VAPT REPORT

K N L Sri Vaishnavi
Cybersecurity
12/1/24

Vulnerability Assessment

And

Penetration Testing

Report

What is a VAPT report?

A vulnerability Assessment and Penetration Testing (VAPT) report typically includes detailed information about the assessment, identified vulnerabilities, and recommendations for mitigation.

Objective:

This vulnerability Assessment and Penetration Testing (VAPT) report outlines the findings and recommendations resulting from the assessment of the windows 7 and kali Linux virtual machines.

Scope:

This report gives a detailed outline about how a kali tool “nmap” is used for port scanning of windows 7 virtual machine installed in VMware.

Key findings:

In windows 7 and in Kali Linux:

By connecting the windows 7 and kali linux on the same network we found the number of open ports in windows 7.

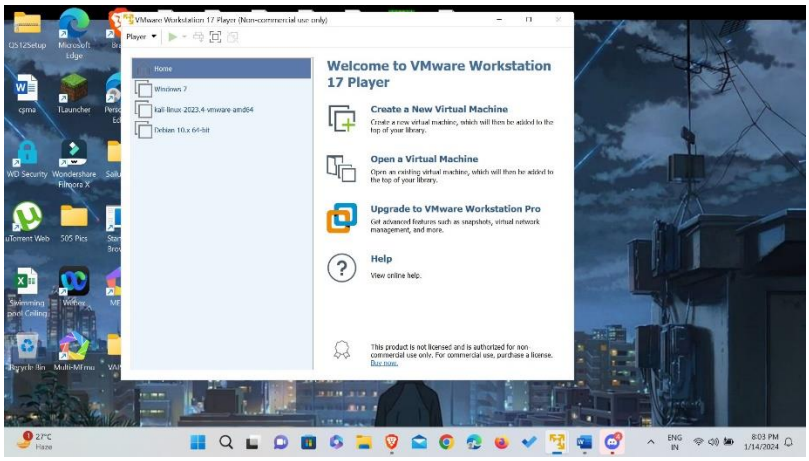
What is the use of using nmap?

Nmap is a pre-installed tool in kali Linux which is typically used for port scanning to gather information about vulnerabilities and assess them.

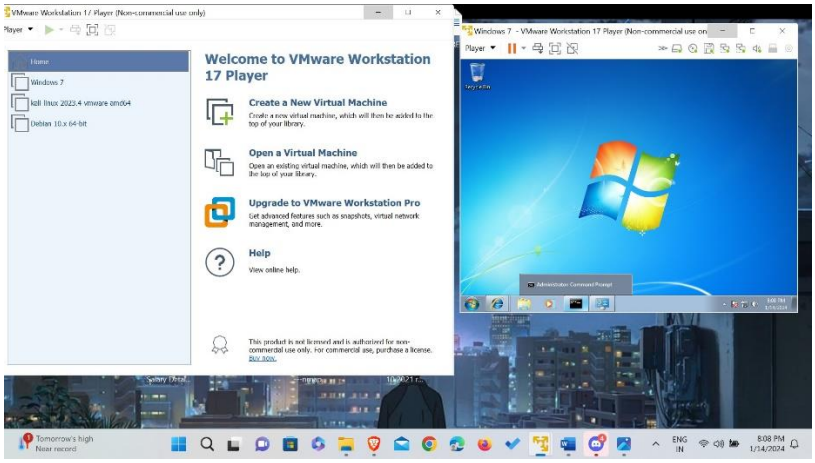
Tools used: nmap.

Steps to use nmap to scan the ports:

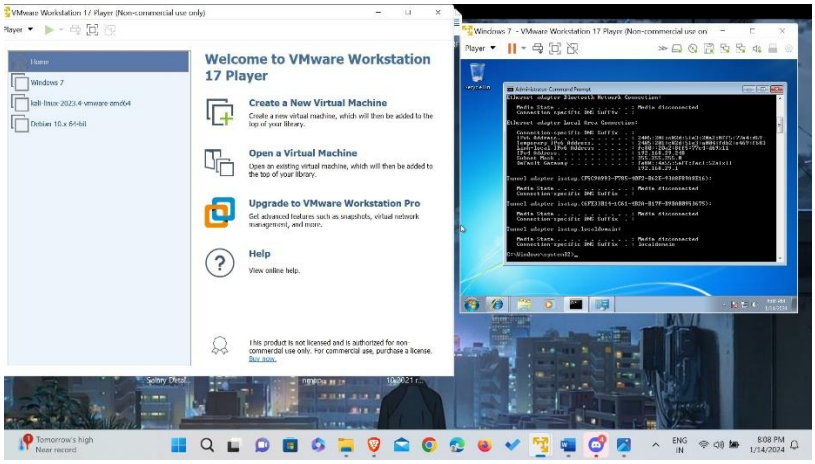
1.install windows -7 and kali Linux on VMware.



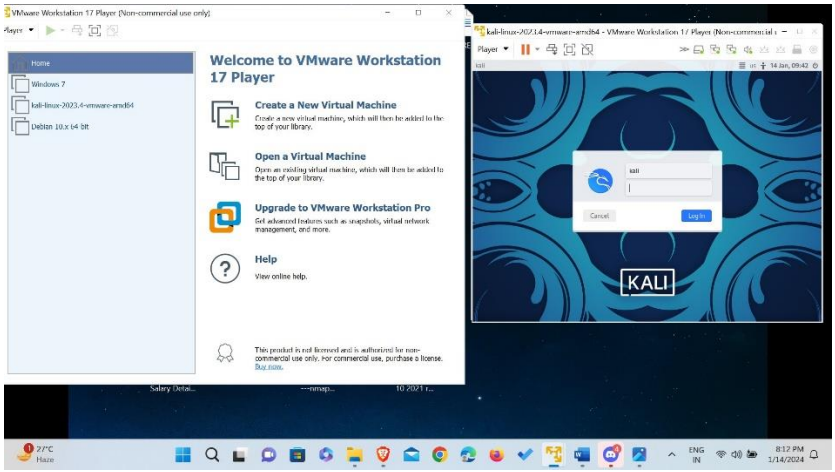
2.start windows 7:



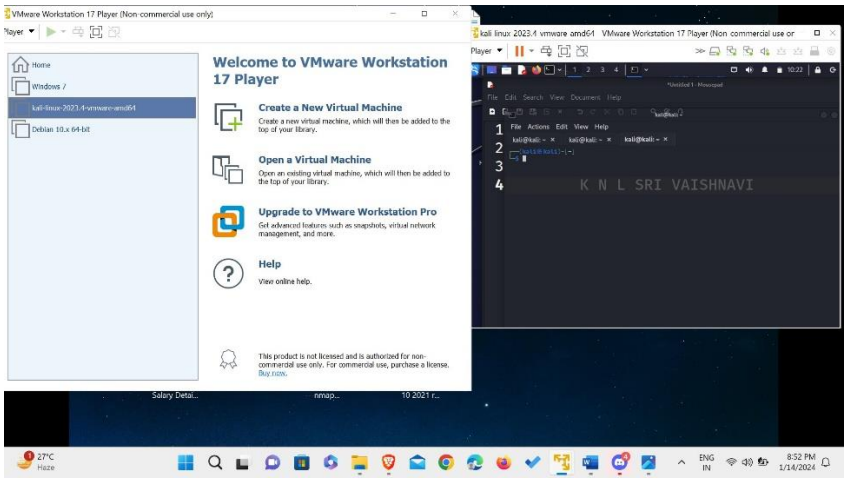
3.select command prompt and get the ip-address:



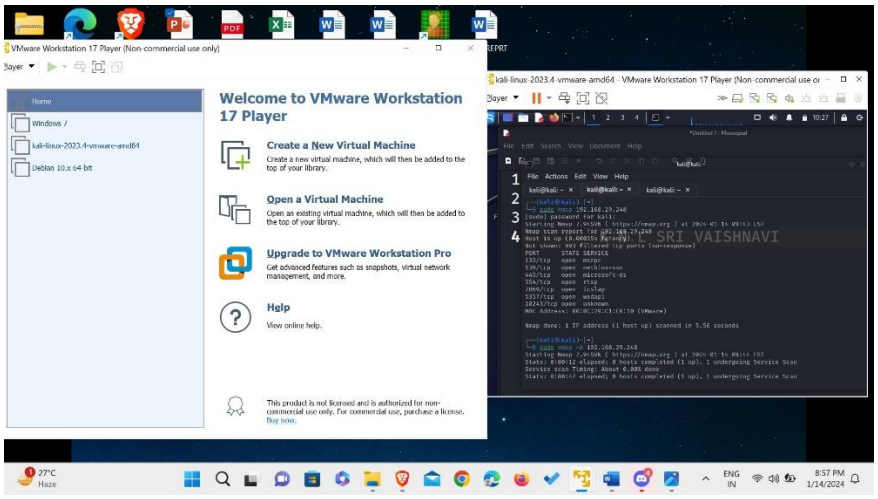
4.Now, open Kali Linux:



5.open terminal:



6.give the command to scan ports in the windows 7:



Explanation of the ports displayed in the terminal:

1.Port 135 (TCP/UDP) - Microsoft RPC (Remote Procedure Call):

Description: The Microsoft RPC service on port 135 is susceptible to remote code execution attacks, allowing an attacker to execute arbitrary code on a vulnerable system.

Risk Level: High

Recommendation: Firewall Configuration: Implement strict firewall rules to limit access to port 135 only to trusted systems.

Patch and Update: Regularly apply security patches and updates to the operating system and RPC service.

Network Segmentation: Consider network segmentation to isolate critical systems from potential threats.

2.Port 139 (TCP/UDP) - NetBIOS Session Service:

Description: Port 139 is associated with NetBIOS, which can be exploited for unauthorized access and file-sharing attacks.

Risk Level: Medium

Recommendation: Disable NetBIOS over TCP/IP:

If not needed, disable NetBIOS over TCP/IP to mitigate potential risks.

Use IPsec: Implement IPsec to encrypt communication over the network and protect against eavesdropping.

3.Port 445 (TCP) - Microsoft-DS (Directory Services):

Description: Port 445 is commonly targeted for attacks like the WannaCry ransomware, exploiting vulnerabilities in Windows SMB protocol.

Risk Level: High

Recommendation: Apply Security Updates:

Regularly apply security updates to address vulnerabilities in the SMB protocol.

Network Isolation: Isolate critical systems from untrusted networks to limit exposure to potential attacks.

4. Port 554 (TCP/UDP) - RTSP (Real-Time Streaming Protocol):

Description: Port 554 is associated with RTSP, which may be susceptible to unauthorized access or potential streaming-related vulnerabilities.

Risk Level: Low to Medium

Recommendation: Restrict Access:

Implement access controls to restrict access to the RTSP service to authorized users.

Update RTSP Server: Keep the RTSP server software up-to-date to address any security vulnerabilities.

5.Port 2869 (TCP) - UPnP (Universal Plug and Play):

Description: UPnP on port 2869 may expose devices to potential exploitation, leading to unauthorized access or device manipulation.

Risk Level: Medium

Recommendation: Disable UPnP:

If not needed, consider disabling UPnP to reduce the attack surface.

Firmware Updates: Regularly check for and apply firmware updates for devices that use UPnP.

6. Port 5357 (TCP) - Link-Local Multicast Name Resolution (LLMNR):

Description: LLMNR on port 5357 may expose systems to man-in-the-middle attacks or unauthorized name resolution.

Risk Level: Low to Medium

Recommendation: Disable LLMNR:

If not needed, consider disabling LLMNR to prevent potential attacks.

Use DNSSEC: Implement DNS Security Extensions (DNSSEC) for secure and authenticated name resolution.

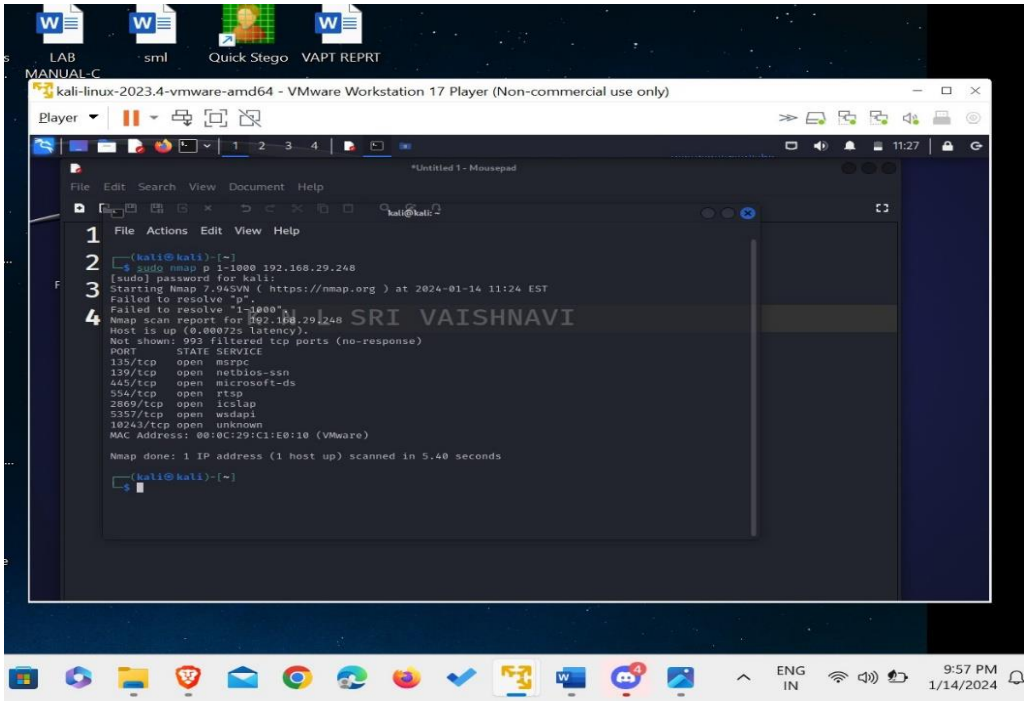
7. Port 10243 (TCP) - Reserved for future use:

Description: Port 10243 is currently unassigned and reserved for future use, and no specific vulnerabilities are known as of now.

Different commands which can be used in kali to gather information about ports using nmap:

1.Basic TCP Port Scan:

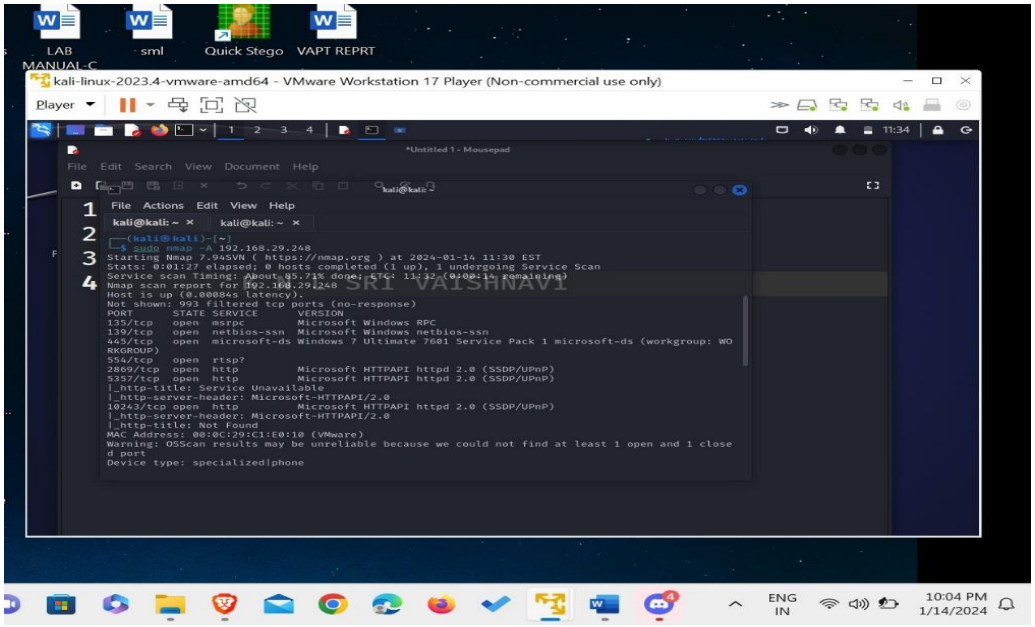
Purpose: Identify open TCP ports on the target system.



2.Aggressive Scan with Service Version Detection:

Purpose: Gather detailed information about open ports and services.

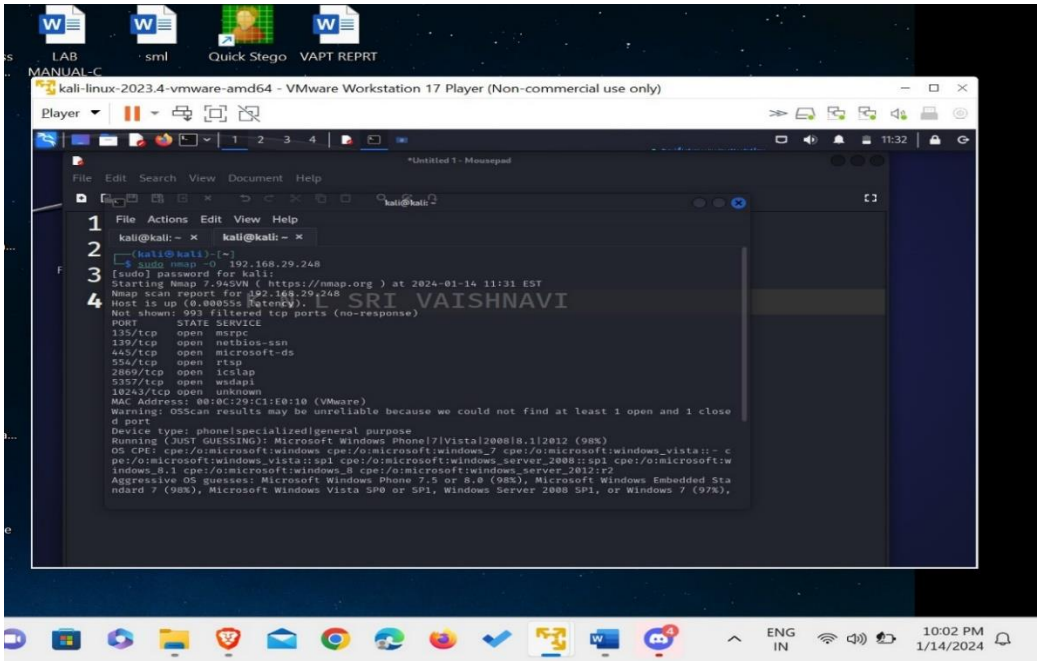
nmap -A <target_ip>



3. Operating System Detection:

Purpose: Attempt to identify the operating system of the target.

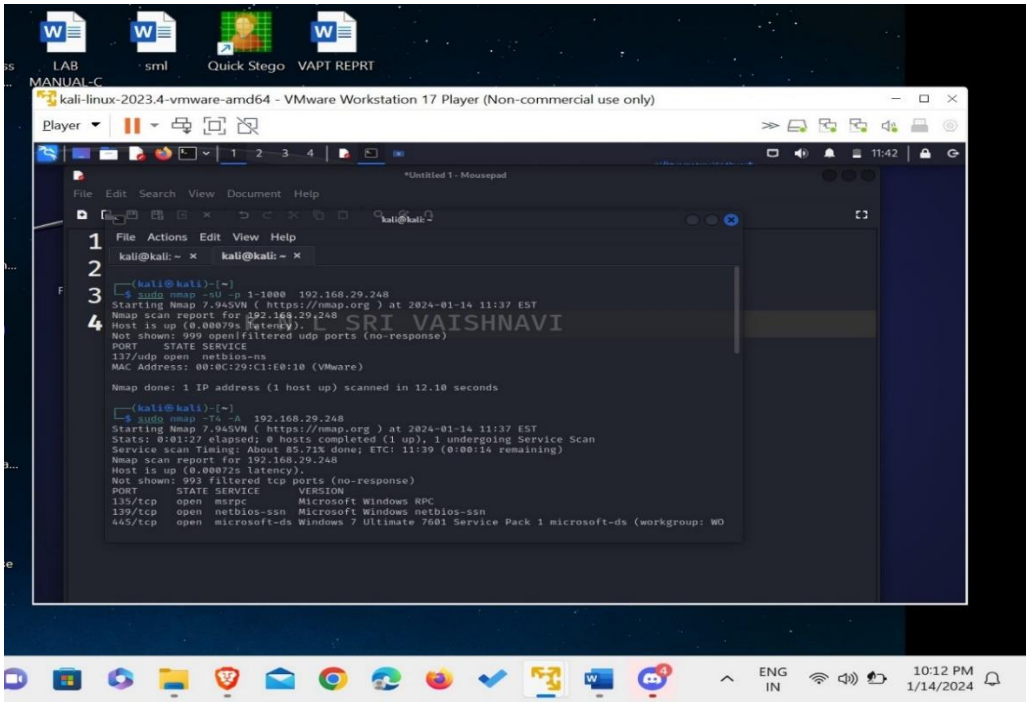
nmap -O <target_ip>



4. UDP Port Scan:

Purpose: Identify open UDP ports on the target system.

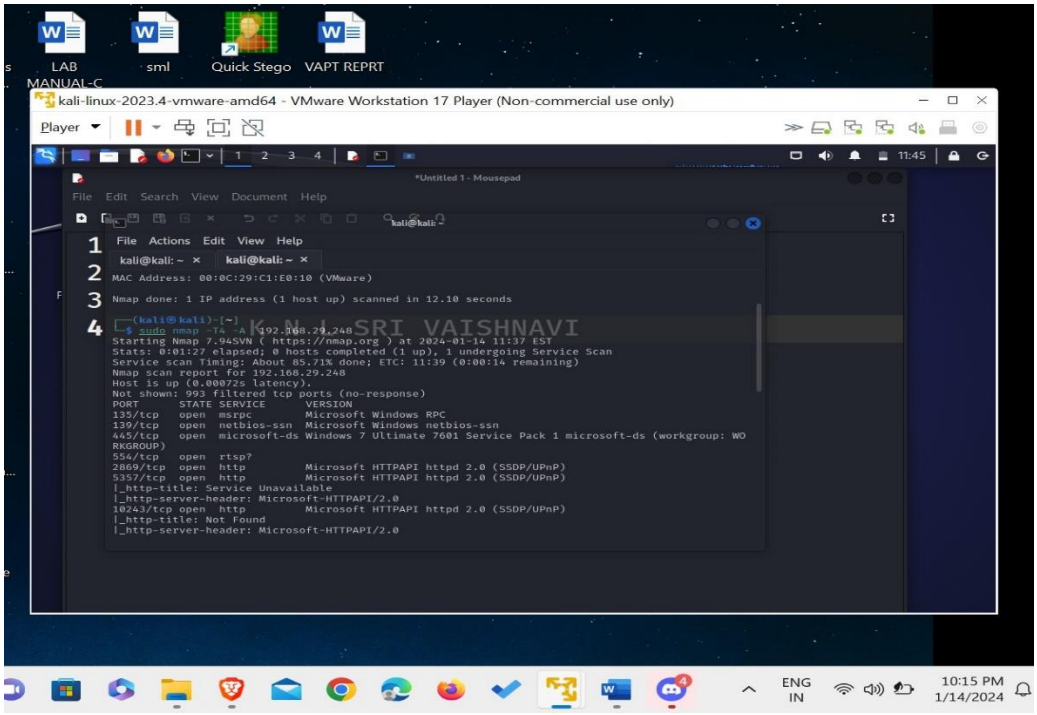
nmap -sU -p 1-1000 <target_ip>



6. Timing and Aggressiveness Control:

Purpose: Adjust the timing and aggressiveness of the scan.

nmap -T4 -A <target_ip>

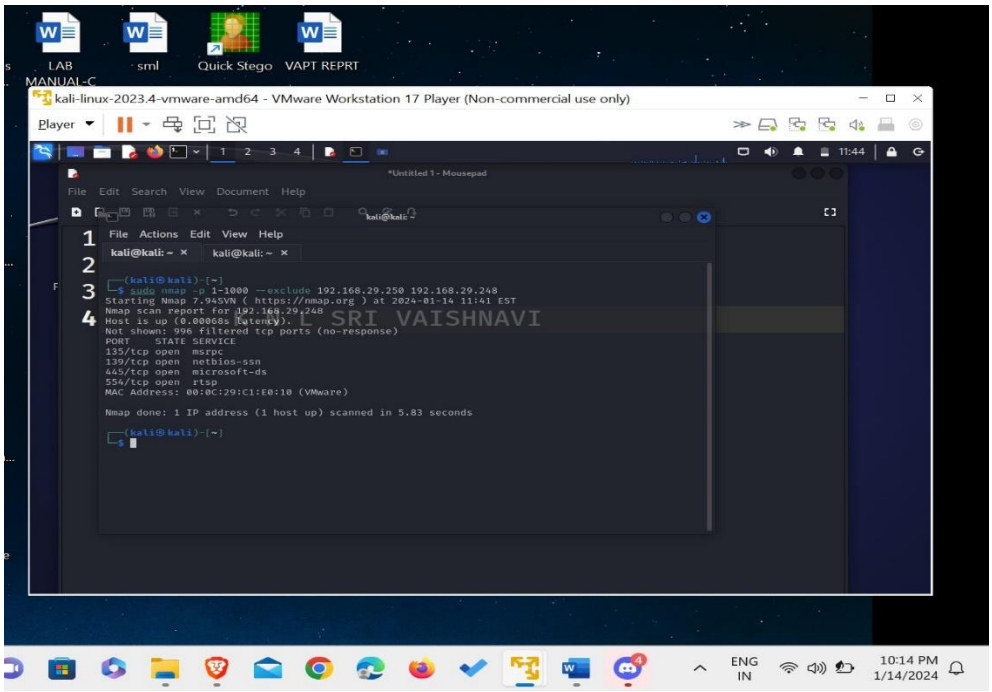


7. Exclude Hosts from Scan:

Purpose: Exclude specific hosts from the scan.

nmap -p 1-1000 --exclude <excluded_ip> <target_ip_range>

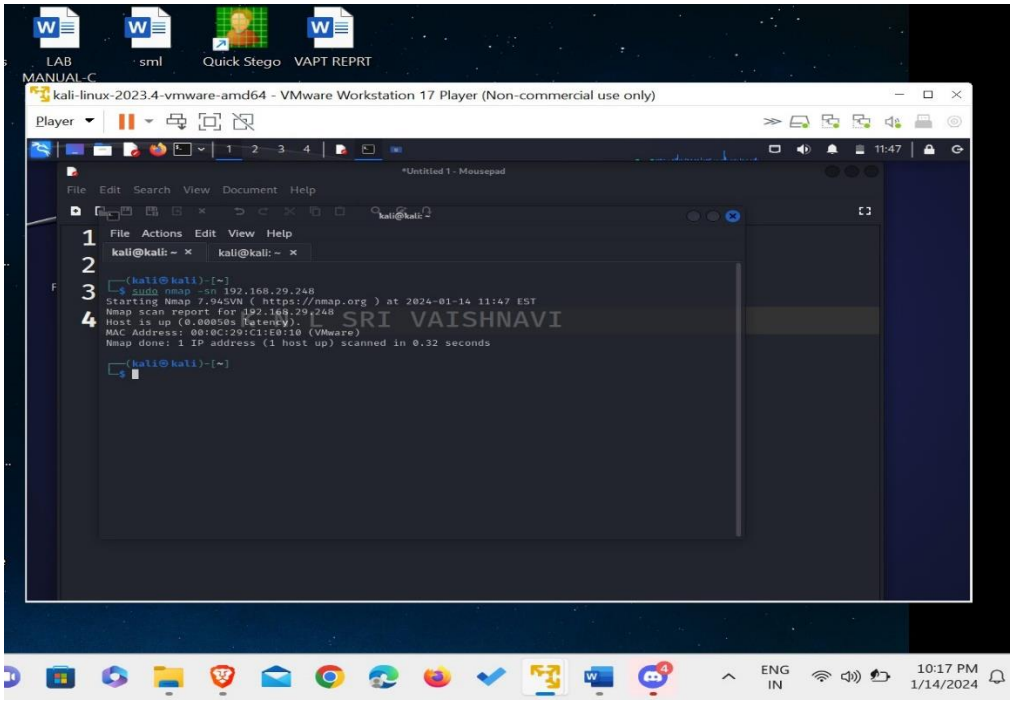
Output to a File (in XML Format):



8. Ping Scan (Check if Hosts are Up):

Purpose: Quickly check if hosts are online.

nmap -sn <target_ip>



Conclusion:

The Vulnerability Assessment and Penetration Testing (VAPT) report provided a comprehensive overview of the assessment conducted on the Windows 7 and Kali Linux virtual machines. The assessment focused on identifying vulnerabilities within the Windows environment and evaluating the security posture of the Kali Linux machine. For the Windows 7, vulnerabilities specific to its were identified, and potential attack vectors and weaknesses in configurations were explored.

THANK YOU.