LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

INT301 – CA03

Name of the student: Amar Jyoti
Section: KE010
Roll no. 27

Name of the faculty: Manpreet Singh
Registration no: 11905396

Introduction :-

In today's interconnected world, networks are critical for communication and data exchange. However, with the growing complexity and size of networks, it becomes essential for organizations to regularly assess the security posture of their networks and identify any potential vulnerabilities. Network scanning is a crucial technique used by cybersecurity professionals to discover devices connected to a network and gather information about them.The objective of this project was to utilize open source software, specifically Nmap (Network Mapper), to perform network scanning and retrieve various details about the devices connected to the network. The information gathered includes IP addresses, hostnames, services running on each host, and the identification of the operating system (OS) running on each host. By conducting comprehensive network scanning, the project aimed to create a report that provides insights into the network's current state, helps identify potential vulnerabilities, and assists in strengthening the overall network security posture.The use of open source software allows for cost-effective and customizable solutions, making Nmap an ideal tool for network scanning. The project followed ethical guidelines and proper authorization to ensure compliance with network security best practices. The resulting report provides valuable information for organizations to make informed decisions and take necessary actions to protect their network from potential security risks.

Objective :-

The objective of the project was to use open source software (specifically Nmap) to perform network scanning and gather information about all the devices connected to the network. This includes retrieving details such as IP addresses, hostnames, services running on each host, and identifying the operating system (OS) running on each host. The ultimate goal was to create a comprehensive report of the network's current state and its connected devices for further analysis and network security assessment.

Scope of the Project:

The scope of this project was limited to utilizing Nmap, an open source software, for network scanning to gather information about devices connected to the network. The project covered the following areas:

Network Scanning: The project focused on using Nmap to scan the network and retrieve details about live hosts, including IP addresses, hostnames, and services running on each host.

Host Information Retrieval: The project aimed to gather comprehensive information about the services running on each host, including service version detection, OS detection, and other configuration details using Nmap's -A option.

Hostname Scanning: The project utilized Nmap's -sL option to scan and retrieve hostnames associated with the IP addresses in the specified subnet.Operating System Identification: The project included using Nmap's OS detection feature to identify the operating system running on each host using the -O option.

Report Generation :-

The project involved creating a report in the form of a text file that contained the results of the network scans, including IP addresses, hostnames, services, and operating systems identified.

The project's scope did not include any actions that could potentially harm or compromise the network or devices, such as exploiting vulnerabilities or performing intrusive scans without proper authorization. The project also followed ethical guidelines and complied with network security best practices to ensure responsible and legal use of network scanning techniques.

The project involved creating a report in the form of a text file that contained the results of the network scans, including IP addresses, hostnames, services, and operating systems identified.

The project's scope did not include any actions that could potentially harm or compromise the network or devices, such as exploiting vulnerabilities or performing intrusive scans without proper authorization. The project also followed ethical guidelines and complied with network security best practices to ensure responsible and legal use of network scanning techniques.

Network Scan Report

Purpose :-

The purpose of this project is to use open source software to scan the netw ork and gather information about network members, including information about services, hostnames, and operating systems.

Tools :-

Nmap (Network Mapper): Open source software for network discovery and security analysis.

Methodology :-

Nmap installation:

Nmap is downloaded and installed from the official website (https://nmap. org/) according to the installation instructions of the relevant project.

Purpose :-

The purpose of this project is to use open source software to scan the netw ork and gather information about network members, including information about services, hostnames, and operating systems.

Tools :-

Nmap (Network Mapper): Open source software for network discovery and security analysis.

Methodology :-

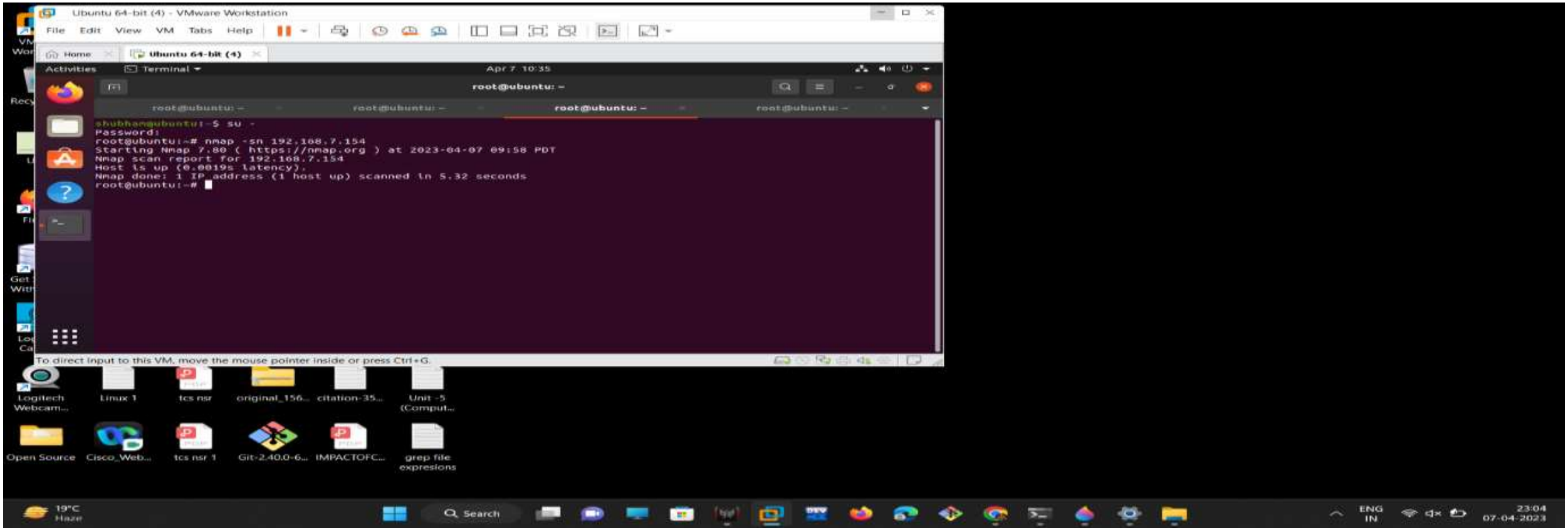
Nmap installation:

Nmap is downloaded and installed from the official website (https://nmap. org/) according to the installation instructions of the relevant project.

Network Scan Report :-

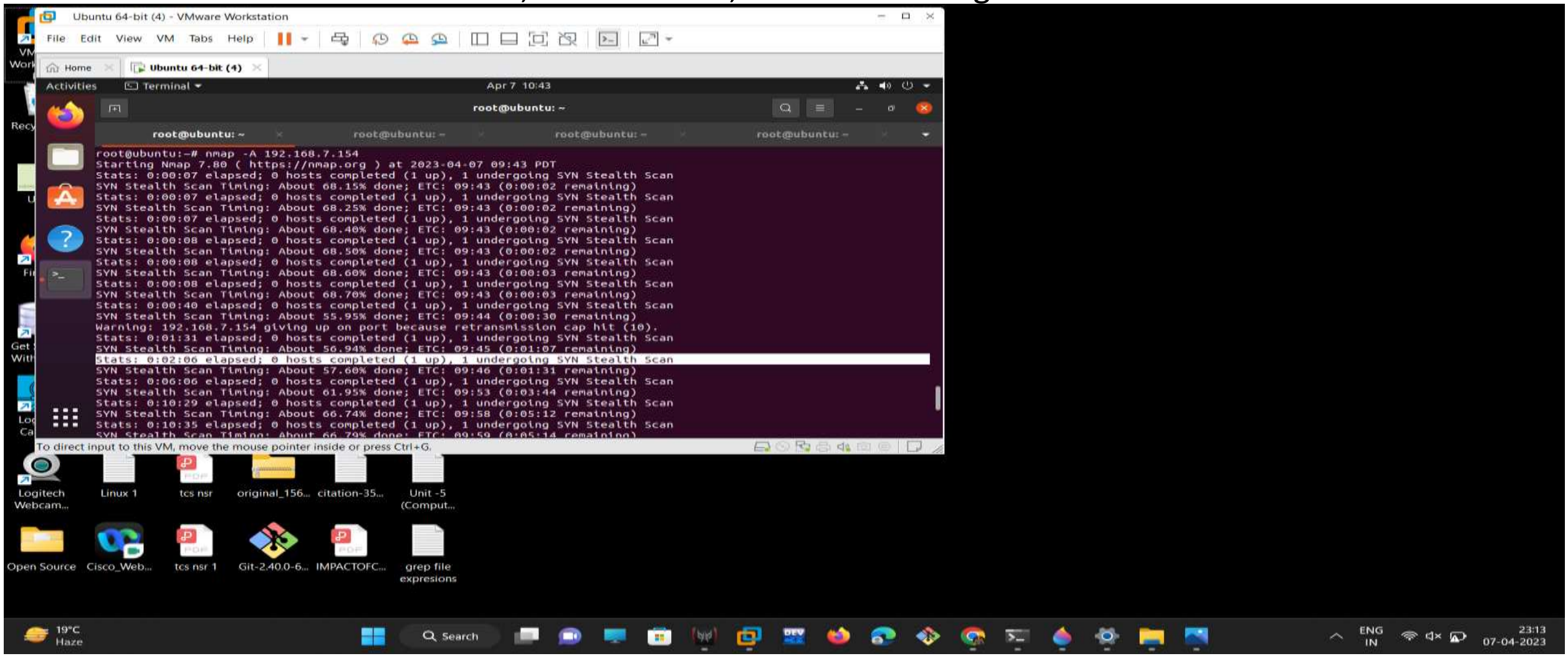
Nmap is running on a specific subnet
(For example, 192.168.1.0/24).
This allows us to discover all active hosts in the subnet and store their IP addresses.

Nmap -sn 192.168.7.154



Retrieving Host Information :-

After identifying the live hosts, a more comprehensive scan was performed using Nmap with the -A option to retrieve detailed information about the services running on a specific host. This included service version detection, OS detection, and other configuration details.



Ubuntu 64-bit (4) - VMware Workstation

File Edit View VM Tabs Help

Home | Ubuntu 64-bit (4)

Activities | Terminal | Apr 8 08:34

root@ubuntu: ~

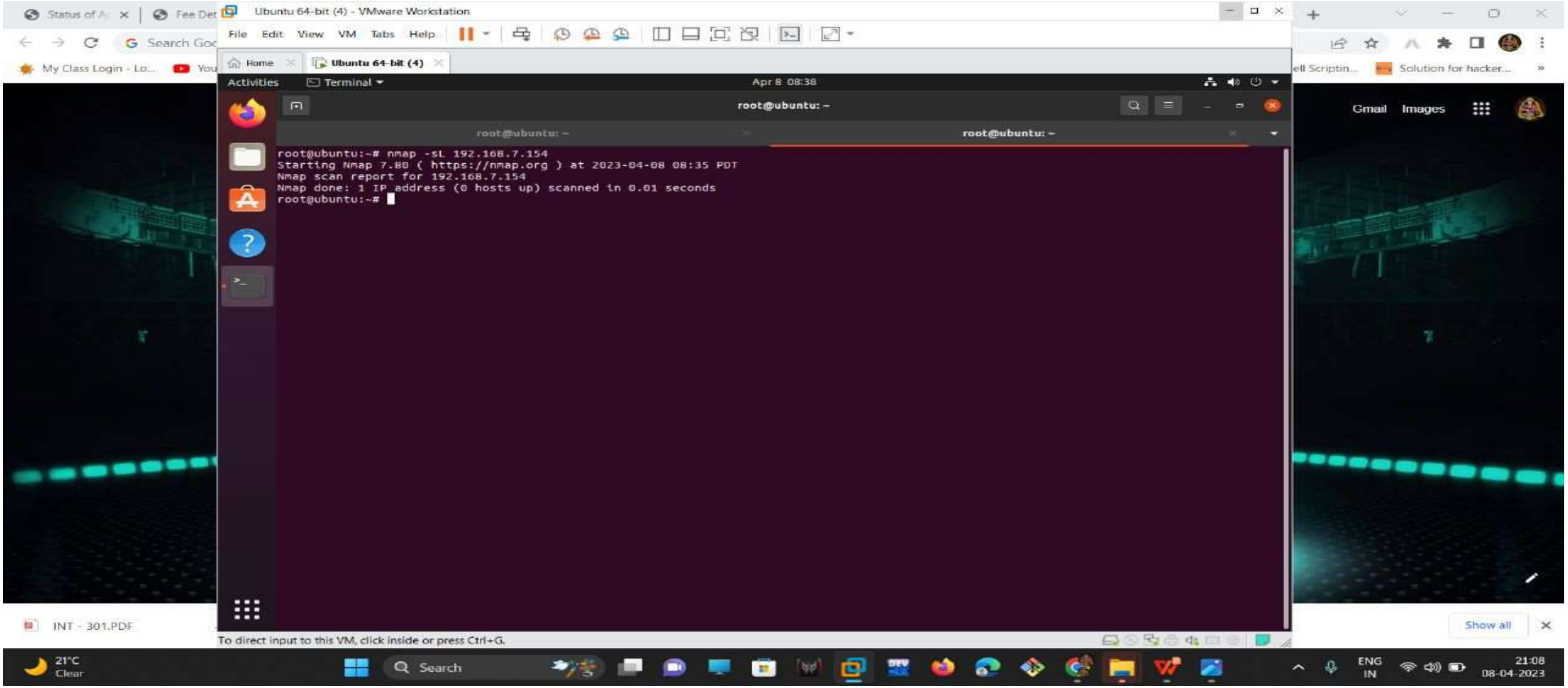
```
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.50% done; ETC: 04:00 (0:00:00 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 14.29% done; ETC: 04:00 (0:00:18 remaining)
Nmap scan report for 192.168.7.154
Host is up (0.0028s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1521/tcp open  oracle-tns      Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -3s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-04-08T11:00:56
|_  start_date: N/A

TRACEROUTE (using port 139/tcp)
HOP RTT     ADDRESS
1   4.37 ms _gateway (192.168.226.2)
2   4.69 ms 192.168.7.154

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.54 seconds
root@ubuntu:~#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NH105 Construction | Search | ENG IN | 21:04 08-04-2023

Hostname Scanning :-

The hostname of the hosts was scanned using the -sL option with Nmap, which performed a simple list scan and displayed the hostnames associated with the IP addresses in the specified subnet.

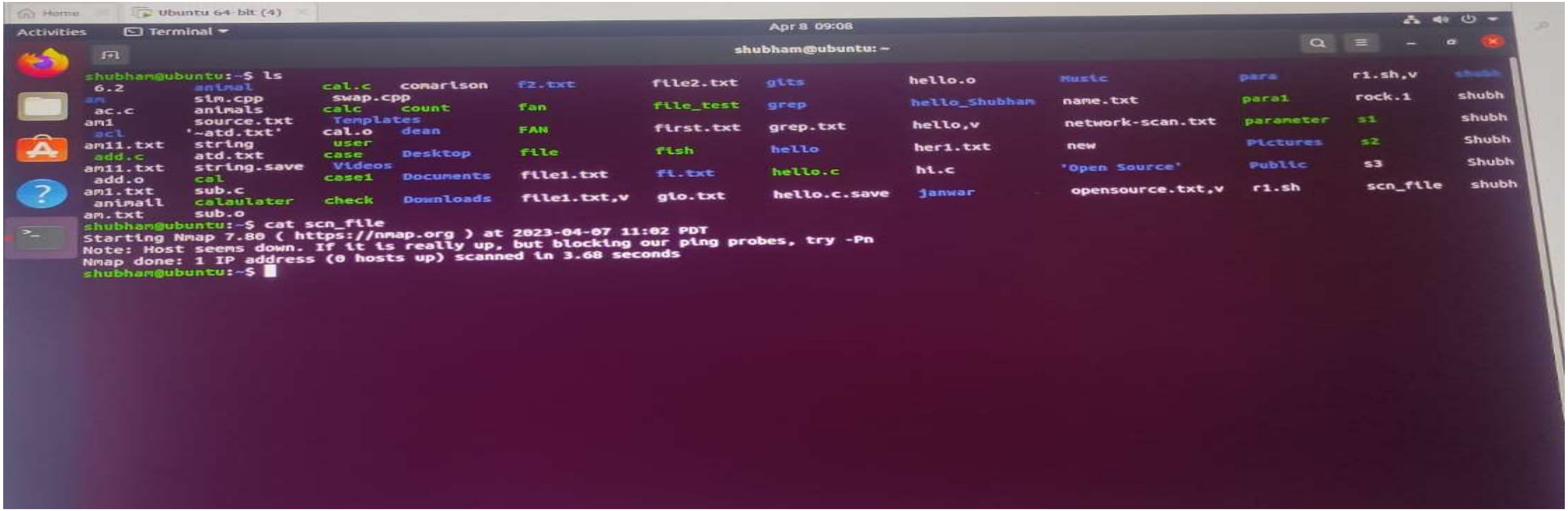


Saving Results :-

The results of the Nmap scans were saved to a text file named "scan_results.txt" using the output redirection (>) feature of the command line. The text file contained the detailed information retrieved from the scans, including the IP addresses, services, hostnames, and operating systems.

Command uses :-

Nmap -A 192.168.7.154 >



Identifying Host Operating System:

Nmap's OS detection feature was used to identify the operating system running on a specific host. The -O option was used with Nmap to enable OS detection for the target host, which displayed the identified operating system.

```
root@ubuntu:~# nmap -O 192.168.7.154
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 10:19 PDT
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 89.45% done; ETC: 10:20 (0:00:07 remaining)
Nmap scan report for 192.168.7.154
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1521/tcp open  oracle
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.07 seconds
root@ubuntu:~#
```