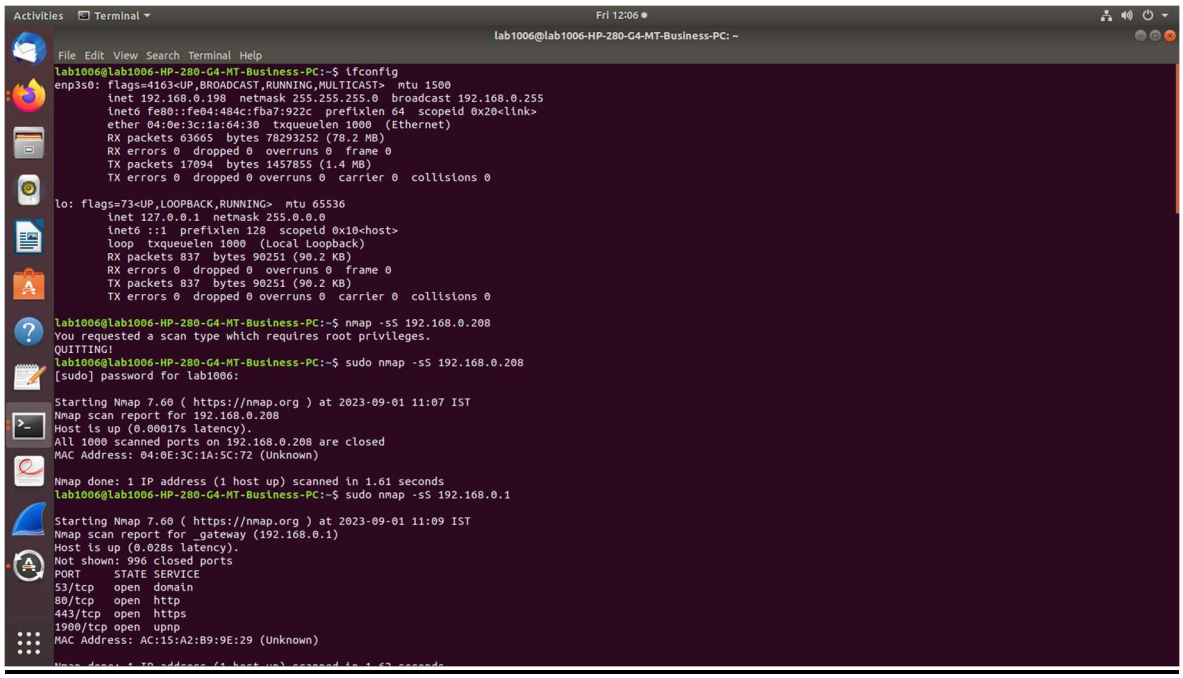


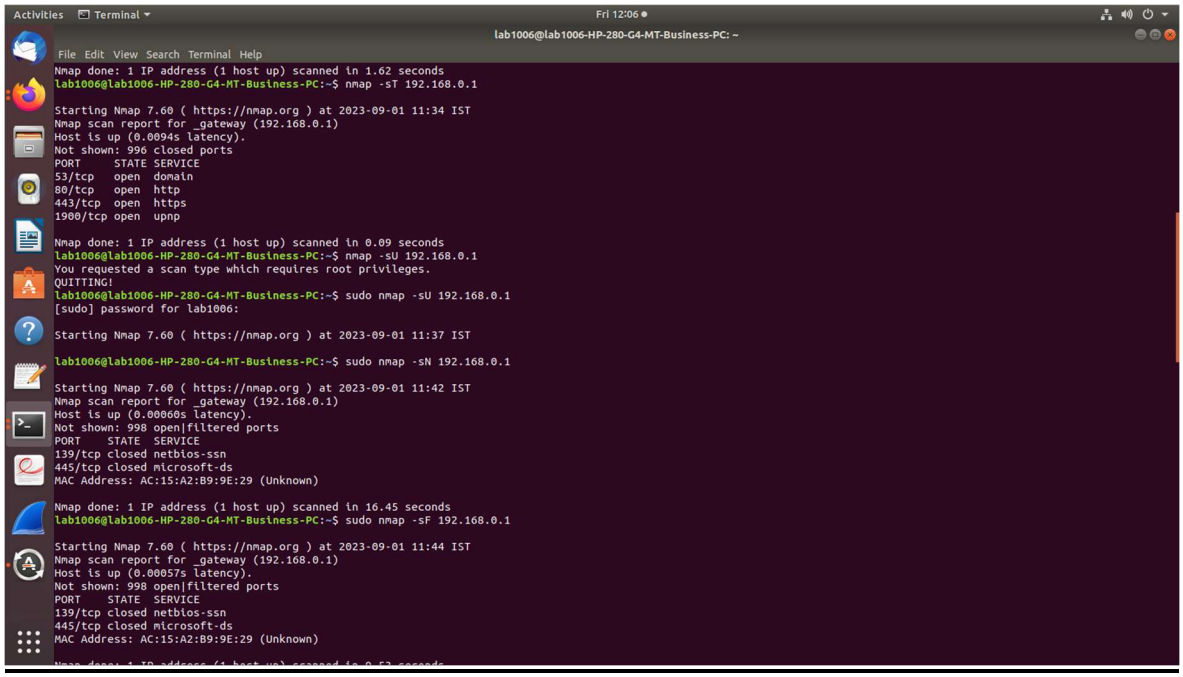
Roll No: 09
Name: Shreya Bagade
Date: 01/09/2023





Roll No: 09
Name: Shreya Bagade
Date: 01/09/2023





Conclusion: This experiment focused on the installation and practical usage of Nmap, a versatile network scanning tool. By exploring various options and techniques, such as scanning for open ports, conducting OS fingerprinting, ping scans, TCP and UDP port scans, we gained valuable insights into network reconnaissance and vulnerability assessment. Nmap's capabilities in mapping network landscapes and identifying potential security risks make it an indispensable tool for cybersecurity professionals and network administrators.